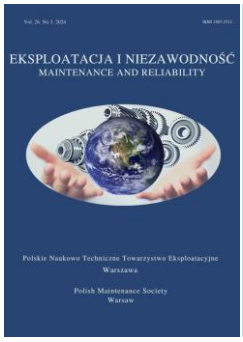


Eksploatacja i Niezawodnosc – Maintenance and Reliability

Volume 26 (2024), Issue 3

journal homepage: http://www.ein.org.pl

Article citation info:
Zhong Y, Li H, Zhuang X, A resilience-driven two-stage operational chain optimization model for unmanned weapon system-of-systems under limited resource environments Eksploatacja i Niezawodnosc – Maintenance and Reliability 2024: 26(3) http://doi.org/10.17531/ein/188198

A resilience-driven two-stage operational chain optimization model for unmanned weapon system-of-systems under limited resource environments

Indexed by: Web of Science Group

Yuanfu Zhong[a], Hongxu Li[a], Xuebin Zhuang[a,*]

[a] School of Systems Science and Engineering, Sun Yat-sen University, China

Highlights

- A task-oriented resilience metric is proposed to characterize the impact of operational chain changes on the resilience of weapon systems.
- A two-stage operational chain optimization model is constructed, considering the behaviours of edge nodes and command nodes in different resilience phases.
- The impact of operational chain optimization on resilience is analyzed in terms of different attack time, intensity, scenarios, task numbers and structures.

Abstract

Enhancing the battlefield resilience of unmanned weapon system-of-systems (UWSoS) through structural reconstruction requires scheduling additional physical resources. However, they are scarce in limited resource environments. To address the challenge of resource constraints, this paper focuses on improving the resilience of UWSoS by optimizing the operational chain of tasks after a disruption. First, a task-oriented resilience metric is proposed to characterize the impact of operational chain variations on UWSoS resilience. Based on this, a two-stage operational chain optimization model for UWSoS under limited resource environments is established, which considers the optimization actions of the edge node and rear command node in different resilience phases after the interruption for resilience enhancement. Finally, extensive simulation experiments validate the effectiveness and superiority of the proposed model. This work can support decision-makers in developing new task plans in disruption scenarios and serve as a transition approach to enhance UWSoS resilience.

Keywords
unmanned weapon system-of-systems, limited resource environments, operational chain optimization, resilience

1. Introduction

The development of information technology has prompted a shift in warfare patterns from traditional platform-centric combat to confrontations between various combat systems [1-3]. In this process, the emergence of Unmanned Weapon System-of-Systems (UWSoS) is crucial for military strategic development. UWSoS integrates various unmanned weapon platforms such as unmanned aerial vehicles (UAV), unmanned boats and unmanned combat vehicles, offering significant advantages in flexible deployment, rapid response, and adaptability to extreme battlefield environments [4-6]. However, UWSoS is susceptible to various external factors, including hostile attacks, electromagnetic interference, and internal system failures, all of which may undermine its mission capabilities on the battlefield [7]. Therefore, in-depth research and ensuring the battlefield anti-interference capabilities of UWSoS have significant military importance to enhance its future combat effectiveness.

Existing methods for enhancing anti-interference capabilities primarily focus on the study of reliability [8, 9], vulnerability[10, 11], and robustness[12, 13]. These methods

(*) Corresponding author.
E-mail addresses: Y. Zhong, zhongyf39@mail2.sysu.edu.cn, H. Li, lihx79@mail2.sysu.edu.cn, X. Zhuang (ORCID: 0000 0001 9456 3506) zhuangxb@mail.sysu.edu.cn,

maintain performance by introducing redundancy in nodes or functions when the system failures. However, the occurrence and intensity of interference are uncertain, and excessive redundant deployments may burden the system without achieving the desired effects. Therefore, there has been a growing interest in methods for rapid recovery from interruptions in recent years [14]. Resilience, as a relatively novel concept, combines the ability to withstand uncertain interferences and recover from disruptive events, and provides a new research direction for UWSoS operations. Resilience is defined as the system's or system-of-systems' ability to resist, maintain, and promptly recover expected performance through strategies and adaptations when faced with threats or disruptions [15, 16]. Subsequently, research on resilience has been widely conducted in fields such as sociology [17, 18], transportation [19, 20], and the military [21, 22].

Resilience assessment is the primary task of resilience research, which can quantify the comprehensive anti-interference capability of different systems. In the military domain, Sun [23] proposed a heterogeneous network structure for swarm systems and assessed the resilience by meta-operational loop counts. Xu et al. [24] calculated the number of anomalous UAVs of the faulty swarm under different time snapshots and used it as a resilience indicator. Wei et al. [25] evaluated the resilience of UAV swarms in terms of swarm topological dynamics. Zhang et al. [26] proposed a dynamic resilience evaluation method for cross-domain swarms in confrontation, calculate the resilience of the system at every moment in real time. Zhou et al. [27] investigated the collective behavior and resilience process of unmanned swarms under different partial failures and strategies through simulations. However, these assessment methods are mainly based on a structural perspective and neglect to consider battlefield mission benefits. Tran et al [28]. introduced an information exchange model for combat networks, which measured system resilience using variations in information gains received at each time step. Li et al [29]. evaluated the resilience of UAV swarms based on mission gains and route costs. However, these evaluation methods ignore the impact of the time factor on swarm resilience. Considering that the combat operation of UWSoS is an operational chain (OC) process that includes observation, positioning, decision, and action, different choices of OCs for tasks can have varying impacts on mission completion time and benefits [30]. Therefore, the above evaluation methodology would not apply to UWSoS, and the resilience assessment for UWSoS needs to consider the two critical factors of time and benefits simultaneously.

Reasonable resilience assessment provides guidance for resilience optimization, and many researchers have developed various resilience enhancing techniques. Lech et al. [31] directed the optimization of system maintenance strategies based on the concept of resilient maintenance. Zhang et al [32] and Xu et al [33]. guided the optimal repair sequence of damaged components through the elastic importance measure of components. However, the methods described above are limited to scenarios with a few damaged entities that can be repaired. Faced with random system failures, Feng et al [34]. optimized the resilience of UAV swarms by changing the formation structure. Chen et al [35]. proposed an adaptive reconstruction strategy for combat networks to enhance resilience against deliberate attacks. Sun et al [23]. presented a multi-swarm cooperative reconstruction approach, achieving high resilience values for equipment systems. Mou et al [36] and Tran et al [37]. enhanced the resilience of UAV swarms under attacks by reestablishing connections between remaining nodes, either randomly or purposefully. In these studies, resilience enhancement is primarily achieved through formation restructuring, system network reconstruction, or link reconnection. However, in limited resource environments, the reconstruction of the structure requires the scheduling of additional physical resources, thus this is not the preferred solution for UWSoS. When faced with destructive threats, it is prioritized to utilize limited physical resources by optimizing the task set’s OC to enhance the resilience of UWSoS. Second, the studies of the above optimization methods are conducted from a global perspective, while the rise of edge nodes has become inevitable in modern warfare [38], and the construction of optimization models should simultaneously consider the role factors of edge nodes.

In response to the aforementioned issues, we investigate the problem of enhancing the resilience of UWSoS when facing deliberate attacks. This study first proposes a task-oriented resilience metric, followed by a two-stage operational chain optimization model to improve UWSoS resilience from

a limited resource perspective. The following is the summary of the main contributions of this study:

- This paper proposed a task-oriented resilience metric for UWSoS, which considers both benefit and time factors in battlefield confrontations and can characterize the impact of changes in the task's OC on UWSoS.
- Considering the optimization behaviors of edge decision nodes and rear command nodes in different resilience phases, a two-stage operational chain optimization model for UWSoS is constructed for resilience enhancement.
- Monte Carlo and the Student's t-test experiments are designed in this paper to analyze the generalized resilience of UWSoS. The results can predict the degree of UWSoS resilience enhancement under different scales and conditions.

The rest of the paper is organized as follows. The background knowledge of UWSoS will be introduced in Section 2. The methodology will be presented in Section 3. Simulation experiments will be given in Section 4. The conclusion will be provided in Section 5.

2. Background

This section reviews knowledge of the UWSoS heterogeneous network structure and resilience process under the mission-based command model.

2.1. UWSoS under mission-based command model

Battlefield confrontation in the information age has shifted from centralized command and control to the mission-based command model [39], which is characterized by centralized command, distributed control, and decentralized execution. According to Cares' information-age combat model and Tan's combat cycle theory [40, 41], battlefield roles can be categorized into the following types: Sensor platforms (S) which are perform early battlefield intelligence, warning, and reconnaissance. Edge decision platforms (D) which are responsible for processing real-time mission intelligence and local task planning decisions. Influencer platforms (I) which are responsible for executing attacks against targets. The command platform (C), distinct from edge decision nodes, typically located in the rear of the battlefield, focuses on long-term objectives and broader battlefield situations, and is responsible for developing initial and post-attack global task plans.

UWSoS is a combination of unmanned weapon platforms located at the front of the battlefield with different capabilities. Abstract each platform as a node, and each flow as an edge. UWSoS can be characterized as a heterogeneous network $G = (V, E)$, where V denotes the set of nodes and E denotes the set of edges. Let $\mathcal{A}^V = \{S, D, I\}$ denote the set of node types, thus $V = V^S \cup V^D \cup V^I$. Similarly let $\mathcal{A}^E = \{S \to S, S \to D, D \to S, D \to D, D \to I\}$denote the set of edge types, and hence$E = E^{S\to S} \cup E^{S\to D} \cup E^{D\to D} \cup E^{D\to S} \cup E^{D\to I}$. Define node type mapping function ϕ_v and edge type mapping function ϕ_e, each node $v \in V$ has $\phi_v(v) \in \mathcal{A}^V$, and each edge $e \in E$ has $\phi_e(e) \in \mathcal{A}^E$.

The UWSoS is also subservient to the global task planning of the rear command platform in the battlefield, and the topological relationship between them can be represented as a directed graph $G_c = (V, E_c)$, where $V = \{v_1, v_2, \ldots, v_n\}$ denotes the nodes in the UWSoS, and $E = \{e_1^c, e_2^c, \ldots, e_{2n}^c\}$ denotes the communication link between each node and the command platform. The UWSoS under mission-based command model is shown in Fig. 1.

Enemy sensors, deciders, and influencer nodes are the targets of military operations, and an OC describes a complete engagement process. Sensor nodes detect enemy targets and, based on the planning of the command platform, deliver intelligence to the edge decision node, $S \to D$. Through data fusion and information analysis, the influencer nodes receive commands from decision nodes and execute strike actions, $D \to I$. Therefore, a primary OC is denoted as $S \to D \to I$. The generalized OC can be denoted as

$v_1 \xrightarrow{e_1} v_2 \xrightarrow{e_2} \cdots \xrightarrow{e_j} v_{j+1}$ with each edge type $\phi_e(e_1), \phi_e(e_2), \ldots, \phi_e(e_j) \in \mathcal{A}^E$, and for the nodes $v_1 \in V^S, v_j \in V^D, v_{j+1} \in V^I, v_{j'} \notin V^I (j' = 2,3,\ldots,j-1)$ [42]. Fig. 1 shows the generalized OC examples with semantic information detailed in Ref. [43].

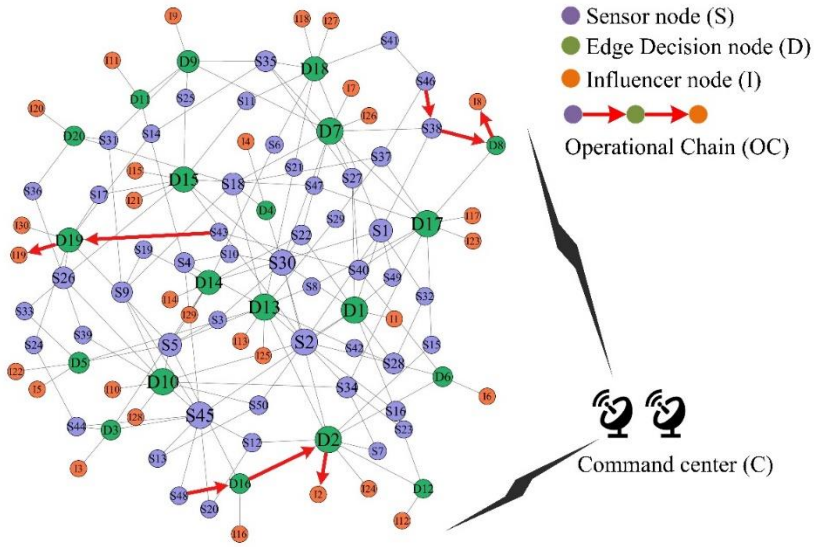


Figure 1. Topology of the UWSoS, generated with reference to [13]. Three OC examples are highlighted in red: $S_{43} \rightarrow D_{19} \rightarrow I_{19}$; $S_{46} \rightarrow S_{38} \rightarrow D_8 \rightarrow I_8$; $S_{48} \rightarrow D_{16} \rightarrow D_2 \rightarrow I_2$.

2.2. The resilience process of UWSoS

The UWSoS resilience process in the mission-based command model is shown in Fig. 2, where the dashed line represents the performance of the UWSoS without measures. At time t_a, the UWSoS is affected by attacks that will cause some of the tasks to not be executed according to the established plan, thus the performance starts to degrade. At this moment, the edge decision node will instantly make local adjustments to the affected OCs to reduce the extent of performance degradation, shown in Fig. 2 as $P_{m1} > P_{m2}$. Simultaneously, based on the local adjustments, the command platform will synchronously conduct global planning for the tasks. At time t_m, the UWSoS receives a new task plan from the command platform, and the performance is gradually restored to P_r.

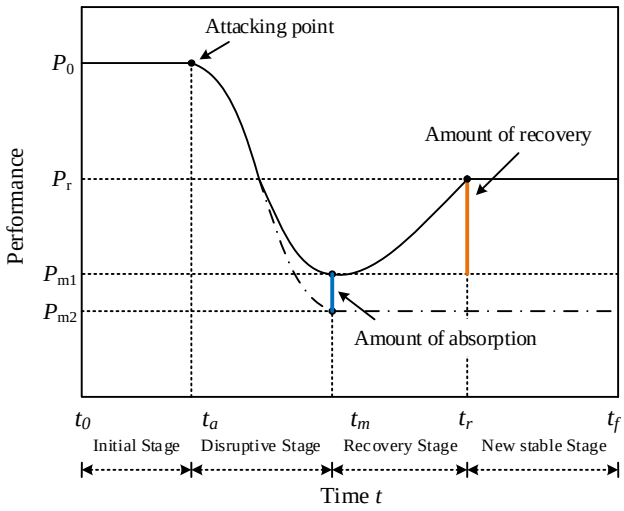


Figure 2. Resilience process of UWSoS.

3. Methodology

This subsection first proposed a task-oriented resilience metric for UWSoS. Then, a two-stage operational chain optimization model under limited resource environments is introduced to improve the resilience of UWSoS after the attack.

3.1. Resilience metric of UWSoS

3.1.1. The performance measure of UWSoS

Define $\mathcal{T} = \{T_1, T_2, \ldots, T_n\}$ to denote the n rounds of battlefield confrontation carried out by the UWSoS, where $T = \{1,2,\ldots,t_{end}\}$ denotes the time step required for the UWSoS to perform tasks in each round of battlefield confrontation. After a round of battlefield reconnaissance, the number of tasks m to be executed by UWSoS depends on the number of sensor nodes $|V^S|$ and the reconnaissance capability value p, which can be expressed as $m = |V^S| \cdot p$. Let $\mathcal{M} = \{M_1, M_2, \ldots, M_m\}$ represent the set of tasks that UWSoS needs to execute. The command platform, upon receiving reconnaissance responses, will make an OC planning for the overall tasks. OC will guide each task to be delivered to nearby edge decision nodes for intelligence processing and ultimately determine which influencer node will carry out the military strike. Assumes that at each time step in the simulation, task information can be transmitted from the current node location to the next node location guided by the OC. Let $\mathcal{L}_{M_i}$ denote the OC allocation for task M_i. Simultaneously, an OC matrix $\boldsymbol{O} \in \{0,1\}^{m \times l}$ is defined to represent the node locations to which each task is

transmitted at time t, where l represents the maximum OC length in $\mathscr{M}$. For task M_i, if it is delivered to location v_j in $\mathscr{L}_{M_i}$, then $O_{i,j} = 1$; otherwise, $O_{i,j} = 0$.

Similarly, for each influencer node, there exists an expected task sequence $L_k = \{M_1^k, M_2^k, \ldots, M_z^k\}$, where $k = 1,2,..,|V^I|$ and z denotes the anticipated number of tasks in L_k. Subsequently, the planned completion time of tasks within the sequence can be expressed as $\zeta(\cdot)$, by Eq. 1:

$$\begin{cases} \zeta(M_q^k) = len(l_{M_q^k}) + \frac{\lambda_{M_q^k}}{c_k} & ,q = 1 \\ \zeta(M_q^k) = len(l_{M_q^k}) + \Gamma_{wait}(M_q^k) + \frac{\lambda_{M_q^k}}{c_k} & ,q = 2,3,\ldots z \end{cases}, \quad (1)$$

Where $len(l_{M_q^k})$ represents the OC length of the task, indicating the time required for task transmission; $\lambda_{M_q^k}$ denotes the task difficulty value, c_k represents the capability value of node I_k, and $\lambda_{M_q^k}/c_k$ represents the time required for task execution; $\Gamma_{wait}(M_q^k)$ represents the waiting delay of a task. When multiple tasks are asynchronously delivered to the same influencer node, the task delivered later must wait for the completion of the previous. The calculation of the waiting delay is as follows:

$$\Gamma_{wait}(M_q^k) = \begin{cases} \zeta(M_{q-1}^k) - len(l_{M_q^k}) & ,if \quad \zeta(M_{q-1}^k) \geq len(l_{M_q^k}) \\ 0 & ,if \quad \zeta(M_{q-1}^k) < len(l_{M_q^k}) \end{cases}. \quad (2)$$

The benefit of UWSoS refers to the task value obtained through the execution of strike tasks, and after the planned completion time of the task is known, the value of each task $\mathcal{V}(M_i)$ is calculated as shown in Eq. 3:

$$\mathcal{V}(M_i) = \Delta^{\zeta(M_i)} + \eta, \quad (3)$$

Where $\Delta^{\zeta(M_i)}$ denotes the base value component and $\Delta \in \{0,1\}$ is the time sensitivity parameter. A low Δ value indicates that the battlefield is more time sensitive. The η is the additional value component, where completed tasks of various difficulties can bring different additional rewards. The task difficulty value λ_{M_i} is taken from the discrete set $\{\lambda_S, \lambda_D, \lambda_I\}$, which represents the difficulty of destroying different types of enemy nodes; and η is taken from the discrete set $\{\eta_S, \eta_D, \eta_I\}$, which represents different amount of additional gain. Define mapping function $\psi(\cdot)$, if $\psi(M_i) = \lambda_S$, then $\eta = \eta_S$.

Define the task plan matrix $\boldsymbol{X}(t) = \left[\boldsymbol{x}_1(t), \boldsymbol{x}_2(t), \ldots, \boldsymbol{x}_{|V^I|}(t)\right]^T$ to represent the completion status for tasks at the planned time $t \in [0, t_{end}]$, where $\boldsymbol{x}_k(t) = [x_k^1, x_k^2, \ldots, x_k^m] \in \{0,1\}^m$, and:

$$x_k^\alpha(t) = \begin{cases} 0 & ,if \quad t \neq \zeta(M_\alpha^k) \\ 1 & ,if \quad t = \zeta(M_\alpha^k) \end{cases}. \quad (4)$$

If UWSoS is not subjected to interference or attacks, and all tasks are executed as scheduled. In that case, the achievable expected gain $\bar{B}(t)$ of the UWSoS can be expressed by Eq. 5:

$$\bar{B}(t) = ||\mathbf{X}(t)\mathbf{Val}^T||_1, \quad (5)$$

where $\boldsymbol{Val} = [\mathcal{V}(M_1), \mathcal{V}(M_2), \ldots, \mathcal{V}(M_m)]$ stands for the task value vector, and $||\boldsymbol{A}||_1$ in this paper is defined as the sum of the absolute values of all elements in matrix $\boldsymbol{A}$.

However, in a confrontation scenario, the UWSoS will be affected by enemy attacks at any moment. Suppose $V!$ represents the set of damaged nodes, and $V/V!$ represents the set of operational nodes, then the node damage matrix of the OC can be expressed as $\boldsymbol{D}^V \in \{0,1\}^{m \times l}$, with matrix elements satisfied:

$$\begin{cases} \mathbf{D}_{i,j}^V = 1 & ,if \quad \{v_j \in V! \,|v_j \in \mathcal{L}_{M_i}\} \\ \mathbf{D}_{i,j}^V = 0 & ,if \quad \{v_j \in V/V! \,|v_j \in \mathcal{L}_{M_i}\} \end{cases}. \quad (6)$$

Similarly, suppose $E!$ denotes the set of damaged edges, and $E/E!$ represents the set of normal edges, then the edge damage matrix of the OC can be denoted as $\boldsymbol{D}^E \in \{0,1\}^{m \times (l-1)}$.

To summarize, the delivery status of each task at time t can be represented by the vector $\boldsymbol{Z}(t) = [Z_1(t), Z_2(t), \ldots, Z_m(t)] \in \{0,1\}^{1 \times m}$, with any given $Z_i(t)$ computed as follows:

$$Z_i(t) = \wedge_{j=\min(t,l)}^{l} \left(\mathbf{O}_{i,j} \Rightarrow \neg\left(\wedge_{p=j}^{l} \left(\mathbf{D}_{i,p}^V \vee \mathbf{D}_{i,p}^{\prime E}\right)\right)\right), \quad (7)$$

Where $Z_i(t) = 1$ indicates that the OC of the task is unaffected by strikes, otherwise $Z_i(t) = 0$. The symbol $\wedge$ represents the logical AND operation. The symbol $\Rightarrow$ represents the implication operation, indicating that if task M_i is guided for intelligence transmission based on OC at time t, then the subsequent condition must be true for the transmission not to be interrupted. The symbol $\vee$ represents the logical OR operation. $\boldsymbol{D}^{\prime E}$ is an extended matrix of $\boldsymbol{D}^E$ to match the size of $\boldsymbol{D}^V$.

Subsequently, the actual gain $B(t)$ of executing tasks by UWSoS at time t can be expressed as:

$$B(t) = ||\mathbf{X}(t)(\mathbf{Z}(t) \circ \mathbf{Val})^T||_1, \quad (8)$$

where the symbol $\circ$ represents the Hadamard product, which signifies the element-wise multiplication of matrices.

Refer to Ref.[29], the costs of UWSoS primarily consist of two parts: physical damage costs and energy consumption for task transmission. Firstly, adversaries can achieve the purpose of affecting or interrupting task delivery by destroying nodes or edges. In this scenario, the cost of damaged nodes or edges within UWSoS is the physical damage cost $U(t)$, calculated as

shown in Eq .9:

$$U(t) = \mathbf{1}^T(\mathbf{H}^V(t)\mathbf{Cov}^T + \mathbf{H}^E(t)\mathbf{Coe}^T), \quad (9)$$

Where $\mathbf{Cov} \in \mathbb{R}_+^{1\times|V|}$, $\mathbf{Coe} \in \mathbb{R}_+^{1\times|E|}$represent the cost vectors of nodes and edges in UWSoS, respectively; $\boldsymbol{H}^V(t) = \mathrm{diag}(h_1^V, h_2^V, \ldots, h_{|V|}^V) \in \{0,1\}^{|V|\times|V|}$ is the damage matrix of the nodes at time t, and $\boldsymbol{H}^E(t) = \mathrm{diag}(h_1^E, h_2^E, \ldots, h_{|E|}^E) \in \{0,1\}^{|E|\times|E|}$ is the damage matrix of the edges at time t.

Secondly, the expected energy consumption for task delivery is calculated as follows:

$$\bar{K}(t) = \sigma \cdot \sum_{i=1}^{m} \min(t, len(\mathcal{L}_{M_i})) - 1, \quad (10)$$

where, $\sigma \in \{0,1\}$ represents the information transmission energy consumption in each time step. It is noted that, due to the impact of strikes, some of the tasks will be abandoned for execution due to interference or node damage. Therefore, the actual transmission energy consumption for task delivery can be expressed as:

$$K(t) = \sigma \cdot \sum_{i=1}^{m} \max(0, \{j-1 |\ \mathbf{O}_{i,j} = 1\}). \quad (11)$$

Based on the costs and benefits of UWSoS, we can further calculate the equation of the net benefits obtained from UWSoS task execution, as shown in Eq. 12:

$$\mathcal{B} = \sum_{t=0}^{end}(B(t) - U(t)) - K(t_{end}). \quad (12)$$

Specifically, suppose UWSoS is not subjected to interference or strikes, and all tasks are executed according to the established plan. In that case, the expected net benefits that UWSoS can achieve are given by Eq. 13:

$$\overline{\mathcal{B}} = \sum_{t=0}^{end}(\bar{B}(t)) - \bar{K}(t_{end}). \quad (13)$$

According to the formulas above, the performance value $P(\tilde{t})$ of UWSoS at time $\tilde{t}$ can be determined as:

$$P(\tilde{t}) = \frac{\mathcal{B}(\tilde{t})}{\overline{\mathcal{B}}} = \frac{\sum_{t=0}^{t_{end}}(B_{\tilde{t}}(t) - U_{\tilde{t}}(t)) - K_{\tilde{t}}(t_{end})}{\sum_{t=0}^{t_{end}}(\bar{B}(t)) - K(t_{end})}, \quad (14)$$

where $\tilde{t} \in [0, \tilde{t}_{end}]$ represents the actual time, and $t \in [0, t_{end}]$ represents the planned time. $\mathcal{B}(\tilde{t})$ denotes the total expected net benefit obtained with the task planning at the actual time step $\tilde{t}$.When $P(\tilde{t}) = 1$, it signifies that UWSoS has achieved the expected benefit during the task execution process.

3.1.2. The resilience measure of UWSoS

Based on the multi-round characteristics of UWSoS battlefield confrontation, its resilience assessment needs to consider both the system performance variation and the impact of the overall task completion time on the system resilience, as shown in Fig. 3.

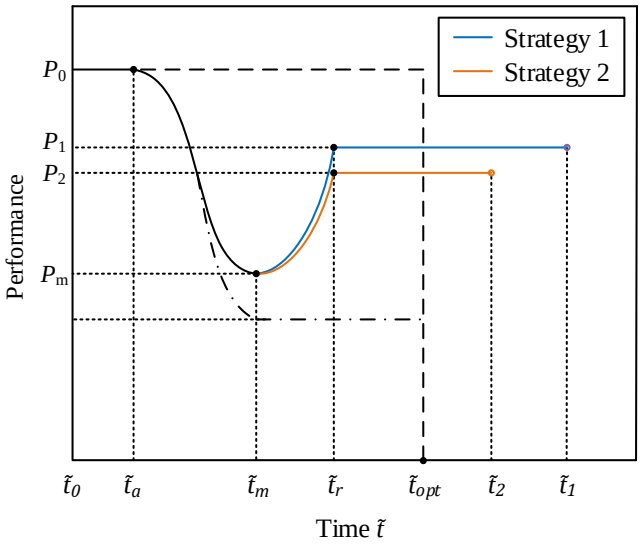


Figure 3. Task-oriented resilience process of UWSoS.

From Fig. 3, assuming that two strategies exist for performance recovery at $\tilde{t}_m$ moment. Strategy 1 can restore UWSoS's performance to P_1, with an overall task completion time of $\tilde{t}_1$; Strategy 2 can restore UWSoS's performance to P_2, with a corresponding overall task completion time of $\tilde{t}_2$; where $P_1 > P_2$, $\tilde{t}_1 > \tilde{t}_2 > \tilde{t}_{opt}$, and $\tilde{t}_{opt}$ is the overall task completion time of the original plan. Consider part of the confrontation scenario, when $P_1 > P_2$ but $\tilde{t}_1 >> \tilde{t}_2$. Although Strategy 2 exhibits inferior recovery performance compared to Strategy 1, it enables UWSoS to accomplish the current round of combat tasks within a shorter timeframe. This capability facilitates the swift transition of UWSoS into subsequent adversarial activities. In contrast, Strategy 1's pursuit of restoring UWSoS to higher performance significantly extends the overall task completion time. Such an extension will be detrimental to the comprehensive task planning of UWSoS in subsequent adversarial engagements. Therefore, taking into account the performance and time factors, the resilience metrics of UWSoS can be formulated as follows:

$$R = \frac{1}{2}\left(\frac{P(\widetilde{t_m})}{P(\widetilde{t_a})} + \frac{P(\widetilde{t_r})}{P(\widetilde{t_a})}\right) \cdot \frac{\sum_{\tilde{t}=0}^{\tilde{t}_f} P(\tilde{t})}{P(\tilde{t}_0)\cdot\tilde{t}_f}, \quad (15)$$

where $\frac{P(\widetilde{t_m})}{P(\widetilde{t_a})}$ and $\frac{P(\widetilde{t_r})}{P(\widetilde{t_a})}$ calculate the ability of UWSoS to absorb disturbances and recover from interruptions, respectively. $\frac{\sum_{\tilde{t}=0}^{\tilde{t}_f} P(\tilde{t})}{P(\tilde{t}_0)\cdot\tilde{t}_f}$calculate the ratio of actual performance to planned performance in the entire task cycle, where $P(\tilde{t})$ represents the actual UWSoS performance at time $\tilde{t}$, and $\tilde{t}_f$ stands for the completion time factor, taking values as follows:

$$\tilde{t}_f = \begin{cases} \tilde{t}_{end} & ,if \quad \tilde{t}_{end} \geq \tilde{t}_{opt} \\ \tilde{t}_{opt} & ,if \quad \tilde{t}_{end} < \tilde{t}_{opt} \end{cases}, \tag{16}$$

where $\tilde{t}_{end}$ represents the actual completion time of the overall task. A higher value of $\tilde{t}_f$ indicates a longer task completion time after recovery and will result in a lower resilience value for UWSoS.

3.2. Two-stage operational chain optimization model

3.2.1. Assumptions

To facilitate understanding of the model, several generic assumptions are given below.

1. The initial OC allocation for UWSoS tasks is assumed to be known. This study does not address the initial OC allocation issue, focusing on the post-damage recovery of UWSoS performance.

2. The efficiency of task information transmission is considered constant, and the processing of task information by nodes and the giving of battle orders are abstracted in a single time step.

3. Each influencer node is assumed to have sufficient power to complete all assigned tasks without regard to the details of its execution, considering only the time factors associated with task transmission and execution.

4. Node Attacks. Each attacked node in the UWSoS is presumed to be completely damaged, leading to the disconnection of associated links. If a node is attacked while holding task information, the tasks will be lost and cannot be reallocated.

5. Link Attacks. For the scenario of link attacks, this paper assumes that an attack on the link between two nodes in the UWSoS will disrupt bidirectional link communication. Unidirectional edge attacks are not considered.

6. UWSoS is under a limited resource environment. The limited resource environment refers to a situation where the resources available in a system or environment are restricted or scarce, and the environment constrains UWSoS from modifying its structure, including adding unmanned weapon nodes or changing the communication links between nodes.

3.2.2. Optimization model

The primary focus of this study is to enhance the post-attack recovery capability of the UWSoS during task execution without modifying its structure,this enhancement is achieved by optimizing the OCs of tasks. The optimization ideas of the two-stage operational chain optimization model (OCOM) are illustrated in Fig. 4.

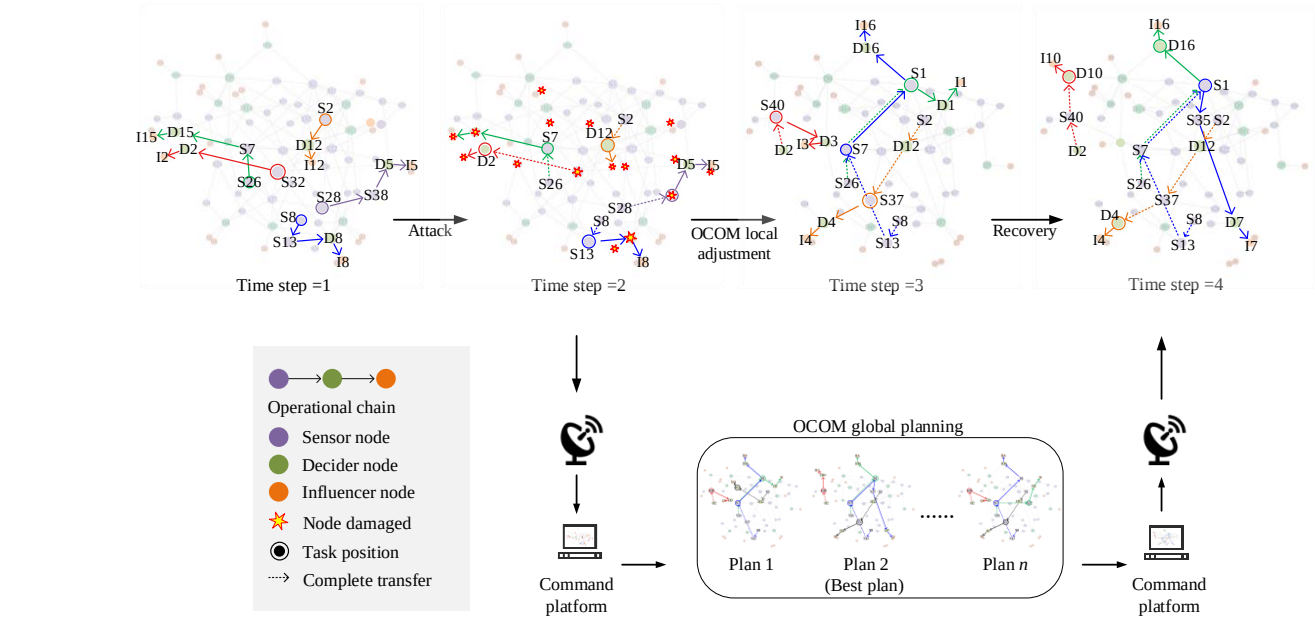


Figure 4. Research idea.

Fig. 4 illustrates the process of OC optimization by UWSoS under limited resource environments. In the initial phase, the network structure of UWSoS and established tasks are known, and we assume a fixed initial OC assignment for tasks. When the UWSoS suffers an attack during the execution of a task, the OC-based task delivery may face the following two scenarios: 1) the task is lost due to node damage, and 2) OC disruption preventing task delivery. The occurrence of these two scenarios

can lead to a decrease in the revenue of the task plans. As depicted in Fig. 4, when the above situation occurs (Time step = 2), OCOM will replan the task OC in two stages.

(1) First stage

The first stage of OCOM is the local adjustment process of the edge decision nodes to the interrupted OCs (Time step = 3), which focuses on the real-time, fast update of the interrupted OC. For each interrupted OC, the node to which the task is delivered is played as a central agent to form a task alliance with N hops as the transmission path for determining the update path of the interrupted OC. The local adjustment action of the edge decision node is considered to be completed in one time step, and each task alliance is synchronized in time. This paper adopts the Contract Network Algorithm as a collaborative strategy for task alliances, and the agent node will broadcast the task information to the task alliance. Upon receiving the broadcast message, the edge decision node calculates the benefit of receiving the task based on the redundant task capabilities of its subordinate influencer nodes and provides feedback. The update of interrupted OC will be accomplished through a bidding mechanism among the nodes, and the updated OC will also be synchronized to the command platform, influencing the value of $P(\widetilde{t_m})$.

(2) Second stage

The second stage of OCOM is the global optimization process of task OC by the command platform. The command platform receives the local adjustment results from the edge decision nodes synchronously at time step 2 and, after one time step of global optimization computation, returns the globally optimized OC information to the UWSoS at time step 4 to achieve the performance recovery and ultimately enhances the resilience of the UWSoS. The optimization in the second stage focuses on the global OC's high gain and low total elapsed time, and thus is a multi-objective optimization problem concerning the recovery performance $P(\tilde{t}_r)$ and the time $\tilde{t}_{end}$. This paper adopts the Non-dominated Sorting Genetic Algorithm (NSGA-II) to solve the optimization result. When the locally adjusted OC information and the damage information of the UWSoS are processed by the computing device embedded with the NSGA-II, the device outputs the feasible solutions on the Pareto frontier as the optimization result. Subsequently, the solution with the highest R value in the Pareto set is computed by Eq. 15 and output as the decision result returned to UWSoS. The resilience metric R is a function of variation performance $P(\widetilde{t_m})$,$P(\tilde{t}_r)$ and time $\tilde{t}_{end}$, therefore can be used to measure the resilience of the optimization results.

3.2.3. Objective function and constraints

Based on the model description, the objective function and constraints of OCOM are given in this section. First, the optimization decision in the first stage is limited by the local perspective, thus the solution with the highest task gain among the finite solutions is taken as the decision result in this stage. Second, the core objective of the second stage optimization is high task gain and low total elapsed time in the global perspective. Thus, the objective function is constructed as the maximum value of the performance $P(\tilde{t}_r)$ and the minimum value of the time $\tilde{t}_{end}$, as shown in Eq. 17, where $\omega_{\tilde{t}}$ and ω_p denote the weight of the time factor and the weight of the recovery performance factor, respectively.

$$\begin{cases} max \ \ \omega_p P(\tilde{t}_r) \\ min \ \ \omega_{\tilde{t}} \tilde{t}_{end} \end{cases}. \tag{17}$$

Subsequently, this subsection gives the constraints of OCOM from two aspects: capability constraints and strategic constraints.

(1) Capability constraints

Under the given assumptions, each influencer node in UWSoS is considered to have a limited task execution capability and must satisfy the following inequality:

$$\left(\sum_{t=0}^{t_{end}} \mathbf{X}_{\tilde{t}}(t)\right)\mathbf{1} \le \mathbf{C}^T, \forall \tilde{t} \in [0, \tilde{t}_{end}], \tag{18}$$

where $\mathbf{C} \in \mathbb{R}_+^{1\times|\boldsymbol{V^I}|}$ denotes the initial task capability vector of the influencer node. This paper establishes a convention for comparing two matrices, if every element in matrix $\boldsymbol{A}$ is less than or equal to the corresponding element in matrix $\boldsymbol{B}$, this relationship will be represented as $\boldsymbol{A} \le \boldsymbol{B}$. Eq. 18 indicates that for the UWSoS task plan $\boldsymbol{X}_{\tilde{t}}(t)$ at any actual time $\tilde{t}$, it must be ensured that the tasks assigned to each influencer node cannot exceed the upper limit of its capability value.

Similarly, UWSoS also needs to ensure that each task guided by OC is only delivered to one influencer node for execution, the constraints need to satisfy Eq. 19.

$$\left(\sum_{t=0}^{t_{end}} \mathbf{X}_{\tilde{t}}^T(t)\right)\mathbf{1} = \mathbf{1}, \forall \tilde{t} \in [0, \tilde{t}_{end}]. \tag{19}$$

(2) Strategic constraints

Eq. 20 constrains OCOM to be executed only when there is

a task loss or OC interruption. Eq. 21 constrains OCOM to reduce the number of tasks executed after an attack when available resources are reduced.

$$\left|\left|\mathbf{1}-\mathbf{Z}(\tilde{t}_a)\right|\right|_1 > 0. \tag{20}$$

$$\left|\left|\sum_{t=0}^{t_{end}} \mathbf{X}_{\tilde{t}}^T(t)\right|\right|_1 \le \left|\left|\sum_{t=0}^{t_{end}} \mathbf{X}^T(t)\right|\right|_1, \forall \tilde{t} \in [\tilde{t}_r, \tilde{t}_{end}], \tag{21}$$

4. Experiment and analysis

In this section, experiments consider two typical enemy attack scenarios: node attack scenarios and link attack scenarios, to demonstrate the feasibility and superiority of the proposed OCOM. The experimental environment employed in this paper consists of a PC with an Intel(R) Core(TM) i7-9750H processor and 32GB of RAM. We utilized PyCharm as the compilation platform for all algorithms in this study. Furthermore, this paper refers to the data in [44], set the value of $\Delta = 0.9$, $\sigma = 0.2$, $\{\lambda_S, \lambda_D, \lambda_I\} = \{4,8,6\}$,$\{\eta_S, \eta_D, \eta_I\} = \{0,0.15,0.1\}$, $\omega_{\tilde{t}} = 0.3$ and $\omega_p = 0.7$.

4.1. Optimization method analysis for UWSoS

To validate the feasibility of the resilience metric and optimization method proposed in this paper, first, we refer to the weapon system topology generator in Ref. [13] and consider a UWSoS consisting of 100 nodes and 334 edges, of which 50 are *S* nodes, 20 are *D* nodes, and 30 are *I* nodes. The topology of UWSoS, as shown in Fig. 1, and the capability attributes of the *I* node are shown in Table 1. Each *I* node can complete up to 2 tasks. The reconnaissance capability of UWSoS is fixed as 0.7, i.e., the surveillance generates 35 task combat scenarios, and the specific task parameters are shown in Table 2. Second, we consider the random node attack strategy (RN) and random link attack strategy (RL) under two typical attack strategies. Based on the UWSoS structure and task parameters mentioned above, suppose the enemy attacks at time step 2, with an attack intensity of 0.3, which means that a random 30% of nodes will be attacked and damaged in the node attack scenario, and a random 30% of links will be interrupted in the link attack scenario.

Table 1. The capability attributes of the *I* node.

Capability	Node
2	$I_1, I_2, I_4, I_6, I_9, I_{11}, I_{12}, I_{14}, I_{15}, I_{16}, I_{20}, I_{21}, I_{25}, I_{26}, I_{29}$
3	$I_3, I_7, I_{10}, I_{13}, I_{17}, I_{18}, I_{19}, I_{23}, I_{24}, I_{27}, I_{28}, I_{30}$
4	I_5, I_8, I_{22}

Table 2. Task parameters and initial OC.

Task	Diff	Operational chain	Benefit	Task	Diff	Operational chain	Benefit
M_{S1}	8	$S_1 \to D_{18} \to I_{18}$	0.7005	M_{S23}	4	$S_{23} \to S_{34} \to D_{17} \to D_8 \to I_8$	0.5105
M_{S2}	6	$S_2 \to D_{13} \to I_{13}$	0.7161	M_{S24}	6	$S_{24} \to D_{19} \to I_{19}$	0.7161
M_{S4}	8	$S_4 \to D_{11} \to I_{11}$	0.6414	M_{S26}	4	$S_{26} \to D_{15} \to I_{15}$	0.6161
M_{S6}	4	$S_6 \to D_{14} \to I_{14}$	0.6161	M_{S28}	8	$S_{28} \to D_6 \to I_6$	0.6414
M_{S8}	6	$S_8 \to D_{17} \to I_{23}$	0.7161	M_{S30}	4	$S_{30} \to D_2 \to I_2$	0.6161
M_{S9}	4	$S_9 \to S_{18} \to D_{13} \to D_5 \to I_{22}$	0.5105	M_{S31}	6	$S_{31} \to D_9 \to I_9$	0.6505
M_{S10}	6	$S_{10} \to S_{30} \to D_4 \to I_4$	0.5714	M_{S32}	4	$S_{32} \to S_1 \to D_1 \to I_1$	0.5305
M_{S11}	4	$S_{11} \to D_{15} \to I_{21}$	0.6161	M_{S33}	6	$S_{33} \to D_5 \to I_{22}$	0.7161
M_{S13}	4	$S_{13} \to S_{45} \to D_3 \to I_3$	0.5305	M_{S34}	6	$S_{34} \to D_{10} \to I_{10}$	0.7161
M_{S14}	4	$S_{14} \to D_{19} \to S_5 \to D_5 \to I_5$	0.5105	M_{S36}	4	$S_{36} \to D_{20} \to I_{20}$	0.6161
M_{S15}	6	$S_{15} \to D_2 \to I_{24}$	0.7161	M_{S37}	6	$S_{37} \to D_{17} \to I_{17}$	0.7161
M_{S16}	6	$S_{16} \to D_{12} \to I_{12}$	0.6505	M_{S38}	8	$S_{38} \to D_8 \to I_8$	0.7661
M_{S17}	6	$S_{17} \to D_{19} \to I_{30}$	0.7161	M_{S39}	6	$S_{39} \to D_{10} \to I_{28}$	0.7161
M_{S18}	4	$S_{18} \to D_7 \to I_{26}$	0.6161	M_{S41}	6	$S_{41} \to D_{18} \to I_{27}$	0.7161
M_{S19}	4	$S_{19} \to D_{14} \to I_{29}$	0.6161	M_{S42}	4	$S_{42} \to D_{13} \to I_{25}$	0.6161
M_{S20}	6	$S_{20} \to S_{45} \to D_{10} \to I_{10}$	0.5714	M_{S46}	6	$S_{46} \to S_{37} \to S_{29} \to D_{13} \to I_{13}$	0.5514
M_{S21}	4	$S_{21} \to D_{13} \to D_5 \to I_5$	0.5961	M_{S47}	4	$S_{47} \to D_{17} \to I_{23}$	0.4514
M_{S22}	4	$S_{22} \to D_7 \to I_7$	0.6161				

(Diff: difficulty value)

Fig. 5 shows the comparison curves with and without OCOM (NOCOM). For the OCOM performance curves, the dashed line is the result of the decision made during the global optimization stage based only on the performance recovery value $P(\tilde{t}_r)$ (OCOM-*P*), and the solid line is the resilience-based decision result (OCOM-*R*). From Fig. 5, we can draw the following three conclusions. First, although the decision result of OCOM-*P* enables the performance of the UWSoS to recover to a higher value after a hit, this decision significantly prolongs the overall task completion time. Conversely, the decision result of OCOM-*R* incurs only a minor loss in performance recovery (only 0.07 lower in the RN scenario and 0.05 lower in the RL scenario, as indicated in Fig. 5), allowing UWSoS to complete the current combat mission in a shorter time and quickly transition to subsequent confrontational events. This demonstrates the effectiveness of the resilience metrics proposed in this paper, and the results of resilience-based decision-making can be more in line with the battlefield reality. Second, according to the results in Fig. 5, the resilience value of UWSoS with OCOM in the node attack scenario is 0.364, while the resilience value without OCOM is 0.210. In the link attack scenario, the resilience value of UWSoS with OCOM is 0.736, while the resilience value without OCOM is 0.296. The experimental results show that OCOM significantly improves the UWSoS resilience, especially in the link attack scenario, demonstrating the effectiveness of the optimization method proposed in this paper. Third, in the node attack scenario, the UWSoS structure will be more severely damaged, leading to task loss, and thus, there is less space available to optimize task OC. In contrast, in the link attack scenario, the probability of task loss is lower, and the space available for optimizing the OC is larger. Thus, OCOM can achieve higher performance gains in this scenario.

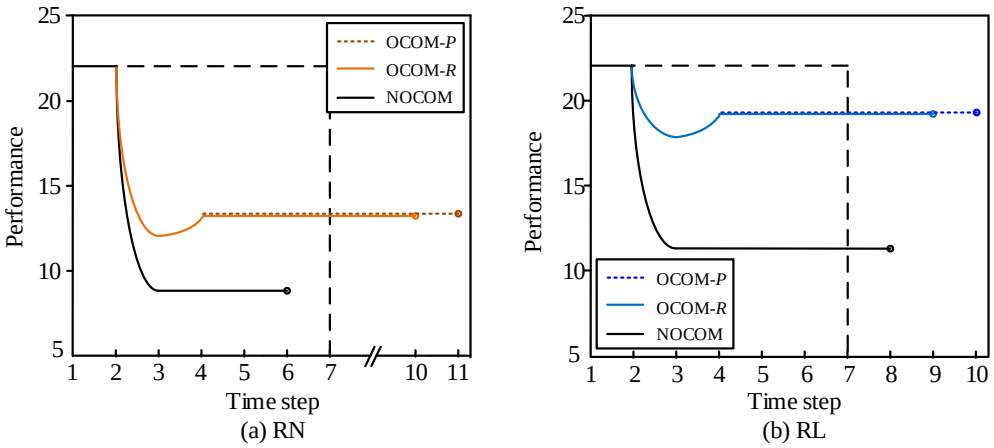


Figure 5. The performance of the UWSoS.

In order to verify the effectiveness of the different optimization stages of OCOM, Fig. 6 shows the results of the OC optimization for part of the tasks in UWSoS. In Fig. 6(a), at time step 1, the initial OC for task $M_{S13}$is $S_{13} \rightarrow S_{45} \rightarrow D_3 \rightarrow I_3$, with a task benefit of 0.5305. The initial OC for task M_{S20} is $S_{20} \rightarrow S_{45} \rightarrow D_{10} \rightarrow I_{10}$. Since task M_{S34} is also delivered to node I_{10} for execution, M_{S20} will experience a waiting delay of 1 time step, and therefore the benefit of task $M_{S20}$is 0.5714. At time step 2, as shown in Fig. 6(b), the decider node D_{10} is attacked and damaged, causing the OC for task M_{S20} to be disrupted, the task M_{S20} cannot be delivered and executed, and the performance of the UWSoS is degraded. At this moment, OCOM first initiates a local adjustment action, updating the OC for M_{S20} to $S_{20} \rightarrow S_{45} \rightarrow D_3 \rightarrow D_{14} \rightarrow I_{29}$, as illustrated in Fig. 6(c). Due to the increased transmission and execution time of M_{S20}, the performance of UWSoS can only recover 0.4938. Simultaneously, OCOM will conduct the second stage of global planning for the tasks at the command platform based on the results of the local adjustments. At time step 4, the UWSoS receives the new task plan, and the OCs of M_{S13} and M_{S20} are updated to $S_{13} \rightarrow S_{45} \rightarrow D_3 \rightarrow D_{14} \rightarrow I_{29}$ and $S_{20} \rightarrow S_{45} \rightarrow D_3 \rightarrow I_3$, respectively. Due to increased transmission time, the benefit of M_{S13} will decrease to 0.4514, while the updated M_{S20} will no longer experience a waiting delay for execution, and the benefit will improve to 0.6305. In the above scenario, OCOM first ensures the continued delivery and scheduled execution of M_{S20}, which is affected by the OC interruption, through the local adjustment action in the first stage, and achieves a performance

degradation of only 0.0731. Subsequently, OCOM performs the global optimization action in the second stage, which improves the overall performance by 0.0531 by co-optimizing OCs of tasks M_{S13} and M_{S20}. Although the overall performance after OCOM optimization is still lower than the initial performance, it achieves a gain reduction of only 0.02. These results indicate that the two-stage optimization actions of OCOM are effective and can generate feasible OC optimization strategies to recover performance in node attack scenarios. Similarly, Fig. 6(e)-(h) provides an example of a link attack scenario.

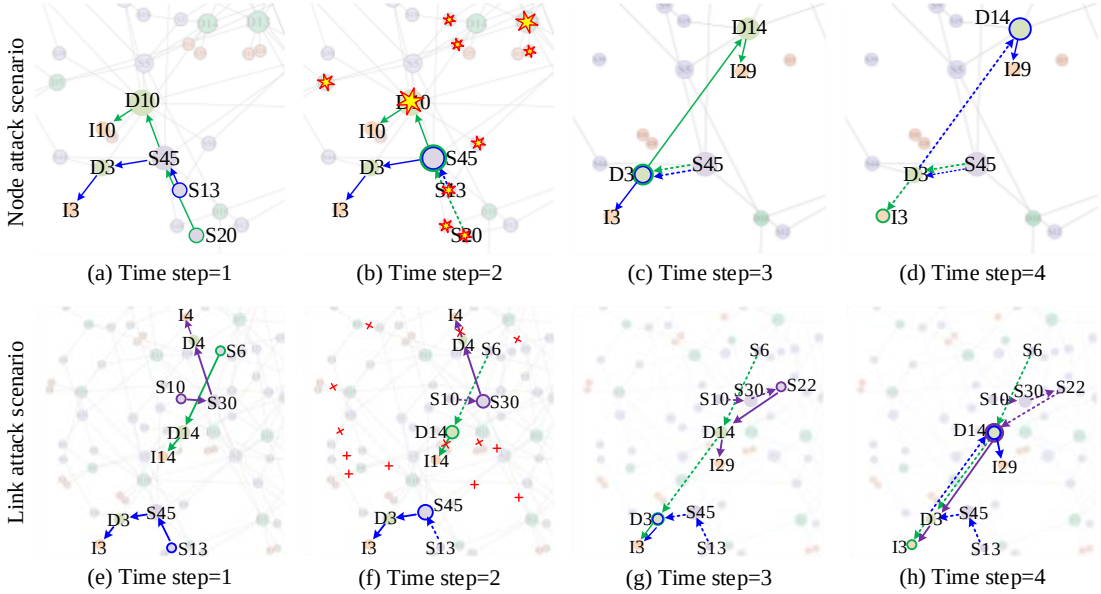


Figure 6. OC optimization progress graph.

Fig. 7 illustrates the resilience trend of UWSoS when it is attacked at different time steps, with the horizontal coordinate of each subfigure indicating the time when the adversary launches the attack from 1 to 5. First, as the adversary's attack time is postponed, the number of completed tasks increases, while the number of tasks affected by the OC interruptions decreases, and thus, the resilience value of UWSoS increases. Second, the resilience values of OCOM and NOCOM gradually converge and eventually become equal when the attack time is shifted back, since the goal of OCOM is to improve resilience by optimizing OC. Under the same conditions, the more OCs are interrupted, the more effective OCOM is. Finally, the use of OCOM makes the resilience value of UWSoS always greater than or equal to the case without OCOM, proving the feasibility of OCOM.

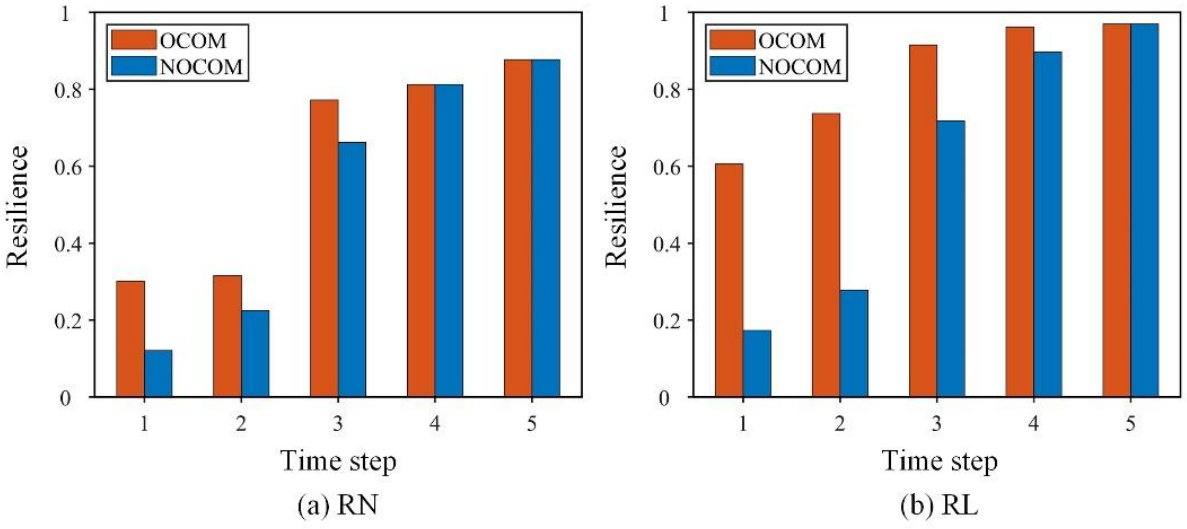


Figure 7. Resilience of UWSoS under different attack time steps.

From the other perspective, we fix the attack time at time step 2, i.e., all the tasks are still in the transmission state, and deeply analyzed the effects of different enemy attack strategies and attack strengths on UWSoS resilience, as shown in Fig. 8. First, we additionally design four types of node attack strategies: sensor node attack strategy (SN) , decider node attack strategy (DN), influencer node attack strategy (IN), and proportionally mixed node attack strategy (MN). These strategies indicate that S, D, and I nodes suffer attacks in descending order of node weights, respectively. $S$and D nodes' weights are equal to their degrees, while the weights of I nodes are calculated as $< D_k, I_j >= d_k \times c_j$, where c_j denotes the capability value of the influencer node and d_k denotes the degree value of the edge decision node connected to the influencer node. Here, $< D_k, I_j >$ indicates that I nodes with higher capability values and connections to large hubs have higher importance levels. It should be noted that when the strike strength is 0.3 and the strike strategy is MN, 30% of S nodes, D nodes, and I nodes will be destroyed, respectively. Second, we also design four additional link attack strategies: a strategy for attacking sensor node links (SL), a strategy for attacking decider node links (DL), a strategy for attacking influencer node links (IL) and proportionally mixed link attack strategy (ML). These strategies indicate that the links connected to the above types of nodes will be attacked in descending order of their betweenness centrality. Last, the horizontal axis of each subgraph in Fig. 8 represents enemy attack intensity ranging from 0.01 to 1.0.

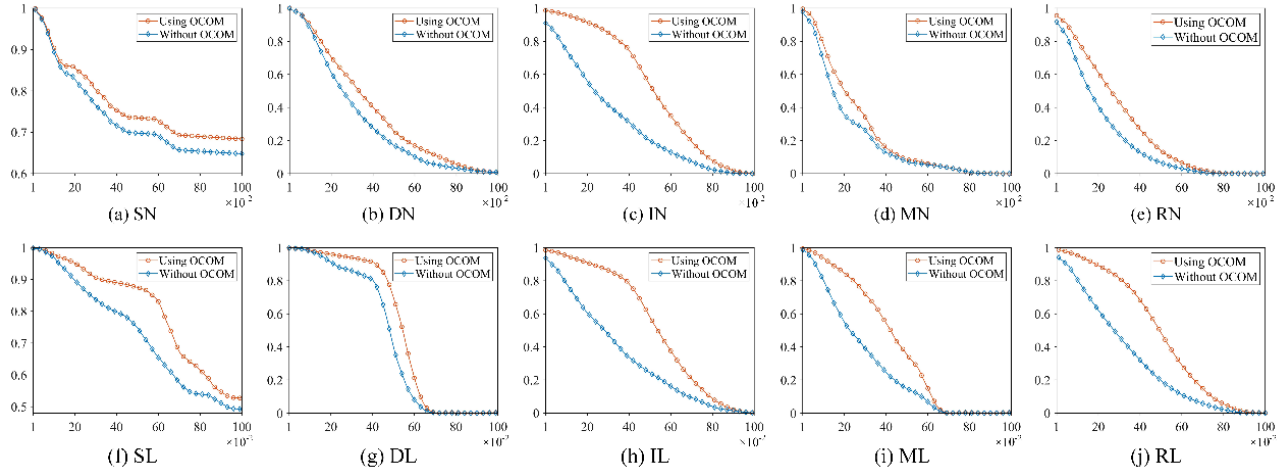


Figure 8. Effect of enemy attack strategies on the UWSoS resilience.

From Fig. 8, we know that, first, as the intensity of the attack increases, the number of affected OCs rises, and the severe damage to the structure of the UWSoS also reduces the number of available resources. Both factors compress the optimization space of OCs, leading to a decreasing trend in the UWSoS's resilience. Second, damage to the D nodes, I nodes, or the corresponding links will reduce the number of I nodes able to take over the task (damaged or unable to communicate). Thus, except for the SN and SL situation, the resilience values obtained with and without OCOM will eventually get close as the intensity of the attack increases. Third, damage to the S node or the link connected does not reduce the number of I nodes in the UWSoS, i.e., the number of available combat resources remains unchanged. Thus, the resilience value of using OCOM in the SN and SL situations will be greater than that of not using OCOM as the intensity of the attack increases. Third, edge betweenness centrality reflects the frequency with which an edge appears in the shortest paths between other nodes. Therefore, comparing node attack scenarios and link attack scenarios, under the same attack intensity, attacking important edges will result in a lower resilience value for UWSoS, especially attacks on links connected to edge decision nodes. Last, under the ten attack strategies for the two typical scenarios, the resilience value of UWSoS obtained using OCOM is always greater than or equal to that obtained by not using OCOM, similar to the conclusion in Fig. 7.

In addition to the OCOM, this study also compared two other methods: Task Reassignment Method (TRAM) and Time-Minimized Resource Optimization Method (TMOM) [29], as shown in Fig. 9. Among them, the TRAM optimally reallocates resources only to the tasks affected by the interruption of the OC, without considering the co-optimization of the OC with the

unaffected tasks. The TMOM pursues the minimization of overall task completion time and does not pursue the maximization of benefits during the optimization process. The comparison between these two methods serves two primary purposes: firstly, to demonstrate that OCOM is not a task random reassignment method, and secondly, to illustrate that exclusively pursuing faster task completion time does not result in higher UWSoS resilience values. We conducted comparisons under four attack intensities: 0.2, 0.3, 0.4, and 0.5. As shown in Fig. 9, OCOM obtained the highest UWSoS resilience values in all situations. This strongly indicates that when UWSoS is under attack, OCOM is the optimal choice.

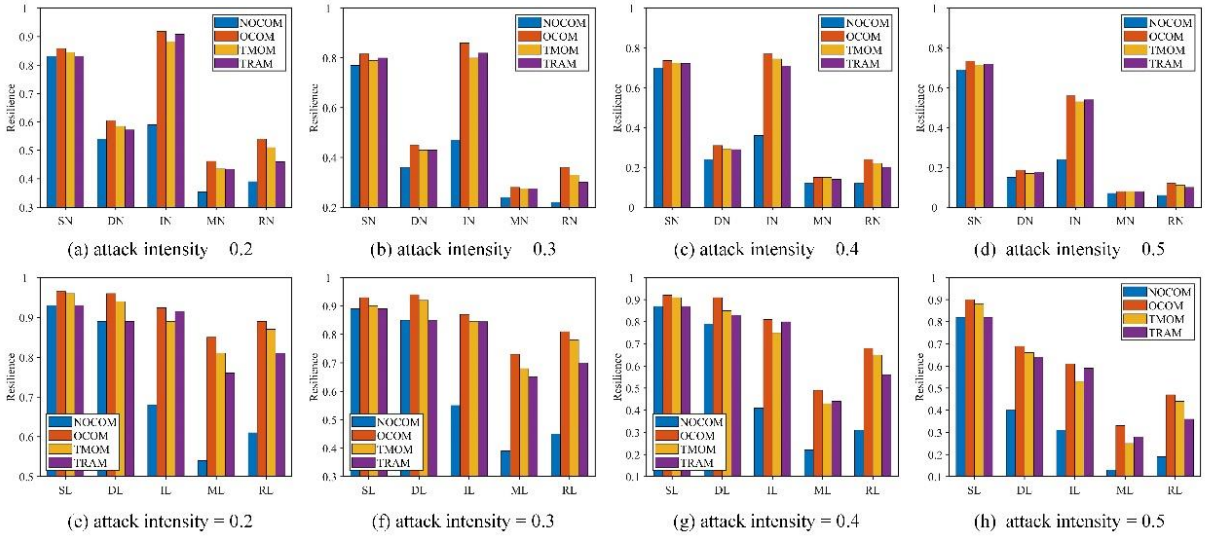


Figure 9. Resilience of UWSoS under different optimization methods.

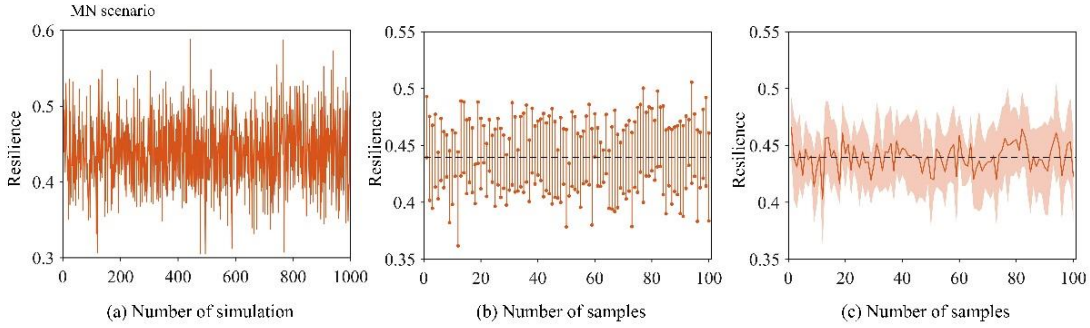
4.2. General resilience analysis for UWSoS

This subsection explored the general resilience of UWSoS. We selected MN and ML as typical attack strategies for node and edge attack scenarios, respectively, and we fixed the attack time step at 2, the attack intensity at 0.2, and employed the Monte Carlo simulation method. Through 1000 random experiments, we estimated the confidence interval for the unknown population mean using the Student's t-test method, see Eq. 22.

$$x_{sos} = \mu_{sos} \pm t_{sos} * \frac{s_{sos}}{\sqrt{n_{sos}}}, \tag{22}$$

where $s_{sos}, u_{sos}, t_{sos}$ and n_{sos} represent the sample standard deviation, sample mean, t_{sos} critical value and sample size, respectively. We chose a receiver field interval of 0.95 and obtained a t value of 2.262 by looking up the table.

First, the simulation method for estimating confidence intervals is explained. The simulation experiment in this subsection assumes that a UWSoS consists of 100 nodes, with 50 *S* nodes, 20 *D* nodes, and 30 *I* nodes, which is the same as subsection 4.1. The reconnaissance capability value of the UWSoS is set to 0.7, and 35 combat tasks will be executed through one round of reconnaissance. These 35 tasks are generated by 35 random *S* nodes in the UWSoS through surveillance, and the probability that the difficulty value of each task is 4, 6, or 8 is 0.5,0.3,0.2, respectively. Each *I* node can handle a maximum of 2 tasks. The cost for each node within the UWSoS is 0.01, and the price for each edge is 0.005. The results from 1000 random simulation experiments are depicted in Fig. 10.



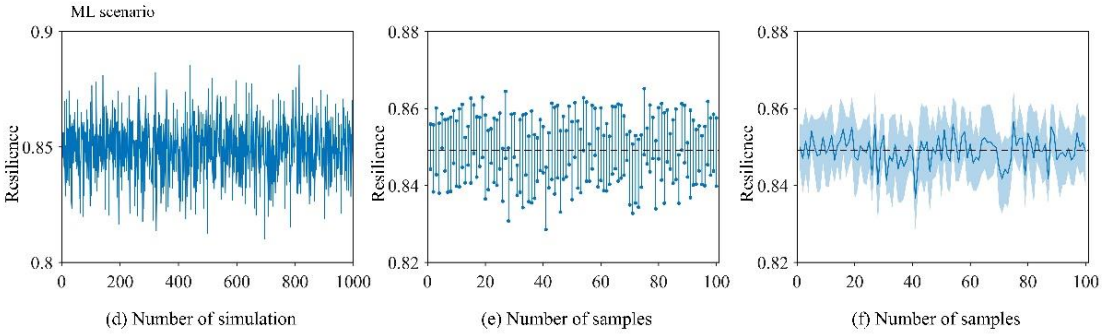


Figure 10. General resilience of UWSoS.

Fig. 10(a) depicts the resilience variation of UWSoS over 1000 simulation experiments in the node attack scenario. Further, we conducted sampling with a sample size 10 from these 1000 simulation experiments. The confidence intervals for the population mean at a 0.95 confidence level were calculated using Eq. 22 for these 100 sets of independent sampling results, as depicted in Fig. 10(b) and (c). The dashed line values in subfigures (b) and (c) are 0.4396, covering the majority of the confidence intervals from 100 independent sampling results. Therefore, it can be used as a reference value for the resilience of the UWSoS comprising 100 nodes with a reconnaissance capability of 0.7 under an attack intensity of 0.2 in the node attack scenario. Similarly, the dashed line value of 0.8491 in subfigures (e) and (f) can serve as a reference value for the resilience of UWSoS in the corresponding link attack scenarios.

Subsequently, this paper verifies the superiority of OCOM through four sets of comparison experiments. Fig. 11 shows the resilience variations of UWSoS of four scales under varying reconnaissance capabilities. The structural information for the four different-sized UWSoS is provided in Table 3. In each subfigure of Fig. 11, the horizontal coordinates indicate the number of simulation groups of 9*100, where 9 denotes nine groups of experiments with UWSoS reconnaissance capabilities p from 0.1 to 0.9, and 100 denotes 100 independent samples of sample size 10 from 1000 simulation results.

Table 3. General properties of UWSoS.

Name	V	E	V^S	V^D	V^I
UWSoS-1	50	164	25	15	10
UWSoS-2	100	334	50	30	20
UWSoS-3	150	504	75	45	30
UWSoS-4	200	674	100	60	40

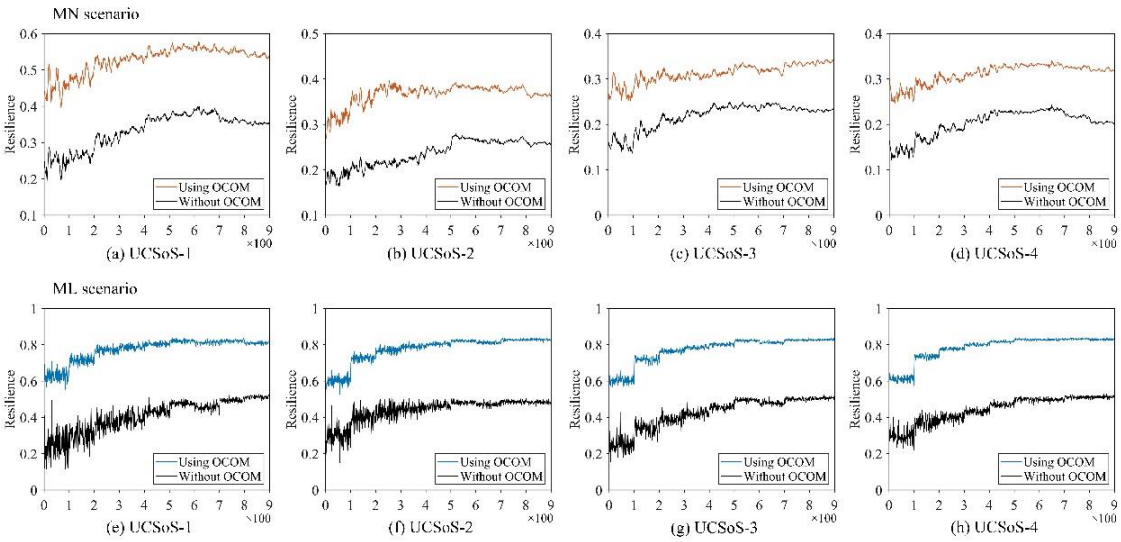


Figure 11. Resilience variation of UWSoS under different reconnaissance capabilities.

From Fig. 11, we can draw the following conclusions. First, with the fixed scale of UWSoS, the resilience of OCOM gradually increases as the reconnaissance capability increases. When the reconnaissance capability is low, the number of tasks

that the UWSoS needs to complete is small, and due to the attack, even if the UWSoS can carry out the optimization of the OC, the task benefit is difficult to cover the cost of physical destruction and the cost of transmission energy consumption. In contrast, as the reconnaissance capability increases, the number of tasks increases, the optimizable space of the OCOM and the overall task gains increase. Thus, UWSoS can achieve higher resilience. Second, under the node attack scenario, the curves of both OCOM and NOCOM show a tendency of increasing and then decreasing. This phenomenon is attributed to the fact that damage to nodes easily leads to a reduction in available resources. As the task quantity approaches the capability limit of UWSoS, the optimization space for OCOM will decrease. In some cases, it may even necessitate the abandonment of the execution of specific tasks, resulting in a declining trend in resilience. Thirdly, with the increase in reconnaissance capability, the resilience values of the 100 sets of samples will tend to stabilize, especially in the case of link attack scenarios. This observation indicates that the number of alternative solutions also grows as the task scale increases. Consequently, the performance recoverability of UWSoS becomes higher, and the degree to which resilience is impacted becomes smaller. Lastly, under different UWSoS scales and varying reconnaissance capabilities, the resilience values of OCOM consistently exceed those without OCOM, demonstrating the superiority of the proposed method in this study.

Furthermore, we constructed four sets of experiments to demonstrate the superiority of OCOM from another perspective, as shown in Fig. 12. Distinguished from Fig. 11, this part of the experiment compares the impact of UWSoS scale variations on resilience values under fixed reconnaissance capability. Four reconnaissance capability values were set at 0.2, 0.4, 0.6, and 0.8. In each subfigure of Fig. 12, the 4 in 4*100 corresponds to the four sets of experiments in which the number of nodes of the UWSoS is 50, 100, 150 and 200, respectively, while keeping other parameters consistent with those in Fig. 11.

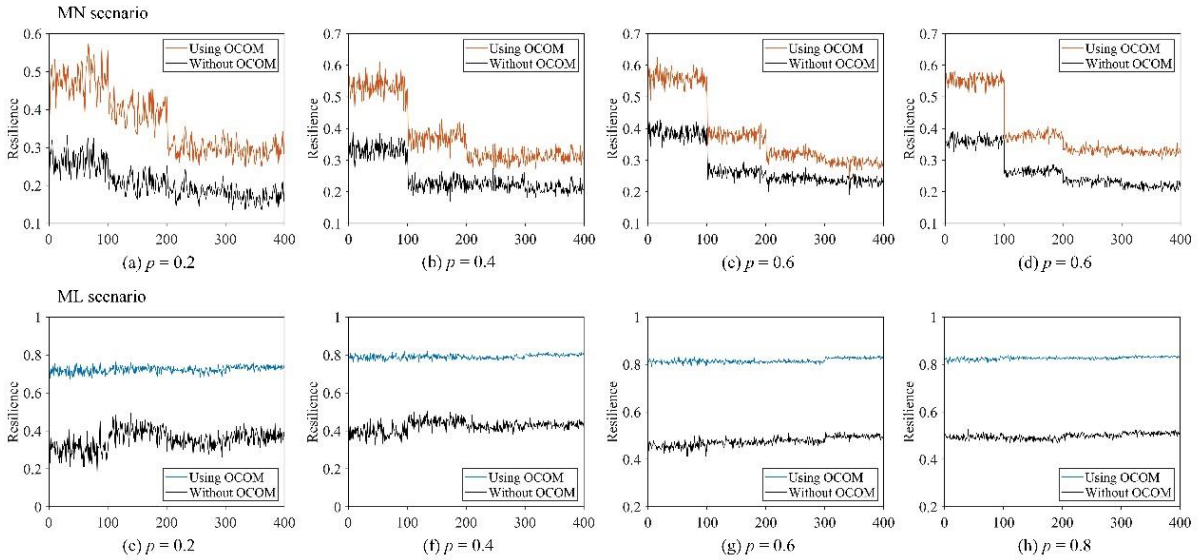


Figure 12. Resilience variation of UWSoS at different scales.

The conclusions drawn from Fig. 12 are as follows. First, in the node attack scenario, the resilience of UWSoS decreases as its scale increases. This phenomenon arises from the heightened significance of large hub nodes with the expansion of the UWSoS scale. Once these critical nodes are compromised, they substantially impact a multitude of OCs, increasing the optimization difficulty of OCOM and compressing the optimizable space, ultimately leading to a decrease in the resilience value. Second, in the link strike scenario, the resilience of UWSoS remains stable as its scale varies. Last, using OCOM consistently results in higher resilience compared to scenarios without OCOM, affirming the proposed methodology's superiority.

5. Conclusions

Enhancing the battlefield resilience of UWSoS holds significant military value. While physical reconstruction methods such as node structure reconfiguration and link rewiring can significantly improve performance on the battlefield, the constraints of finite resources and scheduling limitations

necessitate the development of a transitional approach for enhancing UWSoS resilience. Therefore, this paper takes the OC optimization of tasks as the entry point of UWSoS resilience enhancement research, and proposes OCOM in the case of limited physical resources. With the proposed model, UWSoS can make a new plan for the OC of tasks after the attack, thereby effectively restoring the battlefield performance. By comparing with different optimization models, OCOM can effectively improve the battlefield resilience of UWSoS by comprehensively considering the task's gain factor and completion time factor, while only seeking a faster task completion time or a higher task gain model will not lead to good results. Numerous simulation experiments have demonstrated the model's significant performance in both effectiveness and superiority.

Acknowledgement

This research was supported by the Science and Technology on Information System Engineering Laboratory (No.05202007).

References

1. J. Chen, J. Sun, G. Wang, From unmanned systems to autonomous intelligent systems, Engineering 12 (2022) 16–19. https://doi.org/10.1016/j.eng.2021.10.007
2. B. Clark, D. Patt, H. Schramm, Mosaic warfare: Exploiting artificial intelligence and autonomous systems to implement decision-centric operations, Center for Strategic and Budgetary Assessments, 2020.
3. S. Russell, S. Hauert, R. Altman, M. Veloso, Ethics of artificial intelligence, Nature 521 (7553) (2015) 415–416. https://doi.org/10.1038/521415a
4. W. Yang, H. Qin, J. Wang, Y. Deng, Summary of the development of world military unmanned systems in 2021, Journal of China Academy of Electronics and Information Technology 4 (2022) 368–373.
5. X. Wang, Q. Guo, Research on the test platform of ground unmanned equipment system combined with virtual and real, Computer Simulation 6 (39) (2022) 15–20.
6. X. Chen, N. Bose, M. Brito, F. Khan, B. Thanyamanta, T. Zou, A review of risk analysis research for the operations of autonomous underwater vehicles, Reliability Engineering & System Safety 216 (2021) 108011.
7. Q. Wang, T. Li, Y. Xu, F. Wang, B. Diao, L. Zheng, J. Huang, How to prevent malicious use of intelligent unmanned swarms?, The Innovation 4 (2) (2023). https://doi.org/10.1016/j.xinn.2023.100396
8. A. Rosiński, J. Paś, K. Białek, P. Wetoszka, Method for assessing reliability of the power supply system for electronic security systems of intelligent buildings taking into account external natural interference, Eksploatacja i Niezawodnosc-Maintenance and Reliability (2023). https://doi.org/10.17531/ein/176375
9. M. Oszczypała, J. Ziółkowski, J. Małachowski, Semi-markov approach for reliability modelling of light utility vehicles., Eksploatacja i Niezawodnosc-Maintenance and Reliability 25 (2) (2023). https://doi.org/10.17531/ein/161859
10. D. Choeum, D.-H. Choi, Vulnerability assessment of conservation voltage reduction to load redistribution attack in unbalanced active distri- bution networks, IEEE Transactions on Industrial Informatics 17 (1) (2020) 473–483. https://doi.org/10.1109/TII.2020.2980590
11. T. Wen, Y. Deng, The vulnerability of communities in complex networks: An entropy approach, Reliability Engineering & System Safety 196 (2020) , https://doi.org/10.1016/j.ress.2019.106782
12. G. Bocewicz, E. Szwarc, J. Wikarek, P. Nielsen, Z. Banaszak, A competency-driven staff assignment approach to improving employee scheduling robustness, Eksploatacja i Niezawodnosc-Maintenance and Reliability 23 (1) (2021) 117–131. https://doi.org/10.17531/ein.2021.1.13
13. J. Li, Y. Tan, K. Yang, X. Zhang, B. Ge, Structural robustness of combat networks of weapon system-of-systems based on the operation loop, International Journal of Systems Science 48 (3) (2017) 659–674. https://doi.org/10.1080/00207721.2016.1212429
14. Y. Fu, X. Zhu, A joint age-based system replacement and component reallocation maintenance policy: Optimization, analysis and resilience, Reliability Engineering & System Safety 235 (2023) , https://doi.org/10.1016/j.ress.2023.109240
15. C. S. Holling, Resilience and stability of ecological systems, Annual Review of Ecology and Systematics 4 (1) (1973) 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245

16. P. Trucco, B. Petrenj, Characterisation of resilience metrics in full-scale applications to interdependent infrastructure systems, Reliability Engineering & System Safety (2023) , https://doi.org/10.1016/j.ress.2023.109200
17. H. Mahmoud, T. Kirsch, D. O'Neil, S. Anderson, The resilience of health care systems following major disruptive events: Current practice and a path forward, Reliability Engineering & System Safety (2023) , https://doi.org/10.1016/j.ress.2023.109264
18. M. H. Oboudi, M. Mohammadi, Two-stage seismic resilience enhancement of electrical distribution systems, Reliability Engineering & System Safety (2023) , https://doi.org/10.1016/j.ress.2023.109635
19. M. Taghizadeh, M. Mahsuli, H. Poorzahedy, Probabilistic framework for evaluating the seismic resilience of transportation systems during emergency medical response, Reliability Engineering & System Safety 236 (2023) , https://doi.org/10.1016/j.ress.2023.109255
20. L. Zhen, S. Lin, C. Zhou, Green port oriented resilience improvement for traffic-power coupled networks, Reliability Engineering & System Safety 225 (2022) , https://doi.org/10.1016/j.ress.2022.108569
21. L. Liu, J. Yang, A dynamic mission abort policy for the swarm executing missions and its solution method by tailored deep reinforcement learning, Reliability Engineering & System Safety 234 (2023) , https://doi.org/10.1016/j.ress.2023.109149
22. T. Liu, G. Bai, J. Tao, Y.-A. Zhang, Y. Fang, A multistate network approach for resilience analysis of UAV swarm considering information exchange capacity, Reliability Engineering & System Safety (2023) , https://doi.org/10.1016/j.ress.2023.109606
23. Q. Sun, H. Li, Y. Wang, Y. Zhang, Multi-swarm-based cooperative reconfiguration model for resilient unmanned weapon system-of-systems, Reliability Engineering & System Safety 222 (2022) , https://doi.org/10.1016/j.ress.2022.108426
24. B. Xu, G. Bai, Y. Fang, J. Tao, et al., Failure analysis of unmanned autonomous swarm considering cascading effects, Journal of Systems Engineering and Electronics 33 (3) (2022) 759–770. https://doi.org/10.23919/JSEE.2022.000069
25. K. Wei, T. Zhang, C. Zhang, Research on resilience model of UAV swarm based on complex network dynamics, Eksploatacja i Niezawodnosc-Maintenance and Reliability 25 (4) (2023). https://doi.org/10.17531/ein/173125
26. C. Zhang, T. Liu, G. Bai, J. Tao, W. Zhu, A dynamic resilience evaluation method for cross-domain swarms in confrontation, Reliability Engineering & System Safety 244 (2024) , https://doi.org/10.1016/j.ress.2023.109904
27. X. Zhou, Y. Huang, G. Bai, B. Xu, J. Tao, The resilience evaluation of unmanned autonomous swarm with informed agents under partial failure, Reliability Engineering & System Safety 244 (2024) , https://doi.org/10.1016/j.ress.2023.109920
28. H. T. Tran, M. Balchanos, J. C. Domerc¸ant, D. N. Mavris, A framework for the quantitative assessment of performance-based system resilience, Reliability Engineering & System Safety 158 (2017) 73–84. https://doi.org/10.1016/j.ress.2016.10.014
29. H. Li, Q. Sun, Y. Zhong, Z. Huang, Y. Zhang, A soft resource optimization method for improving the resilience of UAV swarms under continuous attack, Reliability Engineering & System Safety 237 (2023) , https://doi.org/10.1016/j.ress.2023.109368
30. J. Li, D. Zhao, J. Jiang, K. Yang, Y. Chen, Capability oriented equipment contribution analysis in temporal combat networks, IEEE Transactions on Systems, Man, and Cybernetics: Systems 51 (2) (2018) 696–704. https://doi.org/10.1109/TSMC.2018.2882782
31. L. Bukowski, S. Werbin´ska-Wojciechowska, Using fuzzy logic to support maintenance decisions according to resilience-based maintenance concept, Eksploatacja i Niezawodnosc-Maintenance and Reliability 23 (2) (2021). https://doi.org/10.17531/ein.2021.2.9
32. C. Zhang, R. Chen, S. Wang, H. Dui, Y. Zhang, Resilience efficiency importance measure for the selection of a component maintenance strategy to improve system performance recovery, Reliability Engineering & System Safety 217 (2022) , https://doi.org/10.1016/j.ress.2021.108070
33. M. Xu, M. Ouyang, L. Hong, Z. Mao, X. Xu, Resilience-driven repair sequencing decision under uncertainty for critical infrastructure systems, Reliability Engineering & System Safety 221 (2022) , https://doi.org/10.1016/j.ress.2022.108378
34. F. Qiang, H. Xingshuo, S. Bo, R. Yi, W. Zili, Y. Dezhen, H. Yaolong, F. Ronggen, Resilience optimization for multi-UAV formation reconfiguration via enhanced pigeon-inspired optimization, Chinese Journal of Aeronautics 35 (1) (2022) 110–123. https://doi.org/10.1016/j.cja.2020.10.029
35. Z. Chen, D. Hong, W. Cui, W. Xue, Y. Wang, J. Zhong, Resilience evaluation and optimal design for weapon system of systems with dynamic reconfiguration, Reliability Engineering & System Safety (2023) , https://doi.org/10.1016/j.ress.2023.109409
36. Z. Mou, F. Gao, J. Liu, Q. Wu, Resilient UAV swarm communications with graph convolutional neural network, IEEE Journal on Selected Areas in Communications 40 (1) (2021) 393–411. https://doi.org/10.1109/JSAC.2021.3126047
37. H. T. Tran, J. C. Domerc¸ant, D. N. Mavris, A network-based cost comparison of resilient and robust system-of-systems, Procedia

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

38. W. Zhang, S. Huang, C. Zhu, J. Liu, L. Sun, New paradigm of command and control: Edge command and control, Command Information System and Technology 12 (1) (2021) 1–7.
39. K. Zong, F. An, W. Zhao, L. Yan, H. Liu, Analysis of mission-based command of the U.S. Air force for joint operations, Modern Defence Technology 51 (3) (2023) 66–74.
40. J. R. Cares, et al., An information age combat model, Alidade, Inc., Newport, PR, USA (Produced for the Director, Net Assessment, Office of the Secretary of Defense under Contract TPD-01-C-003) (2004).
41. Y. Tan, X. Zhang, K. Yang, Research on networked description and modeling methods of armament system-of-systems, Journal of systems & Management 21 (6) (2012) 781–786.
42. J. Li, J. Jiang, K. Yang, Y. Chen, Research on functional robustness of heterogeneous combat networks, IEEE Systems Journal 13 (2) (2018) 1487–1495. https://doi.org/10.1109/JSYST.2018.2828779
43. D. Zhao, Y. Tan, J. Li, Y. Dou, L. Li, J. Liu, Research on structural robustness of weapon system-of-systems based on heterogeneous network, Systems Engineering-Theory and Practice 39 (12) (2019) 3197–3207.
44. H. T. Tran, A complex networks approach to designing resilient system-of-systems (2015).