Hindawi
Security and Communication Networks
Volume 2018, Article ID 6063837, 14 pages
https://doi.org/10.1155/2018/6063837

Research Article

A Cascading Failure Model for Command and Control Networks with Hierarchy Structure

Xiue Gao,[1,2] Duoping Zhang,[2] Keqiu Li,[1] and Bo Chen[2]

[1]*School of Computer Science and Technology, Dalian University of Technology, Dalian, Liaoning 116024, China*
[2]*School of Information Engineering, Dalian University, Dalian, Liaoning 116622, China*

Correspondence should be addressed to Bo Chen; chenbo20040607@126.com

Received 3 November 2017; Revised 12 January 2018; Accepted 20 February 2018; Published 26 March 2018

Academic Editor: Alessandro Cilardo

Cascading failures in the command and control networks (C2 networks) could substantially affect the network invulnerability to some extent. In particular, without considering the characteristics of hierarchy structure, it is quite misleading to employ the existing cascading failure models and effectively analyze the invulnerability of C2 networks. Therefore, a novel cascading failure model for command and control networks with hierarchy structure is proposed in this paper. Firstly, a method of defining the node's initial load in C2 networks based on hierarchy-degree is proposed. By applying the method, the impact of organizational positions and the degree of the node on its initial load could be highlighted. Secondly, a nonuniform adjustable load redistribution strategy (NALR strategy) is put forward in this paper. More specifically, adjusting the redistribution coefficient could allocate the load from failure nodes to the higher and the same level neighboring nodes according to different proportions. It could be demonstrated by simulation results that the robustness of C2 networks against cascading failures could be dramatically improved by adjusting the initial load adjustment coefficient, the tolerance parameter, and the load redistribution coefficient. And finally, comparisons with other relational models are provided to verify the rationality and effectiveness of the model proposed in this paper. Subsequently, the invulnerability of C2 networks could be enhanced.

1. Introduction

With the constant evolution of information warfare, C2 networks have become the nerve center of the information warfare system in the confrontation environment. On the one hand, it is the key to the victory in the war; on the other hand, it is also the primary target during enemy attacks [1]. To meet the needs of information warfare, C2 networks construct a complex network with the structure of vertical integrations and horizontal interconnections by connecting various command and control nodes [2]. Moreover, it has been shown that C2 networks have the characteristics of scale-free properties, load distribution hierarchy, large gap of node importance [3], and so forth. However, the complexity of C2 networks has also increased the vulnerability of the network. In particular, if the local node has random failures or is under targeted attacks, it may significantly affect the entire network due to the cascade mechanism effect. As a result, the whole network would crash [4–6]. Therefore, the cascading failure has become the focus of network research to improve the invulnerability for C2 networks.

The network cascading failure model with theoretical analysis was firstly proposed by Motter and Lai [7] in 2002. They focused on the cascading failures for scale-free networks and built the first cascading failure model. For concreteness, the initial load of the node is quantified according to its betweenness, and the relationship of load-capacity is linear. After that, many subsequent scholars named the cascading failure model built by Motter and Lai as the ML model. Moreover, they revealed that cascading failures are more likely to occur in the scale-free network under targeted attacks. Under this theoretical framework, scholars have carried out the research on cascading failures in the power transmission network [8–10], traffic network [11–13], Internet [14], military network [15], infectious diseases network [16–18], and so on. In addition, various methods of defining the

initial load of the node and the load redistribution strategy are applied for different networks. Thus, the invulnerability and robustness of the network have been improved.

The major research on cascading failures includes the cascading failure model [19–24], cascade control and defense strategies [25–30], the different attack modes of cascading failures [31–33], and so forth. In particular, the cascading failure model is the most popular research for C2 networks cascading failures. It introduces the definition of initial load and capacity of the node, the load redistribution strategy for failure nodes, the effect of different attack strategies on network cascading failure, and invulnerability evaluation for network cascades. In most of the existing cascading failure models, the initial load of the node is defined according to its importance, compared to the previous initial load which is defined by degrees, betweenness, and its functions [30, 34–36]. The current strategy of allocating load from the failure node is mainly based on local information, namely, allocating the load from the failure node to its neighboring nodes [6, 12, 20, 30, 33]. And there are also some literature sources that allocate the load from the failure node according to global information, this is, recalculate the real-time load of each node based on the shortest path [7, 37, 38]. Hu et al. [37] investigated model for cascading failures with adaptive defense in complex networks by considering interplay between the flow dynamic and the network topology and reallocated the load from overload nodes according the shortest-hop path, which is different form the reallocation strategy distributing the load from failure nodes to their neighbors. This research is of creativity and practical engineering value.

In the field of C2 network cascading failure research, Zhu et al. [38] constructed a C2 network cascading failure model by defining the node initial load based on betweenness. Subsequently, the load from the failed node could be redistributed according to the global routing rule. Zhang et al. [39] came up with a method to define the initial load by considering both the command level and the degree of the node, and they redistributed the load from the failure node to its neighboring nodes based on their spare capacity, which is the conventional load redistribution strategy adopted by most of the cascading models. Based on the analysis of the structure and characteristics of the campaign logistic network, an optimization model for node capacity is proposed by Li et al. [40]. However, this optimization model is not applicable to C2 networks because of the campaign logistic network is random. Moreover, the cascading failure mode was established for military information grid (MIG) in [41], which introduced the cost punish function and the definition of mainstay nodes. Furthermore, the authors verified that the ability of MIG to resist cascade failure could be enhanced significantly by improving the capacity of a few mainstay nodes. Zhang et al. [42] designed the cascading failure model for C^4ISR system structure and they proposed the method for calculating dynamic invulnerability, which focused on the description of attacking models and the calculation methods of the dynamic invulnerability. In addition, since hierarchy structure is quite common in real networks, Yuan [43] proposed a cascading failure model for the complex network with hierarchy structure. In particular, the selected hierarchy network model has a tree-shape backbone and various random hidden linkages. Thus, it is of great significance for researching the cascading failures of C2 networks. Moreover, in order to investigate the invulnerability of the interdependent network against cascading failures, an improved nonlinear load-capacity model was proposed in [35, 36]. Han et al. [44] constructed two-layer interdependent C2 networks by coupling two independent subnets randomly and studied its cascading failures. However, as a result of a typical WS small word and BA scale-free network, the subnet does not comply with the structural characteristics of C2 networks. Wang et al. [45] established a cascading model for the functionally identical coupled network. In addition, they studied the invulnerability of two coupled scale-free networks, two coupled random networks, and scale-free networks. However, these coupled networks are inconsistent with the characteristics of C2 networks.

Some achievements have been made in the research of cascading failures in complex networks and C2 networks. However, these cascading failure models do not consider the characteristics of strict command hierarchy in C2 networks. Therefore, there are two major limits in these models. On the one hand, there is no relationship between the command hierarchy and the degree; the top command nodes are in the most essential positions according to the hierarchical characteristic of C2 networks, but their degrees and betweenness are not as maximized as we expect. Furthermore, the betweenness of leaf nodes at the bottom is zero. Thus, it is inaccurate to indicate the initial load of the node in C2 networks by node importance, such as degree, betweenness, or simply its function. On the other hand, the C2 network studied in this paper is an abstract of the command relation network based on the military organizational system, rather than the communication infrastructure network. There are various command relationships in C2 networks, which include step-level command, leapfrog command, and cooperative command. Each node in C2 networks has its own organizational position and engagement capability; this is, the capacity of each node matches its organizational position. Therefore, the low-level command nodes cannot bear the load or function from the high-level nodes. In that manner, it is quite difficult to apply the conventional load redistribution strategy to C2 networks. Inspired by the above discussion, in this paper, a cascading failure model for C2 networks with hierarchy structure is proposed. Compared with the existing results, the main contributions of this paper are concluded as follows:

(i) a novel cascading failure model for C2 networks with hierarchy structure is proposed in this paper.

(ii) Based on hierarchy-degree, a method of defining the initial load of the node in C2 networks is proposed. By changing the initial load adjustment coefficient, the impact of organizational positions and degree of the node on the initial load and the network invulnerability could be adjusted.

(iii) A nonuniform adjustable load redistribution strategy (NALR strategy) is put forward in this paper. In particular, adjusting the redistribution coefficient could

allocate the load from failure nodes to the higher and same level neighboring nodes based on different proportions.

(iv) We investigated the influence of model parameters on the cascading failure in C2 networks, and the results show that optimal model parameters could enhance the invulnerability of C2 networks. Moreover, the comparisons with other relational models are provided to verify the rationality and effectiveness of the model proposed in this paper.

(v) The cascading failure model proposed in this paper would better reflect the network invulnerability against both failure and attack, and it provides a theoretical basis for designing and optimizing the structure of C2 networks.

For the convenience of our narration in this paper, we built a C2 network with reference to [2, 3, 34, 44], the process is epitomized as follows: The establishment of C2 networks must meet the operational needs and follow the objective laws of the military commanders. And the performance of this law on network model is that the C2 network has a reasonable span and hierarchical structure. The command hierarchy refers to the number of vertical hierarchical structures in C2 network, and the span refers to the number of subordinate command nodes subject to a superior command node. Following the above basic law, the command entities are abstracted into nodes, and the relationships between entities are abstracted as edges, so the command and control system is abstracted into a C2 network. For a given C2 network, $G = (V, E)$ described by the sets of nodes V and links E. More specifically, $V = \{v_1, v_2, \ldots, v_n\}$ describes the set of all levels of command entities, and the total number of nodes is n; $E = \{e_1, e_2, \ldots, e_m\}$ describes the different organizational relationships, which include command relationships and cooperative relationships, and the total number of links is m. Furthermore, the command relationship includes step-level command and leapfrog command. Meanwhile, the cooperative relationship contains internal and external collaboration. For those nodes at the same level, if there is a cooperative relationship between two nodes, then there is a link between them; otherwise, there is no link. For those command nodes at different levels, if there is a commanding relationship between two nodes, then there is a link between them; otherwise, there is no link. Obviously, there is at most one link between any two nodes.

The rest of the paper is organized as follows: Section 2 describes the cascading failure model and the dynamic process in detail. In Section 3, we investigate the effect of the model parameters on C2 networks invulnerability and compare this cascading failure model with other five models. Experimental validation and results are given. Finally, the conclusion of this paper is presented in Section 4.

2. The Cascading Failure Model for C2 Networks

2.1. Definition of Initial Load and Capacity of the Node. Most of the existing cascading failure models directly quantify the initial load of the node according to its degree or betweenness; this quantification method is suitable for telecommunication network, power grid, or social network. However, the C2 network studied in this paper is an abstract of the organizational relationship network based on the military organizational system, rather than the communication infrastructure network. For example, five brigades were subject to a division, and four regiments were subject to a brigade. The load in the model represents the campaign assignment, rather than the information flow. Moreover, due to the obvious hierarchy structure in C2 networks, the nodes at different levels have distinguished importance. In addition, as a result of the leapfrog and collaboration command relationship, there is no obvious relationship between the command hierarchy and degree; the degree is not necessarily bigger when the command hierarchy of a node is higher. Similarly, the degree of node in lower layer is not necessarily small. Therefore, the method of quantifying the initial load according to node's degree or betweenness is not suitable for the C2 networks. It is necessary to introduce the command hierarchy to define the initial load and capacity of the node. Therefore, a hierarchy-degree based method of defining the node's initial load in C2 networks is proposed in this paper. Moreover, this method considers the topology of the network and the organizational position of the node. The initial load $F_i(0)$ of the node v_i could be expressed as

$$F_i(0) = \alpha \times k_i^{\lambda} + (1 - \alpha) \times (D + 1 - d_i)^{\gamma}, \quad (1)$$

where k_i and d_i represent the degree and the command hierarchy of the node v_i, D represents the total command hierarchy of the C2 networks, α, λ, and γ denote the initial load adjustment coefficients, which control the effect of node degrees and organizational positions on the initial node load, $\lambda, \gamma \in [0, \infty)$ and $\alpha \in [0, 1]$. In addition, the hierarchy of initial load could be adjusted by $1 - \alpha$. In particular, a larger value of $1 - \alpha$ would lead to a higher proportion of the network hierarchy in the load definition. Consequently, the hierarchy of the network load distribution would become more obvious. When $\alpha = 0$, the initial load of the node could be defined according to the node's organizational position. However, when $\alpha = 1$, it has been shown that the initial load of the node could only be affected by degrees, regardless of its organizational position.

The capacity of the node is determined based on the ML model. Assume that the capacity C_i of node v_i is linearly proportional to its initial load $F_i(0)$. Therefore, it could be expressed by

$$C_i = (1 + \beta) \times F_i(0), \quad (2)$$

where $\beta \geq 0$ is the tolerance parameter, which measures the node capacity surplus and indicates the network cost. It could be observed that a larger value of β would indicate a bigger capacity surplus and a stronger ability to bear the load for the particular nodes. Therefore, a higher cost of the node and network implies stronger invulnerability of the C2 networks.

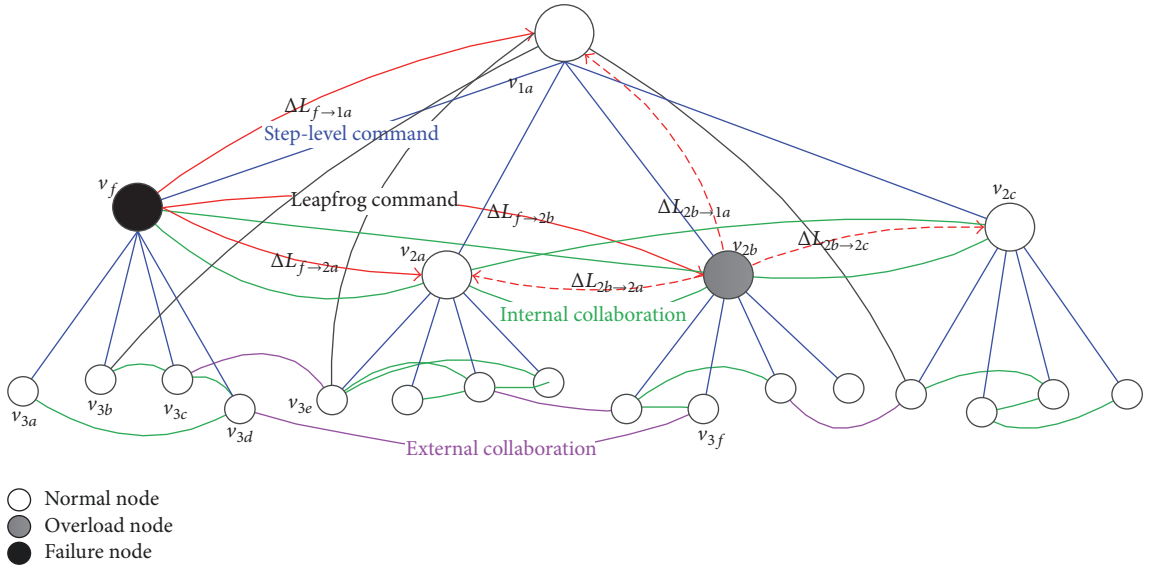

Figure 1: The illustration of the load redistribution for the failure node.

2.2. Load Redistribution for the Failure Node

2.2.1. Load Redistribution Process for the Failure Node. C2 networks have a strict hierarchical structure. In other words, in accordance with certain rules, the load from failure nodes could be distributed to the nodes at the same or upper level. On the contrary, the lower command node could not fully share the load from the upper node, which causes the failure node to reallocate the load to the entire network. Therefore, only the redistribution to the same or higher level is discussed in this paper and the redistribution process could be demonstrated in Figure 1.

If any command node v_f failed, it shows that the current combat unit cannot complete the existing campaign assignment independently, or the combat unit no longer has the ability to accomplish the task. Thus, it needs to assign the current campaign assignment to other combat units. Each node in C2 networks has its own engagement capability, which matches its organizational position; lower-level command nodes may not be able to assume the load or function of higher-level nodes, and the low-level command nodes cannot bear the load or function from the high-level nodes. Thereofe, the load on the v_f would only be transferred to the neighboring nodes at upper and same levels (red real arrows in Figure 1). In particular, the higher or the same level nodes v_{ix} $(i = 1, 2, 3, \ldots;\ x = a, b, c, \ldots)$ receive the incremental load $\Delta L_{f\to ix}$ from the failure node v_f. For example, if the node v_f fails, its immediate subordinate node $v_{3a} \sim v_{3d}$ would accept the leapfrog command from the upper-level node v_{1a} or accept the transfer command from the same level nodes v_{2a} and v_{2b}. However, the concrete application cases shall depend on the actual battlefield environment and the combat missions.

After the neighboring node v_{2b} bears the load from the failure node, its real-time load $F_{2b}(t+1)$ could be expressed as

$$F_{2b}(t+1) = F_{2b}(t) + \Delta L_{f\to 2b}, \tag{3}$$

where $F_{2b}(t)$ denotes the load of the node v_{2b} at the previous time. If the load of the node v_{2b} exceeds its capacity limit, that is,

$$F_{2b}(t+1) > C_{2b}, \tag{4}$$

the node v_{2b} would also fail, which triggers the cascading failure process and causes a new round of load redistribution (red dashed line in Figure 1). Otherwise, if $F_j < C_j$, the node v_j would not fail. To identify the failure nodes, comparisons between the real-time load and the capacity are carried out for each node, until there is no failure node in the network.

2.2.2. Nonuniform Adjustable Load Redistribution Strategy. Based on the redistribution process for the failure node mentioned above, it could be observed that load from the failure node could not be efficiently allocated to its neighboring nodes due to the strict hierarchical characteristics of the C2 networks. Therefore, a nonuniform adjustable load redistribution strategy is proposed in this paper, which allocates load from the failure node to the neighboring nodes at the higher and the same level only. In other words, given any failure node v_f, its load F_f would be allocated to the nonfailed nodes at the higher and same level. This process is based on the proportional coefficient $F(c_j, \eta, C_{j,k})$, which could be expressed by

$$F\left(c_j, \eta, C_{j,k}\right) = \begin{cases} \dfrac{C_j}{\sum_{m\in\Gamma_d} C_m} & \Gamma_s = \varnothing,\ \Gamma_d \neq \varnothing \\ \eta \dfrac{C_j}{\sum_{m\in\Gamma_d} C_m} + (1-\eta)\dfrac{C_k}{\sum_{n\in\Gamma_s} C_n} & \Gamma_s \neq \varnothing,\ \Gamma_d \neq \varnothing \\ \dfrac{C_k}{\sum_{n\in\Gamma_s} C_n} & \Gamma_s \neq \varnothing,\ \Gamma_d = \varnothing, \end{cases} \tag{5}$$

where Γ_s denotes a set of nodes connected to the failure node at the same level, Γ_d denotes a set of nodes connected

to the failure node at the upper level, C_j and C_k represent the capacities of the neighboring nodes at the corresponding level, and $\eta \in (0, 1)$ is the load redistribution coefficient. In particular, a larger value of η would increase the possibility of allocating the load to higher-level nodes. When $\Gamma_s = \varnothing$ and $\Gamma_d \neq \varnothing$, the failure node has no neighboring node at the same level and the load could only be allocated to the neighboring nodes at the higher level. When $\Gamma_s \neq \varnothing$ and $\Gamma_d \neq \varnothing$, the failure node has neighboring nodes at both the same and higher level, and the load would be allocated based on the command ability of upper-level nodes and the cooperative strength of same level nodes. When $\Gamma_s \neq \varnothing$ and $\Gamma_d = \varnothing$, the failure node has no neighboring nodes at the upper level, and the load could only be allocated to the neighboring nodes at the same level. Therefore, the model above takes both the impact of the step-level command ability and the cooperative strength on the load distribution of the failure node into consideration. Furthermore, the weight of influencing factors could be adjusted based on the coefficient η.

Based on the load distribution strategy for failure nodes mentioned above, any neighboring node v_j at the same or upper level for the failure node v_f would get the incremental load $\Delta L_{f \to ix}$, which could be shown as

$$F_j \longrightarrow F_j' = F_j + \Delta F_{f \to j} = F_j + F_f \cdot F\left(c_j, \eta, C_{j,k}\right). \quad (6)$$

Due to the load distribution of the failure node, the load of all nonfailed nodes in the network would be updated for one time. If the load and capacity of the node v_j satisfy (4), it would indicate the failure of the neighboring node v_j, which causes a cascade failure process as demonstrated in Figure 1.

2.3. Invulnerability Measures for Cascading Failures. In this paper, the node survival rate is employed to measure the invulnerability of C2 networks. Moreover, the measure of node survival rate G is defined as follows [6–8, 11]:

$$G = \frac{N'}{N}, \quad (7)$$

where N denotes the number of nodes in the network at the initial time and N' denotes the number of nodes working normally in the network after the termination of a cascade failure. With the consideration of cascading impacts, it could be observed that a larger G would imply less damage caused by the attack on the network. Therefore, the network would perform with better invulnerability.

However, the above indicator evaluates the network ability of resisting cascade failures only in terms of the number of survived nodes in the network. Apparently, they do not consider the ability of bearing the load for each node after each cascade. To tackle this problem, the network bearing capacity CF is presented in this paper, which measures the cascade invulnerability of C2 networks. Moreover, it could be calculated by

$$CF = \frac{\sum_{i \in V} (C_i - F_i)}{\text{Con}\, F}, \quad (8)$$

where F_i and C_i represent the real-time load and initial capacity of the node v_i, V denotes the set of nonfailed nodes, and $\text{Con}\, F$ denotes the sum of initial load for all nodes in C2 networks. It could be observed that a larger value of CF would improve the efficiency of the load redistribution strategy. Meanwhile, the cascade effect caused by the failure nodes would become weaker and the invulnerability of C2 networks would be improved as well.

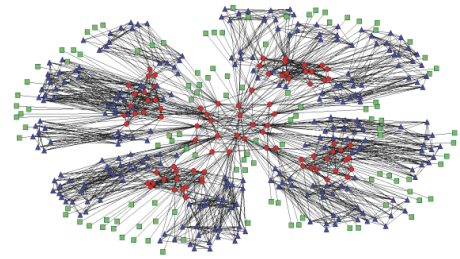

Figure 2: A typical C2 network model.

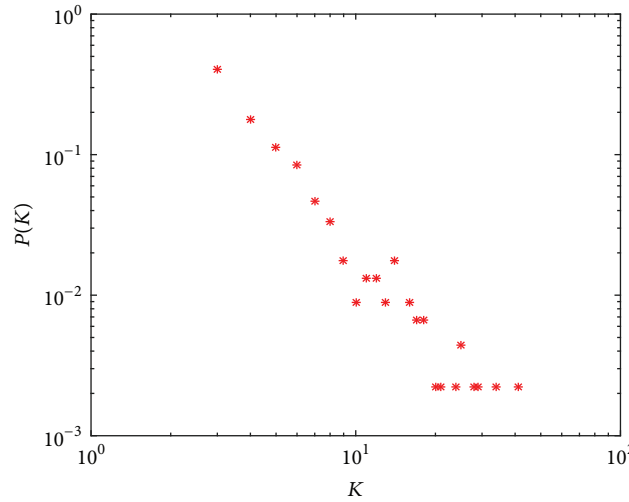

Figure 3: The degree distribution of the C2 network.

3. Experimental Results and Analyses

Figure 2 illustrates a typical C2 networks model, which is constructed to verify the validity and feasibility of the cascade failure model with the hierarchical structure. In this experiment, the network command level is $D = 5$, the span is $S = 4$, and the total number of nodes is $N = 453$, with 85 command nodes (red circles), 256 fire strike nodes (blue triangles), and 112 sensor nodes (green boxes).

It has been extensively verified that the C2 network is a scale-free network [46], in which the majority of nodes have smaller degrees compared to a few nodes with high degrees. Figure 3 demonstrates the degree distribution of the C2 networks constructed in this paper. It could be identified from the figure that the node degree has the scale-free characteristic in this model, which is consistent with the literature [46]. Therefore, it implies that the C2 networks model established in this paper is appropriate.

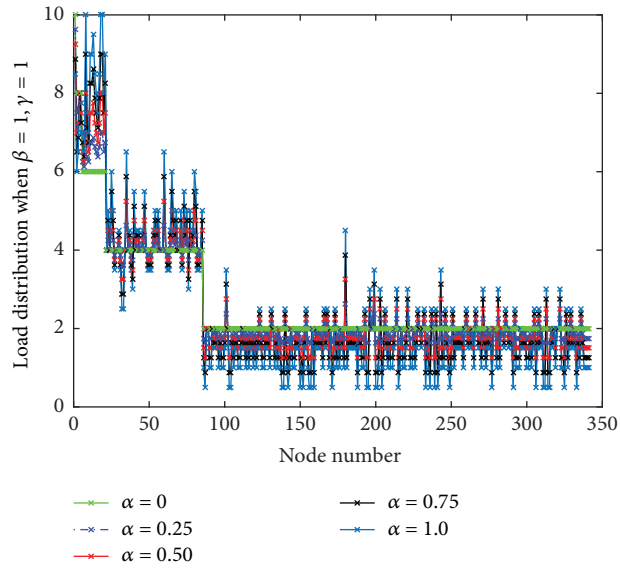

Figure 4: The initial load of the node varies with the coefficient α.

3.1. Effect of Coefficient α on the Network Invulnerability. In the C2 networks with the initial load adjustment coefficient α, parameters λ and γ are initialized as 1 in order to analyze the variation trend of the initial load of the node. When the coefficient α changes values from the set $\{0, 0.25, 0.5, 0.75, 1\}$, the distribution of initial load for node could be collected and shown in Figure 4.

It could be observed from Figure 4 that when $\alpha = 0$, the initial load of each node is determined by its level. In other words, the initial load of each node is positively correlated with the node level. In addition, the load curve demonstrates a significant hierarchical characteristic for the C2 networks. When $\alpha = 1$, the initial load of each node depends on the node degree only, which does not depend on its level anymore. In this case, the load distribution demonstrates no hierarchical characteristics for the C2 networks. When $0 < \alpha < 1$, the initial load of each node is determined by the node degree and its hierarchy. In particular, the smaller value of α would imply the more obvious hierarchy of the initial load. However, because of the differences in topology, the initial load of each note at the same level is different. Consequently, the value of α could never be set to 0. When $\alpha > 0.75$, there is no obvious hierarchical characteristic for the initial load. When $0 < \alpha < 0.75$, the initial load of C2 networks demonstrates obvious hierarchical characteristics, which is consistent with the characteristics of C2 networks.

In order to analyze the impact of the coefficient α on network resistance-cascading failures, some analyses of C2 networks under attacks are carried out. In particular, the invulnerability is measured by both the node survival rate G and network bearing capacity CF, and the other coefficients are initialized as $\lambda = \gamma = 1$, $\beta = 0.15$, $\eta = 0.5$. Figure 5 shows the changing trend of cascading invulnerability in C2 networks along with attacking ratios for different values of α, where 50 rounds of simulations and average calculations are carried out.

It could be observed from Figure 5 that the network performance declined gradually with the increase in the attack ratio p. In particular, when $p > 0.2$, almost all nodes in the C2 networks failed as a result of the cascading effect. When the coefficient α is small, the initial load and capacity of the node are mainly determined by the hierarchy. Moreover, these nodes with big degree could not acquire large capacity, so they might fail as a result of receiving excessive load in the cascade process. When the coefficient α is large, the initial load and the capacity of the load are mainly determined by the degree. In that case, the high-level nodes with small degrees are more likely to fail because of overloading. Meanwhile, the cascade process would be transported to the high level, and the failure scale will increase. Therefore, when the coefficient α in (1) reaches the threshold value α_T, the C2 network has the strongest ability to resist cascade failures.

3.2. Effect of Coefficients λ and γ on the Network Ability to Resist Cascade Failures. To analyze the impact of initial load adjustment coefficients λ and γ on the ability to resist cascading failures, the values of the coefficients λ and γ are chosen from the range $[0, 2]$. And the other parameters are fixed with $\alpha = 0.25$, $\beta = 0.15$, $\eta = 0.5$, $p = 0.15$. Figure 6 demonstrates the trend of C2 networks cascading invulnerability with different coefficients λ and γ, where 50 rounds of simulations and average calculations are carried out.

It could be observed from Figure 6 that with the variation of the coefficients λ and γ, there is no obvious monotony in the node survival rate and the node bearing capacity. Meanwhile, when both λ and γ are larger than 1, the robustness of C2 networks against cascading failures would be improved significantly. Tables 1 and 2 show the largest four sets of data.

It could be concluded that when the other parameters are constant, the optimal values of λ and γ would better reflect anti-cascade failure ability for C2 networks. In particular, under the current parameter setting, the corresponding optimal values of (λ, γ) are (1.34, 1.67) and (1.28, 1.56), which are calculated by the weighted average method when the indices G and CF reach maximum.

3.3. Effect of Coefficient η on Network Resistance-Cascading Failures. To analyze the impact caused by the load redistribution coefficient η on C2 networks resistance-cascading failures, G and CF are still employed to measure cascading invulnerability of C2 networks. The value of the coefficient η is chosen from the range $[0, 1]$ and the other parameters are initialized as $\alpha = 0.25$, $\beta = 0.15$, $\lambda = 1.3$, $\gamma = 1.6$, $p = 0.15$. Figure 7(a) shows the trend of C2 networks cascading invulnerability with different coefficients η, where 50 rounds of simulations and average calculations are carried out. Meanwhile, Figure 7(b) shows the relationship between the network invulnerability and attacking ratio p with different coefficients η.

According to the analysis of Figure 7(a), the network invulnerability improves gradually with the increase in the coefficient η. It could be concluded that it is more likely to allocate the load to the higher node with a larger value

Table 1: The value of γ and λ when G is maximum.

	The 1st group	The 2nd group	The 3rd group	The 4th group
G	0.9789	0.9783	0.9780	0.9774
(λ, γ)	(1.6, 1.6)	(1.4, 1.8)	(1.2, 1.4)	(1.0, 1.9)

Table 2: The value of γ and λ when CF is maximum.

	The 1st group	The 2nd group	The 3rd group	The 4th group
CF	0.2332	0.2320	0.2315	0.2218
(λ, γ)	(1.4, 1.5)	(1.2, 1.8)	(0.9, 1.4)	(1.6, 1.8)

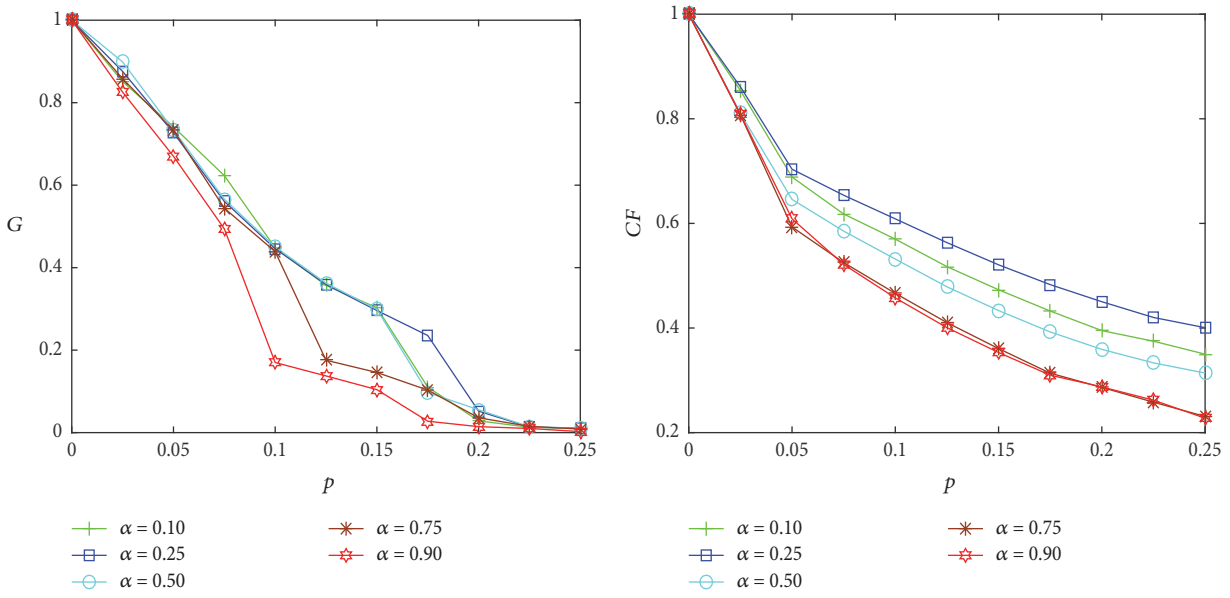

Figure 5: The relationship between the invulnerability and the coefficient α.

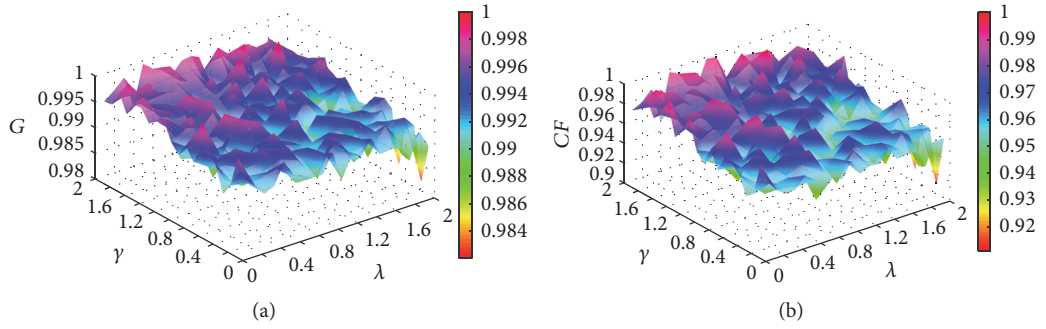

Figure 6: The relationship between the invulnerability and the coefficients γ and λ.

of η. Furthermore, nodes at the higher level have a large overload capacity and they could carry more additional load. Subsequently, the destructiveness of cascading failures could be reduced and the "avalanche" phenomenon could be prevented. Moreover, even if the nodes at the upper level fail due to the excessive load, the failure node would continue to allocate the load to the nodes at the higher and same level based on the load redistribution strategy. In that manner, the cascade propagation could be suppressed by applying the load redistribution strategy proposed in this paper. Although the capacity of the high-level node is large, it also has an upper limit. In particular, when η is larger than the threshold

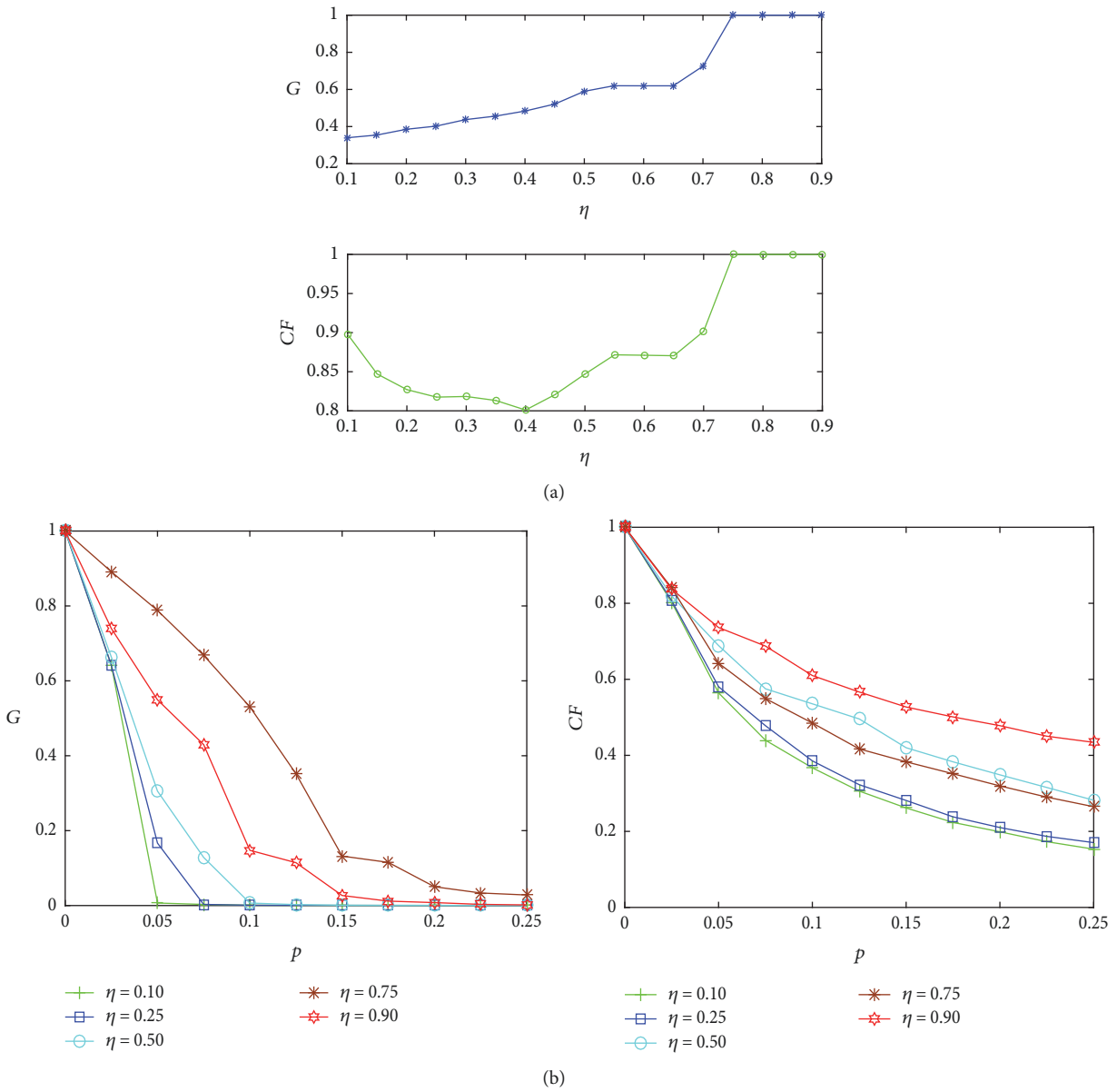

Figure 7: The relationship between the invulnerability and the coefficient η.

$\eta_T = 0.75$, the nodes at the higher level may easily fail because of the additional load from failure nodes at the low level. Thus, the network invulnerability would no longer change with the change of the coefficient η at the end.

A comparison analysis of Figure 7(b) is carried out, which shows that the network invulnerability would be improved gradually with the increase in η. On the one hand, when the coefficient η is small, there is no significant change in the ability of C2 networks to resist cascade failure. It could be observed that the cures in Figure 7(b) almost coincide when $\eta = 0.10$ and $\eta = 0.25$. On the other hand, when η is too large, more load will be assigned to the nodes at the higher level. The excessive load would ultimately cause failures in upper node, which implies that it is not always better to increase the coefficient η.

3.4. Effect of the Tolerance Parameter β on Network Cascading Invulnerability. To analyze the effect of the tolerance parameter β on network invulnerability, G and CF are employed to measure the cascading invulnerability for C2 networks. Moreover, the value of the coefficient β is chosen from the range $[0, 1]$, and the other parameters are initialized as $\alpha = 0.25$, $\lambda = 1.3$, $\gamma = 1.6$, $\eta = 0.80$. Figure 8(a) shows the trend of C2 networks cascading invulnerability with different coefficients β, where 50 rounds of simulations and average calculations are carried out. Meanwhile, Figure 8(b) demonstrates the relationship between the network invulnerability and attacking ratio p with different coefficients β.

It could be observed from Figure 8(a) that the overload capacity of each node would increase with the increase in tolerance parameter β. Consequently, the damage caused by

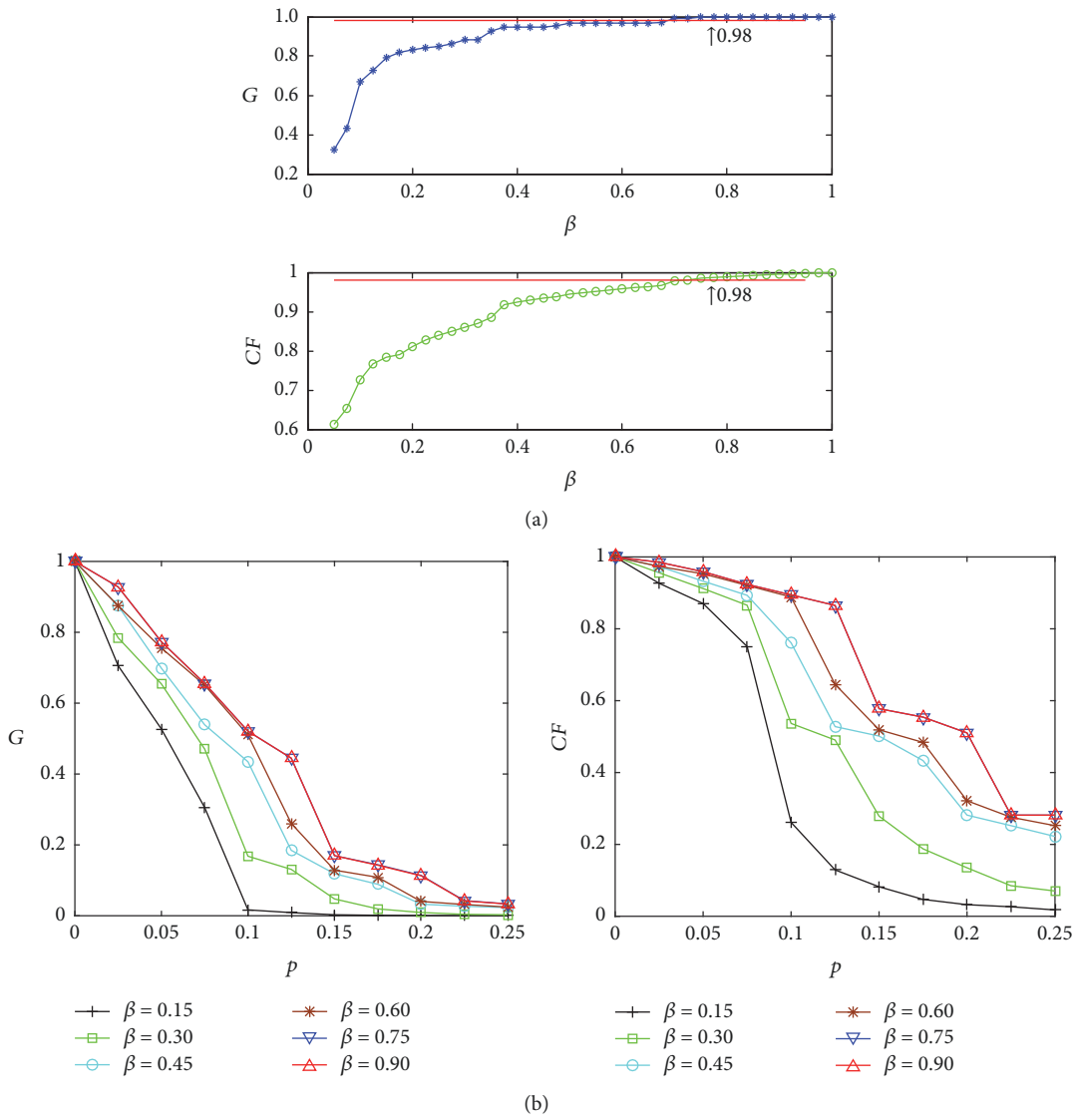

Figure 8: Network invulnerability varies with the tolerance parameter β.

cascading failures could be gradually reduced. Moreover, by analyzing the invulnerability indices G and CF, it could be concluded that the C2 network has better anti-cascade failure abilities with $\beta = 0.65$ and 0.7.

A comparison analysis of Figure 8(b) is carried out, which implies two major conclusions. On the one hand, when the tolerance parameter β is constant, two different invulnerability measure curves demonstrate a decreasing trend with the increase in the attacking ratio p. Therefore, the network performs with worse invulnerability. On the other hand, the network invulnerability increases with the increase in the coefficient β and decreases with the increase in the attack ratio p for the same measure. In addition, it could be observed that a larger value of coefficient β would enlarge the overload capacity of the node and enhance the ability of C2 networks to resist cascade failure. However, increasing the value of the tolerance parameter could increase the cost of nodes and network construction at the same. Therefore, the tolerance parameter should not be very large in practice.

3.5. The Comparisons with Other Relational Models. After analyzing the effect of each parameter in the cascading failure model on the invulnerability of C2 networks, the optimal value of each parameter is fixed. And the simulations in Figure 9 show the effects of initial load quantification methods, load redistribution strategies for the failure nodes, and the cascading failure models on C2 networks. Firstly, the influence of initial load quantification methods for the cascading failure in C2 networks is compared and analyzed under the condition that the load from failure node is allocated according to NALR strategy proposed in this paper; G and CF are employed to measure the cascading invulnerability for C2 networks. Figure 9 shows the trend of C2 networks cascading invulnerability with different initial

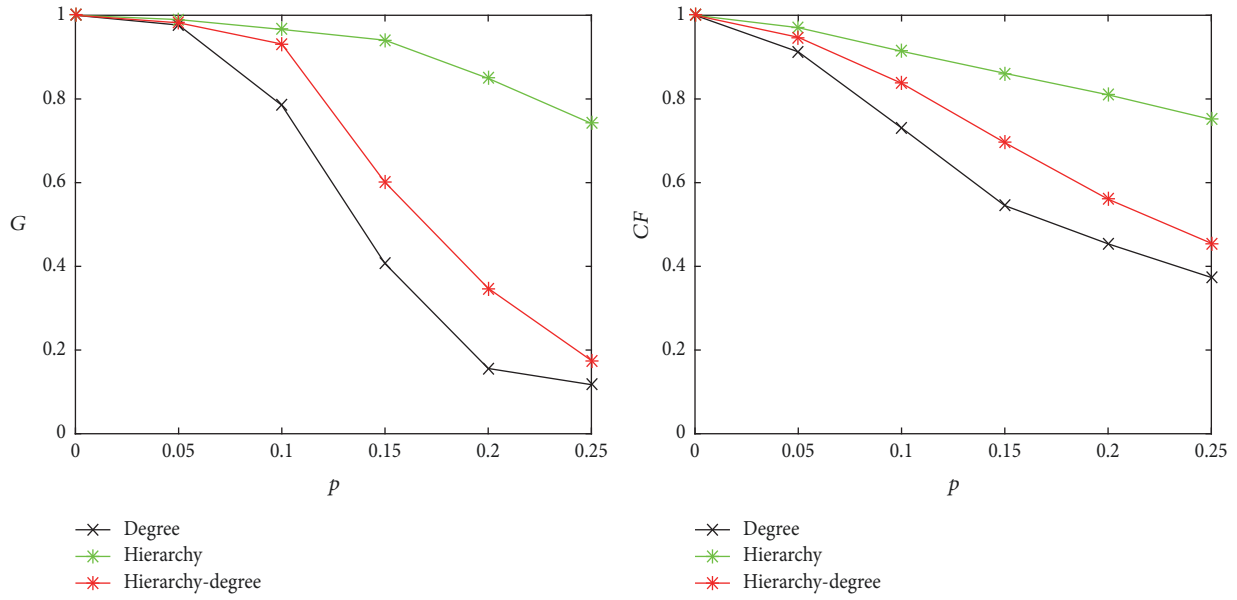

Figure 9: The influence of load quantification methods on C2 networks invulnerability.

load quantification methods, and many rounds of simulations and average calculations are carried out.

By comparing and analyzing the influence of three different load quantification methods on C2 networks invulnerability, the following main conclusions can be reached: (1) In the above three initial load quantization methods, with the increase in the number of important nodes removed, the scale of the failure nodes increases. (2) Compared with the load quantization method based on the degree, the hierarchy-degree method proposed in this paper can make the network better against cascading failure, while the initial load definition based on the level can make the C2 networks have the best ability to resist cascade failure. This is because the NALR strategy allocates load from the failure node to the neighboring nodes at the higher and same level only and thus prevents the cascade failure propagation from high-level nodes to low-level nodes. Although the hierarchy based method of quantifying the node's initial load makes C2 networks better against cascading failure, it leads to the first failure of high-level important nodes, which is not what we expected in the actual network. And what is more, the hierarchy based method of quantifying the node's initial load makes all nodes at the same level have the same initial load, which is inconsistent with the actual situation. Therefore, it is not feasible to define the initial load of the nodes based entirely on hierarchy.

In order to verify the effectiveness and superiority of NALR strategy, which is compared with the conventional load redistribution strategy based on the spare capacity of neighboring nodes, G and CF are still employed to measure cascading invulnerability of C2 networks. Figure 10 shows the trend of C2 networks cascading invulnerability with different load redistribution strategies.

Obviously, compared with the conventional strategy, the C2 network has better ability to resist cascade failure when adopting the NALR strategy proposed in this paper. The reason is that the load of high-level node is relatively large; conventional strategy allocates the load from high-level failure nodes to the lower-level neighboring nodes, which causes more nodes to fail at low layer, because there is a lack of enough spare capacity to absorb the extra load. However, NALR strategy redistributes the load from failure nodes to the higher or same level neighboring nodes, which have larger spare capacity than the lower-level nodes, and they can absorb the extra load, reducing the failure scale. Therefore, the NALR strategy proposed in this paper is more effective and advanced than the conventional strategy.

Furthermore, five kinds of cascading failure models in other literature sources, which adopted conventional load redistribution strategy, are compared with the cascading failure model proposed in this paper. The five relational models are as follows:

(i) The cascading failure model is proposed in this paper; more details are available in Section 2.

(ii) The initial load of the node is quantified according to its degree, and the load-capacity is linear [6, 12, 20, 30, 31, 44, 45], which are expressed as follows:

$$L_i(0) = a * k_i^{\alpha}$$
$$C_i = TL_i(0), \tag{9}$$

where a and α are tunable parameters, k_i is the degree of node v_i, $T > 1$ is the tolerance parameter (equivalent to $(1 + \beta)$ in formula (2)).

(iii) The initial load of the node is quantified according to its degree, and the relationship of load-capacity is nonlinear [35, 36, 47]. This model is expressed as follows:

$$L_i(0) = a * k_i^{\alpha}$$
$$C_i = L_i(0) + n * L_i^m(0), \tag{10}$$

where $m \geq 0$ and $n \geq 0$ are tunable parameters.

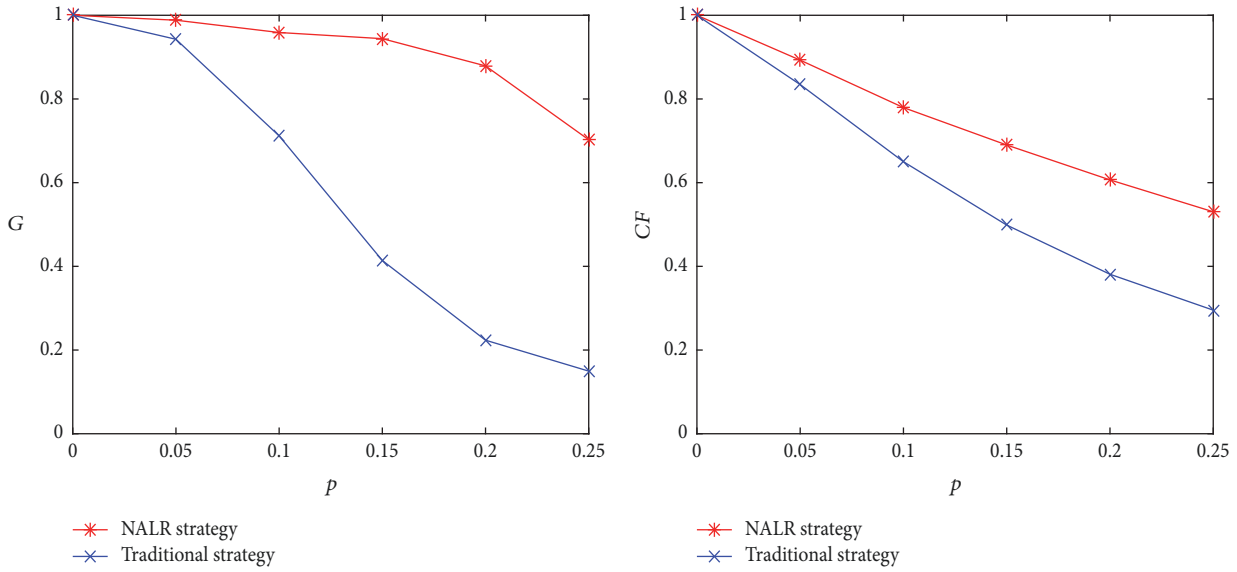

Figure 10: The relationship between the invulnerability and the load redistribution strategies.

(iv) The initial load of the node is quantified according to the node's own degree and its neighboring nodes degree [30]; the relationship between the load and the capacity is nonlinear. This model is expressed as follows:

$$L_i(0) = \left(k_i \sum_{j \in \Gamma_i} k_j\right)^{\theta}$$
$$C_i = TL_i(0), \tag{11}$$

where θ is a tunable parameter.

(v) The initial load of the node is quantified according to its betweenness [7, 38], and the relationship of load-capacity is linear. This model is expressed as follows:

$$L_i(0) = B_i$$
$$C_i = TL_i(0), \tag{12}$$

where B_i is the betweenness of node v_i.

(vi) The initial load of the node takes a random number in the range $[L_{\min}, L_{\max}]$; the relationship between load and capacity is linear, which is common in epidemic spreading models [16, 18]. The initial load and capacity formulas are expressed as follows:

$$L_i(0) = \text{rand}(L_{\min}, L_{\max})$$
$$C_i = TL_i(0), \tag{13}$$

where $[L_{\min}, L_{\max}]$ is the range of random values.

Figure 11 shows the relationship between the network invulnerability and attacking ratio p in different cascading failure models, where many rounds of simulations and average calculations are carried out.

According to the comparison and analysis of Figure 11, the main conclusions are as follows: (1) No matter what kind of cascading failure model, the invulnerability of C2 networks decreases as the attacking ratio p increases. (2) Model (v) has the worst ability to resist cascading failure. The main reason is the hierarchy structure of C2 networks; the high-level nodes are in the network center, and their betweenness are very large; while the low-level nodes are at the network edge, their betweenness is very small. In the whole C2 networks, the range of nodes betweenness is huge, which results in uneven distribution of initial load and capacity. Therefore, the network is extremely fragile to deliberate attacks, which can easily lead to the collapse of the whole network. (3) The cascading failure model proposed in this paper has the best ability to resist cascading failure among the other five models, which is due to the hierarchy-degree based method of defining the node's initial load and the NALR strategy. Compared with conventional load quantization methods, the hierarchy-degree based method proposed in this paper can more strictly distinguish and accurately define the node's initial load in C2 networks. In addition, the NALR strategy can suppress cascading failure propagation and reduce the failure scale. The above analysis also shows that the initial load quantization method and the load distribution strategy have a great influence on the invulnerability of C2 network.

4. Conclusions

In the research of invulnerability for cascading failures in C2 networks, it is necessary to define the reasonable initial load of the node and redistribute the load from failure node. Subsequently, the ability of C2 networks to resist cascading failures could be effectively enhanced, and the invulnerability of C2 networks could be improved too. In this paper, a novel cascading failure model for C2 networks with hierarchy structure is proposed. Moreover, a level-degree based method of defining the initial load and a nonuniform adjustable load redistribution strategy are introduced in

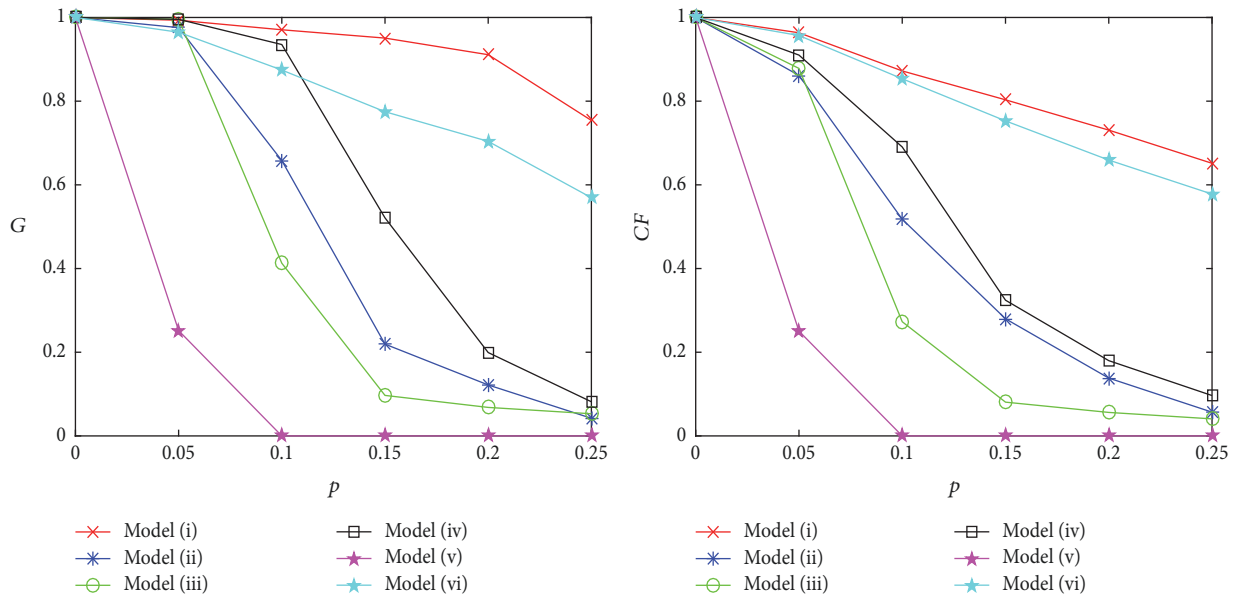

Figure 11: Comparison of different cascading failure models.

this paper. Furthermore, the invulnerability of C2 networks against cascading failures could be significantly improved by changing the initial load adjustment coefficient, the tolerance parameter, and the load redistribution coefficient. The experimental results have shown the existence of optimal network parameters which achieve the best anti-cascade failure ability for C2 networks. Additionally, the simulation results and the comparison analysis show that our model is effective in designing C2 networks with high robustness to cascading failure.

So far, the research in this paper only focuses on node cascading failure, and there is no consideration for edge cascading failure and no consideration for the case that the overload node may return to normal. Furthermore, the network model presented in this paper is static, single layer, and noninteracting. However, the military is dynamic, interdependent network, and the overload node may return to normal, which has been paid attention inevitably. To this end, our future study will focus on the restoration and model of self-healing against cascading overload failures in dynamic C2 network.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the State Key Program of National Natural Science of China (Grant no. 61432002); the NSFC Grants nos. 61772112, 61672379, and 61370199; and the Dalian High-Level Talent Innovation Program (no. 2015R049).

References

[1] X. Hu, X. He, and D. Rao, "A methodology for investigating the capabilities of command and coordination for system of systems operation based on complex network theory," *Complex Systems and Complexity Science*, vol. 12, no. 2, pp. 9–17, 2015.

[2] W. Yunming, C. Si, P. Chengsheng, and C. Bo, "Measure of invulnerability for command and control network based on mission link," *Information Sciences*, vol. 426, pp. 148–159, 2018.

[3] Y. Qi, Z. Liu, and J. Xu, "Research development of complex networks application in combat modeling," *Fire Control & Command Control*, vol. 39, no. 9, pp. 1–4, 2014.

[4] Y. Lu and B. Yang, "Analyzing and modeling cascading failures for inter-domain routing system," *Journal of Systems Engineering and Electronics*, vol. 38, no. 1, pp. 172–178, 2016.

[5] L.-L. Hou, S.-Y. Lao, Y.-D. Xiao, and L. Bai, "Recent progress in controllability of complex network," *Wuli Xuebao/Acta Physica Sinica*, vol. 64, no. 18, Article ID 188901, 2015.

[6] X. Peng, H. Yao, M. Xiao, J. Du, C. Ding, and H. Li, "Cascading failure model for weighted networks and invulnerability analyses," *Journal of Systems Engineering and Electronics*, vol. 36, no. 6, pp. 1096–1102, 2014.

[7] A. E. Motter and Y. Lai, "Cascade-based attacks on complex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 66, no. 6, Article ID 065102, 4 pages, 2002.

[8] Y. Koc, M. Warnier, R. E. Kooij, and F. M. T. Brazier, "A robustness metric for cascading failures by targeted attacks in power networks," in *Proceedings of the 2013 10th IEEE International Conference on Networking, Sensing and Control, ICNSC 2013*, pp. 48–53, France, April 2013.

[9] E. Bompard, A. Estebsari, T. Huang, and G. Fulli, "A framework for analyzing cascading failure in large interconnected power systems: A post-contingency evolution simulator," *International Journal of Electrical Power & Energy Systems*, vol. 81, pp. 12–21, 2016.

[10] J. Wang, "Robustness of complex networks with the local protection strategy against cascading failures," *Safety Science*, vol. 53, pp. 219–225, 2013.

[11] Z. Wang, W. Jie, and Z. Huang, "Closing strategies to control cascading failure in urban traffic networks," *Systems Engineering*, vol. 34, no. 2, pp. 103–108, 2016.

[12] Z.-Y. Jiang, J.-F. Ma, Y.-L. Shen, and Y. Zeng, "Effects of link-orientation methods on robustness against cascading failures in complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 457, pp. 1–7, 2016.

[13] L. Ding and S. Zhang, "Cascading dynamics model for complex communication networks based on local routing," *Complex Systems and Complexity Science*, vol. 11, no. 3, pp. 79–85, 2014.

[14] F. Xie, S. Cheng, and D. Chen, "Cascade based attack vulnerability in complex networks," *Journal of Tsinghua University (Science and Technology)*, vol. 51, no. 10, pp. 1252–1257, 2011.

[15] Y. Yang, J. Li, G. Wang, and M. Nan, "Modeling and characteristic analyzing of operational information flowing based on super-network," *Complex Systems and Complexity Science*, vol. 13, no. 3, pp. 8–18, 2016.

[16] L. Jiang, X. Jin, Y. Xia, B. O. Ouyang, and D. Wu, "Dynamic behavior of the interaction between epidemics and cascades on heterogeneous networks," *EPL (Europhysics Letters)*, vol. 108, no. 5, Article ID 58009, 2014.

[17] Q. Guo, X. Jiang, Y. Lei, M. Li, Y. Ma, and Z. Zheng, "Two-stage effects of awareness cascade on epidemic spreading in multiplex networks," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 91, no. 1, Article ID 012822, 2015.

[18] O. Bo, X. Jin, and Y. Xia, "Dynamic interplay between epidemics and cascades: Epidemic outbreak in uncorrelated networks," *Acta Physica Sinica*, vol. 63, no. 21, Article ID 218902, 2014.

[19] C. J. Tessone, A. Garas, B. Guerra, and F. Schweitzer, "How big is too big? Critical shocks for systemic failure cascades," *Journal of Statistical Physics*, vol. 151, no. 3-4, pp. 765–783, 2013.

[20] J.-W. Wang, "Modeling cascading failures in complex networks based on radiate circle," *Physica A: Statistical Mechanics and its Applications*, vol. 391, no. 15, pp. 4004–4011, 2012.

[21] J. Lorenz, S. Battiston, and F. Schweitzer, "Systemic risk in a unifying framework for cascading processes on networks," *The European Physical Journal B*, vol. 71, no. 4, pp. 441–460, 2009.

[22] W.-X. Jin, P. Song, G.-Z. Liu, and H. . Stanley, "The cascading vulnerability of the directed and weighted network," *Physica A: Statistical Mechanics and its Applications*, vol. 427, pp. 302–325, 2015.

[23] S.-M. Chen, S.-P. Pang, and X.-Q. Zou, "An LCOR model for suppressing cascading failure in weighted complex networks," *Chinese Physics B*, vol. 22, no. 5, Article ID 058901, 2013.

[24] G. Zhang, Z. Li, B. Zhang, and W. A. Halang, "Understanding the cascading failures in Indian power grids with complex networks theory," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 15, pp. 3273–3280, 2013.

[25] Z. Li, Y. Guo, G. Xu et al., "Analysis of cascading dynamics in complex networks with an emergency recovery mechanism," *Acta Physica Sinica*, vol. 63, no. 15, Article ID 158901, 2014.

[26] D. Li, B. Fu, Y. Wang et al., "Percolation transition in dynamical traffic network with evolving critical bottlenecks," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 112, no. 3, pp. 669–672, 2015.

[27] L. Daqing, J. Yinan, K. Rui, and S. Havlin, "Spatial correlation analysis of cascading failures: congestions and Blackouts," *Scientific Reports*, vol. 4, article 5381, 2014.

[28] C. Liu, D. Li, E. Zio, and R. Kang, "A modeling framework for system restoration from cascading failures," *PLoS ONE*, vol. 9, no. 12, Article ID e112363, 2014.

[29] C. Liu, D. Li, B. Fu, S. Yang, Y. Wang, and G. Lu, "Modeling of self-healing against cascading overload failures in complex networks," *EPL (Europhysics Letters)*, vol. 107, no. 6, Article ID 68003, 2014.

[30] J. Liu, Q. Xiong, X. Shi, K. Wang, and W. Shi, "Robustness of complex networks with an improved breakdown probability against cascading failures," *Physica A: Statistical Mechanics and its Applications*, vol. 456, pp. 302–309, 2016.

[31] P. Zhang, B. Cheng, Z. Zhao et al., "The robustness of interdependent transportation networks under targeted attack," *EPL (Europhysics Letters)*, vol. 103, no. 6, Article ID 68005, 2013.

[32] J. Wang, C. Jiang, and J. Qian, "Robustness of interdependent networks with different link patterns against cascading failures," *Physica A: Statistical Mechanics and its Applications*, vol. 393, pp. 535–541, 2014.

[33] K.-M. Lee and K.-I. Goh, "Strength of weak layers in cascading failures on multiplex networks: Case of the international trade network," *Scientific Reports*, vol. 6, Article ID 26346, 2016.

[34] J. Ma, W. Han, Q. Guo, and Z. Wang, "Traffic dynamics on two-layer complex networks with limited delivering capacity," *Physica A: Statistical Mechanics and its Applications*, vol. 456, pp. 281–287, 2016.

[35] J.-S. Wang, X.-P. Wu, and Y.-Q. Chen, "Invulnerability of weighted scale-free networks against cascading failure," *Complex Systems and Complexity Science*, vol. 10, no. 2, pp. 13–19, 2013.

[36] X.-P. Wu, J.-S. Wang, Y.-L. Qin, and Q. Ye, "Invulnerability of small-world network against cascading failure based on nonlinear load-capacity model," *Tongxin Xuebao/Journal on Communication*, vol. 35, no. 6, pp. 1–7, 2014.

[37] K. Hu, T. Hu, and Y. Tang, "Model for cascading failures with adaptive defense in complex networks," *Chinese Physics B*, vol. 19, no. 8, Article ID 080206, 2010.

[38] T. Zhu, G.-C. Chang, S.-P. Zhang, and R.-X. Guo, "Research on model of cascading failure in command and control based on complex networks," *Xitong Fangzhen Xuebao/Journal of System Simulation*, vol. 22, no. 8, pp. 1817–1820, 2010.

[39] B. Fu, D. G. Li, and M. K. Wang, "Review and prospect on research of cloud model," *Application Research of Computers*, vol. 28, no. 2, pp. 420–426, 2011.

[40] T. Li, X. Lü, and Y. Tan, "Optimizing node capacity of campaign logistics networks based on cascading failure," *Complex Systems and Complex Science*, vol. 6, no. 01, pp. 69–76, 2009.

[41] D. Shen and J. Li, "Research on military information grid cascading failure model and robustness strategy," *Systems Engineering and Electronics*, vol. 37, no. 2, pp. 310–317, 2015.

[42] J.-Y. Zhang, K. Yi, H. Wang, J.-F. Zhang, and X.-X. Zhou, "Dynamic robustness measure method considering cascading failure for C4ISR system structure," *Xi Tong Gong Cheng Yu Dian Zi Ji Shu*, vol. 38, no. 9, pp. 2072–2079, 2016.

[43] M. Yuan, "A cascading failure model of complex network with hierarchy structure," *Wuli Xuebao/Acta Physica Sinica*, vol. 63, no. 22, p. 220501, 2014.

[44] H. Han, R. Yang, H. Li, and R. Fan, "Cascading failure of two-layered interdependent command and control network," *Zhongnan Daxue Xuebao (Ziran Kexue Ban)/Journal of Central South University (Science and Technology)*, vol. 46, no. 12, pp. 4542–4547, 2015.

[45] X. Wang, J. Cao, and X. Qin, "Study of robustness in functionally identical coupled networks against cascading failures," *PLoS ONE*, vol. 11, no. 8, Article ID e0160545, 2016.

[46] T. Zhu, G.-C. Chang, R.-X. Guo, and Q. Luo, "Research on centrality model and evaluation of networked command and control," *Xitong Fangzhen Xuebao/Journal of System Simulation*, vol. 22, no. 1, pp. 201–209, 2010.

[47] D.-H. Kim and A. E. Motter, "Resource allocation pattern in infrastructure networks," *Journal of Physics A: Mathematical and Theoretical*, vol. 41, no. 22, Article ID 224019, 2008.