

## Research Article

# Jammer Localization in Multihop Wireless Networks Based on Gravitational Search

Tongxiang Wang <sup>1</sup>, Xianglin Wei <sup>2</sup>, Jianhua Fan <sup>2</sup> and Tao Liang<sup>2</sup>

<sup>1</sup>Graduate School, PLA Army Engineering University, Nanjing 210007, China

<sup>2</sup>Nanjing Telecommunication Technology Research Institute, Nanjing 210007, China

Correspondence should be addressed to Jianhua Fan; 237008273@qq.com

Received 15 January 2018; Accepted 20 March 2018; Published 6 May 2018

Academic Editor: Ilsun You

Copyright © 2018 Tongxiang Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Multihop Wireless Networks (MHWNs) can be easily attacked by the jammer for their shared nature and open access to the wireless medium. The jamming attack may prevent the normal communication through occupying the same wireless channel of legal nodes. It is critical to locate the jammer accurately, which may provide necessary message for the implementation of antijamming mechanisms. However, current range-free methods are sensitive to the distribution of nodes and parameters of the jammer. In order to improve the localization accuracy, this article proposes a jammer localization method based on Gravitational Search Algorithm (GSA), which is a heuristic optimization evolutionary algorithm based on Newton's law of universal gravitation and mass interactions. At first, the initial particles are selected randomly from the jammed area. Then, the fitness function is designed based on range-free method. At each iteration, the mass and position of the particles are updated. Finally, the position of particle with the maximum mass is considered as the estimated jammer's position. A series of simulations are conducted to evaluate our proposed algorithms and the simulation results show that the GSA-based localization algorithm outperforms many state-of-the-art algorithms.

## 1. Introduction

Multihop Wireless Networks (MHWNs) face various security problems due to their shared nature and open access to wireless mediums. Among all the security threats to the MHWNs, one typical case of attacks is jamming attack, which usually emits useless radio signal to disrupt normal communications between wireless devices by occupying the wireless channel or destroying the coupling of protocols with one or many low-end simple off-the-shelf wireless devices [1, 2]. For instance, different from interferences among wireless nodes [3], jamming attack can break down the MAC protocols by sending fabricated ACK or CTS packets to the wireless channel. Generally speaking, jamming attack can be initiated from different protocol layers and decreases the network performance significantly through limited resource consumption, which makes it be widely employed by adversaries.

In order to mitigate the impact of jamming attack and restore the normal communications, a series of anti-jamming

countermeasures have been proposed from multiple network layers, such as channel-hopping, secure routing, and spatial retreat [4–7]. However, these anti-jamming strategies mainly provide useful approaches to avoid or evade an attack in order to maintain the normal operation of wireless networks. Although the negative impact of jamming attack can be mitigated, the networks can only adjust themselves passively without utilizing the information of jamming. Moreover, when conducting the anti-jamming measures, the constraints of wireless devices including limited memory and energy supply and low computation capabilities must be considered.

Besides these passive anti-jamming measures, another way is to locate the jammer and obtain the position information of jammers, which makes it possible to eliminate the jammer from the networks by physical methods or manual ways. Actually, the position information of jammers may allow better deployment of wireless devices and provide useful information when designing MAC or routing protocols.

Up to now, jammer localization has been widely investigated and a number of localization algorithms have been

proposed. In conclusion, exiting jammer localization algorithms can be divided into range-based methods and range-free ones. Range-based algorithms need to estimate the parameters of wireless channel in advance and calculate the relative distance between nodes and the jammer. Although some typical models of wireless channel have been proposed, the parameters of wireless channel can be hardly estimated accurately in real scenario. Besides, the performance of range-free algorithms can be easily affected by the distribution of nodes and the jammer's parameters.

In order to reduce the sensitivity of range-free algorithms and improve the localization accuracy, a robust jammer localization algorithm based on Gravitational Search Algorithm (GSA) is proposed in this paper. At first, several related models, that is, network model, jamming model, and communication model, are illustrated. Then, the GSA-based jammer localization is presented, which mainly consists of selection of initial particles, determination of fitness function, resultant force calculation, and parameters update. At last, a series of simulations are conducted to evaluate the performance of our proposed algorithm. Compared with many state-of-the-art jammer localization algorithms, our algorithm performs better in many different scenarios with different parameter settings.

The architecture of this article is organized as follows. Section 2 summarizes related work. Several related models are introduced in Section 3. Section 4 presents our jammer localization strategy based on GSA in detail. Simulation experiments and results are described in Section 5. The main work is concluded in the last section and some discussions on the future work are highlighted.

## 2. Related Work

Over the past few years, Xu et al. conducted a series of researches on the jamming attack and four basic approaches of jamming attack were proposed [8], which were defined as constant jamming, random jamming, proactive jamming, and reactive jamming. Wei et al. provided a comprehensive survey of the major works done in the field of jammer localization for MHWN [9].

Range-free localization algorithms utilize the geometric knowledge of the jammed area to locate the jammer. Wang and Zheng took the weighted factor determined by the relative position between jammer and node into consideration when modifying the Centroid Localization (CL) [10] and presented Weighted Centroid Localization (WCL). Liu et al. put forward the Virtual Force Iterative Localization (VFIL) to locate the jammer [11]. At first, the jammed area and jamming range were estimated by VFIL. Then, the estimated position of the jammer was amended iteratively in order to cover the most jammed nodes. Sun et al. computed the convex hull that was determined by the boundary nodes to locate the jammer [12]. The minimum circumscribed circle was achieved based on the convex hull and the center of it is the estimated jammer's location. Similarly,  $\alpha$ -hull was adopted by Zhang et al. to obtain circumcircle of the jammed area and then the least square circle was formulated to estimate jammer's location [13]. In addition, Wei et al. also made

the research on the collaborative mobile jammer tracking in MHWN and the jammer is located based on multilateral localization method [14]. For multi-jammers scenario, Cheng et al. put forward the M-clusters and X-ray to estimate jammers' positions, respectively [15]. Wang et al. proposed the  $k$ -mean cluster algorithm based on the neighbor nodes' information to estimate the positions of the jammers [16].

The relationship between jammer and node is established based on wireless channel model to locate the jammer for range-based localization algorithms. Pelechris et al. pointed out that Packet Delivery Rate (PDR) decreased with increasing distance between node and the jammer [17]. So value of PDR could be used to indicate the influence that the jammer had on the node. They proposed a light distributed jammer localization algorithm based on PDR and the node would select the node with minimum PDR from its neighbor nodes as the next hop. Liu et al. proposed the jammer localization algorithm based on the nodes' hearing range [18], which is defined as the maximum distance for the node that can successfully decode the signal generated from other nodes. Wang et al. put forward the scheme to locate the jammer based on the combination of PDR gradient descent and power adaptive technique [19]. The power would increase at the termination node of PDR gradient descent and the localization accuracy was improved a lot compared to that of PDR gradient descent.

## 3. System Models and Problem Formulation

This section analyzes the impact of jamming on the legal communication link and introduces several related models. The nodes in the jammed network can be divided into three categories based on the impact of jamming, that is, unaffected nodes, boundary nodes, and jammed nodes.

*3.1. Impact of Jamming.* According to the characteristic of wireless communication, the signals cannot be decoded correctly if the received SNR is lower than a certain threshold. Assume that the interference among nodes has been avoided through specific MAC or network protocols, such as TDMA and 802.11 DCF. Thus, the overall interference mainly includes the background noise for nonjamming scenes and the background noise and jamming signal for jamming scenes. For the transmitter  $i$  and receiver  $j$ , the received SNR <sub>$ij$</sub>  of node  $j$  is

$$\text{SNR}_{ij} = \frac{P_{ij}}{P_N + P_{jR}}, \quad (1)$$

where  $R$  represents the jammer and  $P_{jR}$  is the received jamming power at node  $j$ .  $P_{ij}$  and  $P_N$  represent the received power of node  $j$  and the power of background noise, respectively. The state of link between node  $i$  and node  $j$  is defined as  $l_{ij}$ :

$$l_{ij} = \begin{cases} 0, & \text{SNR}_{ij} \leq \gamma_0 \\ 1, & \text{SNR}_{ij} > \gamma_0, \end{cases} \quad (2)$$

where  $\gamma_0$  is the received SNR threshold for all the nodes.  $l_{ij} = 1$  denotes the normal communication between node

$i$  and node  $j$ . The communication links among nodes are bidirectional and the link between node  $i$  and node  $j$  is considered to be connected when both the conditions  $l_{ij} = 1$  and  $l_{ji} = 1$  are satisfied.

### 3.2. Related Models

**3.2.1. Network Model.** The characteristics of MHWN model considered in this article mainly include the following.

*Multihop and Stationary.* Once deployed, the position of MHWN node remains unchanged and the nodes communicate with each other through multihop fashion. The nodes are assumed to be time-synchronous, which can be achieved by the clock calibration after initial deployment.

*Location-Aware.* The MHWN nodes can be aware of their own locations and their neighbors' locations through GPS or specific location-aware algorithms and many applications also require the location of nodes in order to provide specific services. Assume that the locations of nodes have been obtained after initial deployment.

*Neighbor-Aware.* Each node can store its neighbors' information and update a neighbor list at regular intervals. The list can be achieved by several routing protocols, such as AODV and DSR.

Besides, each node is equipped with omnidirectional antenna and transmits signals with the same power. In other words, the nodes are homogeneous in MHWN.

**3.2.2. Jamming Model.** The jammer considered in this article remains static and the jamming power remains unchanged. Besides, the constant jammer equipped with omnidirectional antenna is adopted in this article, which transmits RF signals consistently.

**3.2.3. Node Model.** The nodes deployed in the MHWN randomly can be divided into jammed ones, boundary nodes, and unaffected ones according to different degree of jamming produced by the jammer:

- (i) Unaffected node: a node is determined to be unaffected if it can receive packets from all of its neighbors after the appearance of the jammer
- (ii) Boundary node: the node is considered as a boundary node if it loses some of its neighbors, while it can still communicate with part of the unaffected nodes
- (iii) Jammed node: the jammed node is defined as the node that cannot receive any message from all the unaffected nodes and boundary nodes

**3.2.4. Wireless Channel Model.** Typical wireless channel models mainly include free-space propagation model, shadow-fading model, and exponential-fading model [20–22]. The shadow-fading model is adopted here to model the small-scale fading circumstance. If the receiver locates at the

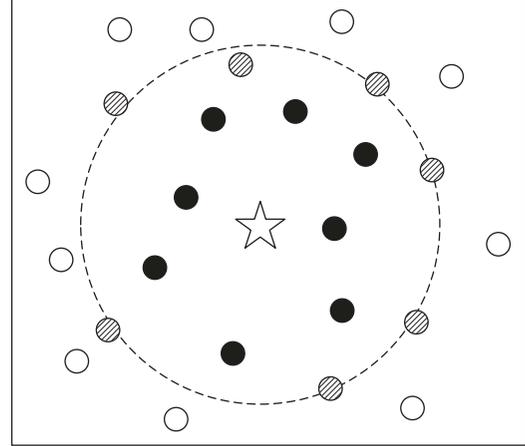


FIGURE 1: Typical scenario of jammed network.

distance  $d$  from the transmitter, the received power ( $PL(d)$ ) is

$$PL(d) = PL(d_0) - 10\eta \log\left(\frac{d}{d_0}\right) + X_\sigma, \quad (3)$$

where  $PL(d_0)$  represents the received power at specific distance  $d_0$  and  $\eta$  is the fading index.  $X_\sigma$  is the Gauss random variable with zero mean and variance  $\sigma^2$ .

**3.3. Problem Formulation.** A typical jammed network scenario is illustrated in Figure 1. We aim at locating the jammer under the above settings by using the jamming information. To achieve this goal, several challenges need be solved and we present our basic ideas here. At first, each node should determine its state based on the neighbors number, received SNR, and so forth. Then, we need to decide the jamming information that could be collected by wireless nodes, such as sensor node. Besides, the information can be used to detect the jammer's existence. At last, an efficient localization algorithm needs to be carefully designed considering both the complexity and accuracy.

## 4. Algorithm Description

**4.1. GSA Principle.** The Gravitational Search Algorithm was proposed by Rashedi et al. in 2009 [23] and the searching progress can be carried out by interaction among particles. In GSA, the particle's position represents the solution of the problem. At first, the initial solution is obtained through the feasible region and the particles' mass is calculated by the fitness function. Then, the interaction among particles is used to update their mass and positions. The particles will move to the particles with larger mass, which represents the better solutions. At last, the particle with the largest mass is considered as the best solution.

GSA has been widely employed in data mining, parameter identification, and multi-objectives decision and achieved good performance. In the problem of jammer localization, the estimated jammer's position is the solution of the problem, which is consistent with the solution of GSA. Therefore, it is feasible to employ the GSA in the jammer localization, which is the basis of our paper.

In order to achieve this target, the challenges and main work in our paper mainly include the following:

- (i) Mapping of particles' positions and jammer's estimated location: in our proposed algorithm, the particle's position represents the jammer's estimated location. With the progress of iteration process, the particles' positions are updated. At the end of the iteration, the position of the particle with the maximum mass is considered as the final estimated jammer's location
- (ii) Selection of initial particles: according to the characteristics of jamming area, the jammer is supposed to be located in its inside. In the initial step of GSA, a specific number of particles are distributed in the jammed area randomly
- (iii) Calculation of fitness function: the jammer is equipped with omnidirectional antenna and the jammed area is about a circle. Thus, the distances between the jammer and boundary nodes that located in the boundary of the jammed area are similar. The fitness function can be determined by the variance of distances between the boundary nodes and the jammer

**4.2. Preliminary.** Generally speaking, the affected nodes (including boundary nodes and jammed nodes) can be used to reflect the existence of jamming attack. Several jamming detection methods have been proposed based on affected nodes' collected jamming information, such as received signal strength and carrier sensing time [8]. However, jamming detection is not our main work and we pay our attention to the localization process, which would be conducted after detecting jamming attack. Assume that each wireless node in the network can work normally and detect the existence of jamming attack correctly.

Before conducting the localization process, each node should determine its state based on the jamming information. If every node tries to communicate with all of its neighbor nodes, the network load would increase a lot. In order to determine its state efficiently, each node maintains its neighbors number and records each neighbor's SNR. Then, it will determine its own state according to Algorithm 1, where parameters  $b$ ,  $c$ , and  $d$  are determined by specific network condition.

**4.3. Information Collection.** Assume that there is a locating node, which is in charge of jammer localization, in the wireless network chosen from the unaffected nodes through some kind of voting algorithm. To realize the localization

```

(1) if a node does not detect jamming attack then
(2)   This node is an unaffected node;
(3) else
(4)   if this node does not lose any neighbor and its
       received SNRs from most of its neighbors' do not
       decrease more than a percent then
(5)     This node is an unaffected node;
(6)   else
(7)     if this node loses more than  $b$  percent of its
          neighbors then
(8)       This node is a jammed node;
(9)     else
(10)      if more than  $c$  percent of its neighbors' SNRs
           decrease more than  $d$  percent then
(11)        This node is a jammed node;
(12)      else
(13)        This node is a boundary node;
(14)      end if
(15)    end if
(16)  end if
(17) end if

```

ALGORITHM 1: Node state determination algorithm.

Node_ID	Destination_node_ID	RJSS	Node_position
---------	---------------------	------	---------------

FIGURE 2: Frame structure of information collection.

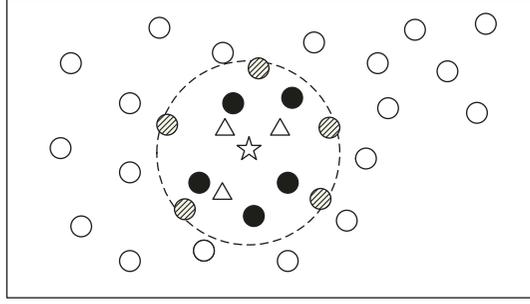
process, it has to firstly collect information from wireless nodes and then execute the localization algorithm.

Based on the analysis in the above section, we have to design an information-collecting protocol to gather necessary RJSS values and other related information of nodes while reducing the transmission overhead introduced by this process, since normal communication among wireless nodes may be damaged or even disrupted by jammer. To achieve this goal, a node is required to report its RJSS values to the locating node if and only if it is determined to be a boundary node.

Each boundary node will send its collected RJSS values and position to the locating node. The basic structure of the reporting packet is shown in Figure 2, where *Node\_ID* and *Destination\_node\_ID* represent the IDs of the boundary node and locating node, respectively. *RJSS* and *Node\_position* are the reported RJSS values and the coordinate values of the boundary node, respectively.

**4.4. Jammer Localization Based on GSA.** The GSA-based jammer localization can be divided into four steps according to GSA principle: selection of initial particles, determination of fitness function, resultant force calculation, and parameters update.

**4.4.1. Selection of the Initial Particles.** The position of particle represents the solution of the problem based on GSA principle. According to the jamming characteristics, the jammer must be within the jammed area. Therefore, the initial particles, which are represented by triangle in Figure 3,



☆ Jammer                      ○ Unaffected node  
 ● Jammed node                △ Particles  
 ⊘ Boundary node

FIGURE 3: Distribution of initial particles.

should be selected within the jammed area. Besides, the velocity and acceleration of the particles are set as zero at the first iteration.

In order to improve the uniformity of the initial particles' distribution, the backward learning method is adopted to promote the performance of the algorithm. Assume that  $N$  particles are deployed in a  $D$ -dimensional space and the position of particle  $i$  is represented as  $X_i = \{x_i^1, x_i^2, \dots, x_i^k, \dots, x_i^D\}$ , where  $x_i^k \in [a_k, b_k]$  and  $a_k$  and  $b_k$  are the lower bound and upper bound in the  $k$ th dimension. Then, the opposite particle of  $x_i^k$  is  $\bar{x}_i^k = a_k + b_k - x_i^k$ . At last, the initial particles and opposite particles are all added to the final particle set. The particles (including initial particles and opposite particles) are deployed in the jammed area formulated by the jammed nodes and the acceleration and velocity of the particles are all set to be zero at the first iteration.

**4.4.2. Determination of the Fitness Function.** The fitness function is designed to evaluate the performance of estimated jammer's position. In the single-jammer scenario, the jammed area is similar to a circle and the distance between boundary nodes and the jammer is approximately equal to the jamming radius. Therefore, we obtain the boundary nodes based on convex hull at first and then the variance of distances between the boundary nodes and the jammer is calculated, which is defined as the fitness function. Suppose that there are  $N$  particles in the MHWN; the position of particle  $i$  is defined as  $X_i = (X_{ix}, X_{iy})$ ,  $i = 1, 2, \dots, N$ . Thus, the fitness function at the  $t$  iteration for particle  $i$  is

$$\begin{aligned} \text{fit}_i(t) &= \frac{1}{M} \sum_{j=1}^M (d_{ij}(t) - \bar{d}_i(t))^2, \quad i = 1, 2, \dots, N, \\ d_{ij}(t) &= \sqrt{(X_{ix}(t) - B_{jx})^2 + (X_{iy}(t) - B_{jy})^2}, \\ \bar{d}_i(t) &= \frac{1}{M} \sum_{j=1}^M (d_{ij}(t)), \end{aligned} \quad (4)$$

where  $M$  is the number of boundary nodes.  $B_{jx}$  and  $B_{jy}$  represent the  $x$  and  $y$  coordinate values for the boundary node  $j$ , respectively.  $d_{ij}(t)$  is defined as the Euclidean distance between particle  $i$  and boundary node  $j$ .  $\bar{d}_i(t)$  is the average Euclidean distance.

**4.4.3. Resultant Force Calculation.** The mass of each particle is determined by its fitness, which can be calculated by

$$\begin{aligned} m_i(t) &= \frac{\text{fit}_i(t) - \text{worst}(t)}{\text{best}(t) - \text{worst}(t)}, \\ M_i(t) &= \frac{m_i(t)}{\sum_{j=1}^N m_j(t)}, \end{aligned} \quad (5)$$

where  $\text{fit}_i(t)$  is the fitness value for particle  $i$  at the  $t$  iteration.  $\text{best}(t)$  and  $\text{worst}(t)$  represent the best value and worst value of the particles at the  $t$  iteration.  $m_i(t)$  and  $M_i(t)$  are the mass and normalized mass for particle  $i$  at the  $t$  iteration, respectively.

The gravitation for particle  $i$  and particle  $j$  in  $d$  dimension can be calculated by

$$F_{ij}^d = G(t) \frac{M_i(t) \times M_j(t)}{d_{ij}^2(t) + \varepsilon} (x_j^d(t) - x_i^d(t)), \quad (6)$$

where  $x_i^d(t)$  and  $x_j^d(t)$  represent the positions of particles  $i$  and  $j$  at the  $t$  iteration, respectively.  $d_{ij}(t)$  represents the Euclidean distance between particle  $i$  and particle  $j$ .  $\varepsilon$  is a small constant and  $G(t)$  indicates the gravity coefficient. The resultant force  $F_i^d(t)$  for particle  $i$  in  $d$  dimension is the resultant force generated from all the other particles:

$$F_i^d(t) = \sum_{j=1, j \neq i}^N \text{rand}_j F_{ij}^d(t), \quad (7)$$

where  $\text{rand}_j$  is a random number in  $[0, 1]$ .

#### 4.4.4. Parameters Update

**Update the Gravity Coefficient.** According to the GSA principle, the gravity coefficient that can be calculated by formulation (8) decreases with the time.

$$G(t) = G_0 \times e^{-\alpha(t/T)}, \quad (8)$$

where  $\alpha$  is the time constant,  $T$  is the maximum number of iterations, and  $G_0$  is the initial value of gravity coefficient.

**Update the Acceleration, Velocity, and Position.** The acceleration of particle  $i$  in  $d$  dimension at the  $t$  iteration is

$$a_i^d(t) = \frac{F_i^d(t)}{M_i(t)}, \quad (9)$$

where  $M_i(t)$  is the normalized mass for particle  $i$ . The velocity and position for particle  $i$  are updated by

$$\begin{aligned} v_i^d(t+1) &= \text{rand}_i \times v_i^d(t) + a_i^d(t), \\ x_i^d(t+1) &= x_i^d(t) + v_i^d(t+1), \end{aligned} \quad (10)$$

where  $v_i^d(t)$  and  $x_i^d(t)$  are the velocity and position, respectively, for particle  $i$  in  $d$  dimension at the  $t$  iteration.

At last, the GSA will be terminated until the time of iterations reaches the threshold and, otherwise, the mass, velocity, and position for all the particles would be updated at the next iteration.

**4.5. Discussions.** In our proposed GSA-based jammer localization algorithm, the fading index of wireless channel and jamming power should be estimated exactly in order to calculate the estimated RJSS values. Due to the fact that the received signal's power and nodes' locations have already been obtained, the fading index of wireless channel can be estimated by the communication among nodes. In this paper, the fading index is assumed to be estimated accurately. However, the jamming power cannot be derived or estimated directly. In order to solve this problem, the jamming power is assumed to be chosen from a series of discrete values, which is also the assumption made in [24]. The proposed localization algorithm will be conducted under these discrete jamming powers and the best position and optimal value under each jamming power will be recorded. In the end, the global optimal value chosen from all the optimal values of different power levels will be chosen and its corresponding jamming power is considered as the real jamming power.

**4.6. Pseudocode.** The pseudocode of GSA-based localization algorithm is illustrated in Algorithm 2. Step (1) is the initialization of related parameters, that is, number of iterations, number of particles, the acceleration, velocity and position of the particles, the gravity coefficient, and the time constant used to update the gravity coefficient.  $N$  particles that present the initial solutions are randomly selected in the jammed area in Step (3). Step (4) calculates the fitness value for each particle and the best value is updated according to the fitness values. The mass and the resultant force will be calculated according to Newton's second law in Steps (6) and (7). The gravity coefficient and acceleration, velocity, and position of the particle will be updated for each iteration in Step (8). After the iterations, the position of particle with maximum mass is considered as the estimated jammer's position.

**Complexity Analysis.** The time complexity of our proposed algorithm is  $O(TN^2)$ .  $T$  is the number of iterations and  $N$  is the number of particles.

## 5. Simulation Experiments

### 5.1. Parameters Setting and Benchmark

**5.1.1. Parameters Setting.** The basic MHWN is established in an area of  $L * L$  square meters and the number of nodes is  $Q$ . The jammer equipped with omnidirectional antenna is deployed in the center of the network with coordinate (200, 200). Other related parameters are represented in Table 1.

**5.1.2. Benchmark.** The algorithms used for comparison with our proposed algorithm are CL, WCL, VFIL, and DCL. These four algorithms are the common localization algorithms

<b>Input:</b> the state and position of MHWN nodes
<b>Output:</b> the estimated jammer's position
(1) <b>Initialize</b> number of iterations ( $T$ ), number of particles ( $N$ ), acceleration, velocity and position of the particle, gravity coefficient and time constant $\alpha$ ;
(2) <b>for</b> $t = 1 : T$ <b>do</b>
(3) Random select $N$ particles in the jammed area;
(4) Calculate the fitness function for each particle;
(5) Save the best value at this iteration and update the global best value;
(6) Calculate the mass and normalized mass of the particles;
(7) Calculate the resultant force in each dimension for all the particles;
(8) Update the gravity coefficient and acceleration, velocity, position of the particle.
(9) <b>end for</b>

ALGORITHM 2: GSA-based localization algorithm.

TABLE 1: Simulation parameters.

Parameter	Meaning	Value
$M$	Simulation times	200
$Q$	Number of MHWN nodes	400
$L$	Radius of MHWN	400 m
$P_j$	Transmitting power of jammer	10 mW
$P_T$	Transmitting power of node	10 mW
$P_N$	Power of noise	-60 dBm
$n$	Fading exponent	2
$G_r$	Gain of the transmitting antenna	1
$G_t$	Gain of the receiving antenna	1
$N$	Number of particles	50
$G_0$	Initial value of gravity coefficient	100
$\alpha$	Time constant	20
$T$	Number of iterations	50

usually used for comparison in most of the papers and the comparison results are convincing.

The average error ( $e$ ) is adopted to measure the performance of our proposed algorithm, which can be calculated by

$$e = \frac{1}{M} \sum_{i=1}^M (\|z_i - \hat{z}_i\|), \quad (11)$$

where  $z_i$  and  $\hat{z}_i$  are the real position and estimated position for  $i$ th simulation. Besides, the cumulative distribution functions (CDF) are also shown below.

**5.2. Performance Comparison and Results Analysis.** We conduct 200 simulations independently and nodes are deployed in the network randomly for each time. Besides, the position of the jammer and the transmitting powers of the jammer and nodes remain unchanged. In this section, the CDF of localization errors and average localization errors are shown.

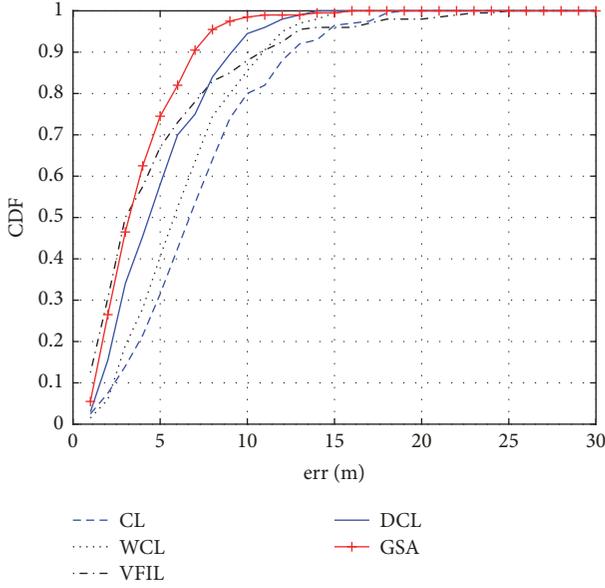


FIGURE 4: CDF of localization errors.

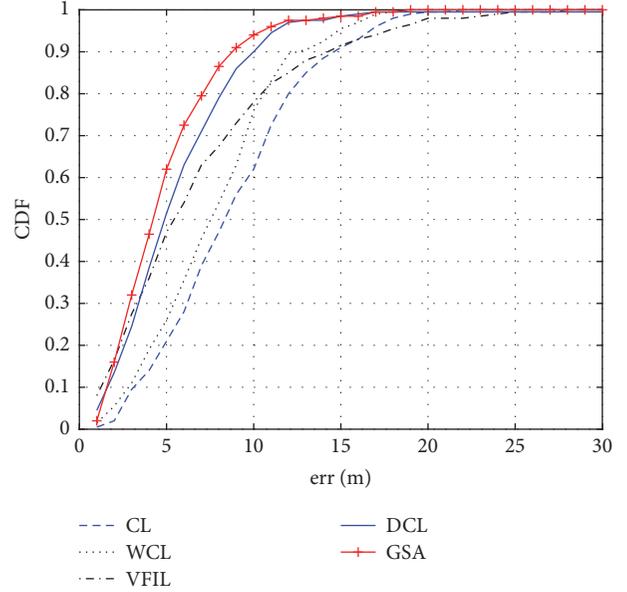


FIGURE 6: CDF of localization errors when the number of nodes is 300.

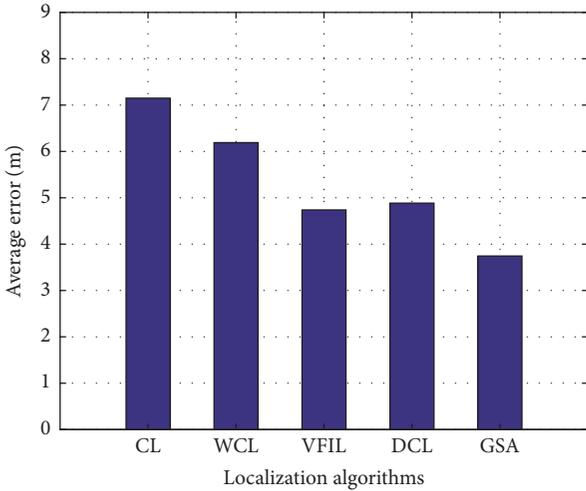


FIGURE 5: Average localization errors.

Besides, the localization errors influenced by the number of particles are also discussed.

**5.2.1. Comparison Results.** We compare the performance of GSA with the exiting localization algorithms, CL, WCL, VFIL, and DCL. Figure 4 presents the CDF of different localization algorithms for 200 simulations and Figure 5 presents the average error of localization. From the figures, we can conclude that the localization error of our proposed algorithm is lower than those of CL, WCL, VFIL, and DCL. Besides, we can conclude that VFIL may be more sensitive to the distribution of nodes for some larger values of localization error. The average localization error of GSA can reach 3.7 m, which is smaller than that of the other algorithms.

**5.2.2. Impact of Node Density.** We compare the localization errors for different node density and the numbers of nodes

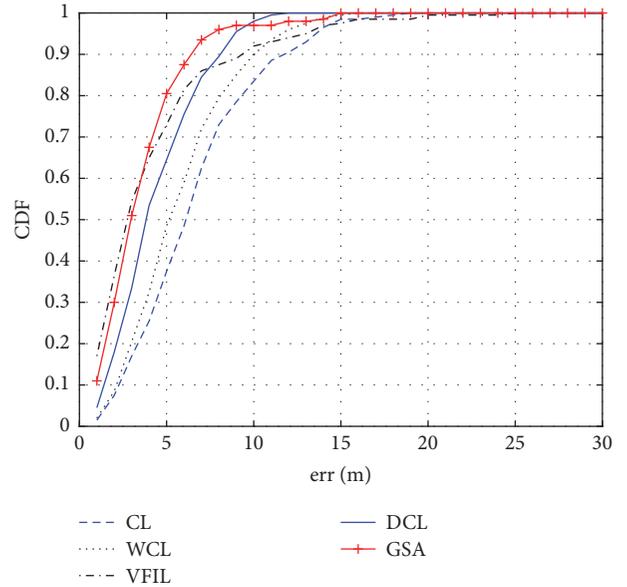


FIGURE 7: CDF of localization errors when the number of nodes is 500.

are set as 300, 400, and 500, respectively. When the area is assumed to be constant, the nodes' number can be utilized to reflect the node density of the network. After conducting 200 simulations independently, the CDFs of localization errors for different nodes' number are illustrated in Figures 6 and 7. The average localization errors of these algorithms decrease with the increasing number of nodes, which is shown in Figure 8. Besides, GSA achieves better performance than the other four algorithms for different nodes' number.

**5.2.3. Impact of Jamming Power.** In order to compare the localization performance for different jamming powers, the

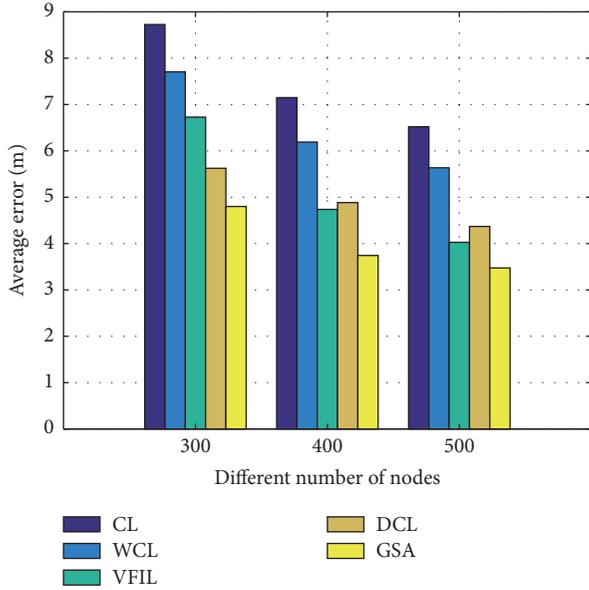


FIGURE 8: Impact of node density.

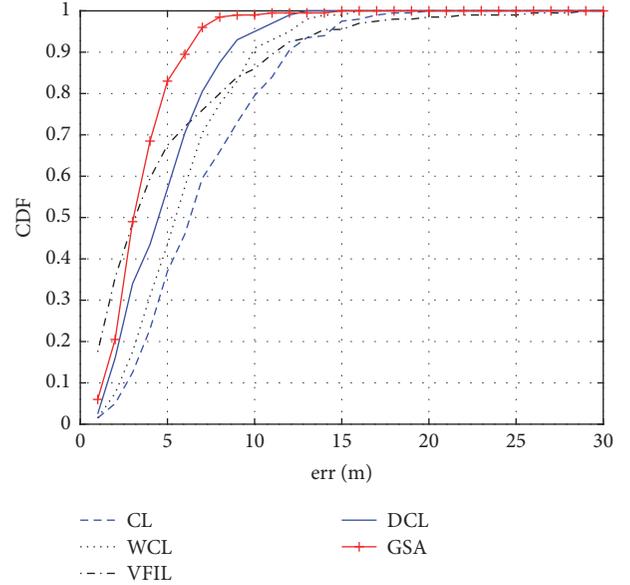


FIGURE 10: CDF of localization errors when the jamming power is 15 mW.

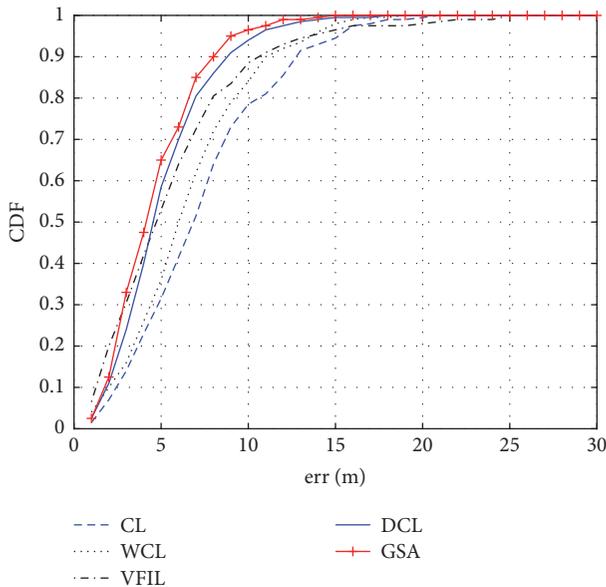


FIGURE 9: CDF of localization errors when the jamming power is 6 mW.

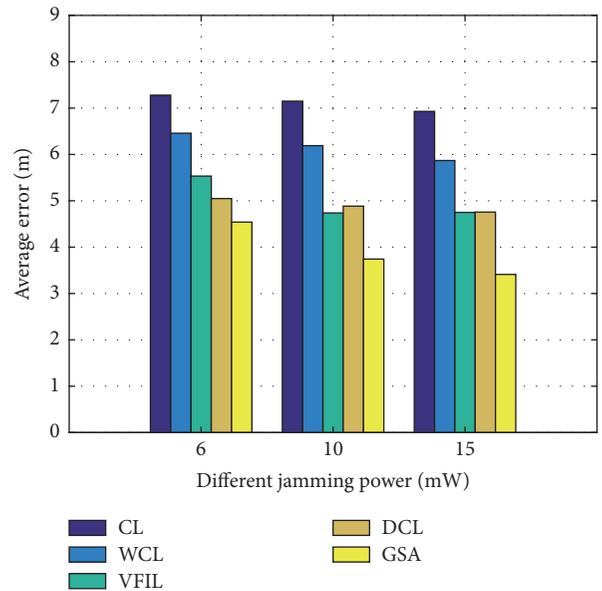


FIGURE 11: Impact of jamming power.

jamming powers are set as 6 mW, 10 mW, and 15 mW. The CDFs of localization errors for different jamming powers are illustrated in Figures 9 and 10. It can be concluded that as the jamming power increases, the localization errors of these algorithms decrease, which is shown in Figure 11. Besides, we can also conclude that the GSA obtains the best performance for the localization obviously.

**5.2.4. Impact of Jammer's Position.** In order to analyze the impact of jammer's position on the localization errors, the jammer is located in the positions of (60, 60), (70, 70), and (200, 200), respectively. When the jammer is located in

(60, 60) or (70, 70), the assumption that the jammed area is a circle is biased and the real jammed area formulated by the jammed nodes is irregular. From Figure 12, it can be seen that when the jammer locates close to the edge of the network, the localization errors increase for the five algorithms. GSA achieves the best localization performance for different scenarios.

Moreover, a comparison table for outcomes of different applied algorithms is illustrated in Table 2. The average localization errors ( $m$ ) for CL, WCL, VFIL, DCL, and GSA under different conditions (including number of nodes and jamming power) are illustrated in the table.

TABLE 2: Average error under different settings.

Number of nodes	Jamming power	CL	WCL	VFIL	DCL	GSA
300	10 mW	8.73	7.71	6.73	5.63	4.80
400	6 mW	7.28	6.46	5.53	5.05	4.54
400	10 mW	7.15	6.19	4.74	4.88	3.74
400	15 mW	6.93	5.87	4.75	4.76	3.41
500	10 mW	6.52	5.64	4.03	4.37	3.47

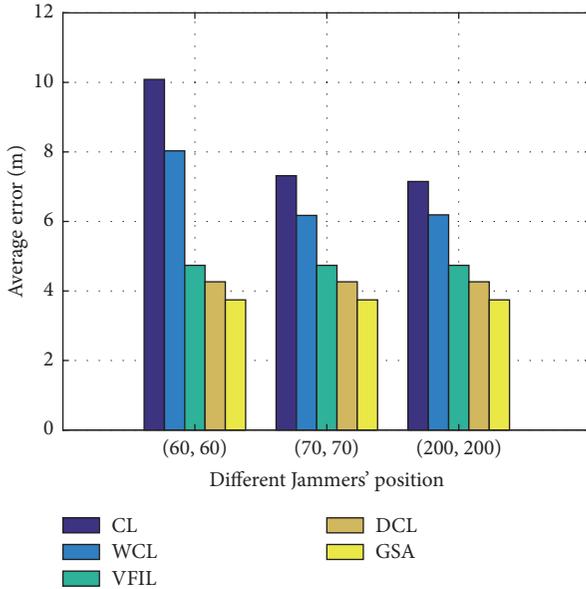


FIGURE 12: Impact of jammer's position.

### 5.3. Impact of Parameters

**5.3.1. Impact of Particles' Number.** The localization performance of our proposed GSA algorithm is discussed under different number of particles. The number of particles is assumed to be 20, 30, 50, and 100, respectively, and the localization results are shown in Figure 13. As the number of particles increases, the localization error decreases a little. However, the complexity of GSA is closely related to the number of particles and the tradeoff between the localization accuracy and complexity should be considered when determining the number of particles.

**5.3.2. Impact of GSA's Iterations.** The localization performance of the GSA-based algorithm is analyzed under different GSA's iterations. The iterations are assumed to be 20, 30, 50, and 80, respectively. The average localization errors for different iterations are illustrated in Figure 14. From the figure, we can conclude that as the GSA's iterations increase, the localization errors decrease. This is due to the fact that GSA searching results will converge to a stable value as the iterations increases. Besides, the complexity of GSA is determined by particles' number and iterations. Although the localization results are more accurate, the execution time of GSA will increase.

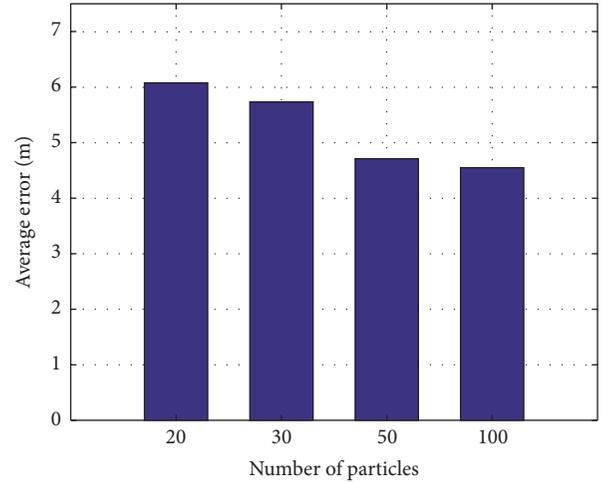


FIGURE 13: Impact of the number of particles.

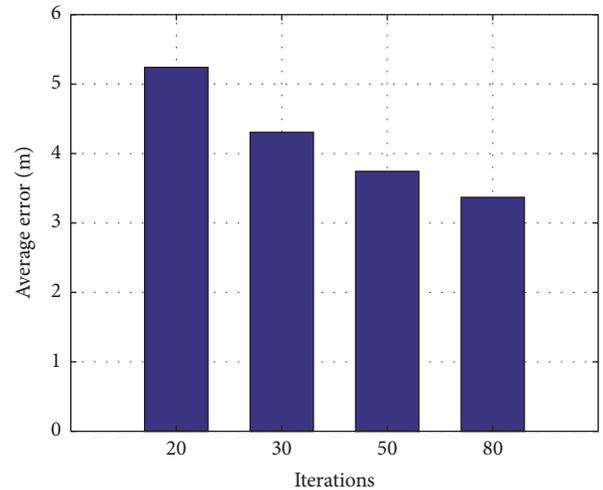


FIGURE 14: Impact of GSA's iterations.

## 6. Conclusion and Future Work

In order to reduce the sensitivity of the existing algorithms to the MHWN nodes deployment and parameters of the jammer for the jammer localization, we have presented a novel localization strategy based on Gravitational Search Algorithm (GSA), which is an evolutionary algorithm based on Newton's law of universal gravitation and mass interactions. The initial particles are assumed to be deployed in the jammed area randomly with acceleration and velocity set to

be zero. The convex hull is adopted to obtain the boundary nodes and these boundary nodes are used to calculate the fitness function for the particles. After the iterations, position of the particle with the maximum mass is considered as the estimated position of the jammer. A series of simulations are conducted and the localization performance of our proposed algorithm is validated. Compared with CL, WCL, VFIL, and DCL, the simulation results show that GSA-based localization algorithm can locate the jammer more accurately.

In the future, we will take the multijammers localization into consideration and put forward efficient localization algorithms.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This research was supported in part by the National Natural Science Foundation of China (Grants nos. 61402521 and 61471392) and Natural Science Foundation of Jiangsu Province, China (Grants nos. BK20140068 and BK20150201).

## References

- [1] S. D. Babar, N. R. Prasad, and R. Prasad, "Jamming attack: Behavioral modelling and analysis," in *Proceedings of the 2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, pp. 1–5, IEEE, 2013.
- [2] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.
- [3] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure Multiple Amplify-and-Forward Relaying with Cochannel Interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.
- [4] Y. Liu, F. Jiang, H. Liu, J. Wu, C. Hu, and M. Zhang, "Interference robust channel hopping strategies for wireless sensor networks," *China Communications*, vol. 13, no. 3, Article ID 7445505, pp. 96–104, 2016.
- [5] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service," in *Proceedings of the 2004 ACM Workshop on Wireless Security, WiSe*, pp. 80–89, October 2004.
- [6] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, Article ID S0167404817301621, pp. 1–12, 2018.
- [7] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Information Sciences*, vol. 412–413, pp. 223–241, 2017.
- [8] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'05)*, pp. 46–57, ACM, Urbana-Champaign, Ill, USA, May 2005.
- [9] X. Wei, Q. Wang, T. Wang, and J. Fan, "Jammer Localization in Multi-Hop Wireless Network: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 765–799, 2017.
- [10] Z.-M. Wang and Y. Zheng, "The study of the weighted centroid localization algorithm based on RSSI," in *Proceedings of the 2014 International Conference on Wireless Communication and Sensor Network, WCSN 2014*, pp. 276–279, Wuhan, China, December 2014.
- [11] H. Liu, X. Wenyuan, Y. Chen, and Z. Liu, "Localizing jammers in wireless networks," in *Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, vol. 25, pp. 1–6, Galveston, TX, USA, March 2009.
- [12] Y.-Q. Sun, X.-D. Wang, and X.-M. Zhou, "Geometry-covering based localization for jamming attack in wireless sensor networks," *Journal of China Institute of Communications*, vol. 31, no. 11, pp. 10–16, 2010.
- [13] J. Zhang, L. Xu, Q. Shen, and X. Ji, "Localization for Jamming Attack in Wireless Sensor Networks," in *Intelligent Data Analysis and Applications*, vol. 370 of *Advances in Intelligent Systems and Computing*, pp. 361–369, Springer International Publishing, 2015.
- [14] X. Wei, T. Wang, C. Tang, and J. Fan, "Collaborative mobile jammer tracking in Multi-Hop Wireless Network," *Future Generation Computer Systems*, vol. 78, pp. 1027–1039, 2018.
- [15] T. Cheng, P. Li, S. Zhu, and D. Torrieri, "M-cluster and X-ray: Two methods for multi-jammer localization in wireless sensor networks," *Integrated Computer-Aided Engineering*, vol. 21, no. 1, pp. 19–34, 2014.
- [16] Q. Wang, J. Fan, X. Wei, and T. Wang, "Multi-jammers localization for multi-hop wireless network," *Journal of Communication*, vol. 37, no. 13, pp. 176–186, 2016.
- [17] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S. V. Krishnamurthy, "Lightweight jammer localization in wireless networks: System design and implementation," in *Proceedings of the 2009 IEEE Global Telecommunications Conference, GLOBECOM 2009*, pp. 1–6, December 2009.
- [18] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 3, pp. 547–555, 2012.
- [19] Q. Wang, X. Wei, J. Fan et al., "A step further of PDR-based jammer localization through dynamic power adaptation," in *Proceedings of the 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015)*, pp. 1–6, Shanghai, China, 2015.
- [20] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM '00)*, vol. 2, pp. 775–784, Tel Aviv, Israel, March 2000.
- [21] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secrecy Cooperative Networks with Outdated Relay Selection over Correlated Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 8, pp. 7599–7603, 2017.
- [22] R. Zhao, Y. Yuan, L. Fan, and Y.-C. He, "Secrecy Performance Analysis of Cognitive Decode-and-Forward Relay Networks in Nakagami-m Fading Channels," *IEEE Transactions on Communications*, vol. 65, no. 2, pp. 549–563, 2017.
- [23] E. Rashedi, H. Nezamabadi-Pour, and S. Saryazdi, "Gsa: a gravitational search algorithm," *Information sciences*, vol. 179, no. 13, pp. 2232–2248, 2009.

- [24] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Error minimizing jammer localization through smart estimation of ambient noise," in *Proceedings of the 9th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, MASS 2012*, pp. 308–316, October 2012.



**Hindawi**

Submit your manuscripts at  
[www.hindawi.com](http://www.hindawi.com)

