electronics

Article

Robustness of Double-Layer Group-Dependent Combat Network with Cascading Failure

Jintao Yu [1,*], Bing Xiao [2] and Yuzhu Cui [3,4]

[1] Department of Information, Air Force Early Warning Academy, Wuhan 430019, China
[2] Department of Intelligence, Air Force Early Warning Academy, Wuhan 430019, China
[3] Research Center for Intelligent Computing Platforms, Zhejiang Lab, Hangzhou 311121, China
[4] Tsung-Dao Lee Institute, Shanghai Jiao Tong University, Shanghai 201210, China
* Correspondence: haleine@ustc.edu

Abstract: The networked combat system-of-system (CSOS) is the trend of combat development with the innovation of technology. To achieve the combat effectiveness, studying the ability of CSOS to cope with external interference is of great importance. Here we report a modeling method of CSOS from the perspective of complex networks and explore the robustness of the combat network based on this. Firstly, a more realistic double-layer heterogeneous dependent combat network model is established. Then, the conditional group dependency situation is considered to design failure rules for dependent failure, and the coupling relation between the double-layer subnets is analyzed for overload failure. Based on this, the initial load and capacity of the node are defined, respectively, as well as the load redistribution strategy and the status judgment rules for the cascading failure model. Simulation experiments are carried out by changing the attack modes and different parameters, and the results show that the robustness of the combat network can be effectively improved by improving the tolerance limit of one-way dependency of the functional net, the node capacity of the functional subnet, and the tolerance of the overload state. The conclusions of this paper can provide a useful reference for network structure optimization and network security protection in the military field.

Keywords: combat network; cascading failure; heterogeneous structure; interdependent; robustness

Citation: Yu, J.; Xiao, B.; Cui, Y. Robustness of Double-Layer Group-Dependent Combat Network with Cascading Failure. *Electronics* **2023**, *12*, 3061. https://doi.org/10.3390/electronics12143061

Academic Editors: Cheng Siong Chin and Myung-Sup Kim

Received: 21 May 2023
Revised: 1 July 2023
Accepted: 10 July 2023
Published: 13 July 2023

1. Introduction

Informatization warfares are systematic combats based on information systems, and information has increasingly become the dominant factor in combat. In actual operations, one or several nodes in the combat network may fail due to combat attacks or random failures. The service processing load of these failed nodes will be transmitted through the information flow and cause secondary failures in other nodes. A larger-scale chain effect caused by the load reallocation can eventually lead to partial failure or even complete collapse of the network. In the current situation, the components and structural relations of the modern combat network are increasingly complex, and information interactions are becoming increasingly frequent. Therefore, studying the characteristics and laws of cascading failure of the combat network through reasonable models is of great importance, which is also beneficial to reducing the risk of cascading failure and making the combat network more robust.

Scholars have proposed many models to study network cascading failure in recent years. For example, for the modeling and analysis of cascading failure, Kinney et al. [1] proposed a cascading failure model based on efficiency analysis for the power grid, considering the situation that the node does not disappear after failure. Wang et al. [2] proposed a stochastic Markov model, which is able to capture the progression of cascading failures by a flow redistribution model. Geng et al. [3] investigated the edge-removal attack's influence on the robustness of complex networks considering load and cascading failure.

With regard to the load redistribution, one of the classical cascading failure models is the "capacity and load" model presented by Motter and Lai [4]. From the way the load is redistributed in this model, Duan et al. [5] proposed a complex network cascading failure model with an adjustable load redistribution range considering the load redistribution heterogeneity, and analyzed the cascading failure conditions on a scale-free network. Yin et al. [6] also proposed the cascading failure model based on the characteristics of the changeable load and the fixed capacity of the node in the scale-free network.

The above modeling and load redistribution methods are all based on single-layer networks. With regard to multilayer networks and their robustness, Yuan [7] introduced a cascading failure model for the complex network with a hierarchical structure. The redistribution method of the model takes the hierarchy and heterogeneity into consideration, of which the network tends to redistribute extra load to intact nodes of the same or higher hierarchies. Ben-Haim [8] studied the hierarchical network with unity of command and discussed how to design the network to manage cascading failures adequately. Multilayer networks are usually characterized by dependencies. Inspired by this, Buldyrev et al. [9] first proposed the cascading failure model of interdependent networks. Adnan et al. [10] reported a hybrid probabilistic modeling method to balance load flow and an assessment algorithm to describe the transient stability in multiple interdependent power grid cascading failures. Zakariya [11] discussed the interdependent power networks' cascading failure models in terms of features, limitations, and computational speed. Peng et al. [12] proposed a model of double-layer network structure with simplicial complexes and discussed the higher-order interactions between the networks. To mitigate cascading failures, Smolyak et al. [13] proposed an intuitive and simple method of protecting the critical nodes, and similar approaches were proposed by Wang et al. [14] and Shen et al. [15]. These robustness and cascading failure studies of multilayer networks take little account of the functional heterogeneity of the nodes.

With regard to the research on combat networks, Guo et al. [16] constructed a cascading failure model in command and control networks and analyzed the influence of load parameters, capacity parameters, and evolution step size on cascading failure invulnerability. Zhang et al. [17] investigated the dynamic load redistribution strategy based on the node's local load rate with respect to the cascading failure transmission of the equipment support network. These works are more focused on cascading failures in single-layer combat networks, similar to complex networks in general; there are also more complex relations among different types of combat networks and the coupled networks are well worth investigating. Hence, Yang et al. [18] firstly explored the cascading failure characteristics and laws of information flowing in combat systems by abstracting network structure in a hierarchical way. Wang et al. [19] proposed the model of the military information systems of systems based on function dependency and analyzed the center of gravity. These works only consider the robustness of the combat network under cascading failures in terms of topology structure but rarely address the functionality of the combat network.

According to the above analysis, although existing research has deepened the theoretical understanding of cascading failures in combat networks, there are still some deficiencies that need to be addressed: (1) The common research mainly focuses on the single-layer network, and there are few kinds of research on the cascading failure model of the combat network with hierarchical structure and coupling characteristics. (2) The research on hierarchical structure modeling and dependent failure of combat networks needs to be further explored as well as the heterogeneity of combat networks. (3) The method of load redistribution needs to consider the actual situation, as the load is not simply distributed equally among all neighboring nodes. To address these problems, we establish a heterogeneous dependent network model with a double-layer structure according to the actual situation of the combat network, design the rules of dependent failure and overload cascading failure, and discuss the robustness of the combat network through simulation experiments. The aforementioned contributions can provide a more comprehensive and realistic perspective to the study of the robustness of combat networks.

This paper is organized as follows. In Section 2, the double-layer combat network model with group-dependent characteristics is established based on real situations at first. In Section 3, the failure model combing conditional group-dependent failure model and cascading failure model is proposed. Attack modes are also classified according to different objects and intentions. In Section 4, some experiments based on the simulated combat networks are carried out to analyze the influence of different parameters and attack modes on system robustness. The conclusions and the future work follow in Section 5.

2. Double-Layer Group-Dependent Combat Network

For the convenience of reading, a glossary of the notations used in this paper is presented in Table 1 .

Table 1. List of symbols.

Symbol	Meaning
G	The complex network, including the communication network G_{W}, the functional network G_{G} and the dependent network G_{D}
V	The nodes set of the complex network, the specific node in it is v_i
E	The edges set of the complex network, the specific edge in it is e_i
N	The number of the nodes set, including N_{O}, N_{P}, N_{D}, N_{A}, N_{W} and N_{G}
$\boldsymbol{S}$	The adjacent matrix of the network
p_{XX}	The probability of two different nodes can connect with each other
L_i	The load of the node v_i
C_i	The capacity of the node v_i
k_i	The degree of the no v_i
ζ_i	The communication connectivity index of node v_i
S_{links}	The amount of total intelligence effectiveness links
S_{huge}	The largest component scale of the combat network
α	The proportion parameter indicating the preference for S_{links} and S_{huge}
f	The nodes failure ratio for the total network
τ	The endurance threshold of connectivity index
$\kappa(\kappa_{\mathrm{W}}/\kappa_{\mathrm{G}})$	The power parameter of node load
$\lambda(\lambda_{\mathrm{W}}/\lambda_{\mathrm{G}})$	The linear parameter of node capacity
$\gamma(\gamma_{\mathrm{W}}/\gamma_{\mathrm{G}})$	The power parameter of node capacity
$\delta(\delta_{\mathrm{W}}/\delta_{\mathrm{G}})$	The bearing range of node when it is overloaded

To be as real as possible, the combat network is modeled from two aspects. One is the communication net in terms of physical combat equipment, and the other is the functional net in terms of logic. For the combat communication net, each piece of equipment is deployed in a dispersed manner in physical locations and undertakes the task of energy and material transmission dominated by information flow. Therefore, combat equipment is the basis for communication and information interaction. An information grid network that achieves high data sharing, efficient information interaction, dynamic port access, and flexible combination requirements is the result of the deep fusion of all types of equipment. The definition of the communication net is given as follows:

Definition 1. *Suppose* $G_{\mathrm{W}} = (V, W_a, E, W_b)$ *is the communication net of combat system-of-system (CSOS), in which the node set is* $V = \{v_1, v_2, \cdots, v_{N_{\mathrm{W}}}\}$, v_i *represents the combat equipment with communication function in the communication net, and* N_{W} *is the number of nodes.* $W_a = \{w_i | v_i\}$ *represents the attributes of the node, including its initial load and bearable capacity. The set of edges is* $E = \{e_1, e_2, \cdots, e_{M_{\mathrm{W}}}\}$, *where* $e_i = \{e_{jk} | v_j \times v_k\}$ *represents the communication relations among different nodes, and* M_{W} *is the number of edges. The existence of edge is mainly determined by infrastructure deployment, affiliation, and mission requirements. It is relatively fixed in general and will be flexible and changeable when carrying out missions.* $W_b = \{w_{jk} | e_{jk}\}$ *is the attribute of the communication edge, such as bandwidth and delay.*

For simplicity, it is assumed that the communication net is fixed and undirected and $W_b = 1$, so the initial perturbation of the network topology and the performance on edges will not be considered. We denote the node of the communication net as node C.

With regard to functional net, the combat units and relations among them in CSOS are usually abstracted into the nodes and edges of the complex network, namely, "O, P, D, A" nodes and the corresponding edges [20]. The "O, P, D, A" nodes represent the intelligence obtaining unit, intelligence processing unit, decision and command unit, and attack or damage unit, respectively, and more details on structural abstraction can be found in [20]. There are complex interaction relations among different units, forming a network structure of heterogeneous components, multipoint interaction, multidomain fusion, and dynamic evolution, so the heterogeneous information network is used for modeling. The functional net of CSOS with heterogeneous information is defined as follows:

Definition 2. *Suppose* $G_{\mathrm{G}} = (V, W_a, E, W_b; \varphi, \psi; V_{\mathrm{G}}, E_{\mathrm{G}})$ *is the functional net of CSOS, where the node set is* $V = \{v_1, v_2, \cdots, v_{N_{\mathrm{G}}}\}$, *and* N_{G} *is the number of nodes.* $W_a = \{w_i | v_i\}$ *represents the service attributes of the functional node, including the service category, processing load, and affordable capacity undertaken by the node.* $E = \{e_1, e_2, \cdots, e_{M_{\mathrm{G}}}\}$ *is the edge set, in which* M_{G} *is the number of edges.* $W_b = \{w_{jk} | e_{jk}\}$ *is an attribute of the edge, indicating the interaction strength of service information. Both nodes and edges have characteristics of type. The type set of nodes is* V_{G}, *and there is a mapping function* $\varphi : V \to V_{\mathrm{G}}$ *that satisfies* $\varphi(v_i) \in V_{\mathrm{G}}$, *while type set of edges is* E_{G} *with mapping function* $\psi : E \to E_{\mathrm{G}}$ *satisfying* $\psi(e_i) \in E_{\mathrm{G}}$. *If* $|V_{\mathrm{G}}| > 1$ *or* $|E_{\mathrm{G}}| > 1$, *then the functional net of CSOS is called heterogeneous combat functional net (HCFN).*

Similarly, for the sake of simplicity, this paper assumes that the service interaction strength of the edge of the HCFN is within the acceptable range, so the attribute characteristics of the edge will not be considered. In addition, the type set of nodes is $V_{\mathrm{G}} = \{$O, P, D, A$\}$, and the type set of directed edge is $E_G = \{$O–O, O–P, P–P, P–D, D–D, D–A$\}$.

It is notable that the functional net is unidirectionally dependent on the communication net to achieve combat utility. Although the obtained and processed intelligence information and command orders are all circulated in the functional net, the information exchanges among the nodes are all based on communication units in practice. Apart from the communication net and the functional net, there is another important network called the dependent net. To build the dependent relation between CSOS, the following two assumptions need to be specified:

(1) The node in CSOS only has a single function, that is, node C of the communication net can only perform information transmission, node O of the functional net can only perform information acquisition, node P can only perform information processing, node D can only perform commands and decisions, and node A can only perform combat attack.

(2) Although the communication net is abstracted from the actual equipment, it is assumed that the constraints of space and time are neglected when it undertakes communication missions. Therefore, the connection conditions will not be taken into consideration for how the functional net depends on the communication net.

On the basis of the above assumptions, we can construct a double-layer heterogeneous dependent combat network (DHDCN) of CSOS when the functional net is relying on the communication net, which is defined as follows:

Definition 3. *Assuming that the communication net of CSOS is* G_{W}, *the corresponding functional net of is* G_{G}. *The coupling relation between two networks is* $E_{\mathrm{D}} = \{E_{\mathrm{GW}}, E_{\mathrm{WG}}\}$, *which means that the functional net relies on the communication net. When the dependency node* $v_{\mathrm{G}}^i \to v_{\mathrm{W}}^j$, *let* $E_{\mathrm{D}}(v_{\mathrm{G}}^i, v_{\mathrm{W}}^j) = 1$ *(for the convenience of calculation,* $E_{\mathrm{D}}(v_{\mathrm{W}}^j, v_{\mathrm{G}}^i)$ *is also equal to* 1*). The dependency nodes and edges form a dependent net as* G_{D}. *All networks above together constitute the DHDCN of CSOS, which is denoted as*

$$G = (G_{\mathrm{G}}, G_{\mathrm{D}}, G_{\mathrm{W}}). \tag{1}$$

The adjacency matrix of DHDCN is expressed as

$$S = \begin{bmatrix} S_G & S_{GW} \\ S_{WG} & S_W \end{bmatrix}, \tag{2}$$

where S_G represents the adjacency matrix of the functional net; correspondingly, S_W and $S_{WG}(S_{GW})$ are the adjacency matrices of the communication net and interdependent net.

It is worth noting that the abovementioned dependencies between heterogeneous coupling networks can be the type of one-to-one, one-to-many, and many-to-one [21]. A form of one-to-many dependency is called group dependency; therefore, a DHDCN with a one-to-many dependency is referred to as a double-layer group-dependent combat network (DGCN).

Example 1. *According to the network model described in Definition 3, the network structure of the DGCN for CSOS is given for a certain combat scenario, as shown in Figure 1. In the figure, the functional net is composed of nodes and edges corresponding to four combat units including O, P, D, and A, and the communication net is composed of nodes corresponding to different communication support units. Based on the dependent net, the functional net and the communication net form asymmetric coupling relations.*

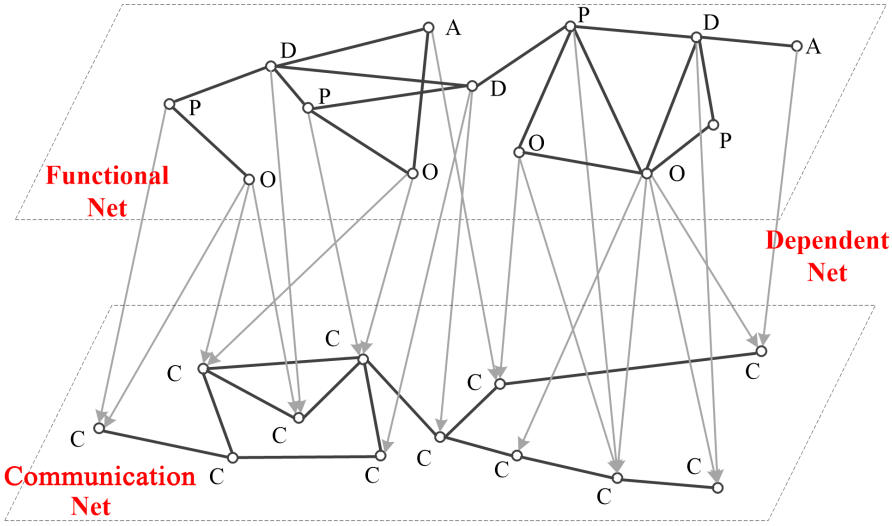


Figure 1. Structure diagram of a DGCN of CSOS.

The widely studied combat cycle model takes the loop composed of the target node T, search node S, decision node D, and influence node I as a measure of combat capability [22]. Inspired by this work, the functional net of CSOS in this paper also presents the flow of information when relying on the communication net's communication nodes. The information flow model based on communication nodes is shown in Figure 2. As we can see from the figure, the red solid lines represent the entire information flow of combat links, and the gray dotted lines indicate the information transmission through the communication net. According to the dependency rule, the information flow of the most typical combat link "O $\rightarrow$ P $\rightarrow$ D $\rightarrow$ A" will be transformed into "O $\rightarrow$ C $\rightarrow$ P $\rightarrow$ C $\rightarrow$ D $\rightarrow$ C $\rightarrow$ A", and other types of combat link can also be obtained similarly. The typical combat link's dynamics follow the rule of "information obtain–intelligence processing–command and decision–combat response (attack)" to form a kill link, and the more concrete concept of it is described in Section 4.1. Once the communication node in Figure 2 is broken, the combat link will be destroyed and CSOS will lose its combat capability. Therefore, the coupling relation between the functional subnet and communication subnet is tighter and more important in the DGCN of CSOS.

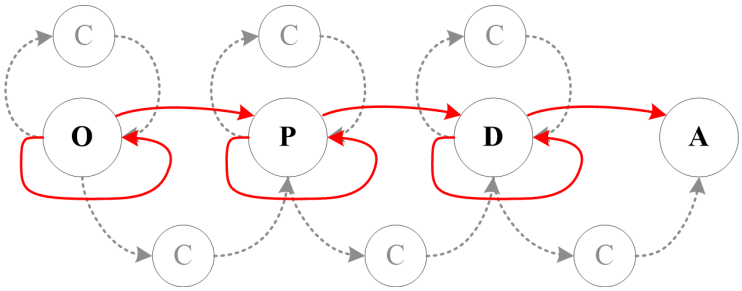


Figure 2. Information flow model based on communication nodes.

3. Cascading Failure Model for DGCN

Most common interdependence network models are based on a one-to-one dependent pattern, which has no feedback characteristics and is convenient for analysis [9]. Quite a lot of studies on the robustness of interdependent networks are also based on this pattern [23–26], but such strict dependencies often do not exist in practice. The situation of one-to-many dependency is relatively common, namely, the aforementioned group dependency [27]. If any one of the depended nodes (communication net nodes) fails, the dependent nodes (functional net nodes) fail according to the traditional analysis method. Therefore, group dependency greatly affects the robustness of the interdependent network. As long as a small number of nodes are attacked, the entire interdependent network may collapse, but the network in real life is not so fragile [28,29]. In addition to wired communication, there are many other communication methods for the communication net of DGCN, such as short-wave communication, ultra-short-wave communication, and satellite communication. Therefore, when the functional net depends on the communication net, as long as a certain percentage of the depended nodes are still working well, the dependent functional nodes will not fail. To build the cascading failure model of DGCN, the failure analyses are as follows:

3.1. Asymmetric Dependent Failure

An asymmetric dependent network is a one-way dependent network. According to the classical dependent failure model [30], the asymmetric dependent failure rules for complex networks are given: For a node that depends on the other subnet, when all its dependent nodes fail or it is not in the maximal component, the node fails; for a node of the relied subnet, when it is not in the maximal component, the node fails. Figure 3 shows a schematic diagram of the asymmetric dependent failure process of a DGCN of CSOS.

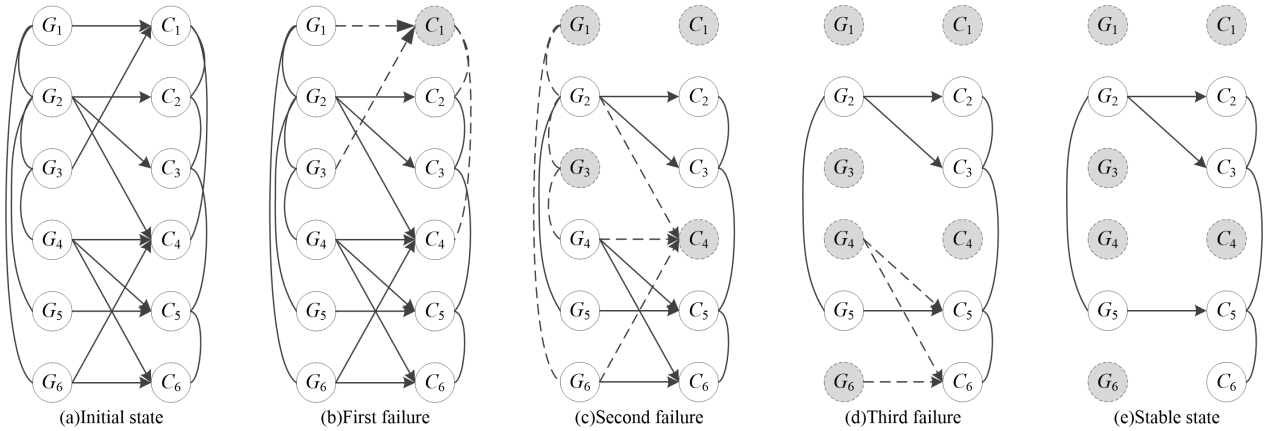


Figure 3. Asymmetric dependent failure process.

The relied communication net node C_1 is initially attacked and then fails. All edges connected to C_1 are removed. So the failed nodes are grayed out and the corresponding connecting edges are dashed while the original dependencies are still represented in solid

arrows. In the second failure, the functional net nodes G_1 and G_3 that depend on C_1 fail due to the previous failure. Node C_4 also fails because it is not in the maximal component. In the third failure, nodes G_4 and G_6 fail because of the disconnection with G_1 and G_3 and they are no longer in the maximal component of the functional network. Node G_2 will stay normal although its connection with node C_4 is interrupted. Since there are no more nodes that meet the failure rules, the failure process stops and a stable state is reached.

3.2. Conditional Group-Dependent Failure

There is a default rule in asymmetric dependent failure, that is, the dependent failure will not happen as long as the dependent relation of nodes is maintained, such as node G_2 in Figure 3. Based on this, a conditional group-dependent failure model is proposed. This model can tolerate the partial dependent failure of nodes, which is shown in Figure 4. a and b are two nodes in network A which depend on network B, the solid lines are the edges still alive, and the dashed lines are the edges that are about to fail.

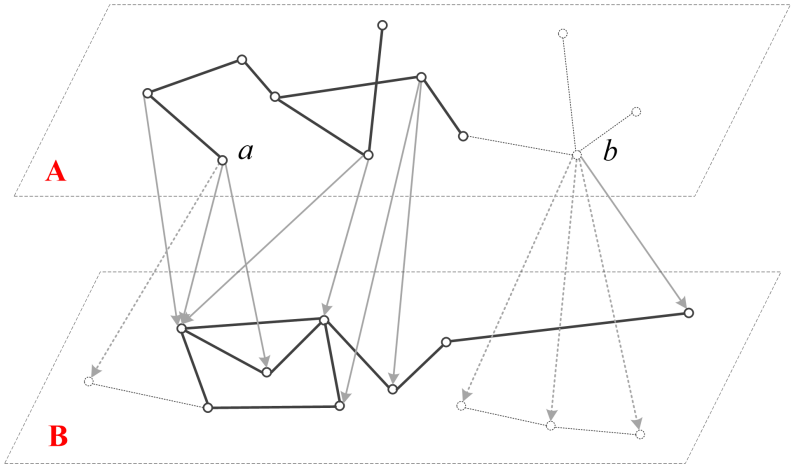


Figure 4. Conditional group dependency failure.

As we can see in the figure, network A is unidirectionally dependent on network B, and the scale of the dependency can be different. If the node x has depended on a number n communication nodes, the capacity of the node v_x is C_x, the capacity of the depended node is C_x^i, and the communication connectivity index of node x is expressed as follows:

$$\zeta_x = \frac{1}{nC_x} \sum_{i=1}^{n} C_x^i \tag{3}$$

When the depended communication nodes fail, the sum elements of ζ_x will decrease correspondingly while n will remain the same. If we set the upper limit of the communication connectivity index as $\bar{\zeta}$, then the normalized connectivity index is $\tilde{\zeta} = \zeta/\bar{\zeta}$. In our conditional group-dependent failure model, the communication connectivity index will decrease as the depended communication nodes are destroyed. When the index is lower than a threshold τ, the communication network cannot ensure that the functional nodes complete the flow of information (the default threshold is $\tau = 0.6$). Therefore, the functional node will conditionally fail. For the node a in Figure 4, its dependent nodes reserve $\frac{2}{3}$, and the connectivity index is $\tilde{\zeta}_a > \tau$, so a still remains normal, while node b will fail as it only has $\frac{1}{4}$ dependent nodes left and the connectivity index is $\tilde{\zeta}_b < \tau$.

3.3. Overload Failure Model

Apart from the dependent failure, it is necessary to consider other problems caused by the internal operating mechanism of DGCN. For the communication net, the communication node has its inherent capacity limit. When the load exceeds the tolerable range, it will lead to cascading failure. The same situation occurs on the functional net when the service

processing is overloaded. Motter and Lai proposed the "M-L" model [4,30] to describe this phenomenon. Based on this, Peng et al. [31] presented a cascading failure model considering the load and combined it with the dependent failure model. Hao et al. [32] proposed a cascading failure model considering the overload state when facing a traffic jam. Inspired by these, we establish a cascading failure model considering the overload state for the communication net and functional net, respectively, and then integrate it with the dependent failure model. The specific process of overload cascading failure is as follows: Each node has an initial load at the beginning; when a node fails due to an attack or other reasons, the load of this node will be redistributed according to certain rules. The load-obtained node will fail with a certain probability. If the node fails, a new round of load redistribution and node failure will be triggered. For the communication net, the load is redistributed among the nodes in the entire network, while the load redistribution is limited to nodes of the same type as to the functional net.

3.3.1. Initial Load

The simplest initial load can be defined as the exponential power of the node degree. However, from the perspective of information interaction, a more reasonable definition of the initial load is the function of the information path, that is, the betweenness of the node [4]. Since betweenness is the global topology information, for large-scale networks, if the structure is not completely known, it is not easy to obtain the initial load, and the complexity of betweenness calculation is very high, which may not be suitable for situations with high real-time requirements. From the perspective of "local definition and local allocation", Wang et al. [33] presented a method for calculating initial loads based on local information, and it was proved that the proposed initial load which uses the function of the product of the node degree k_i and the degree of neighbors k_j is positively correlated with betweenness. According to the above idea, the initial load of the DGCN is defined separately based on the communication net and the functional net.

The initial load of the communication net node is

$$L_{\mathrm{W}}^{i}(0) = \left(k_i \sum_{j \in \Gamma_i} k_j \right)^{\kappa_W}, i = 1, 2, \cdots N_{\mathrm{W}}, \tag{4}$$

where κ_{W} is the adjustment parameter, which is used to control the initial load distribution of communication nodes; Γ_i is the subscript set of neighbors of node v_i.

The initial processing load of the functional net node is

$$L_{\mathrm{G}}^{i}(0) = \left(k_i \sum_{j \in \Gamma_i} k_j \right)^{\kappa_G}, i = 1, 2, \cdots N_{\mathrm{G}}, \tag{5}$$

where κ_{G} is the adjustment parameter, which is used to adjust the initial load distribution of functional nodes; Γ_i is the subscript set of neighbors of node v_i.

3.3.2. Node Capacity

Due to the cost constraints, there is an upper limit of node capacity in a load-induced network. The usual way to define the node capacity is to assume that it is proportional to its initial load. However, in most real networks, a node with a smaller capacity usually has a larger remaining capacity. The relation between node capacity and load is more likely to be a nonlinear model [34,35]. In the DGCN of CSOS, if the initial load of the node is large, it indicates that the node is essential. The more important the node is, the more frequently it interacts with other nodes in information or service processing. Therefore, the corresponding residual capacity of the node is small. On the contrary, the load of the less important node is smaller, and there will be more free capacity [18]. Here, we adopt the nonlinear model to define the node capacity based on Kim's work [34].

The node capacity of the communication net is

$$C_{\mathrm{W}}^{i} = L_{\mathrm{W}}^{i}(0) + \lambda_{\mathrm{W}} \cdot L_{\mathrm{W}}^{i}(0)^{\gamma_{\mathrm{W}}}, i = 1, 2, \cdots N_{\mathrm{W}}, \tag{6}$$

where λ_{W} and γ_{W} are the adjustment parameters.

The node capacity of the functional net is

$$C_{\mathrm{G}}^{i} = L_{\mathrm{G}}^{i}(0) + \lambda_{\mathrm{G}} \cdot L_{\mathrm{G}}^{i}(0)^{\gamma_{\mathrm{G}}}, i = 1, 2, \cdots N_{\mathrm{G}}, \tag{7}$$

where λ_{G} and γ_{G} are the adjustment parameters.

Figure 5 presents the relation between the initial load and capacity in nonlinear and linear forms. It can be seen from the figure that the nonlinear model in this paper conforms to the actual situation analyzed above. Especially, the nonlinear model degenerates into a linear model when $\gamma = 1$, which shows that it is more general.

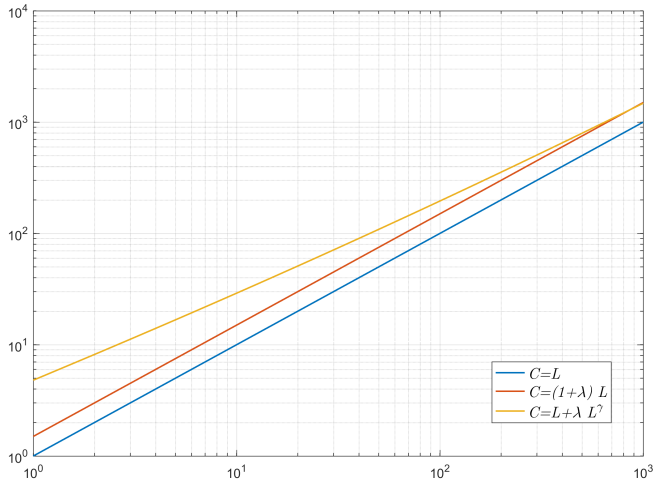


Figure 5. Relation between initial load and capacity.

3.3.3. Redistribution Strategy of Load

After a node fails, the current load will propagate in a certain way. The common redistribution methods such as local redistribution [36], global redistribution [37], and average distribution [38] have different effects on the robustness of the network when facing cascading failures. For the communication net, the communication transmissions are generally addressed according to the principle of the minimum number of hops, so local distribution is more inclined to be adopted. In this paper, we propose a load redistribution strategy from the perspective of the initial static load and subsequent dynamic remaining capacity, which is as follows:

The static allocation ratio for neighbor node v_j of failed node v_i at time 0 is

$$\Pi_{ij}^{s} = \frac{L_{\mathrm{W}}^{j}(0)}{\sum\limits_{j \in \Gamma_i} L_{\mathrm{W}}^{j}(0)}. \tag{8}$$

As for the dynamic allocation at time t, we use the ratio based on the dynamic remaining capacity and it is represented as

$$\Pi_{ij}^{d} = \frac{C_{\mathrm{W}}^{j} - L_{\mathrm{W}}^{j}(t)}{\sum\limits_{j \in \Gamma_i} C_{\mathrm{W}}^{j} - L_{\mathrm{W}}^{j}(t)}. \tag{9}$$

Therefore, the synthetic allocation ratio is as follows:

$$\Pi_{\mathrm{W}}^{ij} = \eta \Pi_{ij}^{s} + (1-\eta)\Pi_{ij}^{d}, \tag{10}$$

where η is the proportion parameter of two redistribution methods. Then, the new obtained load of neighbor node v_j is expressed as

$$\Delta L_{\mathrm{W}}^{ij}(t) = \Pi_{\mathrm{W}}^{ij} L_{\mathrm{W}}^{i}(t). \tag{11}$$

And we can update the load of the communication net's nodes by the following expression:

$$L_{\mathrm{W}}^{k}(t+1) = L_{\mathrm{W}}^{k}(t) + \sum_{j \in \Gamma_k} \Delta L_{\mathrm{W}}^{jk}(t). \tag{12}$$

In the same way, the processing load distribution method of the functional net is easy to obtain. However, it should be noted that the redistribution only occurs among the same type of functional nodes. The node load after a new round of failure is shown as follows:

$$L_{\mathrm{G}}^{k}(t+1) = L_{\mathrm{G}}^{k}(t) + \sum_{j \in \Gamma_k} \Delta L_{\mathrm{G}}^{jk}(t). \tag{13}$$

3.3.4. Failure Status Judgment

In the classical "M-L" model [4], a node has only two states, namely, the normal state and the failed state. Hao et al. [32] proposed a cascading failure model of complex networks considering overloaded nodes. When the load exceeds the capacity of a node, the node will fail with a certain probability in the certain bearing range δ. This state is called the critical state. When the load exceeds the above range, the node fails directly. Motivated by this, the specific rules for judging the failure situation after the node obtains the reallocated load are as follows:

(1) If $L_i(t) \leq C_i$, the node v_i does not fail.

(2) If $C_i < L_i(t) \leq (1+\delta)C_i$, the node v_i is in the critical failure state. Although the load exceeds the capacity of a node, it is still within the affordable range. The more the node is overloaded, the greater the probability of node failure and the failure probability is

$$p_i(t) = \frac{L_i(t) - C_i}{\delta C_i}. \tag{14}$$

When $p_i(t)$ is greater than a random number, the node v_i fails.

(3) if $L_i(t) > (1+\delta)C_i$, the node v_i fails immediately.

In summary, taking the cascading failure of the communication net as an example, the failure probability of node v_i is presented as

$$p_{\mathrm{W}}^{i}(t) = \begin{cases} 0, & L_{\mathrm{W}}^{i}(t) \leq C_{\mathrm{W}}^{i} \\ \frac{L_{\mathrm{W}}^{i}(t) - C_{\mathrm{W}}^{i}}{\delta C_{\mathrm{W}}^{i}}, & C_{\mathrm{W}}^{i} < L_{\mathrm{W}}^{i}(t) \leq (1+\delta)C_{\mathrm{W}}^{i} \\ 1, & L_{\mathrm{W}}^{i}(t) > (1+\delta)C_{\mathrm{W}}^{i}. \end{cases} \tag{15}$$

For the cascading failure of the functional net, the processing load can only be spread among nodes of the same type. Once a functional node fails, the processing load of it will redistribute among neighbor nodes according to the same information transmission or service transactions. If the processing load of the current node has been updated, the probability of whether this node fails is similar to Equation (15), and will not be repeated.

3.4. Attack Mode

In combat confrontation, attacks on combat networks are generally divided into random attacks and intended attacks [39]. The random attack is to randomly select several

nodes to make them invalid, while the intended attack is to make nodes invalid according to a certain order of node importance. Since DGCN is a double-layer network, there are different attack modes for different networks. For example, in different combat phases, the enemy may select specific functional net nodes to attack or destroy the nodes of the communication net randomly. According to the attack object of the combat network and the attack intention, the attack mode can be divided into the following six types:

(1) Random single communication network attack (RSCA): Randomly select nodes with a ratio f from the communication net to attack and let these nodes fail.

(2) Intended single communication network attack (ISCA): Select nodes with a ratio f from the communication net according to the descending node degree, and let them fail by attacking.

(3) Random single functional network attack (RSFA): Randomly select nodes with a ratio f from the communication net to attack and let these nodes fail.

(4) Intended single functional network attack (ISFA): Select nodes with a ratio f from the functional net according to the descending node degree, and let them fail by attacking.

(5) Random double networks attack (RDA): Randomly select nodes with a ratio $0.5f$, respectively, from the communication and functional net to attack, and let these nodes fail.

(6) Intended double networks attack (IDA): Select nodes with a ratio $0.5f$, respectively, from the communication net and functional net according to the descending node degree, and let them fail by attacking.

Different attack modes may have different effects on robustness. Combining the asymmetric dependent failure model and overload cascading failure model, the failure process of the DGCN of CSOS can be represented as Figure 6, in which the dashed boxes of three different colors represent different attacked objects. These nodes in a double-layer network will suffer random attacks or intended attacks. As can be seen from the figure, the failure process of the communication net always leads to the failure of the functional net, so the functional net is more fragile. Any disturbance in the network may cause serious consequences of "failure, disconnection and paralysis".

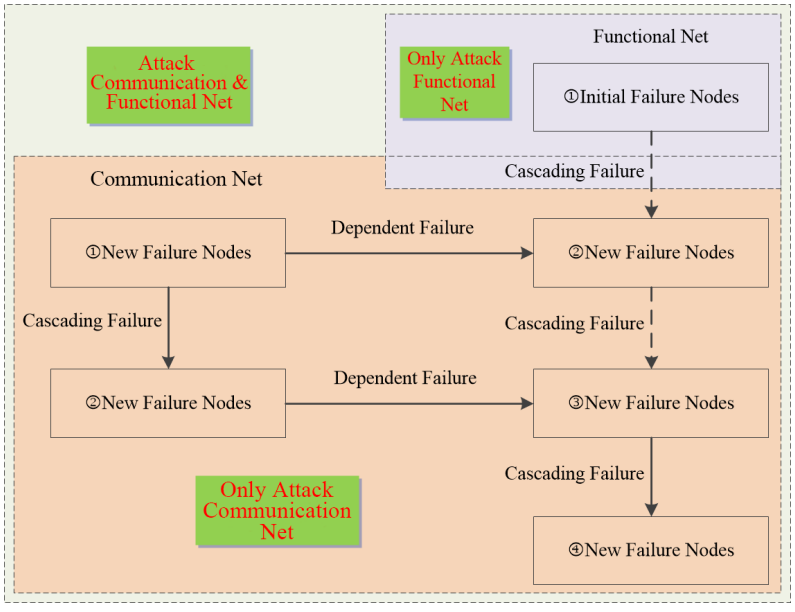


Figure 6. Failure process under different attack modes.

4. Simulation Experiments on Robustness

4.1. Robustness Evaluation Index

The general definition of the robustness of the combat network is the ability of a system to maintain its original functions, characteristics, and organizational structure under external disturbances [40]. In this paper, the robustness of DGCN for CSOS refers to the

ability of a system to continue maintaining combat performance after some nodes failed in the network. Due to the existence of a functional net in DGCN, the performance evaluation can be more real. Here we define the robustness evaluation index from two aspects:

The first aspect of the robustness measure is based on combat network topology. The scale of the maximal component is selected as an index of the damage effect of the combat network. One individual component is a subgraph with connectivity and isolation in the network. As a result, the maximal component is a subgraph with the largest node scale in the network, which is denoted as S_{huge}. With the increase of the scale of the maximal component in the combat network, the interconnections among combat network nodes become closer and the information flow efficiency of the combat network becomes higher. In this paper, we adopt the approach of node shrinking to iteratively calculate the scale of the maximal component [41]. The initial maximal component of DGCN is

$$S_{\text{huge}}(G) = N_{\text{G}} + N_{\text{W}}, \tag{16}$$

where N_{G} and N_{W} are the node number of the functional net and the communication net, respectively.

The second aspect of the robustness evaluation index is based on the operational capability of the combat network. The number of kill links can be used to describe the operational capability of a combat network [42]. In the case of a DGCN of CSOS, the number of combat effectiveness links (CELKs) S_{links} is introduced to measure the operational capability. According to the idea of Boyd's OODA cycle [43], the combat network exerts operational capability by forming a CELK of "intelligence obtaining–intelligence processing–commanding and decision–attack and damage" around the target, namely, the OODA kill link. For a more general CELK, the mutual coordination among the intelligence obtaining node O, the intelligence processing node P, and the commanding and decision node D should also be taken into consideration. The flow of generalized CELK with a target can be demonstrated as the generalized combat effectiveness loop (CELP) (see Figure 7).

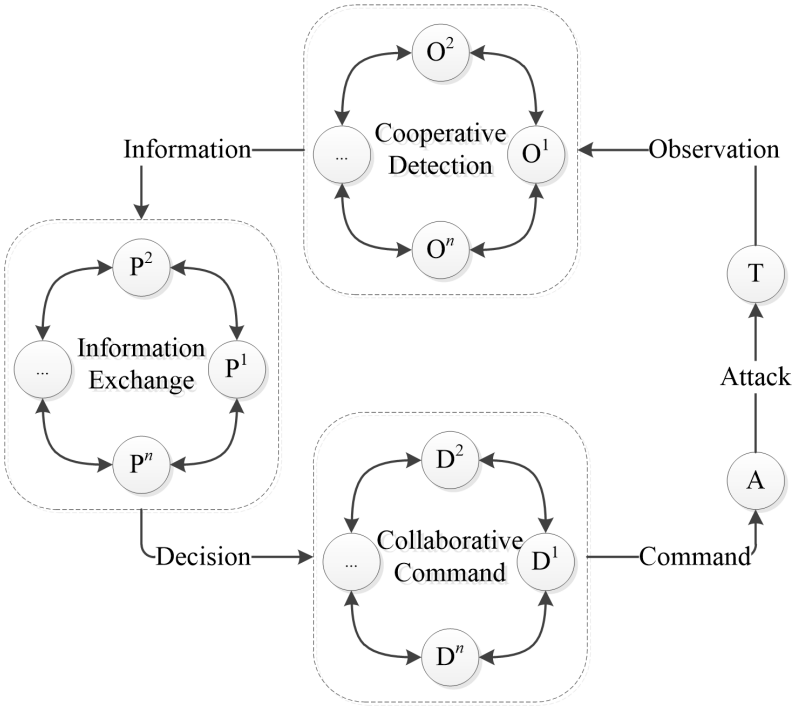


Figure 7. Generalized CELP diagram.

Since the nodes cooperation in generalized CELK may lead to an infinite long link, seven types of CELKs commonly used in practice are selected as the basis for quantity calculation [44]. The detailed description of those CELKs is indicated in Table 2.

Table 2. Seven types of common CELKs and their definitions.

CELK	Definition
O–C–P–C–D–C–A	The standard CELK, including "information obtain–intelligence processing–command and decision–combat response (attack)"
O–C–O–C–P–C–D–C–A	CELK with cooperative detection
O–C–P–C–P–C–D–C–A	CELK with information interaction
O–C–P–C–D–C–D–C–A	CELK with coordinated command
O–C–O–C–P–C–P–C–D–C–A	CELK with cooperative detection and information interaction
O–C–O–C–P–C–D–C–D–C–A	CELK with cooperative detection and coordinated command
O–C–O–C–P–C–P–C–D–C–D–C–A	CELK with cooperative detection, coordinated command and information interaction

The accessibility matrix $\tilde{\boldsymbol{S}}$ of the entire combat network is calculated according to the adjacency matrix $\boldsymbol{S}$ of the functional net:

$$\begin{aligned}(\boldsymbol{S}+\boldsymbol{I})^{(1)} &\neq (\boldsymbol{S}+\boldsymbol{I})^{(2)} \neq \cdots \\ &\neq (\boldsymbol{S}+\boldsymbol{I})^{(r)} = (\boldsymbol{S}+\boldsymbol{I})^{(r+1)} = \tilde{\boldsymbol{S}},\end{aligned} \tag{17}$$

where I is the identity matrix. Equation (17) is the power Boolean operation on $(\boldsymbol{S}+\boldsymbol{I})$, and $r+1$ is the times of power multiplication. The connectivity between intelligence obtaining and attack/damage nodes can be known based on the accessibility matrix. For any node O_{i} and node A_{j}, if $\tilde{\boldsymbol{S}}(i,j)=1$, then O_{i} can reach A_{j} according to a path with practical meaning. Assuming that $\boldsymbol{S}(j,i)=1$, then the number of CELPs is the trace of the product of the corresponding nodes' accessibility matrices, which is also the number of CELKs. Because of the dependency of functional net on the communication net, the information transmission must pass through the communication node, as shown in Figure 2. The CELK should also correspondingly consider the role of communication nodes. Taking the "O→P→D→A" link as an example, the number of this link can be calculated by

$$\begin{aligned}S^{\mathrm{WG}}_{\mathrm{OPDA}}(G) = \mathrm{tr}\{&[\boldsymbol{S}_{\mathrm{OP}} \wedge (\boldsymbol{S}_{\mathrm{OC}} \times \boldsymbol{S}_{\mathrm{CC}} \times \boldsymbol{S}_{\mathrm{CP}})] \times \\ &[\boldsymbol{S}_{\mathrm{PD}} \wedge (\boldsymbol{S}_{\mathrm{PC}} \times \boldsymbol{S}_{\mathrm{CC}} \times \boldsymbol{S}_{\mathrm{CD}})] \times \\ &[\boldsymbol{S}_{\mathrm{DA}} \wedge (\boldsymbol{S}_{\mathrm{DC}} \times \boldsymbol{S}_{\mathrm{CC}} \times \boldsymbol{S}_{\mathrm{CA}})] \times \boldsymbol{S}_{\mathrm{AO}}\},\end{aligned} \tag{18}$$

where $\wedge$ is the Boolean operation of two matrices, that is, if the corresponding element (i,j) in matrix $\boldsymbol{X}$ and $\boldsymbol{Y}$ are both greater than 0, then $\boldsymbol{X}(i,j) \wedge \boldsymbol{Y}(i,j) = 1$. Then, the total number of links is calculated by

$$S_{\mathrm{links}}(G) = \sum_{i=1}^{7} S_{\mathrm{link}_i}(G). \tag{19}$$

The robustness of the combat network in this paper is calculated by relative metrics. For the original combat network G which has not been attacked, the initial largest component scale is $S_{\mathrm{huge}}(G)$. The amount of CELKs is $S_{\mathrm{link}}(G)$. For the attacked combat network G', the corresponding largest component scale and the number of CELKs are $S_{\mathrm{huge}}(G')$ and $S_{\mathrm{links}}(G')$, respectively. We can measure the robustness of the combat network in the following expression:

$$R = \left(\frac{S_{\mathrm{links}}(G')}{S_{\mathrm{links}}(G)}\right)^{\alpha} \left(\frac{S_{\mathrm{huge}}(G')}{S_{\mathrm{huge}}(G)}\right)^{1-\alpha}, \tag{20}$$

where α is a proportion parameter indicating the preference for two different metrics. The default value of α is 0.5.

4.2. Experiment Results and Analysis

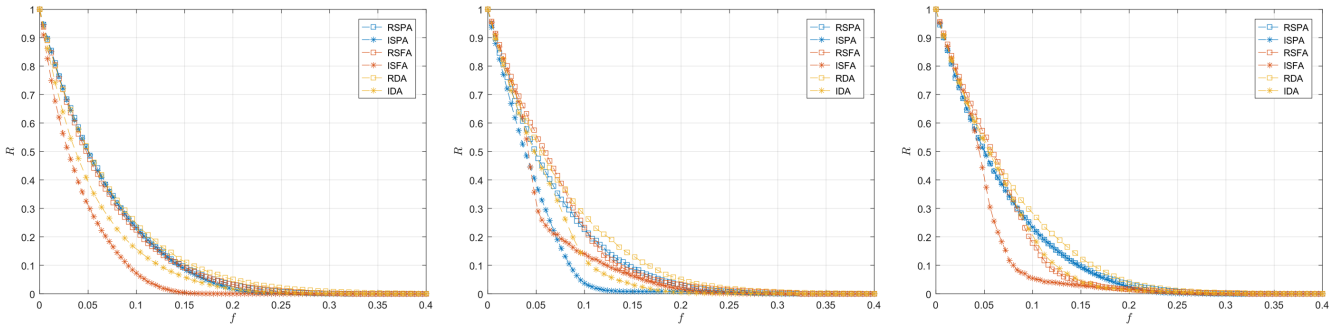
In order to study the robustness of the DGCN of CSOS, the simulation experiment was carried out by using the model network. Model networks such as ER random network [45],

Goh scale-free network with tunable parameter [46], and NW small world network [47] are selected as functional net and communication net, respectively. The network scale of functional net is $N_G = 150$, where $N_O = 50$, $N_P = 40$, $N_D = 30$, $N_A = 30$, and the scale of communication net is $N_W = 100$. As for the parameter setting of the model network, we would like to construct the network close to the real combat network, so the connection probability among different nodes in the ER-net is $p_{OO} = 0.02$, $p_{OP} = 0.03$, $p_{PP} = 0.05$, $p_{PD} = 0.03$, $p_{DD} = 0.05$, $p_{DA} = 0.03$, $p_{AA} = 0.03$, and $p_{CC} = 0.07$. The power exponent of Goh-net is $\beta = 2.3$, and the average degree of the network is $\langle k \rangle = 6$. The functional nodes with different types are connected according to the parameters of the ER-net. The parameters of NW-net are $K = 2$, $p_{OO} = 0.08$, $p_{PP} = 0.1$, $p_{DD} = 0.14$, $p_{AA} = 0.14$, and $p_{CC} = 0.05$. The remaining nodes are also connected according to the parameters of the ER-net. The functional net one-way multiply depends on the communication net, and the scale of group dependency is always 5. To reduce the randomness in the experiment, each type of the above network is repeatedly generated 300 times according to the given parameters. When conducting simulation experiments, unless otherwise specified, the following default parameters are uniformly used: $\tau = 0.6$, $\kappa_G = \kappa_W = 0.5$, $\lambda_G = \lambda_W = 1$, $\gamma_G = \gamma_W = 1.1$, and $\delta_G = \delta_W = 0.3$. The attack mode is IDA (because the enemy tends to attack the combat network by disrupting some specific combat units which contain communication nodes and functional nodes in reality), and the initial failure ratio f ranges from 0 to 0.4.

The simulation software is Matlab 2016b with Windows10, and the hardware configuration is Intel(R) Core(TM) i7-10750H CPU @ 2.60 GHz.

4.2.1. Robustness with Different Attack Modes

On the basis of the default parameters, we change the attack mode to make the nodes fail in the DGCN of CSOS. The combat networks are attacked when the communication net and the functional net are ER-net, Goh-net and NW-net, respectively. To study the influence of asymmetric attack on the robustness of the DGCN of CSOS, the variations of the robustness of the combat networks under six different attack modes are shown in Figure 8. As can be seen from the figure, the robustness of different attack modes with different model network structures is quite different. For attacks on the communication net and when the model network is the ER-net and the NW-net, whether it is a random or intended attack mode, the impact on the robustness of the system is almost the same. When the model network is Goh-net, the deliberate attack on the communication net has the greatest impact on the robustness of the DGCN of CSOS, although the ISFA mode has a better attack effect for a short period of time. For attacks on the functional net and when the model network is the ER net and the NW net, the influence on robustness caused by ISFA mode is the greatest. When the model network is the Goh-net, the effect of ISFA mode is not as good as that of ISPA mode. Generally, deliberate attacks on double-layer networks have an impact on the robustness between that with ISPA mode and ISFA mode. For several types of network models to be attacked in different modes, the influence on the robustness of the combat network is complex, but the common feature is that the impact of deliberate attacks on the robustness is greater than that of random attacks, and random attacks on the double-layer network have a negative impact on the combat network's robustness. Therefore, it is necessary to fully understand the architecture of the attacked object during combat, so that the attack strategy can be reasonably developed to achieve a better combat effect.

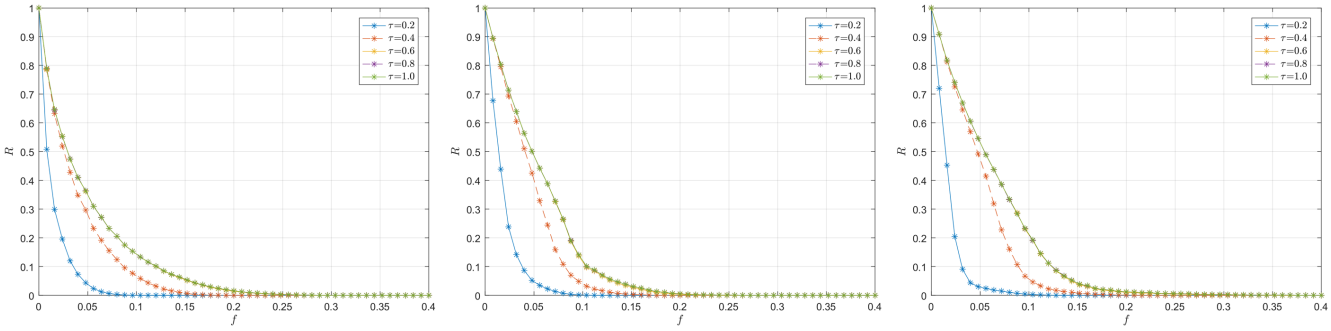


(a)ER (b)Goh (c)NW

Figure 8. Robustness with different attack modes.

4.2.2. Robustness with Different Tolerance Parameter τ

In order to explore the influence of different tolerances on the dependence characteristics of the DGCN of CSOS, the tolerance coefficient is varied in this experiment. Because the dependency scale of the group dependency is always 5, the value of the tolerance coefficient is varying at an interval of 0.2, and the robustness of the DGCN of CSOS when different model networks are used for simulation is shown in Figure 9. It can be seen from the figure that the experiments under the three model networks have a consistent conclusion: the smaller the tolerance coefficient, the worse the robustness of the system. When the tolerance coefficient reaches a certain threshold, there is a certain upper limit for the change of robustness, and the robustness drop curves no longer improve.



(a)ER (b)Goh (c)NW

Figure 9. Robustness with tolerance parameter τ.

4.2.3. Robustness to Different Parameter κ

Changing only the initial load parameters and keeping other parameters stable, we discuss the influence of parameter κ on the robustness of the DGCN of CSOS. Let the load parameter κ_G of the functional net vary from 0.2 to 1.2 at an interval of 0.1, and the parameter κ_W of the communication net also changes according to this rule. Simulation experiments are carried out with different parameters for two different hierarchical networks, and the results are shown in Figure 10. It can be seen from the figure that for the functional subnet, the robustness of the system improves with the increase of κ_G, but the performance improvement is smaller and smaller. When the initial failure ratio is small, the robustness decline curves almost overlap. As the failure ratio increases, the difference becomes obvious. This is because the parameter γ of the node capacity is greater than 1, and the node capacity increases faster as the initial load increases, which appends the remaining capacity. Therefore, the overload cascading failure with a small initial failure ratio is alleviated to a certain extent. However, the robustness curve distinction is not obvious for the combat network with ER-net as the model network. Because the random connection makes the degree distribution more uniform, the node load and capacity are correspondingly more uniform and the difference of attack effect is not obvious. With regard to the communication net, the robustness curves of the DGCN of CSOS almost completely coincide with the

increase of κ_W. This is because the communication net plays the role of intermediary transmission. We found that when R reaches 0 for the first time, the maximal component of the communication net is still larger than the half of initial scale. For these homogeneous nodes of the communication net, as long as the nodes depending on the functional net are still in the maximal component of the communication net, the robustness of the combat network will not change. On the contrary, node failure of the functional net will have a great impact on the robustness.

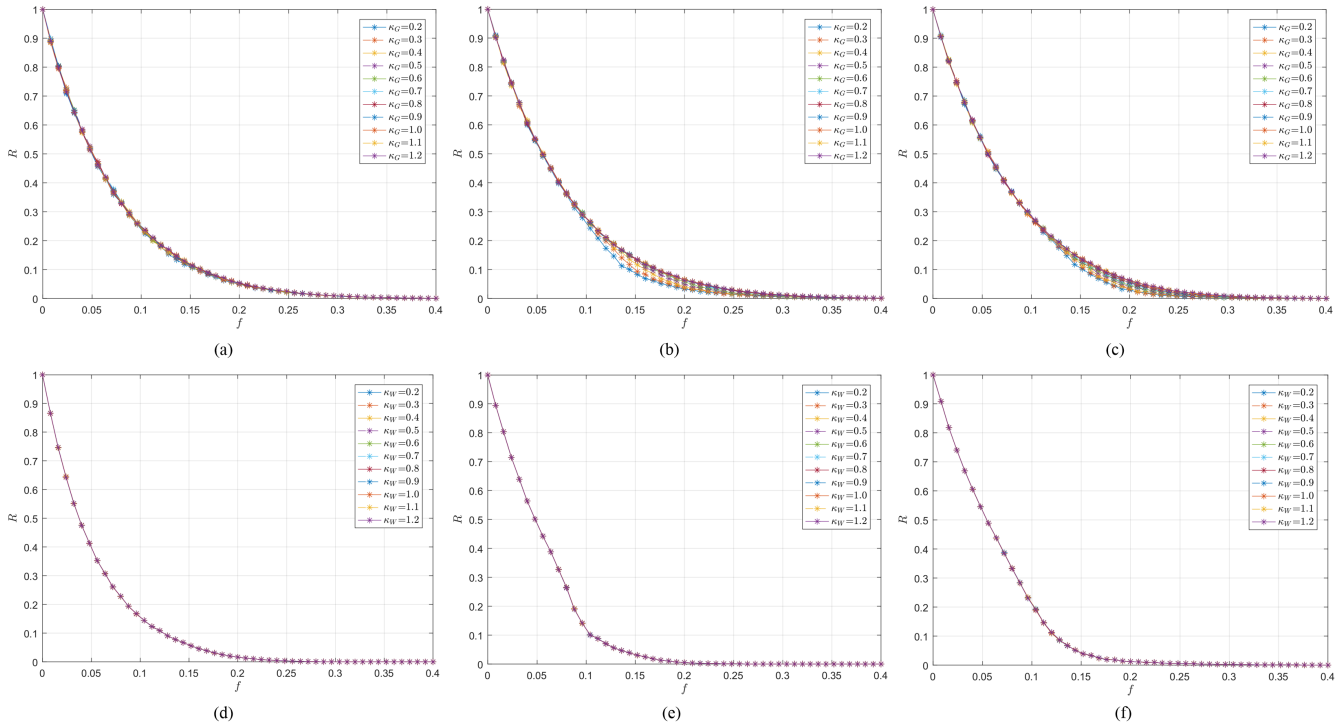


Figure 10. Robustness with different κ. Panels (**a**–**c**) represent the robustness under different κ_G when the subnet is ER-net, Goh-net, and NW-net, respectively; (**d**–**f**) represent the robustness under different κ_W when the subnet is ER-net, Goh-net, and NW-net, respectively.

4.2.4. Robustness to Different Parameter λ

Let the other parameters be fixed apart from the linear parameter of the node capacity. We examine the influence of parameter λ on the robustness of the DGCN of CSOS. Let the parameter λ_G of the functional net change in [0.5, 3] at an interval of 0.5. Similarly, the parameter λ_W of the communication net also varies according to this rule. Simulation experiments are carried out with different parameters for two different hierarchical networks, and the results are shown in Figure 11. It can be seen from the figure that for the functional net, the robustness of the system improves with the increase of parameter λ_G, indicating that increasing the node capacity of the functional net can strengthen the robustness of the system. The magnitude of improvement for different model networks is NW-net $>$ Goh-Net $>$ ER-Net. When the initial failure proportion is small, the robustness-decreasing curves are almost the same, and the proportion of overlap increases with the accumulation of λ_G, indicating that there is an upper limit on the robustness-decreasing curve. As the failure proportion increases, the difference under different conditions is gradually obvious, and then gradually approaches 0 due to the reduction in robustness. For the communication net, the robustness curves of the system almost completely coincide with the increase of λ_W, and the reason is the same as that in Section 4.2.3.

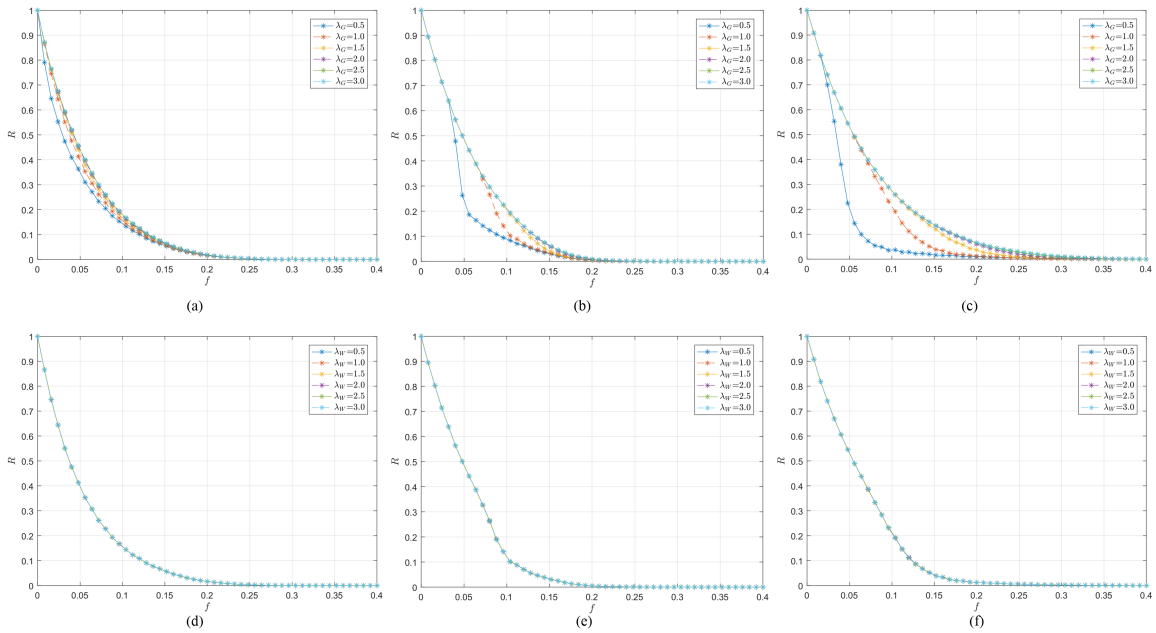


Figure 11. Robustness with different λ. Panels (**a**–**c**) represent the robustness under different λ_G when the subnet is ER-net, Goh-net, and NW-net, respectively; (**d**–**f**) represent the robustness under different λ_W when the subnet is ER-net, Goh-net, and NW-net, respectively.

4.2.5. Robustness to Different Parameter γ

When other parameters remain unchanged, only the nonlinear parameter γ of node capacity is changed, and the influence of this parameter on the robustness of the DGCN of CSOS is investigated. Let the load parameter γ_G of the functional net change in [0.5, 1.2] at an interval of 0.1. Similarly, the parameter γ_W of the communication net also varies according to this rule. Simulation experiments are carried out with different parameters for two different hierarchical networks, and the results are shown in Figure 12. The relevant laws can be analyzed from the figure, and the conclusions are similar to those in Section 4.2.4.

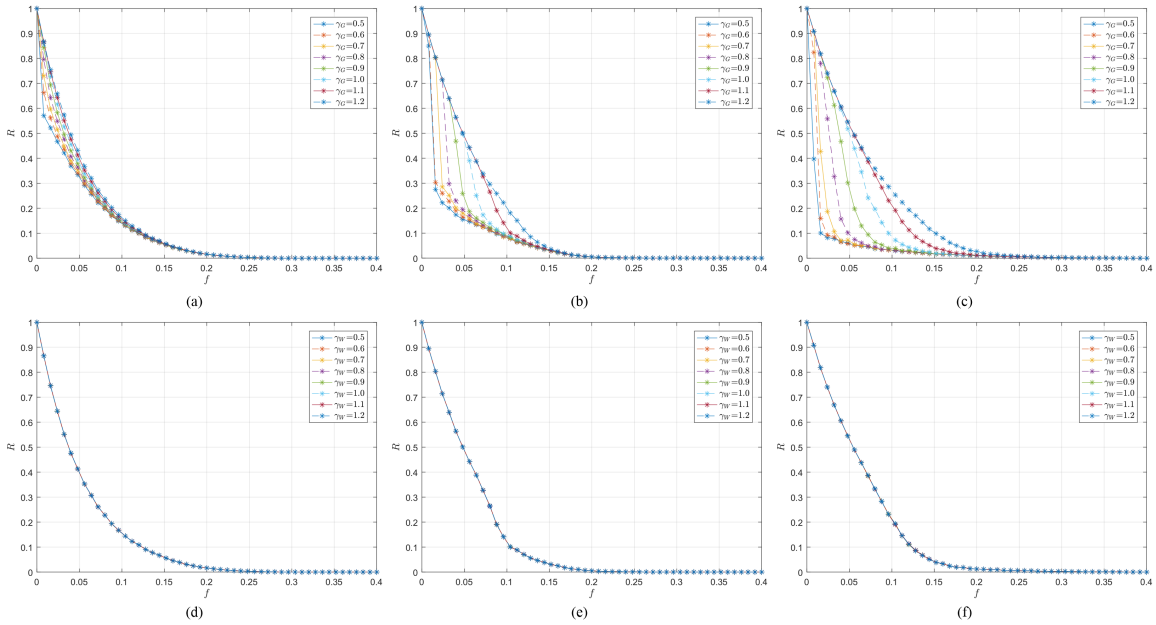


Figure 12. Robustness with different γ. Panels (**a**–**c**) represent the robustness under different γ_G when the subnet is ER-net, Goh-net, and NW-net, respectively; (**d**–**f**) represent the robustness under different γ_W when the subnet is ER-net, Goh-net and NW-net, respectively.

4.2.6. Robustness to Different Parameter δ

Apart from the attack mode, tolerance limit of dependent failure, and parameters of load and capacity, the robustness of the DGCN of CSOS is also affected by the endurance parameter δ. Let the endurance parameter δ_G of the functional net change in [0.1, 0.9] at an interval of 0.1, and the parameter δ_W of the communication net also change according to this rule. Simulation experiments are carried out with different parameters for two different hierarchical networks, and the results are shown in Figure 13. As can be seen from the figure, for the functional net, the smaller the δ_G is, the less robust the combat network is. With the increase of δ_G, that is, the endurance proportion of the overload state increases, the probability of failure in the overload state will decrease. Thus, the robust performance of the system will correspondingly improve. For the communication net, the robustness curves of the system almost completely coincide with the increase of δ_W, and the reason is also the same as that in Section 4.2.3.

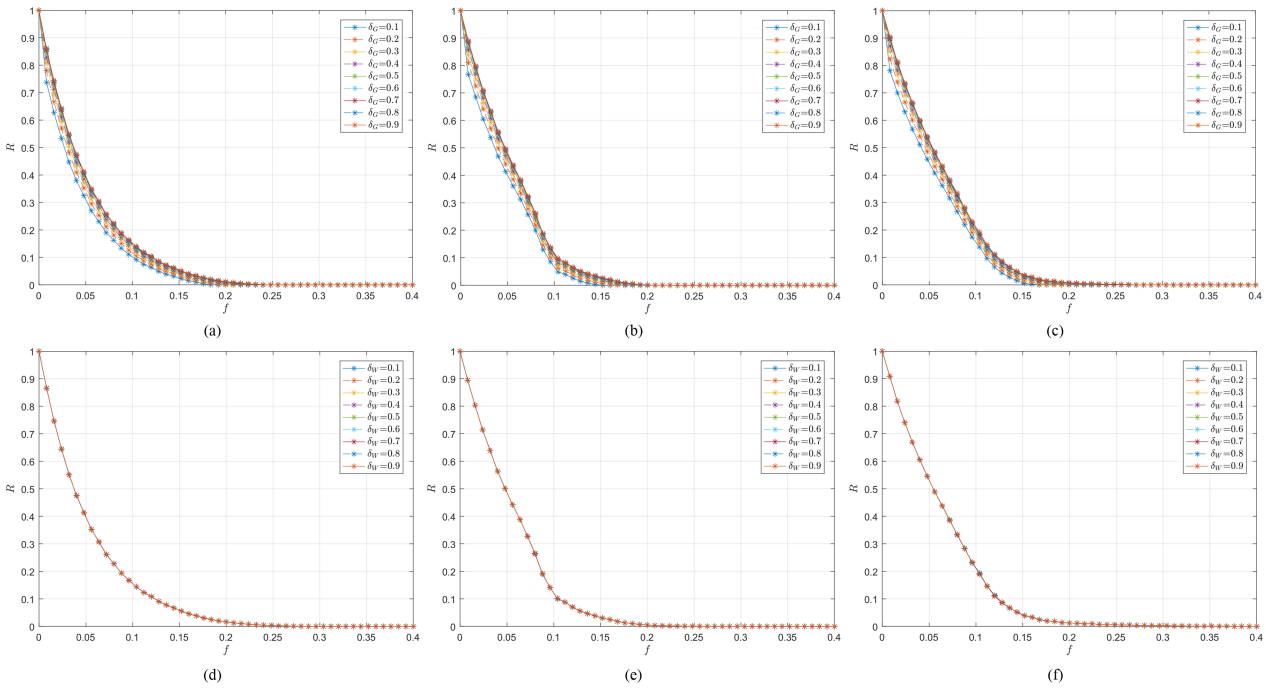


Figure 13. Robustness with different δ. Panels (**a**–**c**) represent the robustness under different δ_G when the subnet is ER-net, Goh-net, and NW-net, respectively; (**d**–**f**) represent the robustness under different δ_W when the subnet is ER-net, Goh-net, and NW-net, respectively.

5. Conclusions

The phenomenon of cascading failure in the DGCN of CSOS will lead to a complete collapse of the system in the face of a relatively small proportion of damage, resulting in the loss of combat effectiveness. Therefore, finding out the reasons that affect the robustness of the combat network and improving the system's capability to further stop the collapse are of great significance. In this paper, we contribute some results as follows:

(1) We established a more realistic combat network model of the DGCN of CSOS.

(2) We designed the cascading failure model of the DGCN by combining the asymmetric dependent failure, conditional group-dependent failure, and overload failure together. We also designed the load reallocation strategy and a more practical robustness index.

(3) We investigated the robustness of the combat network with six different attack modes and different model parameters. The simulation results show that the robustness of the combat network can be effectively improved by improving the tolerance limit of one-way dependency of the functional net, the node capacity of the functional net, and the tolerance of the overload state. When the attack intensity remains steady, the combat network's ability to deal with deliberate attacks is weaker than that with random attacks,

and for different attack methods, different model networks perform inconsistently. It is necessary to design a reasonable network structure to enhance the antidestruction ability of the combat network.

The model established in this paper is more real, and the laws concluded from the simulation experiments have certain reference significance for optimizing the structure of the combat network and improving the robustness of CSOS. The merits and demerits of our method compared with other methods are listed in Table A1. However, there are still some limitations to our study. For one thing, combat networks are modeled statically and only a single type is considered in the overall combat network; for another, there is a lack of data on real combat networks for reasons of secrecy. Therefore, we are going to conduct more research work in the future:

(1) Investigate the impact of collocation of different model networks on robustness;

(2) Obtain the real combat network data in some special situations and verify the effectiveness of the model on real data.

Author Contributions: Conceptualization, J.Y.; methodology, J.Y.; software, J.Y.; validation, J.Y.; formal analysis, J.Y.; investigation, J.Y.; resources, J.Y.; data curation, J.Y.; writing—original draft preparation, J.Y.; writing—review and editing, J.Y. and Y.C.; visualization, J.Y.; supervision, B.X.; project administration, J.Y.; funding acquisition, J.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China under Grant No. 61502522 and National University of Defense and Technology Research Program under Grant No. JS20-10.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to the restricted access to public repositories.

Acknowledgments: The authors would like to express appreciation to the anonymous reviewers and journal editors for their contributions to the smooth publication of this article. The authors also would like to thank the funding support provided by National Natural Science Foundation of China and National University of Defense and Technology.

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

Abbreviations

The following abbreviations are used in this manuscript:

CSOS	Combat system-of-system
HCFN	Heterogeneous combat function
DHDCN	Double-layer heterogeneous dependent combat network
DGCN	Double-layer group-dependent combat network
RSCA	Random single communication network attack
ISCA	Intended single communication network attack
RSFA	Random single functional network attack
ISFA	Intended single functional network attack
RDA	Random double networks attack
IDA	Intended double networks network
CELK	Combat effectiveness link
CELP	Combat effectiveness loop

Appendix A

Table A1. Merits and demerits of the proposed method compared with others.

Method	Merits	Demerits
Our method	Double-layer heterogeneous dependent, more real, the robustness index is close to reality, the cascading failure model is more reasonable.	Lack of examination on real data and research on collocation of different model networks.
Ref. [1–3]	Model construction is quite realistic.	Only considers one layered network.
Ref. [5]	Load redistribution is adjustable.	Parameters are hard to set and the physical meaning is unclear, single layer.
Ref. [7–15]	Studied the cascading failure and robustness of multilayer networks.	Lack of combat meaning of the combat robustness index.
Ref. [16–19]	Extended the cascading failure and robustness analysis to military field.	Lack of combat meaning of the combat robustness index, the one-to-one dependency is too ideal, ignores the critical situation.

References

1. Kinney, R.; Crucitti, P.; Albert, R.; Latora, V. Modeling cascading failures in the North American power grid. *Eur. Phys. J. Condens. Matter Complex Syst.* **2005**, *46*, 101–107. [CrossRef]
2. Wang, Z.F.; Scaglione, A.; Thomas, R.J. A Markov-Transition Model for Cascading Failures in Power Grids. In Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2012; pp. 2115–2124. [CrossRef]
3. Geng, P.; Hao, H.Z.; Yang, A.N.; Liu, Y. Robustness of Complex Networks Considering Load and Cascading Failure under Edge-removal Attack. *arXiv* **2023**, arXiv:2304.01212. [CrossRef]
4. Motter, A.E.; Lai, Y.C. Cascade-based Attacks on Complex Networks. *Phys. Rev. E* **2002**, *66*, 065102. [CrossRef] [PubMed]
5. Duan, D.L.; Wu, J.; Deng, H.Z.; Sha, F.; Tan, Y.J. Cascading failure model of complex networks based on tunable load redistribution. *Syst. Eng.-Theory Pract.* **2013**, *33*, 203–208.
6. Yin, R.R.; Liu, B.; Liu, H.R.; Qian, L.Y. Dynamic fault-tolerance analysis of scale-free topology in wireless sensor networks. *Acta Phys. Sin.* **2014**, *63*, 110205.
7. Yuan, M. A cascading failure model of complex network with hierarchy structure. *Acta Phys. Sin.* **2014**, *63*, 220501. [CrossRef]
8. Ben-Haim, Y. Cascading Failures in Hierarchical Networks with Unity of Command: An Info-gap Analysis. *Int. J. Disaster Risk Reduct.* **2019**, *41*, 101291. [CrossRef]
9. Buldyrev, S.V.; Parshani, R.; Paul, G.; Stanley, H.E.; Havlin, S. Catastrophic cascade of failures in interdependent networks. *Nature* **2010**, *464*, 1025–1028. [CrossRef]
10. Adnan, M.; Khan, M.G.; Amin, A.A.; Fazal, M.R.; Tan, W.S.; Ali, M. Cascading Failures Assessment in Renewable Integrated Power Grids Under Multiple Faults Contingencies. *IEEE Access* **2021**, *9*, 82272–82287. [CrossRef]
11. Zakariya, M.A.Z.; Teh, J. A Systematic Review on Cascading Failures Models in Renewable Power Systems with Dynamics Perspective and Protections Modeling. *Electr. Power Syst. Res.* **2023**, *581*, 108928. [CrossRef]
12. Peng, H.; Zhao, Y.F.; Zhao, D.D.; Zhong, M.; Hu, Z.L.; Han, J.M.; Li, R.C.; Wang, W. Robustness of higher-order interdependent networks. *Chaos Solitons Fractals* **2023**, *171*, 113485. [CrossRef]
13. Smolyak, A.; Levy, O.; Vodenskaand, I.; Buldyrev, S.; Havlin, S. Mitigation of cascading failures in complex networks. *Sci. Rep.* **2020**, *10*, 16124. [CrossRef]
14. Wang, B.C.; Zhang, Z.R.; Qi, X.G.; Liu, L.F. Identify Critical Nodes in Network Cascading Failure Based on Data Analysis. *J. Netw. Syst. Manag.* **2020**, *28*, 21–34. [CrossRef]
15. Shen, Y.; Song, G.H.; Xu, H.L.; Xie, Y.C. Model of node traffic recovery behavior and cascading congestion analysis in networks. *Phys. A Stat. Mech. Its Appl.* **2020**, *545*, 123422. [CrossRef]
16. Guo, X.C.; Ma, R.N.; Wang, G. Modeling and simulation of cascading failure in command and control network. *Comput. Eng.* **2017**, *44*, 294–297.
17. Zhang, Q.; Cao, J.H.; Liang, S.T.; Du, H.D.; Zhang, C. Cascading failure analysis considering load redistribution in equipment support network. *J. Ordnance Equip. Eng.* **2021**, *42*, 86–90.
18. Yang, Y.H.; Li, J.H.; Shen, D.; Nan, M.L.; Cui, Q. Cascading failure model for systematic operations information flowing layered network. *Appl. Res. Comput.* **2017**, *34*, 2099–2103.
19. Wang, Z.; Li, J.H.; Liu, Z.Y.; Kang, D. Modeling and center of gravity analysis for networked information system of system based on function dependency. *Syst. Eng. Electron.* **2021**, *43*, 2876–2883.
20. Lan, Y.S.; Yi, K.; Wang, H.; Mao, S.J.; Lei, M. The model and the analysis method of network centric C^4ISR structure based on super network theory. *Syst. Eng.-Theory Pract.* **2016**, *36*, 1239–1251.

21. Yu, M.G.; Yu, X.H.; Quan, J.C.; Kang, K. Task-oriented and ANP-based requirement satisfactory degree analysis method for net-centric information system-of-systems. *Syst. Eng.-Theory Pract.* **2020**, *40*, 795–806.
22. Tan, Y.J.; Zhang, X.K.; Yang, K.W. Research on networked description and modeling methods of armament system-of-systems. *J. Syst. Manag.* **2012**, *21*, 781–786.
23. Kong, L.W.; Li, M.; Liu, R.R.; Wang, B.H. Percolation on networks with weak and heterogeneous dependency. *Phys. Rev. E* **2017**, *95*, 032301. [CrossRef] [PubMed]
24. Di Muro, M.A.; Buldyrev, S.V.; Stanley, H.E.; Braunstein, L.A. Cascading failures in interdependent networks with finite functional components. *Phys. Rev. E* **2016**, *94*, 042304. [CrossRef] [PubMed]
25. Yuan, X.; Hu, Y.Q.; Stanley, H.E.; Havlin, S. Eradicating catastrophic collapse in interdependent networks via reinforced nodes. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 3311–3315. [CrossRef]
26. Rocca, C.E.L.; Stanley, H.E.; Braunstein, L.A. Strategy for stopping failure cascades in interdependent networks. *Phys. A Stat. Mech. Its Appl.* **2018**, *508*, 577–583. [CrossRef]
27. Wang, H.; Li, M.; Lin, D.; Wang, B.H.; Li, D. Percolation on Networks with Conditional Dependence Group. *PLoS ONE* **2015**, *10*, e0126674. [CrossRef]
28. Wang, H.; Li, M.; Lin, D.; Wang, B.H. Robustness of networks with assortative dependence groups. *Phys. A Stat. Mech. Its Appl.* **2018**, *502*, 195–200. [CrossRef]
29. Zhang, M.; Wang, X.J.; Jin, L.; Song, M. Cascade phenomenon in multilayer networks with dependence groups and hierarchical structure. *Phys. A Stat. Mech. Its Appl.* **2021**, *581*, 126201. [CrossRef]
30. Motter, A.E. Cascade Control and Defense in Complex Networks. *Phys. Rev. Lett.* **2004**, *93*, 098701. [CrossRef] [PubMed]
31. Peng, X.Z.; Yao, H.; Du, J.; Wang, Z.; Ding, C. Load-induced cascading failure in interdependent network. *Acta Phys. Sin.* **2015**, *64*, 048901. [CrossRef]
32. Hao, Y.C.; Li, C.B.; Wei, L. Cascading failure model of complex networks considering overloea nodes. *Syst. Eng. Electron.* **2018**, *40*, 2282–2287.
33. Wang, J.W.; Rong, L.L. A model for cascading failures in scale-free networks with a breakdown probability. *Phys. A Stat. Mech. Its Appl.* **2009**, *388*, 1289–1298. [CrossRef]
34. Kim, D.H.; Motter, A.E. Resource allocation pattern in infrastructure networks. *J. Phys. A Math. Theor.* **2008**, *41*, 224019. [CrossRef]
35. Han, H.Y.; Yang, R.N.; Wang, Z.; Song, X.O. Cascading failure model of asymmetrical interdependent operational networks under edge attack. *J. Harbin Inst. Technol.* **2017**, *49*, 120–125.
36. Hong, C.; Zhang, J.; Wen-Bo, D.U.; Sallan, J.M.; Lordan, O. Cascading failures with local load redistribution in interdependent Watts-Strogatz networks. *Int. J. Mod. Phys. C* **2016**, *27*, 1650131. [CrossRef]
37. Sun, H.J.; Zhao, H.; Wu, J.J. A robust matching model of capacity to defense cascading failure on complex networks. *Phys. A Stat. Mech. Its Appl.* **2008**, *387*, 6431–6435. [CrossRef]
38. Moreno, Y.; Pastor-Satorras, R.; Vazquez, A.; Vespignani, A. Critical load and congestion instabilities in scale-free networks. *Europhys. Lett.* **2003**, *62*, 292–298. [CrossRef]
39. Gao, Y.L.; Chen, S.M.; Nie, S.; Ma, F.; Guan, J.J. Robustness analysis of interdependent networks under multiple-attacking strategies. *Phys. A Stat. Mech. Its Appl.* **2018**, *496*, 495–504. [CrossRef]
40. Di, P.; Hu, T.; Hu, B.; Zheng, J.H. Research on Invulnerability of Combat Net Model Based on Complex Networks. *J. Syst. Simul.* **2011**, *23*, 56–60.
41. Deng, Y.; Wu, J.; Tan, Y.J. A fast connected component algorithm based on hub contraction. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Budapest, Hungary, 9–12 October 2016; pp. 66–69.
42. Zhao, D.L.; Tan, Y.J.; Li, J.C.; Dou, Y.J.; Li, L.C.; Liu, J.Y. Research on structural robustness of weapon system of systems based on heterogeneous network. *Syst. Eng.-Theory Pract.* **2019**, *39*, 3197–3207.
43. Boyd, J.R. *A Discourse on Winning and Losing*; Air University Press: Maxwell AFB, AL, USA, 2018.
44. Yu, J.T.; Xiao, B.; Xiong, J.J. Capability Evaluation of Early Warning Intelligence System-of-Systems Based on Intelligence Effectiveness Loop. *Fire Control Conmand Control* **2022**, *47*, 32–36.
45. Erdos, P.; Renyi, A. On the evolution of random graphs. *Trans. Am. Math. Soc.* **1984**, *286*, 257.
46. Goh, K.; Kahng, B.; Kim, D. Universal behavior of load distribution in scale-free networks. *Phys. Rev. Lett.* **2001**, *87*, 278701. [CrossRef] [PubMed]
47. Newman, M.; Watts, D.J. Renormalization group analysis of the small-world network mode. *Phys. Lett. A* **1999**, *263*, 341–346. [CrossRef]