electronics

MDPI

Article

Evaluation and Optimization of a Command and Control System Based on Complex Networks Theory

Tengda Li *, Gang Wang, Xiangke Guo, Minrui Zhao, Jiayi Liu and Chong Du

Air Defence and Antimissile School, Air Force Engineering University, Xi'an 710051, China
* Correspondence: ltd026@126.com

Abstract: With the rapid development of information technology, network-centric warfare (NCW) has become the main operational style now and even in the future, and the destruction resistance of networks has become one of the most important issues in the field. Based on the complex networks theory, the command and control (C2) network is constructed, and the topology characteristics of the network are analyzed. Aiming at the deliberate attack and random attack, the destruction resistance of C2 network is analyzed and optimized. The simulation results show that the C2 network conforms to the small-world and free-scale characteristics, and it is sensitive to deliberate attack. The strategy of low-degree edge addition can be adopted, that is, by expanding the horizontal contact between the same layer of combat entities and increasing the cross-layer contact between the different layers, the destruction resistance of C2 network can be effectively enhanced. The simulation results have a certain theoretical significance for the establishment of the C2 network and the optimization of destruction resistance of C2 network.

Keywords: complex networks theory; C2 network; topological characteristics; deliberate attack; destruction resistance

check for updates

Citation: Li, T.; Wang, G.; Guo, X.; Zhao, M.; Liu, J.; Du, C. Evaluation and Optimization of a Command and Control System Based on Complex Networks Theory. *Electronics* **2023**, *12*, 1180. https://doi.org/10.3390/electronics12051180

Academic Editor: Dimitris Kanellopoulos

Received: 2 February 2023
Revised: 21 February 2023
Accepted: 22 February 2023
Published: 28 February 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

According to the famous physicist Stephen Hawking, the 21st century is a century of complexity. The study of complex networks is part of complexity theory. Complex networks theory can be used to capture and describe the evolutionary mechanisms, evolutionary laws and overall behavior of a system with the help of graph theory and statistical physics [1–5]. In recent years, with the deepening understanding of scientists, complex networks have gradually become an interdisciplinary emerging and popular area of research. It have been successfully applied in the fields of transportation [6–9], communication networks [10–12], power systems [13,14], biological systems [15,16] and in the military [17–19].

The structure of the C2 system has undergone a transformation from platform-based to network-based, and with the rapid development of information networks, the structure of C2 system based on the idea of network-centric warfare has also evolved greatly. The idea of NCW is to achieve a common perception of the battlefield situation among the various combat entities through the networked connection to achieve maximum network potency factor through synchronization and synergy. The C2 system integrates various command and control resources and realizes information sharing and integrated application among combat elements; thus, this system is a complex network. Its overall performance is not equal to the linear sum of individual performance and has non-parsimony; therefore, it cannot be studied by the traditional reductionist approach.

The relevance of the C2 system to the complex networks theory is that, firstly, the existence of a large number of accusation, reconnaissance, strike power, and other types of nodes in the system and their complex interactions make it necessary to analyze and study them with the help of complexity science; secondly, according to the idea of NCW, the structure of the combat system is essentially a network system composed of interrelated

perception networks, decision networks, engagement networks and basic information grids; therefore, it is a natural research idea to accurately describe and analyze with the help of network theory, which provides a new perspective for the in-depth study of its internal characteristics.

The application of complex networks theory in the military field has been studied by scholars at home and abroad [20–22], mainly including the application of command and control systems, the construction of operational system models using complex networks theory, and the analysis of the performance of the system-of-systems (SoS) model. Lei Chen [23] established a combat system network model based on data from real exercises, and summarized and analyzed the static characteristics and general properties of the network; Zhu J. [24] combined the network indicators and the connotation of warfare, and analyzed the system breaking combat principle based on the perspective of complex networks; in response to the lack of in-depth research on the "cloud combat" system, L P [25] used complex networks theory to establish combat capability indicators and simulate the accusation timeliness of the system; Gang J.X. [26] focused on analyzing the advantages of hyper-network modeling for carrier formation combat systems, addressing issues such as model design, model implementation; to better study the air defense sensors, Sun Y.C. [27] established a topology model of sensor network and used artificial immune algorithm to solve the model; Wang Y.M. [28] used complex networks theory to address the structural characteristics of the accusation control network, focusing on the network destruction resistance measure based on the efficiency of the accusation link. However, the above studies mostly focus on the topology of network, and there are fewer studies related to the optimization of network robustness and vulnerability, especially for C2.

In this paper, starting from the complex networks theory, the network topology diagram of the C2 system is constructed, and the complex characteristics of the network structure are analyzed; then random attack and deliberate attack against this network are simulated, relevant evaluation indexes are selected to measure the destruction resistance of the network, and the adoption of low-degree edge addition strategy is proposed for optimization and improvement.

The main contributions of our work are as follows:

1. A detailed review is performed to analyze the current state of application of complex networks theory in various fields, especially in the military field.
2. In this paper, applying complex networks theory to C2 network provides new ideas for analyzing C2 systems.
3. The topological characteristics and destruction resistance of C2 network are analyzed using complex networks theory by combining qualitative and quantitative methods, and relevant suggestion are provided to improve the destruction resistance of the system.
4. Using relevant theories, we found that C2 network is a small-world network, which is a good basis for further investigation of network properties.

This paper is organized as follows: Section 2 establishes the network structure of the C2 based on complex networks theory; Section 3 introduces and analyzes the specific meaning of C2 network parameters; and Section 4 provides analysis of network topology characteristics and destruction resistance. Section 5 optimizes the C2 network and compares and analyzes the performance of the optimized network. Section 6 is the conclusion.

2. Model Construction

The C2 system, according to the different roles played by each unit, can be divided into early warning units, decision units, and strike units, and the above combat units are seen as nodes; the information interaction between the units is abstracted as edges, and based on complex networks theory, the C2 system can be abstracted as follows:

$$G = (V, E) \tag{1}$$

where V contains the nodes in the network and is a non-empty finite set; $E = \{e_1, e_e, \cdots, e_m\}$ is the connection relationship between nodes in the network.

The network structure can be represented in the form of an adjacency matrix $A_{n\times n} = [a_{ij}]_{n\times n}$. When node i and node j are connected to each other, $a_{ij} = 1$; otherwise, $a_{ij} = 0$.

$$a_{ij} = \begin{cases} 1 & node\ i\ is\ connected\ to\ node\ j \\ 0 & node\ i\ is\ not\ connected\ to\ node\ j \end{cases} \quad (2)$$

2.1. Node

Combining the entity composition, the operational entities are abstracted into the following three types of nodes.

Warning nodes: radar battalions belonging to warning radar tactical-level decision centers are included.

Decision nodes: battle-level decision nodes and tactical-level decision nodes are included.

Strike nodes: strike power battalions belonging to tactical-level decision centers are included.

2.2. Edge

To facilitate the information advantage, there should be a direct communication connection between the tactical level and the fire unit level; the battle-level charge node should be connected to the tactical-level node; and the information should be shared between the nodes of the same level.

If all nodes are directly connected, it will inevitably result in a complex network connectivity; therefore, a suitable complex network model is proposed to solve this problem. In order to investigate and analyze the characteristics between different network models, a total of four network models are designed based on the above node and connected edge relationships, which are shown as follows:

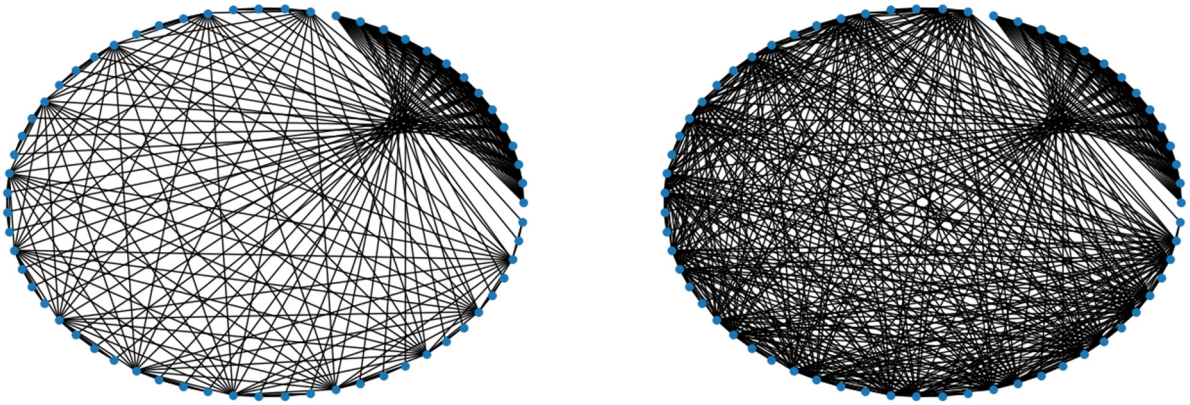
Network A: only one battalion-level node under different tactical-level decision nodes can be interconnected.

Network B: two battalion-level nodes under different tactical-level decision nodes are interconnected.

Network C: a random selection of battalion-level nodes (15 strike unit battalions and 4 radar battalions) under different tactical-level decision nodes are interconnected.

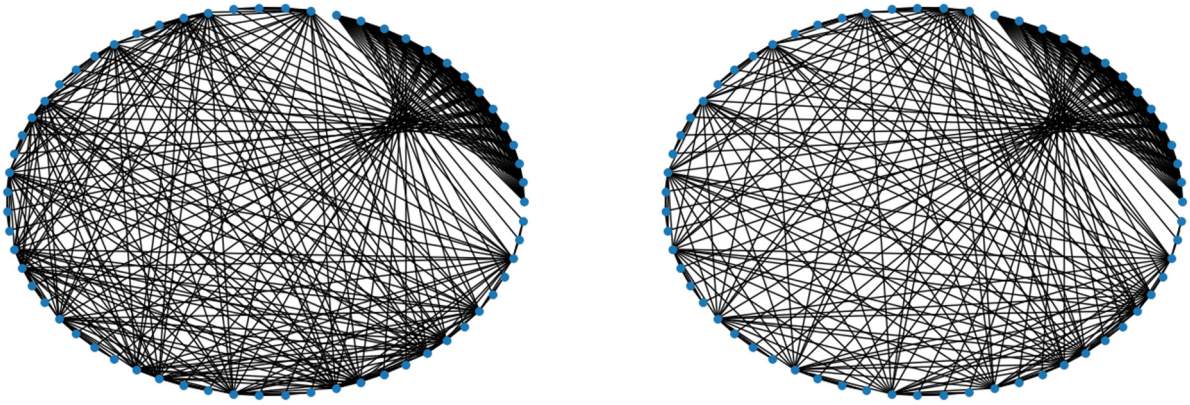
Network D: a randomly selected number of battalion-level nodes (13 strike unit battalions and 4 radar battalions) under different tactical-level decision nodes are interconnected.

The four network models created are shown in Figure 1.



(**a**) (**b**)

Figure 1. *Cont.*



(**c**) (**d**)

Figure 1. The network model of C2 system. (**a**) Network A; (**b**) Network B; (**c**) Network C; (**d**) Network D.

As can be seen from Figure 1, Network A has a simpler structure with fewer edges, while the model is more complex due to the higher number of edges in Network B, Network C, and Network D. The four networks have 287, 521, 374 and 326 connected edges, respectively.

3. Network Characteristics and Index Selection

In order to analyze the commonality and dissimilarity of the four network models, we can consider comparing the networks from multiple perspectives and dimensions, which are mainly divided into topology and destruction resistance research.

3.1. Topology Indicators

(1) The number of edges of the network

The greater the number of edges, the greater the communication between the nodes of the network, and the faster the transmission of instructions; however, at the same time, it makes the network more redundant, which makes the cost of combat much higher and places higher demands on the reliability of the network.

(2) Average node degree and degree distribution

The degree of a node is also known as the degree of association. In a complex network, the degree represents the connectivity of the node with other nodes. The higher the degree, the greater the number of nodes directly connected to a node, the better the connectivity and the corresponding information transmission capability; then, the node can be considered more important in the network, which can be expressed as:

$$D_i = \sum_{j \neq i, j=1}^{N} a_{ij} \tag{3}$$

The average degree is the average of all node degrees and can represent, to some extent, the degree to which individual nodes in the network are directly related, which can be expressed as:

$$\overline{D} = \frac{1}{n}\sum_{i=1}^{N} D_i = \frac{1}{n}\sum_{i=1}^{N}\sum_{j \neq i, j=1}^{N} a_{ij} \tag{4}$$

The degree distribution function $P(k)$ is the probability that a node is randomly selected with degree k, which can be expressed as:

$$P(k) = \frac{N_k}{N} \tag{5}$$

(3) Clustering coefficient and average clustering coefficient average path length

The clustering coefficient of the node in the network is a parameter to measure the degree of node clustering, and the larger the clustering coefficient of a node, the higher the importance of the node in the whole network. Assuming that node i is directly associated with other k nodes, while there are β edges between k nodes, the clustering coefficient C_i of the node is

$$C_i = \frac{2\beta}{k(k-1)} \tag{6}$$

The average clustering coefficient is the average of the cluster coefficients of all nodes, which can be expressed as:

$$\overline{C} = \frac{1}{n}\sum_{i=1}^{N} C_i \tag{7}$$

(4) Path length and average path length

Path length refers to the number of edges on the shortest path connecting node i and node j. The average distance of the nodes is the average of the path length between any two points. The size of this value is inversely proportional to the connectivity of the nodes in the network, which can be expressed as follows:

$$\overline{L} = \frac{2}{n(n-1)}\sum_{1\le i,j\le N} s_{ij}, \forall i, j, i \neq j \tag{8}$$

where s_{ij} is the shortest distance between node i and node j.

3.2. Destruction Resistance Analysis and Index Selection

3.2.1. Destruction Resistance Analysis

The network of C2 system is often attacked, leading to node or edge failure, making the connected network fragmented or even leading to full network damage. Destruction resistance refers to the ability of the network model to operate normally under the circumstances of changes in the operational environment and external disturbances or attacks. It reflects the stability and robustness of the system. The purpose of researching destruction resistance is to optimize the overall network structure and enhance combat effectiveness.

Two types of attacks are usually considered when studying the destruction resistance of the network, mainly random attack and deliberate attack. Random attack is an attack on any node in the network, and there is no purpose and certainty, usually mainly for non-human attacks and damage, such as equipment failure, natural disaster impact, or accidental factors, also known as network robustness analysis; deliberate attack, on the other hand, is mainly a planned and strategic attack on important nodes of the network, which is also known as the vulnerability analysis of the network.

The network attack process of the deliberate attack mode of node-degree-based attack is as follows:

Input: Nodes V of the C2 network and the boundary relationship E between each node

Output: The destruction resistance index data of the whole network.

Workflow:

Step 1 Build the network model of C2 system according to the network nodes and the boundary relationship;

Step 2 According to Formula (3), the degree of a single node is calculated and sorted;

Step 3 Delete the node with the highest degree;

Step 4 Calculate and record the indicators of the current network according to Equations (10)–(12);

Step 5 Check whether the termination conditions are met: all nodes are deleted. If yes, go to **Step6**; Otherwise, go to **Step3** to continue the iteration;

Step 6 Output network indicators. No further action is required.

Based on the existing node-degree attack, this paper proposes a real-time attack mode, that is, first delete the node with the highest degree of a node, recalculate the node degree of the current network, and then delete the node with the highest degree of the current network, and cycle until all nodes are deleted. The attack process is shown in Figure 2. Compared with the static high-node attack strategy, this attack is more aggressive, leaving the network a shorter response time. It is more conducive to the study of network destructiveness.

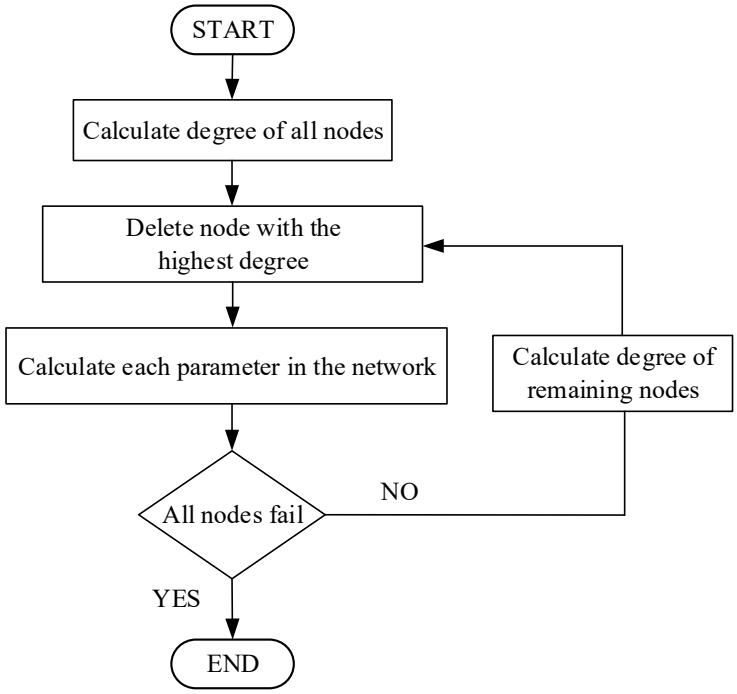


Figure 2. The process of real-time degree priority attack.

3.2.2. Destruction Resistance Index

(1) Average network efficiency

In actual combat, the enemy is likely to target key nodes. After an attack on a key node, it is critical that the connectivity of the entire network is intact, often directly determining the stability of the entire network. Average network efficiency can be used as an indicator to assess the efficiency of the network to some extent.

The network efficiency between i and j is

$$\delta_{ij} = \frac{1}{s_{ij}}, \forall i, j, i \neq j \tag{9}$$

Then the average efficiency of the whole network can be expressed as:

$$\eta = \frac{1}{n(n-1)} \sum_{i,j} \delta_{ij} = \frac{1}{n(n-1)} \sum_{i,j} \frac{1}{s_{ij}}, \forall i, j, i \neq j \tag{10}$$

The higher the efficiency of the network, the higher the connectivity reliability of the network and the higher the resistance of the network to destruction.

(2) Rate of change of network efficiency

The network efficiency will also change after an attack, and the rate of change of network efficiency can be considered an evaluation indicator. Assume that the network efficiency is η before the attack, and the number of nodes is N. After the attack, the network efficiency is η', and the number of nodes is N'. The ratio of the change in network efficiency before and after the change in the node is defined as the rate of change of network efficiency $\Delta\eta$. The larger $\Delta\eta$ indicates the higher importance of its node and the greater the impact on the overall network structure, and its expression is:

$$\Delta\eta = \frac{|\eta' - \eta|}{N - N'} \tag{11}$$

(3) Maximal connected subgraph

When a node is attacked to make the network in a non-connected state, the network will form multiple connected components, and the connected component containing the largest number of nodes is called the maximum connected subgraph. In the reliability analysis of the C2 network, the change of the maximal connected subgraph can visually reflect the topological change of the network before and after the attack.

The ratio of the number of nodes N_0 of the maximal connected subgraph to the number of nodes N of the original network is defined as the ratio of the maximal connected subgraph λ. Its expression is

$$\lambda = \frac{N_0}{N} \tag{12}$$

4. Network Topology Characteristics Analysis

From the topological diagrams of the above four network models, the network organization structure can be grasped more clearly; however, some specific features of the network need to be analyzed by calculating the relevant indicators and combining them with the corresponding military implications.

4.1. Topology Index Analysis

The main statistical characteristics of the four network models are shown in Table 1. To analyze the complex network characteristics more intuitively, two more important parameter indicators: the average clustering coefficient and the average path length are selected to draw bar graphs, as shown in Figure 3.

Table 1. Network topology characteristics.

	NET A	NET B	NET C	NET D
The number of edges	287	521	374	326
Average degree	9.11	16.54	11.87	10.35
Average clustering coefficient	0.844	0.85	0.847	0.846
Average path length	2.159	1.858	2.02	2.09

From the analysis in Table 1 and Figure 3, it can be seen that Network A has the lowest node average degree (9.11), while the average path length is the largest (2.159), indicating that the network relies on a few important nodes, the network information propagation distance is long and the network efficiency is low. Networks B, C, and D, on the other hand, have a decreasing average degree of nodes and clustering coefficient as the number of connected edges decreases, but the average path length gradually increases. The average clustering coefficients of the four networks do not differ significantly, indicating that the four types of edges do not change the closeness of the nodes to a large extent. At the same time, Network B has the largest clustering coefficient, while its average path length is the smallest, indicating that the nodes of its network are closely connected, with faster information transmission and more time-efficient actions. Overall, Network B has the

highest average degree and a greater operational cost for the whole network, yet its average path length is the smallest and the network has a higher information transfer capability. Moreover, its average clustering coefficient increases slightly compared to the other three network structure models, indicating a greater degree of internal information connectivity and information sharing and a greater degree of operational grouping in this network. Therefore, it can be concluded that as the complexity of the network increases, the combat capability of the network can be improved; at the same time, however, it also brings about an increase in the redundancy of the network, an increase in costs, and a higher demand for the security of the communication links.

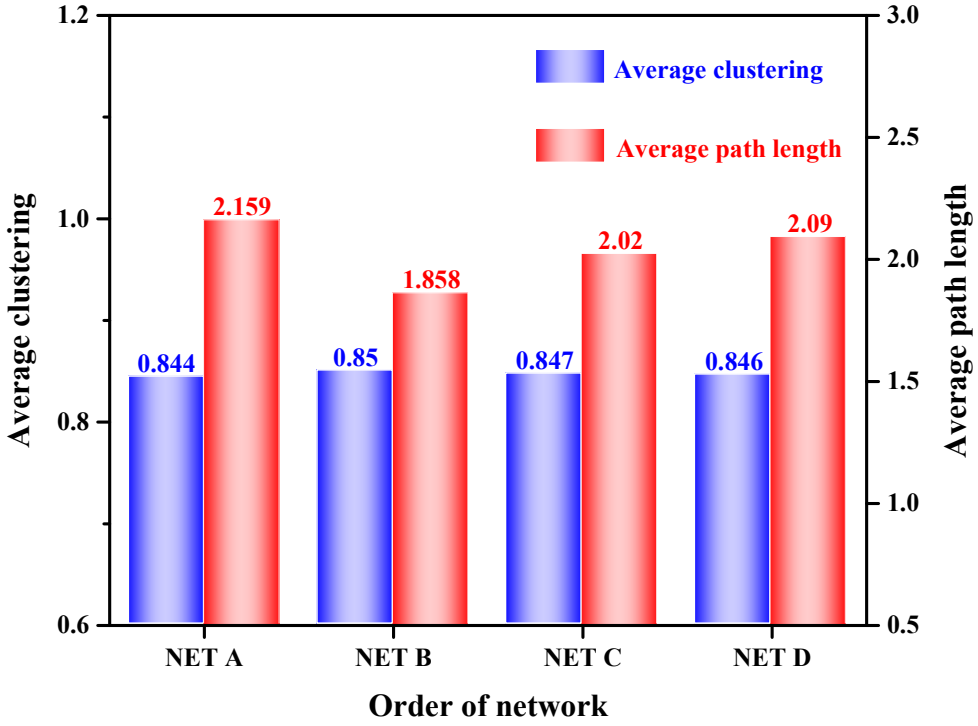


Figure 3. Average clustering coefficient and average path length.

In the C2 network, the degree of a node reflects the relational interactions between operational entities. In general, the greater the degree of a node, the more information that node needs to process and the more important its position in the network. $P(k)$ and degree distribution of the four networks are shown in Figure 4.

The degree of distribution usually has a significant impact on the performance of information dissemination in a network. Analysis of Figure 4 shows that the overall degree value of Network A is lower than the other three networks. The largest overall degree value is for Network B. The percentage of node degrees below 5 for Networks A, C, and D is 57.14%, 47.62%, and 52.38%, respectively, while only 36.51% in Network B.

Critical nodes play an important role in maintaining the function of the C2 network and can influence the efficiency, reliability, and connectivity of the entire network. Therefore, analyzing the critical nodes in the network is of great importance in terms of improving the stability of the network. In each network, the node with the largest node degree is found to be not a critical node in the intuitive sense (battle-level decision node) but 13 tactical-level decision nodes, indicating that their position in the entire network is extremely important and should be given priority protection in actual operations.

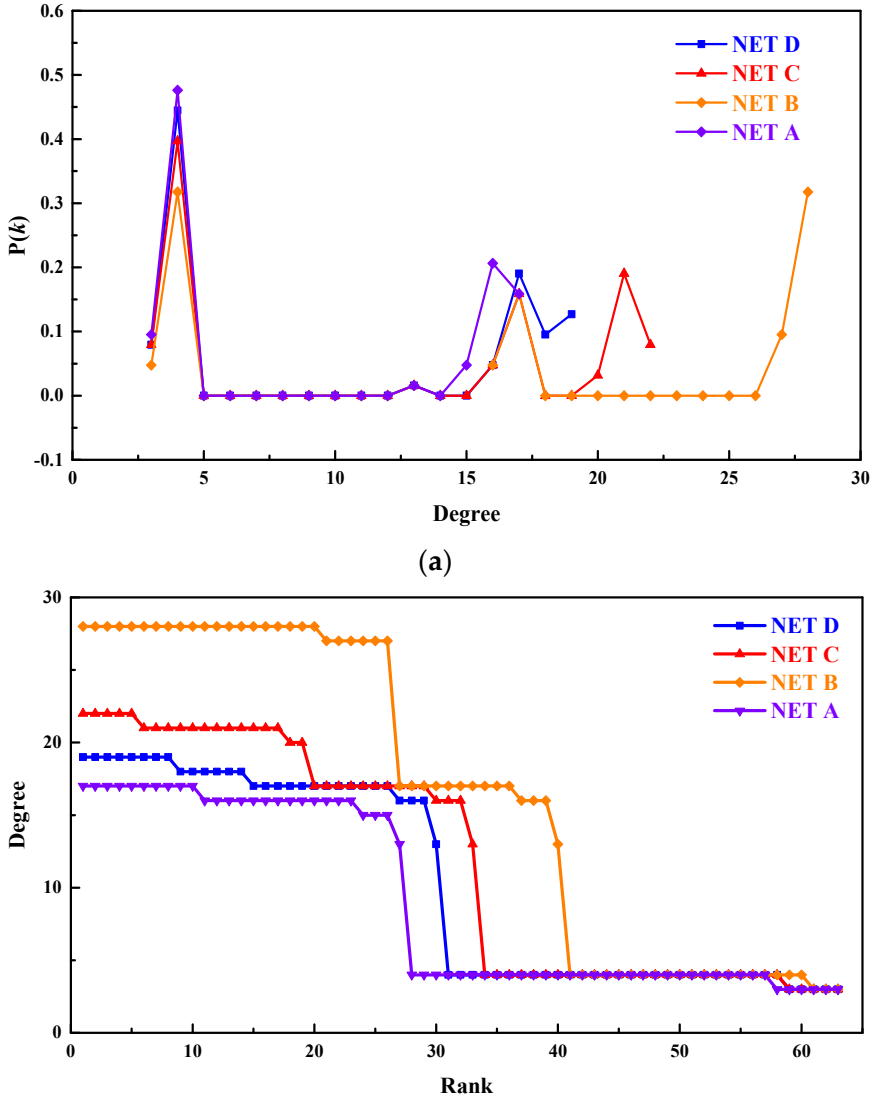


Figure 4. Degree probability distribution and degree distribution. (**a**) Degree probability distribution; (**b**) Degree distribution.

4.2. Network Type Analysis

From the above analysis, it can be seen that the four networks most likely have the small-world characteristic, as they all have larger clustering coefficient and smaller average path length. To verify the accuracy and scientific validity of the above inference, it is calculated and verified according to the determination method of small-world networks. The adjudication conditions for small-world networks are generally:

$$\begin{cases} \overline{L} \geq L_R, \overline{C} >> C_R \\ L_R = \frac{lnN}{ln\overline{D}} \\ C_R = \frac{\overline{D}}{N} \end{cases} \tag{13}$$

where $\overline{L}$ is the average path length, $\overline{C}$ is the average clustering coefficient, N is the total number of nodes, and $\overline{D}$ is the average node degree of the network. The relevant performance metrics of the four networks are shown in Table 2.

The analysis shows that the average path length and average clustering coefficient of the four networks satisfy Equation (13); thus, it can be judged that the four networks have

the small-world characteristic. Therefore most of the nodes in the four networks are not adjacent to each other, but they can reach each other quickly under the action of any other nodes and can better handle various events. The C2 network is a new type of network that lies between the random network and the regular network, providing a new perspective for studying the intrinsic characteristics of the warfare model.

Table 2. L_R and C_R metrics of four network models.

	NET A	NET B	NET C	NET D
N	63	63	63	63
$\overline{D}$	9.11	16.54	11.87	10.35
$\overline{C}$	0.844	0.85	0.847	0.846
$\overline{L}$	2.159	1.858	2.02	2.09
L_R	1.88	1.48	1.67	1.77
C_R	0.14	0.26	0.19	0.16

4.3. Network Potency Factor Analysis

This section represents the operational network as an adjacency matrix, where the maximum eigenvalue of the adjacency matrix reflects the number of loops in the network; the more loops in the network, the fewer nodes and edges the loops experience, the higher the network potency of the architecture.

Cares demonstrated the rationality of using the maximum eigenvalue of the adjacency matrix (PFE) as a network potency evaluation metric and also defined the network potency factor: CNE = PFE/N, where N is the total number of nodes in the network.

As can be seen from Table 3, Network A has a low loop structure, with only 22% of nodes participating in loops, indicating that there are few links between operational entities of different subordinate units, while nearly 40% of nodes in Network B participate in the loop structure, indicating that the horizontal links have increased, with stronger links between decision, warning and strike entities, and the number of loops in the network has increased, increasing the effectiveness of combat system synergy.

Table 3. Network potency factor of four network models.

	NET A	NET B	NET C	NET D
N	63	63	63	63
PET	14	25.33	18.53	15.81
CNE	0.22	0.40	0.29	0.25

Compared to Network A, the network potency factor of Network B, Network C, and Network D is increased by 80.93%, 32.36%, and 12.93%, respectively. All three network models can improve their network potency factor, indicating that the information transfer between each strike and radar battalion is critical and the strikes work more closely together.

4.4. Network Destruction Resistance Analysis

Random attack and deliberate attack based on real-time degree priority are used to launch attack on the network and analyze the destruction resistance of the four types of networks.

4.4.1. Network Efficiency and Rate of Change of Efficiency Analysis

By comparing the network efficiency and rate of change of efficiency to derive the impact law of using different attack methods on the network, the experimental simulation results are shown in Figures 5 and 6.

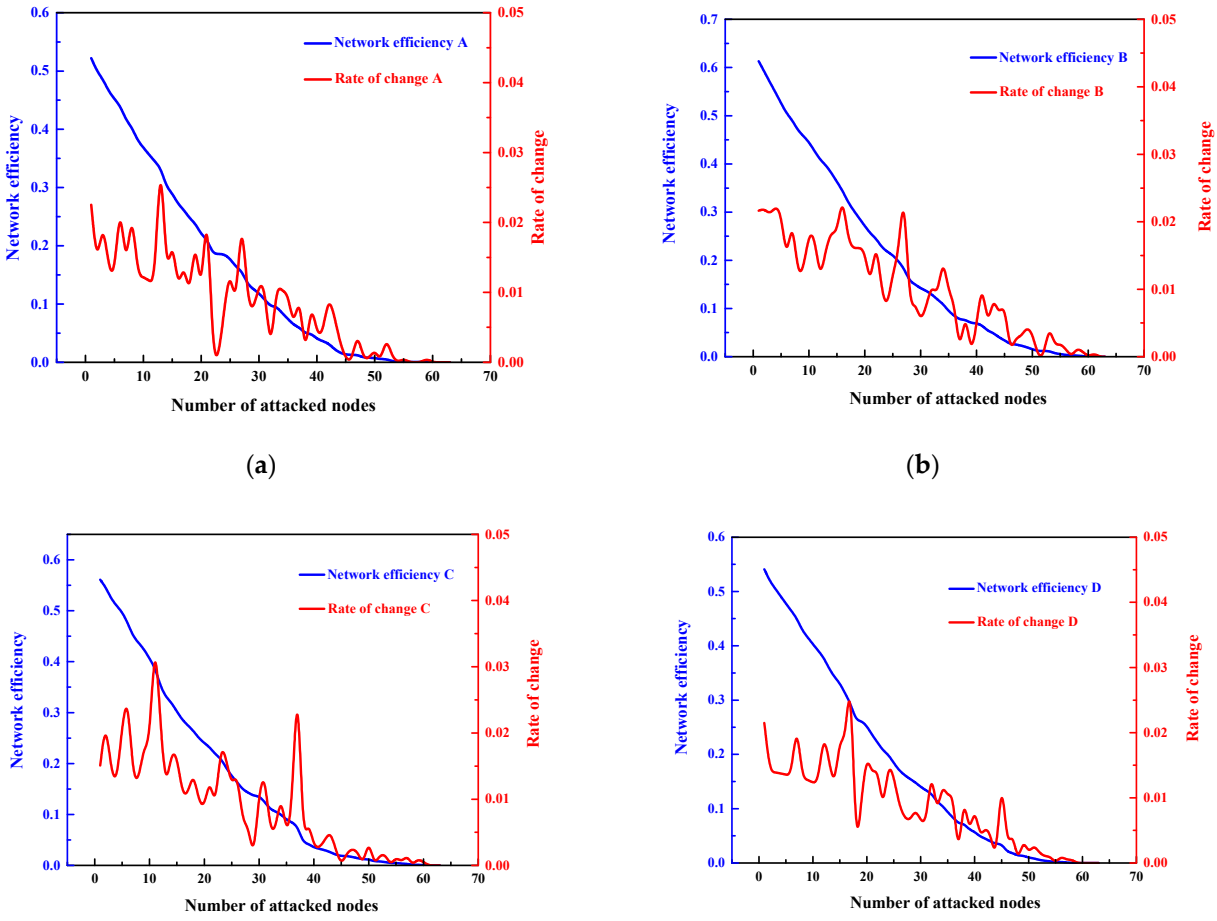


Figure 5. Graph of network efficiency and rate of change under random attack. (**a**) Network A; (**b**) Network B; (**c**) Network C; (**d**) Network D.

Figures 5 and 6 show that the network efficiency and the rate of change of network efficiency vary considerably under different attack methods.

When using the real-time degree priority attack, the network efficiency will drop sharply when the enemy is the first to launch an attack on the key nodes. This is because the real-time degree priority attack first makes the decision nodes fail, which play the role of information relay, resulting in multiple information relay and lower network efficiency. Taking the network efficiency of 0.1 as the measurement standard, when the attack mode based on real-time degree priority is adopted, the failure nodes of Network A, B, C and D reach 28.57%, 47.62%, 39.68% and 34.92%, respectively. When random attack is adopted, the number of failed nodes in Network A, B, C and D needs to reach 49.21%, 53.97%, 52.38% and 53.97%, respectively, indicating that random strategy has little influence on network efficiency.

Comparing the rate of change of network efficiency, it can be seen that some nodes in the network have a much higher impact on the network efficiency than others after failure. When random attacks are adopted, the rate of change is not stable and tends to decrease in a "step", but almost always stays below 0.02; the real-time degree priority attack, on the other hand, has a greater impact on the rate of change of network efficiency, especially in the initial stage.

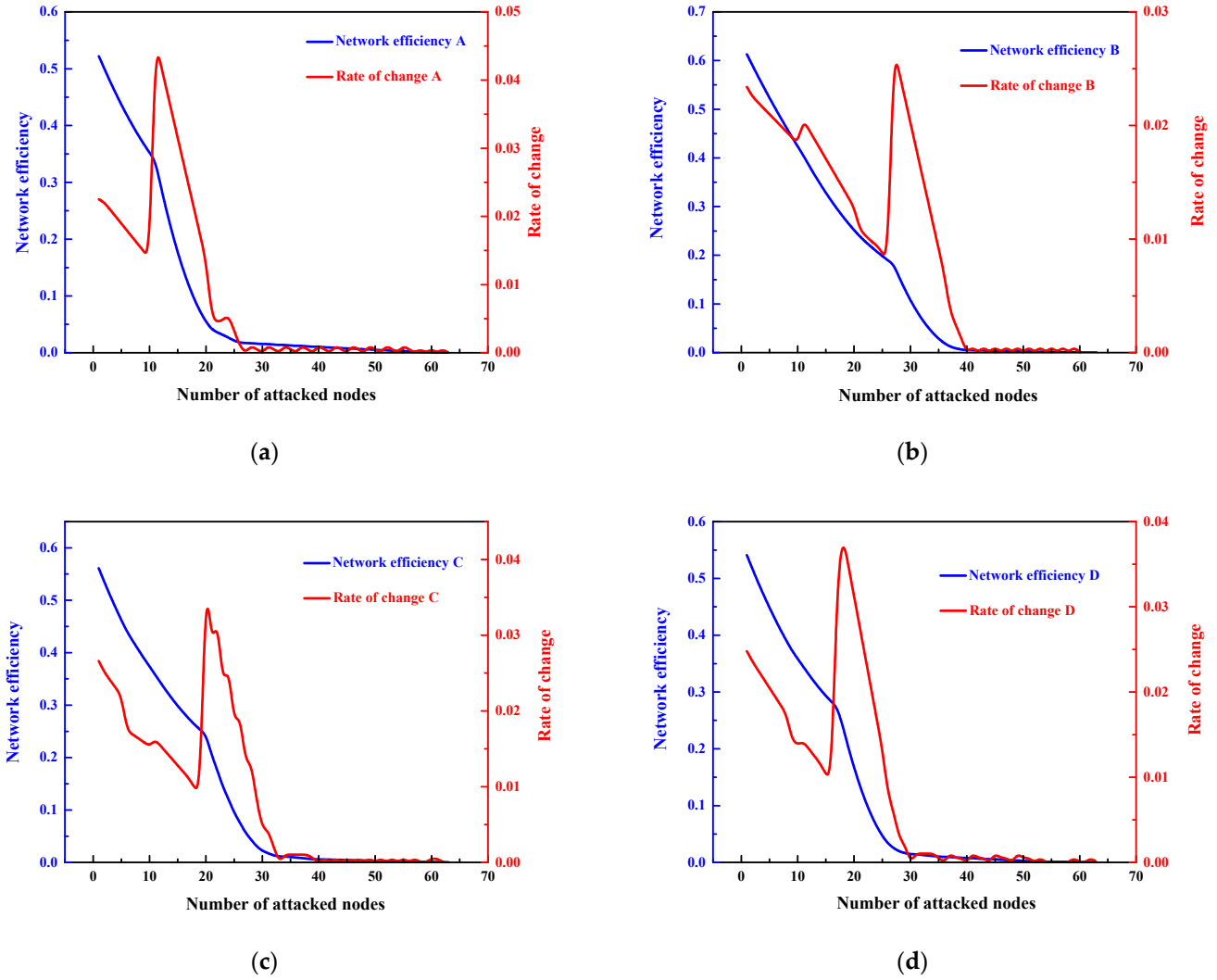


Figure 6. Graph of network efficiency and rate of change under deliberate attack. (**a**) Network A; (**b**) Network B; (**c**) Network C; (**d**) Network D.

Taking the change rate 0.02 as the measurement standard, when the real-time degree priority attack is adopted, the ratio of the change rate greater than 0.02 of Network A, B, C and D reaches 17.46%, 17.46%, 15.87% and 19.05%, respectively. When random attack is adopted, the rate of change of Network A, B, C and D is only 11.11%, 12.70%, 9.52% and 6.35%. The rate of change of deliberate attack is 57.14%, 37.50%, 66.67% and 200% higher than random attack, respectively. The greater the change rate of network efficiency, the greater the impact on the connectivity of the entire network and the greater the damage to the network. Therefore, the damage to the network caused by random attack is lower than that caused by deliberate attack, and the network has better anti-destruction performance in the face of random attack.

Therefore, the four C2 networks show scale-free characteristics, that is, they have good robustness to random attack while showing strong vulnerability to deliberate attack.

4.4.2. Network Potency Factor Analysis

By comparing the network potency factor to derive the impact law of using different attack methods on the network, the experimental simulation results are shown in Figure 7.

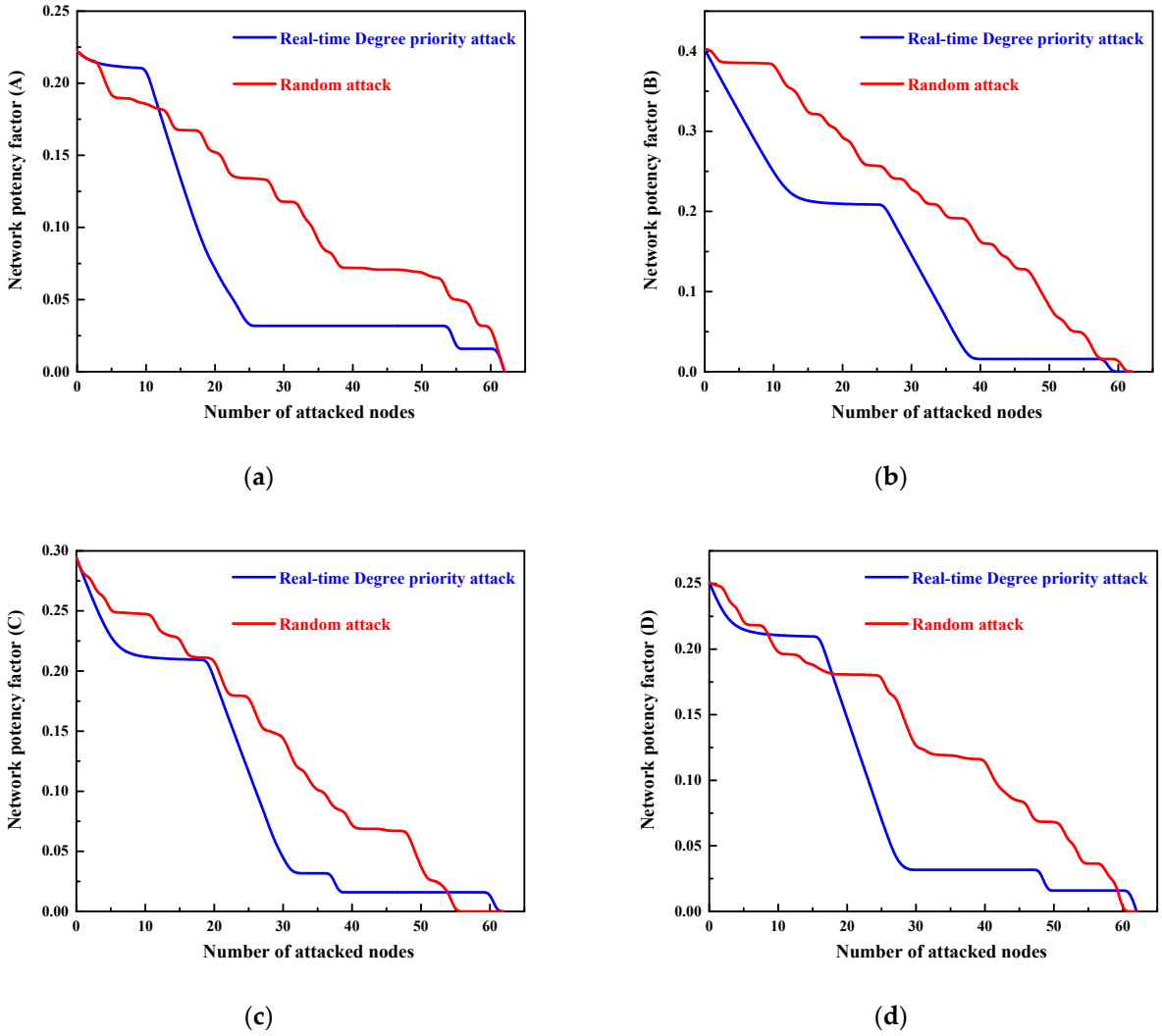


Figure 7. Graph of network potency factor under two attacks. (**a**) Network A; (**b**) Network B; (**c**) Network C; (**d**) Network D.

When random attack is adopted, the change of network potency factor is relatively stable, and the ratio of failed nodes is approximately inversely linear with the network potency factor. When the node fails, the maximum eigenvalue of the adjacency matrix becomes smaller, leading to the reduction in the network potency factor. With the increase in the number of attacked nodes, more and more nodes fail, there is no longer an edge relationship with other nodes, and the maximum eigenvalue of the adjacency matrix decreases until it drops to 0. When the real-time degree priority attack is adopted, the network potency factor drops as a step cliff, mainly because the enemy will concentrate on attacking certain types of nodes. However, after the failure of such nodes, the maximum eigenvalue of the adjacency matrix of the whole network does not change significantly; therefore, the network potency factor does not decrease significantly.

When the real-time degree priority attack is adopted, when the number of failed nodes reaches 30, the network potency factor of Network A, B, C and D is 0.032, 0.146, 0.045 and 0.032, respectively. The potency factor of the whole network has decreased by 58.71%, 63.76%, 84.82% and 87.35%. Under the same conditions, under the random attack is adopted, the network potency factor of Network A, B, C and D is 0.118, 0.225, 0.146 and 0.125, respectively, and the overall network potency factor decreases by 47.00%, 43.00%, 50.30% and 50.35%. Random attack is 73.05%, 35.28%, 69.45% and 74.51% higher than deliberate attacks, respectively.

4.4.3. Maximal Connected Subgraph Analysis

By comparing the maximal connected subgraph to derive the impact law of using different attack methods on the network, the experimental simulation results are shown in Figure 8.

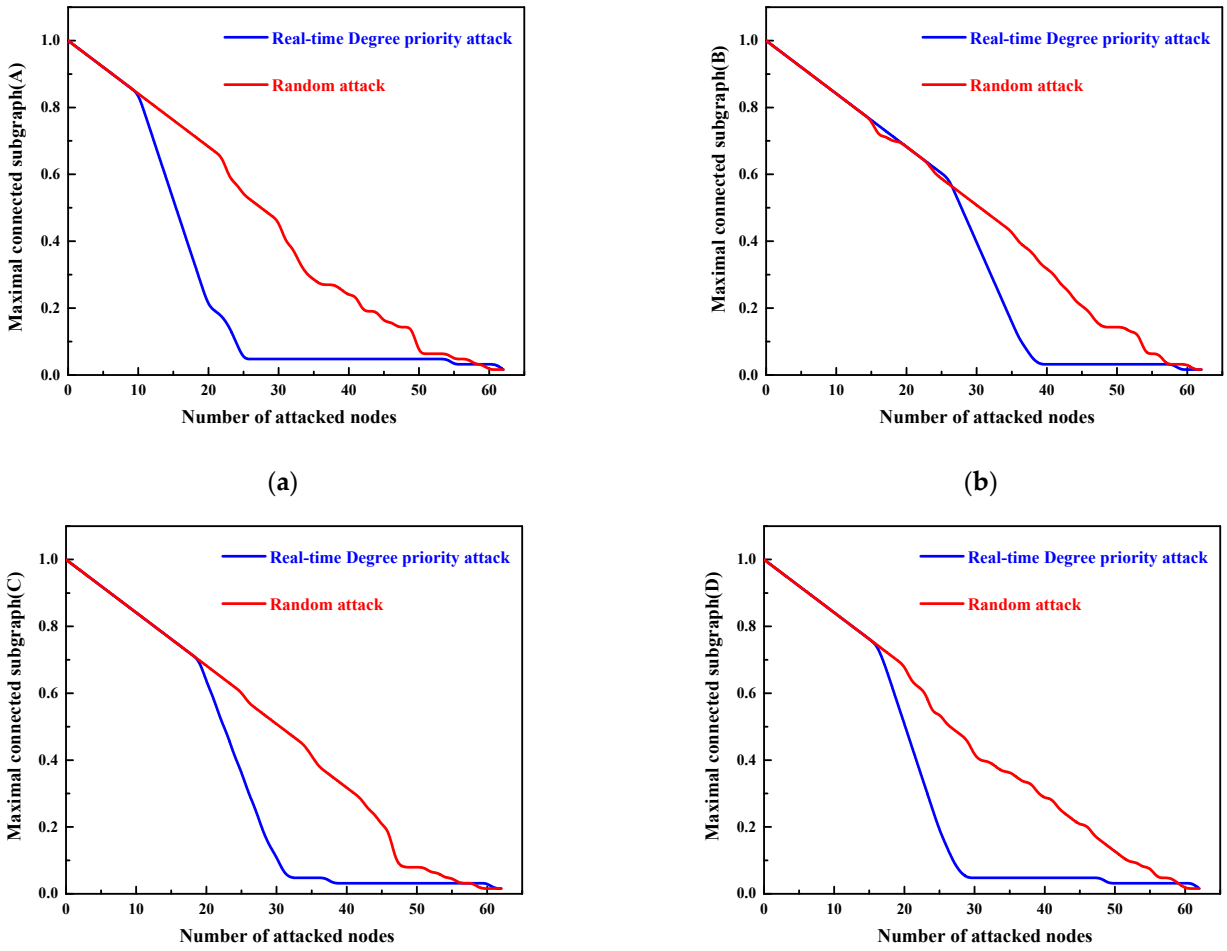


Figure 8. Graph of maximal connected subgraph under two attacks. (**a**) Network A; (**b**) Network B; (**c**) Network C; (**d**) Network D.

Take the analysis of Network A as an example: the maximal connected subgraph in the initial state is 1, and when the proportion of failed nodes is below 15%, the maximal connected subgraph decreases at almost the same rate under two attacks, at which time the maximal connected subgraph is 0.841; however, when the proportion of failed nodes is in the range of 15–40%, the maximal connected subgraph under deliberate attack decreases in a stepwise cliff, at which time the maximal connected subgraph is 0.048, and the network is basically paralyzed; thereafter, the drop slows down, and when the proportion of failed nodes reaches 80%, the network collapses; under the random attack, the whole drop is flat, showing the destruction resistance of the network. At the end of the simulation, the maximal connected subgraph indicator under both attacks becomes flat, indicating that the remaining nodes of the network are no longer interconnected, and eventually the maximum connectivity indicator becomes 0 as the attack continues.

When the real-time degree priority attack is adopted, the maximal connected subgraph drops to a lower level when the proportion of failed nodes in Network A, B, C and D reaches only 40%, 62%, 51% and 46%, respectively, and the network is basically in a paralyzed state; however, when the random attack is adopted, the proportion of failed nodes in Network

A, B, C and D needs to reach 86%, 90%, 89% and this indicates that the random attack has a smaller impact on the maximal connected subgraph. The main reason is that the real-time degree priority attack method will give priority to nodes with large degree values. Such nodes are connected to a large number of nodes in the network, and when attacked, the network structure will change dramatically, the network will be split into multiple independent subgraphs, and the destruction resistance will decrease rapidly.

5. Network Optimization and Comparative Analysis

5.1. Edge Addition Strategy

Taking Network A as an example, it is found that the overall average degree of this network is small and the destructive resistance still has a large deficiency. Considering that increasing the average degree of nodes has a greater effect on the improvement of the destruction resistance of the network, the edge addition to the network is used to improve the average degree of network nodes. The strategy of adding edges in different ways can be classified as follows:

Strategy A: high-degree edge addition. Calculate the degree of the node, select two nodes in the order from high to low to add an edge (not repeated with the original edge), and stop adding edges when the number of added edges is reached.

Strategy B: low-degree edge addition. Calculate the degree of the node, select two nodes in the order from low to high to add an edge (not repeated with the original edge), and stop adding edges when the number of added edges is reached.

Strategy C: add edges randomly. Randomly select two nodes in the network to add an edge (not repeating the original edge), and stop adding edges when the number of added edges reaches.

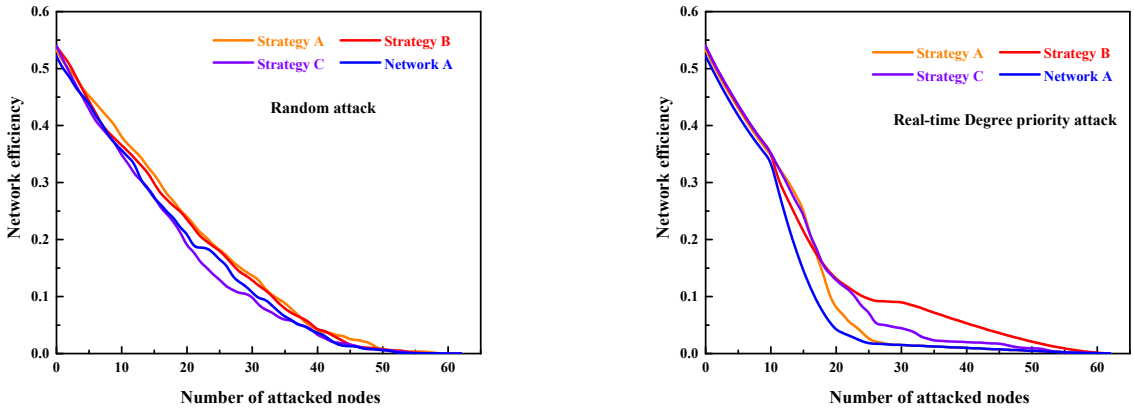
The edge addition rate is defined as:

$$\alpha = \frac{E'}{E} \times 100\% \tag{14}$$

where E' is the number of added edges, and E is the number of original network edges. In this example, α is 10%.

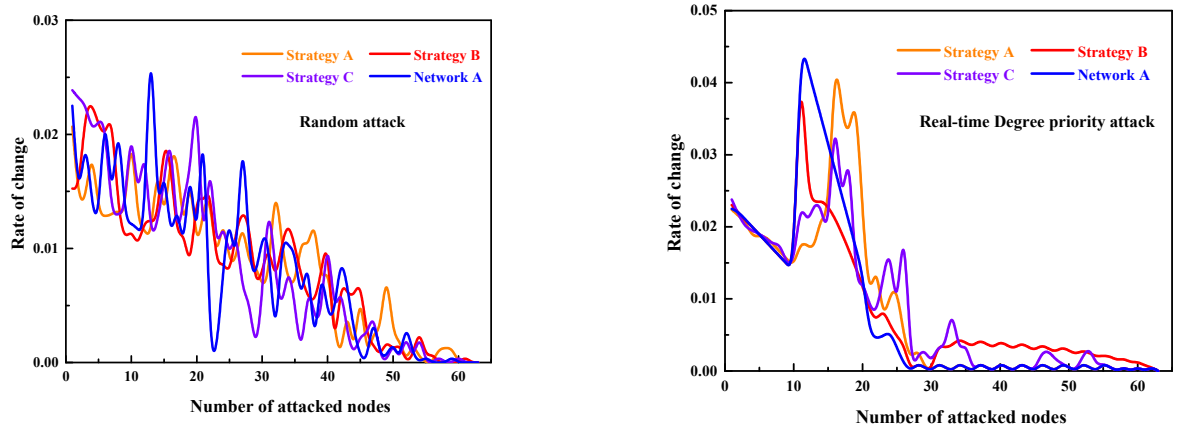
5.2. Model Analysis

After the optimal construction of the network is completed using the above three edge addition strategies, the average efficiency, the rate of change of efficiency, network potency factor and maximal connected subgraph change under the two attack methods are analyzed, respectively. The results are shown in Figures 9–12.



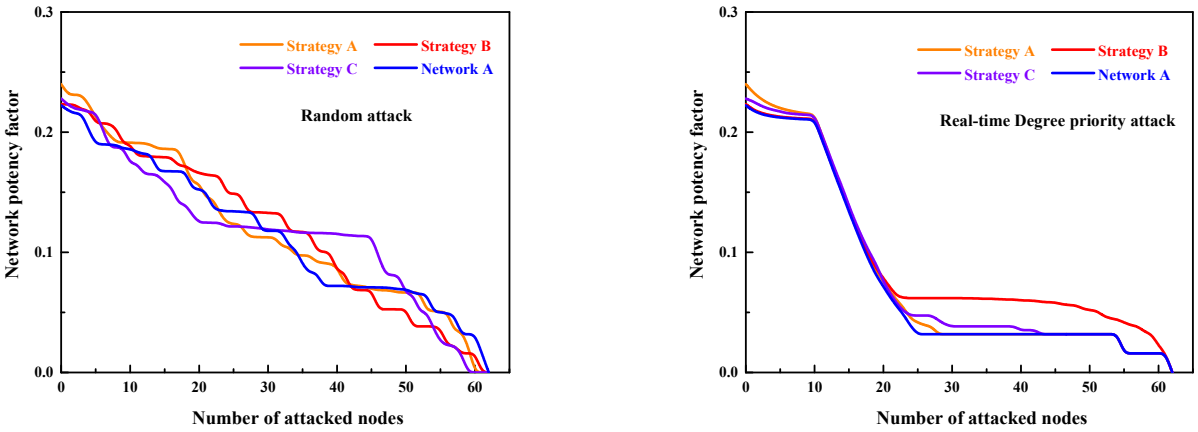
(**a**) (**b**)

Figure 9. Graph of the average efficiency under two attacks. (**a**) Random attack; (**b**) Deliberate attack.



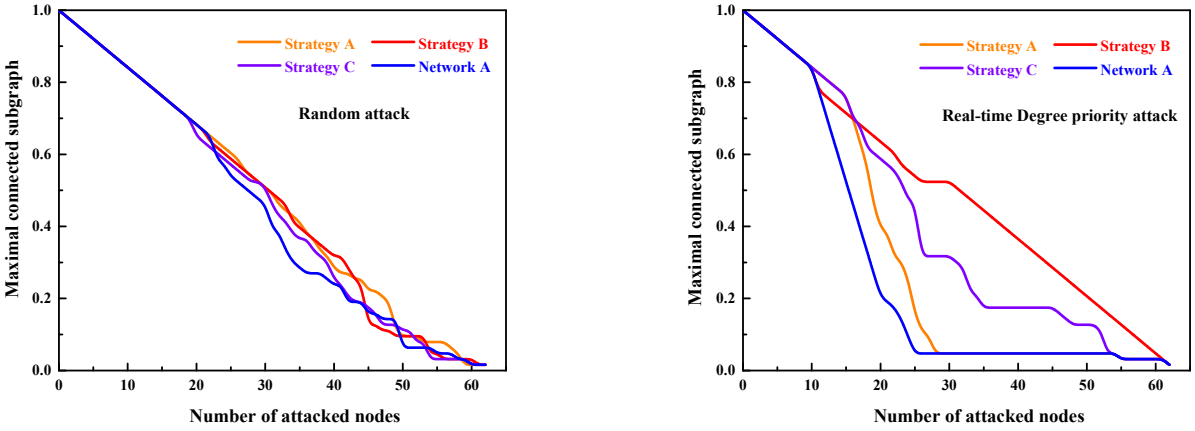
(**a**) (**b**)

Figure 10. Graph of rate of change of efficiency under two attacks. (**a**) Random attack; (**b**) Deliberate attack.



(**a**) (**b**)

Figure 11. Graph of network potency factor under two attacks. (**a**) Random attack; (**b**) Deliberate attack.



(**a**) (**b**)

Figure 12. Graph of maximal connected subgraph under two attacks. (**a**) Random attack; (**b**) Deliberate attack.

It can be concluded from Figure 10 that all three edge addition strategies can improve the initial efficiency of the network to some extent, by 2.07%, 3.22% and 3.45%, respectively, compared with the original network. When dealing with two types of attacks, especially deliberate attack, all three strategies achieve better results. By comparing the change rate of network efficiency, it can be seen that the three optimization strategies can alleviate the change degree of network efficiency, which is conducive to the stability of network.

It can be concluded from Figure 11 that compared to the original network, the initial potency factor of the three optimized networks are improved by 8%, 0.5% and 2.5%, respectively. In terms of the response to the two attacks, the network potency factor is better maintained when the low-degree edge addition strategy is used. When the number of failed nodes reaches 39.68%, the network potency factor of the three networks are 0.042, 0.062 and 0.047, respectively, which are 30.90%, 94.56% and 49.32% higher than the initial network, respectively.

It can be concluded from Figure 12 that the three edge addition strategies can improve the maximal connected subgraph of the network to a small extent. Under the deliberate attack, all three strategies can achieve better results: when the number of failed nodes reaches 19.05%, the maximal connected subgraph of the original model falls off a cliff to a very low level, and the network changes dramatically and is basically in a state of collapse; while the optimized model declines more slowly, and the network collapses when the failure proportion reaches 44%, 94% and 84%, respectively. In particular, the maximum connected subgraph is effectively enhanced when a low-degree edge addition strategy is used.

In terms of coping with the deliberate attack, when the number of failed nodes in the network reaches 35%, the initial efficiency of the network can be improved by 3.22% compared to the original model when using the low degree edging strategy, and by 65.82% and 2.34% compared to the other two edge addition strategies (high-degree edge addition, add edges randomly); the network potency factor can be improved by 0.5% compared to the original model, and by 47.62% and 31.91% compared to the other two edge addition strategies (high-degree edge addition, add edges randomly); the network will only collapse when the maximum connected subgraph ratio reaches 94%. It can be seen that, among the three edge addition strategies proposed in this paper, the low-degree edge addition makes the network model perform better in response to deliberate attack and random attack, and can effectively improve the network's destruction resistance.

This provides a good reference idea to explore the optimized performance of the network's destruction resistance. In actual operations, when the conditions, environment, and technology allow, the use of low-degree edge addition can effectively enhance the network's destruction resistance and operational effectiveness by expanding the horizontal links between combat entities of the same layer and increasing the cross-layer links between combat entities of different levels.

6. Conclusions

This paper proposes a C2 network based on complex networks theory, investigates the topology and destruction resistance of the network model, and draws relevant conclusions. It is shown that the C2 network satisfies small-world, scale-free characteristics and it is particularly vulnerable to deliberate attack. Within a reasonable and network-acceptable range, a low-degree edge addition approach can be considered to enhance the network's destruction resistance. At the same time, the critical nodes of the network should also be protected, which are the core nodes of the network and their robustness plays a key role in the performance of the network, once these nodes are hit, the effectiveness of the network will collapse in an "avalanche". For the study of C2 system, complex networks theory is a very effective theoretical tool, which is a good theoretical guidance for the establishment and optimization of the network model.

However, the following deficiencies remain in this paper.

(1) The weight of the connected edges in the network has not been fully considered, and the connected edges between different nodes have different weights and are of different importance in the network.
(2) The evaluation indexes designed for the study of the destruction resistance are not comprehensive enough, and the relevant index system needs to be studied in depth to make the results more scientific and reasonable.
(3) The current simulation nodes are small in scale and the dynamic changes of the network are not sufficiently considered. Further investigation will be carried out in these three aspects.

Author Contributions: Methodology, T.L. and M.Z.; Software, G.W.; Formal analysis, X.G. and J.L.; Resources, C.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by "Project of National Natural Science Foundation of China", grant number 62106283.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: We thank our teachers, friends and other colleagues for their discussions on simulation and comments on this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Watts, D.; Strogatz, S. Collective dynamics of 'small-world' networks (see comments). *Nature* **1998**, *393*, 440–442. [CrossRef] [PubMed]
2. Barabasi, A.L.; Albert, R. Emergence of scaling in random networks. *Science* **1999**, *286*, 509–512. [CrossRef]
3. Owais, M. Location Strategy for Traffic Emission Remote Sensing Monitors to Capture the Violated Emissions. *J. Adv. Transp.* **2019**, *2019*, 6520818. [CrossRef]
4. Owais, M.; El deeb, M.; Ali Abbas, Y. Distributing Portable Excess Speed Detectors in AL Riyadh City. *Int. J. Civ. Eng.* **2020**, *18*, 1301–1314. [CrossRef]
5. Owais, M.; Ahmed, A.S.; Moussa, G.S.; Khalil, A.A. Integrating underground line design with existing public transportation systems to increase transit network connectivity: Case study in Greater Cairo. *Expert Syst. Appl.* **2021**, *167*, 114183. [CrossRef]
6. Zhang, M.; Huang, T.; Guo, Z.; He, Z. Complex-network-based traffic network analysis and dynamics: A comprehensive review. *Phys. A Stat. Mech. Its Appl.* **2022**, *607*, 128063. [CrossRef]
7. Wang, Y.; Cao, X.; Qin, F.; Tong, L. Vulnerability analysis of the chinese coupled aviation and high-speed railway network. *Chin. J. Aeronaut.* **2022**, *35*, 189–199. [CrossRef]
8. Jiao, J.; Zhang, F.; Liu, J. A spatiotemporal analysis of the robustness of high-speed rail network in China-ScienceDirect. *Transp. Res. Part D Transp. Environ.* **2020**, *89*, 102584. [CrossRef]
9. Sheikh, M.S.; Regan, A. A complex network analysis approach for estimation and detection of traffic incidents based on independent component analysis. *Phys. A Stat. Mech. Its Appl.* **2022**, *586*, 126504. [CrossRef]
10. Jin, K.; Wang, W.; Li, X.; Hua, X.; Qin, S. Exploring the robustness of public transportation system on augmented network: A case from Nanjing China. *Phys. A Stat. Mech. Its Appl.* **2022**, *608*, 128252. [CrossRef]
11. Li, J.; Huang, Z.; Yu, X.; Gao, Y. Structural Analysis of the Overall Hypoxia Response Network. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019; pp. 1469–1473.
12. Owais, M.; Ahmed, A.S.; Moussa, G.S.; Khalil, A.A. Design scheme of multiple-subway lines for minimizing passengers transfers in mega-cities transit networks. *Int. J. Rail Transp.* **2021**, *9*, 540–563. [CrossRef]
13. Zhang, W.; Pei, W.; Guo, T. An efficient method of robustness analysis for power grid under cascading failure. *Saf. Sci.* **2014**, *64*, 121–126. [CrossRef]
14. Meng, Y.; Zhang, H.; Fan, W. Analysis of the network structure characteristics of virtual power plants based on a complex network. *Electr. Power Syst. Res.* **2022**, *204*, 107717. [CrossRef]
15. Wang, T.; Li, H.; Huang, Y. The complex ecological network's resilience of the Wuhan metropolitan area. *Ecol. Indic.* **2021**, *130*, 108101. [CrossRef]
16. Gao, Z.; Gong, Z.; Cai, Q.; Ma, C.; Grebogi, C. Complex Network Analysis of Experimental EEG Signals for Decoding Brain Cognitive State. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *68*, 531–535. [CrossRef]
17. Lu, T.; Chen, K.; Zhang, Y.; Deng, Q. Research on Dynamic Evolution Model and Method of Communication Network Based on Real War Game. *Entropy* **2021**, *23*, 487. [CrossRef]
18. Zaikui, W.; Yaping, M.; Jingrui, S. Research on Network Topology Model of Command Information System Based on Complex Networks. *Command. Control. Simul.* **2011**, *33*, 8–11+29.

19. He, H.; Li, Z.; Wang, W.; Zhou, W.; Zhu, Y.; Li, X. Research on Critical Node Analysis Method of New Combat SoS. In Proceedings of the 2018 IEEE International Systems Engineering Symposium (ISSE), Rome, Italy, 1–3 October 2018; pp. 1–7.
20. Zhang, Q.; Lei, H.M. Research on Network Properties of command and control System Based on Complex Networks Theory. *Strike Control. Command. Control.* **2011**, *36*, 41–44.
21. Zhang, Q.; Li, J.H.; Shen, D.; Ma, C. Research on network modeling and optimization of operation system of systems based on complex network. *Syst. Eng. Electron.* **2015**, *37*, 1066–1071.
22. Kang, B.G.; Choi, S.H.; Kwon, S.J. Simulation-based optimization on the system-of-systems model via model transformation and genetic algorithm: A case study of network-centric warfare. *Complexity* **2018**, *2018*, 232–239. [CrossRef]
23. Chen, L.; Kou, Y.; Li, Z.; Xu, A.; Wu, C. Empirical research on complex networks modeling of combat SoS based on data from real war-game, Part I: Statistical characteristics. *Phys. A Stat. Mech. Its Appl.* **2018**, *490*, 754–773. [CrossRef]
24. Zhu, J.; Shen, S.L.; Bai, C.S. Combat Experiment of SOS Attack Method From the Perspective of the Complex Network. *Command. Control. Simul.* **2017**, *39*, 93–97+105.
25. Liu, P.; Feng, D.; Yan, K. System Model and Simulation of "Cloud Operations" Based on Complex Network. *Command. Control. Simul.* **2016**, *38*, 6–11.
26. Gang, J.X.; Xiong-Bing, Y.E.; Wang, W. Hypernetwork modeling research on carrier formation Figurehting SoS. *Ship Sci. Technol.* **2019**, *41*, 6–11.
27. Chengyu, S.; Maoxing, S.; Hao, S. Optimization design of structure invulnerability for air defense multiple sensor network. *J. Commun.* **2017**, *38*, 118–126.
28. Wang, Y.; Zhang, D.; Pan, C.; Chen, B. Measure of invulnerability for command and control network based on network invulnerability entropy. In Proceedings of the International Conference on Control Science & Systems Engineering, Singapore, 27–29 July 2016; IEEE: Piscataway, NJ, USA, 2016.

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