

Article

Vulnerability Analysis of UAV Swarm Network with Emergency Tasks

Jinglei Li ¹, Qingfeng Yue ¹, Zijia Huang ^{2,*}, Xiaoyu Xie ¹ and Qinghai Yang ¹

¹ The School of Telecommunications Engineering, Xidian University, Xi'an 710071, China; jlli68@xidian.edu.cn (J.L.); 21181214288@stu.xidian.edu.cn (Q.Y.); h578960@163.com (X.X.); qhyang@xidian.edu.cn (Q.Y.)

² The 20th Research Institute of China Electronics Technology Group Corporation, Xi'an 710068, China

* Correspondence: beiyouhzj@163.com

Abstract: With the rapid development of Unmanned Aerial Vehicle (UAV) technology, UAV swarms are used for emergency tasks in various scenarios such as area detection, fire rescue, logistics, and transportation. However, for complex scenarios, UAV swarms are prone to environmental interference that damages their equipment or disrupts their communication links, affecting the normal execution of tasks. In this paper, an information–communication interdependent network model is designed for the vulnerability analysis of UAV swarm networks with emergency tasks. Firstly, from the perspective of network functions of a UAV swarm, we introduce the theory of interdependent networks to abstract the relationship between the UAV swarm's communication network and its information network, where the communication network represents its communication topology and the information network is related to the function of each UAV individual in the UAV swarm. Then, the vulnerability of the UAV swarm is analyzed according to the relationship between network construction costs and network connectivity under environmental interference. Finally, the effectiveness of the vulnerability analysis method is verified through simulation.

Keywords: UAV swarm network; vulnerability analysis; emergency tasks; interdependent network model



Citation: Li, J.; Yue, Q.; Huang, Z.; Xie, X.; Yang, Q. Vulnerability Analysis of UAV Swarm Network with Emergency Tasks. *Electronics* **2024**, *13*, 2005. <https://doi.org/10.3390/electronics13112005>

Academic Editor: Mahmut Reyhanoglu

Received: 22 April 2024

Revised: 9 May 2024

Accepted: 11 May 2024

Published: 21 May 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Unmanned Aerial Vehicle (UAV) swarms, composed of interconnected UAVs coordinated through communication and control systems, efficiently achieve specific tasks or goals. When UAVs fly individually, their limited energy supply constrains their flight distance and operational range. Furthermore, they are susceptible to various interferences, and their communication reliability is relatively low. UAV swarms can achieve collaborative interaction among all nodes through advanced open communication networks, enabling fast and efficient task completion while possessing strong scalability and robustness. For instance, they are used for emergency tasks in various scenarios, such as area detection [1], fire rescue [2], and transportation [3]. For emergency tasks, the quality of communication between UAVs can be disrupted by different environmental factors, such as electromagnetic interference, adverse weather conditions, and geographical obstacles, hindering coordination and information exchange among UAVs. Environmental interference in emergency tasks poses significant challenges to the communication networks of UAV swarms. Meanwhile, the diverse functionalities of individual entities within UAV swarms play distinct roles in emergency tasks, collectively impacting the overall task. Therefore, we need to analyze the vulnerability of UAV network links to ensure that they can work with maximum efficiency in the case of a link failure.

In the early network vulnerability analysis models, all the nodes in the network were classified into one class. The vulnerability assessment method based on expert experience is mainly through the common vulnerability scoring system to assess network

vulnerability [4]. Model-based vulnerability analysis methods mainly include the fractal mechanism-based vulnerability analysis method [5], the general attack tree model-based vulnerability analysis method [6,7], the Bayesian network-based vulnerability analysis method [8], and the cascading failure model-based vulnerability analysis method [9,10]. However, in the real world the composition of many networks is very complex, so it is not appropriate to describe them simply as a single isolated network. Therefore, we need to discuss the classification of UAV nodes in the network and analyze it from the perspective of interdependent networks.

Interdependent networks have been applied to various application scenarios. Zhao studied the vulnerability of a space information network coupled with a communication network and a function network and proposed the concept of the task component [11]. Chen proposed a novel model to investigate the cascading failures in interdependent power grids and communication networks and identified the vital nodes from the perspective of network robustness [12,13]. Reference [14] introduced interdependent networks into scenarios of network cascading failures and studied the effect of degree heterogeneity on the structural vulnerability of interdependent networks when they suffer targeted interference. Building upon this, Liu constructed a two-layer asymmetric dependent network model for unidirectional dependent UAV network physical systems, but did not consider interdependent decision making among clusters [15]. Xing attempted to combine weight analysis methods with interdependent networks, constructed a double-layer dependent network with weights, proposed a cascading failure model, considering node overload and node repair, and constructed three improved strategies based on the weight-based load redistribution strategy [16]. This framework is efficiently applicable to time-dependent multiplex networks. Jia began to analyze networks from the perspective of node and link connectivity. Jia studied the effects of the interdependency characteristics of cross-layer nodes, the connectivity characteristics of intra-layer nodes, the interdependency characteristics of intra-layer nodes, and attack strategies on cascading dynamics [17]. Yang studied interdependent networks based on physical networks and logical networks and analyzed the cascading failure of the model [18]. Zou designed different key fragile dependency links removal strategies based on the assessment of links [19]. And reference [20] presented a method for evaluating the robustness, vulnerability, and efficiency of multi-layer infrastructures using various probabilistic evaluation measures to tackle cascading problems in interdependent critical systems. In general, these studies mainly focused on vulnerability prevention, and did not conduct targeted research on the vulnerability analysis of the network after cascading failures.

In this paper, to effectively convey the functions of UAVs in executing emergency tasks, we combined interdependent networks with UAV networks for our research. According to the network characteristics of the UAV swarm network, in addition to the communication ability between network nodes, situational awareness and the information sharing of the UAV swarm are other major features of the swarm network. For a UAV swarm, a single UAV in the swarm networks is both a network node for communication and a node for information perception and processing [21]. The network can be divided into two layers: a communication network and an information network, where the communication network represents its communication topology influenced by the UAVs' motion trajectory, and where the information network is related to the function of each UAV in the normal execution of emergency tasks. Aiming at the network vulnerability analysis of a UAV swarm with emergency tasks, we have designed a network model of information–communication interdependence, and a link redistribution rule is proposed.

The rest of paper is organized as follows. Section 2 introduces the system model and problem formulation discussed in this paper. Section 3 details the information–communication interdependent network. Section 4 describes the whole network vulnerability analysis process. Experimental results and evaluations are presented in Section 5. Finally, the entire paper is summarized in Section 6.

2. System Model and Problem Formulation

The primary aim of this section is to model the UAV swarm network and its link data capacity, as well as formulating the corresponding problem. This will enable further research on cascading failure and simulation experiments.

2.1. System Model

2.1.1. UAV Swarm Networks

In rescue scenarios, for a UAV swarm, an individual UAV within the system serves not only as a communication network node but also as a node for information perception and processing. In communication networks, the communication links between nodes form the network's topology, responsible for data transmission across the entire network. And in information networks, nodes are responsible for sensing, processing environmental information, and sharing it with other UAVs, primarily tasked with executing network tasks. Information network nodes have faster information processing speeds and stronger task execution capabilities, providing input information for the network. Communication network nodes have a broader communication range and higher-quality communication, serving as intermediary nodes to assist information network nodes in information exchange. The mutual dependence between the two networks forms the information–communication interdependent model of UAV swarm networks: the lower layer constitutes a communication network consisting of UAV nodes and communication links, while the upper layer forms a functional network composed of information perception and processing nodes carrying task payloads and their information–interaction relationships.

As shown in Figure 1, fire rescue is a common emergency task scene. In complex environments like high-rise buildings and outdoor settings, safely implementing firefighting measures has always been a global challenge. UAVs, due to their rapid deployment and flexible operations, can execute multi-UAVs coordinated firefighting strategies for different fire scenarios [2].

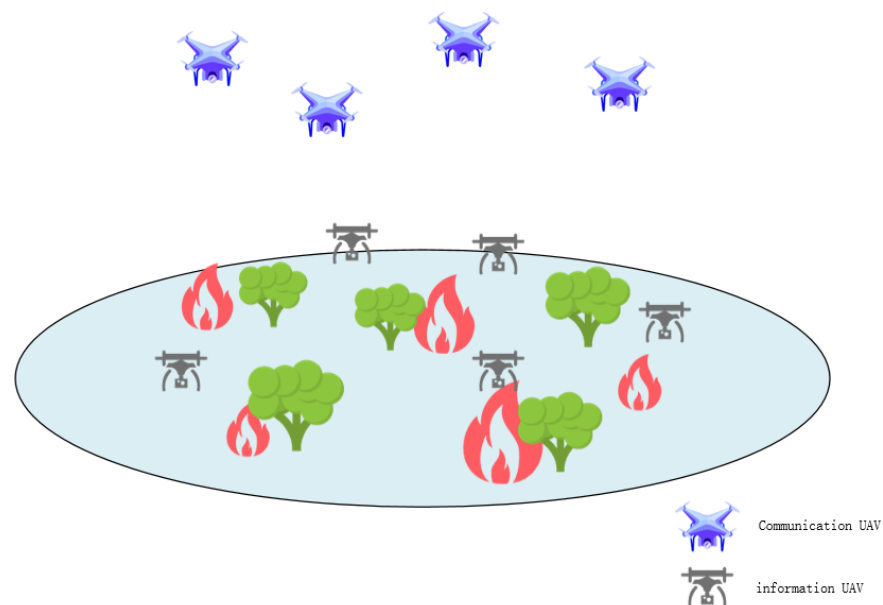


Figure 1. UAV swarm fire rescue scenario.

The communication topology structure of a UAV swarm network is represented by undirected graph G_P , which is composed of the UAV nodes set V_P and the communication links set E_P , and G_P can be expressed as $G_P = (V_P, E_P)$. If the undirected graph G_P contains n nodes, $V_P = \{v_i | i = 1, 2, \dots, n\}$. E_P is the set of communication links in the UAV swarm network, and it can be expressed as $E_P = \{e_{ij}^P | e_{ij}^P = (v_i, v_j), v_i, v_j \in V_P\}$. There can only be

at most one link between two communication nodes in a communication network. The information network of a UAV swarm system can be expressed as $G_F = (V_F, E_F)$. The information nodes are mapped from UAV nodes according to different functions, indicating the different functions of the UAV nodes due to the different task load equipment. If the information network G_F contains m nodes, $V_F = \{v_j | j = 1, 2, \dots, m\}$. The information node has certain information-interaction and information-sharing relationships, which can meet the task requirements of the UAV swarm network. The information interaction between UAV nodes with different functions can be represented by information links, denoted as $E_F = \{e_{ij}^F | e_{ij}^F = (v_i, v_j), v_i, v_j \in V_F\}$.

2.1.2. Link Capacity Model

Motter proposed a cascading failure model, also known as the ML (Motter–Lai) model [9]. He applied it to a scale-free network and a uniform network, respectively. In this model, the initial load L_i is defined by the global characteristic variable betweenness B_i . The initial load of node i in the ML model is formulated as

$$L_i = B_i \quad (1)$$

where B_i is node v_i 's betweenness and L_i represents the node i 's initial data transmission capability. The two variables exhibit a strong positive correlation. For example, the connecting hub of two subnetworks may be a node or a link, although the number of nodes or links connected to it is relatively small. If the node fails or the link is interrupted, connection failure between two small networks may ensue. Therefore, the node plays an extremely important role in the network. The interface number reflects the influence and force of a node or link in the entire network, and it represents the traffic volume of a node or a link. In task execution, communication UAVs, due to their higher computing capabilities, are responsible for calculating the load capacity of various links, and there is a periodic update of the computation results for each UAV in the entire network by communication.

However, in the UAV swarm information–communication interdependent network model, due to the coupling links between the two layers of the network, the initial data transmission capability of the network link needs to be redefined. Firstly, it is assumed that the coupling strength ω_{ij} on the coupling link e_{ij} of the dependent network is related to the node number of UAV nodes at both ends, and the formula is

$$\omega_{ij} = (B_i B_{ij})^\alpha \quad (2)$$

where B_i is node v_i 's betweenness, B_{ij} is link e_{ij} 's betweenness, and α is the weight that controls the coupling strength.

The node betweenness B_i is defined as the number of shortest paths through node v_i in the network; it can be expressed as

$$B_i = \sum_{j \neq i, k \neq i} \frac{\theta_{jk}(i)}{\theta_{jk}} \quad (3)$$

where $\theta_{jk}(i)$ is the number of shortest paths passing through node v_i in the shortest paths between node v_j and node v_k , and θ_{jk} is the number of shortest paths between node v_j and node v_k .

The link betweenness B_{ij} is defined as the number of shortest paths through link e_{ij} in the network; it can be expressed as

$$B_{ij} = \sum_{k \neq i, j, l \neq i, j} \frac{\theta_{kl}(e_{ij})}{\theta_{kl}} \quad (4)$$

where $\theta_{kl}(e_{ij})$ is the number of shortest paths passing through link e_{ij} in the shortest paths between node v_k and node v_l , and θ_{kl} is the number of shortest paths between node v_k and node v_l .

Taking node 4 in Figure 2 as an example, this network consists of seven nodes. Assuming that this network is a communication network, its adjacency matrix E_P is as shown in Table 1. There are three shortest paths between node 1 and node 6, with one of them passing through node 4. Similarly, there are three shortest paths between node 2 and node 6, node 1 and node 7, and node 2 and node 7, all of which pass through node 4. After calculation, the node betweenness centrality of node 4 is found to be 1.33. Likewise, for the link between node 2 and node 4, there is one shortest path passing through this link between node 1 and node 6, and another one between node 1 and node 7. After calculation, the B_{24} is found to be 0.67.

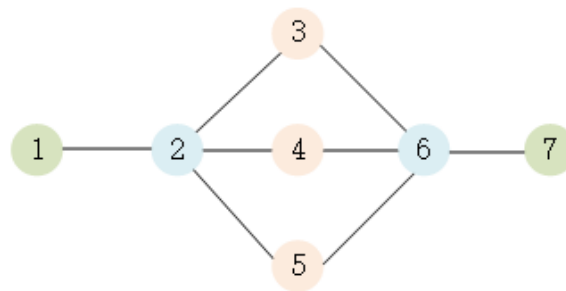


Figure 2. The information–communication double-layer interdependent network model of a UAV swarm.

Table 1. The adjacency matrix E_P

	1	2	3	4	5	6	7
1	0	1	0	0	0	0	0
2	0	0	1	1	1	0	0
3	0	1	0	0	0	1	0
4	0	1	0	0	0	1	0
5	0	1	0	0	0	1	0
6	0	0	1	1	1	0	0
7	0	0	0	0	0	1	0

Due to the coupling link between the two layers of the UAV swarm information–communication network, the initial data transmission capability of a link in a network is not only related to itself but also related to the coupling strength of the coupling link between two nodes on the link and the corresponding node of another network. In other words, this means that when a node communicates with nodes of the same type in the same network layer, it always ensures communication with the nodes of another layer with which it is coupled. In the information–communication interdependent network model, the node v_i in the information network is coupled with the node v_m in the communication network, and the node v_j in the information network is coupled with the node v_n in the communication network. The initial data transmission capability L_{ij} of link e_{ij} in the information network is associated with three factors: the betweenness centrality of the link itself and the betweenness centrality of the coupling links e_{im} and e_{jn} at both ends of the link. The initial data transmission capability L_{ij} is influenced by three factors: the betweenness centrality of the link itself, as well as the betweenness centrality of the connecting links e_{im} and e_{jn} at both ends of the link. It can be defined as

$$L_{ij} = B_{ij} + \frac{B_i}{B_i + B_m} \omega_{im} + \frac{B_j}{B_j + B_n} \omega_{jn} \quad (5)$$

Since the data transmission speed of a link is related to the link's transmission capacity, the data capacity of link e_{ij} can be represented as

$$T_{ij} = (1 + L_{ij})T_0 \quad (6)$$

where T_0 represents the minimum data transmission speed of the network, and T_{ij} represents the maximum data transmission speed of link e_{ij} . Once the data transmission range is exceeded, there is a probability that the link will fail.

2.2. Problem Formulation

In the context of UAV swarm networks, interdependent networks play a crucial role, facilitating efficient collaboration and communication among UAVs, enabling the cluster to execute complex tasks in a coordinated manner. The transmission capability of links is pivotal in maintaining such collaboration, ensuring timely data transmission and the stability of communication links. However, interdependent networks face various challenges, including susceptibility to different attacks and disturbances. Risks such as malicious attacks, network congestion, or node failures may lead to cascading failures within interdependent networks, significantly impacting system stability and reliability. Therefore, conducting vulnerability analysis and implementing appropriate measures, including reallocating network links, is imperative. This helps enhance the system's resilience against disruptions, thereby reducing the risk of attacks or disturbances and ensuring the stable operation of UAV swarm networks.

Generally speaking, the ability of each link in the UAV swarm network to transmit data is limited by the network cost, so it is impossible to endlessly undertake the transmission of a large number of information flows, otherwise it will cause communication blockage or even link interruption. Therefore, we assume that the data transmission capability of each link in the network is directly proportional to the initial data transmission capability L_{ij} of the link. Based on the ML model and other related research definitions, the adjusted data transmission capability L'_{ij} of the link e_{ij} is represented as

$$L'_{ij} = (1 + \beta)L_{ij} \quad (7)$$

where β is the capacity parameter, indicating the ability of the link to process additional data. The larger the value of β , the stronger the ability of the link to process data and the ability of the network to resist attacks.

When we choose the value of β , the construction cost and link transmission capacity should be considered. In real life, the link cost consumption of UAVs is influenced by various factors, such as materials, scenarios, and technologies, making it difficult to define the amount of cost consumption. When the value of β is relatively large, the ability of data transmission in the link of the UAV swarm information-communication network is stronger, and the ability to cope with cascading failures is stronger. In a fire rescue scenario, the interruption of some network links due to high-temperature radiation or the isolation of a burning building only causes a partial failure. The entire network cannot be paralyzed. However, the larger the value of β , the higher the cost of network construction and the more difficult it is to implement. Considering the limited technology and cost, the value of β generally has a certain threshold, and the ability of the whole UAV swarm network to resist cascading failure can be expressed by its threshold β_c . The larger the threshold β_c is, the more the network is vulnerable to cascading failure, and the smaller the threshold β_c is, the more the network is robust against cascading failure. In other words, when $\beta > \beta_c$, the interruption of any link in the network due to fire will not cause the interruption of other links. When $\beta < \beta_c$ is used, the data transmission capacity of links in the network is limited, and the interruption of some links in the network will increase the data transmission volume of other links, which may cause the failure of other links or even the collapse of the whole network. Therefore, in this paper, we studied the impact

of the value of β on the vulnerability of links, providing a reference for builders of UAV network links.

3. Information–Communication Interdependent Network of UAV Swarm

In a UAVs network, communication nodes and information nodes are coupled in a one-to-one or one-to-many manner, with each pair mapping to each other. Information nodes are mapped by communication nodes, meaning each information node uniquely corresponds to a communication node, but one communication node can correspond to multiple information nodes. This is because within a certain range, to ensure the accurate and error-free transmission of information from each information node in the information network, each information node must designate a communication node to receive the information it obtains during operation. This enables personnel to retrieve information through the corresponding communication node when checking the operational status of each information node, facilitating effective management and monitoring of information transmission. Figure 3 is an information–communication double-layer interdependent network model of a UAV swarm. The upper layer is the information network, and the lower layer is the communication network.

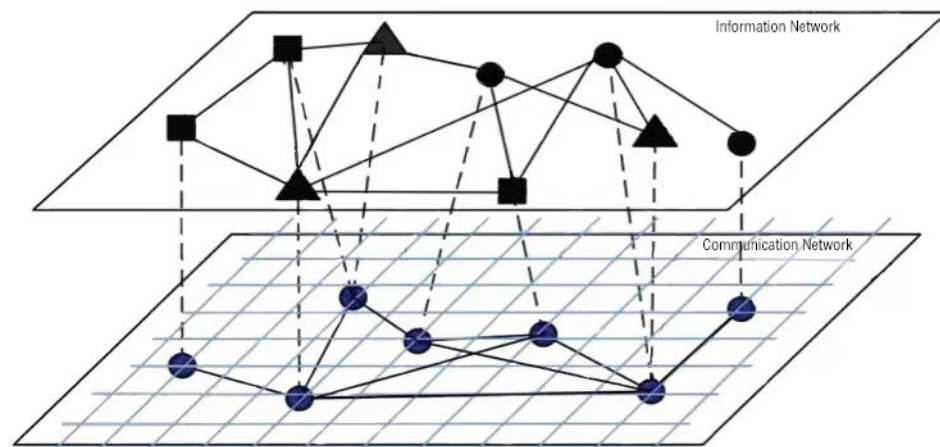


Figure 3. The information–communication double-layer interdependent network model of a UAV swarm.

The communication topology and the information network of a UAV swarm network are interdependent, forming the interdependent network model of the UAV swarm. Nodes in the communication network are mapped to information nodes in the information network in a one-to-one or one-to-many manner. This means that information nodes rely on communication nodes to interact with other nodes in the network, transmitting their perceived and processed data. Similarly, communication nodes need to perceive and process scene information through information nodes to implement corresponding functions. Generally, due to the limited energy of UAV nodes, each UAV typically carries only one task payload, leading to a one-to-one mapping relationship between UAV communication topology and the information network. However, there are rare instances of one-to-many mapping, where each UAV carries multiple task payloads. The information–communication double-layer interdependent network model of a UAV swarm is represented by $G_{P-F} = (G_P, G_F, E_{P-F})$. This representation includes a dependency matrix E_{P-F} that indicates the dependency relationship between nodes in the communication network G_P and nodes in the information network G_F . If there is a dependency between node p_i in the communication network G_P and node q_j in the information network G_F , it is expressed

as $E_{P-F}(i, j) = 1$; otherwise, $E_{P-F}(i, j) = 0$. Supposing $n = |V_P|$, $m = |V_F|$, the dependency matrix E_{P-F} can be expressed as

$$E_{P-F} = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1m} \\ e_{21} & e_{22} & \cdots & e_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & \cdots & e_{nm} \end{bmatrix} \quad (8)$$

4. Vulnerability Analysis of UAV Swarm

The focus of this section is to investigate the cascading failure process of UAV networks and propose a link re-allocation rule based on interdependent networks to address this issue. Additionally, two vulnerability evaluation indicators are defined to assess the effectiveness of the reallocated network.

4.1. Process of Link Cascading Failure

For a UAV swarm network, because different UAVs carry different task loads, UAVs with different functions share data information through information interaction to complete the tasks of the whole system. Therefore, network function has a certain impact on the vulnerability of the UAV swarm network. Due to the complexity of the task scenario, the communication link between UAVs can easily encounter environmental interference leading to link interruption. For instance, UAVs equipped with various communication and imaging devices may lose connection with other UAVs in high-temperature environments or in areas with potential electromagnetic interference. Additionally, they might be unable to operate effectively in the presence of physical obstacles. In such cases, other UAVs need to take on the tasks and the link transmission of the failed UAV [22]. Once a communication link is disconnected, the information exchange between the UAVs will be affected to some extent, or cascading failure will even occur, resulting in other communication links being affected. Therefore, this paper builds an information–communication interdependent model of the UAV swarm, introduces the cascading failure theory, and analyzes the vulnerability of the UAV swarm network under different task loads.

In the UAV swarm information–communication interdependent network, failures can be categorized into intra-network failures and inter-network failures. Intra-network failures refer to the interruption of a network link, leading to the redistribution of load to other links in the network and potentially causing cascading failures. On the other hand, inter-network failures primarily result from the coupling mapping relationship between different networks. When a link in the network is interrupted, one node at each end of the link is removed, potentially causing fragmentation of the entire network. According to percolation theory, nodes in the largest connected subgraph of the network can still function normally, while nodes disconnected from this subgroup may fail, leading to the disconnection of coupling connections.

In a fire rescue scenario, the normal work of the rescue UAV needs the data information support provided by the positioning UAV, the surveying UAV, the reconnaissance UAV, and the monitoring UAV that constitute the most basic functional subgroup. The whole UAV swarm network is composed of multiple functional subgroups interleaved with each other.

However, if the communication link of a reconnaissance UAV is interrupted and the location information sent by the positioning UAV cannot be accepted, the location of the fire site cannot be accurately found and the investigation of the fire area cannot be completed. Thus, the UAV is not in the functional sub-group and cannot play its function, which is equivalent to a fault. The area that should be investigated by this UAV naturally also needs to be investigated by other UAVs. The positioning UAV needs to transmit the location information of the fire area to the other UAVs, which increases the burden of the link. Figure 4 shows a flowchart of the cascading failure of a UAV swarm network information–communication interdependent network.

Figure 5 shows the cascading failure process of the links in the information–communication interdependent network of a UAV swarm: $\{a1, a2, a3, a4, a5, a6\}$ represents a node in the communication network; $\{b1, b2, b3, b4, b5, b6\}$ represents a node in the information network; the solid line represents the communication link or information connection within the network; and the dotted line represents the dependent link between networks.

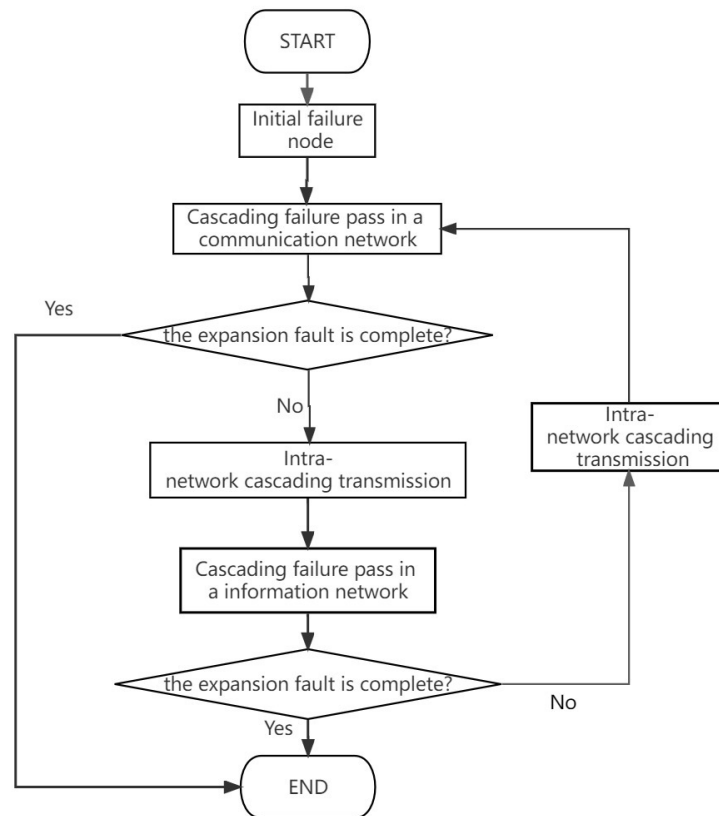


Figure 4. Process of cascading failure of UAV swarm information–communication interdependent network.

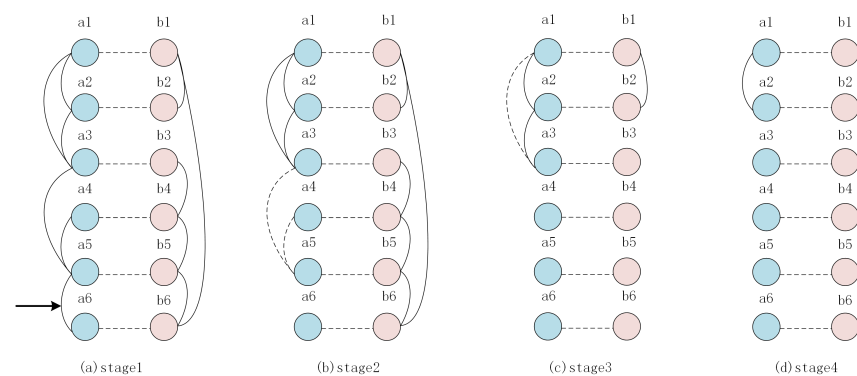


Figure 5. Cascading failure process of information–communication interdependent network link of UAV swarm.

Originally, the network is in a normal and stable operation state. At the initial moment, the link $a5a6$ in the communication network is interrupted, due to the influence of high-temperature thermal radiation. In stage 1, the data carried by link $a5a6$ are redistributed to the adjacent links $a4a5$ and $a3a5$ according to the redistribution rule. If the total amount of data on link $a3a5$ and link $a4a5$ exceeds their carrying capacity after re-allocation, another

round of re-allocation will occur. In stage 2, adjacent links $a1a3$ and $a2a3$ receive the allocated data information. We assume that link $a1a3$ also fails due to the total data volume exceeding the carrying capacity. However, link $a2a3$ has strong load capacity and can withstand excess data without failure. Then, turning to the information networks, in stage 2, because links $a3a5$, $a4a5$, and $a5a6$ in the communication network of the previous stage fail, the information nodes $b3$, $b4$, $b5$, and $b6$ cannot normally interact with the other information nodes through communication links. Therefore, the information links $b3b4$, $b4b5$, $b5b6$, $b1b6$ are faulty. At stage 3, although there is still a communication link between node $a2$ and node $a3$ in the communication network, the information node $b3$ corresponding to the communication node $a3$ has no information edge connection and no longer has information interaction with the other information nodes, so the communication link $a2a3$ is invalid. Finally, the connectivity map is composed of communication nodes $a1$, $a2$, communication link $a1a2$, information nodes $b1$, $b2$, and information link $b1b2$. The remaining functional subgroup in the information–communication interdependent network of the UAV swarm is formed.

4.2. Rule of Load Distribution

The load distribution rule is the core mechanism of intermediate link failure propagation in the load capacity model, which determines the load transfer method and load transfer amount. Because the coupling link in the information–communication interdependent network of a UAV swarm only plays the role of node coupling mapping between the two layers of networks, it cannot transmit data and cannot accept the data information distributed on the interrupted link. Therefore, after a link is interrupted, the data transmitted on the link flow only on the network layer where it resides. Using the low/mid/high-tier airborne wireless network mechanism from Reference Paper [23], we applied it to the two-tier UAV network in this paper and adjusted it based on the UAV-based scenarios. In this paper, the load distribution rule is defined as the optimal allocation according to the capability of the adjacent links of the interrupted link, and the redistribution rule is

$$\Delta L_{ik} = L_{ij} \frac{C_{ik}}{\sum_{a \in \Gamma_i} C_{ia} + \sum_{b \in \Gamma_j} C_{jb}} \quad (9)$$

where ΔL_{ik} is the extra data allocated on link e_{ik} receiving interrupted link e_{ij} ; a represents a neighboring node of node i , while b represents neighboring nodes of node j ; Γ_i represents the set of all neighbor nodes of node v_i ; Γ_j represents the set of all neighbor nodes of v_j .

Figure 6 shows a schematic diagram of link data redistribution in a fire rescue scenario after the communication network in the information–communication interdependent network of the UAV swarm is interrupted. The link e_{ij} in the network is interrupted by high-temperature radiation and cannot synchronize the information perceived by one UAV to the other UAVs, so as to normally perform tasks. The data transmitted on this link are allocated to intact links in the network using the preceding method. As a result, more data are transmitted on other links and the load becomes heavier.

The rule of redistribution begins by identifying neighbor node sets Γ_i and Γ_j of the UAV node v_i at both ends of an interrupted link e_{ij} due to high-temperature radiation or fire isolation. Then, it reallocates the data flow originally transmitted on the interrupted link to the remaining intact link e_{ik} based on a proportional allocation formula $\Delta L_{ik} = L_{ij} C_{ik} / (\sum_{a \in \Gamma_i} C_{ia} + \sum_{b \in \Gamma_j} C_{jb})$. After updating the data carried on the link e_{ik} by the formula $L_{ik}^{new} = L_{ik} + \Delta L_{ik}$ and judging whether $L_{ik} + \Delta L_{ik} > C_{ik}$ is true, if yes, the data on this link exceed its data transmission capacity, resulting in communication congestion and failure. Finally, when a new faulty link occurs, the process loops back to identifying new faulty links until none remain. The pseudocode for this algorithm is shown on Algorithm 1:

Algorithm 1 Redistribute Data After Link Failure

```

1: procedure REDISTRIBUTEDATAAFTERLINKFAILURE(linkFailureList)
2:   Input: linkFailureList                                ▷ List of failed links with data and capacities
3:   Output: None                                           ▷ Data redistribution after link failure
4:   Initialization:
5:      $\Gamma_i \leftarrow \text{getNeighborNodes}(\text{linkFailure.node}_i)$     ▷ Neighboring nodes of node  $v_i$ 
6:      $\Gamma_j \leftarrow \text{getNeighborNodes}(\text{linkFailure.node}_j)$     ▷ Neighboring nodes of node  $v_j$ 
7:   for each  $e_{ij}$  in linkFailureList do
8:     for each  $e_{ik}$  in  $\Gamma_i$  do
9:        $\Delta L_{ik} \leftarrow L_{ij} \times \frac{C_{ik}}{\sum_{a \in \Gamma_i} C_{ia} + \sum_{b \in \Gamma_j} C_{jb}}$     ▷ Calculate extra data allocation
10:       $L_{ik}^{\text{new}} \leftarrow L_{ik} + \Delta L_{ik}$     ▷ Update data carried on link  $e_{ik}$ 
11:      if  $L_{ik}^{\text{new}} > C_{ik}$  then    ▷ Check for communication congestion
12:        handleCommunicationCongestion( $e_{ik}$ )
13:      end if
14:    end for
15:  end for
16: end procedure

```

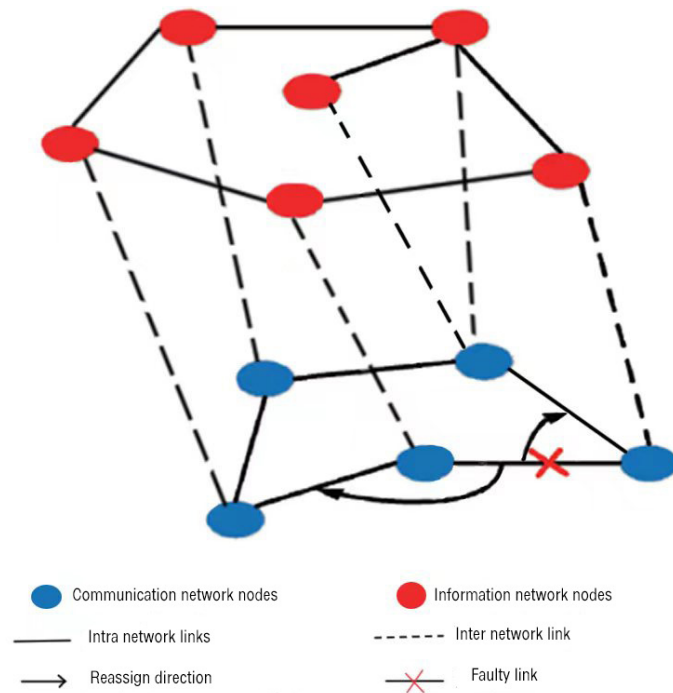


Figure 6. Diagram of redistributing data flows after a communication network link is interrupted.

4.3. Vulnerability Measurement Parameter

After the network status is stabilized, the vulnerability of the UAV swarm interdependent network after link interruption due to complex environment interference is reflected by evaluation indicators. This paper mainly evaluates the vulnerability of UAV swarm networks through the following three evaluation indicators:

- (1) The threshold β_c .

When the capacity parameter β is large, the network links have a strong capacity to carry data information. If other links are interrupted due to environmental interference, cascading faults will not occur, but the cost of building a network is correspondingly high. If the capacity parameter β is small, partial link disconnection will cause partial network crash or even the whole network to crash. The threshold value β_c is the phase transition point where the network cascades, which can measure the vulnerability of the network.

The smaller the value of β_c is, the more vulnerable the network is. The larger the value of β_c is, the stronger the network robustness.

(2) The connectivity indicator P_∞

This is an important indicator to measure the connectivity of the UAV swarm network. It means that after the network cascading failure (caused by the interruption of link e_{ij} in the network due to high-temperature radiation or a fire barrier) ends, one link is randomly selected among the remaining links, and there is a possibility that this link exists in the maximum functional subgroup. Let us break this down for clarity:

We assume the number of links in the information network is k and the number of links in the communication network is l . After the disconnection of link e_{ij} and the subsequent restoration of the network to a stable state following the cascading failure, let M_{ij} represent the number of links in the remaining maximum functional subgroups of communication networks P and information networks F . The larger the value of P_∞ is, the more likely a link is to be in the maximum functional subgroup after the cascading failure is stabilized, and the stronger the network robustness is. The P_∞ is expressed by the formula

$$P_\infty = \frac{\sum_{e_{ij} \in P \cup F} M_{ij}}{(k+l)(k+l-1)} \quad (10)$$

(3) The proportion of faulty links ϕ

We assume that the number of links in the information network is k and that the number of links in the communication network is l . In a complex environment, link e_{ij} is interrupted due to complex environment interference, resulting in a network cascading failure. After the network is restored to a stable state, the number of faulty links in the communication networks P and the information networks F is ϕ_{ij} . The larger the value of ϕ is, the smaller the number of remaining links in the maximum connected subgroup after the cascading failure is stabilized, indicating that the UAV swarm network is more vulnerable. The proportion of faulty links ϕ is expressed in the formula

$$\phi = \frac{\sum_{e_{ij} \in P \cup F} \phi_{ij}}{(k+l)(k+l-1)} \quad (11)$$

5. Simulation Results

The default network parameters for the experiment were initially established for this section. Subsequently, a vulnerability analysis of the network was conducted, following link failures. Finally, experimental results were observed under different network environments by varying the number of link failures and link construction parameters.

5.1. Parameters Setting

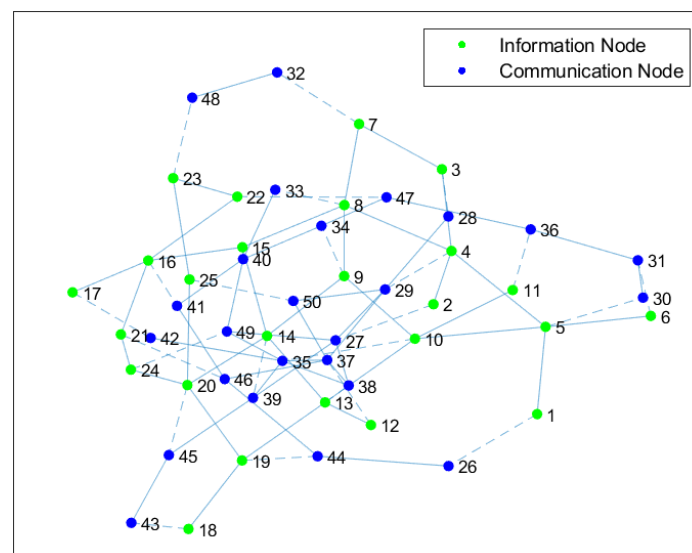
Based on the settings of the UAV parameters in Literature [13] and Literature [18], combined with the experimental conditions achievable by the user, for this section we set simulation parameters for the UAVs. Our experiments constructed a UAV swarm network consisting of 50 UAV nodes, among which there were 25 information nodes and 25 communication nodes, each having a one-to-one coupling relationship with each other. It was assumed that the task scene was a 1000 m × 1000 m fire rescue scene. We used MATLAB for the simulations, to generate the network topology structure, and the default simulation parameters are given on Table 2:

Table 2. Paramater of simulation.

Parameters	Values
size of area	1000 m × 1000 m
flying altitude of information UAVs	20–80 m
flying altitude of information UAVs	100–300 m
number of information node	25
number of communication node	25
number of action node	10
communication range of communication UAVs	30 m
communication range of information UAVs	15 m
speed of UAVs	10–40 m/s
duration of time slot	0.2 s
minimum link transmission speed T_0	2500 bps

5.2. Vulnerability of UAV Swarm Information–Communication Interdependent Network after Links Failure

We defined a communication rule: the default communication range for information UAVs was 50 m, while communication UAVs had a default communication range of 100 m. If two UAVs were within each other's communication range, they could establish a communication link. The nodes between the two networks had a coupling mapping relationship, and the coupling weight was $\alpha = 1$. We used MATLAB (R2023a) software to generate the initial network topology, allowed UAVs to operate for 20 time slots within the specified range based on the listed parameters, and randomly generated data on their links within the range of their own maximum transmission capacity. During the UAV flight, we recorded the network topology positions of the UAVs for each experiment, preparing for subsequent experiments. We used green nodes to represent information nodes and blue nodes to represent communication nodes, and an example of a generated network topology is shown in Figure 7.

**Figure 7.** An example of a generated network topology.

After the network topology was generated, 10 links in the communication network were interrupted randomly by high-temperature thermal radiation in each experiment. The data from these damaged links would be re-allocated to other undamaged links according to the method mentioned above. We recorded the values for each experiment, calculating the final average. Through simulation experiments, we used the threshold β_c , connectivity indicator P_∞ , and the proportion of faulty links ϕ as metrics. The simulation results are depicted in Figure 8.

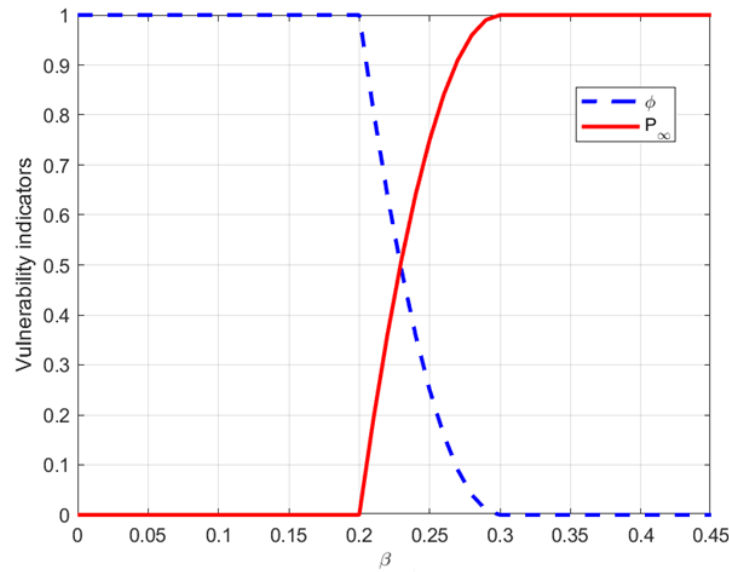


Figure 8. Vulnerability indicator change curve with capacity parameter β .

As shown in Figure 8, when the value of the capacity parameter β was between $[0, 0.2]$, the connectivity indicator P_{∞} was a constant 0, and the proportion of faulty links ϕ was 1. When the capacity parameter β exceeded 0.2, β continued to increase, and the connectivity indicator P_{∞} increased continuously from 0 and reached the maximum when $\beta = 0.3$, P_{∞} approaching 1. The proportion of faulty links ϕ decreased with the increase of β and reached the minimum when $\beta = 0.3$ and ϕ approached 0. Later, as the capacity parameter β continued to increase, the connectivity indicator P_{∞} and the proportion of faulty links ϕ remained stable and unchangeable.

According to the curve trend analysis in the figure, the vulnerability of the network was highest when the tolerance parameter $\beta \leq 0.2$, the connectivity indicator $P_{\infty} = 0$, and the proportion of faulty links $\phi = 1$, which can be denoted as the lower-limit threshold of the capacity parameter β_{min} . That is, if $\beta \leq \beta_{min}$, 10 links in the network were interrupted by high-temperature radiation, the network would completely collapse, due to cascading failure. With the increase of the capacity parameter β , the degree of damage brought about by cascading failures to the whole network was gradually weakened, and the robustness of the network against successive failures was gradually enhanced. But, correspondingly, the higher the cost of network construction, the less the possibility of network implementation. When $\beta = 0.3$, the robustness of the network reached the maximum. Then, when the capacity parameter β was added, the robustness of the network no longer changed, but the cost was still increasing. Therefore, $\beta = 0.3$ was the critical point at which the vulnerability of the network changed, the point at which the network changed from unstable to stable, namely, the threshold value $\beta_c = 0.3$. Furthermore, from the graph, we can observe that the rate of change of the curve varied from fast to slow. We speculate that there were not many portions of the communication links that exceeded the capacity threshold. Only a small increase in the transmission capacity of the original link would be needed to restore it to normal status.

5.3. Influence of Parameters on Vulnerability Analysis

Due to high-temperature heat radiation, we assumed that 1, 10, 20, and 30 links in the communication network were interrupted, respectively. To ensure authenticity, we chose these links randomly. Taking the network connectivity indicator P_{∞} , the proportion of faulty links ϕ , and the threshold β_c as indicators, this paper studied the cascading failure changes of the UAV cluster information–communication interdependent network model, and compared the network vulnerability under different link failure scopes. The simulation results are shown in Figures 9–12.

These figures illustrate the variations in the curve of P_∞ and the capacity parameter β when 1, 10, 20, and 30 links in the communication network were disrupted by high-temperature heat radiation, respectively. The variation trends of the three curves are similar. The general trend was that when the capacity parameter β was small, the vulnerability of the network was high. With the increase of the capacity parameter β , the robustness of the network against successive failures was gradually enhanced.

It can be seen that β_{min} and β_c gradually increased with the increase of the attack degree, which indicates that the connectivity of the network decreased with the increase of the link fault range. That is, the ability of the network to resist cascading failure decreased with the expansion of the attack degree, and the network became more and more vulnerable. This is because when the degree of network faults is large, more network links fail at the same time. As a result, the ratio of reassignment of data received by intact links increases, and the spread of successive network faults is faster.

Additionally, from these graphs, we can observe that the range of curve variation gradually expanded as the number of interfered links increased. This is because with the increase in the number of interfered links, the probability of a single link carrying interfered traffic increases, requiring a greater increase in transmission capacity to adapt to high-load scenarios.

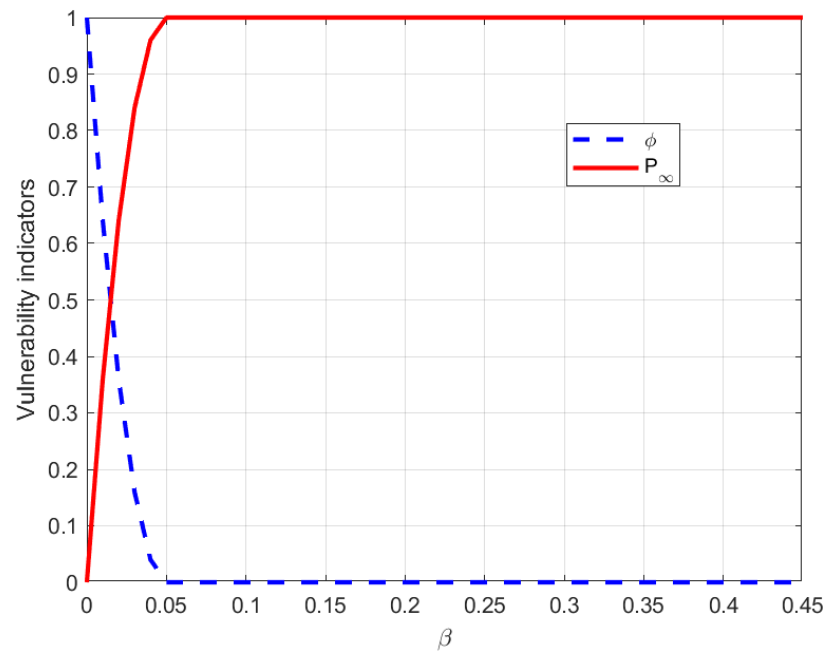


Figure 9. One link in the communication network is interrupted.

Assuming 10 links in the communication network were interrupted, we studied the cascading failure of the UAV swarm information–communication interdependent network model and compared the network vulnerability under different coupling link weights. The simulation results are shown in Figure 13.

As can be seen from Figure 13, if $\alpha = 0.4$, the vulnerability of the network is highest when $\beta \leq 0.3$. With the increase of β , the robustness of the network gradually becomes stronger, and the threshold of the network from unstable to stable is $\beta_c = 0.4$. If $\alpha = 1$, the vulnerability of the network was highest when $\beta \leq 0.2$. With the increase of β , the robustness of the network gradually became stronger, and the threshold of the network from unstable to stable was $\beta_c = 0.3$. If $\alpha = 1.3$, the vulnerability of the network was highest when $\beta \leq 0.1$. With the increase of β , the robustness of the network gradually became stronger, and the threshold of the network from unstable to stable was $\beta_c = 0.2$. And, with the increase of coupling link weight α , the lower threshold β_{min} and threshold β_c of the capacity parameter gradually decreased, and the vulnerability of the network

gradually weakened. This was because when the coupling weight increased, the corresponding coupling strength also increased. According to the load setting rules, the larger the coupling strength, the more initial data transmitted on the link, the stronger the link data transmission capacity, and the more information it can carry during the link data information reassignment. If this does nothing more than to bring the construction cost of the network and the β value of the network topology composition as close as possible to β_c , it will reduce vulnerability and the network will be more robust.

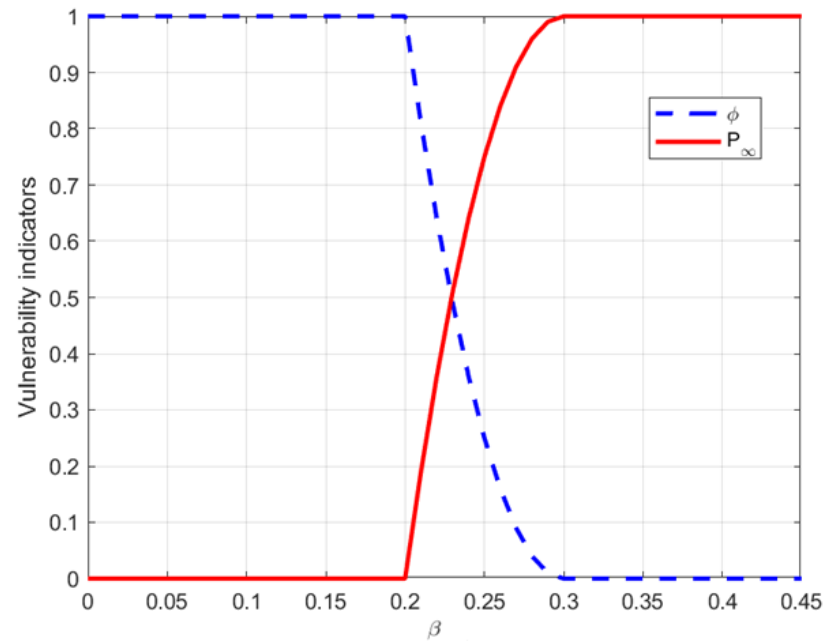


Figure 10. 10 links in the communication network are interrupted.

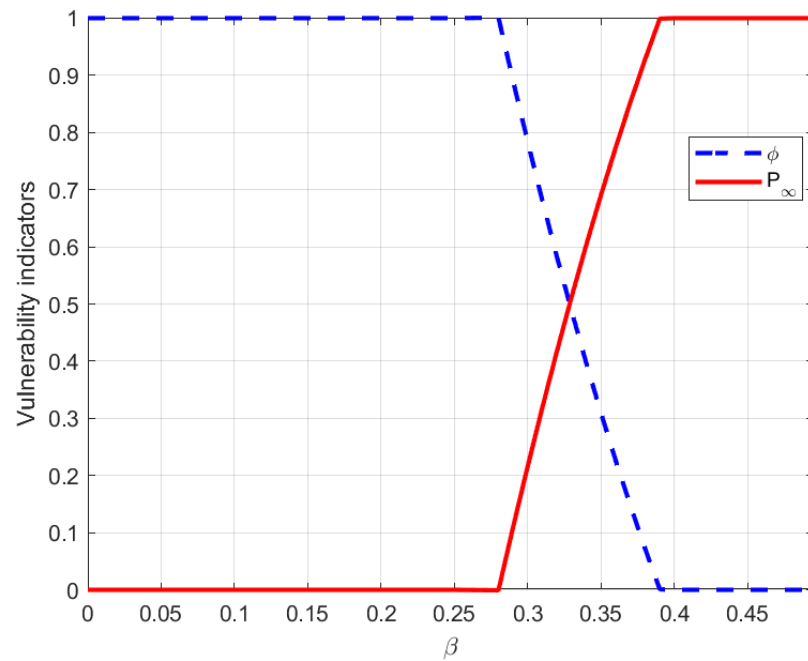


Figure 11. 20 links in the communication network are interrupted.

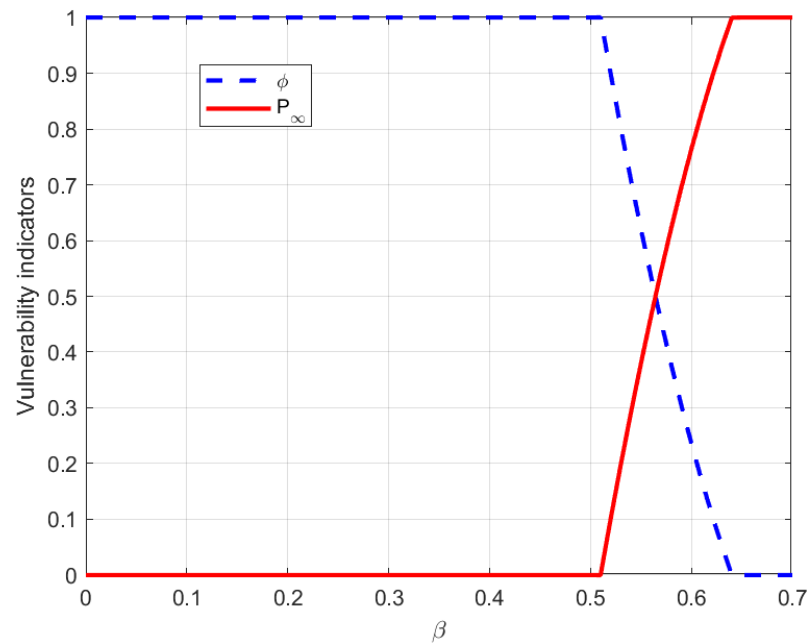


Figure 12. 30 links in the communication network are interrupted.

To continue studying the impact of the coupling link weight coefficient on the overall system performance, we varied the value of the coupling link weight coefficient to observe its effects on the low threshold β_{min} and the threshold β_c .

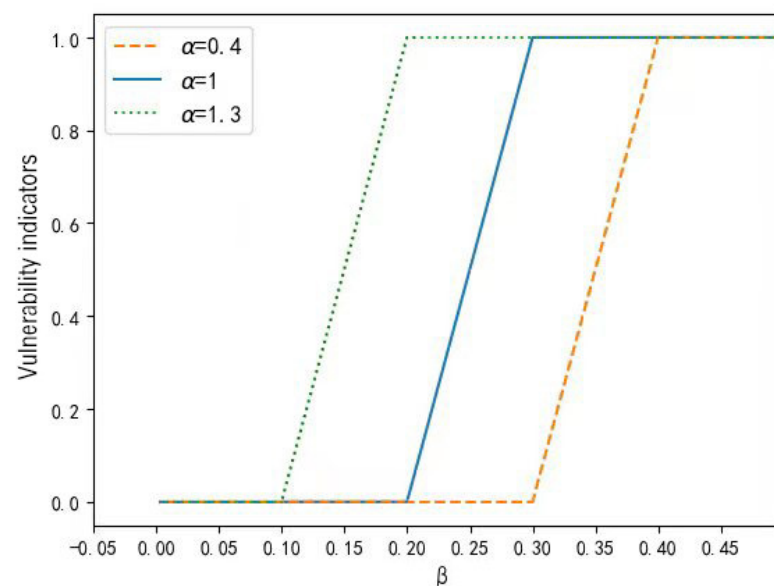


Figure 13. Vulnerability indicators change curve with capacity parameter β .

In Figure 14, we can observe that as α increased, the values of both curves decreased, reaching zero at $\alpha = 2$. Additionally, as α increased, the difference between β_c and β_{min} gradually decreased. At $\alpha = 0$, the difference between them is 0.2, while at $\alpha = 2$, the difference decreases to zero. This was because with the increase in the coupling coefficient, the link transmission capacity of the two UAV networks also increased, and their connection became tighter. Therefore, adjusting the transmission capacity of one link also increased the overall impact on the network.

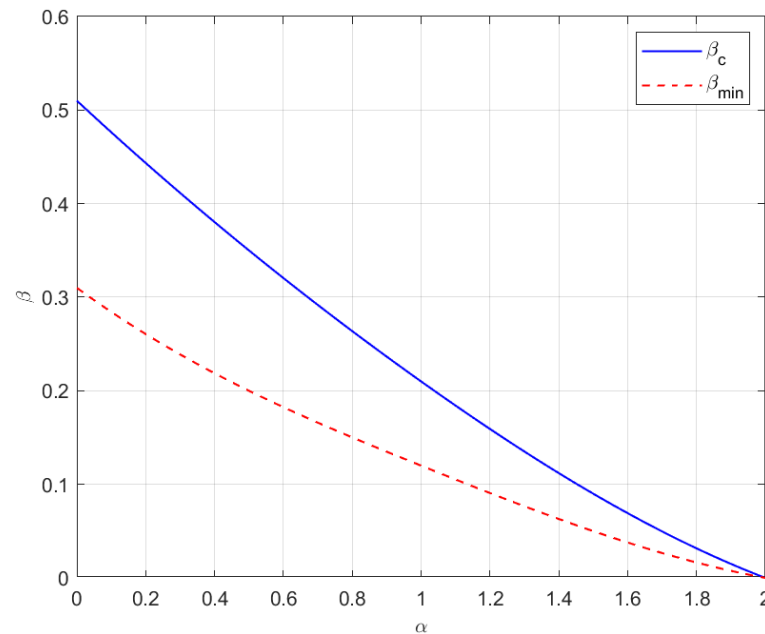


Figure 14. Threshold β change curve with α .

6. Conclusions

This paper proposes a vulnerability assessment method for UAV swarm networks with emergency tasks. Taking the UAV swarm network under a fire rescue scenario as an example, the UAV swarm network can be abstracted as a communication network and an information network. A UAV swarm information–communication interdependent network model with coupling mapping relationship was constructed to simulate the UAV swarm network with emergency tasks. On this basis, considering the successive failures of the interdependent network, a cascading failure model of the information–communication interdependent network of the UAV swarm was constructed, and the vulnerability of the network was analyzed by evaluating the cascading failures of the network. Finally, the vulnerability of the UAV swarm information–communication interdependent network under complex environment interference was analyzed by a simulation experiment, the influences of the fault range of the link in the information–communication interdependent network and of the coupling link weight on the vulnerability of the UAV swarm information–communication interdependent network were compared and analyzed, and the feasibility of the method was verified. In future work, from the perspective of network functions, we will explore the changes in network vulnerability after node failures of different functions in the UAV swarm network, and further explore the vulnerability characteristics of the UAV swarm network.

Author Contributions: Conceptualization, J.L. and Z.H.; methodology, Q.Y. (Qinghai Yang); software, Q.Y. (Qingfeng Yue); validation, X.X.; writing—original draft preparation, Q.Y. (Qingfeng Yue); writing—review and editing, J.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the Natural Science Basis Research Plan in Shaanxi Province of China (2023JCYB555), and by the National Key Research and Development Program of China (2020YFB1807700).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Author Zijia Huang was employed by the company The 20th Research Institute of China Electronics Technology Group Corporation. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

UAVs	Unmanned Aerial Vehicles
ML	Motter–Lai

References

- Memari, M.; Shakya, P.; Shekaramiz, M.; Seibi, A.C.; Masoum, M.A.S. Review on the advancements in wind turbine blade inspection: Integrating drone and deep learning technologies for enhanced defect detection. *IEEE Access* **2024**, *12*, 33236–33282. [\[CrossRef\]](#)
- Wang, K.; Yuan, Y.; Chen, M.; Lou, Z.; Zhu, Z.; Li, R. A study of fire drone extinguishing system in high-rise buildings. *Fire* **2022**, *5*, 75.
- Cvitanić, D. Drone applications in transportation. In Proceedings of the 2020 5th International Conference on Smart and Sustainable Technologies (SpliTech), Split, Croatia, 23–26 September 2020; pp. 1–4.
- Allodi, L.; Banescu, S.; Femmer, H.; Beckers, K. Identifying relevant information cues for vulnerability assessment using cvss. In Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, Tempe, AZ, USA, 19–21 March 2018; pp. 119–126.
- Liu, Y.; Xu, S. Design and simulation of an algorithm for assessing the vulnerability of communication network topology. *Comput. Simul.* **2022**, *39*, 201–204+326.
- Huang, B.; Qin, Y.; Liu, Y.; Ji, D. Vulnerability assessment and risk probability study based on generic attack trees. *Inf. Netw. Secur.* **2022**, *22*, 39–44.
- Yang, Y. Vulnerability assessment model for government network topology based on attack tree model. *Autom. Technol. Appl.* **2022**, *41*, 116–119.
- Wu, Y. Vulnerability assessment of power information physical systems based on bayesian attack graphs. *Electr. Power Electr. Eng.* **2022**, *2*, 6–13+55.
- Motter, A.E.; Lai, Y. Cascade-based attacks on complex networks. *Phys. Rev. E* **2002**, *66*, 065102. [\[CrossRef\]](#) [\[PubMed\]](#)
- Wang, B.; Kim, B.J. A high-robustness and low-cost model for cascading failures. *Europhys. Lett.* **2007**, *78*, 48001. [\[CrossRef\]](#)
- Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [\[CrossRef\]](#) [\[PubMed\]](#)
- Zhao, Z.; Zhangyuan, L.I.; Guo, H.; Yang, M. Research on vulnerability of space information network based on interdependent networks. In Proceedings of the 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 18–21 June 2018; pp. 302–309.
- Chen, Z.; Wu, J.; Xia, Y.; Zhang, X. Robustness of interdependent power grids and communication networks: A complex network perspective. *IEEE Trans. Circuits Syst. II Express Briefs* **2017**, *65*, 115–119. [\[CrossRef\]](#)
- Liu, F.Z.; Xiao, B.; Liu, J.J.; Wang, H.R. Robustness of asymmetric dependent network under cascading failure. *J. Natl. Univ. Def. Technol.* **2021**, *43*, 49–56.
- Gao, J.; Buldyrev, S.V.; Havlin, S.; Stanley, H.E. Robustness of a network of networks. *Phys. Rev. Lett.* **2011**, *107*, 195701. [\[CrossRef\]](#) [\[PubMed\]](#)
- Xing, J.; Chen, C.; Zhu, Z. Cascading failure of double layer networked command information system. *Control. Decis.* **2020**, *35*, 3017–3025.
- Jia, C.; Li, M.; Liu, R. Percolation and cascading dynamics on multilayer complex networks. *J. Univ. Electron. Sci. Technol. China* **2022**, *51*, 148–160.
- Shen, D.; Li, J. Research on military information grid cascading failure model and robustness strategy. *Syst. Eng. Electron.* **2015**, *37*, 310–317.
- Zou, Q.; Ding, L. Research on key fragile dependency links removal strategies in interdependent power and communication networks under cascading failures. In Proceedings of the 2023 3rd International Conference on Neural Networks, Information and Communication Engineering (NNICE), Guangzhou, China, 24–26 February 2023; pp. 565–570.
- Huynh, P.K.; Rahman, M.M.; Yadav, O.P.; Le, T.Q.; Le, C. Assessing robustness and vulnerability in interdependent network infrastructure: A multilayer network approach. In Proceedings of the 2024 Annual Reliability and Maintainability Symposium (RAMS), Albuquerque, NM, USA, 22–25 January 2024; pp. 1–7.
- Li, P.; Mao, P.; Geng, Q.; Huang, C.P.; Fang, Q.; Zhang, J.R. Research status and trend of uav swarm technology. *Aero Weapon.* **2020**, *27*, 25–32.
- Roldán-Gómez, J.J.; González-Gironda, E.; Barrientos, A. A survey on robotic technologies for forest firefighting: Applying drone swarms to improve firefighters' efficiency and safety. *Appl. Sci.* **2021**, *11*, 363. [\[CrossRef\]](#)
- Wang, D.; Al-Ahmed, S.A.; Shakir, M.Z. Optimized link distribution schemes for ultrareliable and low-latency communications in multilayer airborne networks. *IEEE Trans. Ind. Inform.* **2020**, *16*, 5866–5873. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.