Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p27824-cd

An Improved Resilience Evaluation Method for Hierarchical Networked Command and Control System

Zhang Tianwen

National Key Laboratory of Equipment State Sensing and Smart Support, College of Intelligence Science and Technology, National University of Defense Technology, China. E-mail: zhangtianwen.edu@nudt.edu.cn

Bai Guanghan*

National Key Laboratory of Equipment State Sensing and Smart Support, College of Intelligence Science and Technology, National University of Defense Technology, China. E-mail: baiguanghan@nudt.edu.cn

Zhang Mengmeng

National Key Laboratory of Information Systems Engineering, National University of Defense Technology, China. E-mail: 18670381635@163.com

Wang Yang

National Key Laboratory of Equipment State Sensing and Smart Support, College of Intelligence Science and Technology, National University of Defense Technology, China. E-mail: wangyang@nudt.edu.cn

Tao Junyong

National Key Laboratory of Equipment State Sensing and Smart Support, College of Intelligence Science and Technology, National University of Defense Technology, China. E-mail: taojunyong@nudt.edu.cn

Command and control networks play a vital and often decisive role in military operations. Operating in dynamic and uncertain environment, they are exposed to enemy disturbances which may lead to performance degradation, making it crucial to enhance their resilience. Resilience modeling and evaluation are essential to reflect the ability of networked command and control system to maintain reliable and safe operation after actively resisting disturbances, adjusting and recovering. Previous resilience studies mainly focus on command and control network based on functional heterogeneity and its functional chain calculation methods. However, the command and control nodes with different hierarchies involved in reality have rarely been considered. To address this issue, this study proposes an improved resilience evaluation method for hierarchical command and control systems. Firstly, a hierarchical network model for the command and control system is developed, in which a new functional chain search algorithm considering hierarchical heterogeneity is proposed to reflect mission capability. Then, a hierarchy-adapted resilience evaluation method is proposed, including the hierarchy-aware performance metric and its corresponding resilience process model. The proposed method considers both absolute time scales and performance variation process balancing stability, in which different strategy schemes can be compared by distinguishing the resilience of different systems. A case study is given to demonstrate and verify the proposed methods. The proposed method is more realistic and conducive to guiding the operation and maintenance management of networked command and control system.

Keywords: hierarchical command and control system, networked modeling, hierarchy-adapted resilience evaluation, resilience metric, resilience process.

1. Introduction

With the deep integration of intelligent platforms, distributed sensing and communication networks, and intelligent decision-making algorithms in military operations and emergency response, command and control (C2) systems are rapidly evolving into networked complex systems composed of functional units, such as intelligence acquisition, information processing, decision making, and mission execution, together with their supporting links (Turki et al., 2023). For instance, large-scale and long-cycle joint air operations emphasize the effective support of networked C2

systems to functional coupling and linkage aggregation (Zhong et al., 2025). C2 networks can accelerate the transmission and fusion of information to deliver real-time and accurate intelligence and directives, which play a vital and often decisive role in military operations. (Gomes et al., 2024).

However, operating in dynamic and uncertain environment, networked C2 systems are exposed to multi-source disturbances, including random failures, "soft" attacks and "hard" strikes, which may influence reliable and safe operation of a mission (Chen and Zhu, 2019). Therefore, they must be able to withstand disruptions and rapidly recover after them. Resilience, as an extension of reliability, measures the ability of a system to cope with disturbances and recover from them, capturing the full process from degradation to recovery in networked C2 systems (Bai et al., 2020). Incorporating resilience as a metric into capability evaluation helps support decision-making for optimized system design and operations and maintenance management (Masoud and Enrico, 2025).

The concept of resilience originated from the work of Holling, who first proposed "ecosystem resilience" to characterize an ability to absorb disturbances or maintain equilibrium when facing changes of external environment (Holling, 1973). Since then, resilience has attracted considerable attention from researchers in various disciplines, including military science (Goerger et al., 2014). It has been further refined and extended into an important system attribute that complements traditional and emerging metrics in engineering systems, including reliability and robustness, by emphasizing behaviors after disturbances (Geng and Liu, 2025). Therefore, resilience modeling and evaluation are essential to reflect the ability of networked C2 system to maintain reliable and safe operation after resisting disturbances, adjusting and recovering under disrupted.

As a starting point for resilience evaluation, developing an effective model to evaluate the stability of C2 systems under both normal conditions and disturbances remains challenging. Complex network approach provides a viable path for modeling and performance definition consistent with mission mechanisms, enabling resilience evaluation to yield interpretable and reusable engineering insights (Gomes et al., 2024). Modeling C2 systems using this approach typically relies on their logical and physical topologies (Xia et al., 2022; Zheng and Liu, 2023). Mission-oriented structures, such as functional chains, have also been further incorporated to characterize performance (Zhong et al., 2025). Chen et al. [2024] abstracted information flows according to sensing, C2, and strike nodes under an interdependent network framework, highlighting their similarity to kill chains (Han et al., 2023). However, real C2 organizations typically exhibit pronounced hierarchical characteristics (Chen et al., 2025). Current studies mainly focus on C2 network based on functional heterogeneity and its functional chain calculation methods, treating C2 nodes as a single homogeneous layer. This makes it difficult to refine how heterogeneity across C2 hierarchies affects mission, especially in scenarios involving multi-level participation and the coexistence of cross-hierarchy and step-by-step command.

Resilience evaluation typically starts by defining performance metrics that represents mission capability, and then uses a resilience curve to describe its time evolution under disturbance and recovery. Resilience metrics are subsequently computed using ratio, area, or phase-decomposition approaches to capture the curve shape and recovery speed (Bruneau et al., 2003; Zobel, 2011; Henry and Ramirez, 2012; Nan and Sansavini, 2017). The choice of performance metrics is critical. The number of functional chains and its time-varying profile can intuitively reflect resilience. But the roles of C2 nodes at different levels should be differentiated for hierarchical systems, so that metrics capture both mission links and hierarchical heterogeneity, which is more realistic.

Building on general resilience frameworks, research on resilience evaluation for networked C2 systems has developed a range of methods, from decomposition of tolerance, flexibility, and capacity (Pflanz and Levis, 2012) to the process-oriented metrics that explicitly characterize disruption, degradation, and recovery (Alderson et al., 2020; Noran, 2023). Zhang et al. (2021) characterized multiple disruptions under sustained confrontation. For an interdependent C2 network subject to cascading failures, Zhao et al. (2025) measured resilience by the proportion of

remaining available nodes. From an engineering-practice perspective, evaluation methods are summarized into two categories, namely parameter-based and model-based approaches (Qiu et al., 2025). Zhong et al. (2025) decomposed resilience into robustness, adaptive, and responsiveness, and aggregated observable parameters to obtain an overall metric, providing a system-level view. However, resilience is quantified mainly by ratio-type measures defined on a relative time scale. Under different absolute time scales or node backup conditions, different systems may yield identical resilience values, in which metrics cannot distinguish resilience differences of different systems.

This work proposes an improved resilience evaluation method suitable for hierarchical C2 systems. Firstly, a hierarchical networked modeling method for the C2 system is proposed, in which a new functional chain search algorithm considering hierarchical heterogeneity is provided to reflect mission capability with an illustrative example. Based on this, a hierarchy-adapted resilience evaluation is conducted, including performance metrics and resilience process model. An improved resilience method considering absolute time scales and performance variation process balancing stability is proposed.

The remainder of this paper is organized as follows. Section 2 introduces the hierarchical network modelling approach. Section 3 presents the improved resilience evaluation method. Section 4 provides a case study and comparative analysis, and Section 5 concludes the paper and outlines future work.

2. Modeling of Hierarchical Networked C2 System

The proposed modeling method of hierarchical networked C2 System consists in two main parts: A hierarchical network model for the system and a new functional chain search algorithm considering hierarchical heterogeneity to reflect mission capability.

2.1. *Network Model*

A functional chain is a closed-loop task pattern oriented to a given class of targets. Elements along the chain are mutually dependent and operate in sequence based on a pre-planned architecture, thereby producing effect on targets. The number of functional chains reflects the amount of information links among functional modules that can be selected to form a complete operational mission process.A functional chain is built upon a C2 network. According to operational mission requirements, it is formed by information edges of different types among functional modules in the networked C2 system. It is a heterogeneous network with different nodes and edges. In practice, heterogeneous nodes also have hierarchical attributes.

Using a two-state directed network, the structure of the C2 system is represented by a directed graph $G = (V, E) = \left(V_{\mathcal{H}_i}, E\right)$, where $\mathcal{H}$ is the functional attribute of the node set V. Typically, intelligence collection and information processing are considered to be bound together, i.e., deployed at the same site or location. Therefore, intelligence acquisition and processing are treated as one type of node. Accordingly, node types $V_{\mathcal{H}_i} \in \{V_{I_i}, V_{C_i}, V_{A_i}\}, i = 1,2, \dots, N_{V_{\mathcal{H}}}$, are intelligence acquisition and processing nodes V_I, C2 and decision nodes V_C, and mission execution nodes V_A, respectively.

The number of nodes is $N = N_{V_I} + N_{V_C} + N_{V_A}$. In addition, for C2 and decision nodes, there exist hierarchy-constraint characteristics across different tasks and different nodes. C2 and decision nodes with the hierarchy attribute $\mathcal{L}$ is expressed as $V_C^{\mathcal{L}(i)}, i = 0,1, \dots, \ell$. $\mathcal{L} = 0$ denotes the highest command level, and other levels decrease sequentially. The edge set is $E = \{\left(V_{\mathcal{H}_i}, V_{\mathcal{H}_j}\right)\}$, the number of which is $|E| = \left|\left(V_{\mathcal{H}_i}, V_{\mathcal{H}_j}\right)\right|, i, j = 1,2, \dots, N_{V_{\mathcal{H}}}, i \neq j$.

A functional chain consists of V_I, V_C and V_A. A typical simple functional chain can be expressed as $V_I \rightarrow V_C \rightarrow V_A$ (Zhong et al., 2025). This paper extends the simple chain to incorporate functional chains with hierarchy constraints. According to actual C2 situation analysis and information flow portfolios, the interactions between nodes and edges are intricate, which encompasses intelligence-to-execution linkages and hierarchical command flows including hierarchical, cross-hierarchy and same-hierarchy relationships as illustrated in Fig. 1.

To facilitate the computation functional chains, this paper adopts an adjacency

representation to describe the network structure of C2 system: $L = \{v_1 : u_1, v_2 : u_2, \cdots v_n : u_n\}$, where u_i denotes the neighbor-node set of a given node v_i . This representation also indicates that information can flow from a node to its neighbors.

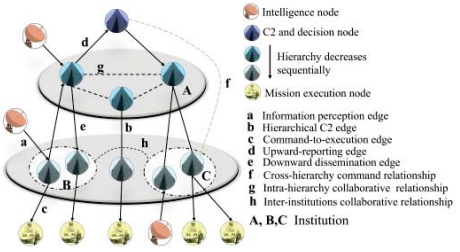

Fig. 1. Network model structure diagram.

2.2. *Functional Chain Search Algorithm*

Based on hierarchical network model, functional chain construction satisfies three assumptions.

1) The chain starts from a node with reconnaissance capability and ends at a node with execution capability. Intermediate nodes must possess C2 capability. Consistent with the simple functional chains, the allowed edges are $E_{V_I V_C}$ and $E_{V_C V_A}$.

2) For nodes with C2 and decision-making capability, there are two cases: upward-reporting and downward dissemination. Downward dissemination must follow the direction from higher-level nodes to lower-level nodes, while any preceding upward-reporting follows the opposite order. Then it is assumed that the information flow contains only one turning point to simplify the representation of the hierarchical C2 process.

3) For both downward dissemination and upward-reporting, this paper assumes two cases: step-by-step command and cross-level command. That is, C2 nodes at different hierarchies do not need to be connected strictly via level-by-level recursion when forming a functional chain. In addition, this study assumes that coordination among nodes within the same hierarchy is not considered, in order to focus on inter-hierarchy relationships. During search, edges are divided into two types: upward-reporting edges $E^{\uparrow}_{V_C^{\mathcal{L}(i)} V_C^{\mathcal{L}(j)}}$ with $\mathcal{L}(j) > \mathcal{L}(i)$ and downward dissemination edges $E^{\downarrow}_{V_C^{\mathcal{L}(i)} V_C^{\mathcal{L}(j)}}$ with $\mathcal{L}(i) > \mathcal{L}(j)$.

The algorithm for searching functional chains considering hierarchical heterogeneity is provided below.

Input: A hierarchical C2 network $G(V, E)$.

Output: The number of functional chains ξ.

Step 1. Initialize parameters. Load the adjacency of the network, including node sets (V_I, V_C, V_A) and edge sets $\left(E_{V_I V_C}, E_{V_C V_C}, E_{V_C V_A}\right)$. Assign a level $\mathcal{L}$ to each $V_C^{\mathcal{L}(c)} \in V_C$. Denote the numbers of nodes by N_{V_I}, N_{V_C}, and N_{V_A}. Proceed to Step 2.

Step 2. Set cursors and initialize $i \in [1, \ldots, N_{V_I}]$, $j \in [1, \ldots, N_{V_C}]$, and $k \in [1, \ldots, N_{V_A}]$ to 1. Proceed to Step 3.

Step 3. Take V_{I_i} as the starting node and select one or more reachable V_{C_j}. For each starting V_{C_j}, perform traversal over the V_C segment under hierarchical constraints, i.e., proceed to Step 4.

Step 4. Perform a two-state depth-first search (DFS) over the V_C nodes. Define a state variable mode $\in \{UP, DOWN\}$. Given adjacency relations $E^{\uparrow}_{V_C^{\mathcal{L}(j)} V_C^{\mathcal{L}(q)}}$ and $E^{\downarrow}_{V_C^{\mathcal{L}(j)} V_C^{\mathcal{L}(q)}}$, set the counting exit condition for either *UP* or *DOWN*. If there exists a path between V_{C_j} and V_{A_k}, then each V_{A_k} forms one functional chain and the count increases by 1. The following recursion rules are defined as followed.

Step 4.1. If mode $= UP$, the search may report upward along $V_C^{\mathcal{L}(q)} \in E^{\uparrow}_{V_C^{\mathcal{L}(j)} V_C^{\mathcal{L}(q)}}$ while remaining in *UP* state. Alternatively, a turning point can be formed at the current step. Search moves downward along any $V_C^{\mathcal{L}(r)} \in E^{\downarrow}_{V_C^{\mathcal{L}(j)} V_C^{\mathcal{L}(r)}}$, switches into the *DOWN* state, and recurses. After that, upward-reporting is no longer allowed.

Step 4.2. If mode $= DOWN$, the search is only allowed to disseminate downward along any $V_C^{\mathcal{L}(q)} \in E^{\downarrow}_{V_C^{\mathcal{L}(j)} V_C^{\mathcal{L}(q)}}$.

Step 5. Advance the outer loop by setting $i = i + 1$ and return to Step 3. Combining all links found from Step 3 to Step 5 yields the total number of hierarchical functional chains ξ.

2.3. *An illustrative example*

Taking the joint strike against a surface target illustrated as an illustrative example, the modeling and dynamic process of a hierarchical C2 network

is illustrated, and the abstracted network is shown in Fig. 2(a). Specifically, the operational target outside the hierarchical C2 network is denoted by v_{12}. The intelligence agencies are denoted by v_6 and v_{11}. v_5 is the execution node. The remaining nodes are used to represent C2 nodes, namely different organizations involved in the operation. Since v_6 transmits information via the information pool (IP), it is assumed to be connected to corresponding nodes. The structure is assumed to represent the architecture prior to disruption.

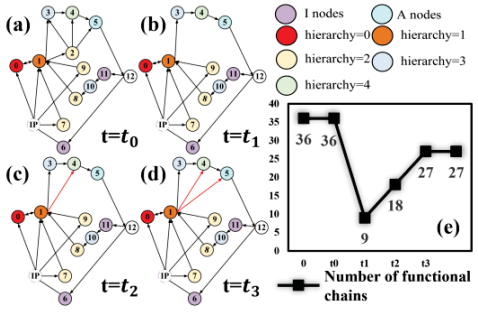

Fig. 2. Schematic diagram of the illustrative example.

The structure after v_2 is disrupted at time t_1 is illustrated in Fig. 2(b). The structure after link reconfiguration at time t_2 is illustrated in Fig. 2(c) with the addition of a connection from v_1 to v_4. The structure after link reconfiguration at time t_3 is illustrated in Fig. 2(d) with the addition of a connection from v_1 to v_5.

Since the capability of the networked C2 system is positively correlated with the number of functional chains, the performance curve of functional chains over time can be used to characterize the ability of the system to maintain its performance under external disturbances and to recover it through corresponding recovery strategies as shown in Fig. 2(e).

3. Improved Resilience Evaluation Method

This section proposes a hierarchy-adapted resilience evaluation method consists in three main parts: Hierarchy-aware performance metric, resilience process model and an improved resilience method.

3.1. *Hierarchy-Aware Performance Metric*

In a hierarchical C2 system, lower-level C2 nodes are typically more numerous and densely distributed, whereas higher-level decision nodes are fewer in number but play a critical role in key missions. If the time-varying curve of functional chains number is used as the performance metric, it often overestimates the contribution of functional chains composed only of lower-level C2 nodes to resilience, and thus fails to capture the performance loss caused by failures of high-level nodes. For example, after a top-level C2 node fails, the number of chains formed by lower-level nodes may still remain large, making the curve appear to decrease slowly. However, most missions are in fact unreachable.

Define the highest decision node level reached by each functional chain ξ as $\pi = min_{V_{C_j} \epsilon \xi \cap V_C} \mathcal{L}\left(V_{C_j}\right)$. Let $\xi_\pi(t)$ denote the number of functional chains at time t whose highest reached level is π, where $\pi = 0,1,2,\dots,\ell$. Introduce level weights $\omega_\pi (0 < \omega_\pi < 1, \omega_0 > \omega_1 > \cdots > \omega_l)$. The level-weighted functional chain value $X^\omega(t)$ is then defined as follows.

$$X^\omega(t) = \sum_{\pi=1}^{\ell} \omega_\pi \, \xi_\pi(t). \tag{1}$$

Based on the above formulation, effective chains that account for actual C2 hierarchy is considered instead of treating all functional chains indiscriminately. Meanwhile, to highlight the retained coverage degree of high-level nodes, the relative coverage within the level range up to π is defined as

$$RC_\pi(t) = \frac{\sum_{j \le \pi} \xi_j(t)}{\sum_{j \le \pi} \xi_j(t_s)}, \tag{2}$$

where $RC_\pi(t_s) = 1$. A coverage correction factor $C_{rank}(t) = \sum_{\pi=1}^{\ell} \omega_\pi \, RC_\pi(t)$. Accordingly, the hierarchy-aware performance metric $P(t)$ is defined as follows.

$$P(t) = \sum_{\pi=1}^{\ell} {\omega_\pi}^2 \cdot \frac{\xi_\pi(t) \sum_{j \le \pi} \xi_j(t)}{\sum_{j \le \pi} \xi_j(t_s)}. \tag{3}$$

3.2. *Resilience Process Model*

Disruptions provide a major motivation for triggering the resilience process of a hierarchical C2 network. Node removal is regarded as a consequence of disruptions. Typical disruption modes generally include the random attack and deliberate attack. In random attacks, a fraction δ of nodes in the network fail and are removed at

random, mainly to be compared with subsequent deliberate attacks.

Deliberate attacks adopt critical-node identification to disrupt systems efficiently. Nodes are ranked in descending order of importance according to a given criterion, and the top δ fraction of high-importance nodes are preferentially attacked and failed. Common importance metrics include degree, betweenness centrality, and PageRank centrality. This study uses PageRank centrality (Brin and Page, 1998) to quantify importance.

After an attack, the network can restore performance and achieve resilience improvement through recovery strategies. Recovery strategies include node backup and reconnection among surviving nodes to reconstruct the network. This study adopts node backup and constructs the resilience process to verify the effectiveness of the proposed resilience method while costs are not considered. Node backup means that, once a functional module fails, it is replaced by its backup module. In practice, node backup is usually reserved for critical nodes, which is also consistent with the characteristics of C2 nodes.

A well-designed resilience metric should capture the essence of system resilience and ensure that the quantified resilience is consistent with its related concepts. To illustrate the construction of a resilience metric, a hypothetical example is provided as shown in Fig. 3.

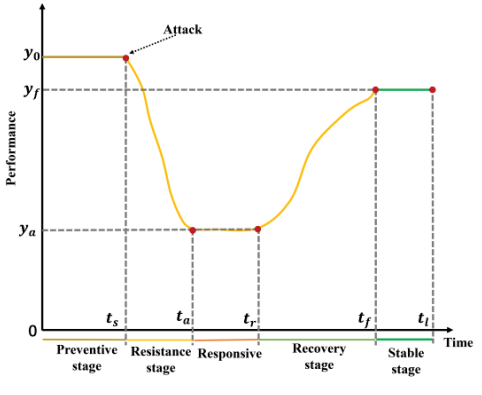

Fig. 3. Resilience process curve.

Assume that the system operates at a normal performance level y_0 before the attack event occurs. When the attack occurs at time t_s, performance begins to degrade until it reaches the minimum level y_a. The time interval from t_a to t_r is regarded as the responsive phase. After t_r, the system starts to recover until it reaches a stable level y_f. Likewise, the interval from t_r to t_f is regarded as the recovery phase. Therefore, performance is characterized from the onset of the attack event through the completion of recovery and stabilization.

3.3. *Improved Resilience Method*

Considering the agility characteristics of C2 systems, Zhong et al. (2025) performs quantitative analysis and aggregation for resilience by using metrics corresponding to three elements as shown in Table 1. This method derives resilience values from performance ratios across different phases on a relative time scale. It can only be used to compare alternative strategy schemes, but it cannot distinguish the resilience levels of different systems, which constitutes a limitation.

Table 1. Existing resilience methods.

Metric Elements	Performance Ratio	Duration Ratio	Aggregation Relationship
Robustness	$\frac{P(t_s)-P(t_a)}{P(t_s)}$	$\frac{t_a-t_s}{t_f-t_s}$	$\frac{1}{DR \cdot DV}$
Adaptive	$\frac{P(t_f)-P(t_r)}{P(t_s)}$	$\frac{t_f-t_r}{t_f-t_s}$	$RR/_{RV}$
Responsiveness	\	$\frac{t_f-t_r}{t_f-t_s}$	$1/_{AV}$
Resilience	$F^{robus} \times F^{adapt} \times F^{respo}$		

To address this issue, this work proposes an improved resilience evaluation method that incorporates an absolute time scale and accounts for both the performance evolution process and stability.

1) Robustness. The proportion of mission performance loss during the resistance stage $[t_s, t_a]$ is defined as follows.

$$\acute{DR} = \frac{1}{t_a - t_s}\int_{t_s}^{t_a}\left(1-\frac{P(t)}{P(t_s)}\right)dt. \quad (4)$$

Corresponding duration factor is $\acute{DV} = t_a - t_s/t_f - t_s$. Accordingly, the re-calculated robustness metric is given as

$$R^{robus} = \frac{1}{max\{\varepsilon, \acute{DR} \cdot \acute{DV}\}}, \quad (5)$$

where ε is a small positive constant introduced to prevent the denominator from becoming 0.

2) Recovery. The proportion of mission performance gain relative to the remaining performance during the recovery stage $[t_r, t_f]$ is defined as follows.

$$\acute{RR} = \frac{1}{t_f - t_r}\int_{t_r}^{t_f}\frac{P(t) - P(t_r)}{P(t_s)}dt. \quad (6)$$

Corresponding duration factor is $\acute{RV} = t_f - t_r/t_f - t_s$. Accordingly, the re-calculated recovery indicator is given as follows.

$$R^{adapt} = \frac{\acute{RR}}{max\{\varepsilon, \acute{RV}\}}. \quad (7)$$

3) Responsiveness. To account for agility, the duration factor of the responsive stage $[t_a, t_r]$ is defined as $\acute{AV} = t_r - t_a/t_f - t_s$. Meanwhile, to capture volatility, a mild variance-based penalty is applied to performance over $[t_a, t_f]$.

$$\emptyset_{var} = \frac{\overline{\frac{P(t)}{P(t_s)}}}{\sigma_{\frac{P(t)}{P(t_s)}}}. \quad (8)$$

$$R^{respo} = \frac{1}{max\{\varepsilon, \acute{AV}\}}\cdot \emptyset_{var}. \quad (9)$$

The value of ϕ_{var} can be adjusted according to the specific fluctuation characteristics of the performance curve. When volatility is not considered, one can set $\phi_{\text{var}} = 1$. Likewise, the rate of change can be distinguished via AV', since it depends on the time point t_r. On this basis, the overall resilience value is computed as:

$$R = R^{robus} \times R^{adapt} \times R^{respo}. \quad (10)$$

4. Case Study

Without loss of generality, the effectiveness of the proposed methods is demonstrated through generated abstract networks as a numerical example in the case study. The number of network nodes is set to $N = 32$, specified as $N_{V_I} = 4$, $N_{V_C} = 14$, and $N_{V_A} = 14$. V_C nodes are divided into three levels, with $N_{V_C^{L(0)}} = 2$, $N_{V_C^{L(1)}} = 4$, and $N_{V_C^{L(2)}} = 8$. Combined with the edge-connection relationships and the connection probability (Zhang et al., 2024), the connection probabilities for each type of edge are set to 0.5 for $V_I \to V_C$, 0.2 for $V_C \to V_C$, and 0.5 for $V_C \to V_A$, to generate the network. In addition, results are averaged over 500 independent experiments.

The hierarchical functional-chain calculation method proposed in this paper is compared with typical functional chains (Zhong et al., 2025) and kill chain calculation method with C2 nodes (Li et al., 2019). Baseline methods compute chains by processing node and edge relationships on the generated hierarchical network structure according to their respective procedures. Among them, kill chain calculation method does not distinguish node hierarchies and explicitly accounts for coordination among C2 nodes. For an effective comparison, given the designed number of hierarchies, we restrict kill chains searched containing no more than five C2 and decision nodes. The statistical results of the functional-chain calculations are shown in Fig. 4 and Table. 2.

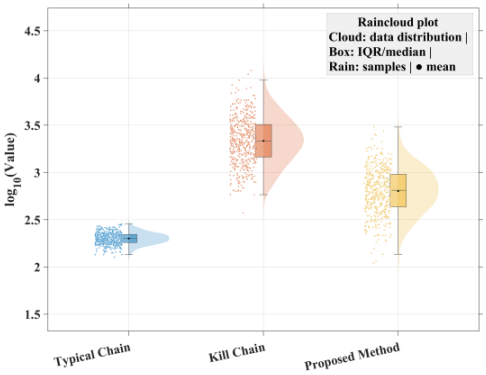

Fig. 4. Comparison of functional-chain.

Table 2. Comparison results of functional-chain search algorithms.

Functional Chain	Typical Chain	Kill Chain	Proposed Method
Mean	202	2536.9	733.47
Std	28.65	1537.51	410.53
Median	200	2163	646.5
Q1	181	1458	433.75
Q3	221	3209.5	955
IQR	40	1751.5	521.25

Results show that, in a large-scale C2 network with hierarchical factors, calculating only typical functional chains cannot sufficiently search the links that actually exist. Because the traditional kill chain does not differentiate the relationships among nodes at different hierarchy levels, it tends to include numerous cross-level combinations that lack real connectivity, leading to substantial redundancy in chain computation. In contrast, the

proposed method preserves heterogeneity among actual links while effectively suppressing redundant searches. Compared with the traditional kill chain, it reduces redundancy by approximately 71% in terms of the mean and 70% in terms of the median, yielding results that better reflect realistic conditions.

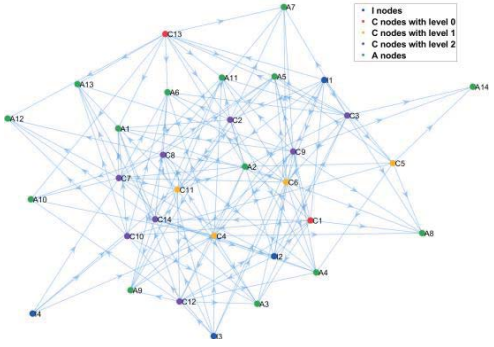

Fig. 5. Illustrative hierarchical C2 network.

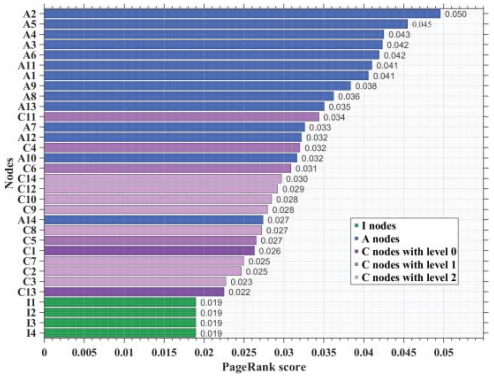

Fig. 6. Node importance distribution.

The network structure aggregated over multiple trials based on the connection probability is shown in Fig. 5. According to the resilience process above, the resilience simulation starts at $t_0 = 0$ and ends at $t_e = 800$ on this network. The attack begins at $t_s = 150$ with attack intensity $\delta = 1/8$. Strategies of the random attack and deliberate attack remain unchanged. However, the interval between successive nodes being attacked and failed is 40 steps for random attacks, whereas the interval is 50 steps for deliberate attacks. After a series of damage assessments and backup preparations, backup-node recovery starts 100 steps after the attack is completed, and recovery is carried out in the order of attacks. The backup recovery interval for each node is 60 steps, and the repair completion time is t_f. It is assumed that the network structure and performance are updated after the completion of each attack and recovery, and $\emptyset_{var} = 1$. The number of backups equals the number of failed nodes, $n = |\delta N| = 4$.Under this resilience process, C2 and decision nodes are attacked and failed via both random attacks and deliberate attacks based on PageRank centrality. Importance distributions of different nodes are shown in Fig. 6. So $C11$, $C4$, $C6$ and $C14$ are attacked under the deliberate attack, while $C10$, $C13$, $C9$ and $C1$ are attacked under the random attack.

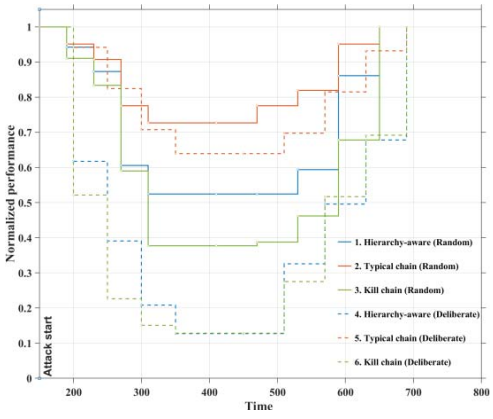

Fig. 7. Comparison of resilience curves.

Table 3. Resilience Results of different methods.

Example	Proposed Method	Baseline
1	53.917	71.517
2	119.16	71.517
3	37.813	71.517
4	26.311	57.214
5	90.879	57.214
6	22.759	57.214

Based on comparative analysis above, we introduce the hierarchy-aware performance metric proposed in Section 3.1 and compare time-varying performance curve with those using metrics of typical functional chains and kill chains. Resulting curves are shown in Fig. 7. Table 3 shows resilience evaluation results using the proposed resilience method and baseline (Zhong et al., 2025).

As can be seen, the existing method yields an identical resilience of 71.517 under random attacks

and 57.214 under deliberate attacks, thereby capturing the higher effectiveness of deliberate attacks. However, for different systems, resilience values remain the same. In contrast, resilience curves clearly indicate that failures of different nodes affect network performance in markedly different ways. For hierarchical C2 network, performance degrades rapidly and resilience is lower. Obviously, under recovery strategies with backup resources used to repair all failed nodes, existing method cannot distinguish resilience across different systems for the same attack strategy on a consistent time scale. Consequently, it has inherent limitations and fails to reflect differences throughout the full process of disturbance absorption and recovery.

By comparison, the improved resilience method not only captures the effectiveness of deliberate attacks but also shows that, under the same attack strategy, the resilience of systems that explicitly differentiate node hierarchies is lower than that of typical functional-chain systems. Moreover, it reveals a key artifact of the kill chain approach. It exhibits a pronounced resilience drop when a failed node disconnects all of its incident edges because it includes redundant links that do not exist in reality. Overall, the proposed resilience method can distinguish between different attack strategies while effectively characterizing the heterogeneous performance dynamics across different systems under attacks.

5. Conclusions and Future Work

In this study, we proposed a hierarchical networked modeling method and an improved resilience evaluation method for hierarchical C2 systems. Case study shows that functional chains searched through the proposed network model can reflect command and control nodes with heterogeneous hierarchy compared with existing network modeling methods. Results obtained from the improved resilience method can effectively distinguish the resilience levels of different systems with the same strategy under node backup conditions compared with the existing resilience method. The proposed method is more realistic and conducive to guiding the operation and maintenance management of networked C2 system, which is also considered extendable to non-military applications, such as emergency management systems involving organizations at different hierarchies.

Future work will focus on refining the proposed resilience method by expanding validation beyond backup condition considered in this work. We will investigate a broader set of disruption and recovery strategies, including both node and edge attack models as well as recovery in order to systematically evaluate resilience. Additionally, the current hierarchical network is assumed to be fixed and static. we will extend the framework using multi-agent approaches to represent dynamic C2 process, thereby enabling performance tracking and resilience evaluation under varying structures and rules.

Acknowledgement

This work was supported by National Natural Science Foundation of China (Grant 72271242).

References

Al Lelah, T., G. Theodorakopoulos, P. Reinecke, A. Javed, and E. Anthi. (2023). Abuse of cloud-based and public legitimate services as command-and-control (C&C) infrastructure: A systematic literature review. *Journal of Cybersecurity and Privacy* 3(3), 558-590.

Alderson, D. L., D. Eisenberg, A. Ganin, M. Kitsak, and I. Linkov. (2020). Operational Resilience of Command and Control Systems to Maintain Multilayered Network Functionality in Response to Large-Scale Disruptive Events. Technical report, Naval Postgraduate School.

Bai, G., Y. Li, Y. Fang, Y. A. Zhang, and J. Tao. (2020). Network approach for resilience evaluation of a UAV swarm by considering communication limits. *Reliability Engineering & System Safety* 193, 106602.

Brin, S., & Page, L. (1998). The anatomy of a large-scale hypertextual web search engine. *Computer networks and ISDN systems* 30(1-7), 107-117.

Bruneau, M., S. E. Chang, R. T. Eguchi, et al. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* 19(4), 733-752.

Chen, B., G. Pang, Z. Xiang, et al. (2024). Modeling dual-layer interdependent command and control networks for integrated reconnaissance-strike and OODA-loop capabilities. *IEEE Transactions on Network Science and Engineering* 11(6), 5744-5759.

Chen, B., L. Sun, Y. Chen, X. Gao, Z. Xiang, Y. Zhang, and S. Chen. (2025). Edge Cascading Failure Model for Command and Control Networks: Integrating Edge Importance and Edge Hierarchy.

IEEE Transactions on Automation Science and Engineering 22, 22715-22728.

Chen, J., and Q. Zhu. (2019). A games-in-games approach to mosaic command and control design of dynamic network-of-networks for secure and resilient multi-domain operations. In *Sensors and Systems for Space Applications XII*, pp. 189-195. SPIE.

Geng, S., and S. Liu. (2025). An agent-based framework for resilience analysis of service networks. *Reliability Engineering & System Safety* 253, 110523.

Goerger, S., A. Madni, and O. Eslinger. (2014). Engineered resilient systems: A DoD perspective. *Procedia Computer Science* 28, 865-872.

Gomes, J. E. C., R. R. Ehlert, R. M. Boesche, et al. (2024). Surveying emerging network approaches for military command and control systems. *ACM Computing Surveys* 56(6), 1-38.

Han, Q., B. Pang, S. Li, N. Li, P. S. Guo, C. L. Fan, and W. M. Li. (2023). Evaluation method and optimization strategies of resilience for air & space defense system of systems based on kill network theory and improved self-information quantity. *Defence Technology* 21, 219-239.

Henry, D., and J. E. Ramirez-Marquez. (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering & System Safety* 99, 114-122.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics* 4, 1-23.

Li, J., Ge, B., Zhao, D., Jiang, J., & Zhao, Q. (2019). Meta-path-based weapon-target recommendation in heterogeneous combat network. *IEEE Systems Journal*, 13(4), 4433-4441.

Nan, C., and G. Sansavini. (2017). A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety* 157, 35-53.

Naseri, M., and E. Zio. (2025). A modelling and computational framework for the assessment of the supply resilience of gas transmission pipeline networks. In *Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference*, pp. 782-789. Research Publishing, Singapore.

Noran, O. (2023). A synergistic approach towards agile and resilient command and control and collaborative networks. In L. M. Camarinha-Matos and F. Fonseca (Eds.), *Collaborative Networks in the Era of Artificial Intelligence*, pp. 815-826. Cham: Springer.

Pflanz, M., and A. Levis. (2012). An approach to evaluating resilience in command and control architectures. *Procedia Computer Science* 8, 141-146.

Qiu, X., L. Li, Z. Dong, and D. Liu. (2025). A dynamic evaluation and analysis framework of C2 system resilience based on complex network. In *2025 IEEE 8th Information Technology and Mechatronics Engineering Conference*, pp. 1142-1152. IEEE.

Xia, W., T. Dong, J. Zhao, and Y. Wang. (2022). Research analysis of networked C2 system based on complex network technology. In *7th International Conference on Information Science, Computer Technology and Transportation*, pp. 1-4. VDE.

Zhang, T., Bai, G., Lv, Y., Zhang, S., & Tao, J. (2024). Performance-based cascading failure analysis of cross-domain unmanned combat system considering logistic support. *IEEE Systems Journal* 18(4), 2109-2120.

Zhang, X. (2021). A new approach to characterizing resilience of command and control systems. In *AIAA SciTech 2021 Forum*, p. 0657.

Zhao, B., M. Wang, W. Lin, and Q. Zhang. (2025). Study on the resilience of command and control networks to cascading failures based on asymmetric group dependencies. *Scientific Reports* 15(1), 29487.

Zheng, J., and D. Liu. (2023). C2 system network modeling and analysis based on bipartite graph. In *2023 IEEE International Conference on Integrated Circuits and Communication Systems*, pp. 1-5. IEEE.

Zhong, Y., Y. Zhang, J. Zhang, and L. Wan. (2025). Research on resilience measurement and optimization of networked C2 system. *Reliability Engineering & System Safety* 261, 111048.

Zobel, C. W. (2011). Representing perceived tradeoffs in defining disaster resilience. *Decision Support Systems* 50(2), 394-403.