Journal of Systems Engineering and Electronics
Vol. 33, No. 3, June 2022, pp.759 – 770

Failure analysis of unmanned autonomous swarm considering cascading effects

XU Bei[1,2], BAI Guanghan[1], ZHANG Yun'an[1], FANG Yining[1], and TAO Junyong[1,*]

1. Laboratory of Science and Technology on Integrated Logistics Support, College of Intelligent Sciences and Technology, National University of Defense Technology, Changsha 410073, China; 2. School of General Aviation, Nanchang Hangkong University, Nanchang 330063, China

Abstract: In this paper, we focus on the failure analysis of unmanned autonomous swarm (UAS) considering cascading effects. A framework of failure analysis for UAS is proposed. Guided by the framework, the failure analysis of UAS with crash fault agents is performed. Resilience is used to analyze the processes of cascading failure and self-repair of UAS. Through simulation studies, we reveal the pivotal relationship between resilience, the swarm size, and the percentage of failed agents. The simulation results show that the swarm size does not affect the cascading failure process but has much influence on the process of self-repair and the final performance of the swarm. The results also reveal a tipping point exists in the swarm. Meanwhile, we get a counter-intuitive result that larger-scale UAS loses more resilience in the case of a small percentage of failed individuals, suggesting that the increasing swarm size does not necessarily lead to high resilience. It is also found that the temporal degree failure strategy performs much more harmfully to the resilience of swarm systems than the random failure. Our work can provide new insights into the mechanisms of swarm collapse, help build more robust UAS, and develop more efficient failure or protection strategies.

Keywords: unmanned autonomous swarm (UAS), failures analysis, cascading failure, resilience.

DOI: 10.23919/JSEE.2022.000069

1. Introduction

Swarm intelligence is a well-studied phenomenon in bees, flocks of birds, schools of fish, etc. Physicists, biologists, and engineers proposed many multi-agent models to present the collective behaviors of these natural swarms [1–6] and revealed that emergence in the swarm can be achieved by individual with very limited abilities. This decentralized approach of nature has inspired the engineering systems to improve with a paradigm shift from a centralized control mechanism to a distributed control mechanism.

Distributed unmanned autonomous swarm (UAS), such as swarm robots [7,8] and unmanned aerial vehicle (UAV) swarm [9], is a scientific and engineering field that deals with the design of collec-tive behaviors for a swarm of relatively incapable individuals to perform complex tasks. This non-centralized control mechanism has gained many potential advantages over a single UAV or robots, including increased speed of task completion through parallelism, improved solutions for tasks, cheaper solutions for complex applications, and often claimed to be scalable, flexible, and highly fault-tolerant [8]. Thus, many studies on UAS have limited their research under safe laboratory settings, where the failure analysis of UAS is rarely considered in the presence of potential threats such as failures caused by internal and/or external factors. However, we find one or more failed agents may suffice to make the swarm collapse in a cascading process and prevent the team from achieving its goal. With many different UASs developed in real-world applications, either in military or non-military scenarios, special attention should be paid to the associated failure problem.

The potential threats of UAS can be divided into self-platform failures and external attacks according to the causes of failures. The self-platform failures are caused by internal reasons, while external attacks are conducted by adversaries or hostile environments. However, few studies have carried out further studies on how much these failures can influence the behaviors of swarm systems. Meanwhile, the UAS as the self-organization system has a certain ability to self-repair. Up to now, the mechanism of failure propagation and self-repair in UAS is not yet to be made clear.

Manuscript received December 04, 2020.

*Corresponding author.

This work was supported by the Science and Technology on Reliability & Environmental Engineering Laboratory (6142004004-2), and the Science Technology Commission of the CMC (2019-JCJQ-JJ-180, ZZKY-YX-10-3).

In this paper, we focus on the failure analysis of UAS to investigate the mechanism of failure propagation and self-repair. Traditionally, reliability is used to evaluate the ability of a system to maintain its normal operation under specific periods and circumstances. However, UAS is a typical distributed system with self-organization and self-repair capabilities. Thus, it is not suitable to use traditional reliability standards. Resilience provides a new approach that system administrators can use in the design and analysis of engineering systems to enhance the ability of such systems to withstand uncertain threats and bounce back from disruption events [9,10]. Since the concept of resilience was first proposed by Holling [11], it has been developed and applied in many fields, including economics, complex engineering, and social science [12,13]. There are three main perspectives of resilience, namely absorption, adaption, and restoration [14 –16]. Thus, compared with the static reliability evaluation, resilience is more appropriate to measure the fluctuation performance analysis of UAS.

Resilience in artificial swarms can be understood as the ability of individuals to repeatedly organize in response to disruptions so that the swarm can maintain or restore to an acceptable level of performance [17]. Many different assessment approaches were proposed to quantitatively assess the resilience of different complex systems [14]. The resilience triangle model proposed by Bruneau et al. [15] is used to measure the resilience loss (RL) of a community to an earthquake, which has been extended to many systems [18,19]. Smaller RL values indicate higher resilience while larger RL values imply lower resilience. However, most of the general resilience measures are regardless of the structure of the system, while the network structure and the resilience of artificial swarm evolve with both space and time. Zhang et al. [20] defined a resilience metric, namely the spatiotemporal congestion cluster to evaluate the resilience of the transportation system, in which the evolution of network structure was taken into consideration. Accordingly, the artificial swarm needs a new resilience metric to reflect the spatiotemporal propagation of failures and the adaptive recovery process.

In this paper, we study the emergent behavior of the systems and reveal the mechanism of failure propagation and self-repair of UAS. The main contributions of our study are summarized as follows:

(i) A framework for failure analysis of UAS is proposed.

(ii) A multi-agent swarm model and the failure model are developed.

(iii) Resilience is used to analyze the processes of cascading failure and self-repair of UAS.

(iv) The mechanism of failure propagation and self-repair in the proposed swarm is investigated.

The remainder of the study is organized as follows: Section 2 introduces the proposed framework for failure analysis for UAS. The multi-agent swarm model is given in Section 3. Section 4 conducts the failure mode and effects analysis (FMEA) for UAS. The failure model including the failure behavior model and failure strategies are developed in Section 5. Section 6 proposes the resilience evaluation metric and measurement. Section 7 provides the simulation studies and discussion. Section 8 concludes this study.

2. Framework for failure analysis of UAS

In order to understand the effect of possible threats on UAS, it is necessary to introduce the definition of UAS. The UAS in this paper refers to those multi-agent systems with a relatively incapable single agent designed such as a desired collective behavior emerging from the local interactions among agents and between the agents and the environment, taking significant inspiration from nature [21]. The main characteristics of UAS are the following [21,22]:

(i) Autonomous agents;

(ii) A large number of agents;

(iii) Few homogenous groups of agents;

(iv) Local sensing and communication capabilities.

In this paper, a framework for failure analysis for UAS is given in Fig. 1. The framework is designed to be applied to examine how much the different failure modes influence the emergent behavior of UAS. It consists of four stages: swarm model development stage, FMEA stage, failure model stage, and resilience evaluation method stage.

The first stage of this framework is to develop the swarm model. The swarm model is designed to exhibit the expected collective behavior. The collective behavior that emerges from swarm systems can be classified into four main categories: spatially-organizing behaviors, navigation behaviors, collective decision-making, and other collective behaviors [22]. These collective behaviors can be combined to tackle complex real-world applications, such as surveillance, tracking, construction, and so on. A typical swarm model consists of three parts: agents, interaction, and individual behavior rule. The agent is the component unit of the swarm systems, such as an UAV, a robot, or a missile. The interaction describes the interaction between agents, such as the topology of the communication network. The behavior rule denotes the behavior that individuals decide to take after receiving information, such as velocity matching, flock centering, or obstacle avoidance [1].

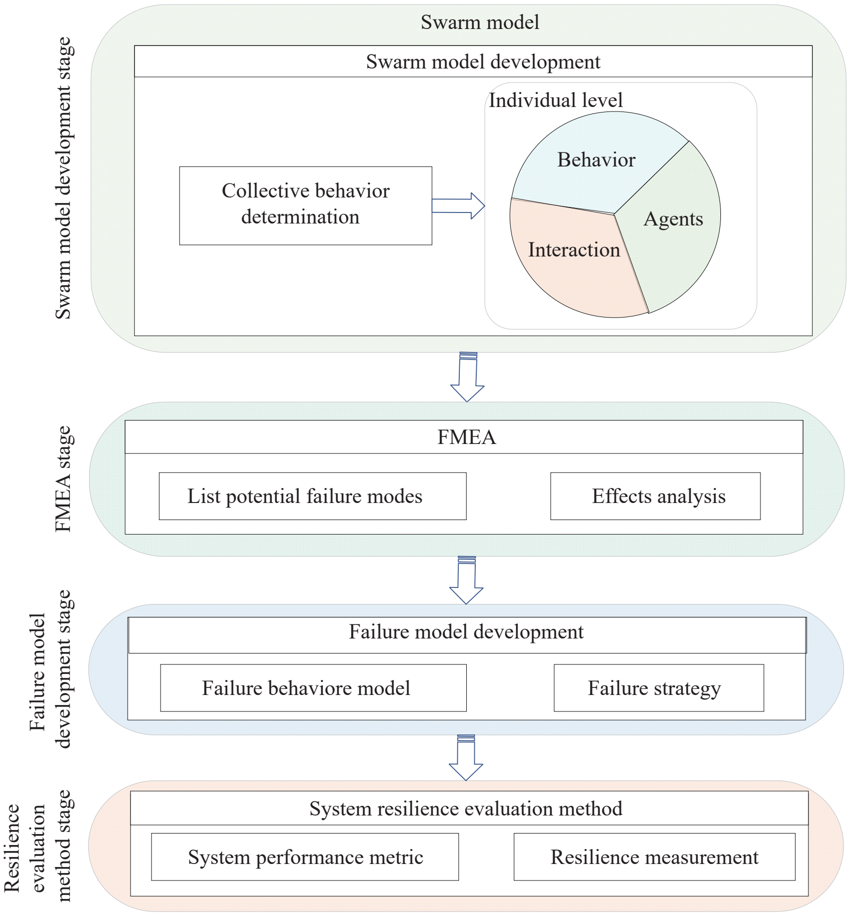

Swarm model development stage
Swarm model
Swarm model development
Collective behavior determination
Individual level
Behavior
Agents
Interaction
FMEA stage
FMEA
List potential failure modes
Effects analysis
Failure model development stage
Failure model development
Failure behaviore model
Failure strategy
Resilience evaluation method stage
System resilience evaluation method
System performance metric
Resilience measurement

Fig. 1 Framework of emergent behavior analysis for UAS under threats

The second stage is the FMEA stage. There are many reasons for the failure of UAS, including internal and external factors. The internal factors are issues within the self-platform design. Others are the external factors, mainly caused by malicious attacks or environmental effects. FMEA is a typical failure analysis technique for identifying, assessing, and eliminating potential failure modes in a wide range of industries [23]. It is used to analyze the failure mode of the single machine in UAS to find the critical failure modes. This stage lays the foundation for the subsequent failure model development stage.

The third stage is the failure model development stage, including the failure behavior model and failure strategies. The critical failure modes obtained from the FMEA stage have a great influence on collective behavior. The failure behavior model is built according to these critical failure modes, which defines the behavior of the failed agents. Then, simulate the behaviors of these failed agents in the simulation to observe the evolution of UAS. The failure strategies are designed to simulate the scope and location of the failed agents in UAS. An UAS is often regarded as a network by taking the agents as nodes and the interactions among them as links [9,24,25]. Thus, a network-based failure strategy is expected to help us to grasp the big picture of the whole system. Albert et al. [26] found the failure of highly connected nodes in a scale-free network can cause more significant damage to the topology than those less connected ones. After that, a series of studies about failure strategies on networks including static networks and temporal networks emerged [26–28]. The metrics to identify the significance of the nodes can be degree, closeness, betweenness, etc. [29].

The fourth stage is the system resilience evaluation method stage, including system performance metric construction and resilience measurement development. The emergent behavior of the swarm could be different before and after a part of agents failed. In this step, according to the expected collective behavior, the corresponding performance metrics are primarily developed to measure system performance. For instance, the order parameter which is represented by the average normalized velocity is proposed to measure the ordered direction of swarming [2]. With the failures of agents, the system performance could fluctuate before and after the failures. Resilience measurement should give a quantitative method to capture the fluctuation. In a word, this step demands system administrators construct system performance metrics based on the expected collective behavior and develop resilience measurements according to their concerned system's capabilities, such as absorption, adaption, or restoration.

3. Multi-agent swarm model

According to the first stage of the framework in Section 2, the swarm model is designed to exhibit the expected collective behavior. In this section, we build a swarm model for flocking which can be classified as having a navigation behavior among the four categories of group behavior. The expected swarm behavior in this swarm model is the cohesive and ordered motion of a group of individuals.

Consider a swarm of N agents moving about in a two-dimensional plane with constant speed v_0 at initial random directions. In each time step Δt, the individual determines its desired direction $\boldsymbol{d}_i(t+\Delta t)$ by assessing the direction and position of neighbors,

Each agent has three individual behaviors, namely avoidance, alignment, and attraction. Obstacle avoidance has the highest priority. They attempt to maintain personal space with a radius of r_0 to avoid collisions with other individuals,

$$\boldsymbol{d}_i(t+\Delta t) = -\sum_{\substack{j\in N_{i0}(t),\\ j\neq i}} \frac{\boldsymbol{x}_j(t)-\boldsymbol{x}_i(t)}{\left|\boldsymbol{x}_j(t)-\boldsymbol{x}_i(t)\right|} \tag{1}$$

where $\boldsymbol{x}_j(t)$ represents the position vector of individual j, and

$$N_{i0}(t) = \{j|\left|\boldsymbol{x}_i(t)-\boldsymbol{x}_j(t)\right| \leqslant r_0\}.$$

If there is no neighbor in this personal space, the individual will tend to become attracted towards and aligned with neighbors within a local interaction range r.

$$\boldsymbol{d}_i(t+\Delta t) = \sum_{j\in N_{ic}(t)} \frac{\boldsymbol{x}_j(t)-\boldsymbol{x}_i(t)}{\left|\boldsymbol{x}_j(t)-\boldsymbol{x}_i(t)\right|} + \sum_{j\in N_{ic}(t)\cup j=i} \frac{\boldsymbol{v}_j(t)}{\lceil \boldsymbol{v}_j(t)\rceil} \tag{2}$$

where $\boldsymbol{v}_j(t)$ is the direction vector of individual j, and

$$N_{ic}(t) = \left\{j|r_0 < \left|x_i(t)-x_j(t)\right| \leqslant r\right\}.$$

Finally, we convert $\boldsymbol{d}_i(t+\Delta t)$ to the unit vector

$$\widehat{\boldsymbol{d}}_i(t+\Delta t) = \boldsymbol{d}_i(t+\Delta t)/|\boldsymbol{d}_i(t+\Delta t)|.$$

4. FMEA

Winfield et al. [30] explored the fault tolerance of a wireless-connected robot swarm through FMEA. The FMEA hazard identified are motor failure, communications failure, avoidance sensor(s) failure, beacon sensor failure, control systems failure, and all systems failure. According to the proposed swarm model, internal and external disturbance acting on a single machine manifest the failure of the subsystems of UAS, namely communication subsystem, sensor subsystem, motor subsystem, control subsystem, etc. We identify the following failure modes, namely, F1, communications failure, F2, avoidance sensor failure, F3, motor subsystem failure, F4, control systems failure, and F5, all subsystems failure.

The effect of each failure mode in the proposed swarm model is similar to the results of [30]. The detailed description is given as follows:

(i) F1: communications failure

Failure of communication subsystem in an individual of UAS means no interaction with others. It becomes physically lost to the swarm. For the swarm, agents with communication failure are simply moving obstacles and have essentially little effect on the collective behaviors.

(ii) F2: avoidance sensor failure

The effect of the avoidance sensor failure on an individual is that the agent may collide with others or obstacles. However, the other agents in the UAS with normal avoidance sensors can avoid it. Thus, when the number of agents with F2 is small, the overall collective behaviors remain unaffected.

(iii) F3: motor subsystem failure

Failure of the motor subsystem in an individual, or a small number of agents means they're not moving. However, given that their communication subsystem and other subsystems continue to function, they are still connected to the swarm. They continue to affect collective behaviors. Swarm may be anchored by stationary agents with F3 which would either impend or at worst prevent the swarm from moving [30]. Thus, the F3 motor subsystem failure is a critical failure mode since one or a small number of agents with F3 could seriously damage our expected "cohesive and ordered motion of a group of individuals" behavior at the swarm level.

(iv) F4: control systems failure

Each agent has three individual behaviors, namely avoidance, alignment, and attraction. Failure of control systems in one or a small number of agents means the agent cannot behave correctly in response to the communications or sensors. The most likely consequence is that they get lost in the environment. In this case, the effect of F4 is transient and can be ignored. The worst case is that agents with F4 are stationary or turning on the spot [30], which has the same effect with F3 motor subsystem failure.

(v) F5: all systems failure

Failures of all systems are the simplest case in which the agents with F5 remain stationary and inactive. In this case, the failed agents are simply static obstacles for the swarm. Thus, although it is the most serious failure mode for a single machine, it is the least serious failure mode for the swarm.

To summarize the above, F3 motor failure causes more serious damage on our expected collective behaviors and it is the most critical failure mode.

5. Failure model

5.1 Failure behavior model

According to the FMEA of Section 4, the failure mode, F3 motor failure, is the critical failure mode. Thus, we build the failure behavior model for agents with failure mode F3. F3 motor failure of agents causes the failed agents stationary but remain in the communication network of the swarm. In fact, except for motor failure, this individual behavior can also be caused by actuators failure, energy shortage, or any attack that makes individuals unable to move without damaging the communication system. Assume all agents in UAS are well-working at the beginning, and there exists time $t_k \geqslant 0$ in the duration of the mission. The attributes of this behavior are as follows:

(i) Agent i behaves normally before t_k and updates its state according to the right update rule.

(ii) Agent i stops changing its state for all $t \geqslant t_k$, i.e., $\boldsymbol{x}_i(t) = \boldsymbol{x}_i(t_k)$ for all $t \geqslant t_k$.

(iii) Agent i conveys the same state to each neighbor.

In [31], LeBlanc et al. defined this failure behavior as crash fault. In the following subsections, we will refer to this failure behavior as crash fault.

5.2 Failure strategies

To simulate the scope and location of the failed agents in the swarm, two strategies which are the commonest failure strategies in complex network are investigated, namely random failure and malicious failure. The metric chosen to identify the significance of the nodes in this paper is degree. Considering the time-varying of the swarm topology, the temporal degree failure [32] is selected to model the malicious failure. Let P denote the percentage of the failed agents, then the number of the failed agents is denoted by N×P.

(i) Random failure

In a random failure, the initially failed agents are randomly chosen with the proportion P, ignoring the network topology and any other properties.

Random failure can mimic failures due to platform defects and external environmental factors.

(ii) Temporal degree failure

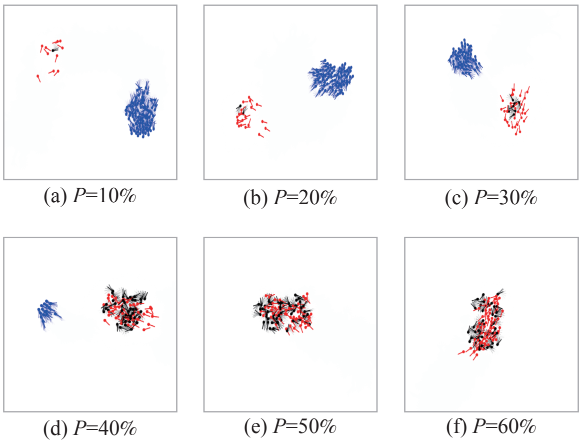
The temporal degree failure is a type of malicious failure strategy. This strategy is designed as a comparison of the random failure to investigate the effect of network topology. We order the agents according to their temporal degree decreasingly and then select the top N×P agents as failure agents. According to the dynamical temporal swarm network, the agent's degree is the number of its neighbors who directly interact with it at time t, which is a temporal variable.

Temporal degree failure can mimic failures due to malicious attacks by the enemy with all the information about the topology.

6. Resilience evaluation method

6.1 System performance metric

The system performance metric is proposed to measure the system's ability to exhibit collective behaviors. In this view, according to the proposed swarm model in Section 3, the expected swarm behaviors are cohesive and ordered motions of a group of individuals. Taking the failed agents with the crash fault into the swarm model, the emergent behavior changed: a part of normal agents or the whole group is anchored by the failed agents, as shown in Fig. 2. The reason is that the wrong information from the failed agents propagated to the rest of the swarm. While normal agents make decisions about their motion next updating according to their received information, including the wrong information from the failed agents. A large amount of wrong information makes normal agents anchored around the failed agents and cannot be able to follow the motion of the swarm. Fig. 2 shows the swarm behaviors with different percentages of failed agents. The red, black, and blue particles refer to failed agents with crash fault, anchored agents, and normal agents respectively. When the percentage of failed agents exceeds 50%, the whole group is anchored and cannot move. The number of anchored agents is an important metric to measure the collapse of the system, and we call these anchored agents cascading failed agents.


(a) P=10% (b) P=20% (c) P=30%

(d) P=40% (e) P=50% (f) P=60%

Fig. 2 Swarm behavior with different percentages of failed agents *P* for the system comprising 100 agents

According to the above swarm behavior, we divide the agents into three types: failed agents, cascading failed agents, and normal agents. Fig. 3 gives the schematic diagram of three types of agents in swarm systems. The failed agents keep their state unchanged, and the cascading failed individual is only temporarily controlled by the failed agents, which can be recovered by interacting with other normal agents. The failed agents and cascading failed agents are included in abnormal agents. The number of cascading failed agents is an important metric to measure the performance of the system.

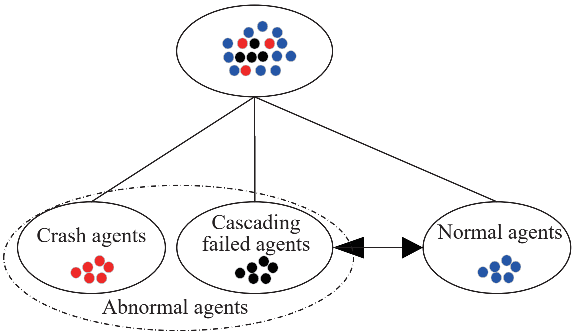


Fig. 3 Schematic diagram of three types of agents in swarm systems

6.2 Resilience measurement

The dynamic interaction network of swarms can be described by $G_r(\boldsymbol{V}(t),\varepsilon_r(\mathrm{t}))$ with node set $\boldsymbol{V}(t)$ and edge set $\varepsilon_r(t)$, where $\varepsilon_r(t)$ is as follows:

$$\varepsilon_r(t)=\left\{(i,j)\,|\,\left\|\boldsymbol{x}_i(t)-\boldsymbol{x}_j(t)\right\|\leqslant r\right\}. \tag{3}$$

One or a small number of agents with crash fault in the UAS can anchor a part of normal agents, which may result in the fragmentation of the whole group into multiple clusters. The clusters with the failed agent are called failure clusters. From the perspective of the network, the cascading failed agents refer to the agents in the same clusters with at least one failed agent and have a small displacement.

Specifically, the failure cluster is built with the abnormal agents (the failed agents and the cascading failed agents) as nodes, the interactions between these abnormal agents as links. In light of the evolution of abnormal agents in the two-dimensional physical space over time, we regard the failure clusters as a three-dimensional spatiotemporal network cluster.

During an observation period, the number of abnormal nodes in each failure cluster at a snapshot of the temporal layer t, $N_f(t)$, varies with time, as shown in Fig. 4. Thus, $N_f(t)$ can be regarded as the cross-section area of the failure cluster at time t, which can reflect the cascading process of failure and the recovery process. In this paper, we take the number of agents in failure clusters, $N_f(t)$, as the performance metric.

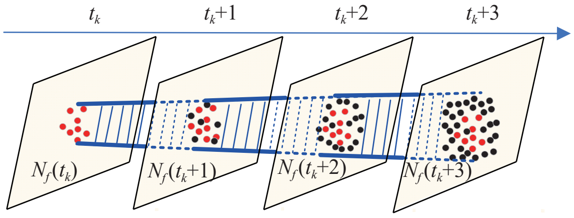


Fig. 4 Evolution of failure cluster

Absorption, adaption, and restoration are the three main perspectives of resilience. Absorption is the degree to which a system is able to absorb shocks posed by a disruption. Adaption is the degree to which a system is able to adapt itself temporarily to new disrupted conditions. Restoration is the degree to which a system is able to restore itself if adaptive capacity is not effective respectively. We analyze the time evolution of $N_f(t)$ to evaluate the resilience performance of the UAS. In the beginning, all individuals coordinate as a cohesive team to move. At time t_k, some of them fail and affect neighboring individuals through the dynamic swarm network in a cascading process. Influenced by the failed agents, some normal agents may be anchored and become cascading failure agents, that is, $N_f(t)$ is getting to increase until time t_a. This phase reflects the absorptive capacity of the UAS. It is worth noting that the cascading failed agents are not static, instead, they move around the failed agents. Subsequently, with the moving of the cascading failure agents, they gather. Then, among the neighbors of some of them, the proportion of failed individuals is getting lower, which will help the agents get rid of the influence of failed agents. And $N_f(t)$ starts to decrease. Suppose that at the time t_r, the swarm recovers to a new stable performance level. This is the recovery process triggered by the self-organization of the individual. Because the swarm recovery phase starts quickly after the failure, the adaptation phase is short.

Based on the resilience triangle assessment approach [15], the timespan between t_k and t_r, which is the lifetime of this failure cluster, is defined as the resilience period (as shown in Fig. 5). The cluster size, which is the total number of nodes (individuals) in the failure cluster during its lifetime, can be regarded as RL in the dynamic swarm network.

$$\mathrm{RL}=\int_{t_k}^{t_r}N_f(t)\,\mathrm{d}t \tag{4}$$

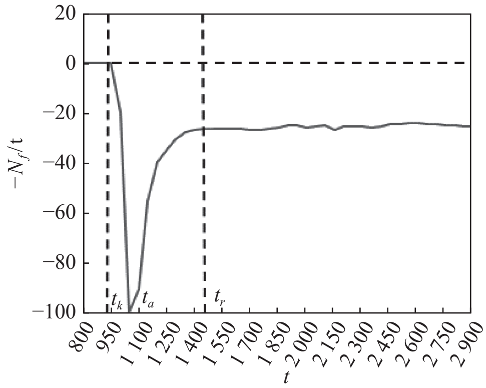


Fig. 5 Illustration of the evolution of a failure cluster

This measurement takes all three capacities, absorption, adaption, and restoration, into consideration.

It is normalized to the following form:

$$\widehat{\mathrm{RL}} = \frac{\int_{t_k}^{t_r} N_f(t)\,\mathrm{d}t}{N(t_k - t_r)} \tag{5}$$

where N represents the total number of individuals.

$\widehat{\mathrm{RL}}$ is a normalized value between 0 and 1. The closer it is to 1, the smaller the resilience is. $\widehat{\mathrm{RL}}$ not only characterizes the cascading effect of failed agents in the spatial dimension but also includes the duration of cascading failed individuals. Thus, the larger the cluster size is, the less resilient the swarm becomes.

7. Simulation studies and discussion

7.1 Parameter settings

Consider a swarm of N agents moving about in a two-dimensional plane with constant speed $v_0 = 1\ \mathrm{s}^{-1}$ at initial random directions. They start in a random position, in which each individual can detect at least one other individual. The zones of repulsion and interaction are centered on the individual, with radii of 1 and 6, respectively. Individual motion is subject to random disturbance, which follows a uniform distribution with the interval $[-\vartheta/2, -\vartheta/2]$, where $\vartheta = 0.1$. The max turning angle of individuals is $\vartheta_{\max}\Delta t$, where $\vartheta_{\max} = 2$.

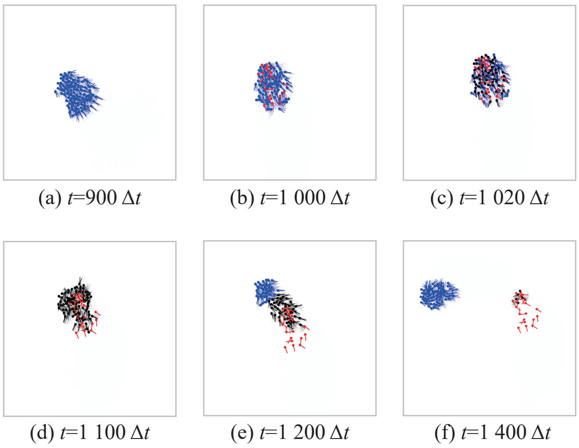
Ten randomly initialized configurations are created for each system comprising 10, 50, 100, 200, 500 individuals respectively. Assume the failed agents are randomly distributed and the failure occurs at time $1\,000\varDelta t$. The simulations are run 200 times, with different percentages of failed individuals. The failure cluster $N_f(t)$ is measured at $t_f\varDelta t - 50\varDelta t$, where the final time step, $t_f = 3\,000$. Simulation parameters are listed in Table 1.

Table 1 Simulation parameters

Parameter	Symbol	Value
Speed/(m/s)	v_0	1
Zone of interaction/m	r	6
Zone of repulsion/m	r_0	1
The max turning angle/(rad/s)	$\vartheta_{\max}$	2
Time step/s	Δt	0.2
Number of individuals	N	10, 50, 100, 200, 500
Failure proportion	P	0—1

7.2 Resilience with different percentages of failed agents

It is shown in Fig. 6 that the snapshots of the simulated failure spread from the failed agents to the whole system and are finally self-repaired to a new stable state. The blue, red, and black particles represent normal agents, failed agents, and the cascading failed agents respectively. Fig. 6. (b)−Fig. 6(d) show the process of cascading failure and Fig. 6. (e)−Fig. 6(f) show the self-repair process. It can also be seen that the agents with a spatial location closer to the failed agents firstly begin to be cascading affected. The failure begins to spread with time until it reaches the system's boundary. Then, the recovery process is started. The agents with spatial location farther from the initially failed agents firstly begin to recover and lead more agents away from the crash fault agents.



(a) t=900 Δt (b) t=1 000 Δt (c) t=1 020 Δt

(d) t=1 100 Δt (e) t=1 200 Δt (f) t=1 400 Δt

Fig. 6 Spatiotemporal evolution of cascading failure in the swarm system with 100 agents and 10% failed agents

Fig. 7 shows the evolution of $N_f(t)$ over time. When some agents fail ($t = 1\,000\Delta t$), a cascading process takes place, the number of abnormal agents $N_f(t)$ increases rapidly to a max value, implying a growing number of agents are anchored by the failed agents. Then, the recovery process occurs and $N_f(t)$ decreases. This is because some agents regroup and get rid of the anchoring of failed individuals. The recovery duration increases as the percentage of failed agents increases, while the new steady-state declines. However, when the percentage of failed agents P = 50%, N_f (t) is unable to change after reaching the maximum value of 100, which means the whole swarm is anchored by the failed agents and unable to recover.

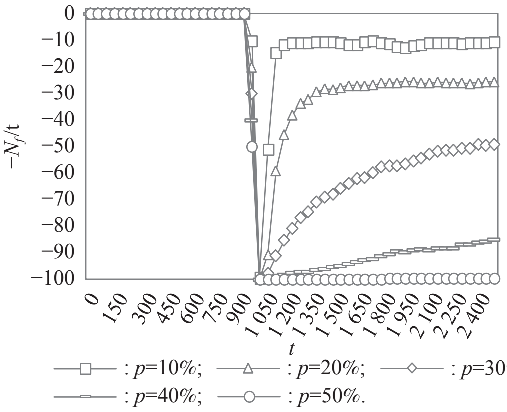


Fig. 7 Evolution of N_f (*t*) with different *P* for the system comprising 100 individuals

Fig. 8 reveals that resilience loss $\widehat{\mathrm{RL}}$ increases as the percentage of failed agents increases. The solid blue line represents the RL of the swarm calculated by (5) based on the simulation data. $\widehat{\mathrm{RL}}$ is monotonically increasing with the increase in the percentage of failed agents P. When P exceeds 50%, $\widehat{\mathrm{RL}}$ is approximately 1, that is, the whole swarm collapses. Hence, P = 50% can be taken as the tipping point of the collapse of the swarm with 100 agents. Besides, the dotted red line $y=\int_{t_0}^{t_r}(P\times N)\mathrm{d}t/N$ $(t_r - t_0) = P$ represents the resilience loss without taking cascading failures into account. The area between the solid blue line and the dotted red line represents the difference of RL whether considering the cascading failures. When $P < 10\%$, the effect of cascading failures is relatively small. It may be explained by the “many wrongs principle” which holds that individual orientation error is suppressed by group cohesion [33]. When $P > 20\%$, the effect of cascading failures experiences a rapid increase. When P=0.5, the whole swarm fails.

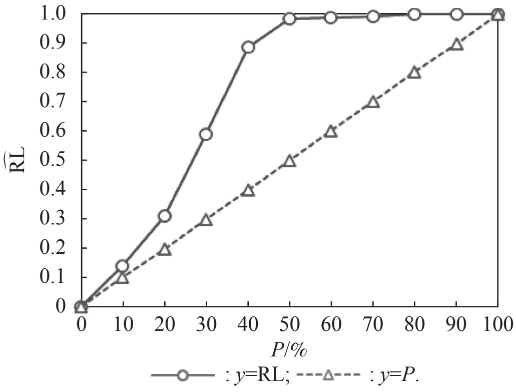


Fig. 8 RL with different *P* for the system comprising 100 individuals

In order to observe the distribution of the number of cascading failed agents N_c, we calculate the proportion of cascading failed agents in 200 experiments, $l = N_c / (1-P)N$. As shown in Fig. 9, the distribution of l is not uniform and presents two levels. The vast majority of l fall in the interval of $l \geqslant 0.9$ and $l \leqslant 0.5$. When $P \leqslant 10\%$, the percentage of $l = 0$ is approximately 1, implying there is almost no cascading failed agents. With P increasing, the percentage of $l = 1$ increases. When $P = 50\%$, $l \geqslant 0.9$ is found in 96 of 100 experiments, implying that the statistical probability that the swarm system collapse is approximately 94%.

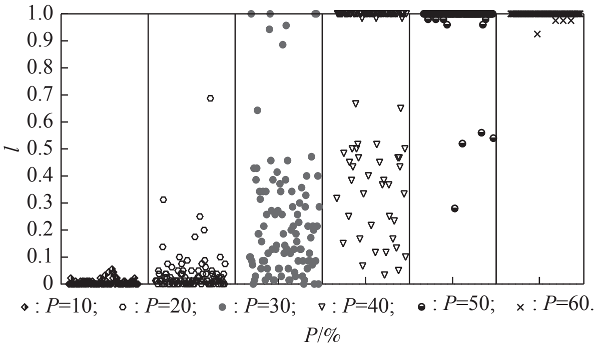
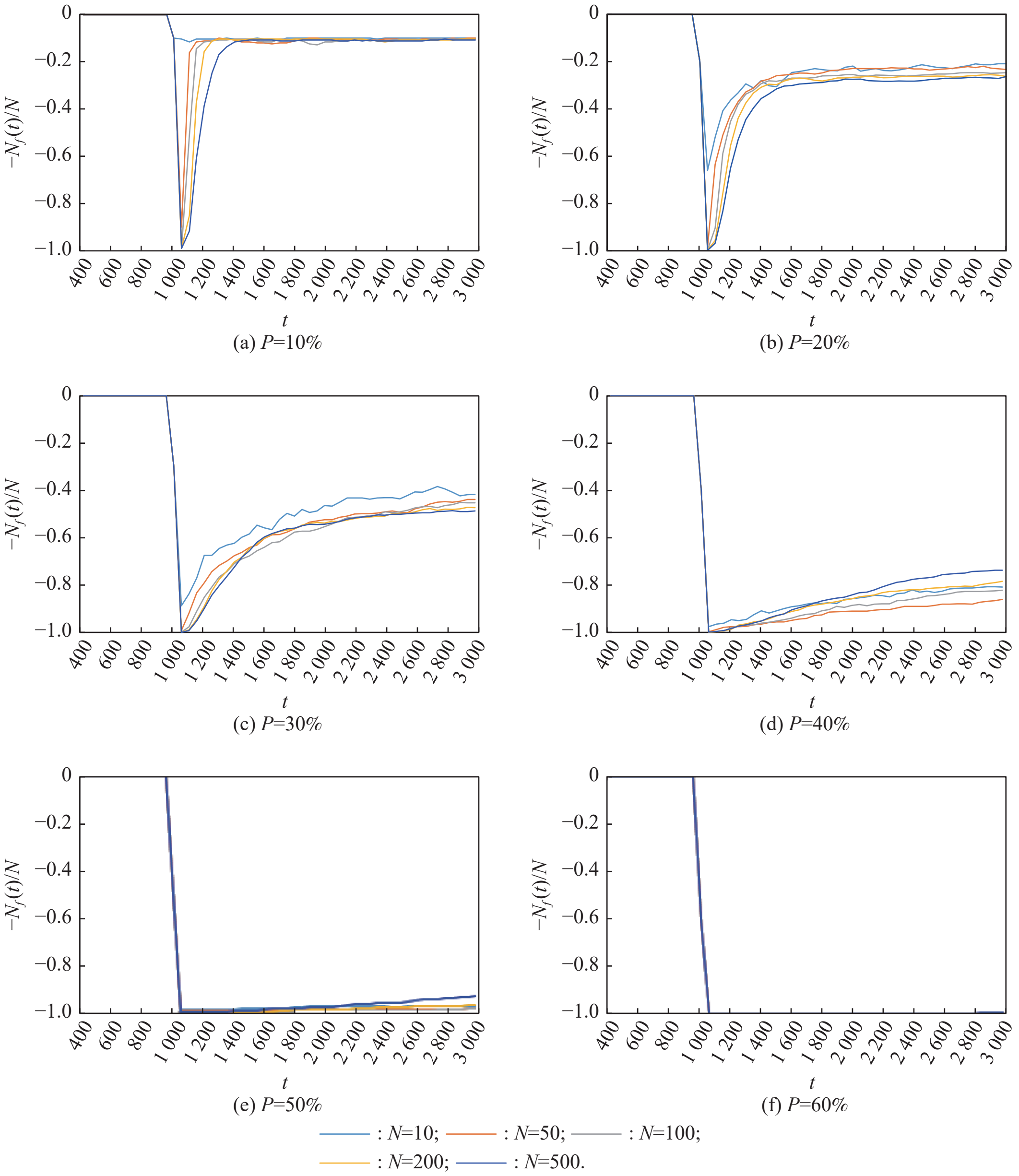


Fig. 9 Distribution of *l* with different *P* for 1 000 experiments where *l*=N_c / (1−*P*)*N*

7.3 Resilience with different swarm sizes

The simulation results in Fig. 10 reveal the influence of failed agents on swarms of different sizes. The ratio $-N_f(t)/N$ is used to measure the influence of different swarm sizes instead of N_f (t). It can be seen that the swarm size can affect the lowest performance level, the duration of self-repair, and the final steady-state. When $P \leqslant$ 30%, swarms with 10, 50, 100, 200, 500 individuals all experienced a significant recovery process. The recovery duration increases as the size of the swarm increases. Meanwhile, the new steady-state declines as the size of the swarm increases. The situation changes when P = 40%. Swarms of large sizes, such as 200 agents and 500 agents, reach a higher new steady-state than that of swarms of small sizes. Nevertheless, all swarms fail with 0.5 failed agents. It also can be seen that the propagation velocity is independent of the swarm size. However, the swarm size can affect the lowest performance level, the duration of self-repair, and the final steady-state.

Fig. 11 shows the resilience loss $\widehat{\mathrm{RL}}$ calculated by (6). When $P \leqslant 30\%$, RL increases as the size of the swarm increases. The main reason is that the larger the swarm is, the longer the recovery time is needed, and the lower the new steady state is. However, when $P > 30\%$, RL of the small swarm increases faster than that of the large swarm. From the perspective of resilience, the swarm with a small size has the advantage in the case of a small percentage of failure individuals ($P \leqslant 30\%$), while the swarm with a large size is better in the case of the large percentage of failure individuals. However, when P reaches 60%, RL of all the swarms of different sizes is approximately 1. Combined with the analysis in Subsection 2.2, we can conclude that the tipping point of collapse of the swarm ($P = 50\%$) is related to the interaction mechanism of the swarm model and independent of swarm size.



(a) P=10%

(b) P=20%

(c) P=30%

(d) P=40%

(e) P=50%

(f) P=60%

Fig. 10 Evolution of $-N_f(t)/N$ with different P for the systems comprising 10, 50, 100, 200, 500 individuals

7.4 Resilience with different failure strategies

The proportion of abnormal agents $N_f(t)/N$ under random failure and temporal degree failure with various failure proportions P has been investigated. Normally, no matter what kind of failure strategies, the final state of $N_f(t)/N$ increases as the failure proportion P grows, and the duration of recovery increases as P increases (Fig. 12). The final steady-state under temporal degree failure is lower than that under the random failure with fixed failure proportion P. While the recovery process starts earlier under degree failure. Fig. 13 shows the comparison of RL under the two failure strategies, which indicates that the temporal degree failure leads to a greater RL than random failure under different failure proportions.

The results in Fig. 12 and Fig. 13 suggest that, in comparison with the random failures, the temporal degree failure can break down the swarm system more efficiently. The reason is that the agents with high degrees are able to influence more agents. An agent with a high degree means that it can interact with more neighbor agents. Once it fails, the wrong information will be quickly transmitted through its neighbor agents, so the temporal failure performs much harmfully to the resilience of swarm systems than the random failure.

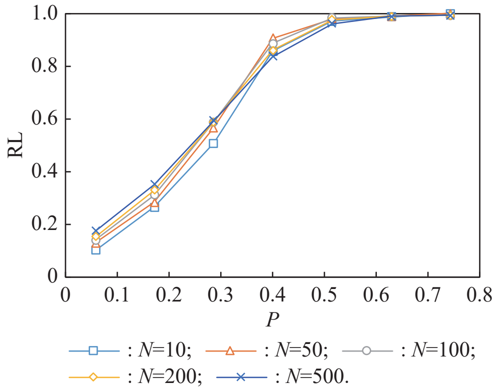
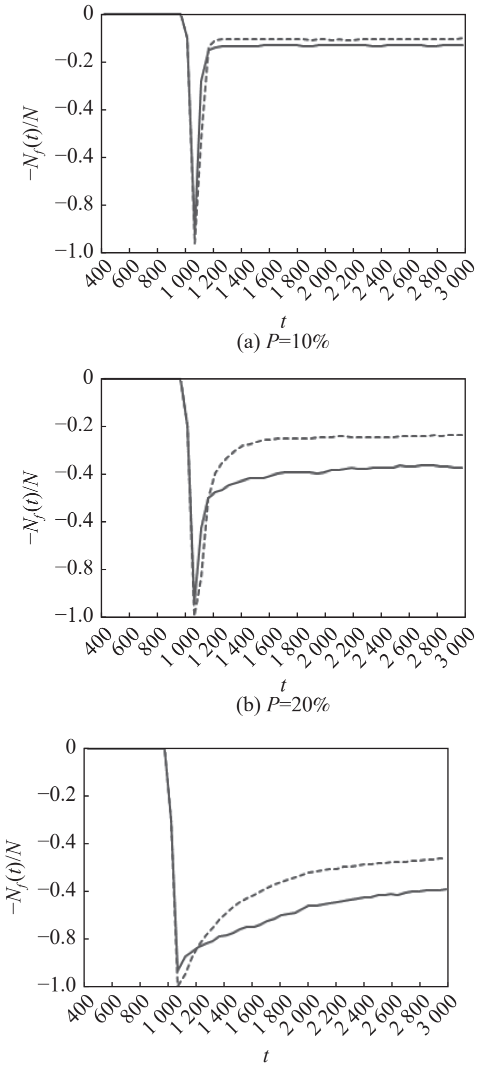


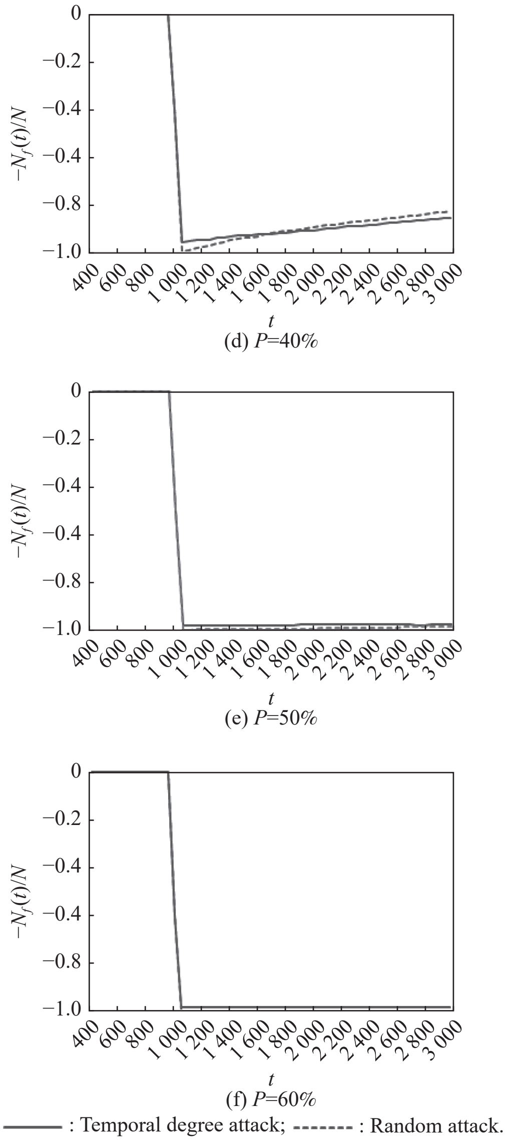
Fig. 11 RL of swarms of different sizes with different *P*



(a) P=10%

(b) P=20%

(c) P=30%



(d) P=40%

(e) P=50%

(f) P=60%

Fig. 12 Comparison of the ratio $-N_f(t)/N$ of random failure and temporal degree failure with different P for N=100

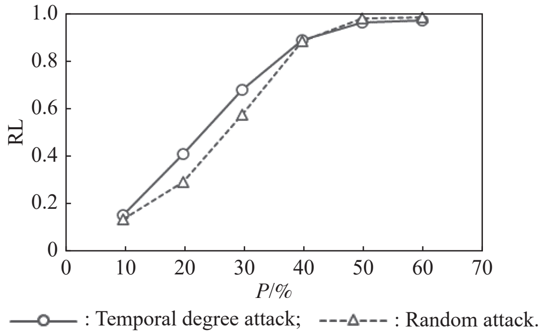


Fig. 13 Comparison of RL under random failure and temporal degree failure with N=100

8. Conclusions

In this study, we propose a framework to describe the method of failure analysis of UAS. A multi-agent swarm model and the failure model are built. In addition, a definition of UAS resilience based on the spatiotemporal evolution of the failure cluster is proposed. Based on the proposed model and method, the internal mechanism of failure propagation and self-reparation of UAS is investigated.

As can be seen from the simulation results, the larger the percentage of failed agents, the longer the recovery duration. While when the percentage of failed agents is close to 50%, the system is no longer able to recover. Note that, all the swarms of different sizes have the same tipping point. Once the proportion of failed agents exceeds this point, the swarm system will collapse completely without the ability to recover. These findings can be used to predict the failure of UAS and to design recovery measures in a stereo way.

In addition, our findings also show the swarm size can affect the lowest performance level, the duration of self-repair, and the final performance level. The larger the swarm, the greater the RL when the percentage of failed individuals is below 30%. The reason is that when $P \leqslant 30\%$ the swarm with a large size recovers to a lower steady-state and needs a longer recovery duration than a smaller swarm. However, larger swarms may recover to a higher steady-state than smaller swarms when the percentage of failed agents exceeds 30%. For example, in our simulation, the new steady state of the large swarm such as 200 or 500 agents is higher than smaller swarms. The above findings reveal that there may be an optimal number of individuals when deploying UAS.

Moreover, it is found that the swarm system is more sensitive to temporal degree failure and agents with a high degree are able to influence more other agents. This finding can be helpful for developing more efficient failure or protection strategies for UAS.

For future research, we plan to improve the swarm models to simulate newly designed collective behaviors based on realistic missions. In addition, failure analysis of UAS under malicious manipulation such as communication manipulation is an interesting topic.

Data availability statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

[1] REYNOLDS C W. Flocks, herds, and schools: a distributed behavioral model. Computer Graphics, 1987, 21(4): 25–34.

[2] VICSEK T, CZIROK A, BEN-JACOB E, et al. Novel type of phase transition in a system of self-driven particles. Physical Review Letters, 1995, 75(6): 1226–1229.

[3] COUZIN I D, KRAUSE J, JAMES R, et al. Collective memory and spatial sorting in animal groups. Journal of Theoretical Biology, 2002, 218(1): 1–11.

[4] COUZIN I D, KRAUSE J, FRANKS N R, et al. Effective leadership and decision-making in animal groups on the move. Nature, 2005, 433(7025): 513–516.

[5] OLFATI-SABER R. Flocking for multi-agent dynamic systems: algorithms and theory. IEEE Trans. on Automatic Control, 2006, 51(3): 401–420.

[6] CUCKER F, SMALE S. Emergent behavior in flocks. IEEE Trans. on Automatic Control, 2007, 52(5): 852–862.

[7] CHAMANBAZ M, MATEO D, ZOSS B M, et al. Swarm-enabling technology for multi-robot systems. Frontiers in Robot and AI, 2017, 4(12): 1–12.

[8] PARKER L. Reliability and fault tolerance in collective robot systems. Handbook of Collective Robotics. KERNBACH S, ed.. Stanford: Pan Stanford, 2013.

[9] BAI G H, LI Y J, FANG Y N, et al. Network approach for resilience evaluation of a UAV swarm by considering communication limits. Reliability Engineering & System Safety, 2020, 193: 106602.

[10] CHENG C C, BAI G H, ZHANG Y A, et al. Resilience evaluation for UAV swarm performing joint reconnaissance mission. Chaos, 2019, 29: 053132.

[11] HOLLING C S. Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 1973, 4(1): 1–23.

[12] PLUMMER R, ARMITAGE D. A resilience-based framework for evaluating adaptive co-management: linking ecology, economics and society in a complex world. Ecological Economics, 2007, 61(1): 62–74.

[13] MADNI A, JACKSON S. Towards a conceptual framework for resilience engineering. IEEE Systems Journal, 2009, 3(2): 181–191.

[14] HOSSEINI S, BARKER K, RAMIREZ-MARQUEZ J E. A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 2016, 145: 47–61.

[15] BRUNEAU M, CHANG S E, EGUCHI R T, et al. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra, 2003, 19(4): 733–752.

[16] HOLLNAGEL E, WOODS D D, LEVESON N. Resilience engineering: concepts and precepts. London: CRC Press, 2006.

[17] SAULNIER K, SALDANA D, PROROK A, et al. Resilient flocking for mobile robot teams. IEEE Robotics & Automation Letters, 2017, 2(2): 1039–1046.

[18] ADAMS T M, BEKKEM K R, TOLEDO-DURAN E J. Freight resilience measures. Journal of Transportation Engineering, 2012, 138(11): 1403–1409.

[19] SAHEBJAMNIA N, TORABI S A, MANSOURI S A. Integrated business continuity and disaster recovery planning: towards organizational resilience. European Journal of Operational Research, 2015, 242(1): 261–273.

[20] ZHANG L M, ZENG G W, LI D Q, et al. Scale-free resilience of real traffic jams. Proc. of the National Academy of Sciences of the United States of America, 2019, 116(18): 8673–8678.

[21] EROL S, WILLIAM S. Swarm robotics. Santa Monica: Springer, 2004.

[22] BRAMBILLA M, FERRANTE E, BIRATTARI M, et al. Swarm intelligence swarm robotics: a review from the swarm engineering perspective. Swarm Intelligence, 2013, 7(1): 1–41.

[23] STAMATIS D H. Failure mode and effect analysis: FMEA from theory to execution. Milwaukee: Quality Press, 2003.

[24] MOHAMMAD K. Resilience and controllability of dynamic collective behaviors. PLOS, 2013, 8(12): e82578.

[25] KOMAREJI M, SHANG Y, BOUFFANAIS R. Consensus in topologically interacting swarms under communication constraints and time-delays. Nonlinear Dynamics, 2018, 93(3): 1287–1300.

[26] ALBERT R, JEONG H, BARABASI A. Error and attack tole rance of complex networks. Nature , 2000, 406(6794): 378–382.

[27] FENG H F, LI C H, XU Y J. Invulnerability analysis of vehicular ad hoc networks based on temporal networks. Proc. of the 2nd IEEE Invulnerability Analysis of Vehicular Ad Hoc Networks based on Temporal Networks, 2016: 2198–2202.

[28] SUR S, GANGULY N, MUKHERJEE A. Attack tolerance of correlated time-varying social networks with well-defined communities. Physica A: Statistical Mechanics and Its Applications, 2015, 420: 98–107.

[29] ZHONG J L, ZHANG F M, LI Z X. Identification of vital nodes in complex network via belief propagation and node reinsertion. IEEE Access, 2018, 6: 29200–29210.

[30] WINFIELD A, NEMBRINI J. Safety in numbers: fault-tolerance in robot swarms. International Journal of Modelling, Identification and Control, 2006, 1(1): 30–37.

[31] LEBLANC H J, ZHANG H T, SUNDARAM S, et al. Resilient continuous-time consensus in fractional robust networks. Proc. of the IEEE American Control Conference, 2013: 1237–1242.

[32] LIU K K, ZHONG J L, BAI G H, et al. Complex networks approach for reliability evaluation of swarm systems under malicious attacks. IEEE Access, 2020, 8: 81209–81219.

[33] SIMONS A. Many wrongs: the advantage of group navigation. Trends in Ecology & Evolution, 2004, 19(9): 453–455.

Biographies

XU Bei was born in 1987. She is currently working toward her Ph.D. degree with National University of Defense Technology, Changsha, China. She is also currently a lecturer with the School of General Aviation, Nanchang Hangkong University, Jiangxi, China. Her research interests include network reliability and system resilience.

E-mail: 70611@nchu.edu.cn

BAI Guanghan was born in 1986. He received his Ph.D. degree in mechanical engineering from University of Alberta, Edmonton, AB, Canada, in 2016. He is currently a lecturer with the Laboratory of Science and Technology on Integrated Logistics Support, National University of Defense Technology. His research interests include network reliability and system resilience.

E-mail: baiguanghan@nudt.edu.cn

ZHANG Yun'an was born in 1983. He received his Ph.D. degree in mechanical engineering from National University of Defense Technology, Changsha, China, in 2014. He is currently an associate professor with the Laboratory of Science and Technology on Integrated Logistics Support, National University of Defense Technology. His research interest focuses on system reliability.

E-mail: yazhang@nudt.edu.cn

FANG Yining was born in 1991. She received her Ph.D. degree in mechanical engineering from University of Alberta, Edmonton, AB, Canada, in 2019. She is currently a lecturer with the Laboratory of Science and Technology on Integrated Logistics Support, National University of Defense Technology. Her research interests include system resilience.

E-mail: fangyining@nchu.edu.cn

TAO Junyong was born in 1969. He received his Ph.D. degree in mechanical engineering from National University of Defense Technology, Changsha, China, in 2000. He is currently a professor with the Laboratory of Science and Technology on Integrated Logistics Support, National University of Defense Technology. His research interests include reliability test and evaluation.

E-mail: taojunyong@nudt.edu.cn