Research Article

Triangle and GA Methods for UAVs Jamming

Yu Zhang^{1,2} and Lisheng Yang^{1,2}

¹ College of Communication Engineering, Chongqing University, Chongqing 400030, China

² Center of Communication & Tracking Telemetering Command, Chongqing 400030, China

Correspondence should be addressed to Yu Zhang; 11305650@qq.com

Received 7 May 2014; Accepted 6 July 2014; Published 5 August 2014

Academic Editor: Qingsong Xu

Copyright © 2014 Y. Zhang and L. Yang. 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.

We focus on how to jam UAVs network efficiently. The system model is described and the problem is formulated. Based on two properties and a theorem which helps to decide good location for a jammer, we present the Triangle method to find good locations for jammers. The Triangle method is easy to understand and has overall computational complexity of $O(N^2)$. We also present a genetic algorithm- (GA-) based jamming method, which has computational complex of $O(\mathcal{L}MN^2)$. New chromosome, mutation, and crossover operations are redefined for the GA method. The simulation shows that Triangle and GA methods perform better than Random method. If the ratio of jammers' number to UAVs' number is low (lower than 1/5 in this paper), GA method does better than Triangle method. Otherwise, Triangle method performs better.

1. Introduction

Unmanned aerial vehicles (UAVs) are used for a wide range of missions [1]. They could be utilized within several kinds of warfare like reconnaissance, battle management, chemical-biological warfare, information warfare, and so forth. They may also be included in other possible warfare such as command/control, force protection, suppression of enemy air defenses, and mine counter measures and psychological operations [2]. But with shared wireless communication media, they are highly sensitive to denial it of service attacks [3]. Jamming is one of these attacks. It is a malicious attack whose objective is to disrupt the communication of the victim network intentionally causing interference or collision at the receiver side [4].

Some defense strategies [4–7] are proposed by researchers against jamming in wireless networks. In [6], general concepts for use of multiple vehicles against RADAR systems are described in terms of cooperative path planning and resource allocation. The authors also present several approaches to solve the technical problems. The authors of [7] plan path for UAVs minimize exposure to threats. In [4, 5] the UAVs jamming problem is formulated as a zero-sum pursuit-evasion game and Isaacs' approach is used to obtain motion strategies for a pair of UAVs to evade the jamming attack.

Different from these works, we do research on jamming UAVs network effectively. Some general jamming attack techniques for wireless networks are described in [8, 9]. Jamming attack and network defense strategies are introduced for wireless sensor networks in [10]. The authors of [5] provide motion strategies for a jammer to jam the communication between a pair of UAVs. However, in this paper we focus on jamming a UAVs network. Multijammers are used to work together to cause maximal damage to the UAVs network. We plan to solve the jamming problem in two steps. Step 1 is jamming the UAVs network with a fixed topology. This topology is a snapshot of UAVs in motion at a specific time. The purpose of this step is to find good locations for jammers to disrupting more UAVs communication links. Step 2 is jamming the network for a period of time. Because UAVs are moving, the topology is continuously changing. The jamming problem is more complex than problem in Step 1. We plan to solve the problem of Step 2 after Step 1, and use the result of Step 1 to design strategies for Step 2. The work of Step 2 will not be carried out in this paper. Here, we just handle the problem of Step 1. We contribute to the UAVs jamming research as follows.

- (1) We state the problem of jamming UAVs network and give out the problem formulation.

FIGURE 1: UAVs system architecture.

- (2) We introduce Triangle method and GA (genetic algorithm) based method for the jamming of UAVs network. They perform significantly better than Random method.
- (3) We analyze the simulation result and show how to choose the UAVs jamming method. With fewer jammers, GA method should be chosen. However, when more jammers are available, Triangle method should be considered firstly.

The rest of the paper is organized as follows. The UAVs jamming problem is introduced formulated and analyzed in Section 2. Based on the theorem proved, Triangle jamming method is presented in Section 3. Evolutionary algorithm of GA is introduced and modified for jamming UAVs network in Section 4. The simulation is carried out and the result is analyzed in Section 5. Finally, conclusion is drawn and our future work is planned in Section 6.

2. Jamming Problem Statement

2.1. UAVs System Architecture. We consider jamming the communication in a UAVs network as shown in Figure 1. The UAVs communicate with each other through data links like Link-16 [11]. The location of a UAV in the global coordinate frame is denoted as (x, y, z) , where x , y , and z represent the UAV's longitude, latitude, and altitude, respectively. The set of all UAV locations is denoted as L . Usually the UAVs locate in a restricted area according to their specific tasks. Figure 1 presents such a task area which is a cylinder. The cylinder's radius and height are set to 20 km and 9 km, respectively.

2.2. Jamming Power to Signal Power Ratios (JSR) Model. The jamming power to signal power ratio at the receiver determines the degree to which jamming will be successful. For digital signals, the jammer's goal is to raise this ratio to a level such that the BER is above a certain threshold. For analog voice signals, the goal is to reduce the articulation performance so that the signals are difficult to understand. The following JSR models at the receiver's antenna are defined in [12].

- (1) R^n Model,

$$\xi = \frac{P_{JT}G_{JR}G_{RJ}}{P_TG_{TR}G_{RT}} 10^{n \log_{10}(D_{TR}/D_{JR})}. \quad (1)$$

- (2) Ground reflection propagation,

$$\xi = \frac{P_{JT}G_{JR}G_{RJ}}{P_TG_{TR}G_{RT}} \left(\frac{h_J}{h_T} \right)^2 \left(\frac{D_{TR}}{D_{JR}} \right)^4. \quad (2)$$

- (3) Nicholson,

$$\xi = \frac{P_{JT}G_{JR}G_{RJ}}{P_TG_{TR}G_{RT}} 10^{4 \log_{10}(D_{TR}/D_{JR})}, \quad (3)$$

where P_{JT} is the power of the jammer's transmitting antenna, P_T is the power of the transmitter, G_{TR} is the antenna gain from transmitter to receiver, G_{RT} is the antenna gain from receiver to transmitter, G_{JR} is the antenna gain from jammer to receiver, G_{RJ} is the antenna gain from receiver to jammer, h_J is the height of the jammer antenna above the ground, h_T is the height of the transmitter antenna above the ground, D_{TR} is the Euclidean distance between transmitter and receiver, and D_{JR} is the Euclidean distance between jammer and transmitter.

We use the Nicholson JSR model (3) in this paper. The value of each parameter may be different in different scenarios. We consider scenario in which parameters are set as follows:

$$\begin{aligned} P_{JT} &= 3, & G_{JR} &= G_{RJ} = 1, \\ P_T &= 1, & G_{TR} &= G_{RT} = 1, \\ \xi_{TR} &= 1.2. \end{aligned} \quad (4)$$

When we put parameters of (4) into (3), $\xi = (P_{JT}G_{JR}G_{RJ}/P_TG_{TR}G_{RT})10^{4 \log_{10}(D_{TR}/D_{JR})} = (3 \times 1 \times 1/1 \times 1 \times 1)10^{4 \log_{10}(D_{TR}/D_{JR})} = 1.2$. We get $D_{TR}/D_{JR} = 0.79527$. If D_{JR} is less than $D_{TR}/0.79527 = 1.25743D_{TR}$, then the receiver cannot get data from the sender successfully. Here, D_{JR} is the distance between a jammer and a UAV, and D_{TR} is the distance between a UAV and another UAV. The condition that a UAV's communication link for receiving data from another UAV is jammed can be represented as

$$D_{JR} \leq 1.25743D_{TR}. \quad (5)$$

2.3. Problem Formulation. When formulating the UAVs jamming problem, the following notations are used. $U = \{1, 2, \dots, n\}$ is the set of UAVs, n is an integer and $n \geq 1$; $J = \{1, 2, \dots, m\}$ is the set of jammers, m is an integer and $m \geq 1$, u_i is used to represent UAV i , and l_i and l_j are the location of UAV i and jammer j . The location of UAV is assumed to be restricted into its task area L . The valid location of UAV i is $l_i \in L$.

All UAVs communicate with bidirectional communication links. UAV i uses link $\text{Link}_{i \rightarrow k}$ to send packets to k . At the same time, UAV k sends packets to i through $\text{Link}_{k \rightarrow i}$. The jamming effect is denoted as JE_{jik} . When $\text{JE}_{jik} = 1$, UAV k will not get packets from i ; that is, $\text{Link}_{i \rightarrow k}$ is jammed by

jammer j . Otherwise, $\text{Link}_{i \rightarrow k}$ is not jammed by jammer j . JE_{jik} is represented as

$$\text{JE}_{jik} = \begin{cases} 1, & \xi = \frac{P_{JT}G_{JR}G_{RJ}}{P_TG_{TR}G_{RT}} 10^{4\log_{10}(D_{TR}/D_{JR})} > \xi_0, \\ 0, & \text{others.} \end{cases} \quad (6)$$

The total jamming effect can be computed through adding jamming effect of all links and is denoted as $z = \sum_{j \in J} \sum_{i,k \in U} \text{JE}_{jik}$. Therefore, the objective function for jammers is to maximize z . The jamming problem can be modeled as

$$\begin{aligned} \max \quad & \left(z = \sum_{j \in J} \sum_{i,k \in U} \text{JE}_{jik} \right) \\ \text{subject to:} \quad & l_i \in L, \quad i \in U. \end{aligned} \quad (7)$$

2.4. Problem Analysis. A term of *jamming area* is used for representing an area in which UAVs' receiving links are disrupted by one or more jammers. Jamming area is defined as follows.

Definition 1 (jamming area). UAV k is sending packets to i through $\text{Link}_{k \rightarrow i}$. UAV k is the sender and i is the receiver. The jamming area JA_{ik} is such an area in which UAV i cannot get the packets from k through $\text{Link}_{k \rightarrow i}$, because of the jamming effect of jammers.

As shown in Figure 2, when UAV 1 is sending packets, UAVs 2 and 3 cannot get its packets through $\text{Link}_{1 \rightarrow 2}$ and $\text{Link}_{1 \rightarrow 3}$, because of the existence of jammer 1. For this case, UAV 1 locates such a point which belongs to the jamming area of UAVs 2 and 3. They are denoted as point $(u_1) \in \text{JA}_{21}$ and point $(u_1) \in \text{JA}_{31}$, respectively. However, the point of UAV 1 does not belong to the jamming area of UAV 4, point $(u_1) \notin \text{JA}_{41}$.

Property 1 (asymmetry). When parameters are set as condition (4), if point $(u_k) \in \text{JA}_{ik}$, point of UAV i may belong to JA_{ki} or may not.

Proof. As shown in Figure 2, the distance between UAV 1 and 2 is Len_1 . When UAV 1 is the sender and UAV 2 is the receiver, UAV 2's jamming area includes all the points whose distance to UAV 2 is less than 1.25743Len_1 . When jammer 1 locates at Point 1, the distance between Point 1 and UAV 1 is less than 1.25743Len_1 , so Inequality (5) holds, point $(u_1) \in \text{JA}_{21}$, and point $(u_2) \in \text{JA}_{12}$. When jammer 1 locates at Point 2, the distance between Point 2 and UAV 1 is larger than 1.25743Len_1 , so Inequality (5) does not hold anymore. At this case, point $(u_1) \in \text{JA}_{21}$, but point $(u_2) \notin \text{JA}_{12}$. $\square$

Property 2 (existence of good location). When parameters are set as condition (4), for any two UAV i and k , there exists location point $\text{point}_{\text{good}}$ for a jammer to disrupt both $\text{Link}_{i \rightarrow k}$ and $\text{Link}_{k \rightarrow i}$; that is, $\text{point}_{\text{good}} \in \text{JA}_{ik}$ and $\text{point}_{\text{good}} \in \text{JA}_{ki}$. When a jammer locates at point $\text{point}_{\text{good}}$, communication between UAV i and k will be blocked.

Proof. When the value of each parameter is set as condition (4), Inequality (5) holds. For any two UAV i, k , the jamming area of UAV i will cover the point of UAV j , and vice versa. Then there definitely exists an intersection between the two jamming areas. For example, there is an intersection between the jamming areas of UAV 4 and 5 in Figure 2. When a jammer is located at any one point in such an intersection, UAV i/k will not receive packets from UAV k/i ; that is, the communication between UAV i, k will be blocked. $\square$

Properties 1 and 2 show the fact that the jamming effect of a jammer is closely related to the jammer's location. Property 1 tells us we can find a location for a jammer to prevent a UAV from receiving packets from others, under condition (4). However the jammer may not prevent the UAV from sending packets successfully. Property 2 states that it is possible to find a location for a jammer to block any two UAVs' communication. Based on these, it is clearly that if we plan to maximize z (7), we should focus on searching such locations for jamming.

3. Triangle Method

For achieving better jamming effect, jammers should be placed to appropriate locations. We present Triangle method to search locations for jammers. The idea of Triangle method is simple. It divides all UAVs into groups. Each group has three UAVs. The algorithm for forming such groups is described in Algorithm 2 from Steps (1) to (11). All UAVs are put into a temporary set S_{UAV} in Step (1). The total number of UAV groups is calculated in Step (2) and saved in gr_{num} . Steps (3) and (4) initialize all UAV groups to null. Function $\text{getrandom}(S_{\text{UAV}})$ in Step (7) returns a random UAV in S_{UAV} . Function $\text{neighbors}(u_1, S_{\text{UAV}}, u_2, u_3)$ in Step (8) may return two closest neighbors of u_1 in S_{UAV} and assign to u_2 and u_3 , respectively. If the number of neighbors in S_{UAV} is less than two, the function may return one neighbor or null. In Steps (9) and (10), u_1 and its returned neighbors are added to a group, and then they are removed from S_{UAV} . The group forming process continues till all groups are formed.

Algorithm 2 (Triangle method. See Figure 3). Consider the following:

- (1) $S_{\text{UAV}} = U$,
- (2) $\text{gr}_{\text{num}} = \lceil |S_{\text{UAV}}|/3 \rceil$,
- (3) for $a = 1$ to gr_{num} ,
- (4) $\text{GR}_a = \emptyset$,
- (5) $a = 1$,
- (6) $S_{\text{UAV}} \neq \emptyset$,
- (7) $u_1 = \text{getrandom}(S_{\text{UAV}})$,
- (8) $\text{neighbors}(u_1, S_{\text{UAV}}, u_2, u_3)$,
- (9) $\text{GR}_a = \text{GR}_a + u_1 + u_2 + u_3$,
- (10) $S_{\text{UAV}} = S_{\text{UAV}} - u_1 - u_2 - u_3$,
- (11) $a++$,
- (12) $L_{\text{select}} = \emptyset$,

FIGURE 2: Jamming area.

FIGURE 3: Triangle method.

Steps from (12) to (15) find locations for UAV groups. The function selectpoint (GR_a) works as follows.

- (1) The group has three UAVs which usually form a triangle. (a) The function calculates the distances between each pair of two points; (b) it finds the two short sides; (c) it selects the point which connects the two short sides as the location for the group.
- (2) The group has two UAVs which usually form a line. (a) The function calculates the midpoint between each pair of two points; (b) it returns the midpoint as the location for the group.
- (3) The group has only one UAV. The function returns the location of the UAV as the location for the group.

The selecting process continues till all locations for groups are found. Function assignlocations (L_{select}, J) assigns the locations found to jammers. If the number of jammer m is equal to or less than gr_{num} , then the first m elements of L_{select} are assigned to jammers accordingly. If $m > gr_{\text{num}}$, then gr_{num} jammers are assigned the locations of L_{select} , and $m - gr_{\text{num}}$ jammers are assigned random locations.

The Triangle method is based on following theorem.

Theorem 3. When parameters are set as condition (4), function selectpoint (GR_a) outputs an optimal location on which if a jammer is placed, all communications among UAVs in the group will be disrupted.

(13) for $a = 1$ to gr_{num} ,

(14) $l_{\text{select}} = \text{selectpoint}(GR_a)$,

(15) $L_{\text{select}} = L_{\text{select}} + l_{\text{select}}$,

(16) assignlocations (L_{select}, J).

Proof. (1) There are 3 UAVs in the group. As shown in Figure 3, the side length Len_3 is not less than Len_1 and Len_2 . So the jammer should be located at the point of UAV 1. When the values of parameters are set as condition (4), Inequality (5) holds. For any two UAV i, k , the jamming area of UAV i will cover the point of UAV j , and vice versa. So point $(u_3) \in \text{JA}_{23}$, point $(u_2) \in \text{JA}_{32}$, point $(u_1) \in \text{JA}_{21}$, and point $(u_1) \in \text{JA}_{31}$. Because $\text{Len}_1 \leq \text{Len}_3$ and $\text{Len}_2 \leq \text{Len}_3$, point $(u_1) \in \text{JA}_{23}$ and point $(u_1) \in \text{JA}_{32}$. Since the jammer is placed at the same location of UAV 1, $D_{JR} \rightarrow 0$, point $(u_1) \in \text{JA}_{12}$, and point $(u_1) \in \text{JA}_{13}$. Therefore all communications among UAVs in the group will be disrupted by the jammer which locates at the point of UAV 1.

(2) There are 2 UAVs in the group. As shown in Figure 3, the jammer will be placed at the midpoint between UAVs 4 and 5. Obviously, point $(u_4) \in \text{JA}_{54}$ and point $(u_5) \in \text{JA}_{45}$. For $\text{Len}_4 \leq \text{Len}_5$, point (Mid) $\in \text{JA}_{54}$, and point (Mid) $\in \text{JA}_{45}$. Therefore the communication between UAVs 4 and 5 will be disrupted by the jammer.

(3) There is only 1 UAV in the group. The location of the UAV is selected as the location for the jammer. At this case, $D_{JR} \rightarrow 0$, $\xi > \xi_0$ in (6) always holds, and all communication links from and to the UAV will be blocked. $\square$

In Algorithm 2, the while loop (Step (6)) will run $\mathcal{N}$ times at most, and $\mathcal{N}$ is the number of UAVs. The function neighbors (Step (8)) search UAV's two neighbors, and each UAV will be visited at most two times. So the code from Steps (6) to (11) has computational complexity of $O(\mathcal{N}^2)$. The code of Step (16) has computational complexity of $O(\mathcal{M})$, where $\mathcal{M}$ is the number of jammers. The overall computational complexity of Algorithm 2 is $O(\mathcal{N}^2)$.

4. GA-Based Jamming Method

GAs are global optimization techniques that avoid many of the shortcomings that exist in classical local search techniques on difficult search spaces [13]. GAs use operators such as reproduction, crossover and mutation as means of preserving beneficial information with the overall goal of finding a better solution to the problem. In addition, genetic algorithms work using codification of the parameter space rather than the parameters themselves. The objective function can be easily defined as a measure of fitness for solution performance which allows the genetic algorithm to retain useful solutions and inhibit those which are less useful.

We propose a GA-based method to solve the UAV jamming problem, as shown in Algorithm 4. The key to finding a good solution using a GA lies in developing a good chromosome representation of candidate solutions to the problem. The chromosome we used includes three parts, xyz , where x , y , and z are of float type and represent a jammer's longitude, latitude, and altitude, respectively. When two chromosomes $x_1y_1z_1$ and $x_2y_2z_2$ cross over, a new chromosome is formed $x_{\text{new}}y_{\text{new}}z_{\text{new}}$. We define them as $x_{\text{new}} = (x_1 + x_2)/2$, $y_{\text{new}} = (y_1 + y_2)/2$, and $z_{\text{new}} = (z_1 + z_2)/2$. A chromosome mutates with a probability of p_{mutation} . The mutation operation is defined as $x_{\text{new}} = \pm 0.8 \times x_{\text{old}}$, $y_{\text{new}} = \pm 0.8 \times y_{\text{old}}$, and $z_{\text{new}} = \pm 0.8 \times z_{\text{old}}$.

A solution of the jamming problem consists of m chromosomes, where m is the number of jammers. The population has $\mathcal{L}$ solutions. Initially, a random parent population P_0 is created. Then binary tournament selection [14], crossover, and mutation operators are used to create an offspring population Q_0 which has $2\mathcal{L}$ solutions. The next parent population P_1 is created by selecting $\mathcal{L}$ solutions from Q_0 with binary tournament method. The new offspring population Q_1 is formed through crossover and mutation operation. The process continues until the last population P_1 is reached.

Algorithm 4 (GA method). Consider the following:

- (1) generate an initial population ($\mathcal{P}$ solution);
- (2) while loop times $< \mathcal{L}$;
- (3) evaluate the fitness of each solution;
- (4) select promising solutions;
- (5) create new solutions incorporate into original population.

The procedure of evaluating the fitness (Step (3)) requires $\mathcal{N} \times \mathcal{N} \times \mathcal{M}$ computations, where $\mathcal{N}$ and $\mathcal{M}$ are the number of UAVs and jammers, respectively. Its computational complex is $O(\mathcal{M}\mathcal{N}^2)$. Since binary tournament solution is used, the procedure of selecting (Step (4)) has computational complex of $O(\mathcal{P})$. The new solutions creating procedure (Step (5)) have computational complex of $O(\mathcal{P} + \mathcal{P}\mathcal{N})$. Therefore the computational complex of Algorithm 4 is $O(\mathcal{L}\mathcal{M}\mathcal{N}^2)$, and $\mathcal{L}$ is the number of evolution iterations.

5. Simulation

The methods provided by this paper are used to jam the communication among 20, 30, 40, and 50 UAVs with 1~20 jammers, respectively. The simulation result is shown in Figure 4. We also include a Random method for comparing Triangle and GJM methods. The Random method works in a simple way. The jammers are located in random positions in this method. The Random method has computational complexity of $O(\mathcal{M})$, where $\mathcal{M}$ is the number of jammers.

We define a new metric to measure the performance of each jamming method.

Definition 5. The ratio of jammed links to total links (RJT) computed by $\sum_{i,k \in U, i \neq k} \text{JammedLink}_{i \rightarrow k} / \sum_{i,k \in U, i \neq k} \text{Link}_{i \rightarrow k}$.

We can see easily from Figure 4 that the number of jammers has tight relation to the overall jamming performance. In Triangle and GA methods, more jammers lead to higher jamming performance. In Figures 4(a) and 4(b), when 8 or more jammers are used, the RJTs of Triangle and GA reach 98% and 97%. In Figures 4(c) and 4(d), when 10 or more jammers are used, the RJTs of Triangle and GA reach 98% and 97%. When 11 or more jammers are used, the RJTs of both Triangle and GA reach 97%. For Random method, it is obvious that, at most time, more jammers yield higher performance.

FIGURE 4: Simulation result.

It is also clear that Triangle and GA methods give out better result than Random method. But there is an exception when 1 jammer is used to jam the communication network with 40 UAVs. All jammers are randomly placed in Random method. One of them happens to be assigned a good location. So the Random method performs better than the Triangle method as shown in Figure 4(c), when both methods use one jammer. This can be explained with the probability. Let the probability for one jammer assigned a good location be p_r ($0 < p_r < 1$). When there are two jammers, the probability becomes p_r^2 . When there are c jammers, the probability decreases to p_r^c . So with the number of jammers increasing, the probability of all jammers assigned good locations is decreasing. That is why, in most cases, the jammers in Random method perform worse than jammers in Triangle and GA methods in Figure 4.

Figure 4 shows that, with a small number of jammers, GA method has better performance than Triangle method. However, with the number of jammers increasing, the performance of Triangle method is improved more than GA method. The gap between these two methods is narrowed. When more jammers are used, Triangle method outputs similar results as GA method does and then does better than GA method. The reason is that GA is a global optimization algorithm, and Triangle method is a local optimization algorithm. When the number of jammers is small, GA can find better locations for jammers than Triangle method does. However, GA method has difficulties to find good locations for a big number of jammers, because of the significantly increased search space. Triangle method outperforms when more numbers of jammers are used. Because the local optimization location for each group is guaranteed, the overall performance (added performance of all jammers) can also be guaranteed. From the simulation, we get a roughly result that when the ratio of jammers' number to UAVs' number is lower than 1/5, GA method may perform better than Triangle method. Otherwise, Triangle method may outperform GA method.

It is also obvious that there is a threshold δ of the number of jammers m . When m is smaller than δ , with the increasing of the number of jammers, the overall jamming performance increases rapidly. When m is larger than δ , with the number increasing, the overall jamming performance increases very slowly. As shown in Figure 4, the thresholds are 7, 9, 10, 11, 12, and 13 for jamming the network with 20, 30, 40, 50, 60, and 70 UAVs, respectively. To maximize the effect of jammers, m should be set as equal to or smaller than δ . For example, when jamming the communication among 50 UAVs, using 11, 12, or 13 jammers outputs the same RJTs in Triangle, GA, or Random methods, respectively. Therefore, 11 jammers are enough for achieving such jamming results. So adding one or two more jammers is meaningless for improving the jamming performance. The thresholds are task dependent and may be decided according to different scenarios.

6. Conclusion

In this paper, we focus on jamming UAVs network efficiently. Firstly, the system architecture is described and the

jamming problem is formulated. We analyze the system's two properties. Secondly, a theorem, which helps to decide locations for jammers, is proved. Based on this theorem, we introduce the Triangle method to solve the jamming problem. Triangle method divides all UAVs into groups. Each group has at most three UAVs. It finds the best location for jamming all UAVs in each group. The overall computational complexity of Triangle method is $O(\mathcal{N}^2)$, where $\mathcal{N}$ is the number of UAVs. Thirdly, we present a GA-based jamming method. The chromosome consists of the longitude, latitude, and altitude of the jammer. New mutation and crossover operations are also redefined. GA method's computational complex is $O(\mathcal{L}\mathcal{M}\mathcal{N}^2)$, where $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$ are the number of evolution iterations, jammers, and UAVs, respectively.

The two methods besides a Random method are simulated in the scenario given in Section 2. The simulation uses number of jammers range from 1 to 20 to jam the network with 20, 30, 40, and 50 UAVs, respectively. The chromosome mutation probability is set as $p_{\text{mutation}} = 0.1$. The result shows the following.

- (1) More jammers yield higher performance.
- (2) At most cases, Triangle and GA methods are significantly better than Random method.
- (3) With a small number of jammers, GA method has better performance than Triangle method. However, with the number of jammers increasing, the performance of Triangle method is improved more than GA method. When the ratio of jammers' number to UAVs' number is higher than 1/5, Triangle method does better than GA method.
- (4) The overall computational complexity of Triangle method is $O(\mathcal{N}^2)$ which is lower than $O(\mathcal{L}\mathcal{M}\mathcal{N}^2)$ of GA method. If computing speed is required, especially for the real time application, Triangle method should be considered.

It should be noted that this paper just does the work of the first step. Here, we assume the topology of UAVs is fixed and does not change. The properties and theorem are deduced under condition (4). The condition can be relaxed to $P_{JT}G_{JR}G_{RJ} \geq \xi_{TR}P_TG_{TR}G_{RT}$. It will be proved in our next step. We will consider jamming the UAVs networks with moving nodes, which have highly dynamic topologies. The work of this paper is the basis for the next step.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work is supported by the Academician Foundation of Chongqing (CSTC2011GGYS0001).

References

- [1] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber attacks—an approach to the risk assessment," in *Proceedings of the 5th International Conference on Cyber Conflict (CyCon '13)*, pp. 1–23, 2013.
- [2] P. Cevik, I. Kocaman, A. S. Akgul, and B. Akca, "The small and silent force multiplier: a swarm UAV-electronic attack," *Journal of Intelligent and Robotic Systems: Theory and Applications*, vol. 70, no. 1–4, pp. 595–608, 2013.
- [3] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "Performance of IEEE 802.11 under Jamming," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 678–696, 2013.
- [4] S. Bhattacharya and T. Basar, "Game-theoretic analysis of an aerial jamming attack on a UAV communication network," in *Proceedings of the American Control Conference (ACC '10)*, pp. 818–823, July 2010.
- [5] S. Bhattacharya and T. Başar, "Differential game-theoretic approach to a spatial jamming problem," in *Advances in Dynamic Games*, vol. 12 of *Annals of the International Society of Dynamic Games*, pp. 245–268, Birkhäuser, Boston, Mass, USA, 2013.
- [6] M. J. Mears, "Cooperative electronic attack using unmanned air vehicles," in *Proceedings of American Control Conference*, pp. 3339–3347, 2005.
- [7] Y. M. Chen and W.-Y. Wu, "Cooperative electronic attack for groups of unmanned air vehicles based on multi-agent simulation and evaluation," *International Journal of Computer Science Issues*, vol. 9, no. 2, p. 1, 2012.
- [8] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.
- [9] A. Mpitzopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.
- [10] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attack strategies and network defense policies in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119–1133, 2010.
- [11] B. Lee, E. Jeong, and S. Choe, "Simulator for tactical data link system with anti-jamming capability," in *Proceedings of the 15th International Conference on Advanced Communication Technology (ICACT '13)*, pp. 789–793, January 2013.
- [12] R. Poisel, *Modern Communications Jamming Principles and Techniques*, Artech House, 2011.
- [13] B. Skinner, S. Yuan, S. Huang et al., "Optimisation for job scheduling at automated container terminals using genetic algorithm," *Computers and Industrial Engineering*, vol. 64, no. 1, pp. 511–523, 2013.
- [14] R. Sivaraj and T. Ravichandran, "A review of selection methods in genetic algorithm," *International Journal of Engineering Science & Technology*, vol. 3, no. 5–6, pp. 3792–3797, 2011.