IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 10, 2022, accepted January 21, 2022, date of publication January 26, 2022, date of current version February 4, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3146431

Improved Beetle Antennae Algorithm Based on Localization for Jamming Attack in Wireless Sensor Networks

YUCHENG LYU[1], YUANBIN MO[1,2], SONGQING YUE[3], AND WENWU LIU[1]

[1]Institute of Artificial Intelligence, Guangxi University for Nationalities, Nanning 530006, China
[2]Guangxi Key Laboratory of Hybrid Computation and IC Design Analysis, Nanning 530006, China
[3]Department of Computer Science and Software Engineering, University of Wisconsin–Platteville, Platteville, WI 53818, USA

Corresponding author: Yuanbin Mo (moyuanbin2020@gxun.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 21466008, in part by the Guangxi Natural Science Foundation under Grant 2019GXNSFAA185017, in part by the Innovation Project of Guangxi Graduate Education under Grant YCSW2022255, and in part by the School Level Scientific Research Projects under Grant 2021MDKJ004.

ABSTRACT When checking and sensing external communication data, wireless sensor networks are susceptible to interfering signals with different frequencies. In order to track the location of the jamming attack point and deploy security defense mechanism, a minimum covered circle jamming attack localization algorithm based on the improved beetle antennae search algorithm is proposed. By comparing the different nodes, the relative coordinates of jamming points which are taken as the initial position of the beetle are determined, judging the fitness values of left and right antennae. Meanwhile, by introducing adaptive step size strategy and adjusting the flight distance, the position of beetle is updated to avoid falling into local extremum. Combining with the characteristics of fast convergence of beetle antennae search algorithm, the optimal solution is found. Using this algorithm, the minimum radius of the circle covered by the jammed nodes and the position of the center of the circle are solved, and the location of the jammer is realized. Simulation results show that, the proposed algorithm is more efficient than the existing algorithm with regard to runtime complexity. The proposed algorithm also excels at lowering the error rate and increasing position performance in different distribution types of networks with different nodes densities and other external factors, the proposed algorithm has lower error rate, better positioning performance in different distribution types of networks with different node densities and other external factors. The runtime complexity of the algorithm is small and the error range is uniform, proving the effectiveness of the algorithm.

INDEX TERMS Wireless sensor networks, beetle antennae search algorithm, minimum covered circle, jamming attack localization.

I. INTRODUCTION

Wireless Sensor Networks (WSN) are a type of wireless network formed by self-organization and widely used in civil and military fields [1]–[4]. Distributed wireless sensor node groups are an important part of wireless sensor networks. The nodes with sensing and communication functions are deployed in or near the monitoring area responsible for collecting and transmitting data between sensors. Due to the exposed nature of wireless links, one critical security issue facing WSNs is jamming attacks targeting signal transmission. Jamming attacks are a special type of denial of service (DoS) attacks where malicious nodes interfere with normal communication among legitimate nodes by sending out interference signals. During the process of data transmission, wireless sensors are susceptible to jamming signals with different frequencies, which may greatly endanger the integrity and confidentiality of the transmitted data, eventually impacting the normal operation of network transmission [5]. The jamming attacks can cause a variety of adverse consequences on the sensor networks within their radiation range. Therefore, when jammers appear, how to quickly detect and accurately locate their attack locations has become an urgent issue to be solved.

A traditional countermeasure for jamming attack is to use the physical layer technology to find the location of jamming

The associate editor coordinating the review of this manuscript and approving it for publication was Lei Shu.

sources and implement the security mechanism, such as direct sequence spread spectrum (DSSS) [6]. However, this method usually comes with high cost and consumes large amounts of power, bandwidth, and storage resources. Researchers also proposed some jamming avoidance strategies to defend against attack signals, such as channel surfing and slot channel [7], but these strategies often cause high computational complexity and need the support of corresponding hardware equipment, resulting in more communication overhead and additional resource investment.

Seeking a method that can not only precisely locate where the jamming attack source is, but also save energy consumption, is currently an emerging research field. Rantna, *et al* proposed a neuro fuzzy disengagement scheme to prevent interference attacks in a WSN, ensuring data transmission by separating the malicious nodes. This method has high throughput and packet delivery ratio (PDR), low latency, but high overhead [8]. Recently, Hu *et al*, proposed centroid localization (CL), CL algorithm is an algorithm that calculates the centroid of the polygon composed of anchor nodes sending information as the coordinate position of unknown nodes, but the positioning accuracy is low [9].

In this paper, a novel algorithm based on range-free positioning is proposed to locate the single jamming source through the minimum coverage of the disturbed nodes in the sensor network. The objective of the research is to improve location accuracy and reduce computational complexity. The proposed algorithm is based on the beetle antennae optimization algorithm that beetle uses its two antennae to search the surrounding environment and move quickly to find the target solution. The rapid convergence of the beetle antennae optimization algorithm is combined with the accurate advantages of the minimum coverage circle to determine the center of the minimum coverage circle that can cover all disturbed nodes in the interference boundary. The algorithm assumes that there is a jamming boundary among specific nodes in the target network to analyze the distribution characteristics of nodes near the jamming area, consequently constructing a virtual node set on the jamming boundary. Using the minimum circle coverage algorithm of curve fitting, the estimated position of the jamming source is found as the initial position of the beetle; then the fitness values of the two antennae of the beetle are compared to determine the updated position. Next, according to the coverage of the jamming range to different types of nodes, some new virtual points are constructed and these points are then refitted and corrected. Meanwhile, the step size of the beetle position is dynamically adjusted to make the beetle moving forward to a more accurate interference source, and eventually the center position and radius of the jamming range are obtained. The simulation results show that the proposed algorithm has good positioning time consumption and positioning accuracy in different distribution types of networks and different node densities.

The main contributions of this study are as follows: ① a single jamming source localization algorithm is proposed based on the swarm intelligence optimization algorithm; ② the traditional beetle antennae algorithm is improved by step size adaptation to overcome the defect where the beetle may fall into the local extreme value during position update; ③ Experimental simulation shows that the positioning accuracy of the algorithm is higher than that of the existing mainstream algorithms, and the algorithm also maintains good results in time complexity and positioning errors with different node distribution types and different node densities.

The remainder of the paper is organized as follows. Section 2 provides an introduction to minimum covered circle (MCC), Beetle Antennae Search, and the improved algorithm of Beetle Antennae Search (IBAS). Section 3 explains in detail how IBAS works with the specific steps of minimum covered circle. In Section 4, we present the simulation and the results about jamming localization in wireless sensor networks. We will conclude our paper with final remarks in Section 5.

II. MODEL AND ALGORITHM

Jammer positioning issue has always been a hot topic in the field of wireless sensor networks. Attackers would block the normal communication of a WSN by deploying jamming sources in the network and performing radio frequency (RF) interference within their radiation range. Because the jamming signal is gradually weakened by factors such as surroundings and terrain during transmission, whether a sensor is being attacked by jamming can be determined according to the change of its communication state. Chowdiry [10] describes how the attackers rely on the detailed knowledge of the network and how the network relies on the detailed knowledge of the attackers, such as interference probability, so that it can be detected. P. Poplip [11] describes the effects of a jamming attack in a mobile dedicated environment where the jammer uses radio waves to interrupt the signals in and out of the mobile nodes. G. Pavani [12] has proposed the packet hiding methods to prevent selective interference attacks and an improved version of anti-interference attack methods. The key to ensure the complete operation of the network is to determine the location of the jamming attack point timely and accurately by the disturbed nodes and remove the impact of the jamming attack.

According to different parameters used, the positioning algorithms can be classified into ranging based positioning and range-free positioning [13]. The ranging-based method works by locating jammers according to the received communication parameter attributes, including received signal strength (RSS) [14], frequency difference of arrival (FDOA), time difference of arrival (TDOA) [15], acceptance rate [16] and their joint positioning technology [17], [18]. This method is relatively accurate in measuring the coordinates of jamming sources, but the errors in the actual communication signal collection process may affect the accuracy of positioning results. The ranging position in algorithm needs to measure the signal strength, arrival time difference and other attributes between network nodes, and estimate the jamming source based on the measured values. Because the communication capability of the node under jamming attack has been partially destroyed and additional hardware overhead is required, the ranging positioning algorithm is not suitable for the determination of jamming attack point.

The range-free method analyzes the location distribution characteristics of target network nodes and uses geometric calculation technology for location. The implementation method is comparatively simple, but the calculation error may fluctuate dramatically under various conditions. Virtual Force Iterative Localization [19] (VFIL), a range-free method, creates a circular jamming coverage using the centroid position and estimated jamming radius calculated by the CL algorithm. It uses the position of the interfered nodes and other nodes in the coverage to adjust the jamming coverage repeatedly until the final conditions are met. Cheng [20] *et al* have proposed a Double Circle Localization algorithm (DCL), which uses the minimum circumscribed circle and the maximum inscribed circle of the disturbed node to estimate the coordinates of the jamming source. The research based on range-free algorithms only need the positions of certain nodes and do not require distance, angle and other information between nodes. The methods have been proved effective in determining the approximate jamming point location, and reduce the overhead of power consumption and computing cost [21]. However, the main problem of range-free algorithm lies in the major location error in high-density WSNs. In recent years, many researchers have tried to combine range-free algorithms with signal ranging to propose new location algorithms. The positioning is extended to mobile jamming sources, directional jamming sources, and multiple jamming sources [22]. In addition, researchers also introduced optimization [23], [24] or clustering algorithm [25] for positioning.

In this paper, an improved beetle antennae minimum coverage location algorithm (IBAS) for range independent single interference source attack is proposed. The goal is to implement positioning in an intuitive way on the premise of less available parameters, so the algorithm could have improved accuracy and stability. Due to the impact of terrain, obstacles and other factors on the interference and communication signals in practical applications, the node signal coverage may vary significantly in different scenarios. In order to facilitate the analysis and comparison of algorithms, this paper mainly considers the deployment of network nodes under relatively flat terrain, and the coverage of interference is simplified to a circular area with the interference source as the center [26], [27].

A. THE MINIMUM COVERED CIRCLE PROBLEM

The problem of minimum covered circle was posed by Sylvester in 1857, which is an important analysis problem in mathematical application to find the minimum circle that can cover a set of points on the plane. For a given set of points on a plane $\{P_i\} = \{(x_i, y_i)\}$, $i = 1, 2, \ldots, n$, if there is a circle C so that all points P_i are in the circle or on the circumference, then circle C is the covering circle of the plane point set. Among all covering circles, the covering circle with the smallest radius is called the minimum covered circle of the point set. At present, one method to solve the minimum covered circle problem involves the concept of α-shell [28] in computational geometry, and the determination of α value is the challenge of this algorithm. Cutting-Plane method [29] is also used to solve the minimum covered circle problem, but this method suffers low calculation speed. Some intelligent optimization algorithms, such as the genetic algorithm can also be used to solve the minimum circle covering problem, but the algorithm is complex and the solution accuracy is relatively low [30]. This paper seeks to solve the problem of minimum covered circle based on the improved beetle antennae algorithm.

To solve the problem of minimum covered circle given the point set $\{P_i\}$ on a plane, the key is the determination of the center and radius of the circle. Therefore, the solution of the minimum covered circle problem is equivalent to finding the extreme value of the objective function, and the objective function is the fitness function. The objective function can be expressed as follows:

$$\begin{cases} (x_i - a)^2 + (y_i - b)^2 \leq r^2 \\ r \to \min, \end{cases} \qquad i = 1, 2, \ldots, n \tag{1}$$

where, (a, b) is the center of the minimum covering circle and r is the radius of the minimum covered circle.

B. BEETLE ANTENNAE ALGORITHM AND ITS IMPROVEMENT

In this sub-section, the traditional Beetle Antennae Search algorithm is introduced first and then the improved algorithm of Beetle Antennae Search is presented.

1) BEETLE ANTENNAE ALGORITHM

Beetle Antennae Search (BAS) [31] is a heuristic optimization algorithm proposed by Jiang and Li in 2018. The idea behind this algorithm is that, odors of prey are equivalent to a function, whose values are corresponding to different points in the space. The two antennae of beetles are able to collect the smell values of two points near themselves, so the beetles can find the point with the most distinguished smell. The specific location of prey is equivalent to the maximum point of the objective function, and the beetle moves towards the location with the distinguished odor step by step. Different from other optimization algorithms, BAS requires only one individual, that is, one beetle, which greatly reduces the amount of computation. Therefore, the process of beetle foraging is the optimization process of beetle antennae algorithm. The specific steps are as follows:

1). Set initial position direction vector of beetle:

$$\overrightarrow{dir} = \frac{rands(Dim, 1)}{\|rands(Dim, 1)\|} \tag{2}$$

where $rands(\cdot)$ is the random function and Dim is the dimension of space. Selection of step factor *step*: the initial step can be as large as possible, preferably equivalent to the maximum length of the independent variable. Eq. (3) is used in each iteration:

$$step_{t+1} = eta * step_t \quad (t = 1, 2, \ldots, n) \tag{3}$$

The value range of decline factor *eta* is between [0, 1], usually taken as $eta = 0.95$; t is the current number of iterations and n is the total number of iterations.

2). Calculate the position coordinates of left and right antennae of a beetle:

$$\begin{cases} x_l = x_t + \dfrac{d_0}{2} * \overrightarrow{dir} \\ x_r = x_t + \dfrac{d_0}{2} * \overrightarrow{dir} \end{cases} \quad (t = 1, 2, \ldots, n) \tag{4}$$

where, x_l represents the coordinate position of the left antennae, x_r represents the coordinate position of the right antennae, x_t represents the centroid coordinate of the beetle in the t-th times iteration, and d_0 represents the distance length between the left and right antennae. This paper sets its value large enough to cover part of the search interval: $d_0 = 3$.

3). Calculate the fitness function $f(\cdot)$, where $f(\cdot)$ represents the odor concentration values to be obtained, expressed as $f(x_l)$ and $f(x_r)$ respectively.

4). Update the beetle's position: by comparing the fitness values of left and right antennae; if $f(x_l) > f(x_r)$, then the beetle moves to the left; on the contrary, the beetle moves to the right. Next position update formula:

$$x_{t+1} = x_t - step * \overrightarrow{dir} * sign(f(x_l) - f(x_r)) \tag{5}$$

where, *step* represents the step size factor of t-th times iterations. In this paper, set the initial beetle step size $step = 1$ and $sign(\cdot)$ be the symbolic function to return the positive and negative of the parameter value.

2) IMPROVED BEETLE ANTENNAE ALGORITHM

According to the principle of traditional beetle antennae algorithm, two primary parameters affecting the performance of the algorithm are the step size of the beetle's position update and its moving flight direction. In order to achieve a better optimization effect in locating the jamming source, and to overcome the disadvantage of the traditional beetle antennae algorithm, which is the tendency to fall into local extreme value when updating the position, we adopted a dynamic adaptive strategy to calculate the step size of the beetle. According to Eq. (3), the step size of beetles decreases linearly. The larger the step size *step*, the stronger the global search ability; the smaller the step size *step*, the stronger the local search ability of the beetle. In addition, BAS algorithm has the disadvantage of slow convergence speed in the later stage. In order to ensure the calculation efficiency and overcome the above problems, so that the step size of beetle position update can be dynamically adjusted, Eq. (3) is changed as the step size of Eq. (6) to improve the performance of the algorithm [32], where $step_{\max}$ is the initial step size of beetle, and the length is 1.

$$step_{t+1} = step_t * \frac{\frac{step_{\max}}{eta} - temp}{5} \tag{6}$$

where, *temp* is used as the compensation value to enable *step* to accurately search in a small range in the later stage. Generally, *temp* is in the range of [0, 2]. After verification, $temp = 1.5$ is taken in this paper. In the early stage of algorithm optimization, beetle expands the search range in the solution space and quickly optimizes with a large step factor; In the later stage of algorithm optimization, after the search solution stabilizes, we let the beetle adopt the small step length factor in order to make the optimization more accurate. In order to more intuitively represent the length change of the two step updates, we use MATLAB to draw the change of each step length of the original step and the dynamically adjusted step as shown in Figure 1:

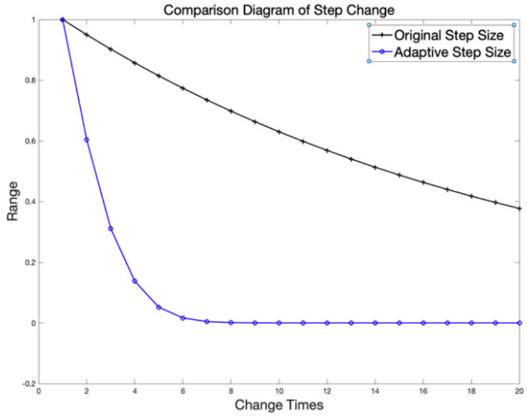

FIGURE 1. Comparison diagram of step decreasing.

It can be seen from Figure 1 that the step size of the typical beetle antennae algorithm changes uniformly every time. The beetle is easy to fall into local optimization due to its step size exploration within a certain range, resulting in solution errors. The step size adaptive strategy is introduced allowing the optimized BAS algorithm to search in a wide range of space at the beginning of search. When iterating half way through, the step length shortens quickly, which narrows the search range. In the later stage of iteration, the speed of step length shortening slows down, which increases its global search ability and improves the search accuracy. The main steps of the IBAS can be summarized in the pseudo code shown in Algorithm 1 below:

C. JAMMING LOCATION MODEL

When a jamming attack occurs in wireless sensor networks, an approximately circular jamming range centered at the jamming source will be generated. The sensor nodes within the jamming range are affected so that they are not able to transmit normal information with the nodes outside the jamming range. Although the signals from the communication nodes at the edge of the jamming range are weakened during the

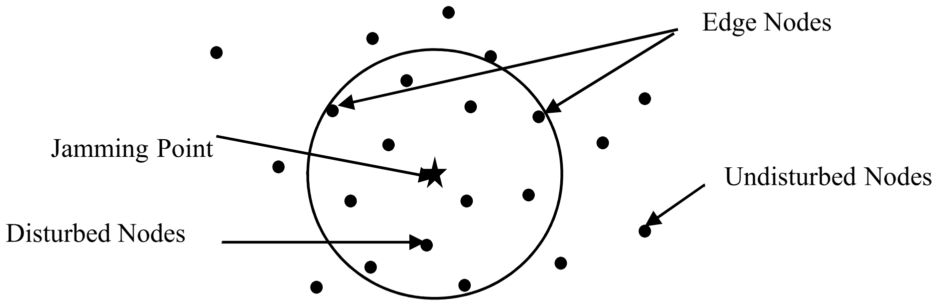

FIGURE 2. Signal jamming attack model.

```
Algorithm 1 IBAS Algorithm
Initialize the position of beetle $x = rands(k, 1)$;
Assign free parameters: distance between the beetle's two
antennae $d = 1$; step size $step = 1$; max iteration $n$; spatial
dimension $k$;
    1. Calculate the fitness of the $x$: $fbest = fitness(x)$;
    2. for $i = 1$ to $n$
            3. Initialization beetle direction vector
               $dir = rands(k, 1)$ by Eq. (2);
            4. Calculate the position of two beetle's
               antennae by Eq. (4);
            5. Initialization beetle antennae coordinate
               $xleft$ and $xright$;
            6. Calculate the fitness of the $xleft$ and $xright$;
            7. Compare $fleft$ and $fright$.
            8. Update the next position of beetle by Eq. (5);
    9. end for
    10. Adaptive step size $size$ by Eq. (6);
    11. $fbest\_store$ = the fitness of the best value;
    12. return $fbest\_store$;
```

attack, these nodes can still transmit some information with nodes being outside the range [33], so as to obtain the location of these disturbed nodes. Quickly finding the jamming source through these nodes and adopting the corresponding security mechanism are key to recover the normal communication of wireless sensor networks.

The target network is based on the following assumptions: it has a total of N nodes, which are arranged in a $L * L$ rectangular area according to certain distribution characteristics, and the communication distance between nodes is d. Node types include jamming source, undisturbed nodes, edge nodes and disturbed nodes. The edge nodes are the target network nodes at the edge of the jamming range that carry out some normal communication. The jamming attack model of wireless sensor networks is depicted in Figure 2:

We used packet send ratio (PSR) to distinguish the different nodes. The general calculation formula of PSR as follows:

$$PSR = \frac{m}{n} \tag{7}$$

where n represents the number of messages to be sent by the node and m represents the number of messages sent successfully. This paper implements this model in the following ways. In the normal operation state, the sensor nodes can obtain their own location information, send message data to adjacent nodes periodically while receiving ACK reply simultaneously. When under the influence of the jamming, the disturbed nodes will not be able to receive or send out data; therefore, causing some unsuccessfully sent messages, that is, $PSR = N_{ACK}/N_{send\_data}$. Where N_{ACK} represents the number of actually received ACK. N_{send_data} represents the number of all sent messages. The normal nodes PSR is approximately 1. The Edge nodes PSR is lower than the average value. The disturbed nodes $PSR = 0$. Then fit the jamming boundary accordingly.

Table 1 listed out the performance comparison and analysis of current jamming location algorithms.

As shown in Table 1, the computational complexity of Centroid Localization (CL) algorithm and weighted-CL algorithm is relatively low, but the positioning accuracy is also low, which could easily lead to unsatisfying positioning results; whereas the location based on signal strength and the minimum covered circle algorithms have strengthened the positioning accuracy, but the positioning times is high, so these algorithms are unable to provide real-time determination of the location of jamming attack. Furthermore, the minimum covered circle algorithm is not sensitive to node density, indicating that the algorithm may have good or bad positioning effects as node density varies. The minimum covered circle algorithm based on the improved beetle antennae algorithm (IBAS) proposed in this paper has high computational complexity, but combined with the characteristics of rapid convergence and optimization of beetle antennae, the positioning time of the algorithm remains fast with better real-time performance. The IBAS algorithm is able to estimate the position of the jamming source more accurately with the minimum covered circle positioning and it also resolves the problem that the minimum covered circle is not sensitive to node density.

III. SPECIFIC STEPS OF MINIMUM COVERED CIRCLE WITH IBAS

According to the signal jamming attack model of wireless sensor networks, the steps of determining the jamming source

TABLE 1. Performance comparison and analysis of current jamming location algorithms.

ALGORITHM	Computational Complexity	Positioning Accuracy	Node Density Sensitivity	Positioning Times
Centroid localization (CL)	Low	Low	Sensitive	Slightly Shorter
Weighted-CL	Low	Low	Sensitive	Long
Location based on Signal Strength	High	Middle	Sensitive	Long
Minimum Coverage Circle	High	Middle	Insensitive	Long
IBAS	High	High	Sensitive	Slightly Shorter

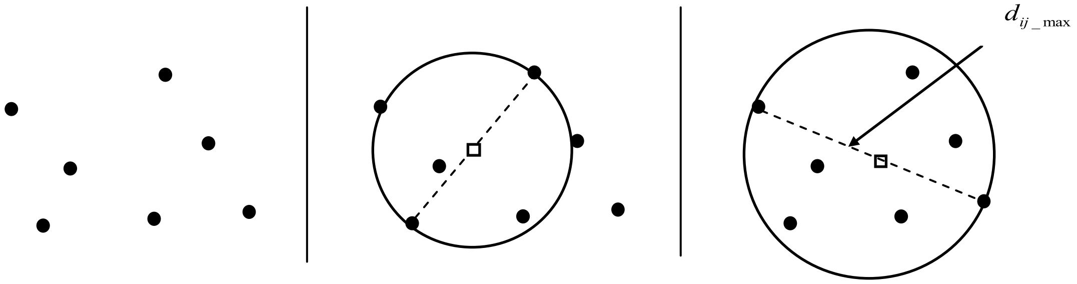

FIGURE 3. Solving disturbed points set and estimating jamming attack source.

attack location based on the minimum covered circle of the IBAS proposed in this paper are as follows:

STEP 1: It is assumed that the disturbed nodes point set is $P = \{p_1, p_2, \ldots, p_n\}$, the position coordinates of each point in point set P can be obtained: $S = \{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$. Calculate the distance $d_{ij}(i \neq j)$ of every two nodes whitin the point set in turn, and find the two nodes $p_i(x_i, y_i)$ and $p_j(x_j, y_j)$ with the longest distance. The distance of the two nodes is $d_{ij\_\max}$, with $(d_{ij\_\max})/2$ as the radius r_{d_ij}, and $O_{d_{ij}}$ as the center. Mark the midpoint $O_{d_{ij}}$ as the estimated position of the jamming attack source.

STEP 2: Take $O_{d_{ij}}$ as the center and make a circle with radius $r_{d_{ij}}$. Determine if there is a point k such that the distance is $d > ((d_{ij\_\max})/2)$ from point k to $O_{d_{ij}}$. If it exists, find the positional relationship between the point k and $P_j(x_j, y_j)$. If the two points are on the same side of the diameter, let k replace $P_j(x_j, y_j)$ and return to **Step 1**; on the contrary, if k and $P_j(x_j, y_j)$ are not on the same side of the diameter, make a circle according to the three points $(k, P_i(x_i, y_i), P_j(x_j, y_j))$, and the center of the circle is the estimated position of the jamming attack point. The calculation example is shown in Figure 3.

STEP 3: After determining and estimating the location of the jamming attack source, initialize the beetle. Place the beetle on point $O_{d_{ij}}$ to overcome the problem of randomness of the initial location of the beetle in the beetle antennae algorithm. Initialize the left and right antennae of the beetle, take the endpoints of the two antennae as trial points, calculate the distance from each disturbed node, and determine whether each point is included in the circle composed of the existing longest radius.

STEP 4: Compare the longest radius length $d_{left\_\max}$, $d_{right\_\max}$ and position recorded after the test of the left and right antennae of the beetle. At this time, the solution recorded by the two antennae of the beetle is the result of covering the positions of all disturbed points. If $d_{left\_\max} < d_{right\_\max}$, the next step is to fly the distance of the step size of the beetle in the left antennae's direction in the next step *step*; On the contrary, if $d_{left\_\max} > d_{right\_\max}$, the beetle needs to fly the distance of the flying step of beetle in the right antennae's direction *step*. The example of the calculation process is shown in Figure 4.

STEP 5: Each time the position of the beetle is updated, its position is more accurate from the position of the jamming attack point. At the same time, adaptively change the step size of the next flight of the beetle according to formula (6). After several iterations, when aimed solution accuracy is met, the location of the beetle is the location of the source point of the minimum covered circle jamming attack point $pbest(x\_best, y\_best)$.

The main steps of the improved beetle antennae jamming location algorithm flow in Wireless Sensor Networks in the pseudo code is shown in Algorithm 2 below.

IV. JAMMING LOCATION IN WIRELESS SENSOR NETWORKS

For the performance of the algorithm, the test examples in reference [30] and. Reference [34]–[36] are compared to genetic algorithm (GA) and minimum covered circle

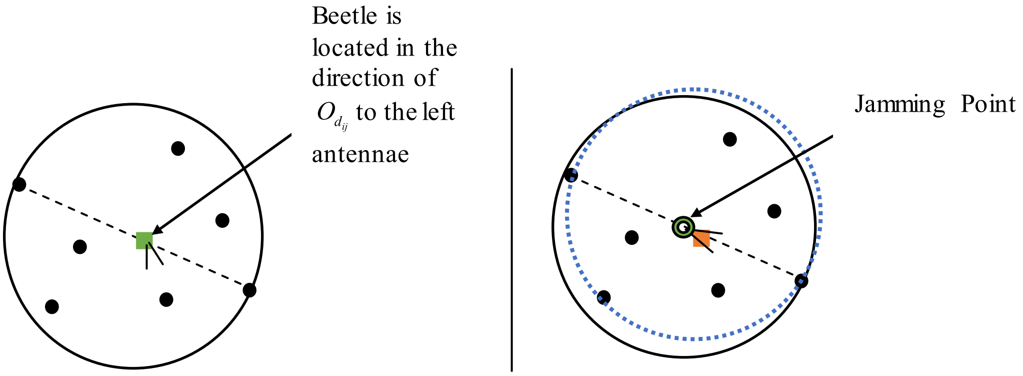
Beetle is located in the direction of $O_{d_{ij}}$ to the left antennae
Jamming Point

FIGURE 4. Accurately determine the jamming attack source.

algorithm (MCC). The reason to compare with the classical genetic algorithm is because the design idea of genetic algorithm is relatively simple to implement and the robustness of the algorithm can solve the minimum coverage; MCC algorithm is a common method to solve the minimum circle of a group of point sets on the covering plane. The algorithm can locate the center of the minimum covered circle with high calculation accuracy. Comparing these two methods with the algorithm in this paper has proved that the minimum covered circle based on IBAS has better performance. The algorithm runs for 5 times and the maximum number of iterations is 300 times. Each time, record the center coordinates of the circle solved, the minimum radius of the covered circle, the number of iterations for optimal value and the running time.

Firstly, the test is carried out from the low-density nodes. Case 1 uses 12 nodes. Table 2 shows the point set tested by case 1, and Table 3 presents the test results of IBAS algorithm and the comparison results of genetic algorithm. Figure 5 shows the minimum coverage result of IBAS algorithm, and Figure 6 demonstrates its convergence effect.

TABLE 2. Case 1. 12 points set coordinates.

Reference [30] Points set(12Points)		
(15.85, 6.05)	(33.65, 17.31)	(22.83, 2.07)
(29.82, 22.11)	(7.3, 10.43)	(26.28, 23.15)
(4.84, 20.32)	(28.15, 6.67)	(14.39, 30.24)
(25.47, 29.46)	(20.85, 11.47)	(30.24, 25.23)

A. CASE 1. 12 POINTS SIMULATION

According to the data of example 1, it can be concluded that in the case of low-density nodes, when compared to the classical optimization algorithm genetic algorithm, the minimum coverage radius obtained by IBAS algorithm is more accurate than genetic algorithm, reaching 14.7086. In terms of the number of iterations, IBAS algorithm needs to run 24 times to solve the optimal value. The genetic algorithm needs 87 times at most; In terms of test time, the shortest running time of IBAS algorithm is 0.041848 second. The good performance is attributed to the rapid convergence of BAS algorithm. The experiment results prove that IBAS algorithm operates well in low-density nodes.

Algorithm 2 Wireless Sensor Network Minimum Coverage Jamming Attack Location Algorithm Based on IBAS

```
Input: Disturbed nodes set $P$; two beetles' distance $d$; step size $step$; max iteration $nMax$;
Output: Best value of jamming source point $pbest$; minimum covered radius $rbest$;
Record the position of the disturbed point;
for $i = 1$ to $n$
    Calculate the distance $dis\_p$ between two different points;
end for
Record the shortest radius $r\_\min$ and the corresponding midpoint $o\_mid$;
Take $o\_mid$ as the center and $r\_\min$ as the radius to determine a circle;
Determine whether there are uncovered points;
Assign the head of beetle $tnx$ as the center of circle $o\_mid$;
for $i = 1$ to $nMax$
    Initialization beetle direction vector $dir = randperm()$;
    Initialization beetle antennae coordinate $xleft, xright$;
    for $j = 1$ to $P$
        Calculate the fitness of the $xleft$ and $xright$;
    end for
    Comparing the fitness values of left antennae $fleft$ and right antennae $fright$;
    Update step size $step$ and two beetles' antennae length $d$;
    Update the location of beetle:
        $tnx = tnx - step * \overrightarrow{d} * sign(fleft - fright)$;
end for
return $pbest$ and $rbest$
```

TABLE 3. Case 1. simulation results.

Serial Number	Algorithm	Center Coordinates	Minimum Coverage Radius	Number of Iterations	Computational Time/s
1	Reference [30] GA	(18.98174,16.27107)	14.71324	87	<1
	IBAS	(18.9785 ,16.2654)	14.7086	24	0.045375
2	Reference [30] GA	(18.98421,16.26316)	14.71451	103	<1
	IBAS	(18.9785 ,16.2654)	14.7086	84	0.044773
3	Reference [30] GA	(18.98341,16.26429)	14.71342	97	<1
	IBAS	(18.9788 ,16.2655)	14.7086	73	0.042345
4	Reference [30] GA	(18.97421,16.26997)	14.71415	189	<1
	IBAS	(18.9786 ,16.2654)	14.7086	65	0.041848
5	Reference [30] GA	(18.98607,16.27320)	14.71416	156	<1
	IBAS	(18.9787 ,16.2655)	14.7086	70	0.042146

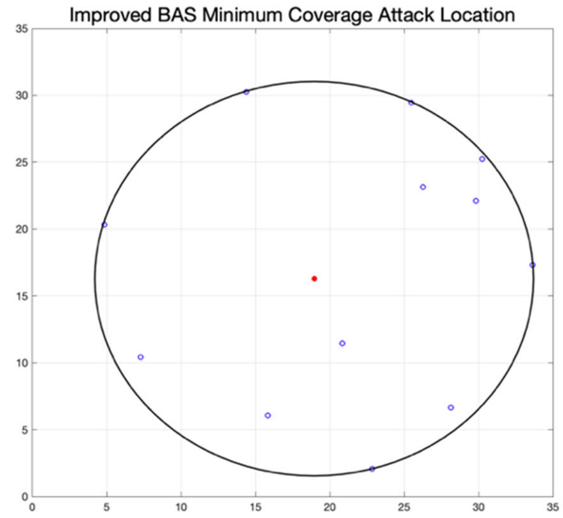

FIGURE 5. Case 1. minimum-coverage attack location.

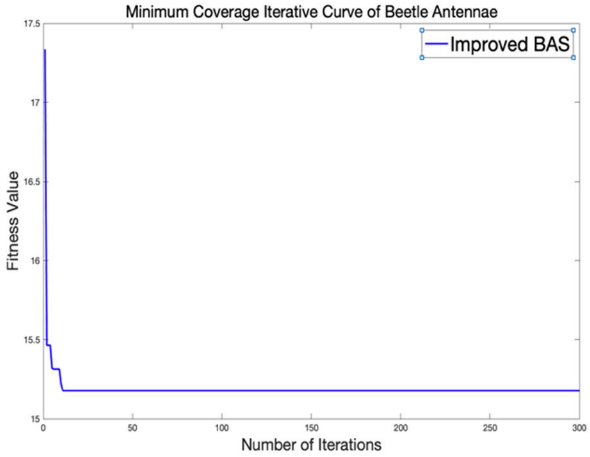

FIGURE 6. Case 1. iteration curve.

B. CASE 2. 32 POINTS SIMULATION

After identifying the algorithm has good optimization effect in low-density WSNs, we then test the performance of the algorithm in high density WSNs. This test is compared with the classical minimum covered circle algorithm (MCC), and the test results are shown in Table 4 with the position information of 32 coordinate points in test example 2. Table 5 shows the average results of IBAS algorithm running for 10 times and the comparison results with other algorithms. Figure 7 shows the coverage of IBAS algorithm tested in 32 nodes. Figure 8 is the convergence effect diagram of algorithm execution.

According to the test results of case 2, the algorithm continues to show good performance in high-density node distribution. The running time is obviously higher than that of MCC algorithm and can obtain the optimal solution in about 110 iterations. The radius of the locating point at the center of the circle is shorter than that in reference [34]–[36], which shows that IBAS algorithm is more accurate. The shortening of the radius of the covering circle makes the positioning of the center of the circle more accurate. These results are also reflected in Table 5.

Through the analysis of the above two examples, it is known that in the five simulation experiments with 12 nodes sets in case 1, the radius of the minimum coverage issue obtained by IBAS algorithm is shortened by $4.64*10^{-3}$, and the location origin is more accurate. The algorithm can find the optimal solution in an average of 65 times iterations, and the number of iterations is at least 22 times less than that of the genetic algorithm. In the test simulation time, the IBAS algorithm shows good time performance; In the 32 nodes sets in example 2, the difference between the radius of the minimum coverage point solved using the improved beetle antennae algorithm and the results in reference [34], [35] is not significant, but the difference is nearly 3mm shorter than the results found in reference [36]; In terms of running time, the simulation time of IBAS is the shortest, which is 0.05s shorter than that in reference [34] and one order of magnitude shorter than that in reference [36]. These two examples can further prove the accuracy of this algorithm for solving the minimum coverage problem in short running time and better

TABLE 4. Case 2. 32 points set coordinates.

Reference [34] Points set (32Points)			
(204.9828, 150.1991)	(136.7159, 216.9052)	(66.8602, 174.3448)	(129.9222, 72.3828)
(227.6585, 171.3656)	(126.4432, 238.4116)	(72.3845, 151.4579)	(147.2975, 76.6586)
(215.9072, 189.2778)	(122.3483, 210.8376)	(96.8459, 138.8606)	(170.2944, 76.9241)
(210.2828, 207.1864)	(110.8179, 214.3355)	(75.6791, 119.0414)	(185.8488, 74.4877)
(194.8090, 202.8531)	(110.3096, 197.0784)	(88.8851, 112.8175)	(195.8983, 88.0569)
(172.8174, 203.4304)	(90.6341, 207.9934)	(103.4154, 100.2979)	(212.0465, 101.6243)
(164.9391, 229.9750)	(71.8974, 196.6280)	(108.7343, 81.1323)	(207.7626, 122.7851)
(151.4924, 209.4311)	(98.8326, 166.8055)	(125.7083, 94.3556)	(223.3142, 137.4447)

TABLE 5. Case 2. simulation results.

Algorithm	Center Coordinates	Minimum Coverage Radius	Number of Iterations	Computational Time/s
Reference [34]	--	90.7312	--	0.016
Reference [35]	--	90.7312	--	--
Reference [36]	(148.1668,153.5580)	87.5902	--	0.145
IBAS	(148.16658060,153.55793589)	87.59024981	110	0.010997

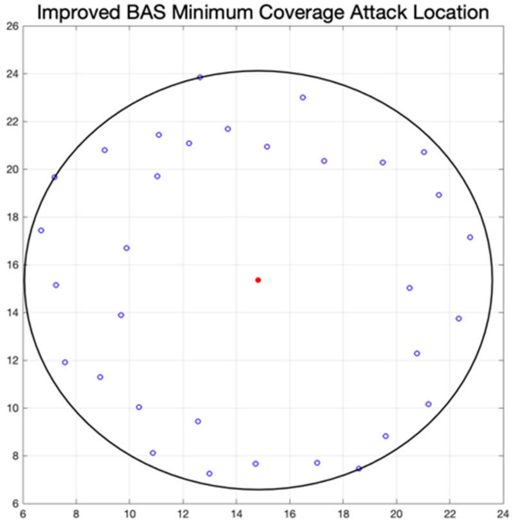

FIGURE 7. Case 2. minimum-coverage attack location.

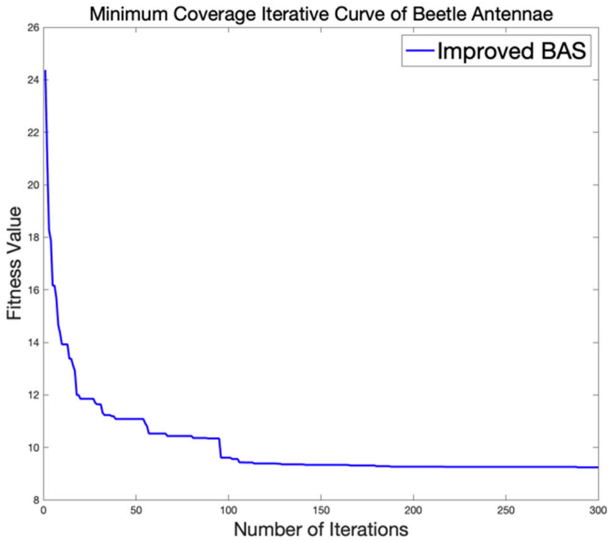

FIGURE 8. Case 2. iteration curve.

accuracy, and thus provide support to the idea of using this algorithm for attack location in wireless sensor networks.

C. CASE 3. JAMMING LOCATION IN WIRELESS SENSOR NETWORKS

Figure 9 shows a square wireless sensor network area with the size of 1000m ∗1000m simulated by MATLAB. The center coordinates of the square wireless sensor network area are (500,500), the coordinates of the lower left corner are (0, 0) and the coordinates of the upper right corner are (1000,1000). The sensor network nodes are randomly assigned within the boundary of this area. Set the center point (500,500) as the jamming attack point and the 375 units length as the interference radius, then all the points within the circle in Figure 9 are the interfered nodes. The sensor network nodes are randomly assigned within the boundary of the area.

The simulation experiment compares the incremental algorithm and $\alpha - MCC$ algorithm in reference [37]. Table 6 shows the jamming attack location determined by 10 times simulation tests after 600 sensor nodes are placed in the area.

It can be seen from table 6 that under the 10 times of simulations, the location of the jamming source is more accurate, and the radius length of the containment coverage circle is shorter, up to 370.2199. While the results of the incremental method and $\alpha - MCC$ algorithm fluctuate greatly, between 375-397, indicating that the improved beetle antennae algorithm in this paper is more stable and more accurate. In order

TABLE 6. Case 3. simulation results.

Times	Incremental Algorithm		α-MCC Algorithm		IBAS	
	(X, Y)	Radius	(X, Y)	Radius	(X, Y)	Radius
1	(490.6,485.1)	389.9	(481.1,493.3)	370.1	(495.7707,494.5528)	372.0039
2	(489.5,487.3)	383.0	(500.5,508.8)	382.9	(499.2306,499.0258)	371.3434
3	(488.1,501.1)	391.8	(499.1,503.6)	388.9	(495.7870,501.0632)	370.0295
4	(500.5,489.6)	383.4	(517.5,502.9)	380.3	(495.4294,500.1466)	372.2849
5	(508.2,494.3)	385.5	(496.4,493.7)	391.8	(496.6400,497.2140)	371.2439
6	(499.5,497.1)	377.4	(504.6,501.2)	396.8	(496.5982,495.1335)	370.2199
7	(494.0,503.1)	393.4	(501.6,487.5)	389.4	(499.4157,499.9860)	372.7444
8	(492.5,497.9)	386.7	(506.0,509.9)	385.3	(497.8775,499.7070)	371.3068
9	(494.9,494.5)	382.2	(496.2,488.2)	388.9	(504.8224,501.2826)	372.4436
10	(496.7,503.4)	397.1	(501.2,504.7)	375.9	(510.4361,502.9680)	371.6838

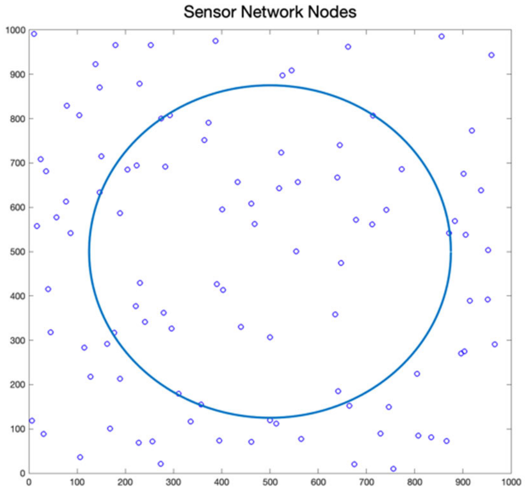

FIGURE 9. Disturbed attack area of sensor network.

to further verify the effectiveness of the IBAS algorithm in solving the minimum coverage jamming location accuracy of wireless sensor networks and shortening the location time, the location error and root mean standard deviation [38] (RMSD) are compared as an evaluation index of jamming attack location. The evaluation formula is as follows:

$$\sqrt{(X_i - \hat{X}_i)^2 + (Y_i - \hat{Y}_i)^2} \tag{8}$$

Formula. (8) is the positioning error, where the Euclidean distance between the estimated position $(\hat{X}_i, \hat{Y}_i)$ and the actual position (X_i, Y_i) of the jamming source is used as the positioning accuracy of each operation of the algorithm.

$$\sqrt{\frac{\sum_{i=1}^{k} ((X_i - \hat{X}_i)^2 + (Y_i - \hat{Y}_i)^2)}{k}} \tag{9}$$

Formula. (9) is the root mean standard deviation, which is the mean value of the sum of squares of the jamming attack source location error, and can reflect the deviation between the algorithm test result and the actual result. Where k is the total number of points. The comparison diagram of positioning error is shown in Figure 10.

According to the data in Table 6, root mean standard deviation of the incremental method is 10.6137, root mean standard deviation of the $\alpha - MCC$ algorithm is 11.6340, and the root mean standard deviation of the minimum coverage algorithm based on the IBAS algorithm is 5.4294. It can be seen from the comparison of Figure 10, the difference of the positioning error for solving the jamming attack positioning problem using the minimum coverage of the IBAS algorithm is smaller than that of the other two algorithms. In 10 times simulation tests, the maximum error of the incremental method reaches about 17.7; the maximum error of the $\alpha - MCC$ algorithm is about 20; and the maximum error of this algorithm is about 11.5. The error fluctuation is more gentle than other algorithms. Therefore, the deviation between the results of the proposed algorithm and the actual results is small, which further proves the effectiveness of solving the jamming attack location problem in wireless sensor networks based on the minimum coverage of the improved beetle antennae algorithm.

In order to explore the external environment and other factors affecting attack location, the performance of each algorithm under different conditions is analyzed and compared by changing the distribution type, node density (number) of the target network nodes.

1) INSPECTION INDEX

In the simulation experiment, the mean absolute error (MAE) and cumulative distribution function (CDF) are selected to evaluate the error between the test result and the actual value. The calculation formula is as follows:

$$MAE = \frac{1}{n} \sum\nolimits_{i=1}^{n} \sqrt{(x_i - x)^2 + (y_i - y)^2} \tag{10}$$

where, n represents the number of tests, (x_i, y_i) represents the jamming source coordinates estimated in the $t - th$ times test, and (x, y) represents the position of the actual jamming source.

$$CDF(x) = P(x \leq a) \tag{11}$$

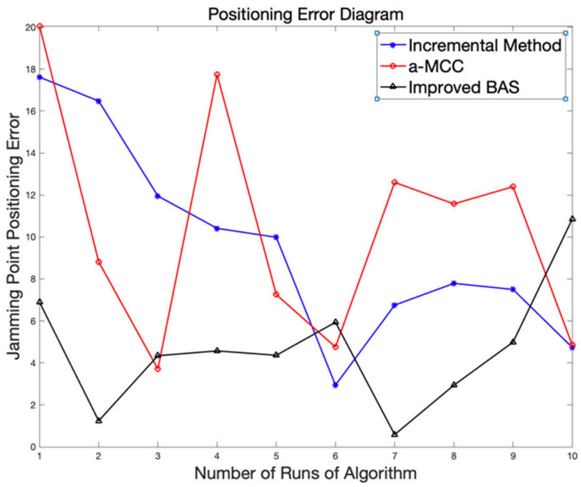

FIGURE 10. **Comparison diagram of algorithms positioning error.**

$CDF(x)$ represents the sum of the probability that the error of all results is not greater than a.

2) INFLUENCE OF NODES DISTRBUTION

The existing research on multi-hop wireless networks primarily adopts uniform distribution and Poisson point process distribution [39] (PPP) to construct simulation networks. Poisson point process is a counting process. The randomly sampled points obey uniform distribution in the range, and the distance between sample points obeys exponential distribution. Poisson point process distribution formula is as follows:

$$P\{N(B) = n\} = \frac{(\lambda\,|B|)^n}{n!} e^{-\lambda|B|} \tag{12}$$

where, λ is a given parameter, which can be called density; $|B|$ represents the mathematical region, that is, two-dimensional plane space. Then the number of random points $N(B) = n$ in region $|B|$ obeys Poisson distribution. At present, the existing research also has different construction methods for uniformly distributed networks, including the following two methods:

① Within the range of regional coordinates, N coordinates are generated, which are subject to the characteristics of random distribution. The point distribution generated in this way is more common. However, the randomness of node distribution is stronger, and the positioning calculation is relatively difficult. Moreover, if the number of points is too small, there may be only one or even no disturbed points in the jamming area. Therefore, the minimum number of nodes selected in this experiment is 100.

② Divide the target area into N grids of equal size, and then put a node at random in each grid. In doing so, the nodes distribution is rather regular and easy to locate and calculate, but the actual application may be limited.

In our study, we use the above two methods to generate uniform distribution network and Poisson point process distribution for different types of distribution networks. For the sake of distinction, the network generated by is ① called uniform network and the network generated by ② is called bisection network. Figure 11 shows three different distribution types of networks.

Firstly, the effects in different nodes distribution networks are compared. In the test example, the jamming radius is set as $r = 50m$, the number of nodes is $n = 300$, and the coordinate position of the jamming source in the center (150, 150) of the sensor network. The CDF curve of each positioning algorithm in the three types of sensor distribution networks is shown in Figure 12:

The experimental results show that the improved beetle antennae algorithm is superior to other algorithms in three different types of network nodes distribution. In the uniform distributed network, the calculation accuracy of attack location error is the best. Because the node distribution of bisection network is fairly regular, the jamming source tends to be in the center, so the calculation accuracy of the improved beetle antennae algorithm decreases slightly. In the distribution of PPP network, due to the relatively dense distribution of nodes in a certain range, the improved beetle antennae algorithm is still not uniformly distributed, and the calculation accuracy of the network is high, but still better than other algorithms.

3) INFLUENCE OF NODES DENSITY

In the above test, the jamming attack location of different network node distribution types is analyzed. The density of sensor network nodes is also an important factor affecting the location calculation. The positioning time efficiency and error results when the sensor network nodes increase exponentially are analyzed next. Similarly, the incremental method, $\alpha - MCC$ algorithm and CL algorithm are used for comparison. The jamming radius is set as $r = 50m$, and the number of wireless sensor network nodes is gradually increased from 100 to 1000. Figure 13 shows the time consumption comparison of the four algorithms. Figure 14 and Figure 15 are comparison diagram of the average error of the radius of the four algorithms in 10 times simulation tests in a uniformly distributed network. The closer the numerical value is to the zero point, the smaller the error is.

As can be seen from Figure 13, with the multiple increase of sensor network nodes, the time consumption of locating jamming attack points by incremental method and CL method increases significantly. The $\alpha-MCC$ algorithm and improved beetle antennae algorithm are less affected by the increase of nodes, and the time increases slightly. The time spent by the improved beetle antennae algorithm in locating the jamming attack source is shorter than that of the $\alpha - MCC$ algorithm, at about 122ms. The time consumed by the incremental method is about 2 times that of the algorithm, about 1.3 times that of the $\alpha - MCC$ algorithm, and about 2.2 times that of the CL algorithm. According to the theory, with the increase of node density, the accuracy of positioning error increases. As seen from Figure 14 and Figure 15, the MAE of the algorithm increases with the increase of the node density of the

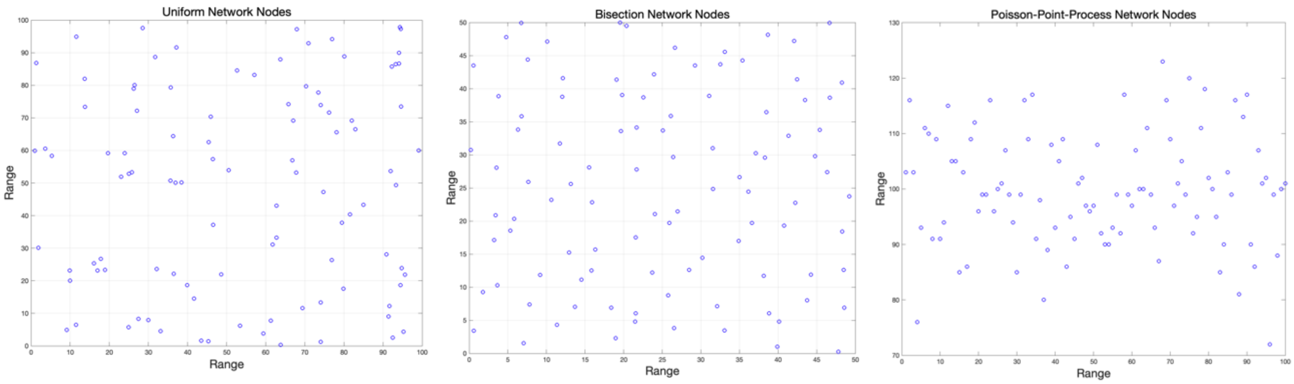

FIGURE 11. Different types of distribution networks.

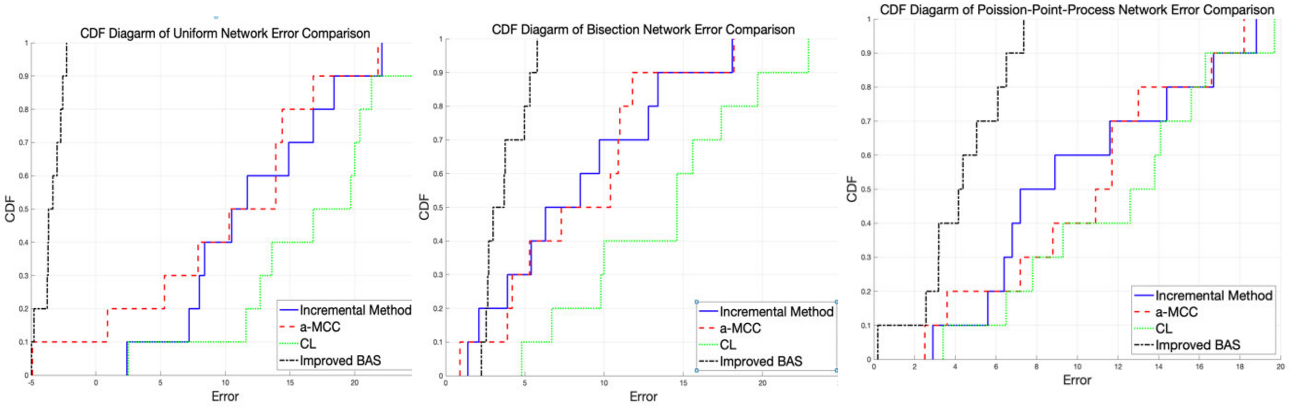

FIGURE 12. Location errors of different distributed network attack.

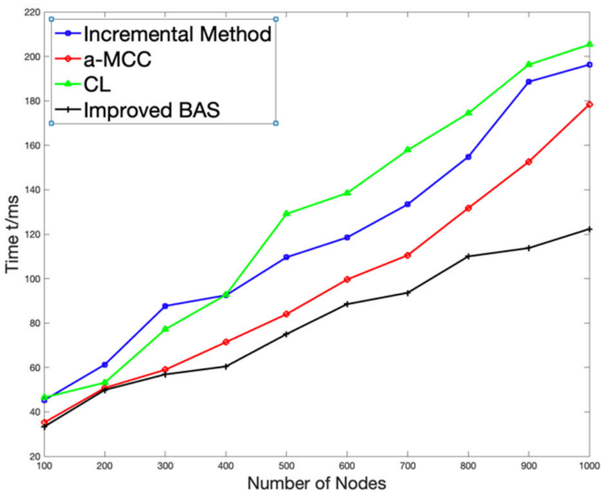

FIGURE 13. Comparison of algorithms time consumption.

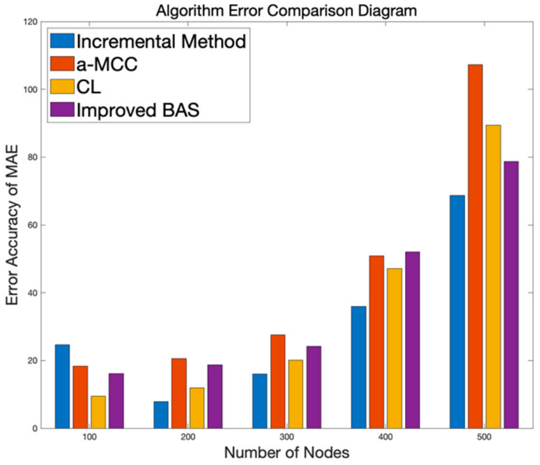

FIGURE 14. MAE values in uniform distributed networks (nodes: 100-500).

sensor network. This is because under different node densities, the setting of the number of iterations of the test example remained consistent at 300. The increase of node density will inevitably lead to the increase of time and complexity of the calculation process, so that the error of positioning calculation of all algorithms increases gradually under the condition of less iterations. However, under the condition of 200-1000 node density, the IBAS algorithm proposed in this

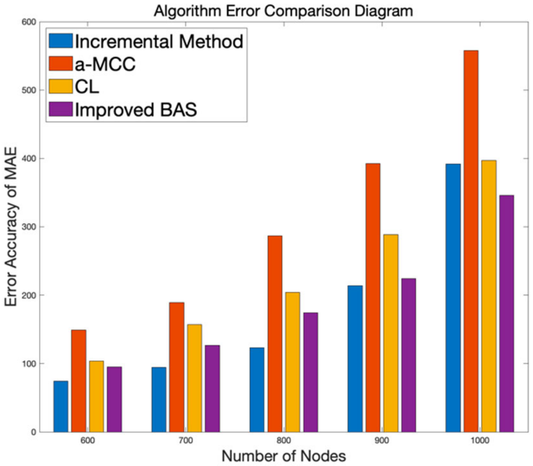

FIGURE 15. MAE values in uniform distributed networks (nodes: 600-1000).

paper has better performance, positioning accuracy and low error. At the same time, Figure 14 shows that when the node density is 100, the value of IBAS algorithm is at the highest, because the calculation result is positive in Formula. (7). In the simulation test, i) the jamming attack source located by IBAS is more accurate, ii) the measured actual point position is more accurate than other algorithms; iii) the positioning position is at a certain distance from the set circle point, which increases the value of MAE. In conclusion, IBAS algorithm has good performance in network distribution with different node density.

Under the condition of uniform node distribution, the comparison CDF diagram of different algorithm errors for different node densities (100-1000) is shown in Figure 16.

According to Figure 16, we can intuitively see the difference of cumulative distribution of solution results of different algorithms under different node densities. The four algorithms are relat ively the same in cumulative distribution. When the number of nodes is small, the error range of the four algorithms is small. IBAS algorithm has less error than the other three algorithms, and the error range is relatively uniform. When the number of nodes increases to $n = 600$, the error range of the four algorithms increases, IBAS algorithm still maintains good solution performance, and the error of $\alpha - MCC$ algorithm is better than CL algorithm and incremental method.

4) INFLUENCE OF ATTACK SOURCE ON JAMMING RADIUS

The jamming range of attack source of sensor network node is another important factor affecting location calculation. The following analyzes the impact of different jamming ranges on attack location in sensor network nodes.

Figure 17 and Figure 18 show the test results of the change of jamming radius in a uniform node distribution network. When $n = 300$ and the jamming source position is (500, 500), the jamming radius takes the positioning effect when $r = 30$, $r = 50$ and $r = 70$ in turn. The test CDF diagram and MAE diagram under different jamming radius are as follows:

As can be seen in Figure 17, regardless of how the jamming radius changes, IBAS algorithm always maintains the optimal result, and the calculation result is more stable than other algorithms. When the algorithm can cover all nodes, it can accurately determine the center of the minimum covered circle covering all nodes. In different node distribution networks, IBAS still shows good optimization results. The solution result of algorithm $\alpha - MCC$ is the second. It can be seen from the analysis and comparison of Figure 18, the average absolute error of IBAS algorithm in PPP network is larger than that of the other two node distribution network models. This is because the distribution density of nodes in PPP network is relatively complex, resulting in the increase of average absolute error. The performance of CL algorithm and incremental algorithm is less ideal. It can be proved that the IBAS algorithm still has good performance under different jamming radius.

After discussing the impact of different node distribution models, different node densities and different jamming radius on the sensor network nodes, in order to describe the model of the sensor nodes more accurately after jamming attack, the impact of the jamming signal strength on the sensor network nodes is further analyzed.

According to the actual situation, when the jamming attack signal is generated, the sensor nodes near the jamming source are subject to strong jamming signal, and there are many affected nodes near the jamming source. When the jamming signal arrives at a node far away from the jamming source, then jamming intensity is low, and fewer nodes are disturbed in the long-distance range. Based on this observation, a multivariate normal distribution model [40] is proposed to simulate the jamming intensity of attack sources.

Multivariate standard normal distribution, also known as multivariate standard Gaussian distribution, is the extension of one-dimensional normal distribution to multi-dimensional. If random variable $X \sim N(\mu, \sigma^2)$ exists, then there is a probability density function:

$$\begin{aligned} P(x) &= \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}(z)^2} \\ 1 &= \int_{-\infty}^{+\infty} P(x)dx \end{aligned} \tag{13}$$

If the element of Formula. (13) changes, the random variables $Z \sim N(0, 1)$ obey the univariate standard Gaussian distribution and its mean value $\mu = 0$, variance $\sigma^2 = 1$, and its probability density function is:

$$P(z) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}(z)^2} \tag{14}$$

The probability density function of multivariate standard Gaussian distribution is derived from formula 14. Suppose that the random vector is $\overrightarrow{Z} = [Z_1, Z_2, \ldots, Z_n]^T$, where $Z_i \sim N(0, 1)(i = 1, 2, \ldots, n)$ and $Z_i, Z_i(i, j = 1, \ldots, n \wedge i \neq j)$ are

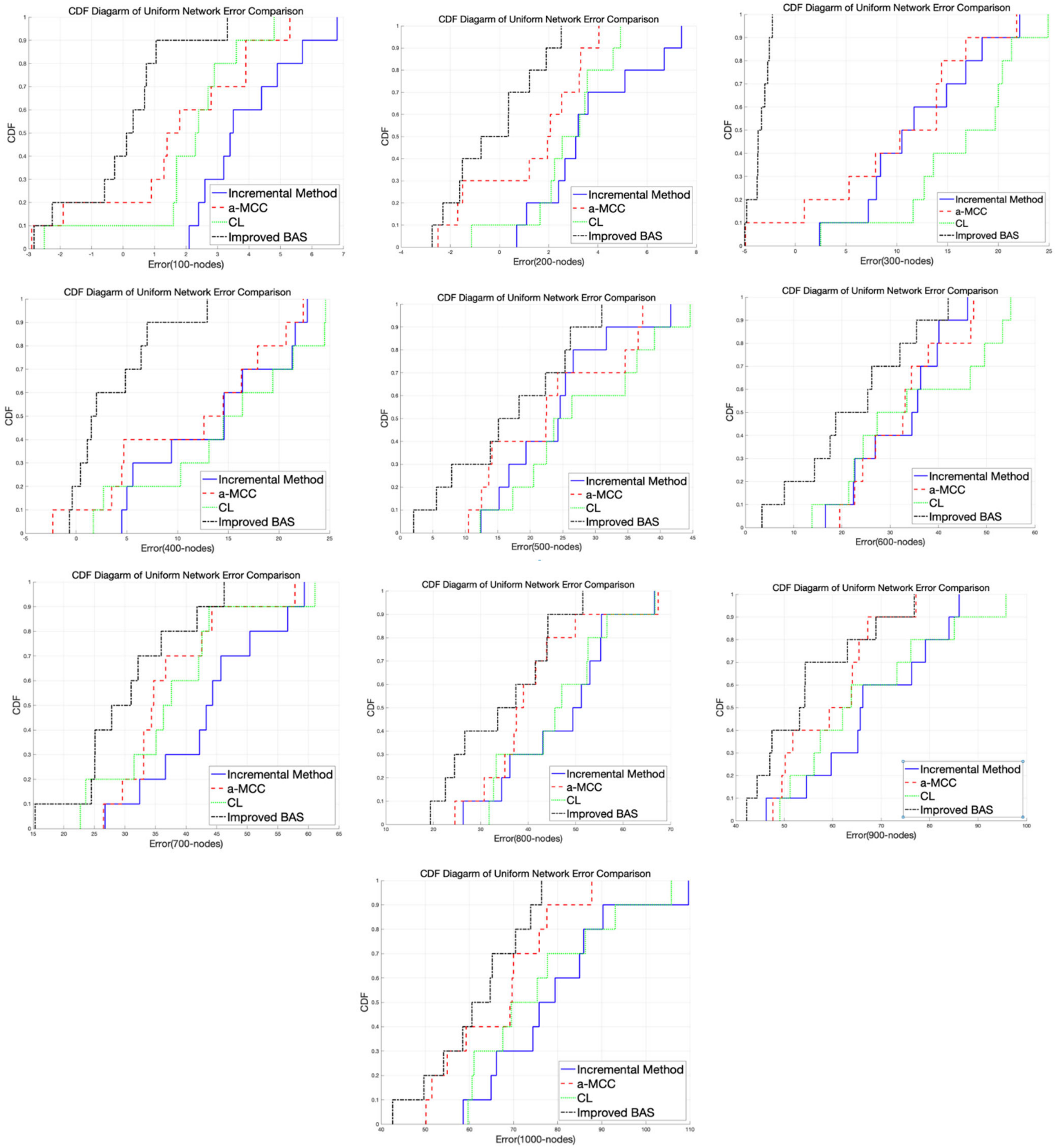

FIGURE 16. CDF values of different node densities in uniform distributed networks (nodes: 100-1000).

independent of each other. That is, each random variable Z_i in the random vector obeys the standard Gaussian distribution and is independent of each other. Then, from the relationship between Formula. (14) and the probability density function of independent random variable, the joint probability density function of random vector $\overrightarrow{Z} = [Z_1, Z_2, \ldots, Z_n]^T$ is obtained as follows:

$$P(z_1, \ldots, z_n) = \frac{1}{(2\pi)^{\frac{\pi}{2}}} e^{-\frac{1}{2}(Z^T Z)} \tag{15}$$

$$1 = \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} P(z_1, \ldots, z_n) dz_1 \ldots dz_n \tag{16}$$

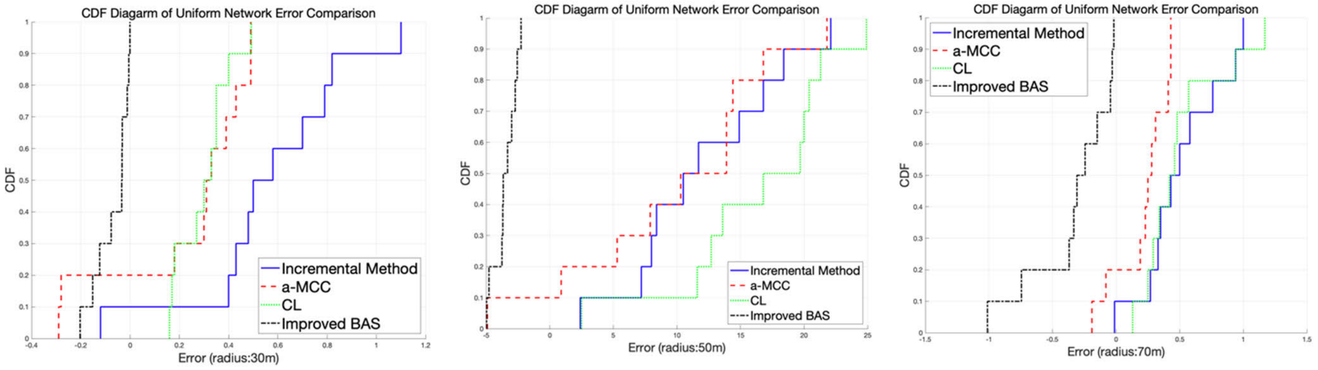

FIGURE 17. Location errors of different jamming radius(radius: 30m-70m).

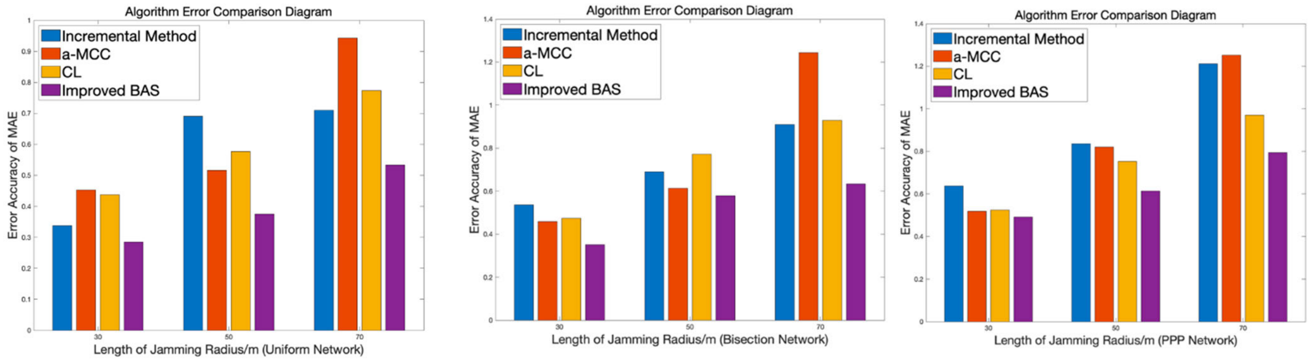

FIGURE 18. MAE values of different jamming radius in different nodes distribution models(radius: 30m-70m).

The random vector $\vec{z} \sim (\vec{0}, I)$ obeys the Gaussian distribution with the mean of zero and the covariance matrix of identity matrix. Since the random vector is $\vec{z} \sim (\vec{0}, I)$, the diagonal element of the covariance matrix is 1 and the other elements are 0. Take the constant $c = P(z_1, \ldots, z_n)$, then the contour of the function $P(z_1, \ldots, z_n)$ is $c' = Z^T Z$. When the random vector $\vec{z}$ is a two-dimensional vector, there are:

$$c' = Z^T Z = (z_1 - 0)^2 + (z_2 - 0)^2 \tag{17}$$

It is known from Formula. (17) that its contour line is a concentric circle centered on $(0, 0)$. The model diagram of simulating disturbed nodes with different intensities is shown in Figure 19 as follows:

Through the nodes generated by multivariate Gaussian distribution, the jamming intensity of the disturbed nodes caused by the jamming signal of the attack source is simulated. In the case of location calculation, the jamming source center is selected as $(500, 500)$ to verify the node in the case of jamming intensity. According to the multivariate standard Gaussian distribution, a total of 300 sensor nodes are generated. Combined with the IBAS algorithm these nodes are simulated and tested to locate the location of the jamming source. The algorithm runs 10 times. Take the coordinate point deviation as the inspection standard:

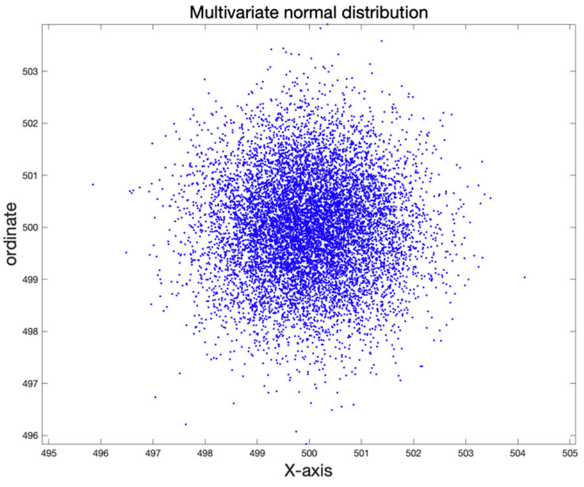

FIGURE 19. Multivariate normal distribution.

$$E = (x_i - x_0)^2 + (y_i - y_0)^2 \tag{18}$$

The test results are as follows in Figure 20 and Figure 21.

Based on the test results, for the positioning test of the interference signal generated by the attack source affecting

TABLE 7. Case 3. comprehensive analysis.

Algorithm	Error Range of Network Node Distribution Type/m		
	Uniform Network	Bisection Network	PPP Network
Incremental Method	(2.4,22.1)	(2.1,18.1)	(2.9,18.8)
$\alpha-MCC$	(-4.9,21.8)	(0.9,18.2)	(2.5,18.2)
CL	(2.5,24.9)	(4.8,19.7)	(3.4,19.7)
IBAS	(-4.9705, -2.2556)	(2.2556,5.7801)	(0.1907,7.3673)

Algorithm	Node Density (1000-6000)		Different Jamming Radius(30m-70m)		
	Error Range/m	Time/ms	30m: MAE	50m: MAE	70m: MAE
Incremental Method	18.2 → 7.4	(180,1085)	0.3378	0.6912	0.7101
$\alpha-MCC$	17.7 → 5.5	(172,379)	0.4522	0.5159	0.9432
CL	20.9 → 9.6	(184,1385)	0.4379	0.5771	0.7735
IBAS	15.4 → 4.9	(152,242)	0.2846	0.3752	0.5334

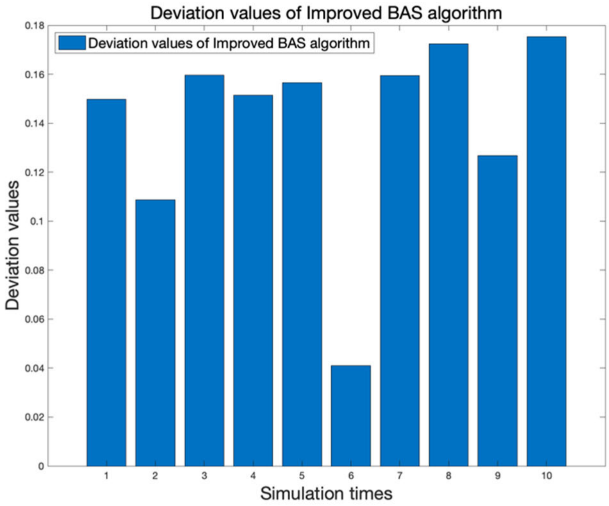

FIGURE 20. Deviation values of location.

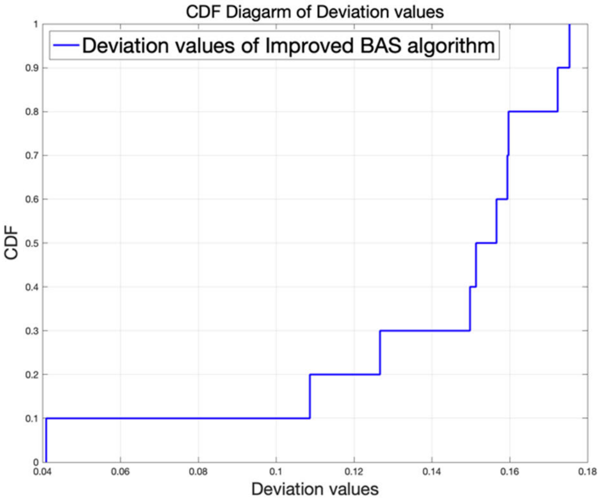

FIGURE 21. Multivariate standard Gaussian distribution deviation.

the nodes with different degrees of interference intensity, the improved beetle antennae algorithm still has good positioning ability. The positioning deviation is uniform and has high positioning accuracy in all 10 tests. The result further verifies the effectiveness of the improved minimum coverage method proposed in this paper. The comprehensive statistical analysis of the algorithm is shown in Table 7.

According to the statistical results in Table 7, the improved beetle antennae minimum coverage attack location algorithm is performing well in locating wireless sensor network attack location, and the location error range is more accurate than other algorithms in different types of network node distribution; In high-density nodes, the positioning time is nearly 30ms shorter than other algorithms, and the positioning error is still less. Under different jamming radius, the accuracy of IBAS algorithm is nearly 0.1 unit better than that of other algorithms when the jamming radius is 30m. When the jamming radius is 50m, the accuracy is at least 0.1 unit higher. When the jamming radius is 70m, the accuracy is nearly 0.2 units higher. Through comparative analysis, we have proved the improved beetle antennae minimum coverage algorithm is an effective solution for locating the attack source promptly when the interference signal occurs in the wireless sensor.

V. CONCLUSION AND FUTURE WORK

In order to more accurately determine the location of a jamming attack source in wireless sensor networks, we have proposed the IBAS algorithm that is able to perform the radius search of jamming signals and locating the position of jamming attack sources taking advantage of fast convergence of individual search of the original beetle antennae algorithm. We performed a series of simulation tests to verify the effectiveness of the IBAS algorithm. In test 1 with 12 points set, when compared with the genetic algorithm, the IBAS algorithm has faster convergence speed, the simulation time is shortened to 0.041848s, and the minimum coverage radius is further shortened to 14.7086. In case 2 with 32 points set, the result show that IBAS algorithm still has the capability to cover all points and the minimum coverage radius. These two examples provide the proof for the effectiveness of the algorithm as a solution to localizing the jamming source in wireless sensor networks.

In addition, we have also tested the performance of the IBAS algorithm with different node distribution types, with the increased number of nodes, with low-density and high-density nodes, with different interference radius of the sources, and with different interference signal strength. We compared the performance with some traditional methods for solving the same problems including incremental method and centroid location method. The IBAS algorithm shows faster positioning speed and more accurate positioning, which provides a solution for quickly finding the location of a jamming source and taking defense measures in time when sensor network nodes are being attacked by interference signals. The traditional centroid localization algorithm has lower computational complexity than the IBAS algorithm, which is what we still need to overcome and improve.

For further research objectives, we will firstly extend our solution to tackling the problem involving multiple jamming sources i.e., to locate the jamming sources when multiple jamming sources are in the presence. Secondly, with the continuous development of engineering technology, the attack jamming source may not appear in a plane. How to establish a positioning model in three-dimensional or even high-dimensional space to find its location is another area that needs us to explore and study.

REFERENCES

[1] Z. Zhou, Y. Wang, P. Li, X. Chang, and J. Luo, "Node location privacy protection in unattended wireless sensor networks," *Math. Problems Eng.*, vol. 2021, pp. 1–17, May 2021, doi: 10.1155/2021/5539382.

[2] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238–1280, 3rd Quart., 2013.

[3] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 4, pp. 42–56, 4th Quart. 2009.

[4] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, Feb. 2016.

[5] Y. Xuan, Y. Shen, N. Nguyen, and M. Thai, "A trigger identification service for defending reactive jammers in WSN," *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 793–806, May 2012.

[6] A. Alagil, M. Alotaibi, and Y. Liu, "Randomized positioning DSSS for anti-jamming wireless communications," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Kauai, HI, USA, Feb. 2016, pp. 1–6, doi: 10.1109/ICCNC.2016.7440626.

[7] H. Wang, S. Duan, and X. Xie, "Randomized positioning DSSS for anti-jamming wireless communications," *J. Electron. Inf. Technol.*, pp. 1–8, Jun. 2021, doi: 10.11999/JEIT210107.

[8] S. R. Ratna, R. Ravi, and B. Shekhar, "An intelligent approach based on neuro-fuzzy detachment scheme for preventing jamming attack in wireless networks," *J. Intell. Fuzzy Syst.*, vol. 28, no. 2, pp. 809–820, 2015.

[9] P. Hu and B. Zhang, "Research on centroid localization algorithm in wireless sensor networks," *J. Phys., Conf.*, vol. 1883, no. 1, Apr. 2021, Art. no. 012026, doi: 10.1088/1742-6596/1883/1/012026.

[10] K. V. Chowdary and S. S. Ali, "Jamming probability and network channel access probability in wireless sensor networks," *Int. J. Comput. Sci. Softw. Technol.*, vol. 5, no. 1, pp. 49–51, 2012.

[11] P. Popli and P. Raj, "Effect of jamming attack in mobile ad hoc environment," *Int. J. Sci., Eng. Technol. Res.*, vol. 5, no. 5, pp. 1521–1526, 2016.

[12] G. Pavani, "Packet-hiding methods for preventing selective jamming attacks," *Int. J. Sci. Eng. Res.*, vol. 6, no. 10, pp. 1011–1016, 2015.

[13] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer localization in multi-hop wireless network: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 765–799, 2nd Quart., 2017.

[14] E. De Poorter, T. Van Haute, E. Laermans, and I. Moerman, "Benchmarking of localization solutions: Guidelines for the selection of evaluation points," *Ad Hoc Netw.*, vol. 59, pp. 86–96, May 2017.

[15] E. Tzoreff and A. J. Weiss, "Expectation-maximization algorithm for direct position determination," *Signal Process.*, vol. 133, pp. 32–39, Apr. 2017.

[16] S. G. Nagarajan, P. Zhang, and I. Nevat, "Geo-spatial location estimation for Internet of Things (IoT) networks with one-way time-of-arrival via stochastic censoring," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 205–214, Feb. 2017.

[17] C. Liu, J. Yang, and F. Wang, "Joint TDOA and AOA location algorithm," *J. Syst. Eng. Electron.*, vol. 24, no. 2, pp. 183–188, Apr. 2013.

[18] T. Tirer and A. J. Weiss, "Performance analysis of a high-resolution direct position determination method," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 544–554, Feb. 2017.

[19] H. Liu, W. X, Y. Chen, and Z. Liu, "Localizing jammers in wireless networks," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun.*, Galveston, TX, USA, Mar. 2009, pp. 1–6, doi: 10.1109/PERCOM.2009.4912878.

[20] T. Cheng, P. Li, and S. Zhu, "An algorithm for jammer localization in wireless sensor networks," in *Proc. IEEE 26th Int. Conf. Adv. Inf. Netw. Appl.*, Fukuoka, Japan, Mar. 2012, pp. 724–731, doi: 10.1109/AINA.2012.11.

[21] Y. Wang, X. Wang, D. Wang, and D. P. Agrawal, "Range-free localization using expected hop progress in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 10, pp. 1540–1552, Oct. 2009.

[22] T. Wang, T. Liang, X. Wei, and J. Fan, "Localization of directional jammer in wireless sensor networks," in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Changsha, China, May 2018, pp. 198–202, doi: 10.1109/ICRIS.2018.00059.

[23] P. Liang, X. Chen, Z. Xue, and R. Khatoun, "A novel range-free jammer localization solution in wireless network by using PSO algorithm," in *Proc. Int. Conf. Pioneering Comput. Scientists, Eng. Educators (ICPSEE)*, Singapore, Sep. 2017, pp. 198–211.

[24] A. K. A. Hwaitat, M. A. Almaiah, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 4, pp. 614–625, 2020.

[25] Q. Wang, X. Chen, Z. Xue, and R. Khatoun, "Multi-hop wireless network oriented multiple jammers localization algorithm," *J. Commun.*, vol. 37, no. 12, 2016, pp. 176–186.

[26] Y. Liu, "A faster algorithm for the constrained minimum covering circle problem to expedite solving *p*-center problems in an irregularly shaped area with holes," *Nav. Res. Logistics*, pp. 1–16, Sep. 2021, doi: 10.1002/nav.22023.

[27] Y. Zheng, H. Zhou, T. Xiang, and X. Luo, "Drone patrol strategy based on minimum circle coverage method," *Pure Math.*, vol. 9, no. 5, pp. 664–672, 2019.

[28] C. Liu and R. Wang, "The coaxial measurement and error analysis of the axle of the bullet train," *China Sci. Paper*, vol. 13, no. 4, pp. 1639–1643, 2018.

[29] Y. Liu, K. Wang, and S. H. Qin, "An effective algorithm for generalized Sylvester equation minimization problem under columnwise orthogonal constraints," *Acta Mathematica Scientia*, vol. 41A, no. 2, pp. 479–495, 2021.

[30] H. Wang and J. Liu, "Finding minimum contain circle of plane finite points with genetic algorithm," *J. Nanchang Univ. Eng. Technol.*, vol. 29, no. 4, pp. 384–386, 2007.

[31] X. Jiang and S. Li, "BAS: Beetle antennae search algorithm for optimization problems," *Int. J. Robot. Control*, vol. 1, no. 1, pp. 1–3, 2018, doi: 10.5430/ijrc.v1n1p1.

[32] J. Yu, H. X. Yuan, Y. H. Yang, S. Zhang, and Q. Fei, "Aero-engine pipe layout optimization based on adaptive beetle antennae search algorithm," *J. Mech. Eng.*, vol. 56, no. 20, pp. 174–184, 2020.

[33] G. Du, S. H. Zhang, and L. Qiu, "WSN node location algorithm based on motion trajectory capture and coupled orthogonal coverage," *Comput. Eng.*, vol. 46, no. 3, pp. 157–163, 2020.

[34] X. Li and J. Zhang, "A joint method for the maximum inscribed circle and minimum circumscribed circle," *Measurement*, vol. 87, pp. 189–193, Jun. 2016.

[35] X. Li and J. Zhang, "Evaluation for the minimum circumscribed circle based on the rotation method," *Meas. Sci. Technol.*, vol. 25, no. 9, Jul. 2014, pp. 1–5.

[36] E. S. Gadelmawla, "Simple and efficient algorithms for roundness evaluation from the coordinate measurement data," *Measurement*, vol. 43, no. 2, pp. 223–235, Feb. 2010.

[37] J. Zhang, L. Xu, and S.-M. Zhang, "α-hulls based localization for jamming attack in wireless sensor network," *J. Comput. Appl.*, vol. 32, no. 2, pp. 461–464, Mar. 2013.

[38] Y. Fan, "Research on jamming attack and jammer localization technology in wireless sensor network," M.S. thesis, Southwest Jiaotong Univ., Chengdu, China, 2018.

[39] R. W. Heath, Jr., M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using Poisson point processes," *IEEE Trans. Signal Process.*, vol. 61, no. 16, pp. 4114–4126, Aug. 2013.

[40] L. Blondell, M. Z. Kos, J. Blangero, and H. H. H. Göring, "Genz and mendell-elston estimation of the high-dimensional multivariate normal distribution," *Algorithms*, vol. 14, no. 10, p. 296, Oct. 2021, doi: 10.3390/a14100296.

YUCHENG LYU received the B.S. degree in software engineering from the Taiyuan Institute of Technology, Taiyuan, China, in 2017. His current research interests include computational intelligence, swarm intelligent optimization, system optimization, and numerical simulation of control systems.

YUANBIN MO received the M.S. degree in mathematics from Guizhou University, Guiyang, China, in 2001, and the Ph.D. degree in control theory and control engineering from Zhejiang University, Hangzhou, China, in 2007. He is currently a Professor with the Guangxi University for Nationalities. His research interests include computation intelligence, system optimization, and numerical simulation of control systems.

SONGQING YUE was the lead in developing the B.S. degree in cybersecurity from the University of Wisconsin Platteville and an online collaborative master's program from the University of Wisconsin System. He received the master's and Ph.D. degrees from The University of Alabama. He has been in charge of designing the curriculum, developing new cyber-security courses, and building a state-of-the-art cyber-security laboratory. He is currently an Associate Professor with the Department of Computer Science and Software Engineering, University of Wisconsin–Platteville. His research interests include cybersecurity, cyber risk management, and software engineering with a special focus on program transformation systems and domain-specific language.

WENWU LIU received the B.S. degree in mechanical engineering and automation from the University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan, China, in 2020. His current research interests include big data analysis and swarm intelligent optimization.