An Improved Ant Colony Algorithm Based Cluster Control Method for Hybrid Networking of UAV Communication

Hanjie Yuan[1*], Yong He[1], Yaohua Zheng[1], Limeng Dong[1], Jianan Yao[1], Yu Zhang[1], Lin Lu[1], Qi Tan[1], Tianhang Jiang[1], Haiao Tan[1]

[1] Guangdong Power Grid Co., Ltd. Zhaoqing Power Supply Bureau, Zhaoqing, Guangdong, 526000, China

*Corresponding author's e-mail: 348508973@qq.com

Abstract. The current UAV cluster control method based on multi-path planning achieves the planning of UAV flight routes through situational awareness technology, which leads to a long planning time due to the lack of defense against attack behaviors. In this regard, a cluster control method based on improved ant colony algorithm for UAV communication hybrid network is proposed. The constraint function of the UAV planning path is established, the attack behavior of the attack nodes is analyzed, the detection and processing method of the attack behavior is proposed, and the planning process of the UAV flight path is constructed. In the experiments, the proposed method is verified in terms of search time. The analysis of the experimental results shows that the UAV cluster control technique constructed by the proposed method possesses a low search time.

Keywords: Hybrid networking; Improved ant colony algorithm; UAVs; Cluster control methods

1 Introduction

The current traditional UAV communication hybrid network cluster control method mainly realizes collaborative decision making of path planning through situational awareness technology. This method can propose the planning strategy of UAV flight routes and realize the control of UAV clusters, but there are also certain limitations. First, in the process of controlling UAVs, the network is usually used as a carrier to realize the transmission of signals between them. The current network environment is complex, and there are usually third-party attacks, which can lead to errors in the transmission of UAV commands, thus affecting the overall control effect and having a negative impact on the search time. The current traditional UAV cluster control method lacks the defense of attack behavior, not only lacks the analysis of the attack behavior, but also has a weak processing and resistance ability for the attack, resulting in a low overall control efficiency. In this regard, it is necessary to analyze the attack behavior of the attacking nodes, and establish a model of forgery attack for the attack charac-

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 421–428, 2022.
https://doi.org/10.2991/978-94-6463-108-1_48

teristics. Through the detection of the attack behavior, the processing of the forgery attack is realized, so as to provide a safe operating environment for the UAV cluster control technology and improve the search efficiency of the task. In this regard, a new type of UAV communication hybrid network cluster control method is needed, aiming to analyze the attack behavior, improve the resistance capability, and build out a perfect UAV control process. The robustness of the ant colony algorithm is more suitable for application in this field, and the convergence speed of its algorithm is faster, which can achieve efficient search [1-3].

2 Modeling UAV communication forgery attack based on improved ant colony algorithm

When controlling a hybrid network cluster for UAV communication, the UAV cluster is usually subject to forgery attacks in many aspects due to the complexity of the network environment. Therefore, it is necessary to detect forgery attacks in real time and adopt technical means to dissolve them in order to provide a good operating environment for UAV clusters [4-6]. The general UAV cluster control algorithm relies heavily on the information of the surrounding environment and cannot adapt quickly to the new environment. Therefore, to solve this problem, we need to establish the constraint function of the UAV planning path model, and then use the improved ant colony algorithm to optimize the solution of the UAV cluster obstacle avoidance model for the communication hybrid network. Firstly, the range of the model boundary needs to be constrained so that the UAV cluster can capture the signal of the forged attack during the actual navigation. If the signal of the forgery attack is successfully captured, the node of the forgery attack needs to be regarded as an obstacle with no motion state and obstacle avoidance is performed. If the signal of the forged attack is not successfully captured during the navigation, the mission can be completed according to the established navigation plan.

The forgery attack refers to the attack on the UAV cluster by forging a certain communication node and setting that node as the target node, thus intercepting the path of the UAV to the actual target node. The specific steps of the forged node attack on UAVs are shown in the following figure.

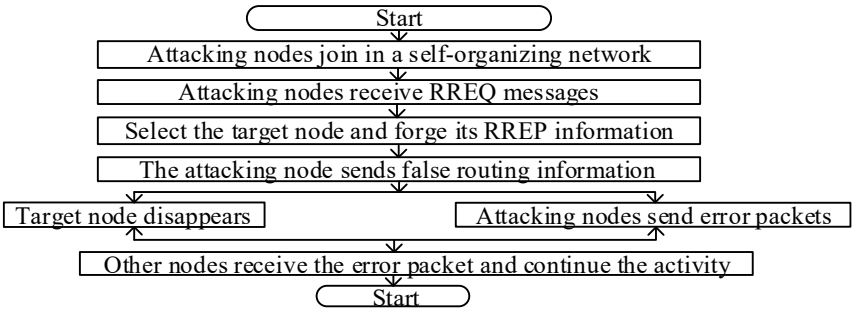

Fig. 1. Flow chart of forgery attack

According to the flowchart of the above forgery attack, it can be seen that the attacking node will first join the hybrid group network to receive the routing request information when it attacks the target UAV. Since the wireless link of the hybrid network summary is in an open state, any node can enter the network, and the attack node can easily get the route request information inside the hybrid network. After getting the route request information, the attack node starts to select any node within the allowed attack range as the target attack node and sends fake route request information to all communication nodes except the target node, so that the target attack node is isolated from the hybrid network, which eventually leads to the target attack node being forced to withdraw from the communication link of the hybrid network. Subsequently, the forged attack node replaces the target node, sends route request information and obtains the data information transmitted by other nodes, and transmits the false data information [7-8]. After receiving the fake data information, the other nodes transmit the information to the decision system, which plans the UAV routes according to the fake information.

According to the process analysis of the forgery attack mentioned above, it is known that when the UAV cluster is planning the path, in addition to avoiding and handling the forgery attack, it is also necessary to constrain the safety distance to prevent the collision between UAVs [9]. In this regard, it is necessary to constrain the path of UAVs with the following formula.

$$\|x_i - x_j\| \geq D \tag{1}$$

Where, $\mathrm{x_i} = [\mathrm{x_i}, \mathrm{y_i}, \mathrm{z_i}]$ represents the coordinate vector of the UAV $\mathrm{UAV_i}$, $\mathrm{x_j} = [\mathrm{x_j}, \mathrm{y_j}, \mathrm{z_j}]$ represents the coordinate vector of the UAV $\mathrm{UAV_j}$, and D represents the safe distance to be maintained for the UAV flight.

Since there is a limit of communication distance in the hybrid network of wireless communication, the communication between UAVs needs to be constrained in order to improve the communication quality as follows.

$$\|\mathrm{x_i} - \mathrm{x_j}\| \leq \mathrm{D_{max}} \tag{2}$$

Where, $\mathrm{D_{max}}$ represents the maximum distance of UAV communication. When the UAV cluster is attacked by forgery, since the information transmitted in the UAV cluster is mainly the location information of the UAV nodes, the attacking node can be regarded as an obstacle node, and the UAV obstacle avoidance operation can be realized by updating the flight environment information. Assuming that the stationary obstacle is a sphere with radius R in the 3D flight environment, a model of the stationary obstacle can be constructed with the center of the sphere as the center coordinate, and the specific model expression is as follows.

$$\begin{cases} \|\mathrm{x} - \mathrm{x_i}\| = \mathrm{R} \\ \|\mathrm{x} - \mathrm{x_{i+1}}\| = \mathrm{R} \\ \mathrm{R} = \max\{\mathrm{D}, \rho\} \end{cases} \tag{3}$$

Where, $\mathrm{x} = [\mathrm{x}, \mathrm{y}, \mathrm{z}]$ represents the coordinates of the node position on the surface of the stationary obstacle, $\mathrm{x_i} = [\mathrm{x_i}, \mathrm{y_i}, \mathrm{z_i}]$ represents the coordinates of the targeted UAV

node position, $x_{i+1} = [x_{i+1}, y_{i+1}, z_{i+1}]$ represents the coordinates of the position of the forged attack node, and ρ represents the step size in the ant colony algorithm.

According to the above steps, the path and communication behavior of the UAV cluster can be planned for the attack characteristics of the attack nodes, providing the basis for the subsequent UAV cluster control method.

3 UAV communication forgery attack detection and handling

For the communication path of the UAV cluster in the hybrid network, the attack characteristics of the attacking nodes are combined with the differential constraints on the dynamic information of the nodes as a way to achieve the detection of forgery attacks, as shown in the following equations.

$$\begin{cases} \left\| x_i^{k-1} - x_i^k \right\| \le \rho, 1 \le k \le \text{ num} \\ \left\| x_i^{k-1} - x_j^k \right\| \le D_{max}, i \ne j \end{cases} \tag{4}$$

Where, x_i^k represents the node-specific position of the i-th drone at moment k and represents the number of iterations of the ant colony algorithm.

If the motion trajectory of the UAV cluster does not meet the above conditions, it means that the UAV cluster is being attacked by the attack node at this moment, i.e., in order to detect the attack behavior, the attack node can be converted into a stationary obstacle, and the processing of the attack behavior can be realized through the UAV obstacle avoidance operation [10]. If the motion trajectory meets the above conditions, it means that the UAV cluster is not under attack at this moment and can fly according to the established planning route.

For the detected attacks, the octree partitioning principle can be used to achieve UAV obstacle avoidance. Assuming that the time series is $t = 1,2,3, \ldots r$, then the UAV data information recorded at each moment is $i_0, i_1, i_2, \ldots i_T$, and the environmental data can be updated for the nth node, as shown in the following expression.

$$p(n \mid i) = \frac{1-p[n|i_{n+1}]}{p[n|i_n]} \cdot \frac{1-p[n|i_{t+1}]}{p[n|i_t]} \tag{5}$$

The logit transformation of the above equation leads to the following expression.

$$\vartheta = \log\left(\frac{p}{1-p}\right) \tag{6}$$

The following expression can be obtained by inverting the above equation.

$$p = \frac{1}{1+\exp(-\vartheta)} \tag{7}$$

where represents log-odds, using $L(n \mid i)$ to represent the log-odds of each communicating node, the following expression can be obtained.

$$L(n \mid i_{1:T}) = L(n \mid i_T) + l(n \mid i_{T-1}) \tag{8}$$

The above formula enables the update of UAV flight environment information and the processing of attack behavior by avoiding stationary obstacles.

4 UAV cluster path planning

Before the UAV cluster path is planned, the UAVs need to be formed, and the formation is done by calling IDs, naming each UAV as UAV+ID, and the specific generation of IDs is done in a three-decimal way, and the specific ID design is shown below.

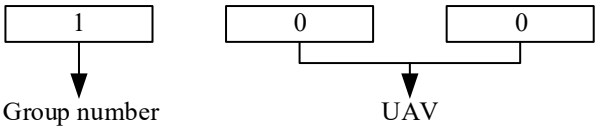

Fig. 2. Drone ID numbering method

The hundreds digit represents the group number of the drone, and the digits and tens digits are combined to represent the ID number of the drone.

After the UAV is numbered in the above way, the path of the UAV can be planned using the ant colony algorithm, and the specific idea is to update the pheromone by setting the enhancement factor of the pheromone. The search of the path is realized according to the updated pheromone [11-13]. According to the ant colony algorithm, the expression of the enhancement coefficient of the pheromone is shown below.

$$Q(i,j) = \begin{cases} A, i = j \\ B, i \neq j \end{cases} \tag{9}$$

Where, $Q(i,j)$ represents the corresponding enhancement coefficient when the UAV node moves from i to j, and A and B represent the ant colony coefficients. Then the corresponding pheromone concentrations can be found, and the expressions are as follows.

$$T_{ij}(t) = \sum_{k=1}^{M} \Delta t_{ij}(t) \tag{10}$$

$$t_{ij}(t+n) = (1-\rho) \cdot T_{ij}(t) \tag{11}$$

$$p_{ij} = \begin{cases} \frac{t_{ij}^{\alpha} \cdot d_{ij}^{\beta}}{\sum_{j \in N_k} t_{ij}^{\alpha}} \\ 0 \end{cases} \tag{12}$$

Where, $T_{ij}(t)$ represents the information concentration between nodes i and j at moment t, α represents the heuristic factor of information, β represents the desired heuristic factor, p represents the information volatility factor, and d_{ij} represents the distance between the UAV cluster and the mission target. The update of the pheromone can be achieved according to the above steps, for which the flow chart of UAV path planning can be constructed as shown in the following figure.

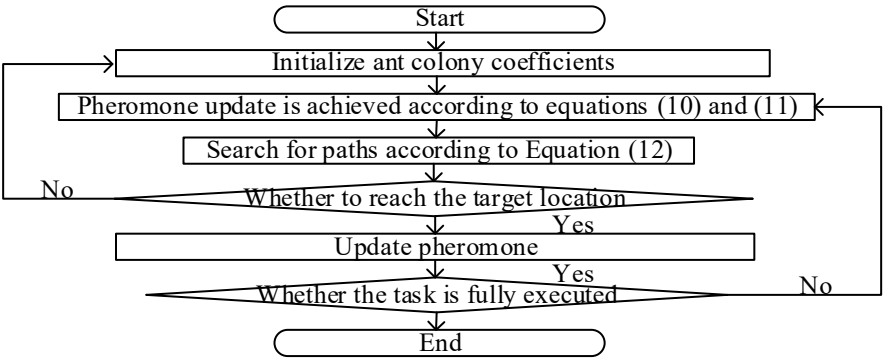

Fig. 3. Flow chart of UAV path planning

According to the above steps, the path planning of UAV cluster can be completed, and this part is combined with the above-mentioned UAV communication forgery attack model establishment and attack detection processing, so that the design of UAV communication hybrid network cluster control method based on improved ant colony algorithm is completed [14-15].

5 Testing and Analysis

5.1 Test Preparation

In order to be able to draw accurate test results, the hybrid UAV communication cluster control method based on improved ant colony algorithm in the paper is tested. To improve the accuracy of the test results, the traditional control methods are used as the comparison objects, which are the UAV cluster control method based on biological cluster behavior and the UAV cluster control method based on multi-path planning. The experiment uses Matlab simulation software to build out a simulation experimental environment, simulating a total of 20-100 search tasks in the environment, with 10 search nodes as test nodes, and three control methods are used to test this test node respectively. To improve the reliability of the experimental results, the same configuration is taken for the three control methods, and the search time required by the control methods in the face of different number of tasks is compared.

5.2 Analysis of test results

The evaluation index of this test is the time required by the UAV cluster control method, and by setting a number of different search tasks and comparing the time required by the control method with different number of tasks, then the effective degree and efficiency of the UAV cluster control method can be judged, and the specific experimental results are shown in the following figure, where the traditional UAV cluster control method 1 represents the UAV based on biological cluster behavior The

specific experimental results are shown in the figure below, where the traditional UAV cluster control method 1 represents the UAV cluster control method based on biological cluster behavior, and the traditional UAV cluster control method 2 represents the UAV cluster control method based on multi-path planning.

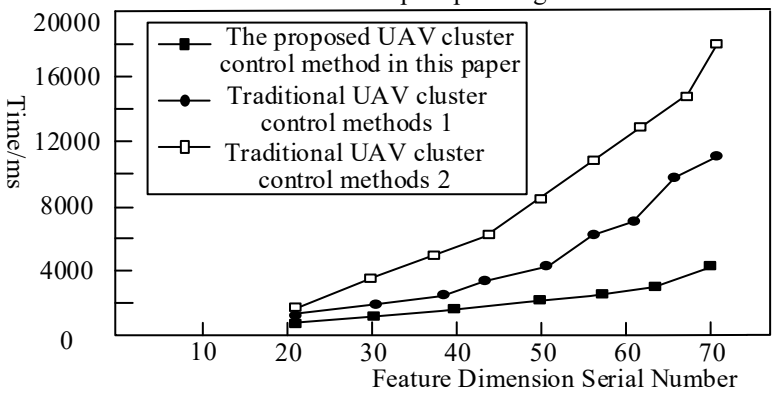

Fig. 4. Search time comparison

According to the above experimental results, it can be seen that the search time required by the UAV cluster control method varies when facing different numbers of search tasks. The larger the number of search tasks, the longer the time required. The time comparison shows that the time required by the hybrid UAV communication cluster control method based on the improved ant colony algorithm proposed in this paper is significantly shorter, which indicates that its control efficiency is higher and can effectively control the UAV cluster.

6 Conclusion

The article proposes a hybrid UAV communication cluster control method combined with improved ant colony algorithm, which effectively circumvents the attacking behavior by analyzing the behavior of attacking nodes and scientifically plans the path of UAV clusters. In the future work, the stability of the UAV cluster management platform still needs to be analyzed and a more adaptable UAV scheduling algorithm is proposed.

References

1. Tian, H. (2021). Research on robot optimal path planning method based on improved ant colony algorithm. International Journal of Computing Science and Mathematics, 13(1), 80-92.
2. Zhao, H., Zhou, H., & Yang, G. (2021, February). Research on Global Path Planning of Artificial Intelligence Robot Based on Improved Ant Colony Algorithm. In Journal of Physics: Conference Series (Vol. 1744, No. 2, p. 022032). IOP Publishing.

3. Yi, N., Xu, J., Yan, L., & Huang, L. (2020). Task optimization and scheduling of distributed cyber–physical system based on improved ant colony algorithm. Future Generation Computer Systems, 109, 134-148.
4. Lv, G., & Chen, S. (2020). Routing optimizationin wireless sensor network based on improved ant colony algorithm. International Core Journal of Engineering, 6(2), 1-11.
5. Chen, Y., & Zhou, X. (2021, February). Path planning of robot based on improved ant colony algorithm in computer technology. In Journal of Physics: Conference Series (Vol. 1744, No. 4, p. 042092). IOP Publishing.
6. Wu, W., & Wei, Y. (2021). Guiding unmanned aerial vehicle path planning design based on improved ant colony algorithm. Mechatronic Systems and Control, 49(1), 48-54.
7. Wu, F. (2021). Contactless distribution path optimization based on improved ant colony algorithm. Mathematical Problems in Engineering, 2021.
8. Xin, C., Luo, Q., Wang, C., Yan, Z., & Wang, H. (2021, March). Research on route planning based on improved ant colony algorithm. In Journal of Physics: Conference Series (Vol. 1820, No. 1, p. 012180). IOP Publishing.
9. Wang, Y., Yang, R. R., Xu, Y. X., Li, X., & Shi, J. L. (2021). Research on multi-agent task optimization and scheduling based on improved ant colony algorithm. In IOP Conference Series: Materials Science and Engineering (Vol. 1043, No. 3, p. 032007). IOP Publishing.
10. Ge, J., Yu, D., & Fang, Y. (2021, April). Multi-dimensional QoS Cloud Computing Task Scheduling Strategy Based on Improved Ant Colony Algorithm. In Journal of Physics: Conference Series (Vol. 1848, No. 1, p. 012031). IOP Publishing.
11. Shi, H. Q., & Hao, Z. (2021, April). A Dynamic Load Balancing Strategy Based on Improved Ant Colony Algorithm. In Journal of Physics: Conference Series (Vol. 1871, No. 1, p. 012140). IOP Publishing.
12. Li, C., Liu, Q., Song, S., Huang, T., & Zhu, Q. (2022, February). Path Planning for Mobile Robots Based on an Improved Ant Colony Algorithm with Gaussian Distribution. In Journal of Physics: Conference Series (Vol. 2188, No. 1, p. 012005). IOP Publishing.
13. Li, S. (2020). Optimization analysis of autonomous obstacle avoidance path for self-driving vehicles based on improved ant colony algorithm. In Journal of Physics: Conference Series (Vol. 1453, No. 1, p. 012057). IOP Publishing.
14. Lu, S. (2020). Multi-objective workshop scheduling of marine production based on improved ant colony algorithm. Journal of Coastal Research, 107(SI), 222-225.
15. Li Keyu, Lu Yonggeng, Bao Shitong&Xu Peizhen. (2021). 3D obstacle avoidance planning of UAV based on improved RRT algorithm Computer Simulation (08), 59-63+96.