Electronic Research Archive

ERA, 32(5): 3316–3333.
DOI: 10.3934/era.2024153
Received: 19 March 2024
Revised: 08 May 2024
Accepted: 09 May 2024
Published: 20 May 2024

http://www.aimspress.com/journal/ERA

Research article

Resilience evaluation and optimization for an air-ground cooperative network

Xiaoyang Xie[1,2], Shanghua Wen[1], Minglong Li[1], Yong Yang[3], Songru Zhang[4], Zhiwei Chen[5], Xiaoke Zhang[6,]* and Hongyan Dui[4]

[1] Department of Intelligent Data Science, College of Computer, National University of Defense Technology, Changsha 410073, China
[2] China Academy of Launch Vehicle Technology, Beijing 100076, China
[3] Shanghai Marine Equipment Research Institute, Shanghai 200031, China
[4] School of Management, Zhengzhou University, Zhengzhou 450001, China
[5] Unmanned System Research Institute, Northwestern Polytechnical University, Xi'an 710109, China
[6] National Key Laboratory for Complex Systems Simulation, Beijing 100101, China

* **Correspondence:** Email: zhangxiaoke2013@hotmail.com.

Abstract: The combat domain of modern warfare is becoming increasingly multidimensional. It is important to evaluate the resilience of the air-ground cooperative network for defending against attack threats and recovery performance. First, a resilience analysis model was proposed to effectively analyze and evaluate the resilience of the air-ground cooperative network. Then, considering the available resources, three dynamic reconfiguration strategies were given from the global perspective to help the air-ground cooperative network quickly recover performance and enhance combat capabilities. Finally, a typical 50-node network was taken as an example to prove the effectiveness and feasibility of the proposed model. The proposed method can provide scientific guidance for improving the air-ground cooperative network combat capabilities.

Keywords: resilience; kill chain; dynamic reconfiguration; air-ground cooperative network

1. Introduction

With the wide application of artificial intelligence in the military field, modern warfare has gradually shifted from platform-based combat to system combat [1,2]. The field of combat is becoming more and more multidimensional, and the trend of joint combat forces is becoming more and more obvious. The air-ground cooperative system is an important component of the tactics for modern warfare [3]. It has an efficient command and control system, cross-service information flow and command flow, and powerful combat power. However, the battlefield is ever-changing, and all combat links are interlocked. The consequences of a mistake will be unimaginable. How the combat system can quickly resist, react, and recover to fulfill the combat mission in the face of internal and external pressures or changes has become a key concern.

In order to study the impact of threat events on the performance of the air-ground cooperative network, it is first necessary to model the cooperative networks. Complex network theory and methods have been widely used in modeling cooperative networks. The construction of a cooperative network model has attracted the attention of some scholars [4–6]. Cares et al. [7] proposed a combat model in the information age based on the OODA combat ring theory, which divides the nodes in the complex military network into observe nodes, decision nodes, and attack nodes. It points out a new direction for the research of complex military network systems. Li et al. [8] built on this foundation by proposing a new methodological framework for heterogeneous network meta-paths that can help specific heterogeneous networks predict multiple types of connections. Li et al. [9] built a time-based operational network by utilizing the concepts of OODA rings and kill chains, which enable capability-oriented equipment contribution analysis. Li et al. [10] explored the functional robustness of heterogeneous unmanned equipment system operations with different types of functional entities and information flows by utilizing OODA ring theory. This can provide valuable insights for operational guidance. Sun et al. [11] proposed a framework to solve the operational network link prediction problem, which only utilizes the topology information of the operational network to predict the network links. Chen et al. [12] constructed a heterogeneous operational network, and based on the structure of the network, designed an operational capability index to evaluate the performance of the dynamic heterogeneous operational network.

Resilience reflects not only the system's own resistance to damage, but also the system's ability to recover after disruption [13,14]. The idea of resilience first appeared in the field of ecology. Subsequently, it has been widely used in many fields, such as infrastructure [15], ecology [16], and military systems [17,18]. In the past few years, resilience metrics and resilience enhancement strategies have become the research hotspots in various fields [19–21]. Geng et al. [22] proposed a framework for assessing resilience under demand-based disruption conditions and comprehensively evaluated the network performance from the perspectives of absorption, adaptation, and recovery. Tran et al. [23] utilized a complex network approach to establish a simulation model of UAV clusters and constructed a resilience evaluation framework applicable to UAV clusters, thereby quantitatively evaluating the operational capabilities of them. Bai et al. [24] proposed an improved UAV-cluster model to incorporate the effect of a limited communication range into the existing model to more specifically evaluate the resilience of UAV clusters during mission execution. Based on this, Cheng et al. [25] proposed an improved comprehensive metric for the quantitative assessment of resilience, which was constructed as the sum of two abilities: absorption and recovery.

On the basis of resilience assessment, many researchers have developed various reconfiguration strategies to enhance resilience. Sun et al. [26] proposed a mission-oriented framework for resilience assessment of unmanned equipment systems and a collaborative reconfiguration model was proposed as a performance recovery strategy. Feng et al. [27] analyzed the resilience of the multi-UAV system throughout the operation period, and improved the resilience by changing the UAV formation. Tran et al. [28] enhanced the resilience of the control system of multi-UAV by randomly connecting the remaining nodes. Pan et al. [29] searched for a resilience-enhancing recovery strategy for the system by analyzing the resilience importance of the damaged components. However, these methods are usually targeted at scenarios where the entity can be repaired. In the real scene, the external environment changes rapidly, and there is little time to repair. At the same time, the application of these methods is limited to single-layer networks or cases with few failed nodes. Therefore, it is necessary to provide dynamic reconfiguration strategies for a collaborative network to enhance its resilience and improve its combat capability quickly.

Therefore, we study the resilience assessment and reconfiguration optimization of cooperative combat networks, focusing on building a reconfiguration model to improve resilience. In this model, all available resources of the system are considered comprehensively, and three dynamic reconfiguration strategies are proposed. The three strategies in the model can be combined according to different failure conditions and scales to help the network quickly reconstruct the kill chain and improve the combat capability. The proposed method can help decision-makers to assess the resilience of the system and give reconfiguration strategies to enhance the resilience.

Assumption：

1) There are redundant base stations and emergency communication measures in the system to ensure the stability of communication. The communication between air and ground units will not be completely disrupted.
2) The support nodes have sufficient resources, and the failure of supply nodes is not considered in this model.
3) The air and ground units are interoperable, enabling collaboration and information sharing.
4) The time of the three dynamic reconfiguration strategies is the same.

2. The air-ground cooperative network model

2.1. The air-ground cooperative network architecture

In order to face the complex combat environment and effectively carry out military missions, it is necessary to have collaboration and cooperation between weapons and equipment, command and control systems. At the same time, with the development of science and technology, different platforms have compatibility. The units in the platform can be interconnected without any obstacles. Complex network theory has been widely used in the field of military operations. In this paper, using the complex network theory, the system of the air-ground cooperative operation with intelligent equipment represented by unmanned aircraft and unmanned vehicles is considered as a special heterogeneous network. The air-ground cooperative operation refers to the combat mode of close cooperation and coordination between air and ground forces to carry out common tasks. In this collaborative approach, air forces (e.g., Unmanned Aerial Vehicles (UAV), helicopters) and ground forces (e.g., troops, Unmanned Ground Vehicle (UGV)) cooperate to jointly complete the target reconnaissance, decision-making, attack, and support tasks.

However, considering the fact that UAV swarm and UGV swarm also need to fulfill their corresponding tasks respectively, as well as the impact of material supply on UAV swarm and UGV swarm during the combat process, we must analyze the task characteristics of each layer respectively and the dependencies between the layers. This particular heterogeneous network can also be constructed as a multilayer heterogeneous network. Weapons and equipment, command centers, and support materials in the system are abstracted as nodes, and commands such as scheduling, control, and maintenance are abstracted as edges. The air-ground cooperative network is shown in Figure 1.

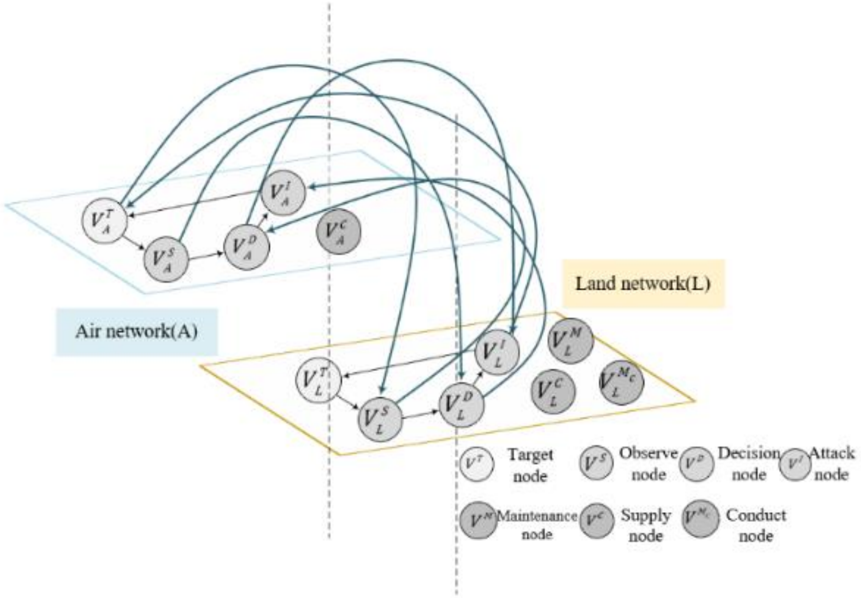


Figure 1. The air-ground cooperative network.

In Figure 1, there are connections between the air network and the ground network. For example, the observe node (V_A^S) in the air network can provide real-time and accurate target information to the ground units. Moreover, it can transmit the obtained information to the ground nodes within its communication range. Such coordination can exist widely between different types of nodes in the cooperative network.

The abstract digraph $\psi = (G, \phi)$ represents the air-ground cooperative network. This is a multilayer heterogeneous network of nodes and edges with different functions. $G = \{G_i; i \in \{A, L\}\}$ represents the set of different levels in the cooperative network. Specifically, G_A is the air network and G_L is the ground network. V_i^j is the set of nodes within the i-th layer of the network in the cooperative operation system, and E_i^{jq} is the set of edges within the i-th layer of the network. $\phi = \{E_{im}^{jq} \in (V_i^j \times V_m^q, V_m^q \times V_i^j); i, m = A, L; j, q = S, D, I, T, C, M; i \neq m\}$ represents the set of nodes and edges in the multilayer heterogeneous network. Specially, M_C is the conduct center. Considering that the maintenance work under coordinated operations is mainly realized by ground-based nodes, such as equipment maintenance bases, airports, and shipyards. The maintenance tasks could not be accomplished on the air platform. Therefore, the ground network includes maintenance nodes and support nodes, and the air network only includes support nodes in this paper.

2.2. The node in the network

The nodes are categorized into operational nodes and support nodes based on the different types of tasks accomplished by different nodes in the cooperative network. According to the theory related to the OODA combat loop, operational nodes can be divided into observe nodes, decide nodes, attack nodes, target nodes. The set of operational nodes is $j_d \in \{S, D, I, T\}$. The different functions and attributes of nodes are as follows:

(i) Observe node (*S*)

Weapons or equipment that perform observe, surveillance, and early warning missions, such as reconnaissance satellites, radars, and capture drones. For an observe node $S_i \in S$, which has some ability to detect reconnaissance targets, the functions and attributes of S_i are represented by

$$S_i = (x_i, y_i, z_i, t_i, d_i), \tag{1}$$

where x_i, y_i, z_i denote the coordinates of S_i, t_i denotes the detection capability of S_i, and d_i denotes the maximum detection distance of S_i. With the development of technology, the detection capability and maximum detection distance of nodes will also be improved. The input parameters of the observe node can be updated to simulate the evolving level of technology.

(ii) Decision node (*D*)

Weapons or equipment that perform command and control tasks, such as C4ISR, space information systems, control centers, etc., for a decision node $D_i \in D$, the attributes of D_i are represented by

$$D_i = (x_i, y_i, z_i), \tag{2}$$

where x_i, y_i, z_i denote the coordinates of D_i.

(iii) Attack node (*I*)

Weapons or equipment that perform fire attack and electromagnetic jamming tasks, such as fighters, frigates, missiles, and electromagnetic jamming radars, for the attack node $I_i \in I$, which has a certain ability to attack or jam a target, the functions and attributes of I_i are represented by

$$I_i = (x_i, y_i, z_i, k_i), \tag{3}$$

where x_i, y_i, z_i denote the coordinates of node I_i and k_i denotes the attacking capability of node I_i. It is worth noting that the range, accuracy, lethality, and other performance of an attack node will improve with the development of technology. Thus, the striking ability of the attack node can be enhanced. By adjusting the input parameters, the performance of the attack node under different technological levels can be simulated.

(iiii) Target node (*T*)

The node will be attacked in the process of operations. For the target node $T_i \in T$, it possesses certain detection difficulty and attack difficulty. When attacking a target, it is necessary to select an operational node with the appropriate detection and attack capabilities. The functions and attributes of T_i are represented by

$$T_i = (x_i, y_i, z_i, b_i, c_i), \tag{4}$$

where x_i, y_i, z_i denote the coordinates of node T_i, b_i denotes the detection difficulty of node T_i and c_i denotes the striking difficulty of node T_i. However, the hiding ability and anti-strike ability of the target node will be improved with the development of technology. The input parameters of the target node can be changed to simulate the evolving level of technology.

According to the different functions of the support nodes, the support nodes can be classified into supply nodes and maintenance nodes. The set of support nodes is $j_b \in \{C, M\}$. The different functions and attributes of support nodes are as follows:

(i) Supply node (*C*)

An entity supply node provides ammunition, fuel, and other materiels for combat equipment. For a supply node $C_i \in C$, the attributes of C_i are represented by

$$C_i = (x_i, y_i, z_i, w_i), \tag{5}$$

where x_i, y_i, z_i denote the coordinates of node C_i and w_i is the supply capacity of the supply node.

(ii) Maintenance node (*M*)

Maintenance nodes provide maintenance services for combat equipment, such as equipment maintenance bases, airports, shipyards, etc. For a maintenance node $M_i \in M$, the attributes of M_i are represented by

$$M_i = (x_i, y_i, z_i, r_i), \tag{6}$$

where x_i, y_i, z_i denote the coordinates of node M_i and r_i is the maintenance capability of the maintenance node.

2.3. The edge in the network

As can be seen from Figure 1, the different operational nodes are connected by directed edges to create a combat ring. These closed chains formed in a cooperative network are called kill chains. The nodes in a kill chain are based on a pre-planned and fixed architecture, and operate interdependently. These kill chains are capable of observing, judging, deciding, and attacking target nodes. They can represent the complete combat path from observation to the destruction of enemy targets. The kill chains are divided into typical kill chains and information-sharing kill chains based on whether information sharing is performed between operational nodes, as shown in Figure 2.

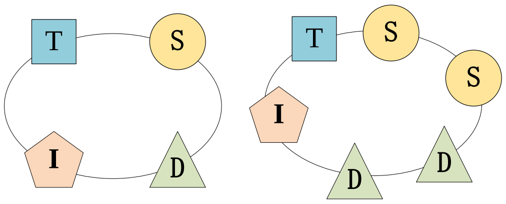


Figure 2. Two types of kill chains.

The observe node and decision node are not single in the information-sharing kill chain, and information sharing exists among multiple observe nodes and decision nodes.

Each kill chain represents a method of attacking a target. For a target, the higher the number of kill chains, the more ways there are to attack this target. Based on the air-ground cooperative network, this paper adopts the adjacency matrix and the arrival matrix to calculate the number of kill chains, taking the typical kill chain $T \rightarrow S \rightarrow D \rightarrow I \rightarrow T$ as an example to calculate the number of kill chains. The adjacency matrixes A_{TS}, A_{SD}, A_{DI}, A_{IT} represent the connectivity between nodes in the network. The arrival matrix A_{TSDIT} of target T can be calculated by

$$A_{TSDIT} = A_{TS} \cdot A_{SD} \cdot A_{DI} \cdot A_{IT}. \tag{7}$$

The number of kill chains of this type can be calculated by

$$N_{TSDIT} = \sum_{i=1}^{|T|} A_{TSDIT}(i,i), \tag{8}$$

where $|T|$ represents the number of target nodes in the network.

3. Failure analysis of cooperative network

The support nodes in the actual combat network generally have more supplies and self-support capabilities. Therefore, the failure of support nodes is not considered in this paper. This section mainly analyzes the failure mode of the operational nodes. Operational nodes (S, D, I) have two failure modes: attack failure and supply failure. Multiple attacks are generally carried out to destroy the target node in the actual combat process. In Figure 3, we take the i-th attack among the multiple attacks as an example to analyze the failure mode of operational node K.

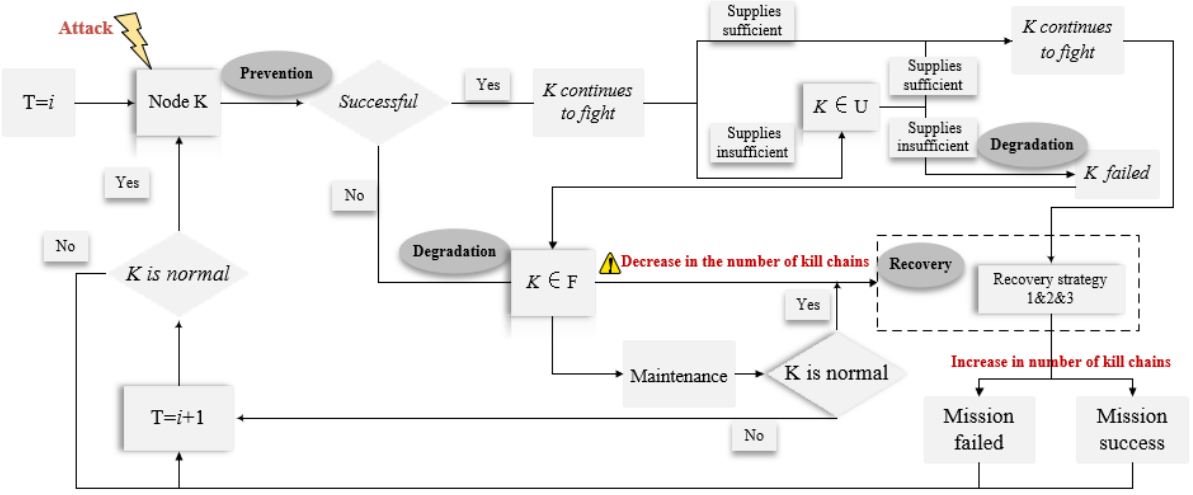


Figure 3. Failure analysis of operational nodes.

As can be seen from Figure 3, the operational node K needs to defend itself against enemy attacks while accomplishing the coordinated mission. At moment T, the operational node K suffers an attack. If the operational node K fails to prevent the attack, the operational node becomes a damaged node. F is the set of damaged nodes. The damaged node K must be repaired before it can return to normal. Since the degree of damage of node K is unknown, node K may be restored during this attack, or it may be restored during the next attack phase. When the combat conditions permit, the damaged node K may rejoin the combat network after maintenance. Based on the above analysis, the failure of the operational node due to an attack is called attack failure.

If operational node K is successful in preventing an enemy attack, the node K will continue to complete that phase of the combat mission. Before attacking the target, the operational node K will check whether the supplies (ammunition, fuel, etc.) are sufficient. When the operational node K has insufficient supplies, it needs to be supplied urgently. U is the set of nodes that need to be supplied urgently. As the combat process progresses, the supply task of the supply nodes increases. When the operational node K cannot be resupplied by the supply nodes in time, the node fails. Based on the above analysis, the failure of the operational node due to insufficient supplies and the inability to be resupplied in time is called supply failure.

As a result of the attack on the network, the number of operational nodes and kill chains are reduced. In order to ensure the success of the attack mission, recovery strategies need to be quickly developed to enhance the combat capability of the cooperative network. A detailed description of the recovery strategies will be detailed in Section 4.

4. Resilience evaluation and optimization

Operational nodes in the multilayer heterogeneous network will not work properly or even fail due to internal and external disturbances. At the same time, this effect will spread and propagate through the structural connection and mission interaction of the network. This will cause a wider range of network performance changes. Based on the failure mode analysis of the operational nodes above, this section focuses on evaluating and enhancing the resilience of the air-ground cooperative network. Three dynamic recovery strategies are proposed in this section, which can provide scientific guidance for the cooperative network to enhance combat capability.

4.1. Resilience evaluation

Definitions and metrics of resilience are varied in different domains. The definition of resilience encompasses three abilities of a system under the influence of a disturbance: the ability to absorb the impact of the disturbance, the degree to restore the system’s performance after an attack, and the speed of recovery after a destructive event. In the air-ground cooperative network, resilience refers to the ability of the system to quickly recover from shocks to ensure that missions are accomplished. The change in performance after an attack on an air-ground cooperative network is shown in Figure 4.

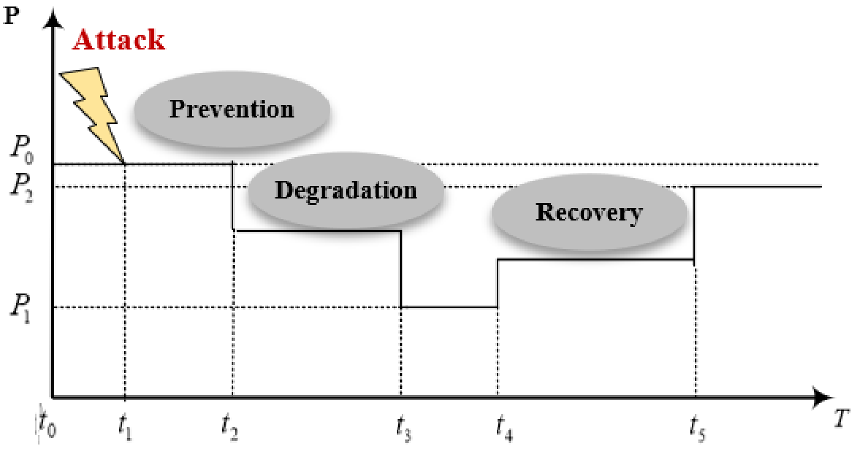


Figure 4. Performance of cooperative network.

At time t_0, the air-ground cooperative network begins to conduct operational missions. The operational nodes rapidly create kill chains according to the combat mission. At this time, the cooperative network has full combat capability, and its performance is the best. With the depth of the combat process, the enemy launches an attack at t_1. The cooperative network enters the self-prevention state. In the prevention stage, the system relies on its own adaptive mechanism to deal with the threat event. If prevention is successful, the system's operational capability is maintained. Otherwise, the system enters the degradation state, and the system combat capability decreases at time t_2. In the degradation stage, the system will reformulate the combat plan according to the current mission and environment. Meanwhile, the supply nodes deploy resources to the operational nodes that urgently need material supply. The system performance degradation time can be neglected. At time t_4, the system enters the recovery phase, and the combat capability starts to recover gradually.

The concept and calculation formula of kill chains are introduced in Section 2. In this paper, the number of kill chains is adopted as the performance index of the air-ground cooperative network. The performance of the cooperative network can be expressed by

$$P(t) = \sum_{TSDIT\in\Gamma} N_{TSDIT}, \tag{9}$$

where Γ is the set of the main types of kill chains in the network. $P(t)$ is the performance function, which is expressed as a function of time t. In this paper, the recovered performance and degraded performance are used to calculate the resilience [30]. Therefore, the resilience of the network can be calculated by

$$R = \frac{P(t_5)-P(t_3)}{P(t_0)-P(t_3)}. \tag{10}$$

4.2. Resilience optimization strategies

In the actual combat process, some operational nodes will fail due to enemy attack or lack of supplies. When a node fails, the connecting edges with the node will fail at the same time. Meanwhile, the number of kill chains that can be formed in the cooperative network will be affected, which will cause the performance of the network to degrade. In order to improve the network combat capability and strike resistance, the failed kill chain will be dynamically reorganized with other nodes of the same function. The closure of the kill chain is achieved by re-establishing the connectivity. In this section, three dynamic recovery strategies are considered: node reconfiguration strategy (Strategy 1), intra-chain reconfiguration strategy (Strategy 2), and inter-chain reconfiguration strategy (Strategy 3). Figure 5 depicts the three dynamic recovery strategies of the kill chain $T \rightarrow S \rightarrow S \rightarrow D \rightarrow I \rightarrow T$. Suppose that a node V_A^S in the network is attacked. V_A^S has failed, and the edges connected to V_A^S have failed.

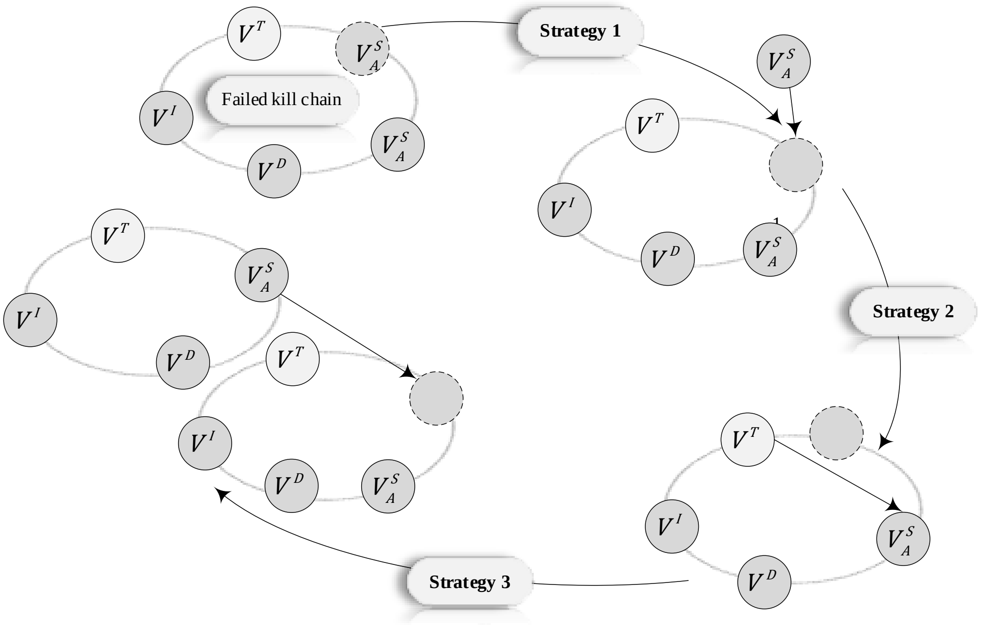


Figure 5. The dynamic recovery strategies of kill chains.

Strategy 1 is the node reconfiguration strategy. Strategy 1 is to select individual nodes of the same type in the whole network to replace the failed node V_A^S. There are some redundant nodes in the cooperative network, which can be quickly put into the combat process to replace the failed node V_A^S. For the V_A^S, we judge the failure mode of it first. After that, the support node will repair it or provide supplies to it. If conditions permit, the failed node can re-engage in the combat process after maintenance. Strategy 2 is the intra-chain reconfiguration strategy. Strategy 2 refers to the selection of the remaining nodes to replace the failed nodes if the remaining nodes in the failed kill chain have the same function of the V_A^S. According to Section 2, the information-sharing kill chains generally have multiple decision nodes and observe nodes, so Strategy 2 is only applicable to information- sharing kill chains. Strategy 3 is the inter-chain reorganization strategy. If there is no node in the failure kill chain that has the same function as the failure node, then it will find the same type of node in other normal kill chains in the network.

The three strategies proposed in this paper can be used at the same time. However, whether the three strategies can be successfully used is related to whether the alternative nodes meet the reconfiguration conditions. Taking the failed node V_A^S as an example, the detection ability of the new node V_{new}^S should be no less than the detection ability of the target node in the current failed kill chain. The node V_{new}^S also satisfies that the target node is within its detection range. If the alternative node does not meet the reconfiguration conditions, it will not be able to reconfigure the kill chain. Figure 6 is the reconfiguration process for the air-ground cooperative network. The algorithm of resilience evaluation and optimization is shown below.

Input: the node connection probabilities P_{SS}, P_{SD}, P_{DI}, P_{IT}, P_{TS}; generate the initial network $\psi = (G, \phi)$, the number of iterations N, simulation time T, node attributes $S_i(x_i, y_i, z_i, t_i, d_i)$, $D_i(x_i, y_i, z_i)$, $I_i(x_i, y_i, z_i, k_i)$, $T_i(x_i, y_i, z_i, b_i, c_i)$, probability of attack failure $(\lambda_S, \lambda_D, \lambda_I)$, probability of supply failure $(\mu_S,\ \mu_D,\ \mu_I)$, probability of maintenance (τ_S, τ_D, τ_I).

Output: the number of kill chain, the resilience of the network.

```
Initialization:  $n = 1,\ t = 1$
 for $n$ to $N$ do
     for $t$ to $T$ do
      Random attack & Deliberate attack
          Random attack: The failure time of nodes follows distribution exponentially. In the
          simulation time range, if the sampling result is within this range, it is considered that the
          node fails randomly.
          Deliberate attack: The node with the highest degree of nodes is selected for deliberate attack.
       Remove the failed nodes and their connected edges.
       Calculate the number of kill chains KL and record the data.
      Performance recovery process: Three dynamic recovery strategies: (i) node reconfiguration
      strategy, (ii) intra-chain reconfiguration strategy, (iii) inter-chain reconfiguration strategy.
      Calculate the number of kill chains and record the data.
      Calculate the resilience of the network and record the data.
    end for
end for
```

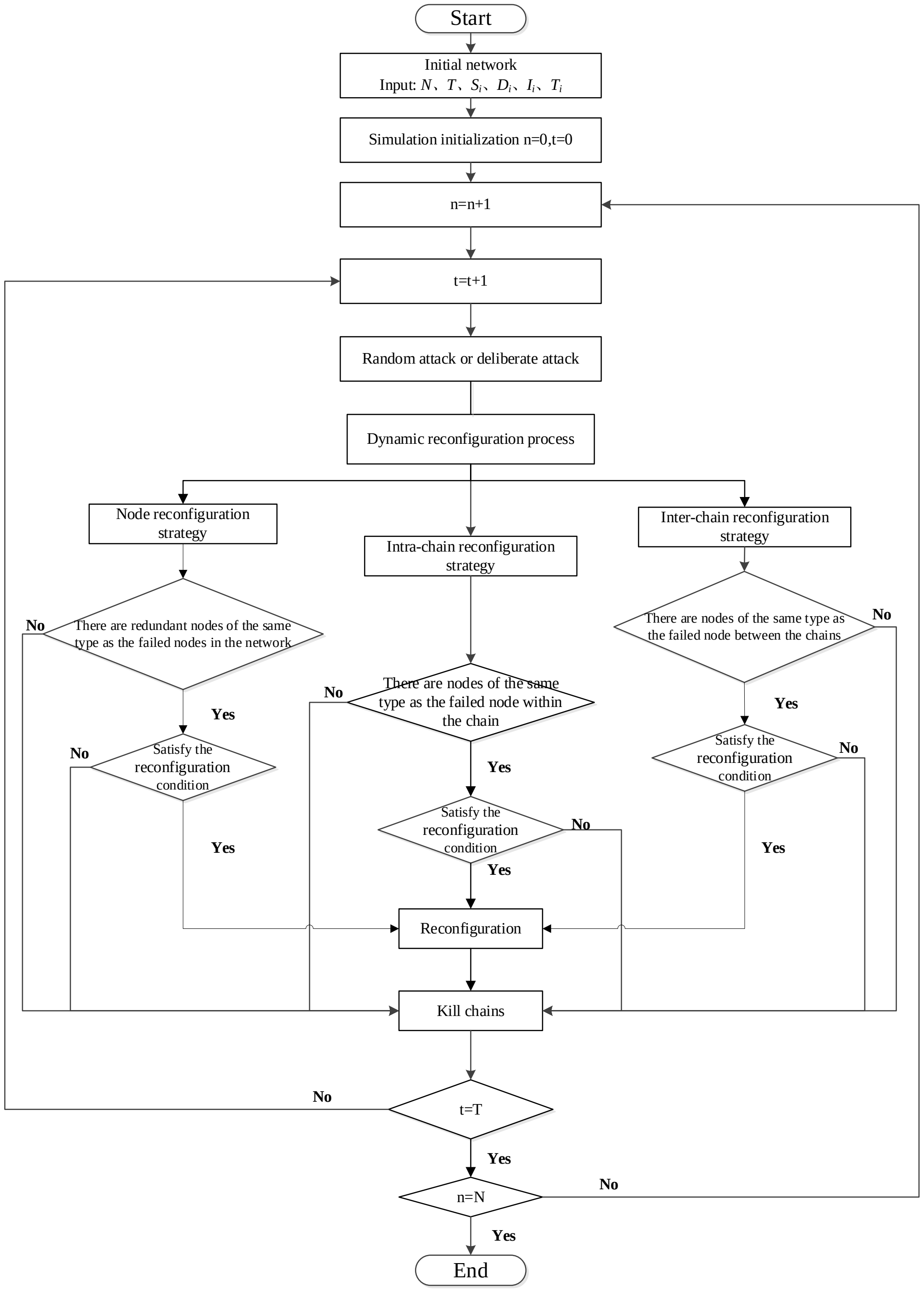

Start
Initial network
Input: N、T、S_i、D_i、I_i、T_i
Simulation initialization n=0,t=0
n=n+1
t=t+1
Random attack or deliberate attack
Dynamic reconfiguration process
Node reconfiguration strategy
Intra-chain reconfiguration strategy
Inter-chain reconfiguration strategy
There are redundant nodes of the same type as the failed nodes in the network
There are nodes of the same type as the failed node within the chain
There are nodes of the same type as the failed node between the chains
Satisfy the reconfiguration condition
Yes
No
Reconfiguration
Kill chains
t=T
n=N
End

Figure 6. The reconfiguration process for the air-ground cooperative network.

5. Result analysis

In this section, an air-ground cooperative network containing 50 nodes is selected to verify the effectiveness of the proposed method. In the air network and the ground network, the number of target nodes is 8, the number of sensor nodes is 8, the number of decision nodes is 3, and the number of attack nodes is 6. The widely used random attack strategy and deliberate attack strategy are selected to attack the operational nodes. The deliberate attack selects the degree prioritized attack strategy.

Figure 7 shows the number of kill chains in the cooperative network under different attack strategies.

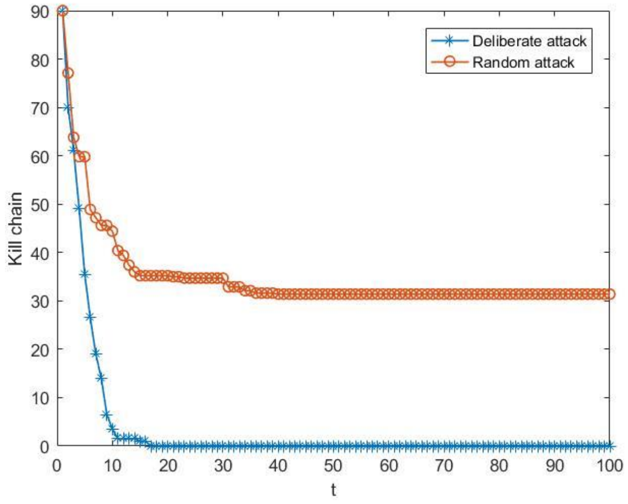


Figure 7. Kill chains under different attack strategies.

The deliberate attack strategy prioritizes nodes with a large node degree for attack. These nodes have more connected edges in the network, which will lead to more kill chain breaks in a short time once they fail. As can be seen from Figure 7, the number of kill chains decreases faster when deliberate attacks are made on the cooperative network, and the combat effectiveness of the network decreases rapidly in a short period of time. As a result, the deliberate attack strategy destroys the network to a greater extent.

Figure 8 shows the number of kill chains with different dynamic recovery strategies under random attacks. The resilience of the cooperative network under random attacks with dynamic recovery strategies is shown in Figure 9.

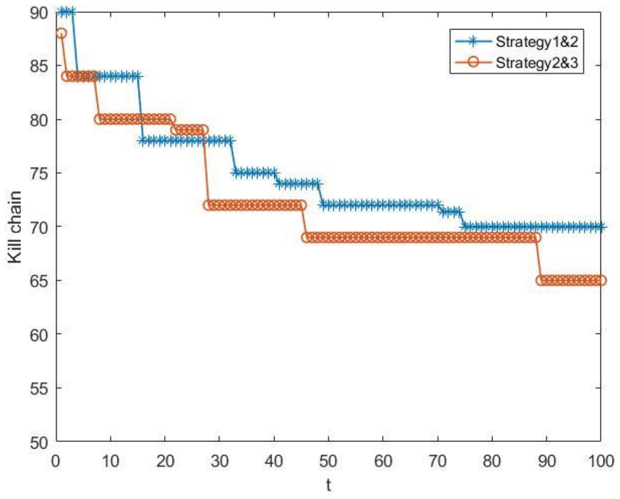


Figure 8. Kill chains with different recovery strategies.

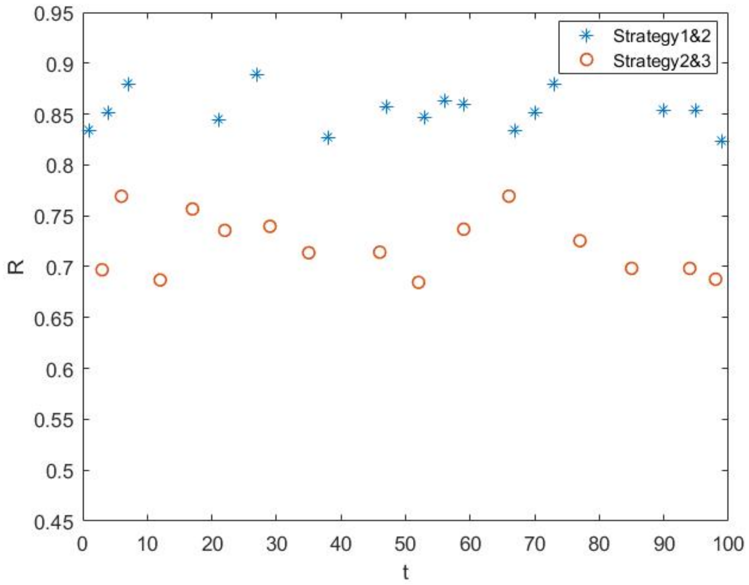


Figure 9. Resilience with different strategies.

It can be seen that the two combined strategies have certain effects on the recovery of network combat capability. In the whole recovery process, with the increase of the number of failed nodes, the number of kill chains under the two combination strategies showed a downward trend. However, in 1000 simulations, the average number of kill chains of strategies 1 and 2 is greater than strategies 2 and 3 because using strategy 1 not only reestablishes the connection edge, but also adds redundant nodes or repair nodes to the combat network. In contrast, using strategies 2 and 3 simply re-closes the kill chain by reestablishing the connecting edge. Considering the limited resources, the number of connections between nodes is affected by their own capacity constraints, the number of channels, and other factors. As a result, the recovery effect is slightly worse than with strategies 1 and 2, but it still helps the collaborative network recover its combat capability.

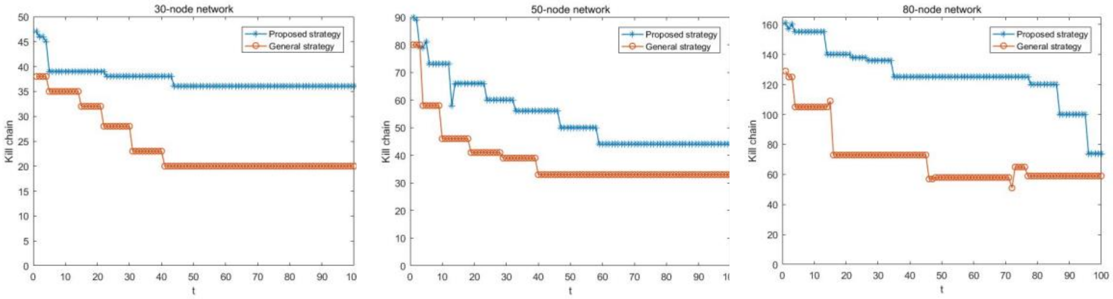
The resilience can be maintained at a high level when adopting strategies 1 and 2 under multiple attacks. This indicates that the cooperative network can recover combat capability in time, and re-close the kill chain quickly to accomplish the combat mission. In addition, the adoption of strategies 2 and 3 can also maintain a certain degree of resilience. In the real combat process, if redundant nodes do not exist in the network or the damaged nodes cannot be repaired in time, then strategies 2 and 3 can also re-close the kill chain quickly. However, due to the limitation of unrepaired failed nodes, the resilience of strategies 2 and 3 is less than the resilience of taking strategies 1 and 2. It should be noted that in actual military activities, the environment changes rapidly and there is great uncertainty. Compared with strategy 1, strategies 2 and 3 can reconstruct the kill chain in a short time and restore combat capability.

In order to ensure the scalability of the proposed recovery strategies in different scale networks, the 30-node network and the 80-node network are selected for comparative analysis. The detailed information of the nodes in the networks is shown in Table 1.

Table 1. The detailed information of the nodes for different networks.

Network	S	D	I	T
30-node	10	4	8	8
50-node	16	6	12	16
80-node	28	8	20	24

The method in the literature [28] has been compared with the model proposed in this paper. The kill chain number of three networks of different sizes under different reconstruction strategies are shown in Figure 10.



(a) 30-node network

(b) 50-node network

(c) 80-node network

Figure 10. The number of kill chains with different strategies for different networks.

As can be seen from Figure 10, under multiple attacks, the proposed method can effectively improve the number of kill chains for different scale networks compared with the method from reference [28]. The three reconfiguration strategies proposed in this paper can be combined according to the specific conditions of the network to reconstruct the kill chain. It can effectively use existing resources, reduce costs, and avoid unnecessary waste of resources.

It is worth noting that the reconfiguration strategy given by the proposed method can provide guidance for operators. However, operators often make decisions based on experience in the real combat environment. This may have a certain impact on the resilience evaluation and optimization of the system. At the same time, different operators have different psychological qualities and abilities, and the accuracy of their decisions is difficult to quantify. In the future, we will incorporate the psychological factors of the operator into the model to explore its impact on the rapid reconfiguration of the kill chain.

6. Conclusions

How the cooperative network can quickly resist, react, and recover from the interference of threatening events to accomplish the combat mission has become a key concern. In order to help combat networks quickly recover combat capability under interference events, this paper established a resilience assessment optimization model for the air-ground cooperative network. Three dynamic reconfiguration strategies were proposed to defend against attack threats. A typical 50-node network is taken as an example to verify the effectiveness of the proposed method through a large number of experiments. Moreover, its effectiveness on three different scale networks was analyzed. Compared with the currently available methods, the three strategies in the model can effectively utilize the existing resources and be combined according to different failure situations and scales. It has significant advantages in increasing the number of kill chains and improving combat capabilities. The dynamic recovery strategies proposed in this paper can help the combat network cope with multi-dimensional and fast-paced combat, and provide scientific guidance for the cooperative combat network to improve combat capabilities.

In fact, the reconfiguration time and cost of different reconfiguration strategies also have a certain impact on the resilience enhancement. In the future, the reconfiguration time and cost of different reconfiguration strategies will be taken into account in our model, and the multi-objective optimization problem will be solved by the collaborative neurodynamic approach. In addition, the nodes in the air-ground cooperative network are interdependent and the coupling relationship among them is close. In the future, we will consider using fuzzy similarity theory [31] to improve the modeling of complex relationships between nodes in the air-ground cooperative network.

Use of AI tools declaration

The authors declare that they have not used artificial intelligence (AI) tools in the creation of this article.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under grant numbers 72101270 and U2341213, and the China Postdoctoral Science Foundation under grant number 2023M732834.

Conflict of interest

The authors declare that there are no conflicts of interest.

References

1. Y. Sun, Z. Fang, Research on projection gray target model based on FANP-QFD for weapon system of systems capability evaluation, *IEEE Syst. J.*, **15** (2020), 4126–4136. https://doi.org/10.1109/JSYST.2020.3027585
2. X. Wang, Y. Zhang, L. Wang, D. Lu, G. Zeng, Robustness evaluation method for unmanned aerial vehicle swarms based on complex network theory, *Chin. J. Aeronaut.*, **33** (2020), 352–364. https://doi.org/10.1016/j.cja.2019.04.025
3. P. Uday, R. Chandrahasa, K. Marais, System importance measures: Definitions and application to system-of-systems analysis, *Reliab. Eng. Syst. Saf.*, **191** (2019), 106582. https://doi.org/10.1016/j.ress.2019.106582

4. Z. Chen, Z. Zhou, L. Zhang, C. Cui, J. Zhong, Mission reliability modeling and evaluation for reconfigurable unmanned weapon system-of-systems based on effective operation loop, *J. Syst. Eng. Electron.*, **34** (2023), 588–597. https://doi.org/10.23919/JSEE.2023.000082
5. K. Yang, J. Li, M. Liu, Complex systems and network science: a survey, *J. Syst. Eng. Electron.*, **34** (2023), 543–573. https://doi.org/10.23919/JSEE.2023.000080
6. J. Sun, B. Ge, J. Li, K. Yang, Operation network modeling with degenerate causal strengths for missile defense systems, *IEEE Syst. J.*, **12** (2016), 274–284. https://doi.org/10.1109/JSYST.2016.2570519
7. J. R. Cares, R. J. Christian, R. C. Manke, Fundamentals of distributed, networked military forces and the engineering of distributed systems, *NUWC-NPT Tech. Rep.*, **11** (2002), 200–209. https://www.researchgate.net/profile/Jeff-Cares/publication/235107120
8. J. Li, B. Ge, K. Yang, Y. Chen, Y. Tan, Meta-path based heterogeneous combat network link prediction, *Phys. A: Stat. Mech. Appl.*, **482** (2017), 507–523. https://doi.org/10.1016/j.physa.2017.04.126
9. J. Li, D. Zhao, J. Jiang, K. Yang, Y. Chen, Capability oriented equipment contribution analysis in temporal combat networks, *IEEE Trans. Syst. Man Cybern.: Syst.*, **51** (2018), 696–704. https://doi.org/0.1109/TSMC.2018.2882782
10. J. Li, J. Jiang, K. Yang, Y. Chen, Research on functional robustness of heterogeneous combat networks, *IEEE Syst. J.*, **13** (2018), 1487–1495. https://doi.org/10.1109/JSYST.2018.2828779
11. J. Sun, J. Li, Y. You, J. Jiang, B. Ge, Combat network link prediction based on embedding learning, *J. Syst. Eng. Electron.*, **33** (2022), 345–353. https://doi.org/10.23919/JSEE.2022.000036
12. L. Chen, C. Wang, C. Zeng, L. Wang, H. Liu, J. Chen, A novel method of heterogeneous combat network disintegration based on deep reinforcement learning, *Front. Phys.*, **10** (2022), https://doi.org/1021245. 10.3389/fphy.2022.1021245
13. C. Cheng, G. Bai, Y. Zhang, J. Tao, Resilience evaluation for UAV swarm performing joint reconnaissance mission, *Chaos*, **29** (2019), 190–200. https://doi.org/10.1063/1.5086222
14. B. A. Alkhaleel, H. Liao, K. M. Sullivan, Risk and resilience-based optimal post-disruption restoration for critical infrastructures under uncertainty, *Eur. J. Oper. Res.*, **296** (2022), 174–202. https://doi.org/10.1016/j.ejor.2021.04.025
15. B. Cai, Y. Zhang, H. Wang, Y. Liu, R. Ji, C. Gao, et al., Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance, *Reliab. Eng. Syst. Saf.*, **209** (2021), 107464. https://doi.org/10.1016/j.ress.2021.107464
16. A. J. Kerkhoff, B. J. Enquist, The implications of scaling approaches for understanding resilience and reorganization in ecosystems, *Bioscience*, **57** (2007), 489–499. https://doi.org/10.1641/B570606
17. Z. Chen, D. Hong, W. Cui, et al., Resilience evaluation and optimal design for weapon system of systems with dynamic reconfiguration, *Reliab. Eng. Syst. Saf.*, **237** (2023), 109409. https://doi.org/10.1016/j.ress.2023.109409
18. Z. Chen, T. Zhao, J. Jiao, J. Chu, Performance-threshold-based resilience analysis of system of systems by considering dynamic reconfiguration, *Proc. Inst. Mech. Eng.*, **236** (2022), 1828–1838. https://doi.org/10.1177/0954405420937528
19. S. Hosseini, D. Ivanov, A. Dolgui, Review of quantitative methods for supply chain resilience analysis, *Transp. Res. Part E: Logist. Transp. Rev.*, **125** (2019), 285–307. https://doi.org/10.1016/j.tre.2019.03.001

20. M. Liu, Q. Feng, D. Fan, H. Dui, B. Sun, Y. Ren, et al., Resilience importance measure and optimization considering the stepwise recovery of system performance, *IEEE Trans. Reliab.*, **178** (2022), 178–185. https://doi.org/10.1109/TR.2022.3196058
21. H. Dui, M. Liu, J. Song, S. Wu, Importance measure-based resilience management: Review, methodology and perspectives on maintenance, *Reliab. Eng. Syst. Saf.*, **235** (2023), 109383. https://doi.org/10.1016/j.ress.2023.109383
22. S. Geng, S. Liu, Z. Fang, A demand-based framework for resilience assessment of multistate networks under disruptions, *Reliab. Eng. Syst. Saf.*, **222** (2022) 108423. https://doi.org/10.1016/j.ress.2022.108423
23. H. Tran, M. Balchanos, J. Domerçant, D. N. Mavris, A framework for the quantitative assessment of performance-based system resilience, *Reliab. Eng. Syst. Saf.*, **158** (2017), 73–84. https://doi.org/10.1016/j.ress.2016.10.014
24. G. Bai, Y. Li, Y. Fang, Y. A. Zhang, J. Tao, Network approach for resilience evaluation of a UAV swarm by considering communication limits, *Reliab. Eng. Syst. Saf.*, **193** (2020), 106602. https://doi.org/10.1016/j.ress.2019.106602
25. C. Cheng, G. Bai, Y. Zhang, J. Tao, Improved integrated metric for quantitative assessment of resilience, *Adv. Mech. Eng.*, **12** (2020), 168–180. https://doi.org/10.1177/1687814020906065
26. Q. Sun, H. Li, Y. Wang, Y. Zhang, Multi-swarm-based cooperative reconfiguration model for resilient unmanned weapon system-of-systems, *Reliab. Eng. Syst. Saf.*, **222** (2022), 108426. https://doi.org/108426. 10.1016/j.ress.2022.108426
27. Q. Feng, M. Liu, B. Sun, H. Dui, X. Hai, Y. Ren, et al., Resilience measure and fformation reconfiguration optimization for multi-UAV systems, *IEEE Internet Things J.*, **11** (2024), 10616–10626. https://doi.org/10.1109/JIOT.2023.3326552
28. H. T. Tran, J. C. Domerçant, D. N. Mavris, A network-based cost comparison of resilient and robust system-of-systems, *Procedia Comput. Sci.*, **95** (2016), 126–133. https://doi.org/10.1016/j.procs.2016.09.302
29. X. Pan, H. Wang, Y. Yang, G. Zhang, Resilience based importance measure analysis for SoS, *J. Syst. Eng. Electron.*, **30** (2019), 920–930. https://doi.org/10.21629/JSEE.2019.05.10
30. Y. Cheng, E. A. Elsayed, Z. Huang, Systems resilience assessments: a review, framework and metrics, *Int. J. Prod. Res.*, **60** (2022), 595–622. https://doi.org/10.1080/00207543.2021.1971789
31. M. Versaci, G. Angiulli, P. Crucitti, D. D. Carlo, F. Laganà, D. Pellicanò, et al., A fuzzy similarity-based approach to classify numerically simulated and experimentally detected carbon fiber-reinforced polymer plate defects, *Sensors*, **22** (2022), 4232. https://doi.org/10.3390/s22114232