sensors

Article

A Low Complexity Persistent Reconnaissance Algorithm for FANET

Yuan Guo [1,2], Hongying Tang [1] and Ronghua Qin [1,*]

[1] Science and Technology on Micro-System Laboratory, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China
[2] The School of Electronic, Electrical and Communication Engineering, University of Chinese Academy of Sciences, Beijing 100049, China
* Correspondence: qinrh@mail.sim.ac.cn; Tel.: +86-173-0183-4283

Abstract: In recent years, with the rapid progress of unmanned aerial vehicle (UAV) technology, UAV-based systems have been widely used in both civilian and military applications. Researchers have proposed various network architectures and routing protocols to address the network connectivity problems associated with the high mobility of UAVs, and have achieved considerable results in a flying ad hoc network (FANET). Although scholars have noted various threats to UAVs in practical applications, such as local magnetic field variation, acoustic interference, and radio signal hijacking, few studies have taken into account the dynamic nature of these threat factors. Moreover, the UAVs' high mobility combined with dynamic threats makes it more challenging to ensure connectivity while adapting to ever-changing scenarios. In this context, this paper introduces the concept of threat probability density function (threat PDF) and proposes a particle swarm optimization (PSO)-based threat avoidance and reconnaissance FANET construction algorithm (TARFC), which enables UAVs to dynamically adapt to avoid high-risk areas while maintaining FANET connectivity. Inspired by the graph editing distance, the total edit distance (TED) is defined to describe the alterations of the FANET and threat factors over time. Based on TED, a dynamic threat avoidance and continuous reconnaissance FANET operation algorithm (TA&CRFO) is proposed to realize semi-distributed control of the network. Simulation results show that both TARFC and TA&CRFO are effective in maintaining network connectivity and avoiding threats in dynamic scenarios. The average threat value of UAVs using TARFC and TA&CRFO is reduced by 3.99~27.51% and 3.07~26.63%, respectively, compared with the PSO algorithm. In addition, with limited distributed moderation, the complexity of the TA&CRFO algorithm is only 20.08% of that of TARFC.

Keywords: unmanned aerial vehicles; FANET; PSO-based; relay node placement; persistent reconnaissance; dynamic threat avoidance; low complexity

check for updates

Citation: Guo, Y.; Tang, H.; Qin, R. A Low Complexity Persistent Reconnaissance Algorithm for FANET. *Sensors* **2022**, *22*, 9526. https://doi.org/10.3390/s22239526

Academic Editors: Xueyun Wang and Stefano Caizzone

Received: 24 October 2022
Accepted: 2 December 2022
Published: 6 December 2022

1. Introduction

Due to recent advances in technology for small unmanned aerial vehicles (UAVs), the application of a flying ad hoc network (FANET) has received a significant boost in the military, industrial, and civil sectors. Small UAVs or quadcopters often have reduced performance in order to reduce weight and cost compared to traditional UAVs that can complete their missions alone. The greatest strength of small UAVs lies in their ability to form a mission network and cooperate to complete complex tasks. As a result, a multi-UAV cooperation, or FANET, has been in the spotlight of the research community over the years. Scholars have made a detailed exploration of the FANET from different perspectives, such as routing protocols, deployment, hierarchical structure, algorithm optimization, and applications.

Various routing protocols have been proposed to optimize the performance of the FANET [1–5]. The authors in [1] have carefully designed the application of IEEE 802.11 MAC in the FANET. Through an exhaustive performance analysis, they have obtained some instructive conclusions. Khan et al. [2] use a specifically designed protocol for FANETs that considers the interest characteristics of FANETs, but the path to destination sometimes is not optimized and creates a closed-loop route. Considering the fast dynamic nature of nodes in FANETs, Rosati et al. propose a technique in [3] to use combined directional and Omni-directional antenna to improve routing path selection and try to minimize the Expected Connection Time (EMC) and the utility function for path selection. To accommodate the communication requirements of a heterogeneous network, Oubbati et al. [4] design an interaction possibility metric in routing protocol. In this way, the protocol improves the extension of networks and coverage of sub-networks assistance to some extent. Focusing on the UAVs' power limitation, Kai [5] structures an energy-efficient cooperative relaying scheme to extend the network lifetime while guaranteeing the success rate.

The excellent mobility of nodes in the FANET makes localization, deployment, and timely optimization of paramount importance [6–9]. The localization of UAVs is a prerequisite for algorithms to maintain network connectivity and threat avoidance, and a well-connected network can also improve localization accuracy through collaboration [6]. In [7], UAVs are envisioned as wireless base stations. The authors first calculated the coverage probability of the downlink, then used circle packing theory to determine UAVs' locations in 3D space to maximize the coverage area and coverage lifetime. Notably, Silva et al. [8] propose a FANET topology coordination protocol based on Software-Defined Network (SDN). By incorporating SDN into the UAV deployment strategy, the article sheds new light on FANET deployment optimization. To cope with the deterioration of the network connection caused by node vulnerability, ways to implement distributed connection maintenance and node importance assessment are extensively investigated in [9].

With the popularity of FANET technology, it has received much research interest in numerous practical applications [10–13]. To realize remote command and situational awareness, the authors in [10] constructed a cooperative monitoring network consisting of multiple UAVs and ground stations. A multi-relay UAV selection scheme based on fuzzy optimization is developed to realize the tradeoff between surveillance performance and connectivity maintenance. The articles [11,12] focus on the application of FANETs in disaster relief. In [11], Joshi et al. deal with the continuous sensing and monitoring of the geographical location of a specific disaster event. Their paper introduces and demonstrates various protocol stacks. A network simulator (NS-3) and a robot simulator (Gazebo) are used in synergy to simulate the disaster event boundary monitoring process. In addition, Sánchez-García et al. [12] propose a distributed algorithm, dPSO, to provide network support for victims and ambulance personnel in disaster areas. In the process of urban's digital and intelligent development, FANET technology is envisaged to play an important part. Siddiqi et al. [13] designed an enhanced Ant Colony Optimization (ACO) technique for traffic detection in remote urban areas, which improves the network life and the number of received packets compared to comparison algorithms.

In the case when continuous reconnaissance is required, the detection range expansion, information transmission, and even network segmentation of a FANET remain hard nuts to crack. Moreover, the safety of UAVs cannot be guaranteed due to natural factors and various enemy air defense operations [14–17]. For example, a common natural threat stems from local magnetic field variations. Sudden magnetic field change can interfere with the magnetic compass used for UAV positioning. The UAV incorrectly assumes that the change in magnetic compass data is due to its position movement and makes corrective actions to deal with it. These actions continue with the magnetic disturbance, and the UAV is out of control as seen from the ground. Moreover, in a hostile environment, the enemy can decrypt the communication protocol of UAVs to gain control. That is a common threat that UAVs face in the process of reconnaissance. Furthermore, acoustic waves are also used to strike UAVs. When the location of a UAV is detected, the acoustic transmitter sends acoustic waves of a specific frequency to its direction, triggering a resonance effect of the

UAV's gyroscope. Once the gyroscope becomes abnormal, the UAV's inability to identify angles could cause it to crash.

Some studies did take the above-mentioned issues into account. Zuev et al. considered the possible threats at the data transfer protocol level, such as hostile devices altering or masking the signals received by UAVs' GPS receivers [15]. They proposed a new method to evaluate UAV security threats based on Two-Criteria Likelihood-Impact scales. In [16], electromagnetic interference is considered, and the interference suppression is realized by optimizing the airborne antenna. Taking targets' movement into account, Song et al. [17] designed a cooperative UAV tracking method based on a sparse A* search and Standoff tracking algorithm. It realizes continuous tracking of moving targets in the task area.

However, as far as reconnaissance missions are concerned, none of the above literature considers the dynamics of the threat to drones. Nowadays, various jamming and hijacking capabilities have been integrated into diversiform mobile anti-reconnaissance devices, making the UAVs' threat change frequently. Only when the security of UAVs is guaranteed can various network architecture schemes and collaborative tasks be executed normally.

To achieve sustained reconnaissance in hostile scenes, in this study we first proposed the Threat Avoidance and Reconnaissance FANET Construction algorithm (TARFC). Then, taking into account the movement of monitored targets and the overall changes in the hostile area, the Total Edit Distance (TED) is defined as a measure of those variations. Finally, the Dynamic Threat Avoidance and Continuous Reconnaissance FANET operation (TA&CRFO) is proposed by incorporating the TED indicator into TARFC. The algorithm reduces the complexity of TARFC by making UAVs execute adaptively and has good application value in actual scenes. The contributions of this paper are as follows:

- We introduce a constraint on the threat probability density function (threat PDF) to model the changing threats in the scene. By transforming the constrained problem into an unconstrained problem using the Lagrange Multiplier method, the PSO-based TARFC algorithm is proposed to find optimal UAV locations that stay away from threats and maintain network connectivity.
- The TED metric is put forward to measure the variation degrees of the FANET and reconnaissance scenarios over different periods of time. According to the TED value, the control center will determine whether to execute overall coordination by sending control commands or to allow each node to perform distributed adaptive adjustments based on their local information. In this way, the dependence of UAVs on the control center can be reduced.
- Combined with the above two, the TA&CRFO algorithm is designed. It can adaptively adjust the topology of the FANET in realistic scenarios and realize the dynamic continuous reconnaissance goal of the FANET with low complexity, even if the monitored targets or scenario' threats are time-varying.

The structure of this paper is organized as follows: Section 2 mainly introduces a hierarchical architecture of the heterogeneous FANET and presents the problem-framing process. In Section 3, the PSO-based TARFC algorithm is proposed to achieve the construction of the FANET reconnaissance network and the threat avoidance in the scenario. Then, the TED metric is designed to measure the relevant changes. Finally, TA&CRFO is proposed to achieve the on-demand collaborative management of UAV nodes during continuous reconnaissance. Subsequently, Section 4 provides some analysis of simulation results, and some conclusions and future directions are described in Section 5.

2. System Model and Problem Statement

In this subsection, we first provide a description of the system model and then formulate an optimization problem that the TA&CRFO algorithm can handle. Tables 1 and 2 present, respectively, the lists of acronyms and variables used in this article for the readers' convenience.

Table 1. List of acronyms.

Acronym	Description
TA&CRFO	Dynamic threat avoidance and continuous reconnaissance FANET operation
UAV	Unmanned aerial vehicle
TARFC	Threat avoidance and reconnaissance FANET construction algorithm
FANET	Flying ad hoc network
ACP	Airborne command and control platform
LoS	Line-of-sight
PSO	Particle swarm optimization
TED	Total edit distance
AUDS	Anti-UAV defensive system
MUs	Monitoring UAVs
RUs	Relay UAVs
PDF	Probability density function
KKT	Karush–Kuhn–Tucker method

Table 2. List of variables.

Variable	Description
A	The ACP of FANET
U	Set of low-altitude drone swarms
R	Set of all RUs
M	Set of all MUs
x_i	Location of node i
V	Node Set
X_V	Set of locations of all nodes in V
ε_m	The MU assigned to mission m
$\rho(m)$	Routing path for mission m
P	Set of all active links
f	Overall performance function
f^C	Network connectivity function
$f^C_{i,j}$	Wireless connectivity quality between i and j
f^T	FANET threat metric
r_{thr}	Threatened radius of UAV
$\varphi(x)$	Threat PDF in related areas
r^C	Maximum communication radius between UAV
r^S	Minimum safety radius between UAV
t, τ	Time
$\vartheta(t)$	FANET in time t
N	Node set in graph theory model
$\sigma(t)$	Edge set in graph theory model
$P_N(t)$	Nodes' position set in graph theory model

2.1. System Model

In recent years, three main strategies have been used to achieve drone swarms' persistent surveillance [8,11–13,18–27]: (i) on-duty UAV replacement scheme based on recharging stations [13,19,25]; (ii) energy-efficiency path planning [20–27]; and (iii) novel structures of UAV teaming [8,11,18,22]. UAV distribution's hierarchical architecture helps plan efficient and adaptive surveillance missions when the surveillance map changes due to weather or invisible factors. The hierarchical structure intends to divide the surveillance task into different platforms such as ground stations, high-altitude UAVs, and UAV sensing swarms. Each platform is in charge of different functions such as control, motion coordination, data transmission, package routing, etc.

We assume that the FANET in this study consists of a high-altitude UAV A, as its airborne command and control platform, i.e., ACP, and set U of drone swarms in low-altitude to perform reconnaissance missions.

If there is any ambiguity, all UAVs are referred to as nodes of the network throughout this article. We identify a node i's location by $x_i \in \mathbb{R}^3$, and a set of all the nodes' locations in set V by $X_V = \{x_i\}_{i \in V}$. To simplify the model, we presume that each UAV can only carry out one reconnaissance operation at a time and that each target that is being scouted should be covered by at least one UAV. As a consequence, we make the assumption that the number of targets to be scouted is not larger than the number of drones that are currently accessible. In our FANETs, the ACP can either hover over the given location or fly around the periphery of the area of interest, while drone swarms have controllable mobility. Therefore, drone movement can be managed by themselves or by the ACP to achieve excellent performance in both network and mission-related factors. Considering the radio propagation model, Friis's free space model [28], the most popular propagation model, is used in this article. According to this radio propagation model, all nodes have the same transmission radius. The connection between two nodes occurs when and only when they are within the transmission radius. One of the crucial research concerns is the energy problem, which includes things such as patterns of energy consumption and battery dynamics. We direct readers to [29] and any references therein because it is outside the scope of this article.

For ease of description, we designate the UAV assigned to reconnaissance mission m as monitoring UAV (MU) and denote it as ε_m. Therefore, the set of MUs can be expressed as $M = \{\varepsilon_1, \ldots, \varepsilon_m\}$. The remaining drones that are not assigned to any reconnaissance mission are used as communication relay nodes in the network, which are in charge of transmitting data between MUs and the ACP in the upper air. Relay UAVs (RUs) is the term we use to identify them, i.e., $R = U \backslash M$.

Figure 1 describes the hierarchical structure of our UAV persistent surveillance team. Because of the quadcopter's limited communication range, the high-altitude UAV undertakes information exchange with the remote ground end. Some necessary control instructions for drone swarms are also sent from the high-altitude UAV since its bigger role is the ACP of the network. Inside the FANET, a buffer layer of UAV swarm between the ACP and ground objects extends this system's ability on connection service and real-time tracking. With many agents within the UAV swarm layer, an adaptive formation policy can be developed to fit various requests, including avoiding dangerous areas such as Anti-UAV Defensive System (AUDS), thunderstorm areas, strong communication interference areas, etc.

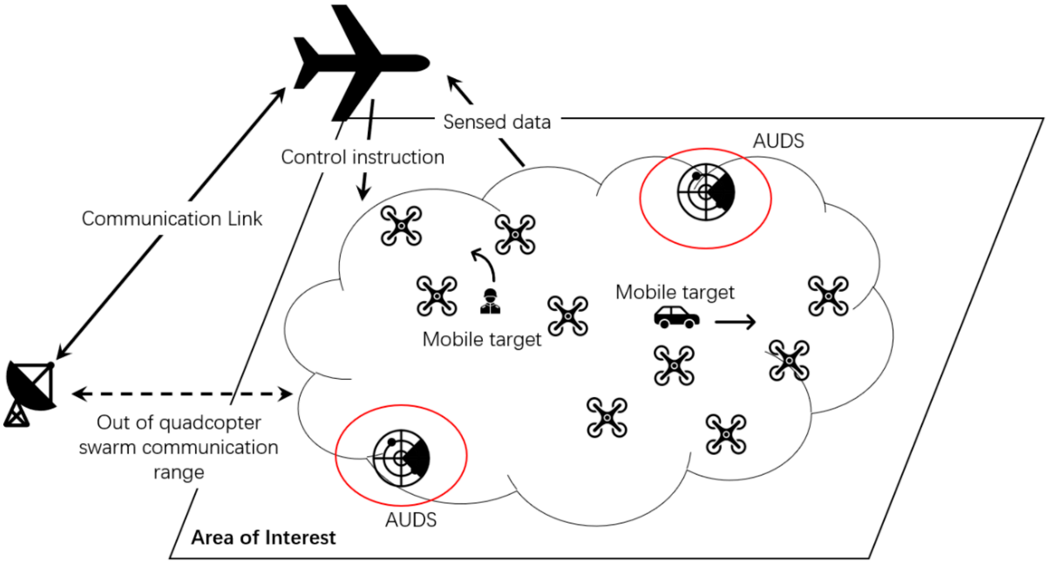

Figure 1. Hierarchical structure of proposed FANET persistent surveillance system.

Next, it is challenging to guarantee direct communication between each UAV node and the ACP to maximize the drone swarm's search and surveillance range. Therefore, multi-hop communication is usually adopted, which requires establishing a routing path for packet transmission. As a result, the choice of routing path significantly impacts the performance of the FANET. When coming up with a solution for the UAV locations, the routing protocol should be considered. Different UAVs may operate in different ideal locations depending on the routing protocol. Therefore, in this paper, we focus on routing protocols that offer a selection of routes between MUs and the ACP based on the positions of the nodes and presumptively employ a routing protocol that is known in advance. Accordingly, we define a routing function,

$$\rho : \{x_{\varepsilon_m}, x_A, X_R\} \Leftrightarrow \rho(m), \tag{1}$$

where $\rho(m)$ is the series of wireless links from the MU ε_m to the ACP A through the relay UAVs in R.

2.2. Problem Formalation

Communication is the basis of cooperation and collaboration between UAVs, which is crucial and essential [10]. For simplicity, we assume that the communication between the UAVs follows the line-of-sight (LoS) model [28,30]. In the following, we introduce the concept of network connectivity and the FANET threat metric.

2.2.1. Network Connectivity

We examine a network connection function that only considers active links in order to more correctly evaluate the network performance of our FANET. An active link is defined as a link that is a part of any routing path that connects the executing MU and the ACP. Due to the node location x_i's differentiable characteristic, we define the network connectivity f^C as the averaged value of all active links' quality, i.e.,

$$f^C(X_V, \rho) = \frac{1}{|\mathrm{P}|} \sum_{(i,j)\in \mathrm{P}} f^C_{i,j}(x_i, x_j), \tag{2}$$

where P is the set of all active links, i.e., $\mathrm{P} = \underset{m\in M}{\cup} \rho(m)$, and $f^C_{i,j}$ represents the quality of the wireless link (i, j). Accordingly, we make the assumption that the $f^C_{i,j}$ can be defined as $\|x_i - x_j\|^p$, where $\|\cdot\|^p$ stands for the Lp-Norm.

2.2.2. FANET Threat Metric

For the sake of practical application, we define the FANET threat metric, f^T, to quantify and uniformly express various threats (military anti-reconnaissance threat, terrain features, weather conditions, communication interference, etc.) that each relay UAV faces in a scene. However, our main concern in this paper is not how to define or measure those threats posed to the UAVs by different factors but how each UAV can stay away from areas with high threat values while ensuring its reconnaissance performance and network connectivity. Therefore, in this paper, we do not discuss the modeling and quantification of the threat metric model. Instead, we give a predefined time-varying threat density distribution for the scenario.

To help readers obtain a more intuitive impression, Figure 2 is used as an example to show the threat density distribution in the reconnaissance area. The threat density may come from anti-drone devices, communication jamming, etc. In the image, the darker the red, the greater the threat is. For each UAV in the simulated area, the threat value is the integral of the threat density in its associated area.

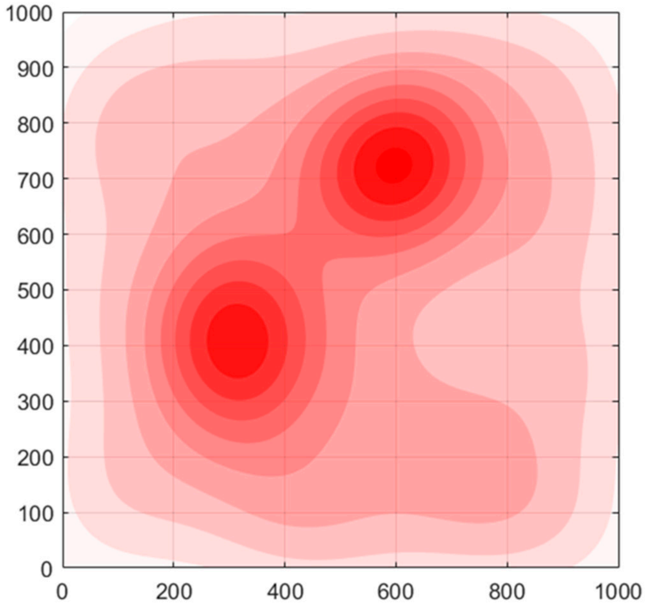

Figure 2. Example of threat density distribution in area of interest.

The f^T is defined by

$$f^T(X_R, \varphi(x), r_{thr}) = \frac{1}{|R|}\sum_{i=1}^{|R|} \oint_{x\in\langle x_i|r_{thr}\rangle} \varphi(x)dx \quad x_i \in X_R, \tag{3}$$

where $\varphi(x)$ is the known scenario's threat Probability Density Function (PDF), and r_{thr} is the threatened radius of drones. Note that $\langle x_i|r_{thr}\rangle$ is the circular region with center x_i and radius r_{thr}. The threat value of each UAV can be obtained by integrating the threat PDF in the corresponding area. When location x_o is outside the defined area D, we define $\varphi(x_o)$ equals the average value of threat PDF in D, i.e., $\varphi(x_o) = \frac{\sum \varphi(x)}{|D|}, \forall x \in D, x_o \notin D$.

2.2.3. Problem Construction

Network connectivity is the guarantee of information interaction between UAVs. Drones can share data with each other only when they are connected to the FANET. The ACP also needs a connected network to control and adjust drone swarms. In addition, ensuring the safety of UAVs is a prerequisite for the regular operation of FANETs. Today, all kinds of jamming and hijacking functions are integrated into various mobile anti-reconnaissance equipment, threatening UAVs' security. Only when the safety of UAVs is guaranteed can drones cooperate to perform complex tasks.

Considering the above two aspects, we define the overall performance function f as a weighted sum of network connectivity and FANET threat metric as shown in Equation (4),

$$\begin{aligned} f\left(X_V, \{\varepsilon_m\}_{m\in M}, \varphi(x), r_{thr}, \rho\right) = \; & w^C f^C(X_V, \rho) \\ & + w^T f^T(X_R, \varphi(x), r_{thr}), \end{aligned} \tag{4}$$

where w^C and w^T are the weights for network connectivity and FANET threat metric, respectively. Then, we can formulate the problem in the following way so that it can be solved by the TA&CRFO algorithm:

$$\underset{\substack{x_u \in D, \;\; \forall u \in V \\ \varepsilon_m \subseteq V, \;\; \forall m \in M}}{\text{maximize}} \quad f\left(X_V, \{\varepsilon_m\}_{m\in M}, \varphi(x), r_{thr}, \rho\right), \tag{5}$$

$$s.t. \;\; \|x_i - x_j\| \le r^C \;\; \forall (i,j) \in \rho(m) \tag{6a}$$

$$\|x_i - x_j\| \geq r^S \quad \forall (i,j) \in V, \quad u \neq v \tag{6b}$$

$$\varepsilon_m \neq \varepsilon_n \quad \forall \varepsilon_m \in M, \forall \varepsilon_n \in M \tag{6c}$$

$$|\varepsilon_m| \geq 1 \quad \forall \varepsilon_m \in M \tag{6d}$$

$$w^C > 0, \quad w^T < 0 \tag{6e}$$

$$\varphi(x_o) = \frac{\sum \varphi(x)}{|D|}, \forall x \in D, x_o \notin D \tag{6f}$$

where r^C, r^S, and r_{thr} represent the maximum allowable link length for reliable direct communication between two nodes, the minimum safety distance to avoid collisions between UAVs, and the threat radius of each relay UAV that can be deployed in a given three-dimensional Euclidean space, $D \in \mathbb{R}^3$, respectively. Constraint (6a) guarantees the UAVs' reliable end-to-end communication. A safe flight distance is produced by constraint (6b) to reduce the danger of UAV crashes. Each UAV can only undertake one mission at a time and at least one UAV is required to complete each task, according to constraints (6c) and (6d). Constraint (6e) means that the overall performance function f increases as the FANET's network connectivity increases and decreases as the FANET threat metric increases. Constraint (6f) describes the threat PDF definition for locations outside the simulation area.

3. Algorithm Description

By taking into consideration the mobility of the monitored targets and the dynamic changes at the scene, we present a description of how to build and run a continuous reconnaissance FANET under problem (5).

In order to facilitate readers' understanding, we first introduce the principle of the basic PSO algorithm. Then, based on the PSO algorithm, we develop the TARFC. Considering the MUs' movement toward the reconnaissance targets and the dynamic change of threat information in real scenarios, the TARFC has difficulty meeting real-time requirements. So, inspired by graph edit distance [31], we design the TED to measure the changes in network topology and scenario's threat distribution at different times. Finally, combined with those mentioned above, we develop the TA&CRFO algorithm. This algorithm realizes the dynamic continuous reconnaissance goal of the FANET in a low-complexity way.

3.1. Rudimentary PSO Algorithm

PSO is a heuristic search algorithm proposed by J. Kennedy and R. Eberhart [32] in 1995. It is a random search algorithm that simulates biological activities and swarms intelligence in nature. The core idea is to use the information sharing of individuals in the group to guide the group's movement in the problem-solving space. In the process of evolution from disorder to order, a feasible solution to the problem will be obtained. In addition to considering the group activities of simulated organisms, it is a swarm intelligence algorithm integrating individual cognition and social influence.

Each particle in PSO iterates to improve its location in the simulation space of the optimization problem, selecting the best position thus far as the final solution at the end of the iteration.

For ease of understanding, we will use the following optimization problem to explain the PSO algorithm:

$$\underset{x \in \mathbb{R}^n}{\text{minimize}} \quad h(x), \tag{7}$$

where $h(\cdot) : \mathbb{R}^n \mapsto \mathbb{R}$ is called an objective function, $\mathbb{R}^n$ is the simulation space, and x is the decision variable.

We suppose that the PSO algorithm operates on a swarm of particles, each of which is represented by its position and velocity, i.e., $(x_i, v_i) \in \mathbb{N}$. Each particle's position corresponds to one of the potential solutions to the problem, as was previously mentioned. So, two special parameters emerge: *pBest* and *gBest*. The position that is the ith particle's pBest, represented by p_i, is the best position that the particle has ever achieved. Analogously, the best position among the pBest of all particles is the unique gBest, represented by g. The ith particle's velocity is updated by adding the stochastically weighted differences between its current position and both its pBest and the gBest, i.e.,

$$v_i^{l+1} = wv_i^l + c_1 u_1 \circ \left(p_i^l - x_i^l\right) + c_2 u_2 \circ \left(g^l - x_i^l\right), \forall (x_i, v_i) \in \mathbb{N}, \tag{8}$$

where w is the inertia weight, c_1 and c_2 are individual cognition parameter and social influence parameter, the index l indicates the PSO algorithm's lth iteration, both u_1 and u_2 are independent random vectors on $[0,1]^n$ with uniform distribution, and the superscript n represents the dimension of the simulation space.

In Equation (8), the inertia term controls the velocity's amplitude, while the cognitive and social terms strike a balance between local search and global search. Equation (9), i.e.,

$$x_i^{l+1} = x_i^{l+1} + v_i^{l+1}, \forall (x_i, v_i) \in \mathbb{N}, \tag{9}$$

can be used to determine the new particle position based on the updated velocity.

The positions of all the particles are updated iteratively in the simulation space by combining their velocities, which are modified in each iteration in accordance with Equation (8). The number of iterations, the swarm's pace of convergence, the algorithm's duration, and other factors can be used as termination conditions. The gBest becomes the top current solution to the unconstrained optimization problem (7) after the PSO algorithm terminates. Figure 3 shows the whole process of the rudimentary PSO algorithm.

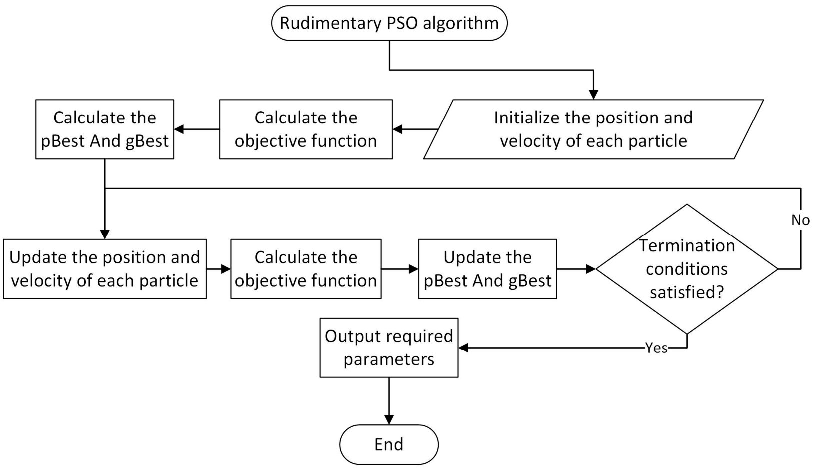
Rudimentary PSO algorithm
Calculate the pBest And gBest
Calculate the objective function
Initialize the position and velocity of each particle
No
Update the position and velocity of each particle
Calculate the objective function
Update the pBest And gBest
Termination conditions satisfied?
Output required parameters
Yes
End

Figure 3. Flow chart of rudimentary PSO algorithm.

Specifically, for FANETs, each particle in the PSO algorithm represents a complete FANET topology distribution scheme. The particle contains information about the UAVs' position vector, the UAVs' velocity vector, the FANET's connectivity value, each UAV's threat value, and the total performance of the scheme. During each iteration, the position vector of UAVs is updated based on the UAVs' velocity vector in the previous round. The total performance values of all particles are compared, and the following iteration will be performed based on the particle with the best total performance.

3.2. PSO-Based TARFC

The PSO algorithm is suitable for solving unconstrained optimization problems such as Equation (7). Hence, in order to use our PSO-based TARFC algorithm, the Lagrange Multiplier and Karush–Kuhn–Tucker (KKT) methods [33] are employed to transform the constrained problem (5) into an unconstrained one. Thus, the reformulated problem is defined as

$$\underset{\substack{(x_i, v_i) \in \mathbb{N}, \forall x_i \in V \\ \varepsilon_m \subset V, \forall m \in M}}{\text{maximize}} \quad \widetilde{f}\left(X_V, \{\varepsilon_m\}_{m \in M}, \varphi(x), r_{thr}, \rho\right) \tag{10}$$

As shown in Equation (11), $\widetilde{f}$ is then obtained by converting the constraints into penalty terms and adding them to the objective function:

$$\begin{aligned} &\widetilde{f}\left(X_V, \{\varepsilon_m\}_{m \in M}, \varphi(x), r_{thr}, \rho\right) \\ &= f\left(X_V, \{\varepsilon_m\}_{m \in M}, \varphi(x), r_{thr}, \rho\right) \\ &+ \sum_{m \in M} \zeta_m \left(\left[\max_{k=1,\ldots,|\rho_m|-1} \delta\left(\rho_m^k, \rho_m^{k+1}\right) - r^C \right]^+ \right)^2 \\ &+ \xi \left(\left[r^S - \min_{\substack{u, v \in M \cup R \\ u \neq v}} \delta(u, v) \right]^+ \right)^2 \end{aligned} \tag{11}$$

Note that ζ_m and ς are negative penalty coefficients corresponding to the end-to-end communication constraint and the safety requirement, respectively. $[\bullet]^+$ stands for $\max\{0, \bullet\}$, which means that if the communication distance and safety distance between two UAVs meet the corresponding constraints, then the penalty term takes the value of zero. The particle i's individual pBest and the gBest are defined as x_i^* and x^*, and the solution x^* that maximizes the $\widetilde{f}$ would be the answer for the problem (5).

Algorithm 1 describes the PSO-based TARFC algorithm in full. Lines 1–4 are the preliminary stage. We first establish some fundamental characteristics (line 1). Then, we set all particles' velocities to zero and their positions to random numbers evenly distributed over the defined simulation space. After that, we initialize all particles whose positions are to be random numbers uniformly distributed in the defined space of the problem (10) and whose velocities are to be all zeros. When the first time the particle i is initialized, its position automatically becomes its pBest position x_i^*, and the routing function $\{\rho_m\}_i^*$ determines its corresponding routing paths (lines 2–4). Following initialization, we identify the particle with the highest penalized performance metric value (since we defined ζ_m and ς are negative penalty coefficients). Then, change the particle g's pBest position x_g^* to the gBest position x^*, and its corresponding routing paths $\{\rho_m\}_g^*$ are also changed as the gBest position's routing path $\{\rho_m\}^*$.

In the iterative stage (lines 5–19), we first obtain the current location of the ACP and mission-execution UAVs, X_A and X_M, as well as the latest threat PDF, $\varphi(x)$, in the scenario. Guided by the above, relay UAVs' velocity, position, routing, and other attributes are updated periodically. To be more specific, the particles' position and speed are changed stochastically based on both their unique pBest position and the overall gBest position as

$$\begin{bmatrix} \mathbf{x}^{l+1} \\ \mathbf{v}^{l+1} \end{bmatrix} = \begin{bmatrix} 1 - c_1\mathbf{u}_1 - c_2\mathbf{u}_2 & w \\ -c_1\mathbf{u}_1 - c_2\mathbf{u}_2 & w \end{bmatrix} \begin{bmatrix} \mathbf{x}^l \\ \mathbf{v}^l \end{bmatrix} + \mathbf{I}_2[c_1\mathbf{u}_1 + c_2\mathbf{u}_2] \begin{bmatrix} \mathbf{p}^l \\ \mathbf{g}^l \end{bmatrix} \tag{12}$$

The index l in Equation (12) is the algorithm's lth iteration. Both $\mathbf{u}_1$ and $\mathbf{u}_2$ are uniformly distributed random vectors.

It should be noted that during the simulation, the speed change could be out of the actual. Hence, we bring in a velocity clamping method [34] as shown in Equation (13),

$$v_{i,j}^{l+1} = \begin{cases} v_{i,j}^{l+1} & \textit{if } v_{i,j}^{l+1} \in \left[-V_j^{\max}, V_j^{\max}\right] \\ \frac{v_{i,j}^{l+1}}{\left|v_{i,j}^{l+1}\right|} V_j^{\max} & \textit{otherwise} \end{cases} \tag{13}$$

where $v_{i,j}^{l+1}$ is the jth element of v_i^{l+1}, and $V_j^{\max}$ is the velocity clamping threshold. If the modified position can obtain better results in $\tilde{f}$, the pBest and gBest for each particle will be altered, as explained in lines 11–18. Eventually, the algorithm terminates when it meets the termination condition, i.e., it runs to a preset number of iterations, or the results no longer improve in a certain number of iterations (line 19).

Algorithm 1. Threat Avoidance and Reconnaissance FANET Construction

```
Input: $r^C$, $r^S$, $r_{thr}$, $X_A$, $X_M$, $\rho$, $\varphi(x)$, $w^M$, $w^C$, $w^T$
Output: $x^*$
1  Set PSO-related parameter, KKT-related parameters.
2  Randomly initialize particles $(x_i, v_i) \in \mathbb{N}$, and establish links $\rho(X_A, X_M, x_i^*)$
3  $g \leftarrow \arg\max_i \tilde{f}\left(X_V, \{\varepsilon_m\}_{m\in M}, \varphi(x), r_{thr}, \{\rho_m\}_i^*\right)$ for each particle $i$
4  $x^* \leftarrow \max(x_g^*)$ and $\{\rho_m\}^* \leftarrow \{\rho_m\}_g^*$
5  While termination conditions are not met
6      Obtain the $X_A$, $X_M$ at the current moment
7      Obtain the threat PDF $\varphi(x)$ of the current search space
8      Update $x_i$, $v_i$ according to (12, 13)
9      For each particle $(x_i, v_i) \in \mathbb{N}$ do
10         $\{\rho_m\}_i \leftarrow \rho(X_A, X_M, x_i)$
11         If $\tilde{f}_t > \tilde{f}_{t-1}$ then
12             $x_i^* \leftarrow x_i$ and $\{\rho_m\}_i^* \leftarrow \{\rho_m\}_i$
13         End if
14     End for
15     $g \leftarrow \arg\max_i \tilde{f}\left(X_V, \{\varepsilon_m\}_{m\in M}, \varphi(x), r_{thr}, \{\rho_m\}_i^*\right)$ for each particle $i$
16     If $\tilde{f}_t\left(X_V, \{\varepsilon_m\}_{m\in M}, \varphi(x), r_{thr}, \{\rho_m\}_i^*\right) > \tilde{f}_{t-1}\left(X_V, \{\varepsilon_m\}_{m\in M}, \varphi(x), r_{thr}, \{\rho_m\}^*\right)$ then
17         $x^* \leftarrow x_i^*$ and $\{\rho_m\}^* \leftarrow \{\rho_m\}_i^*$
18     End if
19 Until termination conditions are satisfied
```

Although the TARFC algorithm provides FANETs with a feasible network construction method to perform reconnaissance tasks in threatening scenarios, in most real reconnaissance missions, such as military target reconnaissance, to remain undetected, UAVs cannot influence the movement of the detected targets or the relevant scene's alteration. This puts forward a "sustainable" reconnaissance requirement for the FANET. As for algorithm II, every FANET adjustment according to the changing targets or scene requires a large number of iterations, which is extremely time consuming. For this reason, in the following

Sections 3.3 and 3.4, we first propose an indicator called Total edit distance to measure the variation degree of the FANET and the threat PDF change in related scenarios. Secondly, a low-complexity algorithm named TA&CRFO is proposed. According to the above indicators, the algorithm can conduct two different adjustment modes for the FANET to meet the needs of "sustainable" in real situations.

3.3. Total Edit Distance

Inspired by the graph edit distance [31,35], we innovate the Total Edit Distance concept to measure the changes in the FANET and the extent of changes in the threat PDF. Our basic philosophy is to avoid frequent routing updates and iterations to reduce computational overhead and preserve overall efficiency to the greatest extent possible. To do this, we will judge whether to execute overall coordination by sending control instructions through ACP or let each node perform distributed adaptive adjustment according to the range of the TED.

Prior to introducing the TED, we briefly describe the graph edit distance [35] here to aid. In graph theory, the graph edit distance measures the dissimilarity between graph Ω_1 and graph Ω_2. Many graph editing operations, such as node and edge additions and deletions, can change one graph into another. With each graph edit operation's cost, the cost of each operation is summed to obtain the total cost of converting the graph Ω_1 to Ω_2, and the smallest cost in this process is defined as the graph edit distance from Ω_1 to Ω_2. Note that different operations usually have various cost functions. Thus, two different sets of operations, with the same outcomes in altering the graph Ω_1 to Ω_2, may be of relatively large distinction regarding the total cost.

We first establish the FANET edit distance to measure the change in the FANET. Then, the threat edit distance is defined to record the fluctuation of threat PDF in associated areas, both of which are based on the graph edit distance principle. As a result, the FANET edit distance and the threat edit distance are added to form the TED.

Unlike normal graph edit operations, our system does not consider the addition or damage of UAV nodes. So, the node sets are the same at different times. That is to say, the FANET edit operations only contain edge changes, such as edge insertion, edge deletion, and edge length change.

We symbolize the FANET as a graph $\vartheta(t)$. The graph consists of the set of nodes N, the set of edges $\sigma(t)$ and their corresponding positions set $P_N(t)$. To transform $\vartheta(t)$ to $\vartheta(\tau)$, where t and τ are adjacent time with $t < \tau$, the minimum edge insertions and deletions can be expressed as

$$d_1(t,\tau) = \sigma(\tau) - \sigma(t), \tag{14}$$

$$d_2(t,\tau) = \sigma(t) - \sigma(\tau), \tag{15}$$

where $d_1(t,\tau)$ is the edge insert operation between time t and τ, the $d_2(t,\tau)$ is the edge delete operation between time t and τ, respectively.

More importantly, we must pay special attention to the changes in edge lengths since the drones in the FANET move vigorously and frequently. Because the edge length between two nodes is closely related to their communication performance, the optimal routing path may differ from time t to time τ. Hence, the total amount of edge length changes between time steps t and τ is how we define the edge length change operation; that is,

$$d_3(t,\tau) = \sum_{i,j\in N} \left| \|p_i(t) - p_j(t)\|_2 - \|p_i(\tau) - p_j(\tau)\|_2 \right| \tag{16}$$

where $p_i(t)$ stands for the position of node i in time step t. Note that TED is applicable to simulations of different dimensions. Depending on the simulated scene's dimensionality, the node i's position p_i can be equivalent to a two-dimensional (x_i, y_i) vector, a three-dimensional (x_i, y_i, z_i) vector, or even a higher-dimensional space vector.

We lastly define the threat edit distance to measure the changes in the scenario's threat density distribution at different times. In the duration of a reconnaissance mission, obtaining global information is laborious and impractical. Moreover, each drone in the FANET is threatened by a limited area in our model. Hence, the threat edit distance is defined as the average change in each UAV's threat value between time t and τ, i.e.,

$$d_4(t,\tau) = \frac{1}{N}\sum_{i=1}^{|N|}\left| \oint_{p\in\langle p_i|r_{thr}\rangle} \varphi(p(t))dx - \oint_{p\in\langle p_i|r_{thr}\rangle} \varphi(p(\tau))dx \right| \tag{17}$$

Finally, the TED between time t and τ is defined as

$$\theta(\vartheta(t),\vartheta(\tau),\mathrm{P}) = \sum_{i=1}^{4} w_i \cdot d_i(t,\tau), \tag{18}$$

where P is the set of all active connections, and w_i is the weight parameter of each edit operation d_i.

A large value of TED implies that the FANET has changed a lot, or the regional threat density distribution varies greatly. In such cases, centralized scheduling is needed to tune the FANET. If the value of TED is within a reasonable range, we may enable each UAV to adjust its speed adaptively to optimize reconnaissance and communication performances. So, the TA&CRFO algorithm is developed to achieve dynamic, persistent surveillance in a less complex way.

3.4. TA&CRFO

We now go into depth about our TA&CRFO algorithm in this subsection. Algorithm 2 presents the pseudo-code. In the preparatory phase (lines 1–2), which usually is the beginning of reconnaissance missions, the high-altitude UAV, known as ACP, constructs the initial FANET by Alg. 1 based on available information. Then, each low-altitude UAV flies to the position specified by the high-altitude UAV. When they arrive, we abstract the FANET into a graph and define it as a reference graph ϑ_{ref} for a particular time.

During the iterative stage (lines 3–16), the high-altitude UAV collects the position information of the scouted targets and evaluates the fluctuation of threat density distribution in the scenarios. Meanwhile, in time t, the ACP calculates the TED $\theta\left(\vartheta_{ref},\vartheta(t-1),\mathrm{P}\right)$ between reference graph ϑ_{ref} and the FANET graph at time step $t-1$ in the current scenario. The $\theta\left(\vartheta_{ref},\vartheta(t-1),\mathrm{P}\right)$ value represents how much the FANET and threat PDF in the scenario have changed from the reference time. We assert that the cumulative changes are insignificant if the TED between them is below the threshold λ. Therefore, by Equations (19) and (20), we have each low-altitude drone adaptively alter its position (lines 7–11).

The right side of Equation (19) is the gradient of the total performance function concerning the position of node x_i at time t. With neighbor UAVs' position information and the threat PDF of related areas, each node's gradient value can be easily obtained.

On the other hand, if the TED is greater than λ, we believe that the distributed position adjustment has lost its meaning since the routing path or scenario's threat PDF may have altered too much. Therefore, we use Algorithm 1 again to reconstruct the FANET network in a centralized way and set the newly configured network as the reference graph ϑ_{ref}.

$$v_i(t) = \nabla_{x_i} f(t) = \nabla_{x_i} f\left(X_V(t), \{\varepsilon_m\}_{m\in M}, \varphi(x(t)), r_{thr}, \rho\right) \tag{19}$$

$$x_i(t+1) = x_i(t) + v_i(t) \tag{20}$$

In other words, at each time, the high-altitude UAV will decide whether to issue instructions to all low-altitude drones for overall control according to $\theta\left(\vartheta_{ref},\vartheta(t-1),\mathrm{P}\right)$. If low-altitude drones receive those instructions, they will obey them. Otherwise, they continue their adaptive location optimization method using local information.

Algorithm 2. Dynamic Threat Avoidance and Continuous Reconnaissance FANET Operation

```
Construct the first FANET using Algorithm 1
Initialize the reference FANET as $\vartheta_{ref}$
For each time $t$ do
    Obtain the $X_A$, $X_M$ at the current moment
    Obtain the threat PDF $\varphi(x)$ of the current simulation space
    If $\theta(\vartheta_{ref},\vartheta(t-1),\mathrm{P})<\lambda$ then
        For each particle $(x_i,v_i)\in\mathbb{N}$ do
            Update $v_i$ depending on (19)
            Update $x_i$ depending on (20)
            $\{\rho_m\}_i \leftarrow \rho(X_A,X_M,x_i)$
        End for
    else
        Update each particle $(x_i,v_i)\in\mathbb{N}$ by Algorithm 1
        Reconfigure the reference FANET, $\vartheta_{ref}=\vartheta(t)$
    End if
End for
```

4. Results

This article considers a 3D scene with a randomly generated threat PDF, in which multiple monitoring UAVs perform reconnaissance tasks at different locations. Various numbers of relay UAVs are provided to forward the detected targets' relevant data and the variation in threat PDF at the scene. The high-altitude UAV, known as ACP, oversees the entire FANET in the whole process.

For the sake of effective comparison, four algorithms, RWP [36], PSO, TARFC, and TA&CRFO, are respectively implemented under the condition that the values of all parameters are consistent. The simulation process is executed on MATLAB. In the simulation, we assume that there are no projectiles in the environment, such as birds or obstacles, which may block the flight path of the UAV, and it is assumed that the battery capacity of the UAVs meets the requirement of continuous reconnaissance.

The alteration of each index in the process of algorithm execution is compared, and the reasons for different results obtained by different algorithms are analyzed. Simulation results demonstrate that the FANET net constructed by the TA&CRFO algorithm is 6.06~7.23% lower than TARFC in connectivity and 0.46~1.21% higher in UAV's average threat value, but the time consumption of the algorithm is only 19.86~20.31% of TARFC. At the cost of other performances' slight impairment, the TA&CRFO achieves UAV's limited distributed control and a significant reduction in computing overhead.

Table 3 describes the simulation scenario and lists the parameters during the simulation. The horizontal dimension of the simulated scenario is set as 1 km × 1 km, and the flight height of the UAV is set to 100 m and 200 m. In valid experiments, the number of RUs ranged from 7 to 19. Given that too few RUs cannot establish communication links at multiple reconnaissance sites simultaneously, too many RUs may not offset the outlay despite the increased performances. We assume that the relay drones can either hover or travel at a maximum speed of 15 m per second. The shortest path routing algorithm, whose link usage is calculated as the cube of its length, is the default routing protocol. In terms of distance, the low-altitude UAVs' safety distance, maximum communication distance, and the diameter of the perceived threat area are set to 20 m, 200 m, and 50 m, respectively. Our work not only uses the original PSO algorithm as the comparison algorithm but also constructs a new one based on the PSO algorithm. Therefore, the PSO-related parameters are listed explicitly for ease of reference. Finally, the parameters related to the KKT method and our algorithms are also listed in Table 3.

Table 3. Setting of simulation parameters.

Parameter	**Value**
Scenario	
Horizontal dimensions	1000 × 1000 m
Vertical dimension	[100~200] m
Number of RUs	[7~19]
RUs' speed	[0~15] m/s
Distances	
Minimum safe distance, r^S	20 m
Maximum link distance, r^C	200 m
UAV's threat perception radius, r_{thr}	25 m
PSO-related	
Number of particles, N_p	50
Number of iterations	400
Inertia weight, w	0.7192
Cognitive parameter, c_1	1.4472
Social parameter, c_1	1.4472
KKT and FANET-related	
ξ, ζ_m	0.5
Connectivity weight, w^C	0.5
Weight of FANET threat metric, w^T	2.5
Weight, of edit operations, w_1, w_2, w_3, w_4	2, 2, 0.3, 40
TED's threshold parameter, λ	5.23

4.1. Scenario Exhibition

In the FANET consisting of the ACP, 12 relay UAVs, and two monitoring UAVs, the TA&CRFO algorithm is used to simultaneously carry out continuous reconnaissance of mobile targets. Figure 4 shows the simulation results at t_i. The circle with the relay UAV as the center in Figure 4 represents the maximum communication range of the RUs. During the reconnaissance, the monitoring UAVs move closely with the movement of monitored targets. Since the trajectory of targets is unpredictable for the ACP, the MUs' movements are completely controlled by themselves. The RUs adjust their positions according to the displacement of the MUs and the variation in threat PDF to avoid hazards and ensure the communication quality between the ACP and the MUs.

4.2. The Simulation Trajectory

Figures 5–7 are the trajectory diagrams of each UAV in the continuous reconnaissance process using TA&CRFO. Only a period of FANET trajectory is shown to facilitate readers' identification. Since the whole network is in 3D space, a multi-angle display is necessary to clearly show the changes in the FANET in the continuous reconnaissance process. Thus, Figures 5–7 are presented as the process's top, left, and front views. Inside these pictures, the colors and shapes of the markings represent different types of UAVs. The lines in different colors represent the moving track of each relay UAV during this time period. Through those figures, it can be observed that the newly formed FANET can play a better relay role in monitoring UAVs at (900, 100, and 100) m and (900, 900, and 100) m, and keep away from positions in high-threat areas of the moment.

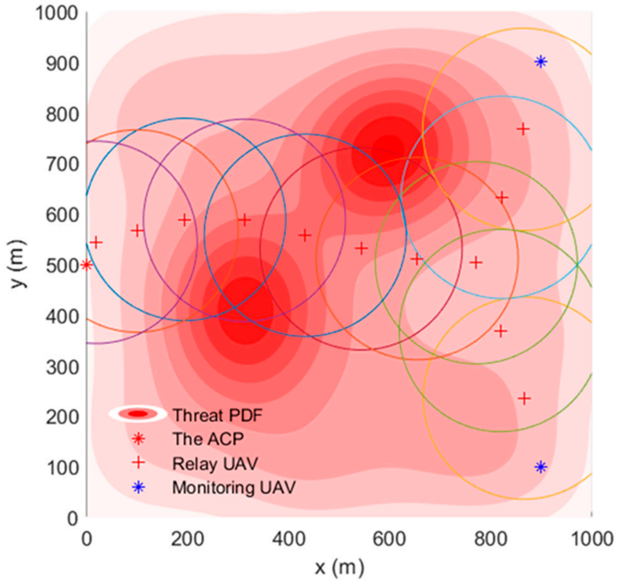

Figure 4. UAVs' topology using TA&CRFO algorithm at t_i.

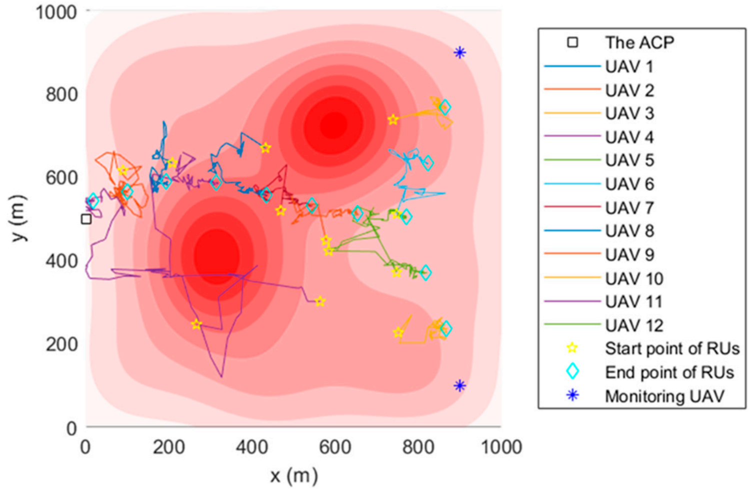

Figure 5. Trajectory of the FANET in a certain time period (Top view).

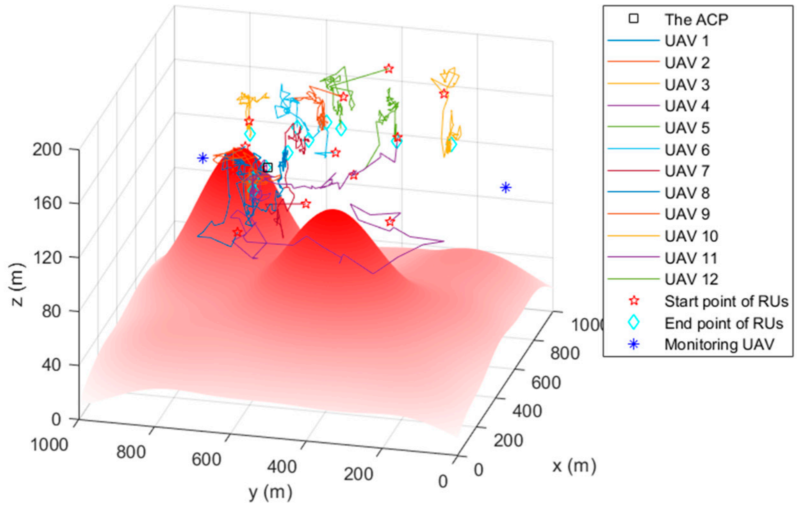

Figure 6. Trajectory of the FANET in a certain time period (Left view).

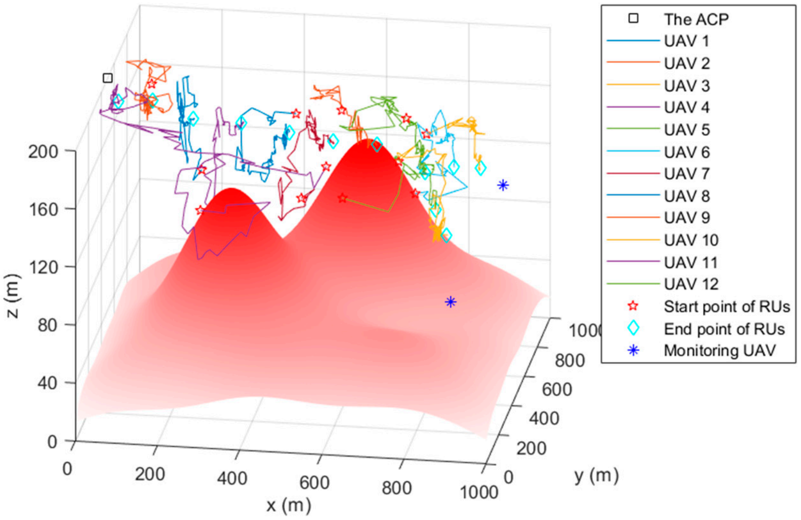

Figure 7. Trajectory of the FANET in a certain time period (Front view).

4.3. Connectivity

Figure 8a,b show each algorithm's network connectivity in the iterative process of FANET construction. To facilitate the demonstration, we select the FANET construction process of different algorithms in the same scene, including identical threat PDF and the movement of monitored targets. Due to limited space, only the process where the RUs' number is 10, 14, and 18 is displayed, respectively. The RWP algorithm is listed separately in Figure 8, considering that the value range of this algorithm's communication performance is quite different from others.

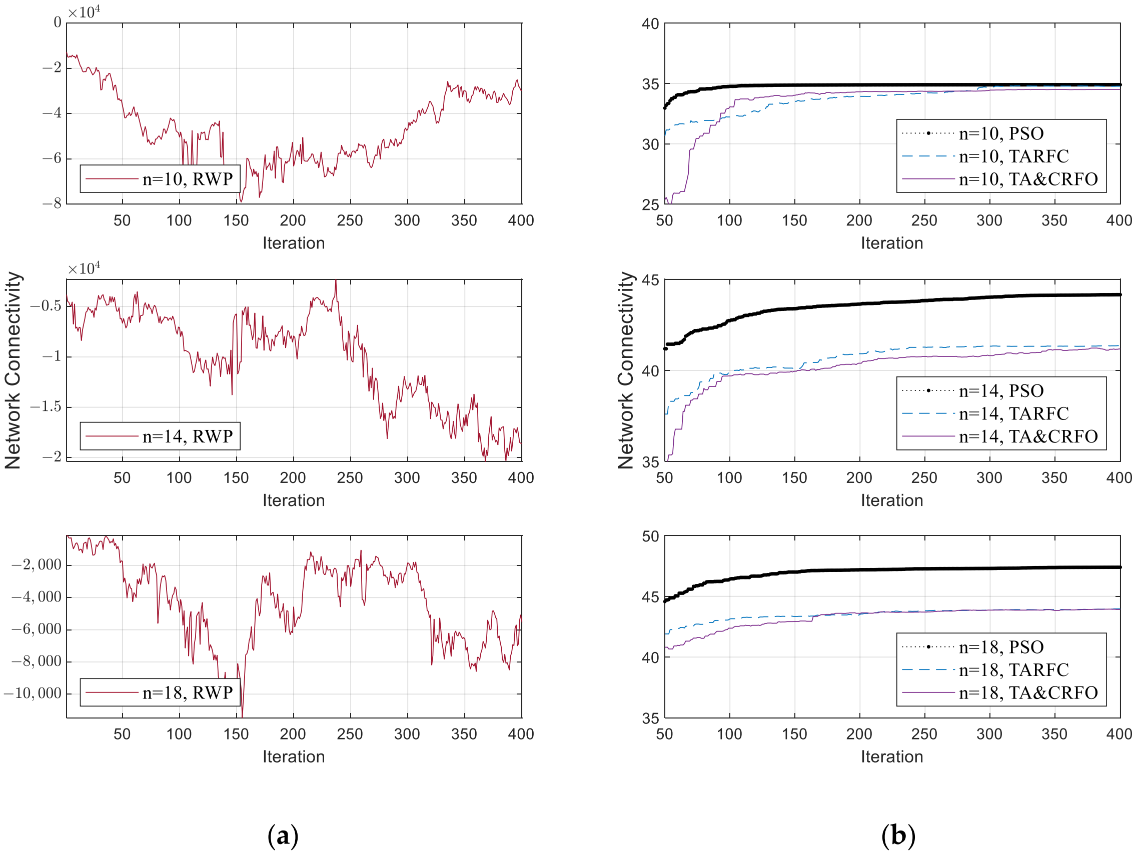

Figure 8. The Network Connectivity fluctuation of algorithms in the iterative process of FANET construction: (**a**) The fluctuation of the RWP algorithm; (**b**) The fluctuation of other algorithms.

RWP is a random movement model. In this model, nodes move randomly without any constraints. The nodes are random in speed, direction of motion, and are independent of each other. However, our reconnaissance targets are not entirely random in the real world. Therefore, after the distance constraint in Equation (6) is converted into a penalty coefficient (Equation (11)), the increase in the penalty term makes the network connectivity of RWP fluctuate randomly in a wide range (shown in Figure 8a). Moreover, the network connectivity of the FANET constructed by RWP does not converge with the iterative process since the nodes' movement in the RWP algorithm has characteristics of randomness and irregularity.

Figure 8b shows the convergence process of PSO, TARFC, and TA&CRFO's network connectivity. Among them, PSO only focuses on optimizing network connectivity, while TARFC and TA&CRFO also consider threat avoidance during the continuous reconnaissance process. Therefore, PSO is slightly better than TARFC and TA&CRFO in terms of network connectivity. TA&CRFO is a simplified version of TARFC in terms of complexity, but as can be seen from the chart, the performance of network connectivity is comparable to that of TARFC. In addition, as the RU number increases, the network connectivity of those algorithms also increases, and their performance shows a tendency toward convergence.

4.4. FANET Threat Metric

In Figure 9, the fluctuation of the UAV's average threat value is presented. Four different colored curves in the picture represent four different algorithms. Similarly, the FANET threat metric with 10, 14, and 18 RUs in the network illustrates the trend of UAV's average threat value with the number of RUs.

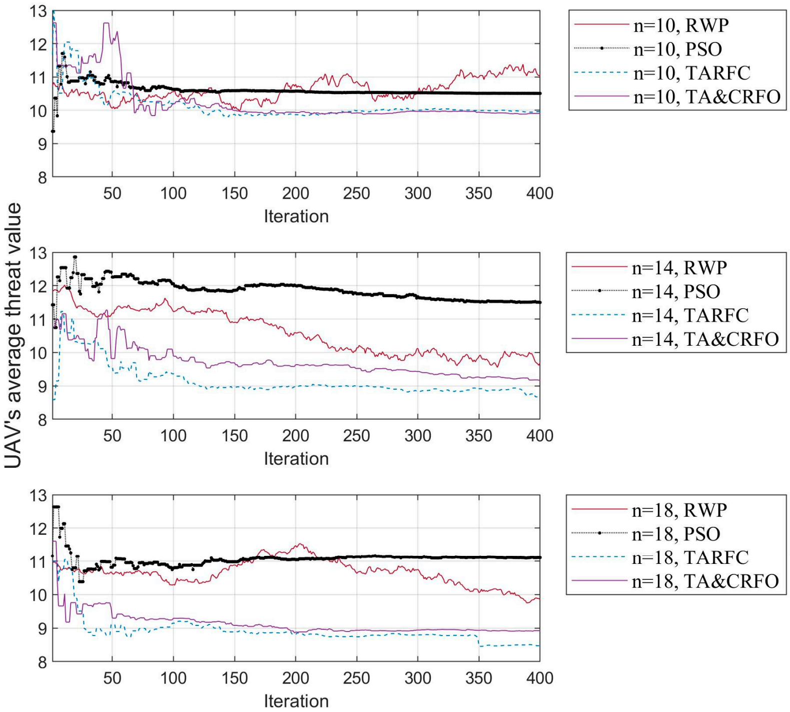

Figure 9. The UAV's average threat fluctuation of different algorithms in the iterative process of FANET construction.

As mentioned above, the excessive randomness of RWP makes the FANET threat metric fluctuate randomly within a wide range of values and does not tend to converge in the iteration process. On the contrary, other algorithms gradually find the UAVs' optimal position in the iteration process, and their FANET threat metric can converge to a small range. In addition, by longitudinal comparison of the three subgraphs, the spatial freedom of each relay UAV increases as the number of RUs increases, which allows them to optimize themselves by reaching better relay positions.

4.5. Detailed Comparison of Algorithms

In this section, we examine the four algorithms from a variety of perspectives, including the overall performance, average threat value for UAVs, longest and shortest link distances between UAVs, and algorithm complexity. In order to ensure the effectiveness of comparative experiments, all parameters in different algorithm experiments are consistent. The results are averaged over 20 repeated experiments.

Due to the randomness of RWP, its total performance (Equation (11)) is not ideal and the value varies rapidly. Thus, Figure 10 shows the overall performance variations of PSO, TARFC, and TA&CRFO as the number of available RUs increases. We notice that the connectivity value of these three algorithms is between 34 and 50, after which they tend to be stable, while the FANET threat metric is in the range of 8–12. To ensure the fluctuation of these two values is consistent, the weight factors w^C and w^T were set to 0.5 and 2.5, respectively.

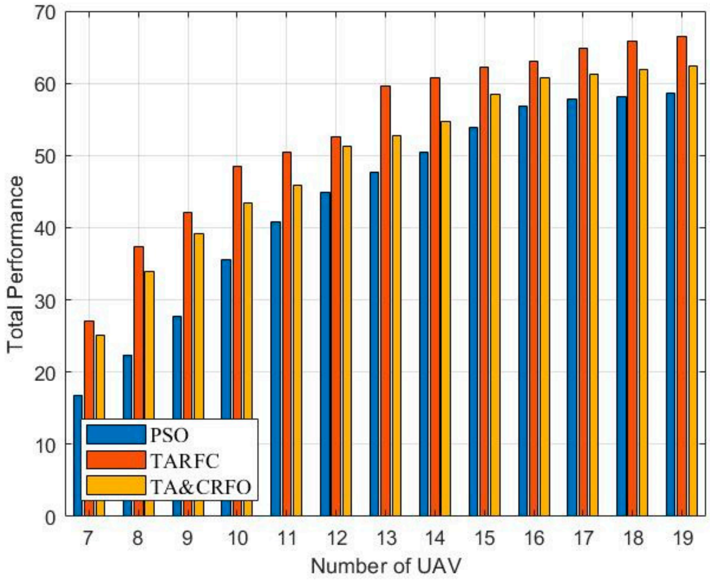

Figure 10. Total Performance of algorithms.

The network's connectivity requires a certain number of UAVs as a guarantee, so the number of RUs starts from seven, according to the simulation experiment. It can be seen that with the increase in RUs, the total performance of the three algorithms becomes larger. However, it should be noted that the performance improvement of PSO mainly comes from network connectivity, so its growth trend gradually decreases. Whereas the performance of TARFC and TA&CRFO is first improved due to network connectivity; then, as the RUs' option space increases, low-threat density areas are selected as relay positions.

Figure 11 presents the UAV's average threat value obtained by constructing the FANET with different algorithms. It is worth mentioning that most places in the scene have a threat PDF between 6 and 13. It can be easily seen that the UAV's average threat value in RWP and PSO does not decrease with the increase in RU number but fluctuates randomly. This is because RWP moves randomly in space, while PSO only cares about the interconnection between nodes and does not consider the threat PDF information in the scene. On the contrary, the UAV's average threat value in TARFC and TA&CRFO is lower than that of the above two algorithms and gradually decreases with the increase in relays. Among them, TARFC is slightly better than TA&CRFO, mainly because TA&CRFO performs distributed adjustments sometimes and cannot keep the optimal global state at all times.

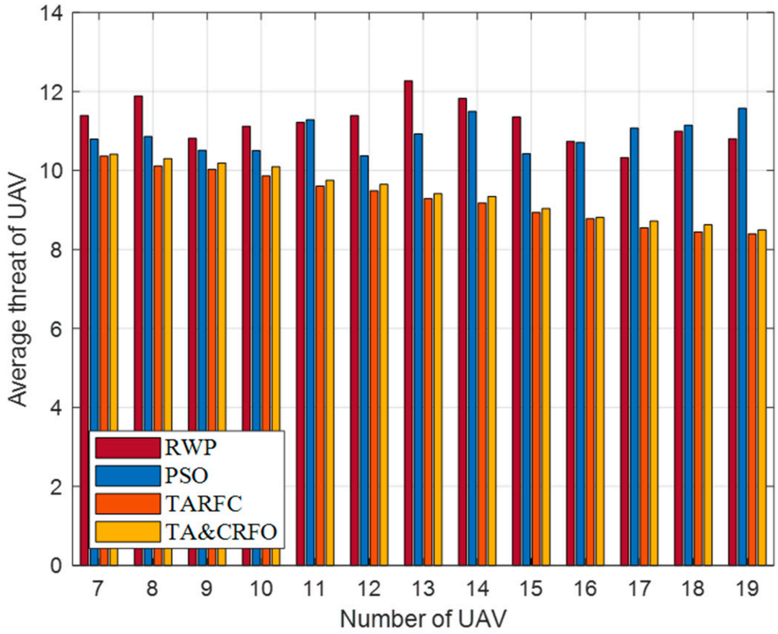

Figure 11. UAV's average threat value with different algorithms.

Figures 12 and 13 show the longest and shortest UAV distance of the FANET constructed by different algorithms. Taken these two metrics together, they demonstrate FANET's compactness and uniformity. As shown in the figures, other algorithms can meet the constraints of the maximum communication distance of 200 m between UAVs and the minimum safe distance of 50 m, except RWP. Among them, with the increase in relays, the decrease in PSO's longest link distance is more significant than that of TARFC and TA&CRFO, while the decline of the shortest UAV distance is smaller than that of TARFC and TA&CRFO. It can be seen that PSO can make the FANET's nodes tend to be evenly distributed. However, for realistic scenarios with uneven threat PDF, algorithms such as TARFC and TA&CRFO obviously have more advantages since they can bypass the high-risk area.

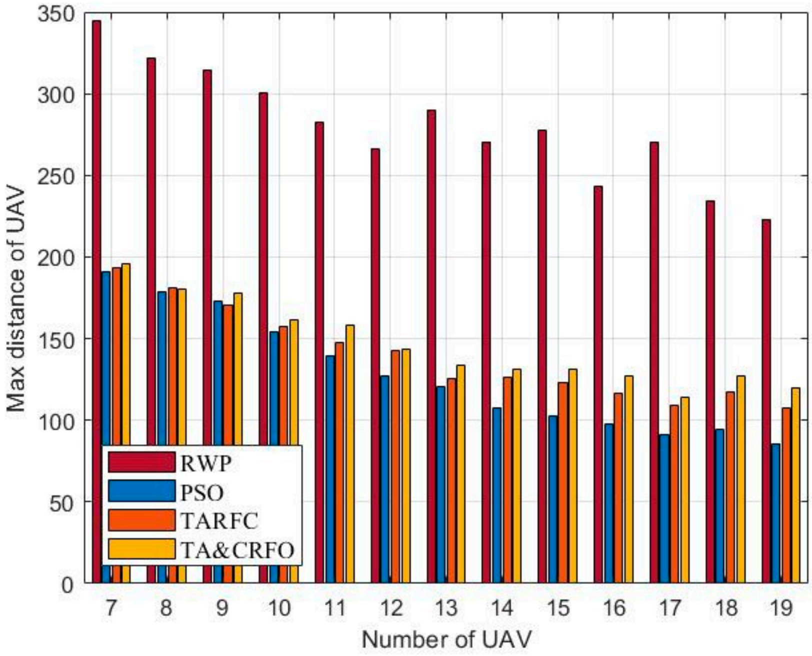

Figure 12. The longest link distance of FANET constructed by different algorithms.

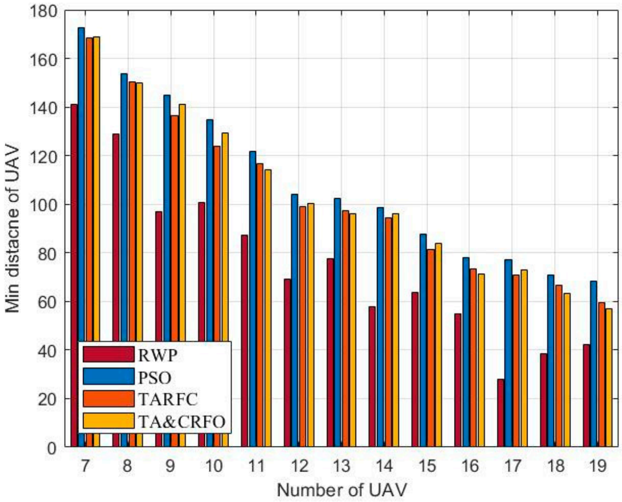

Figure 13. The shortest UAV distance of FANET constructed by different algorithms.

We assume that the high-altitude UAV control center has superior operational capability and can obtain the algorithm's optimization results in milliseconds. However, the FANET results constructed by the algorithm cannot be provided in time due to the limitations of our simulation equipment. To visualize the algorithms' complexity, we use the same parameter settings and scene settings to simulate two detected targets at different positions moving 300 m in a straight line. Continuous reconnaissance is carried out for this process, and the total execution time of each algorithm is calculated (target one from (900, 900, and 100) m to (660, 720, 100) m, and target two from (900, 100, and 100) m to (900, 400, and 100) m). It is assumed that only when the algorithm completes the FANET's construction of time step t will the monitored target will arrive from the position at t to the position at τ.

Figure 14 shows the execution time of different algorithms to complete the entire continuous reconnaissance process. There is no iterative process in RWP, and the selection process at each moment is entirely random, so its average execution time is about 12.46~13.11% of that of PSO and TARFC. TARFC has a similar complexity as PSO, but it optimizes the maintenance of network connectivity and the avoidance of high-threat areas. Based on the original TARFC, TA&CRFO is designed to selectively realize the self-adaptive regulation of UAVs, which effectively reduces the iterative operation of the algorithm. When the parameter threshold λ is set to 5.23, the TA&CRFO's execution time is about 19.86~20.31% of that of TARFC, even though its effect is slightly inferior to that of the TARFC algorithm in other aspects (Figures 9–13).

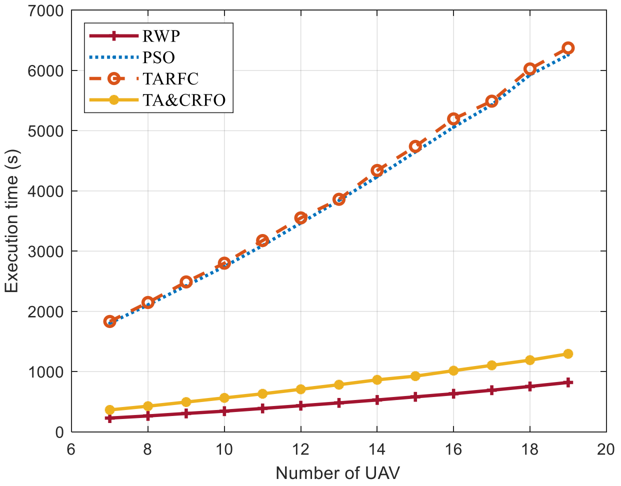

Figure 14. The average execution time of different algorithms.

5. Conclusions and Future Works

This paper presents a layered structure of FANET, in which high-altitude UAVs act as ACPs and multiple UAVs are used for remote relaying and data collection. A "sustainable" dynamic reconnaissance mechanism, TARFC, is constructed considering the movement of reconnaissance targets and the change in various adverse factors in the scenario.

During the simulation, we found that for the FANET, maintaining network connectivity and avoiding local threats during mission execution are two conflicting requirements. The basic PSO only considers network connectivity, which has the best performance in this aspect but is inferior to TARFC and TA&CRFO in terms of threat avoidance. For the latter two algorithms, the weighting values of network connectivity and threat avoidance during simulation must be carefully considered according to realistic requirements. The overall performance of the TA&CRFO algorithm is slightly lower than that of TARFC, but its computational overhead is effectively reduced by decreasing the iterative process. In addition, the computation time required by TA&CRFO increases more slowly as the number of UAVs used in the simulation increases. So, the TA&CRFO algorithm is more suitable for larger-scale FANET.

Of course, the design of indicator functions such as TED also determines the simulation results to a large extent and should be paid special attention.

In this work, the network construction process of Algorithm 1 is carried out on the high-altitude UAV, namely, ACP, which is a centralized approach. The TA&CRFO algorithm is semi-distributed since local neighbor information is used between UAVs when the TED is less than the threshold value. This approach reduces communication overhead and dependence on the central node ACP. In the future, a fully distributed continuous reconnaissance algorithm that completely abandons the central node will bring a greater leap in FANET's adaptability and survivability. In addition, a complex sensing model and connectivity disruption caused by UAV failure will be further considered.

Author Contributions: Conceptualization, Y.G. and R.Q.; methodology, Y.G. and R.Q.; software, Y.G.; validation, Y.G.; formal analysis, Y.G.; investigation, Y.G.; resources, R.Q.; data curation, Y.G.; writing—original draft preparation, Y.G.; writing—review and editing, Y.G. and H.T.; visualization, H.T.; supervision, H.T. and R.Q.; project administration, Y.G.; funding acquisition, H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant number 61901457.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

References

1. Shah, A.; Ilhan, H.; Tureli, U. Designing and Analysis of IEEE 802.11 MAC for UAVs Ad Hoc Networks. In Proceedings of the IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), Columbia Univ, New York, NY, USA, 10–12 October 2019; pp. 634–639.
2. Khan, M.A.; Qureshi, I.M.; Safi, A.; Khan, I.U. Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols. In Proceedings of the Electrical Engineering & Computing Technologies, Karachi, Pakistan, 15–16 November 2017; pp. 1–9.
3. Rosati, S.; Kruelecki, K.; Heitz, G.; Floreano, D.; Rimoldi, B. Dynamic Routing for Flying Ad Hoc Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1690–1700. [CrossRef]
4. Oubbati, O.S.; Lakas, A.; Lagraa, N.; Yagoubi, M.B. CRUV: Connectivity-based traffic density aware routing using UAVs for VANets. In Proceedings of the 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, China, 19–23 October 2015; pp. 68–73.
5. Kai, L.; Wei, N.; Xin, W.; Ren, P.L.; Kanhere, S.S.; Jha, S. Energy-Efficient Cooperative Relaying for Unmanned Aerial Vehicles. *IEEE Trans. Mob. Comput.* **2016**, *15*, 1377–1386.
6. Chen, R.; Yang, B.; Zhang, W. Distributed and Collaborative Localization for Swarming UAVs. *IEEE Internet Things J.* **2021**, *8*, 5062–5074. [CrossRef]

7. Liu, C.; Zhang, Z. Towards a robust FANET: Distributed node importance estimation-based connectivity maintenance for UAV swarms. *Ad. Hoc. Netw.* **2022**, *125*, 102734. [CrossRef]
8. Dapper e Silva, T.; Emygdio de Melo, C.F.; Cumino, P.; Rosario, D.; Cerqueira, E.; Pignaton de Freitas, E. STFANET: SDN-Based Topology Management for Flying Ad Hoc Network. *IEEE Access* **2019**, *7*, 173499–173514. [CrossRef]
9. Mozaffari, M.; Saad, W.; Bennis, M.; Debbah, M. Efficient Deployment of Multiple Unmanned Aerial Vehicles for Optimal Wireless Coverage. *IEEE Commun. Lett.* **2016**, *20*, 1647–1650. [CrossRef]
10. Zhu, Q.; Zhou, R.; Zhang, J. Connectivity Maintenance Based on Multiple Relay UAVs Selection Scheme in Cooperative Surveillance. *Appl. Sci.* **2016**, *7*, 8. [CrossRef]
11. Joshi, A.; Dhongdi, S.; Dharmadhikari, M.; Mehta, O.; Anupama, K.R. Enclosing and monitoring of disaster area boundary using multi-UAV network. *J. Ambient Intell. Humaniz. Comput.* **2022**. [CrossRef]
12. Sánchez-García, J.; Reina, D.G.; Toral, S.L. A distributed PSO-based exploration algorithm for a UAV network assisting a disaster scenario. *Future Gener. Comput. Syst.* **2019**, *90*, 129–148. [CrossRef]
13. Siddiqi, M.H.; Draz, U.; Ali, A.; Iqbal, M.; Alruwaili, M.; Alhwaiti, Y.; Alanazi, S. FANET: Smart city mobility off to a flying start with self-organized drone-based networks. *IET Commun.* **2021**, *16*, 1209–1217. [CrossRef]
14. Naser, M.Z.; Kodur, V.R. Concepts and applications for integrating Unmanned Aerial Vehicles (UAV's) in disaster management. *Adv. Comput. Des.* **2020**, *5*, 91–109.
15. Zuev, A.; Gryb, O.; Shvets, S.; Makarov, V. Evaluating and Ensuring the Cybersecurity of Power Line Remote Monitoring Systems. In Proceedings of the 2018 IEEE 3rd International Conference on Intelligent Energy and Power Systems (IEPS), Kharkiv, Ukraine, 10–14 September 2018.
16. Zhao, N.; Yang, X.; Ren, A.; Zhang, Z.; Zhao, W.; Hu, F.; Rehman, M.U.; Abbas, H.; Abolhasan, M. Antenna and Propagation Considerations for Amateur UAV Monitoring. *IEEE Access* **2018**, *6*, 28001–28007. [CrossRef]
17. Song, R.; Long, T.; Wang, Z.; Cao, Y.; Xu, G. Multi-UAV Cooperative Target Tracking Method using sparse A search and Standoff tracking algorithms. In Proceedings of the 2018 IEEE CSAA Guidance, Navigation and Control Conference (GNCC), Xiamen, China, 10–12 August 2018.
18. Xu, C.; Zhang, K.; Jiang, Y.; Niu, S.; Yang, T.; Song, H. Communication Aware UAV Swarm Surveillance Based on Hierarchical Architecture. *Drones* **2021**, *5*, 33. [CrossRef]
19. Srivastava, A.; Prakash, J. Future FANET with application and enabling techniques: Anatomization and sustainability issues. *Comput. Sci. Rev.* **2021**, *39*, 100359. [CrossRef]
20. Pasandideh, F.; Silva, T.D.e.; Silva, A.A.S.d.; Pignaton de Freitas, E. Topology management for flying ad hoc networks based on particle swarm optimization and software-defined networking. *Wirel. Netw.* **2021**, *28*, 257–272. [CrossRef]
21. Qi, X.; Yuan, P.; Zhang, Q.; Yang, Z. CDS-Based Topology Control in FANETs via Power and Position Optimization. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 2015–2019. [CrossRef]
22. Lin, N.; Fu, L.; Zhao, L.; Min, G.; Al-Dubai, A.; Gacanin, H. A Novel Multimodal Collaborative Drone-Assisted VANET Networking Model. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 4919–4933. [CrossRef]
23. Kim, D.-Y.; Lee, J.-W. Joint Mission Assignment and Topology Management in the Mission-Critical FANET. *IEEE Internet Things J.* **2020**, *7*, 2368–2385. [CrossRef]
24. Zhang, X.; Duan, L. Fast Deployment of UAV Networks for Optimal Wireless Coverage. *IEEE Trans. Mob. Comput.* **2019**, *18*, 588–601. [CrossRef]
25. Li, X.; Yao, H.; Wang, J.; Xu, X.; Jiang, C.; Hanzo, L. A Near-Optimal UAV-Aided Radio Coverage Strategy for Dense Urban Areas. *IEEE Trans. Veh. Technol.* **2019**, *68*, 9098–9109. [CrossRef]
26. Zhou, Z.; Feng, J.; Gu, B.; Ai, B.; Mumtaz, S.; Rodriguez, J.; Guizani, M. When Mobile Crowd Sensing Meets UAV: Energy-Efficient Task Assignment and Route Planning. *IEEE Trans. Commun.* **2018**, *66*, 5526–5538. [CrossRef]
27. Li, J.; Guo, L.; Dong, C. Constructing Small Worlds in WSNs with UAV Trajectory Optimization. In Proceedings of the 2nd International Conference on Telecommunications and Communication Engineering—ICTCE 2018, Beijing, China, 28–30 November 2018; pp. 309–313.
28. Friis, H.T. A Note on a Simple Transmission Formula. *Proc. IRE* **1946**, *34*, 254–256. [CrossRef]
29. Abeywickrama, H.V.; Jayawickrama, B.A.; Ying, H.; Dutkiewicz, E. Comprehensive Energy Consumption Model for Unmanned Aerial Vehicles, Based on Empirical Studies of Battery Performance. *IEEE Access* **2018**, *6*, 58383–58394. [CrossRef]
30. Khawaja, W.; Guvenc, I.; Matolak, D.W.; Fiebig, U.C.; Schneckenburger, N. A Survey of Air-to-Ground Propagation Channel Modeling for Unmanned Aerial Vehicles. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2361–2391. [CrossRef]
31. Gao, X.; Xiao, B.; Tao, D.; Li, X. A survey of graph edit distance. *Pattern Anal. Appl.* **2009**, *13*, 113–129. [CrossRef]
32. Kennedy, J.; Eberhart, R. Particle Swarm Optimization. In Proceedings of the Icnn95-International Conference on Neural Networks, Perth, WA, Australia, 27 November–1 December 1995.
33. Karush, W. *Minima of Functions of Several Variables with Inequalities as Side Conditions*; Springer: Basel, Switzerland, 1939.
34. Bergh, F.; Engelbrecht, A.P. A study of particle swarm optimization particle trajectories. *Inf. Sci.* **2006**, *176*, 937–971.
35. Sanfeliu, A.; Fu, K. A distance measure between attributed relational graphs for pattern recognition. *IEEE Trans. Syst. Man Cybern.* **1983**, *SMC-13*, 353–362. [CrossRef]
36. Agrawal, J.; Kapoor, M.; Tomar, R. A novel unmanned aerial vehicle-sink enabled mobility model for military operations in sparse flying ad-hoc network. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4466. [CrossRef]