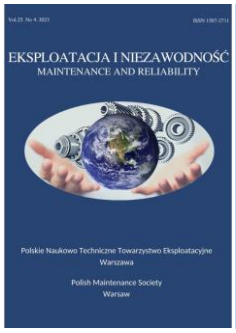


Eksploatacja i Niezawodnosc – Maintenance and Reliability
Volume 25 (2023), Issue 4
journal homepage: http://www.ein.org.pl

Article citation info:
Wei K, Zhang T, Zhang C, Research on resilience model of UAV swarm based on complex network dynamics, Eksploatacja i Niezawodnosc – Maintenance and Reliability 2023: 25(4) http://doi.org/10.17531/ein/173125

Research on resilience model of UAV swarm based on complex network dynamics

Indexed by: Web of Science Group

Kunlun Wei[a], Tao Zhang[a,*], Chuanfu Zhang[a]

[a] School of systems science and engineering, Sun Yat-sen University, China

Highlights

- The influence aspects of resilience on the UAV swarm topology are proposed. Those are incoming degrees, communication types, distance between nodes.
- We conduct the dynamics analyzing in self-dynamic, topology, information transmission, brings a new perspective to the UAV swarm studies.
- We propose a resilience model of UAV swarm based on topology and system's dynamics that incorporates SIS model.

Abstract

Unmanned Aerial Vehicle (UAV) swarms are utilized in various missions and operated within an open environment that is prone to disruptions. The resilience of UAV swarms, an important requirement, mainly revolves around ensuring stable and uninterrupted operations. Malicious attacks can implement the adverse impacts of potential threats through swarm communication links. In this context, the SIS (Susceptible → Infected → Susceptible) method is suitable for describing the information transmission within UAV swarms. An enhanced resilience model of the UAV swarm is proposed in this study, which incorporates the factors of self-dynamics, dynamics of topology, dynamics of information transmission, and SIS into the complex network model. Self-dynamics refer to the internal dynamics of the drones. In this paper, dynamics of topology consist of three factors: the varying distance between drones, the incoming degrees of each drone, and the number of communication types between drones. Lastly, dynamics of information transmission are characterized by SIS. The model proposed in this paper has the capability to effectively capture changes in the network topology as well as the dynamics of the system, which are significant contributors to the loss of resilience. And then, the average number of susceptible drones is utilized as the metric to evaluate the resilience of the swarm. Furthermore, an experiment is conducted where a UAV swarm successfully carries out a surveillance mission to demonstrate the advantages of our proposed method. The proposed model not only enables the support of mission planning but also facilitates the design enhancements of UAV swarms.

Keywords
UAV swarm, resilience, SIS, system dynamics, topology

1. Introduction

In numerous complex systems, resilience plays a vital role as a characteristic enabling them to effectively accommodate errors, failures, and alterations in the surrounding environment, while still preserving their fundamental functionality[10]. This paper defines UAV swarm resilience as the extent to which the interaction between components, the quantity of nodes/edges, and the level of performance deterioration during an attack are intertwined[11]. Unfortunately, the development and application of resiliency technologies to related systems is not widespread. The reason may be that the resilient design of

(*) Corresponding author.
E-mail addresses: K. Wei (ORCID: 0000-0002-3318-7655) weiklun@mail2.sysu.edu.cn, T. Zhang (ORCID: 0000-0002-9161-3210) zhangt358@mail.sysu.edu.cn, C. Zhang (ORCID: 0009-0007-1525-5830) zhangchf9@mail.sysu.edu.cn

complex systems are difficult to assure their safety[31], challenges of integrating change-detection, trial-and-error learning methods, obtaining reliable performance evaluations under constrained evaluation time and improving the safety are hard to meet for swarms[7]. The task of building resilient UAV swarms has been attempted by researchers for the past decade. However, research on current trends shows gaps in swarm designs that make evaluating the resiliency of such swarms less than ideal[25].

The use of UAV swarms is versatile, encompassing various missions such as surveillance, rescue operations, payload delivery, and agriculture[21]. These swarms perform with a self-governance structure, enabling them to autonomously organize and adapt to achieve global mission objectives. Operating in hostile environments, they are susceptible to disruptions, often without prior knowledge of the type and magnitude of these disruptions[36], Accidental disruptions can have adverse effects on the execution of tasks. Enhancing resilience is a crucial approach to improving the swarm's anti-interference capacity[24], yielding both business and safety benefits.

Currently, UAVs are specifically engineered to employ wireless communication for information sharing and interaction[19]. The topology of UAV swarms evolves as the position of each drone changes during different task phases. In order for the swarm to successfully accomplish its mission, it is crucial to ensure efficient and reliable information exchange among all the drones[35]. However, the present research on this subject inadequately addresses the influence of distance and dynamic changes in the structure between UAVs[18].

It is impractical to assume that two far apart UAVs and two close UAVs have the same level of communication quality. Moreover, the links between each pair of UAVs undergo dynamic changes due to the rapid movement of each UAV during the task[38]. Therefore, it is vital to incorporate the factors of topology and distance dynamic changes into the UAV cluster model[3].

The position of drones greatly impacts communication capability and topology, which is why researchers have dedicated their attention to location studies. Dui conducted an analysis of UAV cluster performance, taking into account the varying reliability of drones at different locations[12]. Sadrollah et al. proposed a distributed localization framework that enables fast and reliable dissemination of localized information in flexible three-dimensional networks consisting of UAV swarms. They ingeniously combined Internet of Things technologies with robotics swarms to effectively control UAV swarms. However, it is worth noting that no actual experiments were conducted in this research, and only basic ideas were introduced[27].

A survey conducted by[9] on routing protocols reveals that the majority of advancements prioritize performance over security. However, it should be noted that insecure protocols and networks, even if resistant to connectivity issues, do not necessarily indicate a resilient swarm. The crucial aspects of the communication component that demand attention are connectivity, network coverage, structure. The communication pipeline plays a critical role in facilitating significant swarm functionalities, including data transfer and action control. Ensuring seamless communication is typically the initial stride towards establishing robust systems. Communication-related challenges comprise of delays in information transfer between swarm agents or external entities. Moreover, swarm agents may encounter obstacles hindering their inter-communication for various reasons. Occasionally, communication may even be severed entirely. To address these concerns, ongoing research in formation control, utilizing ad hoc networks, scrutinizes these issues and suggests potential remedies. In the event of certain swarm agents disconnecting, a flexible formation control approach can rearrange the swarm positions, thereby restoring connectivity between the agents. Transmission delays can be effectively mitigated through the implementation of formation switching, which allows swarm agents to utilize alternative topologies. This strategic approach positions the agents in closer proximity to the broadcast handling agents, thereby reducing any potential delays. Additionally, the integration of passive beacons on the ground plays a crucial role in recovering agents from failures. These beacons effectively guide the agents towards failsafe points, ensuring their smooth operation even in the face of challenges. However, the intricate details of the underlying research mechanism behind these advancements have yet to be unveiled.

In a UAV swarm, tasks can be simplified and reduced by assigning them to multiple vehicles. This eliminates the need to develop complex custom systems structures to meet specific

requirements[24]. To design a more resilient UAV swarm capable of successfully performing tasks, it is important to carefully study the topology to identify key determining factors of resilience. There are two types of UAV systems: homogeneous and heterogeneous[17]. In a homogeneous swarm, the homogeneous drones have similar functional and physical characteristics. On the other hand, in a heterogeneous swarm, the drones have different physical characteristics or perform different functions[32,26]. The heterogeneity of UAVs, with their complementary capabilities, can contribute to system resilience[23,15]. However, the impact of heterogeneity on resilience has not been sufficiently explored.

UAVs with high-performance communication capabilities can provide excellent mission services. It is essential to ensure safe and uninterrupted services during critical missions. However, it can be challenging to maintain resilient and reliable communication services in the event of damages to communication facilities[2]. In his paper, Xu introduces a multistate network model for evaluating the reliability of the Unmanned Swarm Information Exchange Network (USIEN). This model takes into account the information exchange capacity and proposes a comprehensive reliability metric for assessing the USIEN's reliability under a set of predefined missions[35]. To enhance the system's performance, it is advisable to establish an appropriate communication path with sufficient resources[22]. Implementing a backup communication path can have a beneficial impact on resilience.

In a UAV swarm, there are frequent and sudden shifts between favorable and unfavorable states in a complex battlefield. These shifts can be triggered by external, internal, or human-induced disruptions, resulting in crashed drones, loss of communication links, or diminished communication capabilitie[1,8]. Based on simulation results, Xu observed that the duration of the recovery phase becomes prolonged as the proportion of failed agents increases. When the number of failed agents approaches fifty percent, the system becomes incapable of recovering. This critical turning point is applicable to swarms of all sizes. Once this percentage of failed agents is reached, the entire swarm system collapses and recovery becomes impossible[34]. Gao et al. present a refined analytical framework that effectively separates the attributes of topology and system dynamics, ultimately consolidating diverse system behaviors into a comprehensive resilience model. Through their analysis, the researchers shed light on specific properties of systems that have the potential to enhance or diminish resilience. This invaluable insight offers a range of strategies for mitigating sudden shifts in biological, ecological, or economic systems. Moreover, it provides valuable design suggestions for technology systems that can withstand internal failures and external disruptions alike. These analytical findings have significant implications for multiple fields and disciplines[13].

Although some insights have been provided by colleagues, the challenges related to modeling the resilience of UAV swarms based on complex network dynamics remain open. These challenges encompass various aspects such as taking into account the network topology and system dynamics, assessing the impact of communication range on swarm performance, exploring the applicability of complex network dynamics to UAV swarms, understanding the factors affecting swarm topology dynamics, and analyzing the self-dynamics of individual drones. Consequently, our research focuses on tackling these issues by developing a resilience model that investigates the influential factors and enhances the swarm's resilience capability. The key contributions of our study are outlined below.

i. The influence aspects of resilience on the UAV swarm topology are proposed. Those are incoming degrees, communication types, distance between nodes.
ii. We conduct the dynamics analyzing in self-dynamic, topology, information transmission, brings a new perspective to the UAV swarm studies.
iii. We propose a resilience model of UAV swarm based on topology and system's dynamics that incorporates SIS model.

The remainder of this paper is organized as follows. The preliminaries mainly introduce description of UAV swarm system, and SIS model. Dynamics Analysis of UAV Swarm is provided in Section 2. In Section 3, resilience model of UAV swarm based on complex network dynamics is investigated. In Section 4, illustrative experiments are conducted to verify the proposed method. Finally, our conclusions and future work are given.

2. Preliminaries

Consider the scenario of monitoring an unidentified battlefield zone $\Omega \in R^2$ using a fleet of UAVs. The UAVs, denoted as UAVs = $[v_1, v_2,\ldots, v_n]$, possess identical capabilities and attributes. For the purpose of simplification, this study only focuses on the surveillance capability of the UAVs, disregarding physical characteristics such as weight, size, and shape. Each vehicle v_i carries out surveillance tasks independently within its sensing range r_i, where r_i represents the radius of the target area it can surveil. Communication links enable the exchange of information between the drones, allowing them to collaborate and accomplish the surveillance mission (as shown in Fig. 1). The mission performance, which refers to how well the system performs its expected capability in an assigned mission at a given time t.

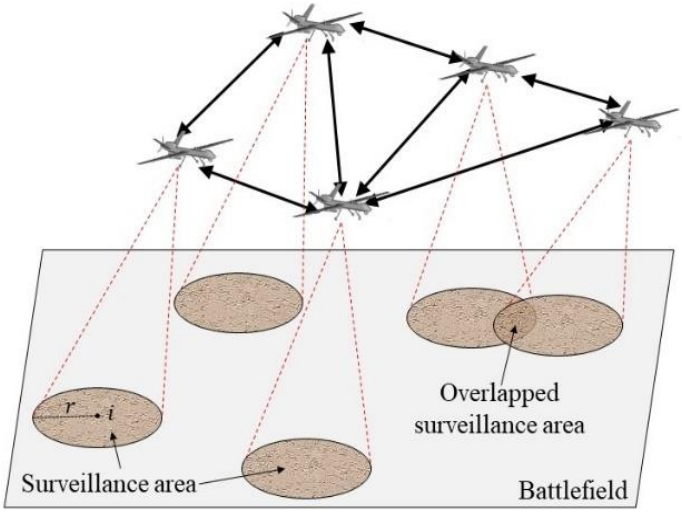


Fig. 1. A collaborative mission utilizing a UAV swarm.

It can be observed from this that information transmission plays a vital role in the UAV cluster system in order to fully maximize its operational efficiency and perform tasks successfully. A UAV swarm transmits data through a predefined communication topology and utilizes this transmitted data to accomplish collaborative system tasks. The effectiveness of the information communication link and the precision of the data content ultimately determine the safe operation and overall success of the UAV swarm. A swarm of UAVs perceives the physical world using sensors and carries out tasks in the physical world using actuators. The controller processes information from the sensors and other intelligent agents, and then transmits response data to the actuators in order to have complete control of the entire system. Generally, the information in a UAV swarm system is primarily made up of three main data transmission links: sensor-controller (S-C), controller-actuator (C-A), and controller-controller (C-C). It is important to note that malicious attacks can target these three data links, potentially compromising the UAV swarm system's mission capability. The S-C and C-A links are known as the internal data links within the intelligent unit, while the C-C link is referred to as the inter-agent data link. The variable u_s represents the input of the ith UAV actuator, which may experience actuator failure during system operation. Similarly, y_s represents the output of the ith UAV senser, which may experience sensor failure during system operation[20].

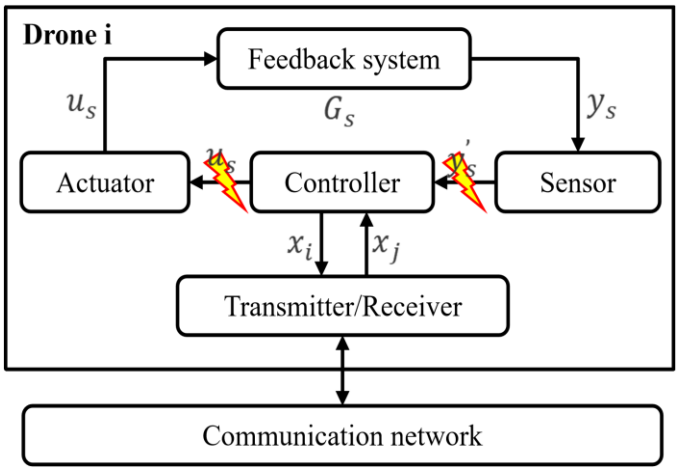


Fig. 2. Communication link structure and attack points of UAV swarm.

2.1. Description of UAV swarm system

Figure 3 illustrates each UAV as a node, clearly differentiated by its respective number. The size of the nodes in Fig. 3 denotes the surveillance area covered by the drones, while the black lines symbolize communication links established between them.

The UAV swarm is prone to a range of disruptions, including network attacks, adverse weather conditions, and opposition defense. The main aim of this study is to investigate how the UAV swarm reacts to these disruptions, in order to ensure its resilience against functional failures or performance deterioration. In Fig. 3, each UAV is depicted as a node and clearly differentiated by its respective number. The size of the nodes in Fig. 3 denotes the surveillance area covered by the drones, while the black lines symbolize communication links

established between them.

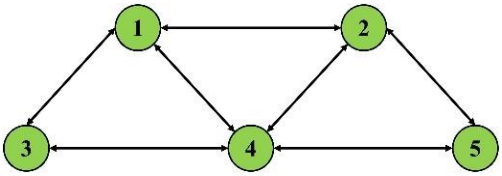


Fig. 3. The abstract description of UAV swarm.

Consider a UAV swarm consisting of N vehicles whose activities $x_i = (x_1, \ldots, x_N)^T$ follow the N-dimensional coupled nonlinear equations[6]. Each drone is expressed by a time related activity $x_i(t)$, $i=1,\ldots,N$, whose meaning is decided by the specific mission, in this paper, it denotes the probability of information tampering of drone i by $0 \le x_i(t) \le 1$ from its neighbors. The system's dynamics is driven by

$$\frac{dx_i(t)}{dt} = M_0\left(x_i(t)\right) + \sum_{j=1}^{N} A_{ij} M_1\left(x_i(t)\right) M_2\left(x_j(t)\right) \quad (1)$$

$M_0(x_i(t))$ captures drone's self-dynamics. $M_1(x_i(t))$ and $M_2(x_i(t))$ account for the impact of i's interacting vehicles. $A_{ij}=A_{i\leftarrow j}$ is a directed link outgoing from j, incoming to i, reflects the weight topology and dynamic of the UAV swarm. The solution of Eq. (1) offers the i's resilience function $x_i(A_{ij})$, which captures the possible states of drone i as a solution of (1). The Eq. (1) shows that the activities of UAV swarm depend on the topology and the system's dynamics. In Eq. (1), resilience loss can be affected by any alteration of the N^2 parameters in A_{ij}, each change corresponding to a different kind of perturbation.

2.2. SIS model

The UAV swarm is vulnerable to various disruptions, such as network attacks, severe weather, and opponents' defense. To study the spread of information within the UAV swarm, we consider each individual UAV as a node[33,37], These nodes can be in a susceptible (S) or infected (I) state. Malicious attacks propagate the negative effects of potential threats and disruptions through swarm communication links. Following a commonly used epidemiological approach, when discussing information spread between nodes, we ignore the specific details of infection within a single UAV and instead view each vehicle as being in one of a small number of discrete states, such as susceptible or infected[16]. Therefore, the transitions in dynamics within the UAV swarm can be described using an SIS model. In Eq. (2), a susceptible drone (S) can become infected by abnormal information from its infected neighbors (I), with a probability denoted as β[14]. This results in the creation of two infected drones after the infection process.

$$S + I \xrightarrow{\beta} 2I \quad (2)$$

The infected drones(I) recover to susceptible(S) with the probability of σ. And the drones can be infected immediately once they are cured.

$$I \xrightarrow{\sigma} S \quad (3)$$

Thus, the dynamic transitions between the susceptible drone and the infected drone, shown in Fig. 4.

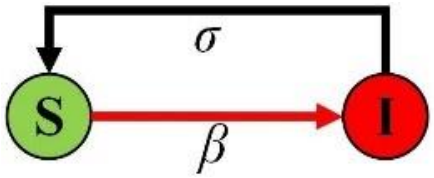


Fig. 4. Dynamic transition diagram for SIS model.

In the UAV swarm, the SIS model is utilized to illustrate an infection process, as shown in Fig. 5, In this model, green nodes represent susceptible drones, whereas red nodes depict infected ones. Initially, at step 0, all drones are in the susceptible state. In step 1, drone 3 falls victim to an attack by opponents and consequently becomes infected. Later, drone 4 also becomes infected through the A_{34} link. The newly infected drone 4 then proceeds to transmit the infection to drone 2 via the A_{42} link. Subsequently, owing to their self-cure ability, the infected drones ultimately regain their susceptible state.

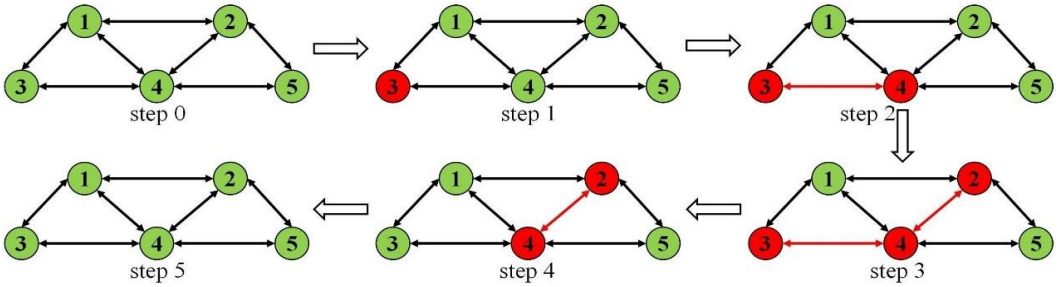


Fig. 5. Infection process of a UAV swarm.

3. Dynamics Analysis of a UAV Swarm

3.1 Self-dynamics of single drone

$M_0(x_i(t))$ analyzing, accounting for i's self-dynamic, is the first step in the research of the UAV swarm's dynamic. It is important to note that the information transmitted between the actuator, controller, and sensor within a single drone (as shown in Fig. 2) is not completely secure and may be subject to loss or alteration. To simplify matters, we assume that the probability of information tampering between the sensor-controller (S-C) and controller-actuator (C-A) links is independent. Additionally, the probability of tampering is the same for the controller-controller (C-C) link, which is represented as $x_i(t)$. The probability of unchanged information transmission in the S-C and C-A links is respectively denoted as 1- $x_i(t)$. Consequently, the dynamic of inner node i is regulated by expression (4).

$$\left(1 - x_i(t)\right)^2 \tag{4}$$

Eq. (4) describes the recovery process of S-C and C-A. The recovery process of an infected drone occurs at a rate proportional to σ and the probability of being infected, $x_i(t)$. Thus, by combining the inner recovery probability of $(1- x_i(t))^2$ with σ and $x_i(t)$ as the form of multiplying, we obtain the self-dynamics of a single drone in Eq. (5).

$$M_0\left(x_i(t)\right) = -\sigma x_i(t)\left(1 - x_i(t)\right)^2 \tag{5}$$

3.2 Dynamics of topology

Although, the topology plays a significant role in the dynamics of a UAV swarm, the research in influence factors of topology dynamic is short. The links between each pair of UAVs undergo dynamic changes due to the rapid movement of each UAV during the task. Therefore, the distance greatly impacts communication capability and topology. On the other hand, the communication pipeline plays a critical role in facilitating significant swarm functionalities, including data transfer and action control. Ensuring sufficient communication links is typically the critical stride towards establishing robust systems. In a UAV swarm, tasks can be simplified and reduced by assigning them to multiple vehicles. The heterogeneity of UAVs, with their complementary capabilities, can contribute to system resilience. So, distance, communication links and heterogeneity are seen as three important factors of topology dynamics in this paper.

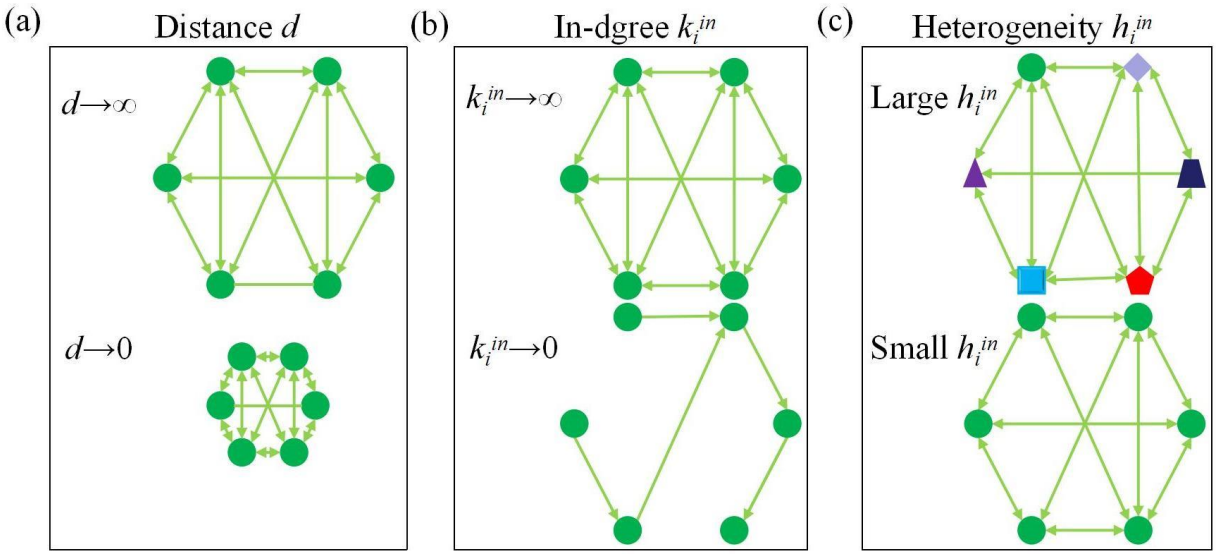


Fig. 6. The meanings of d_{ij}, k_i^{in}, h_i^{in}.

d_{ij}, k_i^{in}, h_i^{in} represent three characteristics of A_{ij}. The meanings of d_{ij}, k_i^{in}, h_i^{in} are shown in Fig. 6(a-c). d_{ij} denotes the distance between drone j and i, d_c means the minimal range of communication. When $d_{ij}<d_c$, communication quality between node j and i is uninfluenced by distance. Intuitively speaking, the longer the distance between two nodes, the smaller weight. Therefore, the value of A_{ij} and the d_{ij} shows a negative correlation. In this paper, we think A_{ij} is proportional

to the inverse square of the distance. k_i^{in} is the incoming degrees of i. The value of k_i^{in} and the number of neighbors shows a positive correlation. But, the weight of interaction between drones i and j, A_{ij}, has a negative correlation with k_i^{in}. That is, when k_i^{in} is large, neighbor j has a minimal contribution to drone i, and vice versa. In this paper, we think A_{ij} is proportional to the inverse of the k_i^{in}. h_i^{in} denotes the number of communication types (such as WiFi, 5G, satellite communication and so on) between node i and its neighbors. The more types of communication, the bigger h_i^{in}. A higher h_i^{in} makes it a much harder to achieve attack by adversaries. So, h_i^{in} can contribute to enhance the resilience capacity of UAV swarm. In this paper, we think A_{ij} is proportional to k_i^{in}.

Based on the analysis of dynamical relationship between A_{ij} and d_{ij}, k_i^{in}, h_i^{in}, we take the form of Eq. (6) to model the weight topology of the UAV swarm.

$$A_{ij} = \begin{cases} \frac{h_i^{in}}{k_i^{in}} & ,d_{ij} \le d_c \\ \frac{h_i^{in}}{\left[\left(\frac{(d_{ij}-d_c)}{S}\right)^2 + 1\right] k_i^{in}}, & d_{ij} > d_c \end{cases} \quad (6)$$

3.3 Dynamics of information transmission

Information attacks are a regular occurrence in UAV swarm operations, indicating the likelihood of information tampering on drone i, with a range of $0 \le x_i(t) \le 1$. According to SIS, mapping the Eq. (1)

$$M_1\big(x_i(t)\big) = \beta(1 - x_i(t)), M_2\left(x_j(t)\right) = x_j(t) \quad (7)$$

When drone i is susceptible (with a probability of 1 - $x_i(t)$) and at least one of its neighbors j is infected (with a probability of $x_j(t)$), drone i can also become infected with a probability of

$$\sum_{j=1}^{N} A_{ij} M_1\big(x_i(t)\big) M_2\left(x_j(t)\right) = \sum_{j=1}^{N} A_{ij}\beta(1 - x_i(t))x_j(t) \quad (8)$$

So, the dynamic of information transmission between UAVs can be described as Eq. (8). With the A_{ij} expressed in Eq. (6), the dynamics of information transmission can be characterized in the form of Eq. (9).

$$\begin{cases} \sum_{j=1}^{N} \frac{h_i^{in}}{k_i^{in}}\beta(1 - x_i(t))x_j(t) & ,d_{ij} \le d_c \\ \sum_{j=1}^{N} \frac{h_i^{in}}{\left[\left(\frac{(d_{ij}-d_c)}{S}\right)^2 + 1\right] k_i^{in}}\beta(1 - x_i(t))x_j(t), & d_{ij} > d_c \end{cases} \quad (9)$$

The dynamic of UAV swarm is formed in Eq.(10).

$$\frac{dx_i(t)}{dt} = \begin{cases} -\sigma x_i(t)(1 - x_i(t))^2 + \sum_{j=1}^{N} \frac{h_i^{in}}{k_i^{in}}\beta(1 - x_i(t))x_j(t) ,d_{ij} \le d_c \\ -\sigma x_i(t)(1 - x_i(t))^2 + \sum_{j=1}^{N} \frac{h_i^{in}}{\left[\left(\frac{(d_{ij}-d_c)}{S}\right)^2 + 1\right] k_i^{in}}\beta(1 - x_i(t))x_j(t), d_{ij} > d_c \end{cases} \quad (10)$$

4. Resilience model of UAV swarm

The behavior of the UAV swarm is determined by Eq. (1), which is further explained in more detail in Eq.(10). The first component on the right-hand side of Eq.(10) represents the individual dynamics of each drone, while the second component represents the interactions between drone i and its neighboring drones. The parameters β and σ are not affected by the drones themselves and remain constant.

The fixed points of Eq.(10) are found by Eq.(10) to zero, namely as Eq.(11). $x_i(t)$, $i=1,\ldots,N$ is decided by β, σ, d_{ij}, k_i^{in}, h_i^{in}. β, σ reflect the dynamics of information transmission and d_{ij}, k_i^{in}, h_i^{in} relate to the topology and dynamic of UAV swarm system. The solution of Eq.(10) offers the i's resilience function $x_i(A_{ij})$.

$$\begin{cases} -\sigma x_i(t)(1 - x_i(t))^2 + \sum_{j=1}^{N} \frac{h_i^{in}}{k_i^{in}}\beta(1 - x_i(t))x_j(t) = 0 & ,d_{ij} \le d_c \\ -\sigma x_i(t)(1 - x_i(t))^2 + \sum_{j=1}^{N} \frac{h_i^{in}}{\left[\left(\frac{(d_{ij}-d_c)}{S}\right)^2 + 1\right] k_i^{in}}\beta(1 - x_i(t))x_j(t) = 0, & d_{ij} > d_c \end{cases} \quad (11)$$

During the mission, the topology of UAV swarm changes with time, and the d_{ij}, k_i^{in}, h_i^{in} are three time-varying factors, which can be rewritten to d^t_{ij}, $k_i^{in,t}$, $h_i^{in,t}$. The solution of Eq.(11) provides Eq. (12).

$$x_i(t) = \begin{cases} 1 - \frac{\beta}{\sigma}\sum_{j=1}^{N} \frac{h_i^{in,t}}{k_i^{in,t}} & ,d_{ij} \le d_c \\ 1 - \frac{\beta}{\sigma}\sum_{j=1}^{N} \frac{h_i^{in,t}}{\left[\left(\frac{(d^t_{ij}-d_c)}{S}\right)^2 + 1\right] k_i^{in,t}}, & d_{ij} > d_c \end{cases} \quad (12)$$

$x_i(t)$ represents the possible states of drone i as a solution of Eq.(10). $x_i(t)$ shows that the activities of the UAV swarm depend on the topology and the dynamics. In this paper, any modifications in β, σ, d^t_{ij}, $k_i^{in,t}$, $h_i^{in,t}$, which correspond to different types of disturbances, will elicit an unpredictable reaction from the UAV swarm. Such disturbances can severely damage the resilience of the UAV swarm. For example, when

a swarm perform a surveillance mission, drones could be attacked inevitability and unpredictably. For instance, during a surveillance mission, the drones in the swarm can be attacked unexpectedly and unavoidably. These attacks have the potential to disrupt or affect the communication link between the attacked drones and the unaffected ones, or even completely remove the attacked drones from the swarm. Once removed, these drones become incapable of contributing to the surveillance mission, resulting in a reduction or interruption of the mission itself. During the surveillance mission, the attacked or infected drones are unable to fulfill their tasks, and the performance of the swarm relies heavily on the unaffected drones. So, Thus, the resilience of a UAV swarm can be assessed by the susceptible drone variable, $x_i^s(t)$. In this paper, we consider the average value of $x_i^s(t)$ as an indicator of the resilience of a UAV system. That is

$$\langle x \rangle = \frac{1}{N}\sum_{s=1}^{N} x_s(t) =$$

$$\frac{1}{N}\sum_{s=1}^{N}\begin{cases} 1-\frac{\beta}{\sigma}\sum_{j=1}^{N}\frac{h_s^{in,t}}{k_s^{in,t}} & ,d_{ij} \le d_c \\ 1-\frac{\beta}{\sigma}\sum_{j=1}^{N}\frac{h_s^{in,t}}{\left[\left(\frac{\left(d_{ij}^t-d_c\right)}{s}\right)^2+1\right]k_s^{in,t}}, & d_{ij} > d_c \end{cases} \quad (13)$$

$\langle x \rangle$ is the function of β, σ, d_{sj}^t, $k_s^{in,t}$, $h_i^{in,t}$, exposing the resilience of the UAV swarm depends on the topology, weights, and the system's dynamic. d_{sj}^t, $k_s^{in,t}$, $h_i^{in,t}$ are the parameters of susceptible drones at time t.

5. Case study

In this section, we present an experiment conducted using a multi-agent simulation where a UAV swarm over a battlefield area to perform surveillance. Each UAV independently carries out the surveillance task within the designated battlefield zone. The drones are able to collaborate and successfully complete the surveillance mission through communication links that facilitate the exchange of information between them, as depicted in Fig. 1. In Section 5.1, we provide the background information on the experiment and case settings. Section 5.2 presents the simulation results, comparisons of results, as well as detailed discussions.

5.1. Mission background and experiment settings

We applied the proposed method in a scenario where a UAV swarm is assigned to maintain surveillance in a battlefield, as depicted in Fig. 7.

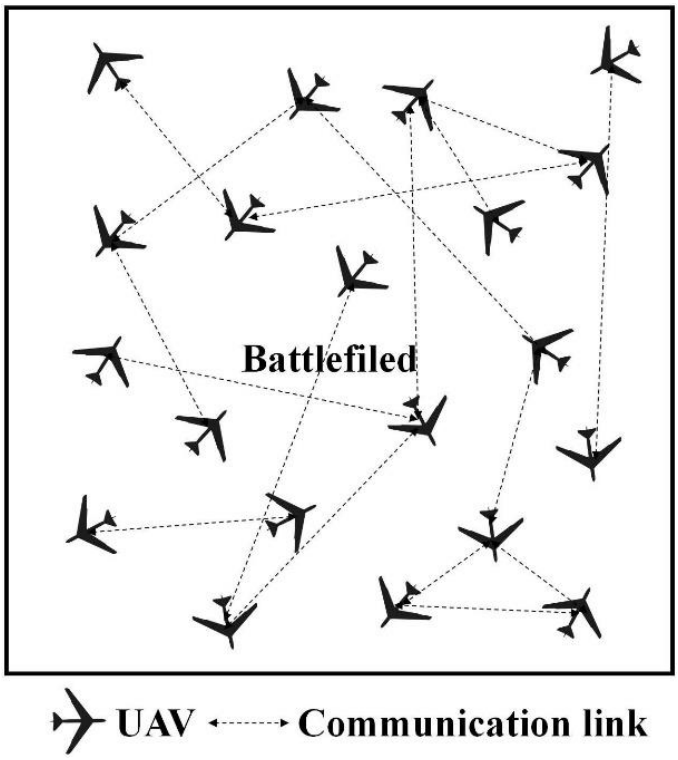


Fig. 7. Surveillance mission over a specified battlefield.

In Fig. 7, the drones are interconnected through a Mobile Ad Hoc Network (MANET), allowing them to share information during the mission. MANET refers to a wireless network comprising a collection of mobile nodes that are connected wirelessly, independent of any fixed infrastructure. It possesses the remarkable ability to self-configure and self-heal. Each node actively participates in routing by forwarding data for other nodes. Within a MANET, every drone has the freedom to move independently in any direction, resulting in frequent changes in its links to other drones. The determination of which nodes should forward data is dynamically made based on network connectivity and the routing algorithm employed.

The complex networks approach is widely applied to model several real-world systems. Tran et al.[28] applied a complex networks approach to model three different scenarios of the UAV swarm. They generated the initial network topology using scale-free networks with preferential attachment[4,5]. The network damage is implemented by removing drones in a targeted manner[29], with a preference for removing drones with a higher number of neighbors during each threat event. For network recovery, link rewiring is conducted in a preferential

manner[30], prioritizing the rewiring of drones with a higher number of neighbors. In this paper, we adopt the initial swarm topology with scale-free networks used in[28,29]. Initially, the swarm consists of m_0 fully connected nodes, and when a new drone joins the existing network, it introduces m (where $m \leq m_0$) links. The probability of the newcomer drone, j, linking with an existing drone, i, is determined as:

$$P_{j\to i} = \frac{k_i}{\sum_{l=1}^{N_t} k_l} \quad (14)$$

The objective of the swarm is to effectively monitor the entire battlefield, reducing any blind spots. The number of surviving drones serves as a performance metric for assessing the resilience of the UAV swarm. In this paper, we quantify the resilience of a UAV system by considering the average value of $x_i^s(t)$, namely $\langle x \rangle$. $\langle x \rangle$ is the function of β, σ, d_{sj}^t, $k_s^{in,t}$, $h_i^{in,t}$, exposing the resilience of the UAV swarm depends on the topology, weights, and the system's dynamic. d_{sj}^t, $k_s^{in,t}$, $h_i^{in,t}$ are the parameters of susceptible drones at time t. Other information is given as follows:

- Initially, N drones are dispersed across the battlefield at the beginning of the task, and then proceed to navigate using a random walk search pattern throughout the surveillance mission.
- The battlefield zone is a square grid with size S = 1000 × 1000 patches. The vehicle moves with a rate of v patch/s, surveils $s \times s$ patches of battlefield.
- There are formidable ground opponents who possess strong defense capabilities. The attacks are unpredictable, occurring at random intervals. When an attack targets one UAV, it propagates through communication links in the form of SIS. Consequently, the targeted UAV is temporarily incapacitated, unable to monitor the battlefield.
- The information is transmitted between drones using Wi-Fi, Bluetooth and ZigBee, which are the most common communication types.

The presented model and the experiment settings are simulated in MTALAB 2021, Windows 10, 11th Gen Intel(R) Core i7-1165G7 @ 2.80 GHz, 16 GB RAM. The experiment terminates after the disruption-restore events. In this experiment, a drone is randomly attacked by an adversary, resulting in the infection of its links. This marks the onset of disruption. Subsequently, the infected information spreads throughout the UAV by the means of SIS. Simultaneously, the swarm employs resilience technologies to restore the infected drones to a susceptible state, with a probability denoted as σ. As the spreading reaches equilibrium, the swarm transitions into a new stable state. The parameters setting for the mission and swarm are given in Table 1.

Table 1. Parameters for the mission and swarm.

Parameter	Value
N	100
m_0	10
m	2
v	random from 0 to 10
s	20
σ	0.1
β	0.15
$h_i^{in,t}$	1

A simulation is characterized by a distinct set of inputs provided to the model. The simulation concludes upon the completion of disruption-recovery events. As the simulation is stochastic in nature, 10 repetitions are conducted for each scenario. The stochasticity arises from randomness in the random walk, the BA algorithm, node removals, and the SIS algorithm. The total number of susceptible UAVs is acquired for each step during the simulation. Subsequently, we obtain the resilience values of $\langle x \rangle$ by Eq. (13).

5.2. Results and analysis

5.2.1. Case

In the first example, we assume all d_{ij} is below d_c, that is $d_{ij} \leqslant d_c$, and

$$\langle x \rangle = \frac{1}{N}\sum_{s=1}^{N}\left(1 - \frac{\beta}{\sigma}\sum_{j=1}^{N}\frac{h_s^{in,t}}{k_s^{in,t}}\right) \quad (15)$$

In order to mitigate the influence of stochasticity in the BA algorithm, we performed simulations using four distinct BA networks. The outcomes obtained with various initially attacked UAVs are illustrated in Fig. 8.

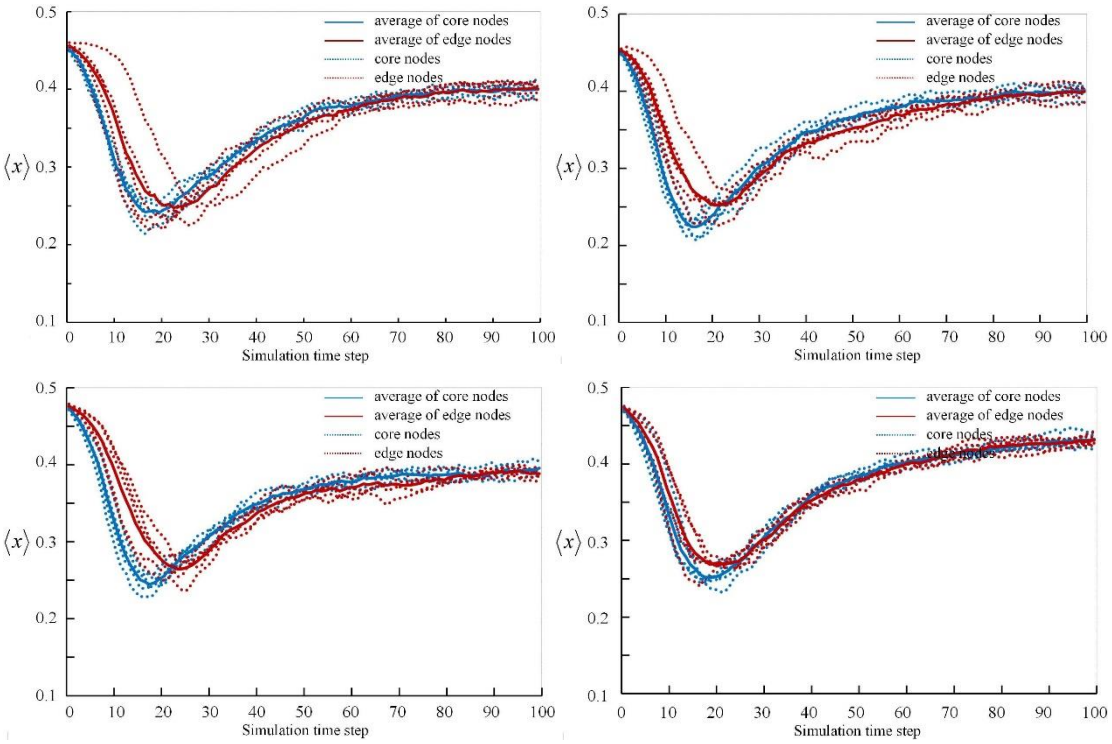


Fig. 8. $\langle x \rangle$ with $d_{ij} \leqslant d_c$ under different initial attacked UAV.

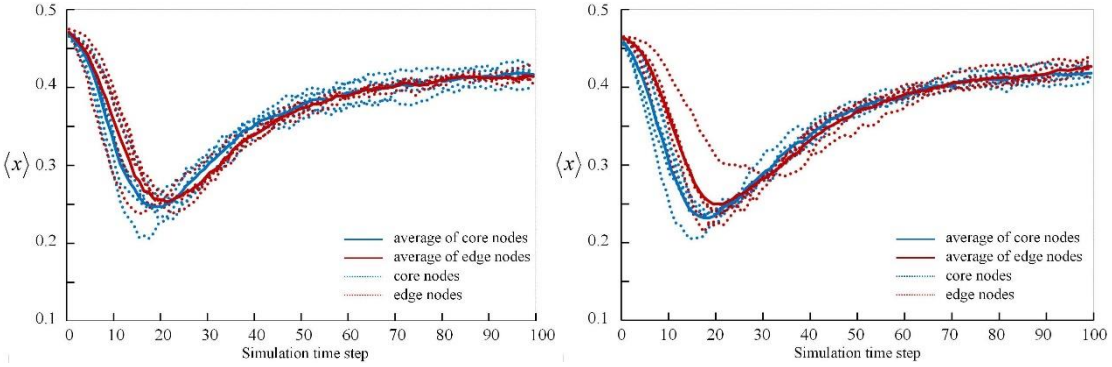
In Fig. 8, the blue dashed lines represent the simulation results of the core nodes (the top 5 according to incoming degree), averaged 10 replications for each case. The blue solid line represents the average of the blue dashed line. Similarly, the red dashed lines represent the simulation results of the edge nodes (the bottom 5 according to incoming degree), averaged over 10 replications for each case. The red solid line represents the average of the red dashed line. As shown in Fig. 8, when the attack begins at core nodes, the resilience of the swarm decreases more rapidly compared to that of edge nodes. Additionally, when the attack originates from edge UAVs, the performance of the swarm varies significantly. This may be due to the fact that core nodes are able to spread the attack more quickly through their numerous neighbors compared to edge nodes. These conclusions hold true for all subgraphs in Fig. 8. Although the network topologies of the four subgraphs differ, the comparison among them shows minimal disagreement. Therefore, it can be concluded that the network topology has no influence on the performance of the UAV swarm.

5.2.2. Case 2

Renew the assumption of all d_{ij} is below 100, and d_c is 0, that is

$$\langle x \rangle = \frac{1}{N}\sum_{s=1}^{N}\left(1-\frac{\beta}{\sigma}\sum_{j=1}^{N}\frac{h_s^{in,t}}{\left[\left(\frac{d_{ij}^t}{S}\right)^2+1\right]k_s^{in,t}}\right) \tag{16}$$

To mitigate the impact of stochasticity in the initial position, we conducted simulations using four distinct initial position networks. The results, illustrating various initial attacked UAVs, are presented in Fig. 9.



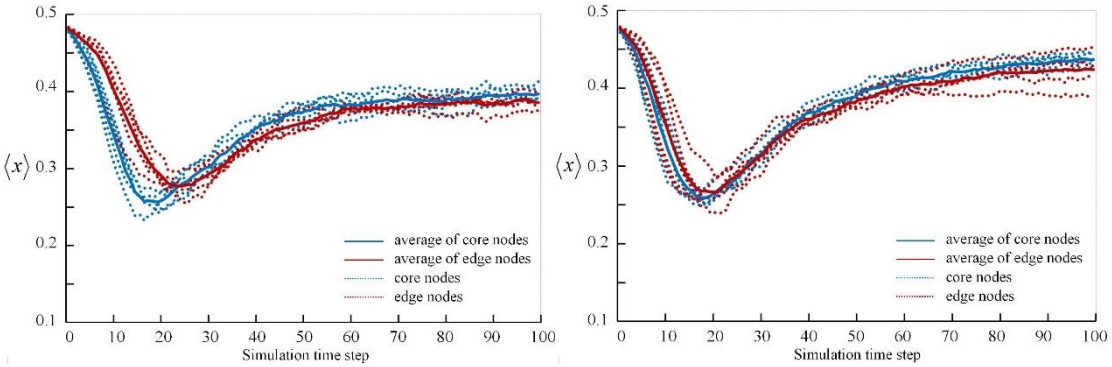


Fig. 9. $\langle x \rangle$ with d_c=0.

In Fig. 9, the lines have the same meaning as in Fig. 8. As shown in Fig. 9, we can draw similar conclusions as in Fig. 8. Additionally, the initial positions of the four subgraphs are different. The results indicate that the distinction between core nodes and edge nodes is little. The comparison reveals negligible discrepancies with varying initial positions. Thus, the initial position of the swarm has little impact on the results, providing strong support for the conclusion of d_c=0.

5.2.3. Case 3

Taking the assumption of d_{ij} is at random, that is

$$\langle x \rangle = \frac{1}{N}\sum_{s=1}^{N} \begin{cases} 1 - \frac{\beta}{\sigma}\sum_{j=1}^{N} \frac{h_s^{in,t}}{k_s^{in,t}} & ,d_{ij} \le d_c \\ 1 - \frac{\beta}{\sigma}\sum_{j=1}^{N} \frac{h_s^{in,t}}{\left[\left(\frac{\left(d_{ij}^t - d_c\right)}{s}\right)^2 + 1\right] k_s^{in,t}} & ,d_{ij} > d_c \end{cases} \quad (17)$$

To eliminate the impact of stochasticity in the BA algorithm and the initial position, we performed simulations using four different initial position networks and the BA algorithm. Fig. 10 displays the results obtained when different initial attacked UAVs were employed. These results demonstrate a similarity to case 2, thereby further validating the credibility of the conclusion.

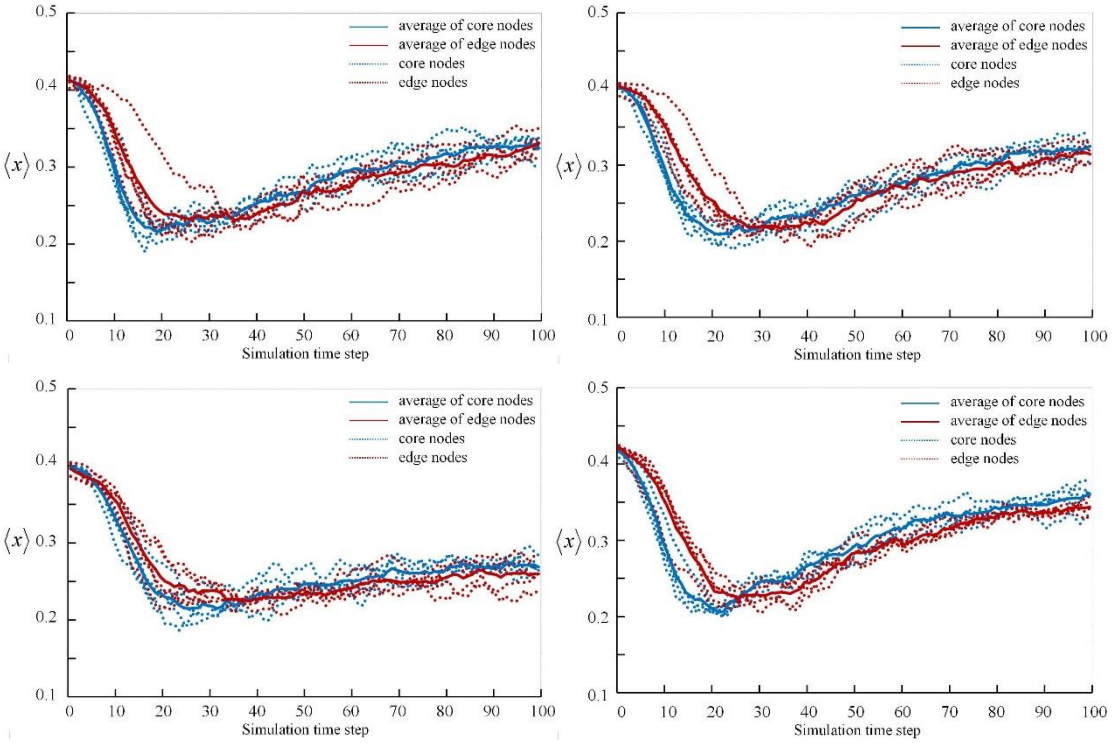


Fig. 10. $\langle x \rangle$ with changing d_{ij}.

A careful comparison of Fig. 8 - Fig. 10 highlights some significant findings. It becomes evident that the communication range plays a crucial role in both system performance and resilience. A greater communication range can greatly enhance the anti-interference capability of a UAV swarm. Additionally, the core nodes are found to have a more pivotal role in

information propagation as compared to the edge nodes. This underscores the fact that the system's performance and resilience are heavily reliant on these core nodes.

6. Future work

In this study, we focus on the performance decrease of the UAV swarm caused by inevitable disruptive events and uncertain threats such as malicious attacks by enemies. However, SIS model is a brief and incomplete account of malicious attacks propagation in a UAV swarm, the actual situations are more complicated. Additionally, we did not consider the interplay between the incoming degrees and the communication types. Finally, the dynamics of a UAV Swarm are the key factors of swarm resilience, its study is still a big challenge for researchers. In the further, we plan to study a more realistic situation of malicious attacks and try to make a step forward in dynamics of UAV swarms.

7. Conclusions

This article discusses the resilience performance of against malicious disturbances in drones or links attacks, which are responsible for causing resilience loss. We consider the dynamic states of the swarm and the real-time position of the topology, and propose an enhanced UAV swarm resilience model that incorporates the impact of topology, system dynamics, and SIS into the complex network model. This model effectively captures changes in network topology and system dynamics caused by malicious attacks. We conducted an experimental study in which a UAV swarm carried out a surveillance mission, and the simulation results affirm the credibility of our approach. Moving forward, our focus will be on achieving resilience in a UAV swarm under more complex forms of information propagation.

Definitions/Abbreviations

UAV – unmanned aerial vehicle
SIS – Susceptible → Infected → Susceptible
USIEN – unmanned swarm information exchange network
S-C – data transmission links between sensor and controller
C-A – data transmission links between controller and actuator
C-C – data transmission links between controller and controller
MANET – Mobile Ad Hoc Network

References

1. Bai A., Luo Y., Zhang H., Li Z., L 2 - gain robust trajectory tracking control for quadrotor UAV with unknown disturbance. Asian Journal of Control; 24(2022):3043-3055. https://doi.org/10.1002/asjc.2711.
2. Bai C., Yan P., Yu X., Guo J., Learning-based resilience guarantee for multi-UAV collaborative QoS management. Pattern Recognition; 122(2022)108166. https://doi.org/10.1016/j.patcog.2021.108166.
3. Bai G., Li Y., Fang Y., Zhang Y-A., Tao J., Network approach for resilience evaluation of a UAV swarm by considering communication limits. Reliability Engineering & System Safety; 193(2020)106602. https://doi.org/10.1016/j.ress.2019.106602.
4. Barabási A-L., Albert RJs., Emergence of scaling in random. Networks.science; 286(1999)509-512. https://doi.org/10.1126/science.286.5439.509.
5. Barabási A-L., Albert R., Jeong HJPASM., Applications i., Mean-field theory for scale-free random networks. Physica A: Statistical Mechanics and its Applications; 272(1999) 173-187. https://doi.org/10.1016/S0378-4371(99)00291-5.
6. Barzel B., Barabási A., Universality in network dynamics. Nature Physics; 9(2013)673-681. https://doi.org/10.1038/nphys2741.
7. Bossens DM., Ramchurn S., Tarapore DJCRR., Resilient robot teams: a review integrating decentralised control, change-detection, and learning. Current Robotics Reports; 3(2022)85-95. https://doi.org/10.1007/s43154-022-00079-4.
8. Chebbi J., Briere Y., Robust active disturbance rejection control for systems with internal uncertainties: Multirotor UAV application. Journal of Field Robotics; 39(2022):426-456. https://doi.org/10.1002/rob.22058.
9. Chen X., Tang J., Lao SJAS., Review of unmanned aerial vehicle swarm communication architectures and routing protocols. Applied

Sciences; 10(2020)3661. https://doi.org/10.3390/app10103661.
10. Cohen R., Erez K., Ben-Avraham D., Havlin S., Resilience of the internet to random breakdowns. Physical review letters; 85(2000)4626. https://doi.org/10.1103/PhysRevLett.85.4626.
11. da Fontoura Costa L., Reinforcing the resilience of complex networks. Physical Review E; 69(2004)066127. https://doi.org/10.1103/PhysRevE.69.066127.
12. Dui H., Zhang C., Bai G., Chen L., Mission reliability modeling of UAV swarm and its structure optimization based on importance measure. Reliability Engineering & System Safety; 215(2021)107879. https://doi.org/10.1016/j.ress.2021.107879.
13. Gao J., Barzel B., Barabási A-L. Universal resilience patterns in complex networks. Nature; 530(2016) 307-312. https://doi.org/10.1038/nature16948.
14. Harush U., Barzel B., Dynamic patterns of information flow in complex networks. Nature communications; 8(2017):1-11. https://doi.org/10.1038/s41467-017-01916-3.
15. Hua Y., Dong X., Li Q., Ren Z., Distributed adaptive formation tracking for heterogeneous multiagent systems with multiple nonidentical leaders and without well‐informed follower. International Journal of Robust and Nonlinear Control; 30(2020)2131-2151. https://doi.org/10.1002/rnc.4891.
16. Kephart JO., White SR., Directed-graph epidemiological models of computer viruses. In: Computation: the micro and the macro view. Computation: the micro and the macro view; (1992)71-102. https://doi.org/10.1142/9789812812438_0004.
17. Kopeikin A., Clare A., Toupet O., How J., Cummings M., Flight testing a heterogeneous multi-UAV system with human supervision. AIAA Guidance, Navigation, and Control Conference; (2012)4825. https://doi.org/10.2514/6.2012-4825.
18. Li X., Chen C., Lyu Y., Xie KJIJoR., Control N., Event‐based resilience to DoS attacks on communication for consensus of networked Lagrangian systems. International Journal of Robust and Nonlinear Control; 31(2021)1834-1850. https://doi.org/10.1002/rnc.5013.
19. Li Y., St-Hilaire M., Kunz T., Improving routing in networks of UAVs via scoped flooding and mobility prediction. 2012 IFIP Wireless Days. IEEE; (2012)1-6. https://doi.org/10.1109/WD.2012.6402827.
20. Ma X., Dong W., Jin M., et al., Consensus tracking control for uncertain non‐strict feedback multi‐agent system under cyber attack via resilient neuroadaptive approach. International Journal of Robust and Nonlinear Control; 32(2022) 4251-4280. https://doi.org/10.1002/rnc.6035.
21. Mukherjee A., Misra S., Chandra VSP., Obaidat MS., Resource-optimized multiarmed bandit-based offload path selection in edge UAV swarms. IEEE Internet of Things Journal; 6(2018)4889-4896. https://doi.org/10.1109/JIOT.2018.2879459.
22. Ordoukhanian E., Madni AM., Introducing resilience into multi-UAV system-of-systems network. In: Disciplinary Convergence in Systems Engineering Research. Disciplinary Convergence in Systems Engineering Research. Springer International Publishing; (2018)27-40. https://doi.org/10.1109/ISSE46696.2019.8984509.
23. Ordoukhanian E., Madni AM., Model-based approach to engineering resilience in multi-UAV systems. Systems; 7(2019)11. https://doi.org/10.3390/systems7010011.
24. Ordoukhanian E., Madni AM., Resilient multi-UAV operation: key concepts and challenges. 54th AIAA Aerospace Sciences Meeting; (2016)0475. https://doi.org/10.2514/6.2016-0475.
25. Phadke A., Medrano FAJD., Towards Resilient UAV Swarms—A Breakdown of Resiliency Requirements in UAV Swarms. Drones; 6(2022)340. https://doi.org/10.3390/drones6110340.
26. Ren Y., Zhang K., Jiang B., Cheng W., Ding Y., Distributed fault‐tolerant time‐varying formation control of heterogeneous multi‐agent systems. International Journal of Robust and Nonlinear Control. International Journal of Robust and Nonlinear Control; 32(2022)2864-2882. https://doi.org/10.1002/rnc.5870.
27. Sadrollah GP., Barca JC., Khan AI., Eliasson J., Senthooran I., A distributed framework for supporting 3D swarming applications. 2014 International Conference on Computer and Information Sciences (ICCOINS); IEEE, (2014)1-5. https://doi.org/10.1109/ICCOINS.2014.6868347.
28. Tran HT., A complex networks approach to designing resilient system-of-systems. Georgia Institute of Technology; 2015. http://hdl.handle.net/1853/54384.
29. Tran HT., Domerant JC., Mavris DNJPCS., A Network-based Cost Comparison of Resilient and Robust System-of-Systems. Procedia

Computer Science; 95 (2016)126-133. https://doi.org/10.1016/j.procs.2016.09.302.

30. Tran HT., Domerçant JC., Mavris DNJTJoDM., Simulation., Evaluating the agility of adaptive command and control networks from a cyber complex adaptive systems perspective. The Journal of Defense Modeling and Simulation; 12 (2015)405-422. https://doi.org/10.1177/1548512915592517.
31. Vachtsevanos G., Lee B., Oh S., Balchanos MJJoI., Systems R. Resilient design and operation of cyber physical systems with emphasis on unmanned autonomous systems. Journal of Intelligent & Robotic Systems; 91(2018)59-83. https://doi.org/10.1007/s10846-018-0881-x.
32. Valavanis KP., Vachtsevanos GJ., Handbook of unmanned aerial vehicles. Dordrecht: Springer Netherlands; 1(2015). https://doi.org/10.1007/978-90-481-9707-1.
33. Wierman JC., Marchette DJ., Modeling computer virus prevalence with a susceptible-infected-susceptible model with reintroduction. Computational statistics & data analysis; 45(2004)3-23. https://doi.org/10.1016/S0167-9473(03)00113-0.
34. Xu B., Bai G., Fang Y., Tao J., Failure analysis of unmanned autonomous swarm considering cascading effects. Journal of Systems Engineering and Electronics; 33(2022):759-770. https://doi.org/10.23919/JSEE.2022.000069.
35. Xu B., Liu T., Bai G., Tao J., Zhang Y-a., Fang Y., A multistate network approach for reliability evaluation of unmanned swarms by considering information exchange capacity. Reliability Engineering & System Safety; 219(2022)108221. https://doi.org/10.1016/j.ress.2021.108221.
36. Zhen Z., Chen Y., Wen L., Han B., An intelligent cooperative mission planning scheme of UAV swarm in uncertain dynamic environment. Aerospace Science and Technology; 100(2020)105826. https://doi.org/10.1016/j.ast.2020.105826.
37. Zhu Q., Yang X., Ren JJCiNS, Simulation N., Modeling and analysis of the spread of computer virus. Communications in Nonlinear Science and Numerical Simulation; 17(2012)5117-5124. https://doi.org/10.1016/j.cnsns.2012.05.030.
38. Zou Y., Meng Z., Distributed hierarchical control for multiple vertical takeoff and landing UAVs with a distance‐based network topology. International Journal of Robust and Nonlinear Control; 29(2019)2573-2588. https://doi.org/10.1002/rnc.4513.