Chinese Journal of Aeronautics, (2020), 33(1): 352–364

Chinese Society of Aeronautics and Astronautics
& Beihang University

Chinese Journal of Aeronautics

cja@buaa.edu.cn
www.sciencedirect.com

Electronics and Electrical Engineering and Control–Research Article

Robustness evaluation method for unmanned aerial vehicle swarms based on complex network theory

Xiaohong WANG [a], Yuan ZHANG [a], Lizhi WANG [b,c,*], Dawei LU [a], Guoqi ZENG [b,c]

[a] *School of Reliability and Systems Engineering, Beihang University, Beijing 100083, China*
[b] *Unmanned System Institute, Beihang University, Beijing 100083, China*
[c] *Key Laboratory of Advanced Technology of Intelligent Unmanned Flight System of Ministry of Industry and Information Technology, Beijing 100083, China*

Received 14 January 2019; revised 6 March 2019; accepted 31 March 2019
Available online 31 May 2019

KEYWORDS

Complex networks;
Dynamic reconfiguration;
Information correlation;
Robustness evaluation;
Unmanned Aerial Vehicles (UAV)

Abstract Unmanned Aerial Vehicle (UAV) swarms have been foreseen to play an important role in military applications in the future, wherein they will be frequently subjected to different disturbances and destructions such as attacks and equipment faults. Therefore, a sophisticated robustness evaluation mechanism is of considerable importance for the reliable functioning of the UAV swarms. However, their complex characteristics and irregular dynamic evolution make them extremely challenging and uncertain to evaluate the robustness of such a system. In this paper, a complex network theory-based robustness evaluation method for a UAV swarming system is proposed. This method takes into account the dynamic evolution of UAV swarms, including dynamic reconfiguration and information correlation. The paper analyzes and models the aforementioned dynamic evolution and establishes a comprehensive robustness metric and two evaluation strategies. The robustness evaluation method and algorithms considering dynamic reconfiguration and information correlation are developed. Finally, the validity of the proposed method is verified by conducting a case study analysis. The results can further provide some guidance and reference for the robust design, mission planning and decision-making of UAV swarms.

[*] Corresponding author.
E-mail addresses: wanglizhi@buaa.edu.cn (L. WANG), zengguoqi@buaa.edu.cn (G. ZENG).

Peer review under responsibility of Editorial Committee of CJA.

ELSEVIER Production and hosting by Elsevier

https://doi.org/10.1016/j.cja.2019.04.025

1. Introduction

Unmanned Aerial Vehicles (UAVs) have been increasingly utilized by both military and civilian organizations because they are less expensive, lead to zero casualty, and provide greater flexibilities. With the development of network communication and intelligent theory, in the near future, swarms of UAVs will replace single UAV use.[1] In comparison, UAV swarms have larger scale, higher operational efficiency, and stronger survivability. Therefore, they have a wider application potential in cooperative search, reconnaissance, war fighting, and other missions.[2] In recent years, many studies have been conducted on UAV swarms or other multi-agent system,[3,4] such as autonomous collaboration[5], communication control,[6,7] formation control,[8] and path planning.[9] However, for the UAV swarms used in the military, the complicated and changeable battlefield environment brings about considerable uncertainties and unforeseen circumstances.[10] The UAV swarms need to guarantee the success of the mission even if they lose a part of the UAVs. This puts forward higher requirements for the robustness of such a system.[11] Therefore, it is of great importance to study the robustness evaluation of UAV swarms considering their dynamic evolution. This work provides technical support to ensure the high reliability and security of UAV swarms. It also contributes to the formation design, mission management, and operational strategy adjustment for the system.

The robustness of UAV swarms reflects the ability to maintain function and complete missions after losing some UAVs. However, UAV swarms are large-scale complex systems with a complicated hierarchy, dynamic characteristics, and various formation-control methods.[12,13] When performing missions, they might encounter many different types of attacks and lose some UAVs. Thus, UAV swarms need dynamic reconfiguration to ensure the integrity of communication and meet other requirements.[14] Furthermore, the communication network of the UAV swarms has information correlation, because it may be attacked by viruses during electronic warfare, which may lead to a cascade failure.[15] Therefore, it is very challenging to establish an effective model to evaluate the robustness of a UAV swarming system that fully considers the abovementioned dynamic evolution processes. To achieve our objective, the first problem to be solved was the modeling of these dynamic evolutions. However, it was difficult to do so with the traditional models. A large number of studies have focused on the analysis and modeling of complex systems.[16–18] In the reliability field, there are some key methods including agent-based models,[19,20] Bayesian network models,[21,22] system dynamics,[23] the Petri-net method,[24,25] complex-network theory,[26,27] and other modeling methods. In recent years, the complex network theory has proven to be a fertile ground for the modeling of complex systems. This method has been widely applied in power grids, infrastructure, transportation systems, manufacturing, and other fields.[28,29] A UAV swarming system has some similar characteristics and can be naturally mapped into complex networks to describe them. The dynamic evolution relationship of the system can also be described by changing its nodes and edges.[30,31] Moreover, in our previous studies, three typical structures of UAV swarming systems were modeled and topologically analyzed by using a multi-layer complex network.[32] The results showed that the complex networks satisfied the small-world characteristics and scale-free properties. On this basis, we applied the complex network theory to analyze and model the dynamic evolutions of UAV swarms, namely dynamic reconfiguration and information correlation, for future robustness evaluations.

At present, few studies have been conducted on the reliability and robustness of UAV swarms, and hence, there are few references for our work. However, the research on the robustness of complex networks can provide us with some ideas.[33] The focus of robustness in complex networks is the response of the network to the removal of nodes or edges.[34] A UAV swarming system is a multi-layer complex network with multiple functional correlations. When the nodes suffer from an external attack or internal damage, the uncertainty of the impact on the entire system increases. Therefore, the traditional methods and conclusions on the robustness of single-layer complex networks cannot be fully applied to that of multi-layer networks. With respect to the robustness of multi-layer complex networks, Bilal et al. proposed the robustness quantification of hierarchical complex networks under targeted failures.[35] They analyzed 10 different real-world networks with varying graph characteristics by using the classical robustness metrics. Buldyrev simulated and analyzed the catastrophic cascade of failures in interdependent networks.[36] Thacker et al. characterized critical national infrastructures as a system-of-systems and developed a methodology to perform a multi-scale disruption analysis. Furthermore, the fault propagation principles in a multi-layer network system are obtained through simulation analysis.[37] In general, the methods of evaluating the robustness of complex networks mainly consider the random attacks or targeted attacks to the network structure and complex networks with a cascade failure.[38,39] However, these methods have no specific research objects and are unable to contain the specific application environment of UAV swarms, so it is difficult to reflect the dynamic evolution relationship mentioned above. In addition, many scholars have proposed some robustness metrics for specific systems. Some of them only focus on single topological characteristic parameters in graph theory. That is, the robustness evaluation strategy is used to analyze the change in a single parameter caused by node removal,[40] such as the node degree and the average path length. Because different topology parameters reflect different properties and vary with node removal, scholars have proposed some comprehensive metrics for robustness evaluation.[41] However, most of them measure the weight of the metrics according to the characteristics of the specific system, and there is no general comprehensive robustness metric. Therefore, on the basis of the existing research, we established a general comprehensive robustness evaluation metric for UAV swarms. The corresponding robustness evaluation methods and algorithms are proposed according to the dynamic evolution models including dynamic reconfiguration and information correlation.

To this end, in this study, the complex network theory was adopted to explore the robustness evaluation of UAV swarms. By doing so, on the basis of our previous research, we established the dynamic evolution models considering dynamic reconfiguration and information correlation for three typical structures of UAV swarms. These models were used to further propose robustness evaluation methods and algorithms combining the comprehensive robustness metric that we built and the evaluation strategies, random attacks, or targeted attacks. The robustness evaluation result could be used to provide reference for the formation control, mission assignment, operational decision making, and other tasks related to the UAV swarms.

The rest of this paper is organized as follows: In Section 2, a generalized description of the complex network modeling for a UAV swarming system is provided. The dynamic evolutions of the system, namely dynamic reconfiguration and information correlation, are analyzed and modeled. In Section 3, robustness evaluation methods, including comprehensive robustness metric, evaluation strategies, and evaluation algorithms with dynamic evolutions, are presented. In Section 4, a case study is provided to illustrate the validity of the proposed method. Some conclusions and future works are presented in Section 5.

2. Complex network modeling for dynamic evolution of UAV swarming system

2.1. System description and modeling

A UAV swarming system is a flock of UAVs that carry different payloads for multiple missions. The system composition could contain numerous components, but, more generally, the vehicle, the payload, and the ad hoc network are the critical ones.[42]

UAV swarms have a certain structure to facilitate formation control or to accomplish specific missions. In general, their structure is related to the autonomy level and the formation-control algorithm. In our previous work, we chose three structures of UAV swarms based on three types of control algorithms, namely a control structure based on the behavior-based method (Structure 1), on leader-follower strategy (Structure 2), and on autonomous control (Structure 3).[32] The behavior-based method is based on the flocking of pigeons that exists in a hierarchical leadership network; here, pigeons follow the individuals in the upper ranks and lead the flights of individuals in the lower ranks.[43] The schematic representation of such a structure is shown in Fig. 1(a). In Structure 2, each leader and its followers form a community, and the leaders can communicate with each other. The followers only communicate with their leaders and the UAVs that are adjacent to them.[44] The corresponding schematic representation is shown in Fig. 1(b). Structure 3 has no fixed structure that the UAVs can automatically organize, communicate, and coordinate with each other. In this paper, we continue to consider these three structures as the study objects.

On the basis of the complex network theory, a system can be described by a network in which the nodes represent the subsystems and link the physical or logical connections among them.[45] Therefore, UAV swarms are considered to consist of three interdependent complex network layers, namely the communication layer, the structure layer, and the mission layer, denoted as G_a, G_b, and G_c, representing ad hoc network, vehicle, and payload, respectively. Three networks are abstracted into graphs on the basis of the graph theory. It is supposed that a UAV swarming system consists of n vehicles and m types of payloads. For each payload, there are n_i (i = 1,2,…, m) vehicles, where $n_1 + n_2 + \ldots + n_m = n$. The concrete network layers, interlayer relationships, and structure modeling algorithms for the three structures of UAV swarms were discussed in detail in our previous paper.[32] A schematic of the network representation based on a multi-layer complex network for UAV swarms is illustrated in Fig. 2. The normalized description of this complex network is shown in Table 1. Ref. [32] also verified the correctness and the validity of the model. Therefore, it was used for the following dynamic topology analysis and robustness analysis.

2.2. System dynamic evolution analysis and modeling

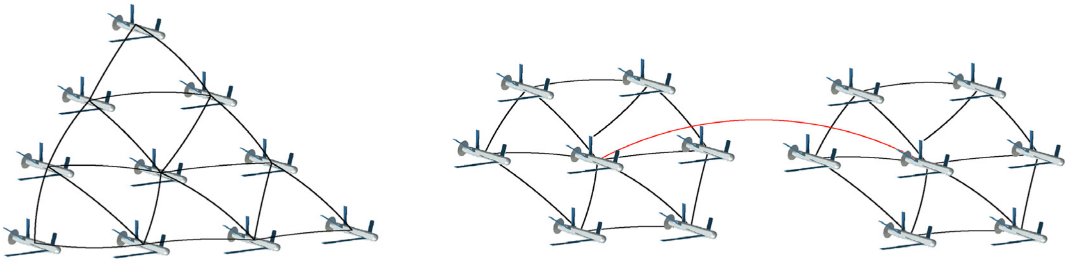
The robustness in complex networks refers to the ability to maintain function and structural integrity with the removal of nodes or edges.[34] As for the UAV swarming networks, removing nodes often mean being attacked. However, some dynamic evolution processes exist in UAV swarms when under attack. As mentioned, one is dynamic reconfiguration, and the other is information correlation by virus propagation that leads to a cascade failure. Therefore, these processes may have a considerable effect on system robustness. The analysis and modeling of these processes are the premise of the robustness evaluation. In a complex network, the dynamic changes can be expressed by the changes in the nodes and the edges. Therefore, we modeled the dynamic evolution processes by adopting and extending our model in Section 2.1.

Because of the functional correlation between the nodes, the removal of nodes in one layer will lead to the removal of nodes in other layers along with the removal of the interlayer edges.[32] In a UAV swarming network, when the nodes in the structure layer are removed, the nodes in the communication layer and the mission layer connected to them are also removed accordingly. Similarly, when the nodes in the communication layer fail, the connected nodes in the mission layer will lose their function and be removed accordingly.

Next, the two dynamic evolution processes for UAV swarms are defined and modeled below.

(1) Dynamic reconfiguration process

Dynamic reconfiguration refers to the process of quickly recovering the system's capabilities and reconstructing its


(a) Structure 1

(b) Structure 2

Fig. 1 Schematic diagram of typical structures.

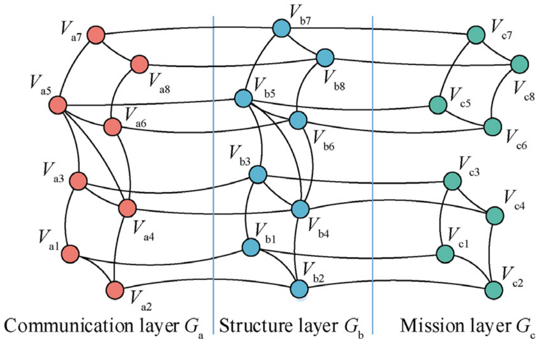


Fig. 2 Schematic of network representation.

Table 1 Normalized description of network.

Composition	Drawing	Denotation
Layers	▱▱▱	G_q (q = a,b,c)
Nodes	●	V_{qi} (q = a,b,c;i = 1,2,...,8)
Layer edges	—	E_{qi} (q = a,b,c;i = 1,2,...,8)
Interlayer edges	- · - ·	$L=\{L_i\}$ (i = 1,2, ...,8)

Table 2 Pseudo code of algorithm 1.

```
Dynamic reconfiguration relationship 1
Input: (A) UAV swarming network $G_a$, $G_b$, $G_c$
       (B) set of residual nodes $U_q(q = a,b)$
Output: new UAV swarming network $G_a$, $G_b$, $G_c$
▷ dynamic reconfiguration in communication layer $G_a$
for each node $V_{ai}$ in $U_a$ do
    if $V_{ai}$ an isolated node then
        randomly choose node $V_{aj}$ from $U$
        add edge between $V_{ai}$ and $V_{aj}$
    end if
end for
▷ dynamic reconfiguration in structure layer $G_b$
for each node $V_{bi}$ in $U_b$ do
    if $V_{bi}$ an isolated node then
        randomly choose node $V_{bj}$ from $U$
        add edge between $V_{bi}$ and $V_{bj}$
        add edge between $V_{ai}$ and $V_{aj}$
    end if
end for
return $G_a$, $G_b$, $G_c$
```

structure and function when under attack. In a complex network, it reflects the case wherein the system reconnects the edges after losing the nodes. The process needs to be modeled in order to evaluate the robustness of UAV swarms with dynamic reconfiguration. As for a UAV swarming network, its dynamic reconfiguration process mainly includes two types of relationships.

(A) Dynamic reconfiguration relationship 1

Dynamic reconfiguration relationship 1 exists in all the three structures of UAV swarms. When multiple attacks occur and some nodes are lost, there may exist nodes, called isolated nodes, all of whose neighbor nodes have been removed. To restore their communication and let them continue to perform tasks, they must be connected to other UAVs. That is, the isolated nodes are randomly connected to the adjacent nodes or nodes with a large node degree. The process is shown in Fig. 3.

This relationship may exist in both the communication layer and the structure layer of the UAV swarming network. However, the corresponding processes are slightly different because of the functional correlation mentioned above. Moreover, the aforementioned two situations do not occur at the same time. Therefore, the specific algorithm of dynamic reconfiguration relationship 1 can be expressed in Table 2.

(B) Dynamic reconfiguration relationship 2

Dynamic reconfiguration relationship 2 mainly exists in Structure 2. In Structure 2, the leader needs to be designated, and the followers need to be defined to follow the leader. In order to maintain the formation, a temporary leader will be chosen from the followers when their leader is attacked and removed from the UAV swarming network. Furthermore, the temporary leader will reconnect with all of its followers and the other leaders. The process is shown in Fig. 4.

Similarly, this relationship may exist in both the communication layer and the structure layer of the UAV swarming network. We set a UAV swarming system consisting of n vehicles and m types of payloads, that is, there are m leaders. Then, the specific algorithm of dynamic reconfiguration relationship 2 can be expressed in Table 3. In this algorithm, V_{qi} means the ith node in the UAV swarming network. When the dynamic reconfiguration exists in the communication layer, q = a. Similarly, when the relationship exists in the structure layer, q = b. When the new leaders are determined, the follower still exists in the case wherein all of the neighbor nodes except for its leader are removed. At this time, the isolated nodes are processed according to dynamic reconfiguration relationship 1.

(2) Information correlation process

In the communication layer, the failure of an information delivery node directly affects the other nodes, which is called information correlation. As the wireless communication network of the UAV swarms is the basis to receiving instructions and completing missions, it will inevitably become the focus attack object. In general, viruses and malicious programs are implanted into the network. Depending on the spread of viruses, a node being attacked can cause the other connected nodes to fail, that is, a cascade failure. This will finally lead

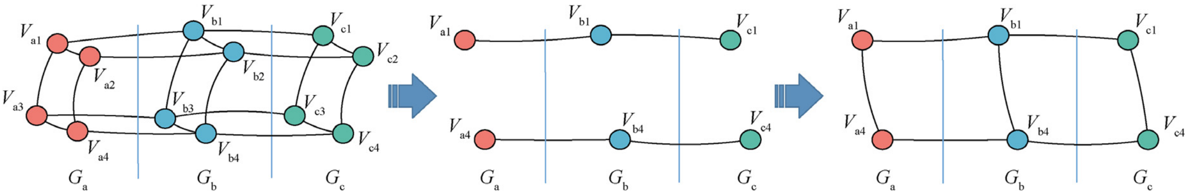


Fig. 3 Dynamic reconfiguration relationship 1.

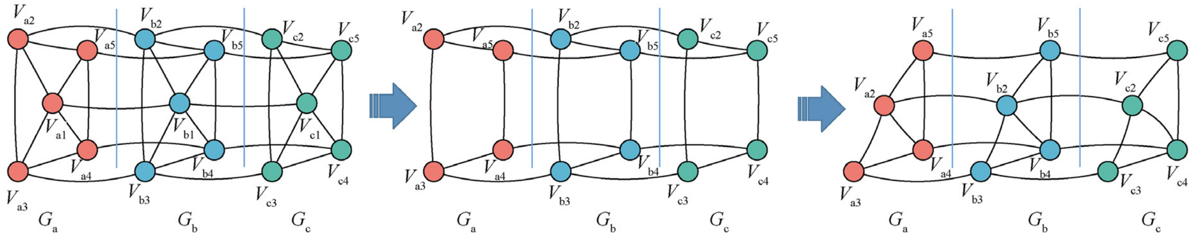


Fig. 4 Dynamic reconfiguration relationship 2.

Table 3 Pseudo code of algorithm 2.

Dynamic reconfiguration relationship 2

Input: (A) UAV swarming network G_a, G_b, G_c; (B) set of removed nodes $R_q(q = \text{a,b})$; (C) set of leader nodes L_q; (D) set of followers nodes $N_q[m]$

Output: new UAV swarming network G_a, G_b, G_c

```
for each node $V_{qi}$ in $L_q$ do
    if $V_{qi}$ in $R_q$ then
        randomly choose node $V_{qj}$ from $N_q[i]$
        delete $V_{qi}$ from $L_q$
        add $V_{qj}$ to $L_q$
        delete $V_{qj}$ from $N_q[i]$
        ▷ dynamic reconfiguration in communication layer $G_a$
        for each node $V_{ap}$ in $N_a[i]$ do
            add edge between $V_{aj}$ and $V_{ap}$
        end for
        for each node $V_{al}$ in $L_a$ do
            add edge between $V_{aj}$ and $V_{al}$
        end for
        ▷ dynamic reconfiguration in structure layer $G_b$
        for each node $V_{bp}$ in $N_b[i]$ do
            add edge between $V_{bj}$ and $V_{bp}$
            add edge between $V_{aj}$ and $V_{ap}$
        end for
        for each node $V_{bl}$ in $L_b$ do
            add edge between $V_{aj}$ and $V_{al}$
        end for
    end if
end for
return $G_a$, $G_b$, $G_c$
```

to an interruption of the communication. This process is shown in Fig. 5.

At present, three types of ad hoc communication networks (ad hoc mobile networks, wireless sensor networks, and wireless mesh networks) can be utilized in UAV swarms owing to their mobility, network topology dynamics, and self-organization.[46] In recent years, many researchers have studied virus propagation laws in such networks. Most of them have described a process based on the classical epidemiological propagation models. The classical models include the SIS (Susceptible Infected Susceptible) model, SIR (Susceptible Infected Recovered) model, and the SEIR (Susceptible Exposed Infected and Resistant) model.[47] In this study, we established a fault propagation model for the communication layer of UAV swarms according to the SIR model. The specific concepts of the model are as follows:

(A) Susceptible state S: Nodes become susceptible when they come into contact with infected nodes.

(B) Infected state I: Nodes are already infected by virus and will spread virus to neighbor nodes.

(C) Removed state Re: Nodes have already recovered health or disappeared. They cause no effect on the other nodes, and the virus cannot be spread to them.

(D) Infection rate β: This is the probability that susceptible nodes become infected after coming into contact with the infected nodes.

(E) Removal rate γ: This is the probability that the infected nodes turn into the removed state.

It is assumed that a UAV swarming system consists of n vehicles and each of them is in the susceptible state. When $t = 0$, m infected nodes appear in its communication layer. Therefore, over time, the infected nodes have a probability β of infecting a susceptible node. Moreover, the infected nodes have the probability γ of becoming in the removed state. Nodes in the removed state can be represented as node removal in complex networks because they have no contact with the nodes in the other two states.

The specific information correlation process is described as follows:

Steps 1. When $t = 0$, set m infected nodes randomly.

Steps 2. Judge whether the infection rate β is reached. If so, one node is randomly selected from the neighbor nodes of the infected nodes and turned into the infected state.

Steps 3. Judge whether the removal rate γ is reached for the infected nodes. If so, turn them into the removed state. Remove them from the network and delete the corresponding nodes in the mission layer.

Steps 4. Let $t = t + 1$, and repeat Steps 2 and 3 until there is no node left in the communication layer.

3. Robustness evaluation method for UAV swarming system

The robustness of UAV swarms reflects the ability to maintain function and complete missions under attack. The methods and results for robustness evaluation will be different in different structures, attack strategies and dynamic evolution processes. Due to the complex characteristics and irregular dynamic evolution of the structure and function of the UAV swarms, it brings more difficulties in the process of program implementation. Besides, the UAV swarming system is a multi-layer complex network, the traditional methods of evaluation using a single robustness metric cannot cover its features. Thus it is challenging and necessary to create a general comprehensive robustness evaluation metric.

In this section, we establish the robustness evaluation metric and the attack strategies for UAV swarming networks. The robustness evaluation methods and algorithms of UAV

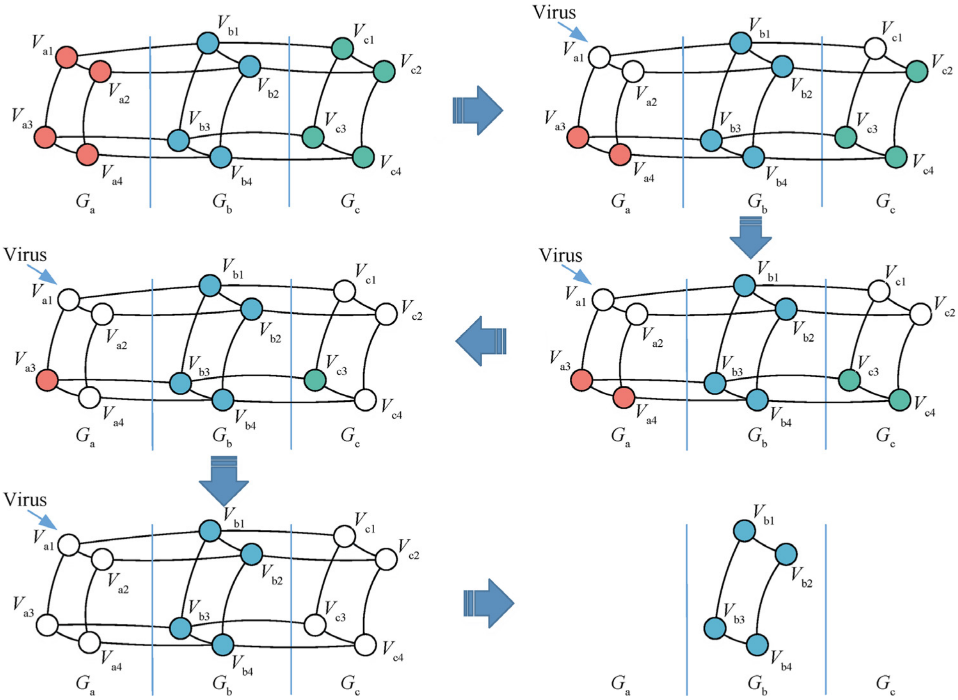


Fig. 5 Information correlation (cascade failure) process.

swarms are proposed considering the two dynamic evolution relationships modeled in Section 2.2.

3.1. Establishing robustness metric

To evaluate the robustness of a UAV swarming system effectively, it is necessary to establish a comprehensive robustness metric that matches its mission characteristics. Although there have been many studies on the robustness metric, to the best of our knowledge, no general metric has been designed so far. Among these, average node degree, clustering coefficient, and average path length are the most commonly used robustness topological metrics. For a UAV swarming network, these metrics can be defined as follows[32]:

(1) Average node degree

The degree of a node in a network is the number of connections that it has to the other nodes. The node degree in a UAV swarming network can be divided into two parts: the degree of node V_{qi} calculated from its network layer, denoted as $k_{qi}(G_q)$ (q = a,b,c), and the degree calculated by the connections with nodes in other layers, denoted as k^l_{qi}. Here

$$\begin{cases} k^l_{qi} = 1 & V_{qi} \in G_{\text{a}}|G_{\text{c}} \\ k^l_{qi} = 2 & V_{qi} \in G_{\text{b}} \end{cases} \quad i = 1, 2, ..., n \tag{1}$$

Then, the node degree of V_{qi} can be expressed as

$$k_{qi} = k_{qi}(G_q) + k^l_{qi} \quad q = \text{a, b, c}; \qquad i = 1, 2, ..., n \tag{2}$$

The average degree can be written as

$$k = \frac{1}{3n} \sum_{q=\text{a}}^{\text{c}} \sum_{i=1}^{n} k_{qi} \tag{3}$$

(2) Clustering coefficient

A clustering coefficient is a measure of the degree to which the nodes in a graph tend to cluster.[48] It can be calculated by using the ratio of the edges E_{qi} among k_{qi} adjacent nodes of nodes V_{qi} and the total number of possible edges $k_{qi}(k_{qi} - 1)/2$, that is,

$$C_{qi} = \frac{2E_{qi}}{k_{qi}(k_{qi} - 1)} \tag{4}$$

Then, the clustering coefficient of the network can be written as

$$C = \frac{1}{3n} \sum_{q=\text{a}}^{\text{c}} \sum_{i=1}^{n} C_{qi} \tag{5}$$

(3) Average path length

The average path length, representing the tightness of connections between the nodes in a network, can be used to measure the efficiency of the network.[48] It is defined by the arithmetic mean of the shortest path d_{ij} $(i,j = 1, 2, ..., n)$ between a node pair, that is,

$$L = \frac{2}{3n(n-1)} \sum_{i>j} d_{ij} \tag{6}$$

According to the complex network characteristics of UAV swarms, there is no practical significance of the interlayer edges. Therefore, we did not choose the average path length as the robustness topological metric for UAV swarms. In addition to the average node degree and the clustering coefficient, a metric considering the transmission performance of the communication layer, network efficiency, was chosen.

(4) Network efficiency

The efficiency of two nodes i and j is expressed as the reciprocal of their distance $1/d_{ij}$. Therefore, the network efficiency is expressed as the average of the node efficiency in the communication layer.

$$E = \frac{1}{n(n-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \tag{7}$$

In addition, for different tasks and emphases of UAV swarms, an appropriate adjustment of the robustness topological metrics can be conducted.

However, for different network structures of UAV swarms, the variation of these metrics is different. In order to clearly characterize the dynamic process of the robustness evaluation, a sensitivity analysis is needed to set the weights for the topological metrics when determining a comprehensive robustness evaluation metric. In general, if a metric changed considerably with variations in the network, we assigned it a larger weight because it reflected the characteristic changes of the network very well. The sensitivity analysis approach is described below.

For UAV swarms consisting of n vehicles, remove the network nodes (communication layer or structure layer) and calculate the topological metrics s_k (k = 1,2,.., p) in succession. Then, each metric can get a set of metric changes Δs_{ki} (i = 1,2,. . ., n) and the average of metric changes$\overline{\Delta s_{ki}}$. The variance of the metric changes can be calculated as

$$S_k^2 = \frac{\sum_{i=1}^{n} \left(\Delta s_{ki} - \overline{\Delta s_{ki}}\right)^2}{n} \qquad k = 1, 2, ..., p \tag{8}$$

Then, the above process is repeated N times to obtain the mean of the variance of the metric changes, which can be expressed as

$$\overline{S_k^2} = \frac{1}{N} S_k^2 \qquad k = 1, 2, ..., p \tag{9}$$

The weight of each topological metric w_k in the comprehensive robustness metric can be determined according to $\overline{S_k^2}$.

$$w_k = \frac{\overline{S_k^2}}{\sum_{k=1}^{p} \overline{S_k^2}} \qquad k = 1, 2, ..., p \tag{10}$$

Finally, the comprehensive robustness metric of the UAV swarming network can be obtained by using the normalization method.[41]

$$R = \sum_{k=1}^{p} w_k \frac{s_k - \min(s_k)}{\max(s_k) - \min(s_k)} \tag{11}$$

where R represents the robustness of the UAV swarming network and $R \in [0,1]$. The higher numbers indicate better robustness.

3.2. Establishing robustness evaluation strategies

Node removal is an important part of a robustness evaluation, and a robustness evaluation strategy is a method of removing nodes. Therefore, the selection of different strategies may have a considerable effect on the evaluation results of the UAV swarming system. At present, there are mainly two types of attacks: random attack and targeted attack.[49] Random attacks can be divided into the random removal of nodes and the random removal of edges. Targeted attacks can be divided into node degree-based attacks and clustering coefficient-based attacks.[50] In general, the evaluation strategy should be selected to be consistent with the actual mission scenarios and functional characteristics of the system.[51]

A UAV swarming system may encounter random attacks and fixed-point attacks from the enemy when performing missions. Therefore, both random attacks and targeted attacks should be considered when analyzing this system's robustness. Most attacks are shots of a single UAV, which can be expressed as the removal of nodes. In a fixed-point attack, the enemy usually attacks the leader UAV, which connects to more UAVs first, that is, a node degree-based attack.

Therefore, based on the structural and functional characteristics of the UAV swarming network, the robustness evaluation strategies selected in this study can be described in detail as follows.

(1) Random attacks

Imitating the mission scenario of UAV swarms, random attacks can be manifested in two ways. (A) Simulate a physical attack. The node $V_{\mathrm{b}i}$ in the structure layer is randomly removed, and the connected nodes in the communication layer $V_{\mathrm{a}i}$ and the mission layer $V_{\mathrm{c}i}$ are also removed. (B) Simulate a wireless network attack. The node $V_{\mathrm{a}i}$ in the communication layer is randomly removed, and the connected nodes in the mission layer $V_{\mathrm{c}i}$ are also removed.

(2) Targeted attacks

In an imitation of the fixed-point attacks of UAV swarms, the nodes with the largest node degree are removed first. Then, the nodes in the UAV swarming network are removed from large to small. Moreover, there are two ways of removing nodes in the structure layer and the communication layer. The specific removal method is similar to a random attack.

3.3. Robustness evaluation algorithm considering dynamic reconfiguration

As mentioned above, UAV swarms need dynamic reconfiguration to improve their flexibility and robustness. In this section, we will evaluate the robustness and the changes in the network topology when the UAV swarms are attacked considering dynamic reconfiguration. According to the analysis of the robustness evaluation strategies, random attacks and targeted attacks will be adopted in the structure layer and the communication layer. The comprehensive robustness metric proposed in Section 3.1 was used to evaluate the robustness of the UAV swarming system. The process is shown in Fig. 6.

In this process, two evaluation strategies, random attacks and targeted attacks, do not occur at the same time. Moreover, the same attack is considered in the communication layer and in the structure layer of the UAV swarming network. Therefore, the specific algorithm can be described in Table 4.

3.4. Robustness evaluation algorithm considering information correlation

A robustness evaluation considering information correlation is aimed at analyzing the effect of a cascade failure in a communi-

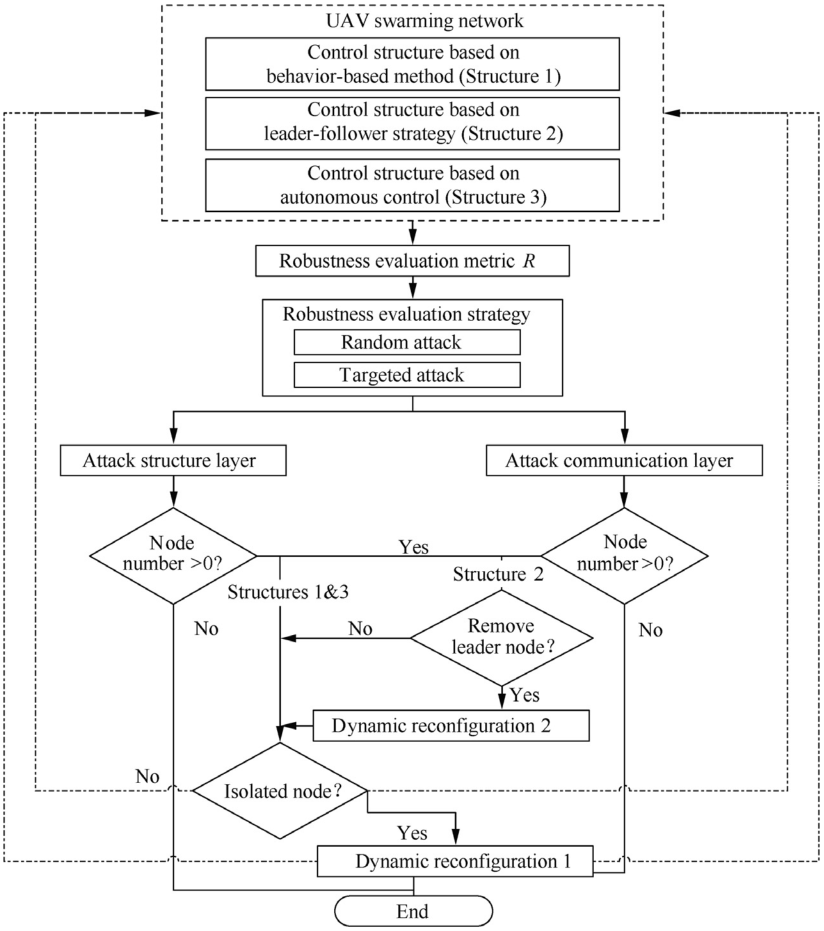

UAV swarming network
Control structure based on behavior-based method (Structure 1)
Control structure based on leader-follower strategy (Structure 2)
Control structure based on autonomous control (Structure 3)
Robustness evaluation metric R
Robustness evaluation strategy
Random attack
Targeted attack
Attack structure layer
Attack communication layer
Node number >0?
Yes
Node number >0?
Structures 1&3
Structure 2
No
No
Remove leader node?
No
Yes
Dynamic reconfiguration 2
No
Isolated node?
Yes
Dynamic reconfiguration 1
End

Fig. 6 Flowchart of robustness evaluation considering dynamic reconfiguration.

Table 4 Pseudo code of algorithm 3.

```
Robustness evaluation algorithm 1
Input: UAV swarming network $G_a$, $G_b$, $G_c$
Output: set of robustness evaluation metrics
while node number > 0 do
  ▷ node removal in communication layer $G_a$
    randomly or targeted choose nodes $V_{ai}$ from $G_a$
    delete $V_{ai}$ from $G_a$
    delete $V_{ci}$ from $G_c$
  ▷ node removal in structure layer $G_b$
    randomly or targeted choose nodes $V_{bi}$ from $G_b$
    delete $V_{ai}$ from $G_a$
    delete $V_{bi}$ from $G_b$
    delete $V_{ci}$ from $G_c$
    go to Algorithm 1 or 2
    calculate the comprehensive robustness metric $R$
end while
return $R$
```

cation network of UAV swarms caused by the network virus propagation. As in Section 3.3, we chose a random attack and a targeted attack as the robustness evaluation strategies. The comprehensive robustness metric R was used to evaluate the robustness of the UAV swarms. The specific process is shown in Fig. 7.

This is a time-dependent process, so the evaluation strategy is only reflected in the initial selection of the infected nodes. We assume that each node in the communication layer is in the susceptible state. When $t = 0$, m infected nodes appear. We set S as the set of nodes in the susceptible state and I as the set of nodes in the infected state. Based on the information correlation process modeled in Section 2.2, the specific algorithm can be described in Table 5.

4. Case study

In Sections 2 and 3, we modeled two dynamic evolution processes, namely dynamic reconfiguration and information correlation, of UAV swarms and proposed the corresponding robustness evaluation algorithms. In this section, the validity of the methods is verified by using a case study. We also analyzed the effects on the robustness of UAV swarms under different structures, evaluation strategies, and attack targets. The case description is as follows[32]:

(1) The UAV swarming system consists of 55 vehicles. Every 11 vehicles carry a specific type of payload to execute a certain mission.
(2) For Structure 1, the control structure is set to be a classic pigeon flock with one "leader".

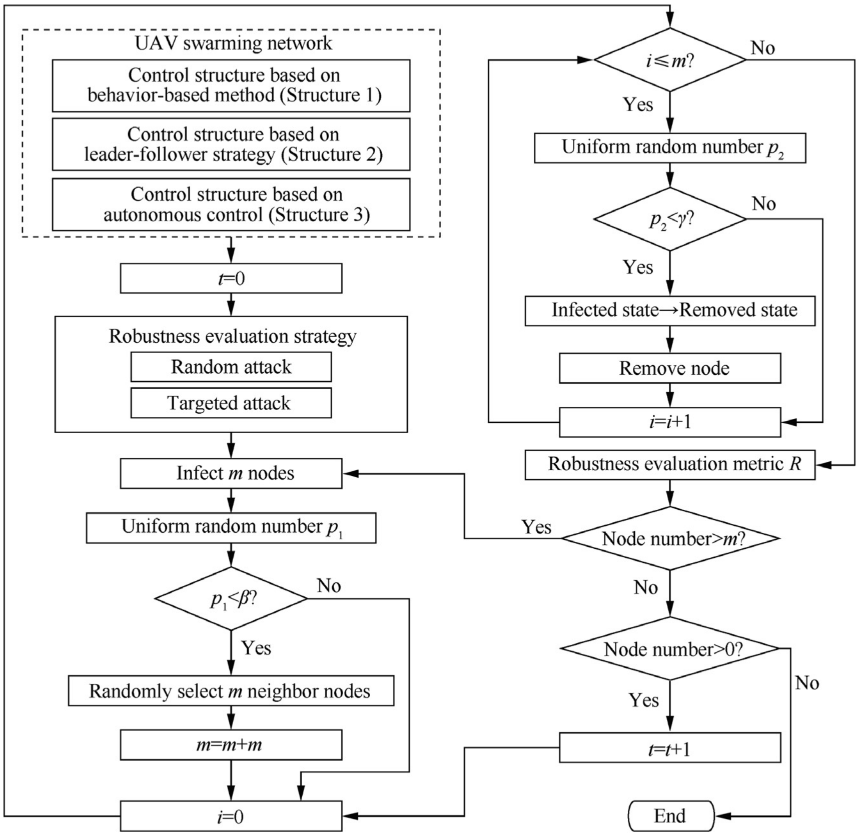

UAV swarming network
Control structure based on behavior-based method (Structure 1)
Control structure based on leader-follower strategy (Structure 2)
Control structure based on autonomous control (Structure 3)
t=0
Robustness evaluation strategy
Random attack
Targeted attack
Infect m nodes
Uniform random number p_1
$p_1<\beta$?
No
Yes
Randomly select m neighbor nodes
m=m+m
i=0
$i\leq m$?
No
Yes
Uniform random number p_2
$p_2<\gamma$?
No
Yes
Infected state→Removed state
Remove node
i=i+1
Robustness evaluation metric R
Yes
Node number>m?
No
Node number>0?
No
Yes
t=t+1
End

Fig. 7 Flowchart of robustness evaluation considering information correlation.

(3) For Structure 2, there are five leaders, and each one has 10 followers.
(4) For Structure 3, let each vehicle be connected with four to five adjacent ones with a random topology.

Python Network X was utilized to program the modeling algorithm to visualize the network structures and further the robustness evaluation. The visualization complex network model of the three structures is shown in Fig. 8.[32] The nodes of the communication layer, the structure layer, and the mission layer in these complex networks are expressed as blue, red, and yellow dots, respectively. The black lines in the figure represent the edges.

4.1. Robustness evaluation considering dynamic reconfiguration

According to the robustness evaluation algorithm of UAV swarming systems considering dynamic reconfiguration, we evaluated the robustness of the aforementioned three networks. Random attacks and targeted attacks were chosen to attack the structure layer and the communication layer of these networks.

Three robustness topological metrics, namely average node degree k, clustering coefficient C, and network efficiency E, were selected to compose the comprehensive robustness evaluation metric of this case. As mentioned in Section 3.1, we conducted 50 sensitivity analyses for each situation of the three networks. Then, the weights w_1, w_2, and w_3 of each robustness topological metric were determined, and $w_1 + w_2 + w_3 = 1$. The comprehensive robustness metric R was simulated and obtained.

$$R = w_1\frac{k-\min(k)}{\max(k)-\min(k)} + w_2\frac{C-\min(C)}{\max(C)-\min(C)} + w_3\frac{E-\min(E)}{\max(E)-\min(E)} \tag{12}$$

Assume that the failure threshold of system robustness was $R = 0.6$, and thus the robustness for 1 simulation of the three networks under random attacks is shown in Fig. 9. Fig. 10 shows the system robustness under targeted attacks.

To decrease chanciness and randomness, we simulated the aforementioned process 30 times. Then, the robustness of the three networks considering dynamic reconfiguration was obtained as shown in Table 6. The number in the table represents the percentage of network losing nodes when the system robustness reached the failure threshold to the total number of nodes.

The network structure design is very important for the robustness and performance of the UAV swarms. From this case, we can find that under the same attack strategy and dynamic evolution process, the robustness evaluation result is strong related to the structure of the UAV swarming network. Based on the formation design and control strategy, we can transform the UAV swarms into a complex network model. Then the system robustness of the UAV swarms can be evaluated according to the method that we proposed, so that the optimization of the formation design can be carried out to improve the robustness and performance.

Table 5 Pseudo code of algorithm 4.

Robustness evaluation algorithm 2

Input: (A) UAV swarming network G_a, G_b, G_c; (B) Infection rate β ; (C) Removal rate γ

Initialization: $S[x]$, $I[z]$, $t = 0$

Output: set of robustness evaluation metrics

```
for $p = 1$ to $m$ do
  randomly or targeted choose nodes $V_{ai}$ from $G_a$
      add $V_{ai}$ to $I[z]$; $z = z + 1$
      delete $V_{ai}$ from $S[x]$
end for
while $S[x]$ or $I[z]$ not empty do
    for $i = 1$ to $z$ do
      generate random number $r$
      if $r < \beta$ then
         randomly choose nodes $V_{aj}$ from $S[x]$
         add $V_{aj}$ to $I[z]$; $z = z + 1$
         delete $V_{aj}$ from $S[x]$
       end if
    end for
      for each node $V_{ak}$ in $I[z]$ do
      generate random number $r$
      if $r < \gamma$ then
         delete $V_{ak}$ from $G_a$, $I[z]$; $z = z - 1$
         delete $V_{ck}$ from $G_c$
    end if
  end for
  calculate the comprehensive robustness metric $R$
  $t = t + 1$
end while
return $R$
```

It can be seen that the robustness of Structure 3 is better than that of the other two structures under a random attack, but the opposite is true under a targeted attack. The system robustness under a targeted attack is better than that under a random attack. The robustness of attacking the communication layer is close to that of the structure layer, but the former is relatively better.

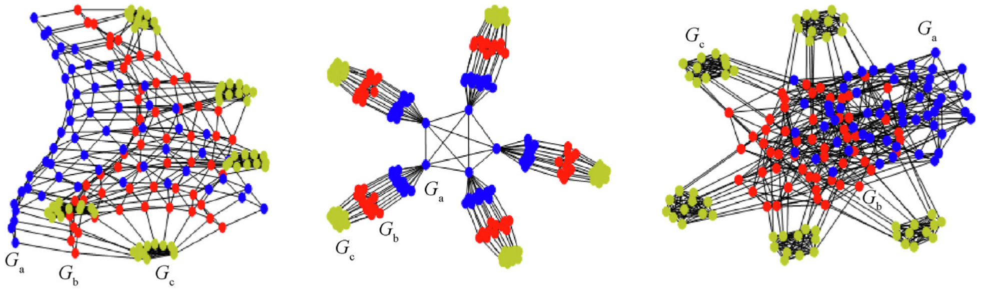
To demonstrate the effect of dynamic reconfiguration on system robustness, we evaluated network robustness without considering it in the comparison. The evaluation strategies, attack targets, and metric selection were the same as before. The weight of each robustness topological metric was determined by using a sensitivity analysis to calculate the comprehensive robustness metric. After 30 simulations, the corresponding network robustness was as shown in Table 7.

In comparison, the robustness of UAV swarms considering dynamic reconfiguration was better in any situation. This conclusion showed that dynamic reconfiguration improved the robustness of the UAV swarming systems to a certain extent during mission execution.

4.2. Robustness evaluation considering information correlation

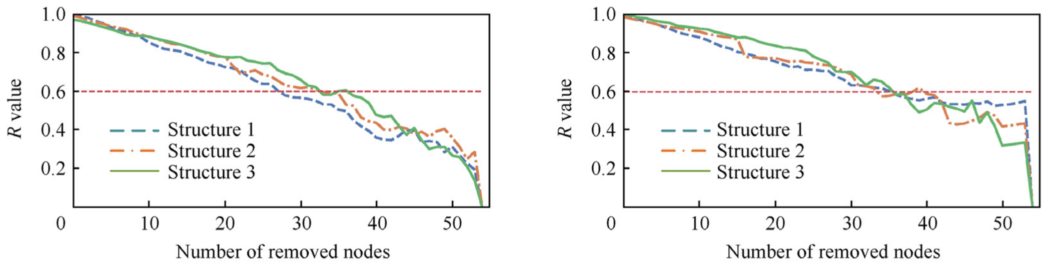
According to the robustness evaluation algorithm of UAV swarms considering information correlation, we evaluated the robustness of these three networks. Random attacks and targeted attacks were chosen to attack the communication layer of these networks.

We set all the nodes of UAV swarming network in the susceptible state, and m infected nodes were found when $t = 0$. Furthermore, we set the infection rate to $\beta = 0.6$ and the removal rate to $\gamma = 0.01$. Similarly, three robustness topological metrics, namely average node degree k, clustering coefficient C, and network efficiency E, were chosen to compose the comprehensive robustness evaluation metric. We conducted 50 sensitivity analyses for each situation of the three networks to determine the weights of each metric. Then, the



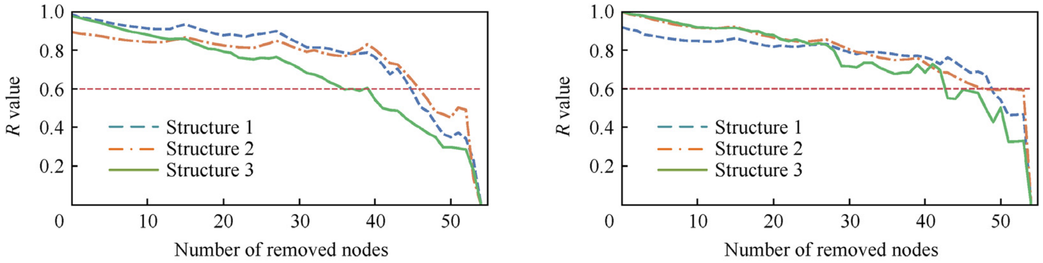
(a) Structure 1 (a) Structure 2 (c) Structure 3

Fig. 8 Complex network model of UAV swarms.[32]



(a) Attack in structure layer (b) Attack in communication layer

Fig. 9 System robustness under random attack.



(a) Attack in structure layer

(b) Attack in communication layer

Fig. 10 System robustness under targeted attack.

Table 6 Robustness evaluation results of 30 simulations.

Strategy	Robustness evaluation results			
	Attack target	Structure 1	Structure 2	Structure 3
Random attack	Structure layer	0.586	0.541	0.601
	Communication layer	0.645	0.575	0.676
Targeted attack	Structure layer	0.818	0.856	0.745
	Communication layer	0.949	0.893	0.916

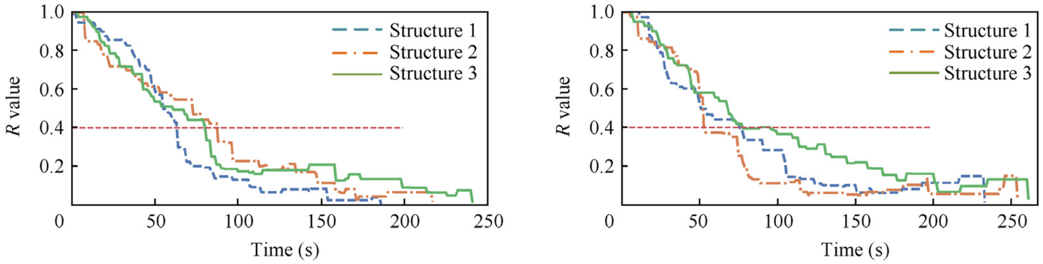
Table 7 Robustness evaluation results without considering dynamic reconfiguration.

Strategy	Robustness evaluation results			
	Attack target	Structure 1	Structure 2	Structure 3
Random attack	Structure layer	0.475	0.465	0.565
	Communication layer	0.594	0.565	0.623
Targeted attack	Structure layer	0.818	0.836	0.709
	Communication layer	0.891	0.873	0.824

comprehensive robustness metric R was simulated and obtained.

We let the failure threshold of the communication network robustness be $R = 0.4$; the robustness of the three networks under a random attack is shown in Fig. 11(a) and that under a targeted attack in Fig. 11(b).

Similarly, we simulated the aforementioned process 30 times. The robustness of three networks considering information correlation was obtained as shown in Table 8. The number in the table represents the percentage of the current time when the system robustness reached the failure threshold to the total time when the communication network was destroyed.



(a) System robustness under random attack

(b) System robustness under targeted attack

Fig. 11 System robustness considering information correlation.

Table 8 Robustness evaluation results of 30 simulations considering information correlation.

Strategy	Robustness evaluation results			
	Attack target	Structure 1	Structure 2	Structure 3
Random attack	Communication layer	0.265	0.233	0.275
Targeted attack	Communication layer	0.247	0.238	0.290

It can be seen from the figures and the table that the communication network crashed more slowly under a targeted attack than under a random attack. That is, the UAV swarms persisted longer under the influence of virus propagation. The robustness of these three UAV swarming networks was not considerably different, but the robustness of Structure 3 was relatively better.

4.3. Discussion

Firstly, the complexity of the robustness evaluation algorithms proposed in this paper will not increase exponentially with the increase of the number of UAVs. They have fixed polynomial time and do not have the problem of space explosion. Therefore, the methods have strong stability. Besides, the iteration number of the algorithms are related to the number of UAVs, and there is no endless loop. The value range obtained is in (0,1) and terminated with 0, so the algorithm is convergent.

Secondly, from the above case study and analysis, we found that the comprehensive robustness metric proposed in this paper decreased monotonously with the removal of nodes. This conformed to the general law of a robustness analysis. It also reflected the effect of node reduction on the structure and the function of UAV swarming networks, which showed their ability to maintain function and complete missions after being attacked. Besides, multiple robustness topological metrics were used in the comprehensive metric, whose weights were determined by a sensitivity analysis. This measured the system robustness more comprehensively and considered the changes in different network properties to be more pertinent.

Finally, according to the comparative analysis, the UAV swarms had higher system robustness when considering dynamic reconfiguration than that when considering non-reconfiguration. Moreover, the robustness evaluation considering information correlation could simulate the effect of a cascade failure caused by virus propagation. The methods and results were in accord with the actual mission scenarios and characteristics of the UAV swarms. Therefore, it was proved that the proposed method was correct and valid.

5. Conclusions and future work

Considering the increasing requirements for the robustness and reliability of UAV swarms, a robustness evaluation method based on their mission scenario was proposed on the basis of our previous study on the modeling framework of a UAV swarming system. To achieve this, we first built the complex network models for three typical UAV swarm structures and then analyzed the dynamic evolution that appeared in the application scenarios. Moreover, the dynamic evolution models considering dynamic reconfiguration and information correlation were established on the basis of the complex network theory. Then, according to the structural characteristics and the attack forms of the UAV swarms, we presented the comprehensive robustness metric and the evaluation strategies including a random attack and a targeted attack. Finally, the robustness evaluation methods and algorithms for UAV swarms considering the two dynamic evolution processes were proposed.

To verify the correctness and validity of the proposed method, a case study was conducted for the analysis and comparison. The results confirmed that the proposed method effectively simulated the structural changes of UAV swarms in a changeable mission environment. The comprehensive metric had the ability to measure the structure robustness of a UAV swarming network. The robustness evaluation results can be further used for system design, path planning, mission decision making, and other management work of UAV swarms.

There are many challenges to be addressed in our future work: (A) Many assumptions and structural limitations were considered to simplify the model. More flexible models can be studied in the future. (B) In future research, transfer speed, transmission range, and other factors can be considered under information correlation for the robustness evaluation. (C) From the perspective of reinforcement, the influence of the network growth on the UAV swarms' robustness can be studied.

Acknowledgements

This study was co-supported by the National Natural Science Foundation of China (No. 51805016) and Field Foundation of China (No. JZX7Y20190242012001).

References

1. Wei Y, Brian BM, Madey GR. An operation-time simulation framework for UAV swarm configuration and mission planning. *13th Annual International Conference on Computational Science*; 2013 Jun 5–7; Barcelona, Spain; 2013. p. 1949–58.
2. Brust MR, Zurad M, Hentges L, Gomes L, Danoy G, Bouvry P. Target tracking optimization of UAV swarms based on dualpheromone clustering. *3rd IEEE International Conference on Cybernetics*; 2017 Jun 21-23; Exeter, England. Piscataway: IEEE Press; 2017. p. 1–8.
3. Xi JX, Wang C, Liu H, Wang Z. Dynamic output feedback guaranteed-cost synchronization for multiagent networks with given cost budgets. *IEEE Access* 2018;**6**:28923–35.
4. Xi JX, Wang C, Liu H, Wang L. Completely distributed guaranteed-performance consensualization for high-order multiagent systems with switching topologies. IEEE Trans Syst Man, Cybern Syst 2019, 49(7):1–11.
5. Sampedro C, Bavle H, Sanchez-Lopez JL, Fernandez-Ramon AS, Rodriguez-Ramos A, Molina M, et al. A flexible and dynamic mission planning architecture for UAV swarm coordination. *International conference on unmanned aircraft systems*; 2016 Jun 7-10; Arlington, VA. Piscataway: IEEE Press; 2016. p. 355–63.
6. Liu J, Yu Y, Sun J, Sun CY. Distributed event-triggered fixed-time consensus for leader-follower multiagent systems with nonlinear dynamics and uncertain disturbances. *Int J Robust Nonlinear Control* 2018;**28**(11):3543–59.
7. Liu J, Yu Y, Wang Q, Sun CY. Fixed-time event-triggered consensus control for multi-agent systems with nonlinear uncertainties. *Neurocomputing* 2017;**260**:497–504.
8. Rosalie M, Danoy G, Chaumette S, Bouvry P. Chaos-enhanced mobility models for multilevel swarms of UAVs. *Swarm Evol Comput* 2018;**41**:36–48.
9. Xiong CK, Chen DF, Lu D, Zeng Z, Lian L. Path planning of multiple autonomous marine vehicles for adaptive sampling using Voronoi-based ant colony optimization. *Rob Auton Syst* 2019;**115**:90–103.
10. Wu HS, Li H, Xiao RB, Liu J. Modeling and simulation of dynamic ant colony's labor division for task allocation of UAV swarm. *Phys A Stat Mech Its Appl* 2018;**491**:127–41.
11. Yuan ZH, Jin J, Sun LL, Chin KW, Muntean GM. Ultra-reliable IoT communications with UAVs: A swarm use case. *IEEE Commun Mag* 2018;**56**(12):90–6.

12. Madni AM, Sievers MW, Humann J, Ordoukhanian E, Boehm B, Lucero S. Formal methods in resilient systems design: Application to multi-UAV system-of-systems control. *Discip Converg Syst Eng Res* 2017;**15**(3–4):407–18.
13. Hocraffer A, Nam CS. A meta-analysis of human-system interfaces in unmanned aerial vehicle (UAV) swarm management. *Appl Ergon* 2017;**58**:66–80.
14. Liu JJ, Wang WP, Li XB, Wang T, Wang TQ. A motif-based mission planning method for UAV swarms considering dynamic reconfguration. *Def Sci J* 2018;**68**(2):159–66.
15. Weng LG, Liu QS, Xia M, Song YD. Immune network-based swarm intelligence and its application to unmanned aerial vehicle (UAV) swarm coordination. *Neurocomputing* 2014;**125**:134–41.
16. Bjerga T, Aven T, Zio E. Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliab Eng Syst Saf* 2016;**156**:203–9.
17. Liu P, Yang LX, Gao ZY, Li SK, Gao Y. Fault tree analysis combined with quantitative analysis for high-speed railway accidents. *Saf Sci* 2015;**79**:344–57.
18. Niu R, Cao Y, Ge XC, Tang T. Applying system thinking to learn from accident of modern automatic control systems. *Chinese J Electron* 2014;**23**(2):409–14.
19. Fan DD, Theodorou EA, Reeder J. Model-based stochastic search for large scale optimization of multi-agent UAV Swarms. *8th IEEE symposium series on computational intelligence*; 2018 Nov 18-21; Bengaluru, India. Piscataway: IEEE Press; 2019. p. 2216–22.
20. Kho J, Tran-Thanh L, Rogers A, Jennings NR. An agent-based distributed coordination mechanism for wireless visual sensor nodes using dynamic programming. *Comput J* 2010;**53**(8):1277–90.
21. Wang JB, Wang XH, Wang LZ. Modeling of BN lifetime prediction of a system based on integrated multi-level information. *Sensors* 2017;**17**(9):1–20.
22. Ren Y, Fan DM, Ma XR, Wang ZL, Feng Q, Yang DZ. A GO-FLOW and dynamic Bayesian network combination approach for reliability evaluation with uncertainty: A case study on a nuclear power plant. *IEEE Access* 2017;**6**:7177–89.
23. Elsawah S, Pierce SA, Hamilton SH, Van DH, Haase D, Elmahdi A. An overview of the system dynamics process for integrated modelling of socio-ecological systems: Lessons on good modelling practice from five case studies. *Environ Model Softw* 2017;**93**:127–45.
24. Wang R, Zheng W, Liang C, Tang T. An integrated hazard identification method based on the hierarchical Colored Petri Net. *Saf Sci* 2016;**88**:166–79.
25. Zhu QH, Zhou MC, Qiao Y, Wu NQ. Petri net modeling and scheduling of a close-down process for time-constrained single-arm cluster tools. *IEEE Trans Syst Man, Cybern Syst* 2018;**48**(3):389–400.
26. Fan WL, Liu ZG, Hu P, Mei SW. Cascading failure model in power grids using the complex network theory. *IET Gener Transm Distrib* 2016;**10**(15):3940–9.
27. Mureddu M, Facchini A, Scala A, Caldarelli G, Damiano A. A complex network approach for the estimation of the energy demand of electric mobility. *Sci Rep* 2018;**8**(1):1–8.
28. Cuadra L, Salcedo-Sanz S, Del SJ, Jiménez-Fernández S, Geem ZW. A critical review of robustness in power grids using complex networks concepts. *Energies* 2015;**8**(9):9211–65.
29. Fichera A, Frasca M, Volpe R. Complex networks for the integration of distributed energy systems in urban areas. *Appl Energy* 2017;**193**:336–45.
30. Aldrich PR, El-Zabet J, Hassan S, Briguglio J, Aliaj E, Radcliffe M. Monte Carlo tests of small-world architecture for coarse-grained networks of the United States railroad and highway transportation systems. *Phys A Stat Mech Its Appl* 2015;**438**:32–9.
31. Xu ZW, Sui DZ. Small-world characteristics on transportation networks: A perspective from network autocorrelation. *J Geogr Syst* 2007;**9**(2):189–205.
32. Wang LZ, Lu DW, Zhang Y, Wang XH. A complex network theory-based modeling framework for unmanned aerial vehicle swarms. *Sensors* 2018;**18**(10):1–24.
33. Caschili S, Medda FR, Wilson A. An interdependent multi-layer model: Resilience of international networks. *Networks Spat Econ* 2015;**15**(2):313–35.
34. Manzano M, Calle E, Torres-Padrosa V, Segovia J, Harle D. Endurance: A new robustness measure for complex networks under multiple failure scenarios. *Comput Networks* 2013;**57**(17):3641–53.
35. Bilal K, Manzano M, Erbad A, Calle E, Khan SU. Robustness quantification of hierarchical complex networks under targeted failures. *Comput Electr Eng* 2018;**72**:112–24.
36. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. *Nature* 2010;**464**(7291):1025–8.
37. Thacker S, Pant R, Hall JW. System-of-systems formulation and disruption analysis for multi-scale critical national infrastructures. *Reliab Eng Syst Saf* 2017;**167**:30–41.
38. Šimon M, Dirgová LI, Huraj L, Hosťovecký M, Pospíchal J. Combined heuristic attack strategy on complex networks. *Math Probl Eng* 2017;**2017**:1–9.
39. Wang ZY, Hill DJ, Chen G, Dong ZY. Power system cascading risk assessment based on complex network theory. *Phys A Stat Mech Its Appl* 2017;**482**:532–43.
40. Zhou YM, Wang JW. Efficiency of complex networks under failures and attacks: A percolation approach. *Phys A Stat Mech Its Appl* 2018;**512**:658–64.
41. Solé RV, Rosas-Casals M, Corominas-Murtra B, Valverde S. Robustness of the European power grids under intentional attack. *Phys Rev E - Stat Nonlinear, Soft Matter Phys* 2008;**77**(2):1–7.
42. Beard R, Rabbath AC. Networked UAVs and UAV Swarms. In: Valavanis KP, Vachtsevanos GJ, editors. *Handbook of Unmanned Aerial Vehicles*. The Netherlands: Springer; 2015. p. 1983–2019.
43. Nagy M, Vasarhelyi G, Pettit B, Roberts-Mariani I, Vicsek T, Biro D. Context-dependent hierarchies in pigeons. *Proc Natl Acad Sci* 2013;**110**(32):13049–54.
44. Dehghani MA, Menhaj MB. Communication free leader-follower formation control of unmanned aircraft systems. *Rob Auton Syst* 2016;**80**:69–75.
45. Xu J, Wickramarathne TL, Chawla NV. Representing higher-order dependencies in networks. *Sci Adv* 2016;**2**(5):1–11.
46. Yanmaz E, Yahyanejad S, Rinner B, Hellwagner H, Bettstetter C. Drone networks: Communications, coordination, and sensing. *Ad Hoc Netw* 2018;**68**:1–15.
47. Shi HJ, Duan ZS, Chen GR. An SIS model with infective medium on complex networks. *Phys A Stat Mech Its Appl* 2008;**387**(8–9):2133–44.
48. Wang YH, Bi LF, Lin S, Li M, Shi H. A complex network-based importance measure for mechatronics systems. *Phys A Stat Mech Its Appl* 2017;**466**:180–98.
49. Dong GG, Gao JX, Du RJ, Tian LX, Stanley HE, Havlin S. Robustness of network of networks under targeted attack. *Phys Rev E – Stat Nonlinear, Soft Matter Phys* 2013;**87**(5):1–11.
50. Zhang WP, Xia YX, Ouyang B, Jiang LR. Effect of network size on robustness of interconnected networks under targeted attack. *Phys A Stat Mech Its Appl* 2015;**435**:80–8.
51. Wang JW, Rong LL. Robustness of the western United States power grid under edge attack strategies due to cascading failures. *Saf Sci* 2011;**49**(6):807–12.