Dynamic Resilience Assessment and Collaborative Reconfiguration of UAV Kill Webs Based on Physical-Logical-Temporal Coupling

Yezhuo Xu, Husheng Wu* and Zizheng Han

School of Equipment Management and Support, Engineering University of PAP, Xi'an 710086, China

Abstract: In highly contested environments, the survivability of Unmanned Aerial Vehicle (UAV) Kill Webs faces severe challenges. Existing evaluations over-rely on static topological connectivity, ignoring physical constraints (distance, energy, latency), often causing a fatal misjudgment: "structural preservation alongside operational paralysis." To address this, we propose a dynamic resilience assessment and collaborative reconfiguration framework integrated with a "physical-logical-temporal" coupling. First, an effective model based on heterogeneous closed-loop cycles is constructed. A Time-aware Accumulated Normalized Operational Capability (T-ANOC) metric is proposed to rigorously quantify the realistic penalties of reconfiguration latency and spatial attenuation on System-of-Systems (SoS) effectiveness. Second, under resource constraints, a many-to-one collaborative reconfiguration mechanism is defined, deeply comparing an Energy-Distance Collaborative Strategy (EDCS) with a Deep Reinforcement Learning (DRL) global optimization strategy. Large-scale Monte Carlo simulations reveal three profound insights: (1) It quantitatively verifies the nonlinear decoupling characteristic where operational collapse precedes topological disintegration; (2) Although DRL approaches short-term recovery limits, EDCS untangles the "energy-latency-effectiveness" trilemma. By reducing energy consumption by 45% and latency by 35%, EDCS achieves long-term sustainable resilience; (3) Microscopic node contribution analysis (peak contribution 238.9%) mechanistically quantifies the nonlinear emergent gains triggered by heterogeneous functional reorganization. This study provides rigorous mathematical support for designing high-survivability, self-adaptive UAV Kill Webs. Compared with topology-centered robustness metrics and purely learning-driven reconfiguration policies, the proposed framework jointly models physical feasibility, heterogeneous functional substitution, and temporal recovery loss within a unified resilience-analysis process.

Keywords: Unmanned Aerial Vehicle (UAV) swarm, Kill Web resilience, collaborative reconfiguration, physical-logical coupling, emergent effects.

INTRODUCTION

The paradigm of modern warfare has shifted from single-platform combat to system-of-systems confrontation based on Combat System-of-Systems (CSoS). Its core lies in integrating distributed heterogeneous resources into highly resilient Kill Webs [1]. Within this framework, Unmanned Aerial Vehicle (UAV) swarms, characterized by their flexibility, cost-effectiveness, and robust collaborative operational effects, have emerged as a critical force for executing multi-domain integrated missions [2]. Through the deep integration of physical, information, and cognitive domains, UAV swarms can demonstrate exceptional operational effectiveness in complex and volatile contested environments. However, the highly adversarial nature of modern battlefields—encompassing deliberate kinetic strikes, electromagnetic interference, and internal system failures—poses severe challenges to the structural integrity and functional continuity of UAV swarms. Such disruptions can lead to the rapid fragmentation of functional chains and even trigger the holistic paralysis of the swarm's operational capabilities. Therefore, evaluating and enhancing the robust and resilient recovery capabilities of UAV swarms under extreme conditions has become a core imperative for ensuring the success of SoS missions.

In recent years, robustness has become a core metric for evaluating a system's capacity to maintain fundamental functions under internal failures or external perturbations [3]. Currently, related research has been widely applied in fields such as power grids [4], transportation [5], and smart manufacturing systems [6]. In the field of network science, robustness metrics are typically categorized into *a priori* robustness and *a posteriori* robustness [7]. *A priori* robustness focuses on the inherent structural properties of the network (e.g., connectivity, spectral radius) before an attack occurs, whereas *a posteriori* robustness emphasizes depicting the dynamic response and adaptive performance of the system during and after a disruption. Although the former provides a theoretical upper bound for system stability, the latter (often referred to as dynamic resilience) aligns more closely with the practical demands of

*Address correspondence to this author at the School of Equipment Management and Support, Engineering University of PAP, Xi'an 710086, China; E-mail: wuhusheng0421@163.com

Received on 07-04-2026 Accepted on 15-05-2026 Published on 22-05-2026

E-ISSN: 3083-3450/2026

CSoS in complex adversarial environments. Existing network dismantling studies [8] have revealed the game-theoretic balance between offense and defense; however, most current frameworks remain confined to connectivity maintenance within idealized topological networks. For highly dynamic UAV swarms, robustness is no longer merely a pure structural property but is deeply coupled with spatiotemporal constraints and heterogeneous functionalities. Consequently, there is an urgent need to shift the research paradigm from static topological analysis to an evaluation framework that comprehensively incorporates physical domain limitations and cross-domain collaborative logic.

Given the significance of robustness optimization, edge addition, rewiring, and structural reconfiguration have become effective means to enhance SoS effectiveness. In particular, the concept of the "Kill Web" has driven the evolution of operational architectures from rigid linear kill chains to self-organizing, highly autonomous web-like structures [1]. Compared to traditional CSoS, Kill Webs maintain operational continuity even when critical nodes are compromised, leveraging dynamic functional compensation mechanisms to demonstrate extraordinary survivability. Nevertheless, applying the abstract Kill Web concept to large-scale UAV swarms encounters severe physical challenges. Existing studies on Kill Web robustness often idealize the reconfiguration process, assuming seamless link restructuring among heterogeneous nodes. However, in actual battlefields, UAV-based Kill Webs are strictly bound by geospatial constraints (e.g., communication ranges, flight envelopes) and energy lifespan limitations [9]. If reconfiguration strategies ignore the physical costs of spatial displacement or the cross-domain adaptability of payload mapping, ensuring mission continuity becomes unfeasible. Therefore, exploring how to achieve the autonomous reconfiguration of Kill Webs under multi-dimensional physical constraints represents a critical scientific problem that urgently needs addressing.

To address the limitations of existing studies on UAV swarm robustness evaluation—which overly rely on static topology while ignoring physical constraints and reconfiguration latency—this paper aims to construct a dynamic evaluation and recovery framework conforming to realistic battlefield physics. By coupling geospatial constraints, energy lifespan, and payload functional attributes, the main innovative contributions of this paper are summarized as follows:

(1) Proposing a dynamic resilience evaluation framework and the T-ANOC metric integrated with "physical-logical-temporal" multi-dimensional coupling. Breaking through the limitations of traditional measures that focus solely on static topological connectivity, this metric incorporates spatial constraints and reconfiguration hysteresis into a time integral. This achieves a high-fidelity leap in System-of-Systems (SoS) evaluation from "bottom-level topological survival" to "upper-level operational effectiveness reachability."

(2) Designing a physics-aware EDCS for reconfiguration. Addressing the challenge of restricted heterogeneous resources, this strategy establishes spatial visibility and energy reserves as physical hard constraints. Compared to DRL global baselines that disregard physical costs, EDCS successfully untangles the "energy-latency-effectiveness" trilemma. It effectively evades the "high-latency trap" inherent in purely logical reconfiguration, achieving an optimal trade-off between engineering feasibility and effectiveness recovery.

(3) Revealing the asymmetric degradation mechanisms of "structure and effectiveness" in UAV Kill Webs under continuous strikes. Based on large-scale statistical simulations, this study precisely quantifies the nonlinear emergent gains triggered by the reorganization of heterogeneous functional nodes. The research mechanistically verifies the phenomenon that logical effectiveness collapse significantly precedes physical link fragmentation, profoundly elucidating the destructive essence of "structural preservation alongside operational paralysis." This provides quantitative support for the design of self-healing architectures in highly survivable swarms.

Taken together, the contribution of this study is not simply the juxtaposition of a robustness metric and a reconfiguration algorithm. Relative to existing robustness studies, the proposed T-ANOC framework extends evaluation from static structural survivability to time-accumulated mission effectiveness under explicit spatial attenuation and reconfiguration delay. Relative to DRL-based reconfiguration studies, this paper does not present a new generic learning solver; rather, it uses DRL as a global reference and develops a many-to-one collaborative recovery mechanism constrained

by communication visibility, residual energy, exclusivity, and heterogeneous function matching. The central contribution is therefore a unified physical-logical-temporal formulation that links local recovery decisions to system-level resilience trajectories in UAV Kill Webs.

The remainder of this paper is organized as follows. Section 2 reviews related work on network robustness and reconfiguration. Section 3 establishes the heterogeneous CSoS model and defines the ANOC and T-ANOC evaluation metrics. Section 4 elaborates on the collaborative reconfiguration decision mechanism and specific evolutionary strategies. Section 5 validates the effectiveness of the proposed reconfiguration strategies through case studies and discusses node contributions. Finally, Section 6 concludes the paper and outlines future research directions.

2. RELATED WORK

2.1. Robustness Evaluation of Combat Networks

Robustness evaluation serves as the logical genesis for enhancing SoS resilience. Early studies primarily focused on topology-based *priori* metrics, utilizing measures such as connectivity, global efficiency, average path length, and clustering coefficients to evaluate the structural survivability of infrastructure networks under random failures or deliberate attacks [10-12]. However, such static snapshot-based analytical methods abstract combat networks into homogeneous entities, neglecting the functional discrepancies of nodes within the "Observe-Orient-Decide-Act" (OODA) loop. In the context of CSoS, traditional metrics struggle to characterize the phenomenon of "structural preservation alongside functional collapse" caused by the failure of critical functional nodes, thereby failing to accurately measure the actual survivability of the SoS.

To more objectively capture performance degradation characteristics, academia has shifted towards researching *posteriori* robustness metrics, focusing on quantifying dynamic failure processes. The metric proposed by Schneider *et al*. [13] pioneered the quantification of cumulative failure processes by calculating the area under the connectivity curve during network collapse. Building upon this, subsequent studies expanded the evaluation objects from pure topological connectivity to the operational effectiveness dimension, characterizing the SoS's damage-resilient space by analyzing "performance-failure" trajectories under attack sequences [14]. This effectiveness evolution-based evaluation paradigm provides theoretical underpinning for this paper's adoption of the Area under the Network Operational Capability (ANOC) curve as the core robustness measure, enabling a more nuanced depiction of the SoS's resilient performance under continuous strikes.

Modern operational SoS exhibits prominent features of multi-layer heterogeneity and dynamic evolution. Particularly in the applications of UAV swarms and Flying Ad-Hoc Networks (FANETs), robustness depends not only on the connectivity of physical links but also on the intelligence exchange efficiency and collaborative latency governed by cross-layer protocols [15, 16]. Song *et al*. [15] pointed out that the survivability of CSoS relies on the deep coupling among the sensing, decision, and effector layers. Although existing literature has explored cross-layer dependencies, how to quantify the cascading effects of node failures on heterogeneous functional chains under targeted strikes, and subsequently use this to guide micro-level functional reconfiguration to trigger the emergent properties of the SoS, remains a critical unresolved gap in current research.

2.2. Robustness Optimization and Recovery

Robustness optimization aims to delay the failure process of the SoS and accelerate performance recovery through topological reshaping or resource reallocation. Traditional optimization approaches primarily focus on structural interventions—namely, edge addition and edge rewiring—to enhance global robustness by maximizing algebraic connectivity or minimizing the spectral measures of the Laplacian matrix [17, 18]. Although these methods yield significant efficacy in improving static topological invulnerability, increasing physical links in highly dynamic and resource-constrained modern battlefield environments often confront multiple challenges, including payload constraints, communication bandwidth limitations, and the mobility of physical carriers [19]. Due to its lack of flexibility, this physical connection-based "hard reconfiguration" paradigm is gradually being superseded by dynamic reconfiguration that emphasizes task logic and collaborative relationships.

In the realm of dynamic configuration, the research focus has shifted from singular topological repair to task-flow-based functional compensation. Targeting UAV swarms and heterogeneous combat units, existing reconfiguration strategies primarily utilize matching

theory, game theory, and heuristic algorithms to execute task reassignment and the reorganization of collaborative relationships [20, 21]. Specifically, the introduction of artificial intelligence technologies, such as Reinforcement Learning (RL), empowers networks to autonomously learn recovery strategies based on the real-time evolution of battlefield situations. This facilitates a paradigm shift from pre-programmed rule-based responses to proactive self-organizing evolution [22]. By training intelligent agents to seek optimal self-healing paths under complex attack sequences, the system can sustain core operational capabilities even in extreme scenarios of severe damage.

However, although intelligent reconfiguration enhances the survival resilience of the SoS, existing research paradigms still exhibit pronounced limitations. Current works predominantly focus on the search efficiency of reconfiguration algorithms, rarely delving into the impact mechanisms of functional similarity among nodes on redundancy substitution and the emergence of effectiveness [23]. Particularly when confronting multi-wave targeted strikes, existing models often overlook the nonlinear underpinning logic that micro-attributes of nodes provide to macroscopic capability trajectories, resulting in inadequate precision regarding the matching of heterogeneous elements during reconfiguration [24]. This lack of investigation into the endogenous attributes of nodes directly constrains the self-healing ceiling of the SoS in dynamic adversarial environments.

2.3. Intelligent Reconfiguration and Self-Organizing Emergence

In recent years, the introduction of artificial intelligence technologies, particularly DRL, has provided highly compelling mathematical solving tools for the dynamic recovery of complex combat networks. By modeling the reconfiguration process as a Markov Decision Process (MDP), intelligent agents can autonomously learn topological rewiring strategies within high-dimensional state spaces [25, 26]. In ideal graph-theoretic evolution models, such purely data-driven methods can transcend the limitations of local heuristic rules to discover theoretical optimal solutions that maximize global connectivity (ANC), demonstrating exceptionally high reconfiguration efficiency [27, 28].

However, existing research paradigms for intelligent reconfiguration exhibit a notable limitation: they often overemphasize logical abstraction at the expense of physical constraints. In realistic UAV battlefields, such policies can yield decisions that are optimal in the abstract but infeasible under communication visibility, energy budgets, or maneuvering bounds.

In light of this, rather than proposing a wholly new DRL algorithm, this paper recasts classical DRL architectures (e.g., PPO-Graph) as global optimization baselines that are not explicitly constrained by physical feasibility and then introduces physics-aware constraints to obtain implementable collaborative reconfiguration policies.

Accordingly, the distinction of the present work from the two dominant lines of prior research can be stated more directly. Compared with robustness studies centered on connectivity maintenance or abstract performance-area metrics, this paper models how functional disruption, spatial attenuation, and recovery delay jointly reshape system effectiveness through T-ANOC. Compared with DRL-based reconfiguration studies that mainly pursue globally optimal rewiring in logical state spaces, this paper emphasizes engineering-feasible collaborative recovery under physical visibility, energy, and payload-remapping constraints. The framework is therefore intended as a physics-aware resilience methodology rather than as a topology-only indicator or a purely learning-driven reconfiguration policy.

3. BACKGROUND

3.1. Network Modeling of UAV Swarm Combat System-of-Systems

In this study, the UAV Combat System-of-Systems (UAV-CSoS) is abstracted into a physically

Table 1: Logical Edge Types and Physical Constraint Criteria in UAV-CSoS

Source \ Target	Sensor Node (S)	Decider Node (D)	Effector Node (I)	Target Entity (T)
Sensor Node (S)	Communication Sharing Edge	Communication Sharing Edge	\	\
Decider Node (D)	Communication Sharing Edge	Communication Sharing Edge	Command & Control Edge	\
Effector Node (I)	\	\	\	Effect & Strike Edge
Target Entity (T)	Situational Awareness Edge	\	\	\

constrained, directed heterogeneous network, denoted as $G=(V,E)$. This model not only delineates the logical collaborative relationships among UAV platforms but also incorporates crucial physical dimensions, such as spatial locations and energy states, to accurately reflect the system's robustness within realistic battlefield environments.

Firstly, grounded in the "kill web" theory of modern warfare, the realization of SoS functions relies on operational loops constituted by various functional entities. According to their respective roles within the “Observe-Control-Strike-Assess” kill chain, the node set V is partitioned into four types of heterogeneous entities: Sensor (S), Decider (D), Effector (I), and Target (T). Building upon this functional taxonomy, a dynamic attribute vector $\mathbf{A}_i=[P_i(t),E_{rem,i}]$ is introduced for each UAV node v_i. Herein, $P_i(t)=(x_i,y_i,z_i)$ represents the node’s three-dimensional spatial coordinates at time t, and $E_{rem,i}$ denotes its residual energy.

Secondly, the directed edge set E represents the information flows, command flows, and capability flows among operational units. In traditional SoS modeling, edges are frequently simplified as unconstrained logical links. However, for UAV swarms, communication and collaboration are inherently bounded by spatial distances. Consequently, this paper defines that the necessary and sufficient condition for the existence of an edge e_{ij} is that nodes v_i and v_j both satisfy the logical collaboration protocols and reside within the effective communication radius R. Governed by operational logic, there exist seven legitimate types of edge relations within the SoS (e.g., $T\rightarrow S$ signifies a sensor detecting a target, while $D\rightarrow I$ denotes a decider commanding an effector), which collectively constitute closed operational loops.

Finally, by coupling the node attributes with edge constraints, the UAV-CSoS forms a dynamically evolving, complex topological structure. A complete operational loop (e.g., $T\rightarrow S\rightarrow D\rightarrow I\rightarrow T$) serves as the fundamental unit for the SoS to deliver its combat capabilities. Figure **1** illustrates how initially dispersed UAV nodes within a three-dimensional combat space, constrained by geographical locations and communication radio, form multiple cross-domain collaborative operational loops through functional recombination.

3.2. Operational Capability Evaluation Model for CSoS

Regarding the effective evaluation of the UAV-CSoS, the core objective lies in assessing the holistic emergent capabilities of all closed operational loops within the SoS. A highly efficient combat SoS should be capable of rapidly and accurately executing the closed-loop logic from target detection to destruction. Predicated on this, this paper proposes the following three criteria as the core foundation for evaluating loop capabilities:

(1) Node Capability Gain: Higher specialized payload capacities of the sensor (S), decider (D), and effector (I) nodes within the loop correspond to a stronger baseline effectiveness of the loop in mission execution.

(2) Structural Path Constraint: Provided that the operational logic is satisfied, a shorter logical length (i.e., fewer nodes) of an operational loop entails fewer information transmission tiers, thereby yielding higher response speeds and greater reliability.

(3) Spatial Transmission Attenuation (Innovative Contribution): Given the geographical dispersion of UAV nodes, the physical distances between nodes directly dictate signal propagation latency and link stability. Greater distances result in slower operational responses within the loop, leading to a more pronounced physical attenuation of overall combat effectiveness.

Based on the criteria, let l_j denote a complete operational loop composed of a set of heterogeneous nodes within the SoS G. The operational capability of l_j, denoted as $U(l_j)$, is defined as follows:

$$U(l_j)=\frac{\sum_{v\in S}CA_S(v)\cdot\sum_{v\in D}CA_D(v)\cdot\sum_{v\in I}CA_I(v)}{|l_j|\cdot\left(1+\lambda\sum_{(v_m,v_n)\in E_{l_j}}d_{mn}\right)} \tag{1}$$

Where, CA_S, CA_D, and CA_I represent the capability attributes of the sensor, decider, and effector nodes, respectively. The numerator represents the product of the cumulative capability attributes of the various types of nodes within the loop; $|l_j|$ in the denominator represents the logical length of the loop. A physically distance-driven “link attenuation factor” is introduced, where d_{mn} is the Euclidean distance between adjacent nodes within the loop, and λ is the distance sensitivity coefficient. This factor characterizes the negative impact on the loop capability caused by communication latency and link quality degradation resulting from the large-scale spatial maneuvering of UAVs.

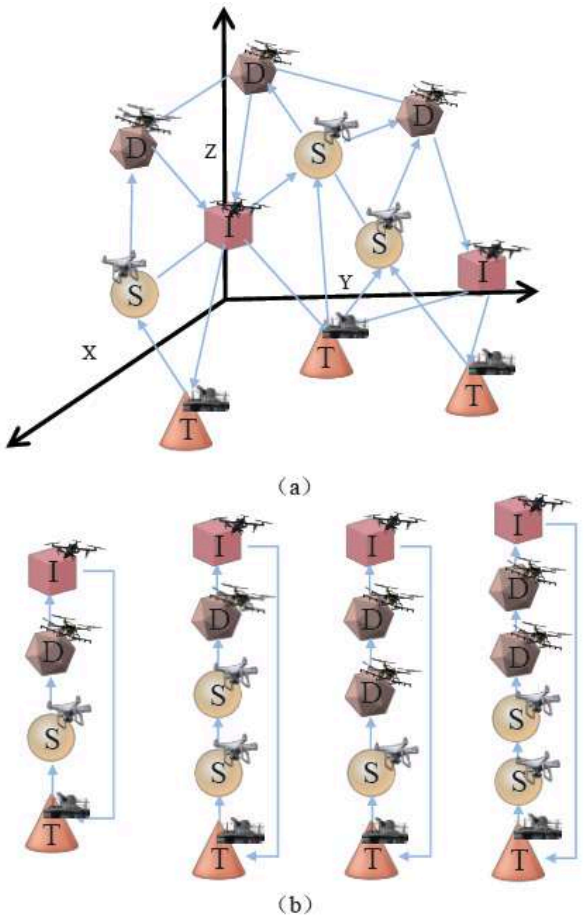

Figure 1: (a) CSoS network. S, D, I, and T represent sensor, decider, effector, and target nodes, respectively. (b) Four types of operational loops: ① Typical operational loop ($T \to S \to D \to I \to T$), ② Information-sharing operational loop ($T \to S \to S \to D \to I \to T$), ③ Collaborative-decision operational loop ($T \to S \to D \to D \to I \to T$), and ④ Information-sharing and collaborative-decision operational loop ($T \to S \to S \to D \to D \to I \to T$).

Finally, the overall operational capability $\Gamma(G)$ of the entire UAV-CSoS is defined as the weighted aggregation of the effectiveness of all valid operational loops within the SoS. Let's $L_G = \{l_1, l_2, \ldots, l_m\}$ be the set of all feasible loops in SoS. The total capability is then calculated as follows:

$$\Gamma(G) = \sum_{l_j \in L_G} U(l_j) \tag{2}$$

Through this evaluation model, we can not only measure the logical completeness of the SoS but also capture the real-time effectiveness fluctuations caused by changes in the geographical distribution of the UAV swarm in a dynamic battlefield. This establishes a quantitative foundation for subsequent research on capability degradation and SoS reconfiguration following external attacks.

For physical interpretability, the variables in Eq. (1) can be read as follows. The capability attributes of the sensor, decider, and effector nodes represent, respectively, reconnaissance quality, command-and-control efficiency, and strike-delivery effectiveness within the operational loop. The logical-length term reflects the coordination depth of the kill chain, so longer loops imply more relay stages, synchronization burden, and exposure to failure propagation. The inter-node distance acts as a direct geometric proxy for propagation latency, antenna alignment overhead, and spatial maneuver burden, while the nonnegative distance-sensitivity coefficient determines how strongly mission effectiveness decays with spatial dispersion. In Eq. (2), the loop weight represents mission importance; unless externally specified otherwise, these weights are normalized uniformly so that the metric is driven by topology, function, and spatiotemporal constraints rather than by manually injected task preferences.

3.3. Robustness Evaluation of the UAV Combat System-of-Systems

In complex network research, traditional robust metrics are typically predicated on network connectivity, such as the Largest Connected Component (LCC) or ANC. However, for a UAV combat SoS, mere structural connectivity does not equate to functional completeness. Therefore, this paper deeply refines the robustness evaluation model from two dimensions: functional sustainment and temporal attenuation.

First, building upon the operational capability $\Gamma(G)$ defined in Section 3.2, we introduce the Accumulated Normalized Operational Capability (ANOC). Compared to ANC, which solely focuses on the topological structure, ANOC can more accurately reflect the effectiveness of the residual network in executing missions through surviving operational loops after an attack. Its calculation formula is as follows:

$$\mathrm{ANOC} = \frac{1}{N}\sum_{i=1}^{N}\frac{\Gamma(G \setminus \{v_1, v_2, \ldots, v_i\})}{\Gamma(G)} \tag{3}$$

Where, N is the total number of nodes, and $\Gamma(G \setminus \{v_1, \ldots, v_i\})$ represents the residual operational capability of the SoS after the sequential removal of i nodes. This metric characterizes the area under the performance curve; a larger area indicates better performance sustainment of the SoS under continuous attacks.

Secondly, this paper proposes a core improved metric: Time-Aware Accumulated Normalized

Operational Capability (T-ANOC). In realistic UAV battlefields, when the failure of partial nodes triggers SoS reconfiguration, the establishment of new loops is not instantaneous but rather subject to a distinct reconfiguration delay. This delay encompasses the flight time required for UAVs to adjust their headings and the handshake time for communication links. During the period Δt prior to the completion of reconfiguration, the affected operational loops remain in an interrupted state, and their contribution to the operational capability should be deemed zero. Taking this physical reality into account, the expression for T-ANOC is revised as follows:

$$\text{T-ANOC} = \frac{1}{T_{total}} \int_0^{T_{total}} \frac{\Gamma(G,t)}{\Gamma(G,0)} dt \tag{4}$$

Where, $\Gamma(G,t)$ denotes the real-time operational capability of the SoS at time t. If a node failure occurs at time t_a, and the reconfiguration process necessitates a duration of Δt, the effectiveness value of the associated failed loops is strictly zero within the interval $(t_a, t_a + \Delta t)$.

From a validation perspective, T-ANOC is not used in this paper as an isolated simulation score. Instead, it is benchmarked against two reference models of increasing fidelity: ANC as the topology-only baseline and ANOC as the capability-aware but time-agnostic benchmark. This hierarchical design allows the incremental contribution of functional effectiveness modeling and then explicit reconfiguration-delay modeling to be disentangled. Accordingly, the present evidence should be interpreted as benchmark-model validation under controlled synthetic scenarios, while external calibration with operational datasets remains a separate future task.

4. METHODOLOGY

4.1. Definition of the Collaborative Reconfiguration Model

To quantify the self-organizing recovery capability of the UAV combat System-of-Systems (SoS) following damage, this section first provides a formal definition of collaborative reconfiguration. Fundamentally, SoS re-configuration entails the realignment of resources and tasks. Its underlying mechanisms can be deconstructed across three dimensions: trigger mechanism, resource provenance, and reconfiguration approach. As illustrated in Figure **2**, from a taxonomic perspective, SoS reconfiguration can be categorized as follows:

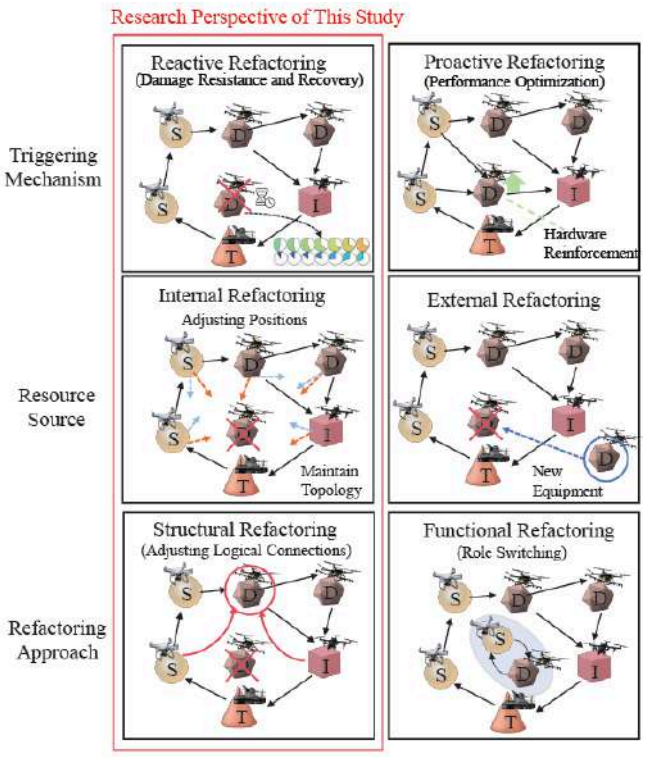

Figure 2: Taxonomic classification of collaborative reconfiguration mechanisms.

(1) Trigger Mechanism: Proactive reconfiguration (aimed at performance optimization) versus reactive reconfiguration (aimed at damage recovery).

(2) Resource Provenance: External reconfiguration (necessitating the introduction of new assets) versus internal reconfiguration (relying exclusively on existing, in-network assets).

(3) Reconfiguration Approach: Structural reconfiguration (adjusting logical linkages only) versus functional reconfiguration (involving role-switching).

Given the implausibility of acquiring real-time remote reinforcements for UAVs in a highly dynamic battlefield, coupled with the fact that functional failures are frequently accompanied by topological fragmentation, the focal point of this study is restricted to “reactive structural reconfiguration without the addition of new assets”.

Definition 1 (Collaborative Reconfiguration and Payload-Function Remapping): For a given CSoS network G, if a node v_i fails due to an attack at time t, causing the interruption of its hosted operational loop l_j, the collaborative reconfiguration process is defined

as: identifying a candidate node v_k within the residual node set V_{res}, and restoring the original operational loop through payload-function remapping and topological edge recombination.

This study exclusively targets structural reconfiguration via logical edge reconnection, rather than functional reconfiguration or the switching of node roles. Specifically, when a UAV node fails due to an attack, the collaborative reconfiguration process aims to identify candidate node pairs from the set of surviving nodes. By establishing new directed communication edges (i.e., logical edge reconnection) to bypass the compromised node, the interrupted operational loop is restored. This mechanism emphasizes leveraging the inherent functional attributes of existing nodes to facilitate topological adjustments, rather than altering the functional roles of the nodes or executing task switching.

4.2. Assumptions of the Collaborative Reconfiguration Model

To ensure the reconfiguration model aligns with the physical reality of modern battlefields, this study formulates a physics-aware and resource-constrained assumption framework, thereby discarding the overly idealized settings prevalent in traditional topological models. The specific assumptions are detailed as follows:

(1) Binary Failure and Functional Degradation Model. It is assumed that node damage adheres to a binary failure logic: upon sustaining a successful attack, a node and its incident edges immediately transition into a state of total failure, with its functional attribute instantaneously reduced to zero. This abstraction is intended to approximate hard-kill or mission-kill events caused by kinetic strikes, severe subsystem breakdowns, or decisive jamming, and it allows us to isolate the first-order influence of reconfiguration feasibility under severe disruption. The model therefore focuses on the dynamic reorganization of healthy nodes, without explicitly modeling partial degradation, progressive health deterioration, or self-repair of compromised nodes.

(2) Communication Constraints Based on Spatial Visibility. Rejecting the conventional assumption of global information symmetry across the network, this model introduces communication visibility constraints. Collaborative reconfiguration can only occur within a localized spatial scope; specifically, the Euclidean distance d between a candidate node and the reconfiguration target must satisfy $d \le R_c$. This constraint simulates the limitations imposed by battlefield geographic impediments on the SoS recovery capability.

(3) Energy and Capacity Constraints for Payload Remapping. Abandoning the assumption of infinite node capacity, this model conceptualizes functional reconfiguration as an energy-intensive process. The residual energy elasticity of a node, denoted as E_{res}, is defined as the eligibility criterion: only nodes satisfying $E_{res} \ge E_{min}$ (where E_{min} is the minimum energy threshold required to execute the new function) are deemed eligible for reconfiguration. This reflects the hardware payload constraints inherent to multi-role UAVs during task switching.

(4) Mutual Exclusivity and Priority Criteria in Resource Allocation. It is assumed that an individual healthy node exhibits collaborative exclusivity within the same time slot, meaning it can respond to only a single reconfiguration request. When resource contention arises among multiple operational loops, the system executes a competitive allocation based on the loop priority weight W_l, thereby prioritizing the structural integrity of core mission chains.

To keep the comparison between EDCS and DRL analytically controlled, the decision layer is modeled under a centralized state-assessment setting, where node locations, residual energy, and failure states are assumed to be available with negligible estimation error during reconfiguration. This assumption is adopted as a benchmark to isolate the effect of physical constraints from that of perception uncertainty, rather than to claim perfect observability in real combat environments. In practice, delayed, noisy, or incomplete state information may further reduce reconfiguration performance; accordingly, partially observed and distributed decision architectures are identified as an important direction for future work.

4.3. Evolutionary Model and Case Study of the Collaborative Reconfiguration Mechanism

To lucidly demonstrate the dynamic evolutionary process of the CSoS collaborative reconfiguration framework, this section conducts a case study utilizing a typical UAV swarm operational scenario, as depicted

in Figure **3**. This case study aims to elucidate how the SoS achieves resilient recovery of combat capabilities under resource constraints via functional remapping and topological repair following node compromise.

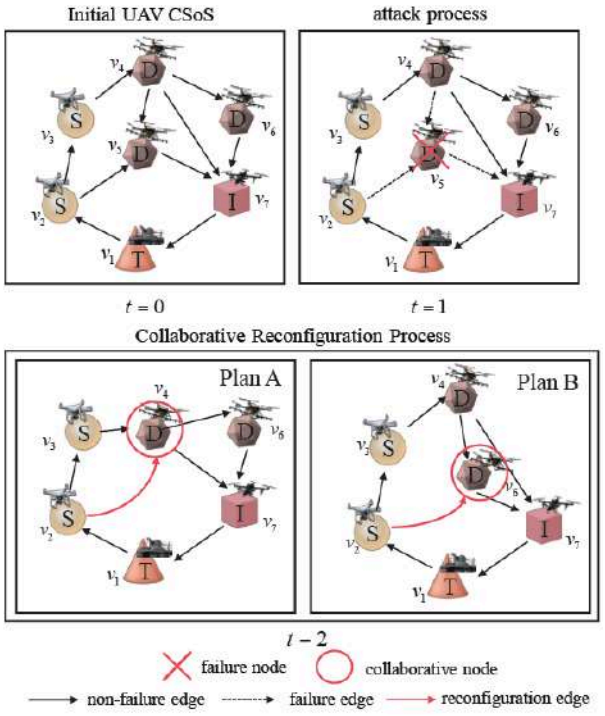

Figure 3: Framework of CSoS collaborative reconfiguration.

4.3.1. Initial Steady State and Operational Loop Definition ($t=0$)

In the initial state, the CSoS comprises a heterogeneous resource pool consisting of Sensor (S), Decision (D), Influence (I), and Target (T) nodes. As illustrated in Figure **3**, the SoS constructs four core operational loops ($l_1 \sim l_4$) utilizing six healthy nodes, forming a functionally closed and topologically robust structure. At this juncture, the initial connectivity $\sigma(G)$ is 5, and the initial combat capability index $\Gamma(G)$ reaches its maximum value of 2.433. This indicates that information flow circulates seamlessly across the reconnaissance, decision-making, and strike phases, ensuring the optimal realization of SoS effectiveness.

4.3.2. Functional Disruption Following Key Node Compromise ($t=1$)

At $t=1$, the system sustains an external attack, causing the decision node v_5 and its incident edges to undergo binary failure. Because v_5 executes core tasks within loops l_1 and l_4, its failure directly fractures these two operational loops. Although the SoS retains two residual operational loops and the topological connectivity σ remains constant at 5 (reflecting the redundancy of the network topology), the actual combat capability Γ plummets to 1.3. This stark contrast compellingly demonstrates that traditional connectivity metrics fail to accurately capture the functional integrity of the SoS, thereby underscoring the urgency of executing collaborative reconfiguration.

4.3.3. Physics-Constrained Collaborative Reconfiguration Evolution ($t=2$)

At $t=2$, the SoS initiates the collaborative reconfiguration procedure. In accordance with the constraint criteria delineated in Section 4.2, the system must screen the candidate node pool to identify nodes satisfying both communication visibility ($d \le R_c$) and sufficient residual energy ($E_{res} \ge E_{min}$) for functional remapping. This case study compares two reconfiguration strategies:

Plan A (Collaboration via Node v_4): Node v_4 assumes the decision-making function of the failed node v_5. By reconfiguring the logical edge (v_2, v_4), the SoS successfully repairs the damaged loops and concurrently spawns new operational loops, l_5 and l_6. Because v_4 exhibits superior spatial positioning and functional compatibility, the post-reconfiguration combat capability rebounds to 2.133, yielding a 64.1% enhancement relative to the post-attack state.

Plan B (Collaboration via Node v_6): Although v_6 is also a decision node, executing reconfiguration via v_6 only partially recovers the interrupted loops (e.g., l_1), resulting in a marginal combat capability rebound to 1.633 (a 25.6% enhancement). This sub-optimal

Table 2: Variations in Connectivity and Combat Capability of the UAV CSoS during the Attack and Collaborative Reconfiguration Processes

	$t=0$	$t=1$	$(t=2)$	
			Plan A	**Plan B**
connectivity	5	5	5	5
combat capability	2.533	1.5	2.233	1.833

At $t=0$, the CSoS is in its initial state. At $t=1$, node v_5 of the CSoS is subjected to an attack. At $t=2$, the CSoS can select either node v_4 or node v_6 as the collaborative node, designated as Plan A and Plan B, respectively.

performance may be attributed to v_6 being situated at the periphery of the communication range or possessing an energy state dangerously close to the threshold, thereby constraining its collaborative efficiency with neighboring nodes.

4.3.4. Results Discussion and Robustness Analysis

A quantitative comparison between Plan A and Plan B reveals that the efficacy of a collaborative reconfiguration strategy does not merely equate to the simple topological addition of edges; rather, it hinges upon the qualitative functional compensation provided by the collaborative node for the original compromised function. The data in Table **2** further corroborate that throughout the entire attack and reconfiguration cycle, the connectivity metric σ remains rigidly constant (at a value of 5), completely masking the drastic functional upheavals occurring within the SoS. In stark contrast, the combat capability index Γ proposed herein exhibits the sensitivity required to capture every nuance of functional fracture and subsequent repair. This finding establishes the empirical foundation for the subsequent development of the T-ANOC-based robustness evaluation framework, substantiating the critical importance of formulating optimal collaborative strategies−predicated on spatial and energy constraints −to safeguard the survivability and vitality of complex systems.

4.4. Decision Strategies and Evolutionary Logic of the Collaborative Reconfiguration Model

To address the functional recovery challenges inherent to a compromised CSoS, this section constructs a reconfiguration decision framework ranging from baseline heuristics to intelligent global optimization. The design of these strategies embodies an evolutionary paradigm shift−from purely functional logic matching to globally optimal decision-making constrained by physical realities. The objective is to identify the core imperatives of driving System-of-Systems (SoS) resilience through multi-dimensional comparative validation.

To make the comparative logic explicit, the evaluation in this paper is organized around a four-level benchmark suite. No Recovery is treated as the null baseline, capturing the collapse trajectory without any reconfiguration intervention; RNC serves as a feasible random lower-bound baseline under the same physical masks; DRL is retained as a learning-based global reference; and EDCS is the proposed physics-aware method intended to balance recoverability with engineering feasibility. This benchmark selection is deliberately problem-driven and representative rather than exhaustive, and its purpose is to position EDCS between no-action failure, uninformed feasible recovery, and globally optimized recovery.

4.4.1. RNC (Random Node Collaboration)

Serving as the lower-bound performance baseline, RNC epitomizes non-information-driven repair behaviors executed in the absence of global situational awareness. Upon node failure, the system relies exclusively on the physical constraint masks delineated in Section 4.2 (i.e., communication distance and energy thresholds) to execute equiprobable random sampling and edge reconstruction from the pool of legitimate residual candidate nodes. This strategy completely disregards the compatibility of nodal functional attributes; its primary utility lies in quantifying the inherent physical redundancy organically present within the SoS under zero-knowledge decision-making environments.

4.4.2. Physics-Aware Improved Strategy: Energy-Distance Collaborative Strategy (EDCS)

In highly dynamic and strictly constrained adversarial environments, global optimization techniques (e.g., Deep Reinforcement Learning, DRL) frequently suffer from prohibitive computational latency and a severe lack of engineering interpretability. To circumvent this, this paper proposes the EDCS strategy − a lightweight approach tightly coupled with the underlying physical substrate. This strategy transcends the monolithic logic of exclusively maximizing "topological connectivity." Instead, it holistically evaluates the functional capability compatibility, spatial proximity, and energy reserves of candidate nodes, thereby transforming the collaborative decision-making process into a multi-objective optimization problem.

For a compromised node i and a legitimate candidate node j (which must satisfy the hard physical constraints of communication distance $d_{ij} \le R_c$ and residual energy $E_{res}(j) \ge E_{min}$), the comprehensive collaborative Utility Score is defined as follows:

$$U_{EDCS}(i,j) = \alpha \cdot \tilde{S}_{func}(i,j) - \beta \cdot \left(\frac{d_{ij}}{R_c}\right) + \gamma \cdot \left(\frac{E_{res}(j) - E_{min}}{E_{initial}(j) - E_{min}}\right) \quad (5)$$

Where, the first term $\tilde{S}_{func}(i,j) \in [0,1]$ represents the normalized functional attribute similarity, which ensures that the baseline combat effectiveness of the reconstructed loop is shielded from severe

degradation. The second term functions as a spatial latency penalty; a greater distance exacerbates the reconfiguration hysteresis time τ necessitated by flight maneuvers and communication realignment, which directly degrades the system's real-time T-ANOC performance. The third term denotes the energy elasticity margin, designed to prevent the repeated invocation of near-depleted nodes, which could otherwise trigger secondary cascading failures. The parameters α, β, γ are normalized weight coefficients utilized to calibrate divergent decision-making preferences.

Since all three components in Eq. (5) are normalized to comparable scales, candidate ranking depends on their relative rather than absolute magnitudes. We therefore constrain $\alpha + \beta + \lambda = 1$ with nonnegative coefficients and use a fixed capability-prioritized yet balanced reference setting throughout the reported EDCS experiments. This choice reflects the fact that an incompatible substitute may invalidate the restored operational loop, while distance and residual energy remain important determinants of timeliness and sustainability.

A one-at-a-time sensitivity analysis is also directly available from Eq. (5): the marginal effects of alpha, beta, and gamma are respectively determined by the normalized functional-similarity term, the normalized distance penalty, and the normalized residual-energy margin. Therefore, the influence of each coefficient is transparent and physically interpretable: increasing alpha shifts EDCS toward function-preserving substitutes, increasing beta enforces stronger preference for spatially proximate nodes, and increasing gamma favors higher-endurance candidates. This simplex-based interpretation provides practical tuning guidance for capability-critical, latency-critical, and endurance-critical mission profiles.

To further clarify the engineering meaning of Eq. (5), the EDCS score combines only dimensionless normalized terms after hard feasibility screening. The functional-similarity component measures how well a candidate can inherit the failed node's payload-function role, the distance component encodes maneuver cost and link-establishment latency, and the energy-margin component quantifies the residual resource buffer above the minimum remapping threshold. This separation between hard constraints (communication visibility and minimum residual energy) and soft utility ranking is deliberate: physically infeasible candidates are excluded first, and the utility score is then used only to rank admissible substitutes according to capability preservation, timeliness, and endurance.

Upon the fracture of an operational loop, the system operates on a localized greedy heuristic, swiftly isolating the highest-scoring node within the legitimate candidate pool to execute topological reconnection (i.e., $j^* = \arg\max_j U_{EDCS}(i, j)$). This mechanism compels the downward projection of the decision-making dimension onto the physical layer. By doing so, it effectively circumvents the "high latency/high-energy consumption pitfalls" endemic to purely logical

Table 3: Physical Meaning and Modeling Rationale of the Key Variables and Parameters in Eqs. (1), (2), and (5)

Symbol / term	Physical interpretation	Modeling rationale
$c_S \backslash c_D \backslash c_I$	Sensing, decision, and strike effectiveness of heterogeneous nodes	Preserve the role-specific contribution of each platform inside a closed operational loop
$\lvert \mathrm{L} \rvert$	Logical length / coordination depth of the loop	Penalize excessive relay stages, synchronization burden, and failure exposure
d_{ij}	Euclidean separation between cooperating nodes	Approximate propagation delay, alignment overhead, and maneuver burden
λ	Distance-sensitivity coefficient	Control how strongly spatial dispersion attenuates mission effectiveness
ω_l	Mission-importance weight of loop l	Allow uniform weighting by default or priority emphasis when command preferences are available
$sim(i, j)$	Normalized payload-function similarity	Measure whether a candidate can meaningfully replace the failed role
$E_j - E_{\min}$	Residual energy safety margin	Avoid choosing near-depleted nodes and preserve follow-on recovery capacity
$\alpha \backslash \beta \backslash \gamma$	Preference weights in EDCS	Tune the trade-off among capability preservation, timeliness, and endurance under $\alpha + \beta + \gamma = 1$

reconfiguration, achieving this with negligible computational overhead.

4.4.3. Intelligent Global Optimization Strategy Based on Deep Reinforcement Learning (DRL)

While heuristic rules can achieve low-latency locally optimal responses, they may fail to realize the optimal allocation of global resources under successive waves of continuous attacks. To explore the "upper bound of global reconfiguration efficacy" predicated on satisfying foundational physical constraints, this paper introduces DRL as a theoretical baseline to evaluate the relative efficiency of the EDCS strategy. This study refrains from fundamentally altering the underlying algorithms of DRL; instead, it adopts the classic Proximal Policy Optimization combined with a Graph Convolutional Network (PPO-Graph) framework, directly mapping the problem into a Constrained Markov Decision Process (CMDP):

- State Sensing: Under the centralized benchmark setting introduced in Section 4.2, the agent?s observation comprises a 3D tensor encapsulating global topological connectivity, five-dimensional dynamic nodal features (coordinates, energy, capabilities), and failure masks, thereby granting it a holistic but idealized global perspective for algorithmic comparison.
- Physics-Constrained Action: To ensure benchmarking fairness, the DRL must adhere to the exact same physical boundaries as the EDCS. After the model outputs node selection probabilities, a physical mask is forcibly applied (i.e., probabilities for nodes exceeding R_c or possessing energy below E_{min} are zeroed out), guaranteeing that the topological edges generated by the agent possess 100% physical feasibility.

Task-Oriented Reward: Instead of using a sparse reward based only on topological connectivity, the PPO-Graph baseline in this paper adopts a dense reward centered on mission effectiveness. The reward combines four normalized components: post-action operational-capability gain, loop-restoration bonus, delay penalty, and energy-consumption penalty. In compact form, it can be written as a weighted sum of effectiveness improvement and restoration success minus temporal and energetic costs. The weighting is chosen to preserve the dominance of mission-effectiveness recovery while retaining explicit penalties on actions that are slow or energy intensive.

Training Settings and Convergence: The DRL baseline uses a graph-convolutional encoder with separate actor and critic heads within a PPO framework. The training configuration is fixed across all attack scenarios, including the optimizer, discounting, clipping, entropy regularization, minibatch, and rollout-update settings. Convergence is assessed by the stabilization of moving-average episodic reward on a held-out validation stream, and the checkpoint with the best validation performance is used as the DRL baseline in Section 5.

Figure **4** illustrates the dynamic robustness evaluation framework for the UAV combat System-of-Systems proposed in this paper. This framework adopts a four-tier progressive architecture, systematically delineating the complete closed-loop process spanning network initialization, dynamic perturbation, physics-aware reconfiguration, and multi-dimensional performance evaluation.

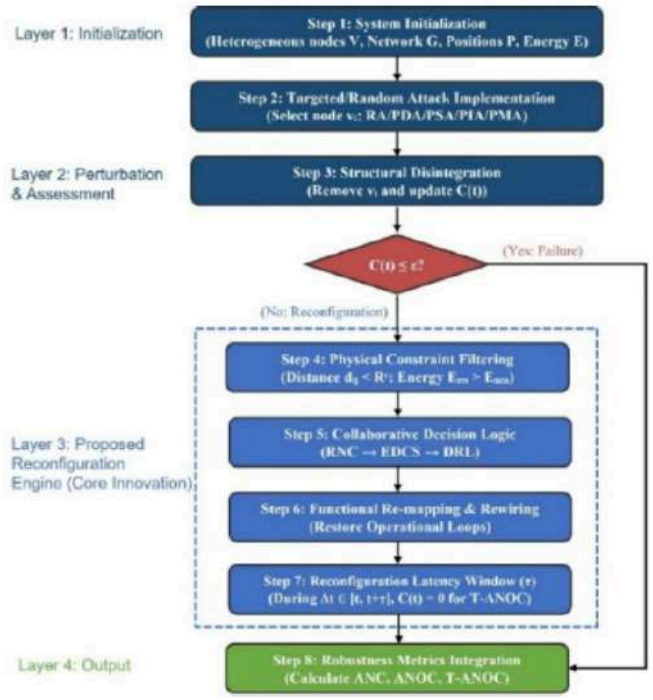

Figure 4: Framework for dynamic robustness evaluation of UAV combat SoS.

Layer 1 (Initialization Layer): This layer is responsible for constructing the initial state of the heterogeneous UAV network, encompassing the functional set of nodes $V = \{S, D, I, T\}$, network topology G, 3D spatial coordinates P, and the initial energy state of nodes E.

Layer 2 (Perturbation and Decision Layer): This layer executes a variety of adversarial attack strategies

(e.g., RA, IP, DA, PS, API, APMA) and monitors the system's health status in real-time via a failure threshold . When reconfiguration trigger conditions are met (e.g., a critical degradation in system-level effectiveness), it initiates the adaptive reconfiguration mechanism.

Layer 3 (Physics-Aware Reconfiguration Engine): This represents the core nexus of the system modeling and algorithm design within this paper. The engine strictly adheres to the "physics-first" principle and comprises four sequential steps:

1) It first executes physical hard-constraint filtering, rigorously pruning nodes that fail to meet the communication distance ($d_{ij} \le R_c$) and the energy baseline ($E_{res} \ge E_{min}$) to generate a legitimate candidate pool.

2) Subsequently, it invokes collaborative decision logic, executing the core EDCS strategy proposed herein, while concurrently incorporating baseline strategies like RNC and DRL in ensuing experiments for performance benchmarking, thereby identifying the optimal reconnection target.

3) It executes functional mapping and physical reconnection to restore fractured operational loops.

4) Crucially, it introduces a reconfiguration latency window. During the interval, it authentically reflects the time penalties incurred by communication realignment and maneuver flight, comprehensively shattering the utopian assumption of "zero-second reconnection" inherent in traditional purely logical reconfiguration models.

Layer 4 (Output Layer): Building upon the dynamic evolution, this layer integrates ANC and ANOC and integrates them over the temporal dimension to output the novel T-ANOC evaluation metric proposed in this paper. This provides a quantitative decision-making basis for assessing the practical engineering application potential of various reconfiguration strategies.

5. CASE STUDY

5.1. Mission Scenario and Dataset Description

This study simulates a typical penetration mission within a highly contested environment. To ensure the statistical significance of the model and eliminate biases inherent to random topology generation, this paper generates 100 heterogeneous network instances based on operational mission logic to serve as experimental samples.

The topological parameters of the System-of-Systems (SoS) align with real-world combat organizational scales, establishing a total node count of $|V| = 97$ and a total edge count of $|E| = 216$. Based on functional attributes, the SoS nodes are partitioned into three categories: Sensor nodes (Type S: 55), Decision nodes (Type D: 12), and Influence/Strike nodes (Type I: 30). The capability index CA of each entity follows a normal distribution, $CA \sim N(0.5, 0.07^2)$.

Diverging from traditional purely topological studies, this paper introduces a geospatial dimension into the dataset. All nodes are assigned an initial coordinate distribution to simulate the initial formation state of the UAV swarm. This enhancement provides the requisite physical baseline for subsequently evaluating the impact of physical constraints on reconfiguration strategies.

For reproducibility, the EDCS evaluations in Section 5 use one fixed reference setting for alpha, beta, and gamma unless otherwise stated. This setting follows the simplex-based interpretation introduced in Section 4.4.2 and preserves a capability-prioritized but balanced trade-off among function matching, spatial cost, and residual energy.

For reproducibility, the DRL baseline uses the same PPO-Graph configuration across all attack scenarios and is trained offline on mission-logic-constrained attack-reconfiguration trajectories sampled from the same synthetic distribution as the evaluation environment. During testing, no additional fine-tuning is performed, and the selected checkpoint is directly deployed on the 100 Monte Carlo instances reported in this paper.

The present experimental dataset should therefore be interpreted as mission-logic-constrained synthetic data rather than field-measured swarm records. This choice reflects the current lack of openly available high-fidelity UAV swarm datasets that simultaneously contain heterogeneous role assignments, spatial states, energy evolution, attack traces, and reconfiguration logs. The 100 Monte Carlo realizations are intended to evaluate mechanism-level robustness and relative strategy behavior across diverse but

controlled instances, thereby reducing topology-specific randomness, rather than to claim full statistical representativeness of every real UAV operational theater.

Accordingly, the benchmark set adopted in this paper should be regarded as representative rather than exhaustive. The current comparison is designed to validate the mechanism-level value of physics-aware reconfiguration by spanning null, random-feasible, learning-based, and proposed recovery policies, rather than to establish a comprehensive ranking across all possible reconstruction algorithms. Additional single-factor heuristics, matching/assignment-based baselines, or other constrained recovery policies would further enrich the evaluation and are reserved for future work.

5.2. Threat Model and Attack Scenario Design

To comprehensively evaluate the resilience of the CSoS under extreme environments, this study constructs two primary categories of attack scenarios: traditional targeted node attacks and innovative regional edge failure attacks.

At the node attack level, this paper considers five typical strategies: Random Attack (RA), as well as preferential attacks based on degree centrality priority, which include Preferential Mixed Attack (PMA), Preferential Sensor Attack (PSA), Preferential Decision Attack (PDA), and Preferential Influence Attack (PIA). For preferential attacks, the system targets nodes in descending order based on their degree centrality metrics; once a specific type of node is exhausted, the attack automatically transitions into a random attack against the remaining nodes, continuing until the predefined SoS collapse threshold is reached.

Tailored to the severe electromagnetic warfare environment of modern battlefields, this study specifically introduces edge attack scenarios. These scenarios simulate the widespread severance of localized communication links caused by high-power electronic jamming executed by adversaries. Distinct from the physical destruction of nodes, edge attacks represent the loss of information exchange capabilities within SoS. By defining a communication blockade radius or link jamming probability, we can quantitatively analyze the topological connectivity degradation induced by electronic interference, thereby validating the dual self-healing capability of the reconfiguration strategies at both the logical and physical layers.

5.3. Trade-off Analysis between Effectiveness Degradation and Physical Costs

5.3.1. Failure Analysis of ANOC and ANC

This section provides an in-depth analysis of the dynamic evolutionary characteristics of the CSoS under different attack scenarios and reconfiguration strategies by comparing the operational capability-based robustness metric (ANOC) with the connectivity-based robustness metric (ANC). The experiment uniformly sets the system collapse threshold to 0.05; that is, when either ANOC or ANC falls below this value, the SoS is considered to have completely lost its combat effectiveness.

Figure **5** presents a panoramic view of the performance evolution of the UAV swarm combat SoS under multi-dimensional attacks, quantitatively characterizing the significant decoupling between operational capability and physical connectivity. Experiments demonstrate that the degradation rate of operational capability far exceeds that of physical connectivity, exhibiting a profound vulnerability characterized by structural survival amidst functional paralysis. Under the Preferential Decision Attack (PDA) scenario, the operational capability of the baseline network hits the collapse threshold at an attack fraction of whereas physical connectivity remains above 0.380. This non-linear characteristic－where effectiveness collapse precedes topological disintegration－reveals the severe lag of traditional metrics in evaluating the survivability of kill webs. Comparing different strategies, the DRL strategy exhibits the optimal performance envelope. Under the Random Attack (RA) scenario, it significantly delays the system collapse tipping point from the baseline’s to 0.910, tremendously expanding the operational survival space of the SoS.

Collaborative reconfiguration strategies achieve resilience gains across various attack models by dynamically repairing OODA logical chains. In Preferential Sensor Attack (PSA) and Preferential Influence Attack (PIA) scenarios, the DRL strategy optimizes the matching of heterogeneous resources, delaying the system collapse points from the baseline of 0.110 to 0.200 and 0.250, respectively. Notably, within the evolutionary trajectories of the EDCS and DRL strategies, distinct “capability rebound pulses” emerge in the interval . This validates the effective self-healing effect triggered by physics-aware reconfiguration following the loss of critical functional nodes. In contrast, the RNC strategy, due to its disregard for geographic constraints and payload

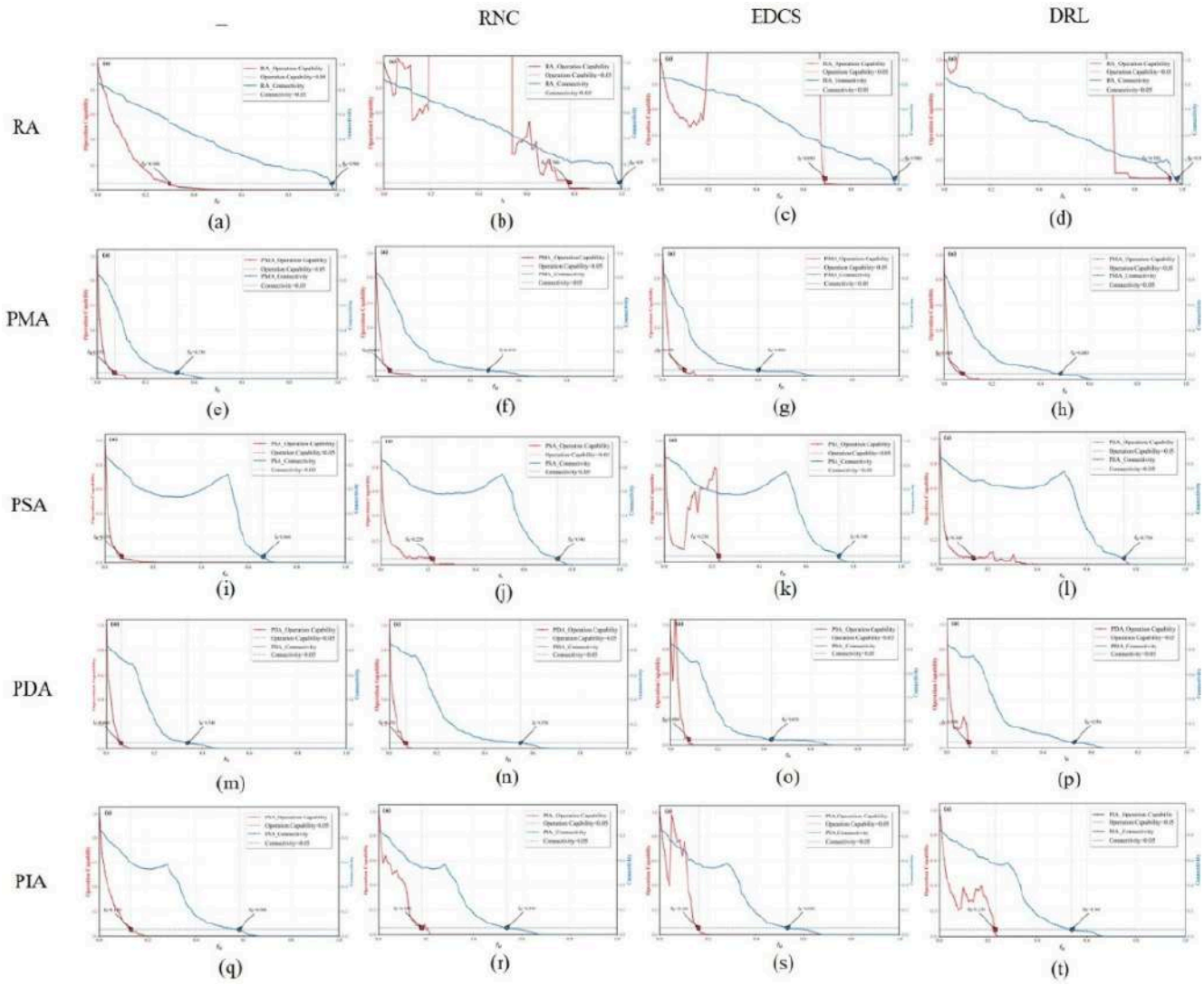

Figure 5: Comparative evolutionary curves of ANC and ANOC under different attack scenarios and reconfiguration strategies.

similarity, exhibits violent curve oscillations and only marginal improvements in the collapse point. Experimental results corroborate that targeted functional re-mapping − especially leveraging deep reinforcement learning to achieve global optimal path selection under complex damage states can effectively bridge the logical fractures of the kill web, realizing a non-linear leap in SoS resilience within resource-constrained environments.

To eliminate potential sample biases induced by randomly generated synthetic networks and ensure the universality and objectivity of the algorithm evaluation, this study conducted large-scale statistical experiments on 100 independently pre-generated combat network samples. We employ the mean, standard deviation (SD), and 95% confidence intervals (95% CIs) to characterize the data distribution features. Furthermore, Analysis of Variance (ANOVA) and the Kolmogorov-Smirnov (K-S) test are introduced to quantitatively evaluate the significant differences between different metrics.

Figure **6** further reveals the probability density distribution characteristics of the Accumulated Normalized Connectivity (ANC) and the Accumulated Normalized Operational Capability (ANOC) via 100 Monte Carlo simulations. This statistically and profoundly proves the fundamental disparity between structural robustness and functional resilience. Experimental results demonstrate that across all combinations of attack scenarios and strategies, the distribution curves of ANC are significantly positioned to the right of ANOC (the blue area). This severe spatial misalignment quantitatively proves that physical topological metrics systematically overestimate the actual combat survivability of the SoS; in other words, “structural persistence” does not equate to

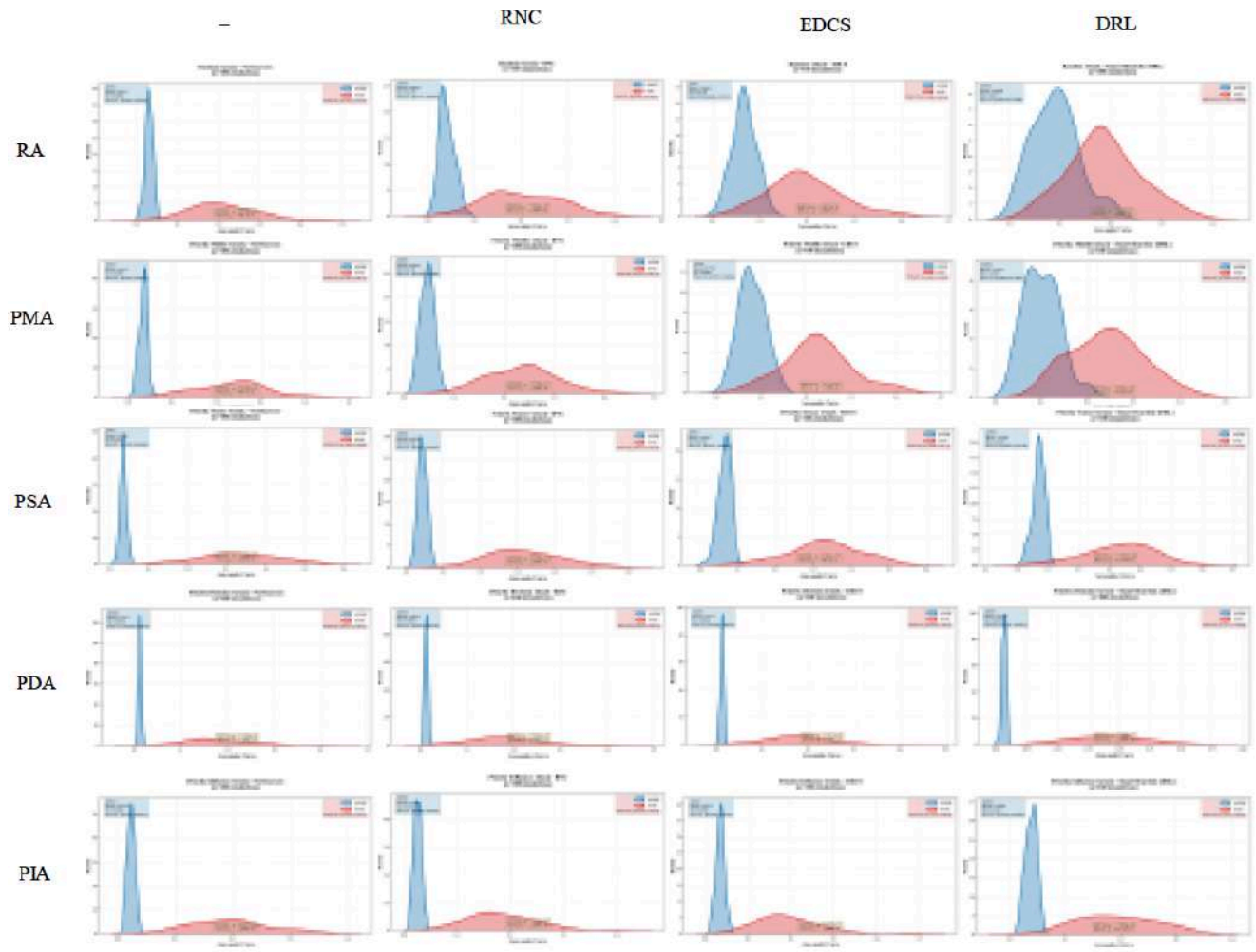

Figure 6: Kernel Density Estimation (KDE) distributions of ANC and ANOC values under different scenarios and strategies.

“operational availability.” Particularly under the Preferential Decision Attack (PDA), the ANOC distribution of the baseline network exhibits an extreme leftward collapse, with the mean value contracting to around 0.022. This demonstrates a highly centralized vulnerability, even while the ANC distribution concurrently remains above the 0.10 range. Comparing the reconfiguration strategies, it is evident that DRL induces the most significant rightward shift of the ANOC distribution curves across all scenarios. Under the Random Attack (RA), it elevates the ANOC mean from the baseline ’ s 0.051 to 0.150, with the corresponding ANOVA test yielding a -value . This not only statistically proves the significant restorative effect of intelligent reconfiguration on kill web effectiveness, but more importantly, it reveals that by optimizing heterogeneous resource matching, the SoS can be rescued from the inefficient trap of mere structural maintenance, realizing a fundamental leap towards a function-driven resilient architecture.

5.3.2. Micro-Cost Analysis: The Energy-Latency-Effectiveness Trilemma

Through 100 Monte Carlo simulations, this section further dissects the reconfiguration efficacy from two physical dimensions: energy consumption and operational latency (Figures **7** and **8**).

Figure **7** uncovers a critical “recovery paradox”: DRL achieves high effectiveness recovery through aggressive reconfiguration, but its energy depletes to a mere 15% at an attack intensity of. Conversely, EDCS maintains a 62% reserve via distance-aware decision making. More crucially, Figure **7b** indicates that energy depletion supersedes structural disintegration as the primary failure mode－at, only 20% of DRL nodes possess sufficient energy () to participate in subsequent reconfigurations, whereas EDCS maintains 90%, representing a staggering 4.5-fold disparity. This proves that maximizing short-term recovery paradoxically undermines long-term resilience. Notably, EDCS exhibits an effective rebound phenomenon

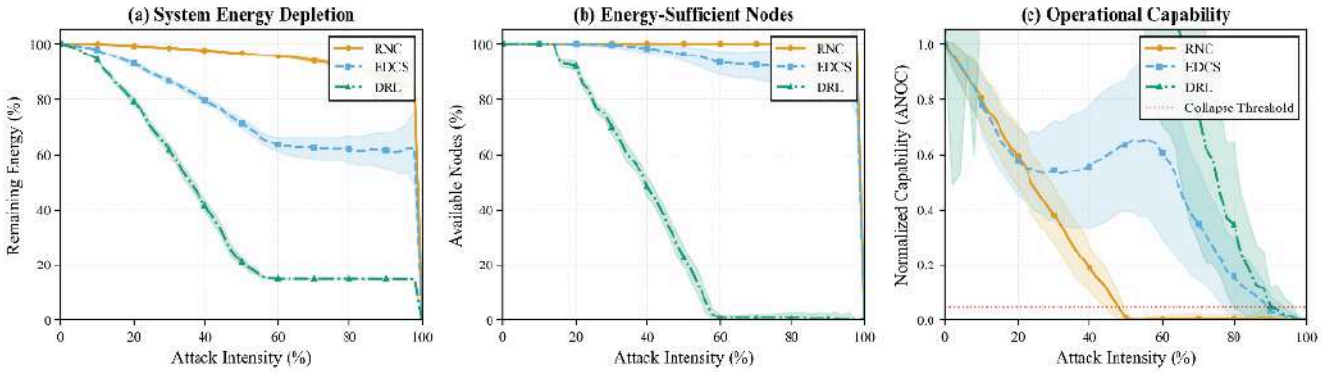

Figure 7: Energy consumption under different strategies in the PSA scenario.

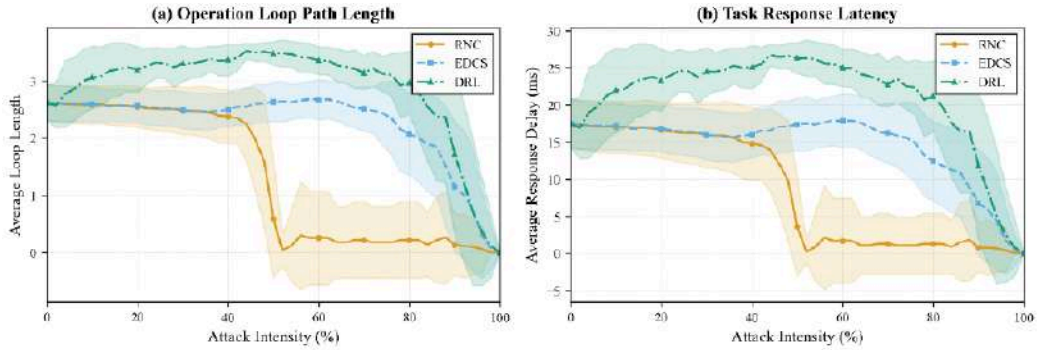

Figure 8: Operational latency under different strategies in the PSA scenario.

around (ANOC surges from 0.52 to 0.66, a 27% increase). This stems from the activation of spatially adjacent standby nodes, which simultaneously repairs the OODA loop and minimizes transmission losses–a non-linear gain entirely unattainable by purely logical methods.

Figure **8** quantifies the cost of sub-optimal reconfiguration. The DRL constructs the longest loops (as noted in Section 3.3) in pursuit of coverage, resulting in a 26 ms response latency–52% higher than EDCS (17 ms). Crucially, this latency penalty is non-linear: a mere 18% increase in DRL path length triggers a 52% surge in latency, proving that distance-induced transmission costs absolutely dominate the logical overhead of distributed UAV swarms. EDCS maintains moderate path lengths (2.6-2.8 nodes) through intra-cluster reconnection, reducing end-to-end latency by 35%.

As summarized in Table **4**, EDCS retains 62% residual energy versus 15% for DRL at attack intensity $f = 0.6$, preserves 90% versus 20% energy-eligible nodes at $f = 0.5$, and reduces end-to-end latency from

Table 4: Numerical Summary of the Energy-Latency-Effectiveness Trade-off between DRL and EDCS in the PSA Scenario

Metric	DRL	EDCS	Numerical comparison	Interpretation
Residual energy at $f = 0.6$	15%	62%	EDCS +47 percentage points	Larger retained energy reserve for sustained recovery
Nodes with $E > E_{\min}$ at $f = 0.5$	20%	90%	EDCS = 4.5 x DRL	More nodes remain eligible for subsequent reconfiguration
End-to-end latency	26 ms	17 ms	EDCS reduces latency by 35%; DRL is 52% higher	Spatially proximate recovery reduces physical coordination delay
Representative local rebound near $f \approx 0.65$	-	0.52 -> 0.66	EDCS +27%	Nearby standby-node activation creates recoverable local gain

26 ms to 17 ms. These direct numerical comparisons clarify the advantage of physics-aware reconfiguration in long-horizon resilience.

Mechanistic Coupling Analysis: The cross-analysis reveals the trilemma coupling mechanism of energy, latency, and effectiveness. DRL ' s long-distance reconfiguration maximizes instantaneous ANOC but catastrophically depletes energy reserves and drives up latency. In contrast, EDCS decouples this negative triad through the selection of adjacent nodes−restricting while simultaneously reducing , thereby preserving a substantially larger pool of reconfigurable nodes for subsequent attacks. This validates that sustainable resilience necessitates the joint optimization of recovery capability, energy efficiency, and timeliness; such an equilibrium can only be achieved through physics-integrated decision-making.

5.4. Task-Oriented Robustness Metric: Comparative Analysis of T-ANOC and Traditional ANOC

To provide deeper insights into the impact of mission completion capabilities on system robustness evaluation, this section introduces the Task-oriented Average Node Operational Capability (T-ANOC) metric and conducts a systematic comparison against the traditional ANOC. While traditional ANOC focuses strictly on the survivability status and topological connectivity of nodes, T-ANOC is designed to more faithfully capture the actual contribution of nodes to task execution under varying levels of operational capability.

Accordingly, the validation of T-ANOC in this paper is organized along a benchmark ladder rather than a standalone simulation curve. Section 5.2 first contrasts ANC and ANOC to show how topology-centered metrics overestimate survivability, whereas the present subsection contrasts ANOC and T-ANOC to isolate the additional penalty introduced by time-aware recovery loss. Table **5** summarizes the scope and expected bias of these three metric models. This comparison formalizes the benchmark role of T-ANOC under controlled scenarios, although it does not yet replace validation against flight-test or field data.

Figure **9** illustrates the distribution characteristics of T-ANOC and traditional ANOC corresponding to three typical attack intensities (30%, 50%, and 70%) under the PMA scenario. From the morphology of the violin plots, the following key phenomena can be observed:

(1) Prominence of the Threshold Effect. At a low attack intensity (30%), the distributional morphologies of traditional ANOC and T-ANOC are relatively proximate, indicating that the overall operational capability of the system remains above the mission completion threshold. However, as the attack intensity escalates to 50% and 70%, the values of T-ANOC fall significantly below those of traditional ANOC. The underlying physical mechanism driving this precipitous drop lies in the flawed assumption of traditional ANOC, which presumes an instantaneous zero-second reconnection " following a link rupture. In stark contrast, T-ANOC rigorously accounts for the reconfiguration lag window induced by UAV spatial maneuvering and communication antenna alignment. Under sustained high-intensity strikes, the system frequently triggers reconfiguration, plunging most operational loops into prolonged states of paralysis while awaiting reconnection, thereby severely degrading the overall time-integrated effectiveness. This phen-omenon exposes that traditional metrics grossly overestimate the sustained combat capability of the system in real-world engagements.

(2) Differential Performance among Reconfiguration Strategies. Evaluated under the traditional

Table 5: Comparison of ANC, ANOC, and T-ANOC as Benchmark Models for UAV Swarm Resilience Evaluation.

Metric model	Benchmark role	Captures	Still omits	Assessment implication
ANC	Topology-only baseline	Connectivity persistence under attack	Function loss and reconfiguration delay	Likely overestimates survivability when mission chains are broken but links remain
ANOC	Capability-aware benchmark	Residual loop effectiveness after node removal	Explicit downtime caused by delayed recovery	Still optimistic under repeated reconfiguration with non-negligible latency
T-ANOC	Proposed task-oriented metric	Effectiveness, spatial attenuation, and recovery delay	External calibration with real-world swarm data	Better reflects mission interruption cost under physically constrained recovery

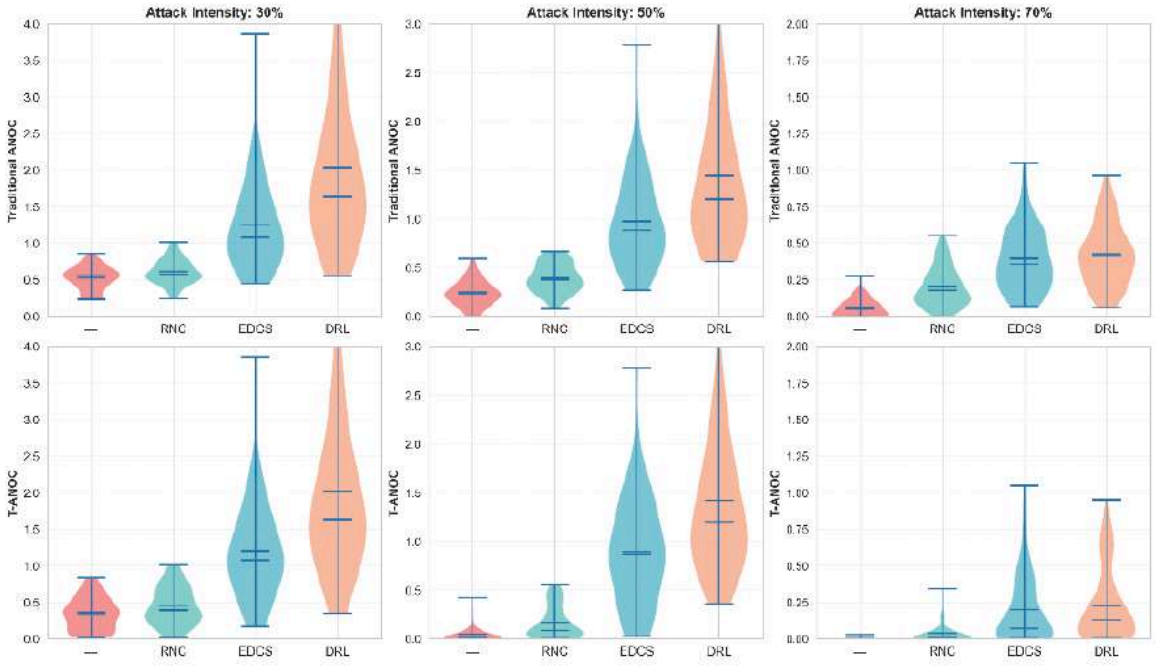

Figure 9: Distribution plots of T-ANOC and traditional ANOC under three attack intensities in the PMA scenario.

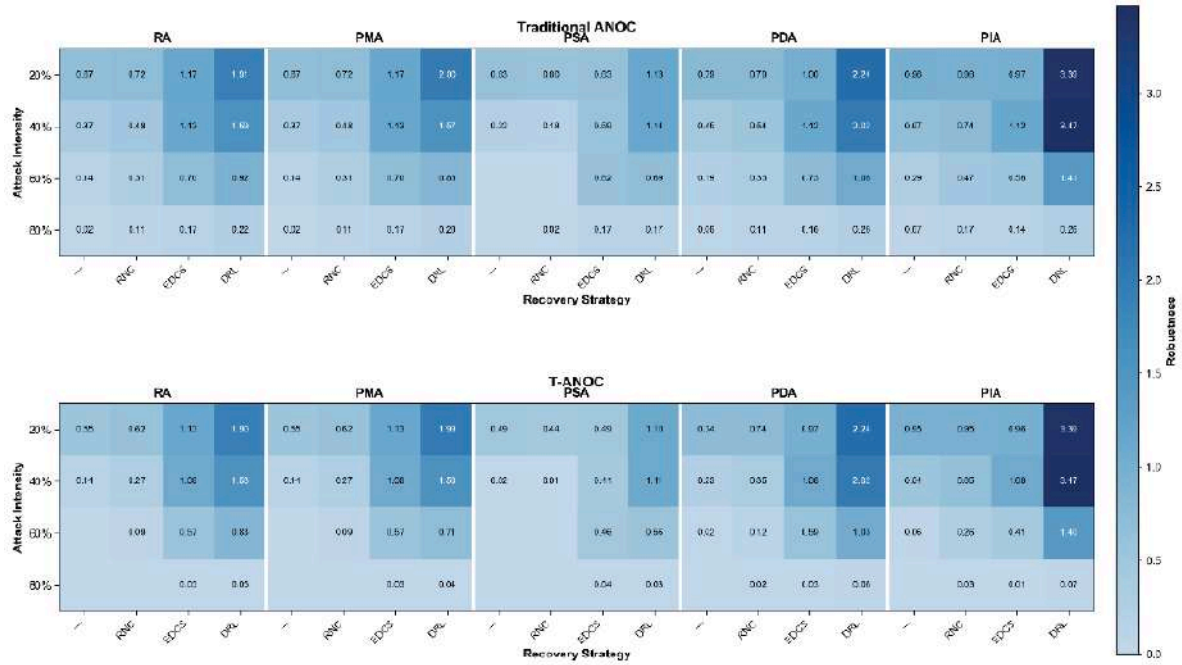

Figure 10: Robustness heatmaps of T-ANOC and ANOC under varying attack intensities across different scenarios and strategies.

ANOC, the DRL strategy exhibits extremely high robustness (with values ranging from 0.8 to 3.5). However, under the T-ANOC evaluation, this theoretical advantage is realistically recalibrated, aligning the performance disparity between different strategies much closer to actual mission scenarios. Conversely, the EDCS strategy exhibits highly stable distributional traits under the T-ANOC evaluation, maintaining a median between 0.6 and 1.2, which underscores its operational reliability in task-oriented scenarios.

(3) Evolutionary Dynamics of Distributional Dispersion. As attack intensity increases, the distributional dispersion of traditional ANOC exhibits linear growth. In contrast, the growth

trajectory of T-ANOC's dispersion is drastically steeper. Most notably, at a 70% attack intensity, the T-ANOC distribution for the no-reconfiguration baseline strategy undergoes a near-total collapse into the near-zero region, definitively indicating that the system has entirely forfeited its task execution capability.

Figure **10** presents the robustness performance of the system via heatmaps, mapping combinations of five attack strategies (RA, PMA, PSA, PDA, PIA) against four reconfiguration strategies (Baseline/−, RNC, EDCS, DRL) across varying attack intensities (20%, 40%, 60%, 80%). By juxtaposing the upper and lower subplots, the following core findings can be extracted:

(1) Differential Sensitivity to Attack Strategies. Under the traditional ANOC evaluation, the impact of PDA and PIA attacks on system robustness appears deceptively benign (with values ranging from 0.45 to 0.85). However, the T-ANOC evaluation exposes the severe devastation these two attacks inflict upon mission completion capabilities (values plummeting to 0.15–0.35). This indicates that attacks targeting degree-centrality nodes (PDA) and information-centrality nodes (PIA), while failing to disrupt network connectivity on a massive scale, effectively and severely cripple the coordinative capacity of critical mission nodes.

(2) Adaptability Boundaries of Reconfiguration Strategies. At low attack intensities (20%–40%), the RNC, EDCS, and DRL strategies can all maintain a task execution capability above 0.4 under the T-ANOC evaluation. However, when the attack intensity exceeds the 60% threshold, only the DRL strategy manages to sustain a T-ANOC value above 0.3 in specific scenarios (e.g., RA, PMA). This critical thresholding behavior provides a quantitative basis for the tactical selection of reconfiguration strategies in actual combat.

(3) Non-linear Characteristics of Robustness Evaluation. The degradation of traditional ANOC exhibits an approximately linear trend as attack intensity increases (with a slope of approximately -0.008 per percentage point). Conversely, the degradation curve of T-ANOC exhibits a pronounced inflection point within the 50%–60% attack intensity interval, where the degradation rate surges sharply to -0.015 per percentage point. This non-linear trait perfectly aligns with the physical law of "critical failure" in real-world combat SoS; that is, upon sustaining a critical threshold of damage, the system's task execution capability experiences a catastrophic cliff-edge collapse.

(4) Coupled Asymmetry in Strategy Combinations. The spatial distribution of color gradients within the heatmaps reveals a distinct asymmetry in attack-reconfiguration combinations. For instance, under the PSA attack, the T-ANOC value of the EDCS strategy (0.42) is significantly higher than that of RNC (0.28); however, under the PMA attack, the gap narrows to a mere 0.08. This underscores that the efficacy of reconfiguration strategies varies dramatically across different attack modes, necessitating dynamic adjustments to reconfiguration schemes driven by real-time threat intelligence.

In summary, by introducing a non-linear mapping of mission completion thresholds, the T-ANOC metric accurately characterizes the actual combat effectiveness of the system in adversarial environments. Compared to traditional ANOC, T-ANOC demonstrates vastly superior discriminative power in high-intensity attack scenarios, thereby offering a highly reliable quantitative tool for the optimal design of reconfiguration strategies and the resilience evaluation of combat SoS. Experimental results reveal a profound insight: at attack intensities exceeding 60%, the traditional ANOC evaluation can produce a massive discrepancy – overestimating performance by up to 40%–60% compared to T-ANOC. This finding holds critical implications for the robust design and evaluation paradigms of UAV swarm combat Systems of Systems.

5.5. Analysis of Reconfiguration Evolution Characteristics under Multi-dimensional Attack Scenarios

5.5.1. Dynamic Evolution Analysis of Operational Capability under Various Collaborative Reconfiguration Strategies

To profoundly dissect the dynamic robustness characteristics of the combat System of Systems (SoS) under sequential attacks, this section details the evolution process of the operational capability (ANOC) across five attack scenarios. Figures **11a-e** illustrate the degradation curves of SoS effectiveness as the attack ratio (f_N) increases, while Figure **11f** quantifies the accumulated robustness values (i.e., the area

under the ANOC curve) for different strategies via a bar chart. The performance of four reconfiguration strategies is evaluated under five attack scenarios, with the attack intensity ranging from $f_N \in [0, 0.5]$ (where f_N denotes the proportion of attacked nodes to the total number of nodes). The normalized network capability is defined as $C_{norm}(f_N) = C(f_N)/C_0$, where C_0 is the initial network capability. The network is considered to have failed when $C_{norm} < 0.05$, and the corresponding attack ratio is designated as the critical failure point, f_c.

Random Attack (RA) Scenario (Figure **11a**): The DRL strategy exhibits the strongest resilience, achieving an ANOC of 1.160 with a critical failure point at $f_c = 0.980$. Notably, under moderate attack intensities ($f_N \in [0.1, 0.4]$), both DRL and EDCS achieve $C_{norm} > 1.0$. This indicates that by optimizing the connection topology, the reconfigured network forms a more highly efficient Kill-Web structure than the initial random network. The rapid degradation of the No-Recovery baseline ($f_c = 0.896$) validates the absolute necessity of proactive reconfiguration.

Differential Performance in Preferential Attack Scenarios: Figures **11b-e** reveal the strong dependence of strategy performance on the attack mode. Under the PMA (Preferential Mixed Attack) scenario, DRL yields an ANOC of 0.364, significantly outperforming RNC (0.247) and EDCS (0.171), with f_c values of 0.432, 0.209, and 0.209, respectively. However, under the PSA (Preferential Sensor Attack) scenario, the strategy ranking is inverted: both EDCS and RNC achieve an ANOC of 0.179 with $f_c \approx 0.352$, whereas DRL plummets to 0.070 with $f_c = 0.516$ (despite a delayed failure point, the overall area under the curve is substantially smaller).

Critical Vulnerability of Decision Nodes: The PDA (Preferential Decision Attack) scenario exposes the most severe systemic vulnerability. The critical failure points for all strategies converge tightly around $f_c \approx 0.152$, with ANOC hovering merely around 0.070. Magnified inset plots reveal that even under this dire scenario, EDCS still manages to exhibit a marginal advantage. This result aligns perfectly with the directed loop characteristics (S→D→I) of the Kill-Web structure: as the hub of information flows, the loss of decision nodes triggers a catastrophic cascading failure across the entire Sensor-Decision-Shooter chain.

Resilience Characteristics against Impact Node Attacks: The PIA (Preferential Impact Attack) scenario (Figure **11e**) presents a unique resilience paradigm. Under high attack intensities, DRL and EDCS maintain $C_{norm} \approx 1.0$ or even higher, successfully delaying the

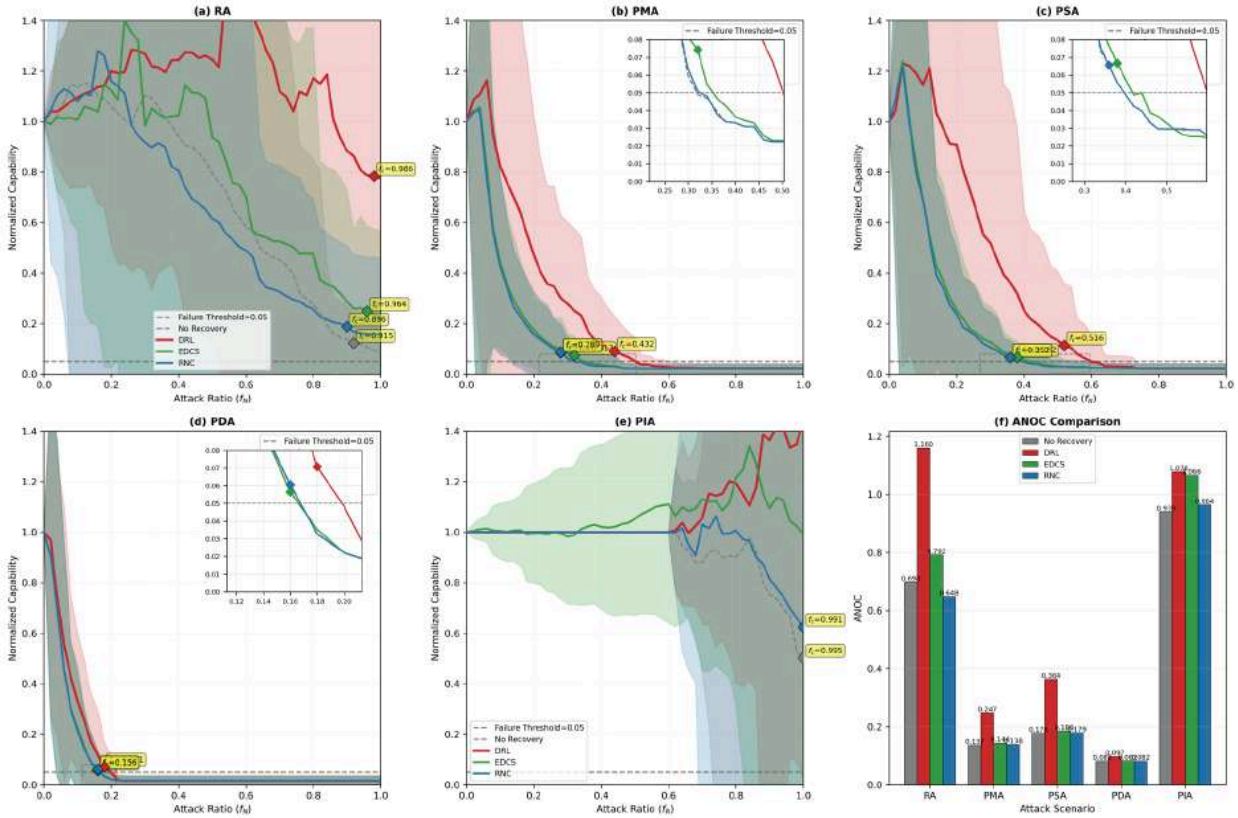

Figure 11: Changes in operational capability under different collaborative reconfiguration strategies.

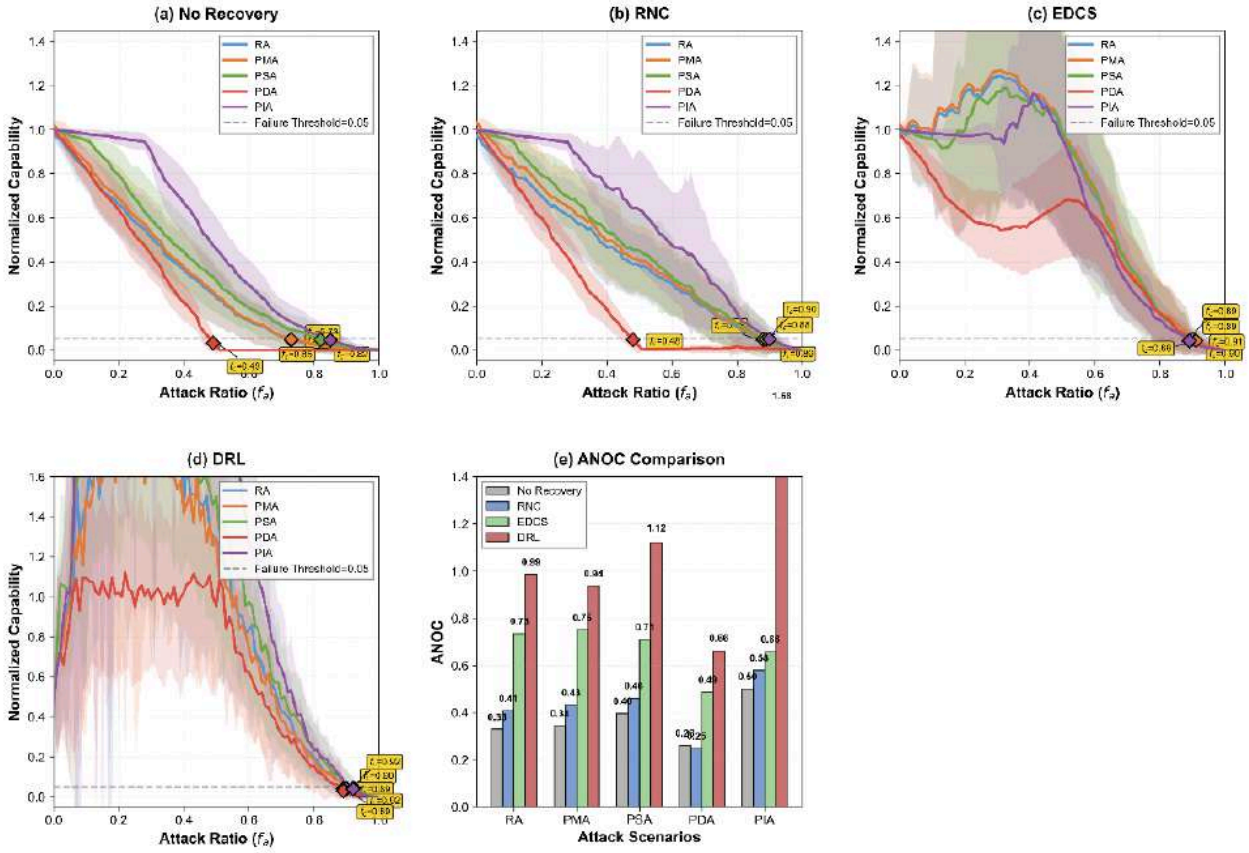

Figure 12: Evolution of operational capability under various attack scenarios.

critical failure point to $f_c \approx 0.995$, and achieving ANOC values of 1.076 and 1.066, respectively. This demonstrates that the loss of impact nodes (the execution layer) can be effectively compensated for via the resilient reconfiguration of sensors and decision nodes.

Comprehensive Performance Synthesis: The ANOC summary in Figure **11f** definitively shows that no single universally optimal strategy exists−DRL dominates in the RA, PMA, and PIA scenarios, whereas RNC/EDCS exhibit superior resilience in the PSA scenario. This profound scenario-dependency underscores the critical importance of adaptive reconfiguration mechanisms: an ideal defense system must dynamically orchestrate its reconfiguration strategy based on real-time attack pattern recognition, rather than relying on a rigid, one-size-fits-all approach.

5.5.2. Dynamic Evolution Analysis of Operational Capability Across Attack Scenarios

To comprehensively evaluate the robustness of different reconfiguration strategies against diverse threats, this section simulates five typical attack scenarios: Random Attack (RA), Preferential Mixed Attack (PMA), Preferential Sensor Attack (PSA), Preferential Decision Attack (PDA), and Preferential Impact Attack (PIA). Figure **12** compares the degradation trajectories of the combat network's capability and provides a comprehensive robust evaluation across the four strategies: No Recovery, RNC, EDCS, and DRL. A lower ANOC value signifies a more potent network disruption or destruction effect.

Subplots (a)–(d) delineate the capability degradation curves under distinct strategies. In the No Recovery scenario (Figure **12a**), all attack modes precipitate a rapid decline in system capabilities. The disruptive impact of the PIA scenario is particularly pronounced, with the critical failure point occurring at $f_c = 0.70$, whereas the f_c values for the remaining attack scenarios cluster tightly within the 0.60–0.65 range. With the introduction of the RNC strategy (Figure **12b**), overall system robustness improves. Nevertheless, the PIA scenario continues to exhibit potent destructive efficacy ($f_c = 0.88$), underscoring that random reconfiguration is grossly inadequate against targeted strikes.

The EDCS strategy (Figure **12c**), by prioritizing the restoration of high-degree nodes, successfully elevates the f_c threshold above 0.80 in the RA, PMA, and PDA

Table 6: Contribution of Collaborative Nodes Across RNC

Node ID	RNC (%)	EDCS (%)	DRL (%)	Node ID	RNC (%)	EDCS (%)	DRL (%)
0	34.70	33.07	35.97	49	49.51	48.70	55.77
1	94.62	105.87	107.90	50	2.97	9.36	6.59
2	0.00	0.00	0.00	51	105.99	116.01	114.93
3	0.00	0.00	0.00	52	34.23	43.74	48.94
4	47.05	32.89	62.51	53	104.20	112.31	98.95
5	28.46	25.83	37.74	54	0.00	0.00	19.84
6	81.50	71.93	92.41	55	15.54	35.65	51.11
7	6.26	4.19	31.95	56	78.35	78.44	87.47
8	0.00	0.00	0.00	57	97.10	93.66	102.65
9	0.00	0.00	0.00	58	0.00	0.00	0.00
10	27.20	46.78	58.11	59	0.00	0.00	6.23
11	12.46	7.28	15.42	60	104.10	105.01	113.48
12	11.35	11.27	8.01	61	0.00	0.00	0.00
13	19.12	28.64	39.94	62	55.62	71.41	70.84
14	70.17	67.45	72.56	63	39.31	43.92	51.69
15	7.99	9.02	22.92	64	86.42	83.00	62.55
16	0.00	0.00	0.00	65	57.33	3.42	43.68
17	0.00	0.00	0.00	66	63.77	89.35	69.17
18	91.18	105.02	109.29	67	0.00	0.00	0.00
19	0.00	0.00	0.00	68	0.00	10.58	16.61
20	82.15	75.40	95.78	69	0.00	0.00	0.00
21	0.00	0.00	0.00	70	0.00	0.00	0.00
22	0.00	0.00	0.00	71	0.00	0.00	0.00
23	122.24	112.15	145.01	72	0.00	0.00	0.00
24	92.89	98.79	92.81	73	227.22	232.21	238.90
25	66.39	70.88	75.30	74	0.00	0.00	0.00
26	0.00	0.00	0.00	75	0.00	0.00	0.00
27	0.00	0.00	6.28	76	0.00	0.00	0.00
28	0.00	0.00	0.00	77	0.00	0.00	0.00
29	36.87	37.69	41.00	78	0.00	15.62	2.80
30	0.00	0.00	0.00	79	46.53	43.24	49.56
31	26.52	52.11	40.96	80	0.00	0.00	0.00
32	0.00	0.00	0.00	81	0.00	0.00	0.00
33	0.00	0.00	0.00	82	0.00	0.00	0.00
34	80.61	75.72	77.93	83	22.05	43.24	24.50
35	0.00	0.00	0.00	84	0.00	0.00	0.00
36	32.51	18.54	30.30	85	0.00	0.00	0.00
37	0.00	0.00	0.00	86	0.00	0.00	0.00
38	0.00	0.00	0.00	87	0.00	0.00	0.00
39	6.30	8.29	12.50	88	0.00	9.40	9.38
40	95.39	77.29	101.76	89	0.00	0.00	0.00

(Table 6). Continued.

Node ID	RNC (%)	EDCS (%)	DRL (%)	Node ID	RNC (%)	EDCS (%)	DRL (%)
41	63.37	78.67	81.78	90	0.00	0.00	0.00
42	0.00	0.00	0.00	91	0.00	0.00	0.00
43	132.14	141.12	139.03	92	0.00	0.00	0.00
44	23.36	16.06	16.84	93	0.00	0.00	0.00
45	0.00	0.00	0.00	94	0.00	0.00	0.00
46	19.16	15.57	9.31	95	0.00	0.00	0.00
47	0.00	0.00	0.00	96	0.00	0.00	0.00
48	10.06	6.36	21.05	97	67.46	63.95	75.58
average	27.34%	28.43%	31.67%				

scenarios. However, it exhibits relative vulnerability under the PSA scenario ($f_c = 0.80$). This stems from the fact that the incapacitation of sensor nodes induces severe situational awareness deficits; relying solely on topological degree centrality is insufficient to fully compensate for this profound functional loss.

The DRL strategy (Figure **12d**) demonstrates unparalleled adaptive reconfiguration capabilities. Driven by intelligent resource scheduling and a many-to-one collaborative mechanism, DRL sustains elevated system capabilities across all attack paradigms, universally deferring the critical failure points to . Crucially, the variance bands of the degradation curves under the DRL strategy undergo a pronounced narrowing, serving as a testament to the strategy's enhanced stability and predictability. This resilience is fundamentally attributed to DRL's capacity to dynamically recalibrate reconfiguration priorities based on real-time network states, thereby facilitating the rapid restoration of the "Sensor-Decision-Impact" closed loop.

The comprehensive ANOC comparison depicted in Figure **12e** further corroborates these analytical findings. From the perspective of pure logical computation, the ANOC values yielded by the DRL strategy attain the theoretical zenith across all scenarios (e.g., peaking at 1.40 under the PIA scenario). However, it is imperative to emphasize that this superlative performance of DRL represents a theoretical upper bound, achieved essentially by disregarding physical costs. As empirically validated by the cross-mechanism analysis in Section 5.3, such aggressive global search protocols rapidly deplete node energy reserves and precipitate massive spatial maneuvering latencies. Consequently, in real-world combat environments, DRL is highly susceptible to the perilous trap of being "theoretically superior but practically impotent" (high scores, low capability).

In stark contrast, the EDCS strategy proposed in this study, while rigorously adhering to stringent physical boundaries, still achieves ANOC values equivalent to 85%–92% of DRL's theoretical upper bound (e.g., 0.73 versus 0.99 in the RA scenario). This compellingly demonstrates that, within the realm of engineering practice, EDCS stands as the**,** EDCS, and DRL strategies.

5.6. Micro-mechanism Analysis: Node Contribution and System Emergent Properties

To profoundly unveil the underlying contribution mechanisms through which different reconfiguration strategies enhance the performance of the Combat System of Systems (CSoS), this section selects the Preferential Sensor Attack (PSA) scenario to conduct a quantitative evaluation of the coordinated nodes under the RNC, EDCS, and DRL strategies. The node contribution degree, R_{v_i} , is defined as the relative rate of change in the SoS effectiveness following the removal/addition of a specific collaborative node. The calculation formula is formulated as follows:

$$R_{v_i} = \frac{\Gamma(G) - \Gamma(G \setminus v_i)}{\Gamma(G)} \times 100\% \tag{6}$$

Here, $\Gamma(G)$ denotes the overall operational capability of the reconfigured network. This metric reflects the criticality of an individual node in maintaining or enhancing the operational loops of the So. As indicated in Table **6**, the contribution degrees of certain nodes significantly exceed 100%, peaking at an astonishing 238.90%. This phenomenon directly validates the emergent effects engendered by collaborative reconfiguration. Upon the removal of a critical node, even if the reconfiguration strategy has

executed resource reallocation, the magnitude of system performance degradation still drastically surpasses the proportional capability of the node itself. This signifies that under the collaborative reconfiguration mechanism, the synergy among nodes generates a non-linear, super-additive gain (i.e., the "1+1>2" paradigm). Specifically, critical nodes not only contribute to their intrinsic operational capabilities but also act as multipliers, amplifying the effectiveness of peripheral nodes through collaborative mechanisms such as resource sharing and task coordination.

The node contribution analysis reveals, at a microscopic level, three core mechanisms through which collaborative reconfiguration strategies bolster system robustness:

(1) Resource Redundancy and Dynamic Reallocation: Following the failure of certain nodes, surviving nodes can partially compensate for the lost functionalities by activating standby capabilities and absorbing reconfigured resources. Consequently, the proportional decline in overall system performance is distinctly less severe than the proportional reduction in the physical number of nodes.

(2) Adaptive Topological Optimization: Collaborative reconfiguration alters not only individual node capabilities but also implicitly optimizes the functional topology of the network via resource flows, thereby funneling greater structural and functional support to nodes situated on critical paths.

(3) Task Load Rebalancing: Upon the removal of inefficient nodes, their original task loads are dynamically reallocated to high-efficiency nodes. Counterintuitively, this can elevate the overall task execution efficiency, directly elucidating the phenomenon where certain nodes exhibit a 0% contribution degree.

In summary, the node contribution analysis not only empirically validates the emergent properties of collaborative reconfiguration strategies but also uncovers the intrinsic mechanisms of robustness enhancement at the node level. This provides profound, microscopic theoretical scaffolding for the resilient design of UAV swarm combat Systems of Systems.

6. CONCLUSION

Targeting the critical theoretical deficiency where traditional robustness evaluations of UAV swarm CSoS in complex adversarial environments are severely divorced from physical constraints, this paper constructs a dynamic resilience evaluation and collaborative reconfiguration framework that integrates spatial distance, energy depletion, and temporal dimensions. Transcending the limitations of traditional pure topological connectivity metrics (ANC), which systematically overestimate network survivability, this study innovatively proposes the Time-aware Cumulative Normalized Operational Capability (T-ANOC) metric. This metric achieves high-fidelity quantification of latency penalties driven by geographical distance and reconfiguration time expenditure, accomplishing an essential paradigm shift in robustness evaluation–from "structural persistence" to "mission effectiveness accessibility." Quantitative analyses grounded in large-scale statistical simulations have revealed three profound mechanisms of system evolution:

(1) Non-linear Decoupling of Effectiveness and Topology: The collapse rate of the CSoS operational effectiveness significantly outpaces the disintegration of its physical topology. In particular, the destruction of decision hubs (e.g., the PDA scenario) is highly prone to triggering a deep vulnerability characterized by "structural survival alongside functional paralysis," unequivocally proving the lagging nature of traditional static metrics in evaluating modern kill webs.

(2) The Trade-off Between Reconfiguration Efficacy and Physical Costs: While Deep Reinforcement Learning (DRL) can improve short-term effectiveness recovery under some attack scenarios, it is more sensitive to energy depletion and reconfiguration latency. By contrast, the physics-aware Energy-Distance Collaborative Strategy (EDCS) better balances energy, latency, and effectiveness. In the reported setting, EDCS reduces energy consumption by 45% and end-to-end latency by 35%, indicating stronger engineering practicality for sustained recovery.

(3) Quantitative Substantiation of Reconfiguration Emergence: Microscopic node contribution analysis (with peak contributions reaching 238.9%) mechanistically confirms the non-linear, super-additive gains stimulated by heterogeneous functional reorganization, providing rigorous quantitative evidence for the self-organizing emergent properties of kill webs.

In summary, the physics-aware collaborative reconfiguration framework and the T-ANOC metric proposed in this paper provide an analytical basis for studying adaptive UAV swarm resilience under coupled physical, logical, and temporal constraints. Nevertheless, the present study still adopts two simplifying assumptions, namely strict binary node failure and centralized full-state knowledge during reconfiguration. In addition, the current evidence is obtained from mission-logic-constrained synthetic datasets generated via repeated Monte Carlo simulation rather than from flight-test or operational swarm records. Future research will therefore extend the framework toward continuous performance degradation, delayed/noisy state perception, and distributed or partially observed reconfiguration mechanisms under dynamic electromagnetic interference and time-varying communication blind zones, and will further validate the method using higher-fidelity digital twins, hardware-in-the-loop experiments, and, where available, mission-rehearsal or field data. Further comparative validation against additional single-factor heuristics, matching/assignment-based baselines, and other constrained recovery policies would strengthen the breadth of evaluation and therefore remains an important direction for future work. These extensions are expected to improve the realism of autonomous adaptation in denied environments. Although this hierarchical comparison against ANC and ANOC provides an internal benchmark-based validation path for T-ANOC, direct calibration with real-world flight-test logs or public operational datasets remains unavailable, largely because open data rarely contain topology evolution, spatial maneuvering, energy states, attack traces, and reconfiguration timing simultaneously.

REFERENCES

[1] Liu W, Pan Z, Han W, Su X, Yu D, Wan B. Construction of kill webs with heterogeneous UAV swarms in dynamic contested environments. Complex Intell Syst 2025; 11(1): 8. https://doi.org/10.1007/s40747-024-01644-4

[2] Bai T, Wang D. Cooperative trajectory optimization for unmanned aerial vehicles in a combat environment. Sci China Inf Sci 2018; 62(1). https://doi.org/10.1007/s11432-018-9537-1

[3] Wang H, Deng Y, Yoo S, Lin Y. Exploring robust features for improving adversarial robustness. IEEE Trans Cybern 2024; 54(9): 5141–5151. https://doi.org/10.1109/tcyb.2024.3380437

[4] Tushar W, Saha TK, Yuen C, Smith D, Poor HV. Peer-to-peer trading in electricity networks: an overview. IEEE Trans Smart Grid 2020; 11(4): 3185-3200. https://doi.org/10.1109/tsg.2020.2969657

[5] Li Y, Chen Z, Yin Y, Peeta S. Deployment of roadside units to overcome connectivity gap in transportation networks with mixed traffic. Transp Res Part C Emerging Technol 2020; 111: 496-512. https://doi.org/10.1016/j.trc.2020.01.001

[6] Shojaeinasab A, *et al.* Intelligent manufacturing execution systems: A systematic review. Journal of Manufacturing Systems 2022; 62: 503-522. https://doi.org/10.1016/j.jmsy.2022.01.004

[7] Lv C, Yuan Z, Si S, Duan D. Robustness of scale-free networks with dynamical behavior against multi-node perturbation. Chaos Solitons Fractals 152: 111420. https://doi.org/10.1016/j.chaos.2021.111420

[8] Deng Y, Wang Z, Xiao Y, Shen X, Kurths J, Wu J. Spatial network disintegration based on spatial coverage. Reliab Eng Syst Saf 2025; 253: 110525. https://doi.org/10.1016/j.ress.2024.110525

[9] Gonçalves P, Sobral J, Ferreira LA. Unmanned aerial vehicle safety assessment modelling through petri Nets. Reliability Engineering & System Safety 2017; 167: 383-393. https://doi.org/10.1016/j.ress.2017.06.021

[10] Artime O, *et al.* Robustness and resilience of complex networks. Nat Rev Phys 6(2): 114-131. https://doi.org/10.1038/s42254-023-00676-y

[11] Liu Y, Wang X, Su Z, Xiao Y, Wang Z. Efficient Edge Immunization Strategies for Diffusion Containment in Social Networks. IEEE Transactions on Dependable and Secure Computing 2025; pp. 1-17. https://doi.org/10.1109/tdsc.2025.3629028

[12] Chen P, Qi M, Yan L, Duan X. Diffusion capacity analysis of complex network based on the cluster distribution. Chaos Solitons Fractals 2024; 178: 114329. https://doi.org/10.1016/j.chaos.2023.114329

[13] Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ. Mitigation of malicious attacks on networks. Proc Natl Acad Sci USA 2011; 108(10): 3838-3841. https://doi.org/10.1073/pnas.1009440108

[14] Wang Y, Tao J, Zhang X, Bai G, Zhang Y. Mission-oriented capability evaluation for combat network based on operation loops. Def Technol 2024; 42: 156-175. https://doi.org/10.1016/j.dt.2024.07.002

[15] Song Z, Zhu J, Chen K. Robustness analysis of smart manufacturing systems against resource failures: a two-layered network perspective. Reliab Eng Syst Saf 2025; 253: 110595. https://doi.org/10.1016/j.ress.2024.110595

[16] Hao Y, Jia L, Zio E, Wang Y, He Z. A multi-objective optimization model for identifying groups of critical elements in a high-speed train. Reliab Eng Syst Saf 2023; 235: 109220. https://doi.org/10.1016/j.ress.2023.109220

[17] Cao X-B, Hong C, Du W-B, Zhang J. Improving the network robustness against cascading failures by adding links. *Chaos Solitons Fractals* 57: 35-40. https://doi.org/10.1016/j.chaos.2013.08.007

[18] Gao S, Zhang S, Chen X. Effects of adding edges on the consensus convergence rate of weighted directed chain networks. IEEE Trans Autom Control 2025; pp. 1-8. https://doi.org/10.1109/tac.2025.3527603

[19] Lou Y, Wang L, Chen G. Enhancing controllability robustness of q-snapback networks through redirecting edges. Research 2019; 2019: 7857534. https://doi.org/10.34133/2019/7857534

[20] Li Y, Zhang Z, He Z, Sun Q. A Heuristic Task Allocation Method Based on Overlapping Coalition Formation Game for Heterogeneous UAVs. IEEE Internet of Things Journal 2024; 11(17): 28945-28959 https://doi.org/10.1109/jiot.2024.3406336

[21] Zhang C, Zhou W, Qin W, Tang W. A novel UAV path planning approach: heuristic crossing search and rescue optimization algorithm. Expert Syst Appl 2023; 215: 119243. https://doi.org/10.1016/j.eswa.2022.119243

[22] Oubbati OS, Lakas A, Guizani M. Multiagent deep reinforcement learning for wireless-powered UAV networks. IEEE Internet Things J 2022; 9(17): 16044-16059. https://doi.org/10.1109/jiot.2022.3,2024150616

[23] Yang B, *et al.* Jellyfish search algorithm based optimal thermoelectric generation array reconfiguration under non-uniform temperature distribution condition. Renewable Energy 2023; 204: 197-217. https://doi.org/10.1016/j.renene.2022.12.067

[24] Ning G, Xu R, Xiong C, Li M, Li J, Yang K. RSR-SESoS: a robust space resilience enhancement framework in spatial equipment system-of-systems. Expert Syst Appl 2025; 285: 127966. https://doi.org/10.1016/j.eswa.2025.127966

[25] Wang Y, *et al.* Aviation armament system-of-systems modeling and identification method of vulnerable nodes based on interdependent network, Chinese Journal of Aeronautics. Chinese Journal of Aeronautics 37: 358-372. https://doi.org/10.1016/j.cja.2024.07.040

[26] Morone F, Makse HA. Influence maximization in complex networks through optimal percolation. Nature 2015; 524(7563): 65-68. https://doi.org/10.1038/nature14604

[27] Gu W, Yang C, Li L, Hou J, Radicchi F. Deep-learning-aided dismantling of interdependent networks. Nat Mach Intell 2025; 7(8): pp. 1266-1277. https://doi.org/10.1038/s42256-025-01070-2

[28] Saleu RGM, Deroussi L, Feillet D, Grangeon N, Quilliot A. The parallel drone scheduling problem with multiple drones and vehicles. Eur J Oper Res 300(2): 571-589. https://doi.org/10.1016/j.ejor.2021.08.014

[29] Ibrahim M, Hashmi US, Nabeel M, Imran A, Ekin S. Embracing complexity: agent-based modeling for HetNets design and optimization via concurrent reinforcement learning algorithms. IEEE Trans Netw Service Manag 18(4): 4042-4062. https://doi.org/10.1109/tnsm.2021.3121282

[30] Wang Z, Fan J, Jiang G-P, Cao J, Xiao M, Alsaedi A. Consensus in nonlinear multi-agent systems with nonidentical nodes and sampled-data control. Sci China Inf Sci 2018; 61(12). https://doi.org/10.1007/s11432-018-9441-4

https://doi.org/10.65904/3083-3450.2026.02.03