Hindawi
Mobile Information Systems
Volume 2018, Article ID 6404136, 11 pages
https://doi.org/10.1155/2018/6404136

Research Article

Cascading Failure Model for Command and Control Networks Based on an *m*-Order Adjacency Matrix

Yun-ming Wang,[1,2] **Bo Chen**,[2,3] **Xiao-shuang Chen**,[2] **and Xiu-e Gao**[3]

[1]*School of Electrical and Information Engineering, Dalian Jiaotong University, Dalian 116028, Liaoning, China*
[2]*Communication and Network Laboratory, Dalian University, Dalian 116622, Liaoning, China*
[3]*College of Mechanical and Electronical Engineering, Lingnan Normal University, Zhanjiang 524048, China*

Correspondence should be addressed to Yun-ming Wang; wang19871128@126.com

Received 14 September 2018; Revised 12 November 2018; Accepted 21 November 2018; Published 18 December 2018

Academic Editor: Yuh-Shyan Chen

Cascading failure models for command and control networks (C2 networks) continue to be a challenging and important research area. Current solutions share a common limitation because the solutions focus only on the importance of each node in isolation using one index rather than considering the contribution degree of neighboring nodes, which makes the initial load definition inaccurate and affects the cascading invulnerability of the network. To address this limitation, a new cascading failure model for C2 networks is proposed. The new model CFM_{AdjM}, which is based on an *m*-order adjacency matrix, proposes a method of initial load definition using the contribution degree of *m*-order neighboring nodes and defines the nonlinear load capacity model according to the nonlinear relationship between load and capacity. Finally, the influence of model parameters on the cascading failure of C2 networks is analyzed through simulation, and the results demonstrate that the new model effectively resists the cascading failure and enhances the survivability of the network by defining the initial load and adjusting the coefficient appropriately.

1. Introduction

Command and control networks (C2 networks), as the hub of command and information transmission, are critical to victory in warfare. With continuous improvements in the degree and level of battlefield information, interactions within C2 networks have become more frequent. In addition, the organizational structure of C2 networks has become increasingly complex, exhibiting the characteristics of heterogeneous nodes, multiple links, and so on. In addition, C2 networks exhibit the characteristics of typical complex networks [1]. Because of their vital role, achieving invulnerability of C2 networks is essential. Each node in C2 networks has corresponding loads, and the network must adapt when one or more nodes are destroyed in combat [2, 3]. For the network to adapt to the loss of one or more nodes in combat, the loads of the destroyed nodes are reallocated to the neighboring nodes [4, 5]. However, the reallocation of loads may result in neighboring nodes exceeding their load capacity, causing the nodes to fail and new rounds of load redistribution. This can lead to a chain reaction, which eventually results in partial or complete network collapse. Such phenomena are referred to as network cascading failure [6, 7]. The role of cascading failure mechanisms can have a substantial impact on the entire network, even resulting in its collapse [8, 9]. In other words, cascading failure of C2 networks can be more destructive than common faults [10, 11]. Therefore, studying the cascading failure mechanism of C2 networks with complex network theory is of great significance to contain the probability of cascading failure and improve network invulnerability. This has become a hot research topic in the field of military research.

At present, many scholars at home and abroad study the cascading failure problem of complex networks. The main method still involves establishing a load capacity cascading

failure model. In particular, the three key problems that must be addressed include the following: the means of determining the initial load of the nodes [12, 13], the ways of defining the maximum capacity of the nodes, and the means of reassigning the load of a failed node to other nodes in the network [14, 15].

In terms of initial load definition, there are two primary means: one is to define the initial load based on nodes [16, 17] and the other is to define the initial load according to the edge [18]. The former mostly uses node importance to define the initial load [19], which is computed based on the degree of the node, the node strength, the mean degree of the neighbor node, the betweenness, the random walk betweenness, and other conventional and improved indicators. The latter defines the initial load based on the contribution of the edge. In [20], an initial load definition method based on the degree of a node was proposed. This method considers the local information of the network but demonstrates limited accuracy. In [21], the influence of the initial load and the parameter distribution of the tolerance coefficient on the cascading failure were studied, and a cascading failure probability model was proposed based on the mean field theory. An initial load definition method based on the degree of a node and betweenness centrality was proposed in [22]. This method improves the robustness of the scale-free network against cascading failure. Based on the coupling effect of a network, a recent report [23] established a cascading failure model by adjusting the contribution of links to the load, and the more the links contribute to the load, the better the robustness of the network. Literatures [24, 25] define the initial load of an edge based on the betweenness of the endpoints of the edges and explain the cascading failure mechanism in the network by using the node capability coefficient and the betweenness-degree contribution value.

In terms of load capacity models, the first one involves statistical distribution based on node attributes [26, 27]. The second is based on the classic ML model defined by Motter and Lai [28], in which the capacity is directly linear to the initial load. This model is widely used. The third is based on the KM model proposed by Kim et al. [29], in which there is a nonlinear relationship between capacity and initial load. By studying four practical networks, the KM model reflects the nonlinear relationship between load and capacity. In other words, smaller capacity nodes have larger idle capacity. This conclusion has drawn the attention of many scholars. Subsequent research [30] introduced a stochastic method of achieving an optimal heterogeneous allocation of node capacity and compares the load capacity allocation performance of N order and $N-1$ order by using node deliberate attacks and random failure. In addition, a new model of cascading failure capacity was proposed in [31], which allocates additional capacity to nodes with larger load and larger degree to ensure network robustness.

Considering the hierarchical structure characteristics of C2 networks and the influence of neighboring nodes, a cascading failure model of a C2 network based on an m-order neighborhood matrix is established, hereafter referred to as $\mathrm{CFM}_{\mathrm{AdjM}}$. A method of initial load definition based on m-order neighboring node contribution is first proposed, considering both the importance of nodes and the contribution degree of the m-order neighboring nodes. Secondly, a nonlinear load capacity model is established. Finally, the effectiveness and feasibility of this cascading failure model for C2 networks proposed in this paper is verified through simulation.

2. Establishing a Cascading Failure Model for Command and Control Networks

2.1. The Method of Defining Initial Load Based on the Contribution Degree of the m-Order Neighboring Nodes. The definition of the initial load has an important influence on the cascading failure of C2 networks, and the rationality of the initial load definition determines the ability of the network to resist cascading failure [32, 33]. Furthermore, the definition of initial load largely depends on the importance of nodes. This implies that the evaluation of node importance is directly related to determining the merits and failures of a cascading failure model [34]. Most of the existing cascading failure models of C2 networks directly use the single index such as degree of the nodes [4, 11] or betweenness [35] to quantify the initial load of nodes. The complexity of a C2 network structure makes it difficult for a single index to accurately measure the importance of the nodes. The importance of nodes is affected by the network structure and exhibits a strong correlation with its neighboring nodes.

According to the theory of spatial autocorrelation, the closer the distance between node pairs in complex networks, the greater the contribution to each other's importance, conversely, the lesser the contribution to each other's importance. In addition, the importance of contribution values degrades exponentially with the increase in distance. The C2 network is a type of complex network with scale-free characteristics, and the degree follows the power law distribution, which implies that fewer nodes have a larger degree and a larger number of nodes have relatively smaller degree. Therefore, this paper considers the important contribution of neighboring nodes in evaluating the importance of nodes in C2 networks and proposes an initial load definition method based on the contribution degree of the m-order neighboring nodes. Betweenness is a global variable that reflects the role and influence of nodes in the entire network. According to the concept of betweenness and the operation command process of OODA [2], we first provide the definition of a sensing node, a command node, and a fire node in C2 networks. On this basis, the concepts of combat link and combat link betweenness are proposed.

Definition 1. Sensor nodes refer to combat units with capabilities such as early warning, detection, reconnaissance, and surveillance, including early warning radars, reconnaissance radars, among others.

Definition 2. Command nodes refer to combat units with capabilities such as intelligence fusion, command and decision-making, and information coordination and distribution, including command organization, intelligence processing agency, among others.

Definition 3. Fire nodes refer to combat units with capabilities such as interception, attack, and damage, including all types of air defense weapons.

Definition 4. Combat link refers to one or more links of detection-command-fire formed by the operational information flow from sensor nodes to fire nodes via the decision fusion of command nodes.

A schematic of a combat link is shown in Figure 1. When the sensor nodes discover the enemy target, they send the information to the command nodes, and then, the command nodes forward the target information to the peer nodes or report/issue the information to higher/lower nodes. After cooperative decision-making of a number of command nodes, the combat command is issued to the fire strike nodes, and finally, the fire strike nodes attack the incoming enemy target. In this process, information transmission will pass through several combat links.

Definition 5. The combat link betweenness of a node is defined as the ratio of the shortest combat link passing through this node in the network.

Therefore, the combat link betweenness of a node is defined as the ratio of the number of nodes in the shortest combat link in the network. The combat link betweenness can be used to measure the importance degree of nodes in a C2 network: the larger the combat link betweenness, the more information flows through the node.

The combat link indicates that the combat information flow is sent by the sensing node, via the command node, and finally to the link formed by the fire strike node. Because the sensing node and the fire strike node itself are isolated relations, their connections are transmitted through the command node. Therefore, the starting point of the network is the sensing node, the ending point is the fire strike node, and the nodes passing through the link include the command node. The combat link betweenness of the command node v_c can be expressed in the following equation:

$$b_c = \sum_{i=1}^{n_i} \sum_{j=n_i+n_c+1}^{N} \frac{m\left(O_i, D_c, F_j\right)}{m\left(O_i, F_j\right)}. \tag{1}$$

Among them, $m(O_i, F_j)$ indicates the number of the shortest combat links between the sensing node O_i and the fire strike node F_j, $m(O_i, D_c, F_j)$ indicates the number of shortest combat links between the sensing node O_i and the fire strike node F_j through the command node D_c. The larger the combat link betweenness, the more information flows through the node.

The hierarchical structure of C2 networks makes the operational command and cooperative communication capability of high-level nodes significantly higher than that of low-level nodes. Therefore, the bearing capacity of nodes is related to their location in the hierarchy: the higher the hierarchy, the greater the initial load. Considering both the network hierarchy and combat link betweenness, the initial load of the node v_c can be defined as follows:

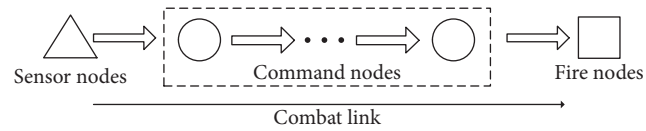

Figure 1: Schematic of the combat link.

$$L_c^{b'} = u\left(\frac{b_c}{d_c}\right)^{\alpha}, \tag{2}$$

where b_c denotes the combat link betweenness of nodes, u and α are adjustable parameters, d_c indicates the hierarchy of the node v_c, the smaller the d_c, the higher is the level, and b' is an identifier of the initial load L_c. Because the C2 network has the characteristic of the strict hierarchical structure, the manuscript adds the hierarchy of the C2 network to the original definition of the initial load which is based on the combat link betweenness, and then gives a new definition of the initial load.

The above definition of the initial load only considers the importance degree of the node itself. However, the neighbor node also has a certain dependence and important impact. Therefore, an initial load definition method based on the contribution degree of m-order neighboring nodes is proposed in this paper.

Because the C2 networks cannot only rely on the node degree, the combat link betweenness, or any other single index to evaluate the importance of nodes, the network characteristics must comprehensively consider multiple characteristic indexes simultaneously. Therefore, the node importance degree I_i can be defined as follows:

$$I_i = \begin{bmatrix} u & \gamma & \cdots & \gamma^m \end{bmatrix} \cdot \begin{bmatrix} \delta_{i,1} & \delta_{i,2} & \cdots & \delta_{i,n} \\ \sum_{j\in\pi^{(1)}(i)} \delta_{j,1} & \sum_{j\in\pi^{(1)}(i)} \delta_{j,2} & \cdots & \sum_{j\in\pi^{(1)}(i)} \delta_{j,n} \\ \vdots & \vdots & \vdots & \sum_{j\in\pi^{(2)}(i)} \delta_{j,n} \\ \sum_{j\in\pi^{(m)}(i)} \delta_{j,1} & \sum_{j\in\pi^{(m)}(i)} \delta_{j,2} & \cdots & \sum_{j\in\pi^{(m)}(i)} \delta_{j,n} \end{bmatrix} \cdot \begin{bmatrix} \omega_1 \\ \omega_2 \\ \omega_3 \\ \vdots \\ \omega_n \end{bmatrix}. \tag{3}$$

Among them, m indicates the order, $\sum_{j\in\pi^{(m)}(i)}\delta_{j,n}$ is the importance degree contribution of the set of m-order neighbor nodes of the command node v_i to the command node v_i under the constraint of the n^{th} index, ω_i is the weight proportion for different indexes, the sum of the weight of each index is 1, which implies that $\sum_{i=1}^{n}\omega_i = 1$, The importance degree of each index factor can be dynamically adjusted by flexibly adjusting the coefficient ω_i, and u and γ are adjustable parameters.

Because each index has a large range of values, it is necessary to normalize each element $\sum_{j\in\pi^{(m)}(i)}\delta_{j,n}$ in the evaluation index, for convenience, to make $\sum_{j\in\pi^{(m)}(i)}\delta_{j,n}=\delta_{i,n}^{(m)}$, and we can obtain the following equation:

$$\delta_{i,j}^{'(k)}=\frac{\delta_{i,j}^{(k)}-\min\limits_{k=0,1,2,\ldots m}\delta_{i,j}^{(k)}}{\max\limits_{k=0,1,2,\ldots m}\delta_{i,j}^{(k)}-\min\limits_{k=0,1,2,\ldots m}\delta_{i,j}^{(k)}},\quad j=1,2,\ldots,n. \tag{4}$$

When only considering the impact of the degree index on the importance of nodes, we can obtain the following equation:

$$I_i^k=u\frac{k_i}{d_i}+\gamma\sum_{j\in\pi^{(1)}(i)}\frac{k_j}{d_j}+\gamma^2\sum_{j\in\pi^{(2)}(i)}\frac{k_j}{d_j}+\cdots+\gamma^m\sum_{j\in\pi^{(m)}(i)}\frac{k_j}{d_j}. \tag{5}$$

Among them, k_i and k_j indicates the degree of node i and node j.

When only considering the impact of the combat link betweenness on the importance of nodes, we can obtain the following equation:

$$I_i^b=u\frac{b_i}{d_i}+\gamma\sum_{j\in\pi^{(1)}(i)}\frac{b_j}{d_j}+\gamma^2\sum_{j\in\pi^{(2)}(i)}\frac{b_j}{d_j}+\cdots+\gamma^m\sum_{j\in\pi^{(m)}(i)}\frac{b_j}{d_j}. \tag{6}$$

Among them, I_i is the importance degree of the node v_i, and $\pi^{(m)}(i)$ represents all node sets that are connected to the node v_i with a distance of m and is also called the m-order neighboring node set of the node v_i. u and γ are adjustable parameters that satisfy the following conditions:

$$u+\gamma+\gamma^2+\cdots+\gamma^m=1. \tag{7}$$

Because γ follows the rule of geometric series, the equation (7) can be simplified as follows:

$$u+\frac{\gamma(1-\gamma^m)}{1-\gamma}=1. \tag{8}$$

When the importance of a node in C2 networks is calculated, the importance degree in addition to the contribution degree of its neighboring nodes is considered. As the importance degree itself is still greater than the contribution degree of neighboring nodes, $0<\gamma<u<1$, the value of u is greater than 0.5, and the value of γ is less than 0.5. The larger the value of u, the importance of the node will depend more on its own importance degree.

Therefore, the expression of the importance degree of the node that simultaneously considers the local feature index and the combat link betweenness of the global feature index is shown in the following equation:

$$I_i=\omega_1 I_i^k+\omega_2 I_i^b. \tag{9}$$

Among them, ω_1 and ω_2 indicate the degree and adjustable parameter of the combat link betweenness, respectively, $\omega_1+\omega_2=1$.

In summary, the initial load of the node based on the contribution degree of m-order neighboring nodes can be defined as follows:

$$L_i=I_i. \tag{10}$$

The definition considers the degree of the node and the combat link betweenness. The importance degree of the node uses local and global factors. The method not only analyzes the importance degree of the node itself but also considers the contribution degree of m-order neighbor nodes to determine the initial load of the nodes more accurately and improve the cascading invulnerability of the network.

2.2. Defining the Nonlinear Capacity Model in CFM_{AdjM}. The load capacity indicates the maximum capacity value of the load that the node can bear [36]. The larger the load capacity, the higher the construction cost, and excessive load capacity will also result in wasted resources. Therefore, the load capacity should be suitable, and the load of each node in the C2 networks should have an upper bound value. The load and capacity of real-world networks are nonlinear. In other words, small capacity network nodes have larger unused idle capacity, which is quite different from the traditional theory that the capacity is linearly related to the load. Kim and Motter verified the nonlinearity of load capacity through real-network simulation such as air transport, highway, power supply line, and the Internet [9]. The hierarchy and nonlinearity of C2 network structures also determine the nonlinearity of the load capacity. The nonlinear function of the load capacity of C2 networks is defined as follows:

$$C_i=L_i+\beta L_i^{\alpha},\quad i=1,2,\ldots,n. \tag{11}$$

Among them, L_i is the initial load of the node v_i and α and β are the adjustable parameters of the load capacity of nodes, $\alpha,\beta\geq 0$, the larger the values of α and β, the more additional load the node can bear and the stronger the invulnerability of the network, but the network cost will also increase. It is necessary to balance the invulnerability and the cost of the network. By adjusting the two parameters, the nonlinear relationship between the load capacity and the initial load can be analyzed, and a reasonable load capacity can be obtained.

When $\alpha=1, C_i=(1+\beta)L_i$, the relationship between initial load and load capacity is linear, and the model degenerates to the classic ML model. Figure 1 illustrates the relationship between the load capacity and the initial load for the nonlinear load capacity model and the linear ML model in the logarithmic coordinate system.

It can be observed from Figure 2 that the capacity of the ML model is proportional to the initial load. When the initial load of the nonlinear load model is small, the load capacity is larger and the surplus capacity is relatively large. When the initial load is larger, the load capacity is less than the load capacity of the ML model and the surplus capacity will be smaller.

When the relationship between the initial load and the load capacity of the nonlinear capacity model is more reasonable, it can describe the relationship between the load capacity and the initial load more accurately. When the initial load is small, it is necessary to have large load capacity

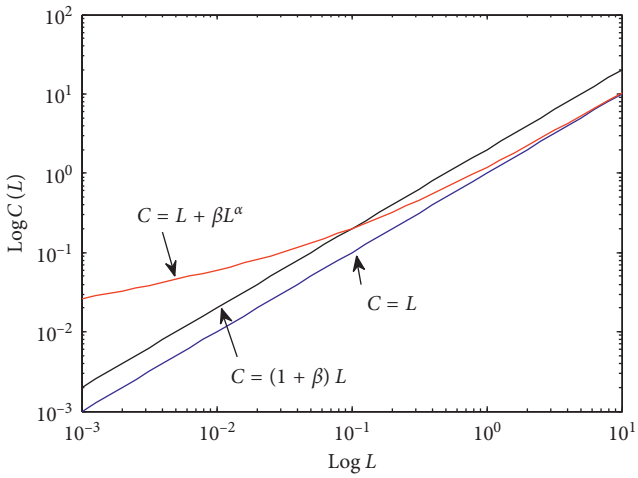

Figure 2: Relationship between load capacity and initial load.

to prevent the cascading failures. When the initial load is large, even if the fault occurs, the initial load is enough to bear other load tasks, and it does not require a large load capacity, which can reduce construction costs.

Therefore, the nonlinear load capacity model is more in line with the actual load capacity requirements of the C2 networks, which not only reduces the construction cost but also demonstrates better ability to resist cascading failure.

2.3. The Load Redistribution Strategy Based on Spare Capacity. Common load redistribution mechanisms are primarily based on the capacity of neighboring nodes. The larger the capacity, the more load is allocated. But in practice, the nodes with large capacity do not necessarily bear more loads. The strategy must also consider the initial load of the nodes. If the initial load of a node is already very large and then additional load is allocated to the node, it will easily result in excess load capacity and result in more serious cascading failure. Therefore, the load redistribution strategy should be based on spare capacity. To reduce the cascading failure scale of C2 networks, we allocate the load of the failure node v_i to its neighbor's nodes according to their spare capacity. So, if the node v_i fails, its neighboring node v_j would receive the extraload ΔL_j, which can be shown in the following equation:

$$\begin{aligned}\Delta L_j &= L_i \frac{C_j - L_j}{\sum_{m\in\Gamma_i}(C_m - L_m)} \\ &= L_i \frac{L_j + \beta L_j^{\alpha} - L_j}{\sum_{m\in\Gamma_i}(L_m + \beta L_m^{\alpha} - L_m)} \\ &= L_i \frac{I_j^{\alpha}}{\sum_{m\in\Gamma_i} I_m^{\alpha}},\end{aligned} \tag{12}$$

where Γ_i denotes the neighboring node set of v_i, L_m and C_m represent the load and capacities of the neighboring node v_m in the set Γ_i, and L_j and C_j represent the load and capacities of the failure node v_j.

So, the load of the node v_j is updated as follows:

$$L_j' = L_j + \Delta L_j. \tag{13}$$

Further, if the load $F_j(t)$ of the node v_j exceeds its capability C_j, then

$$F_j(t) > C_j. \tag{14}$$

The node v_j would also fail, which triggers the cascading failure of C2 networks.

3. Simulation Verification and Analysis

Based on the C2 network model established in the literature [37], the effectiveness and feasibility of the cascading failure model of C2 networks proposed in this paper are verified. This reference takes an air defense C2 network system of the Army as an example. A typical C2 network model is established, and it includes three types of nodes and three kinds of relations of exchanging information. The total number of nodes is 5,213, and among them, the number of command nodes is 1,023; the number of sensor nodes is 350; the number of fire nodes is 3,840. The number of command layer is 5.

The technique for order of preference by similarity to ideal solution (TOPSIS), as a method of determining the index weight, has been widely used in the evaluation of node importance in complex networks. In this paper, the technique is used to solve the weight coefficient of the degree and the combat link betweenness in the evaluation index of node importance. The results are as follows: $\omega_1 = 0.37$ and $\omega_2 = 0.63$.

Considering the hierarchy of the C2 network structures and the complexity of the algorithm, the order number of the neighboring node and the hierarchy of the network in the simulation are set as the same, and so, we set $m = 4$.

To effectively evaluate the importance of each node in the C2 networks and to verify the importance of the node method, the most reasonable initial load is obtained by adjusting the initial load parameter u ($u \in \{0.6, 0.7, 0.8, 0.9, 1.0\}$) to improve the anticascading failure ability of the C2 networks. The change curve of the node importance is shown in Figure 3.

By comparing the changes in the importance of nodes at different parameters u, the following conclusions can be drawn:

(1) When $u = 1.0$, the importance of a node is only relevant to its own attributes. In other words, the importance of a node is determined by the degree of the node itself and the combat link betweenness without considering the influence of the neighboring nodes. As a typical complex network, C2 networks exhibit scale-free characteristics, and the network has more edge nodes. It can be observed from Figure 3 that the importance curve of the edge node is a straight line because the edge node has a value of 1, and the value of combat link betweenness is 0. The comprehensive calculation is still a fixed value, which presents a straight line trend. Consequently, the importance of the edge nodes is not distinguished.

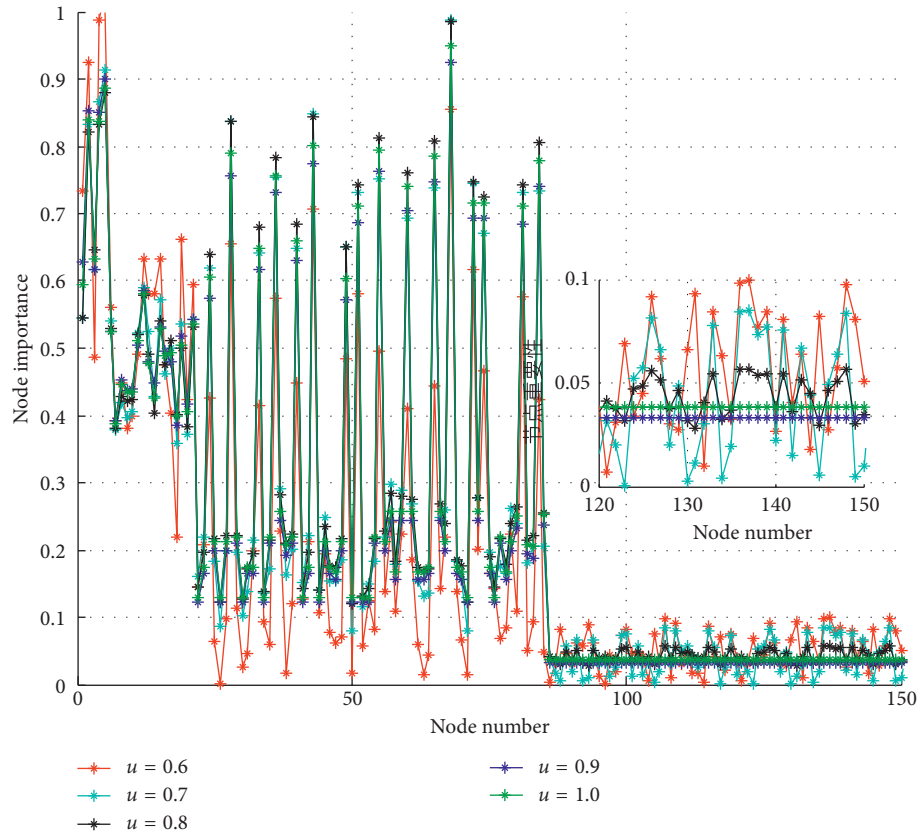

Figure 3: The change of node importance with parameter u.

Considering only the importance of the node itself cannot effectively identify the differences between nodes and reduces the accuracy of the initial load of nodes in C2 networks.

(2) When $0.5 < u < 1$, the importance of nodes is determined by their own importance and the contribution degree of neighboring nodes. As u decreases, the effect of m-order neighboring nodes on the node increases, which not only provides an accurate evaluation of the importance of central nodes but also distinguishes the importance of edge leaf nodes. Therefore, the use of the contribution degree of m-order neighboring nodes method can better describe the importance of nodes and provide more accurate initial load value.

The average scale of failure as an important indicator of network performance can analyze the effect of dynamic cascading failure on the invulnerability of the network. It is defined as follows:

$$\mathrm{CF} = \frac{1}{N(N-1)} \sum_{v_i \in V} \mathrm{CF}_i. \tag{15}$$

Among them, CF_i is the total number of other nodes that have failed, which is caused by the network node v_i that has failed, $0 \le \mathrm{CF}_i \le N-1$. The smaller the value of CF, the stronger the cascading invulnerability of the C2 networks; otherwise, the weaker the cascading invulnerability of the C2 networks. When $\mathrm{CF} \approx 0$, the network is almost intact and invulnerability is strong. When $\mathrm{CF} \approx 1$, the network is almost collapsed and invulnerability is weak.

To further analyze the behavior of $\mathrm{CFM}_{\mathrm{AdjM}}$, when the value of the initial load parameter u is set, the performance of the cascading invulnerability of C2 networks is improved. The average failure scale CF is considered the cascading invulnerability evaluation index, and when the parameter α assumes different values, changes in the trend of cascading invulnerability with the tolerance parameter β is comprehensively compared, as shown in Figure 4.

Based on the comparative analysis of different parameters, it can be seen that the smaller the value of parameter u, the faster the average failure scale CF drops and the better the cascading invulnerability of the network. When $\alpha < 1$, the invulnerability of the C2 network is greatly affected by the initial load. The results then indicate that the cascading invulnerability of $u = 0.6$ is the strongest. In the initial load definition, the more the contribution of the neighboring nodes is considered, the better is the cascading invulnerability of the network. When $\alpha \ge 1$, the capacity of each node gradually increases. At this time, the cascading invulnerability is greatly affected by capacity and less affected by the initial load parameter u. Therefore, all the curves of u in the graph are more intensive, and the degree of discrimination is not large, but the cascading invulnerability of $u = 0.6$ is better.

As the tolerance parameter β increases, the average failure scale CF decreases gradually, and the larger the value

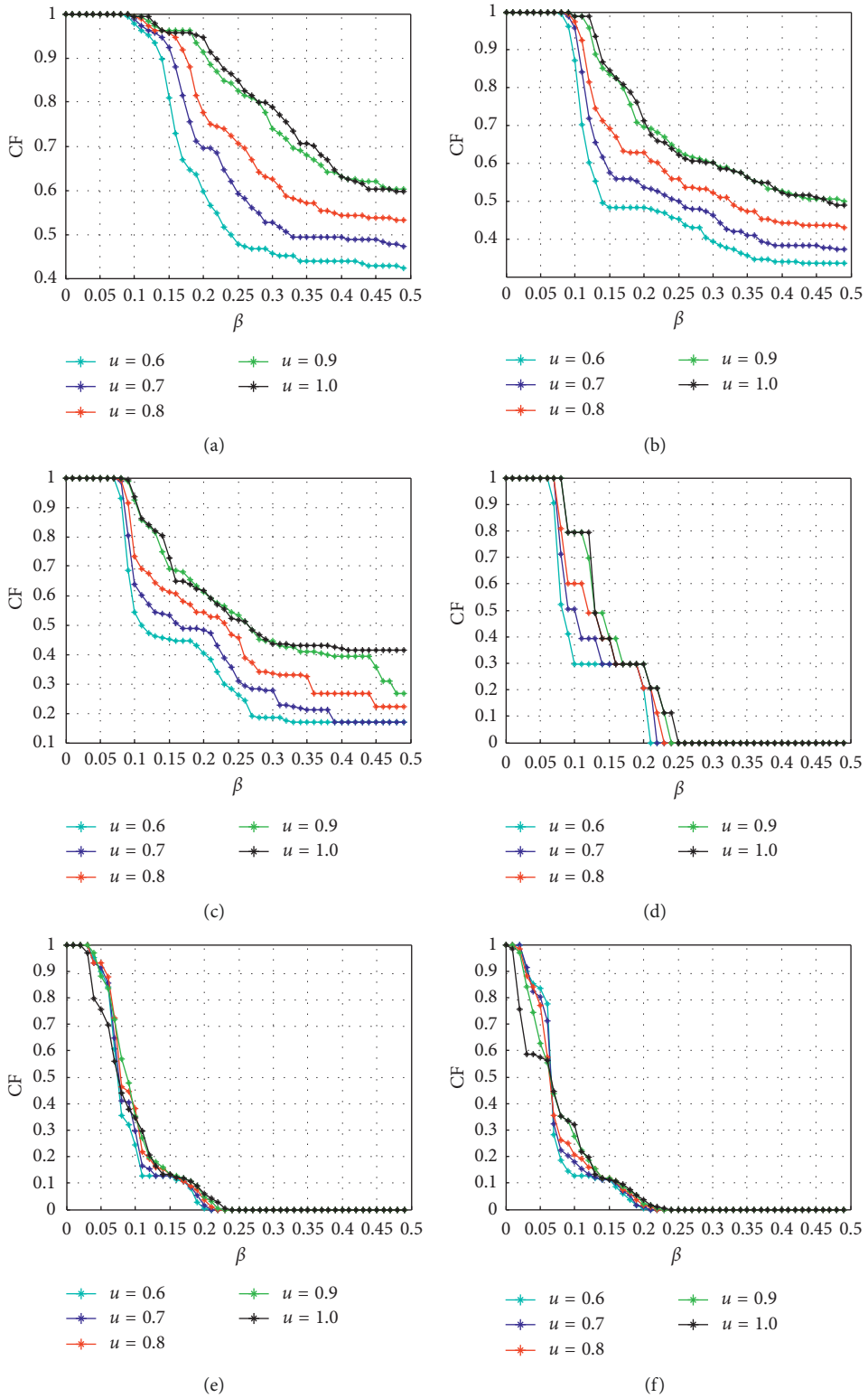

FIGURE 4: Influence of initial load parameter u on cascading invulnerability. (a) $\alpha = 0.4$. (b) $\alpha = 0.6$. (c) $\alpha = 0.8$. (d) $\alpha = 1.0$. (e) $\alpha = 1.2$. (f) $\alpha = 1.4$.

of parameter α, the faster the average failure scale CF decreases. The larger the values of the tolerance parameter β and parameter α, the smaller the average failure scale CF and the stronger is the anticascade failure capability of the network. This is consistent with prior analysis in which the greater the nonlinear load capacity, the stronger is the anticascading failure capability. However, if the parameter α is too large, the improved cascading invulnerability of the

network is achieved at the expense of additional wasted resources and increased construction costs.

In order to verify the effect of the nonlinear parameter α on the cascading invulnerability of the network, $\alpha \in \{0.6, 0.8, 1.0, 1.2, 1.4\}$ is adopted, setting the parameter $u = 0.6$, and the change curve of the network invulnerability with the parameter β is shown in Figure 5, after the average value of 50 simulations is calculated.

It can be seen from Figure 5 that the average failure scale CF decreases rapidly with increasing values of the parameters α and β, and the anticascade failure ability of the C2 network is also correspondingly improved. However, when β is greater than 0.2, changes in the trend tend to be a straight line and has little effect on the average failure scale of the network. Similarly, the greater the value of α, the greater the load that the node can bear. The possibility of cascading failures in the C2 networks is reduced, but if α is too large, the construction cost will rise. When $\alpha \geq 1$, the average failure scale decreases rapidly. When $\beta = 0.2$, CF drops to 0, and the network does not result in any cascading failure phenomenon. This leads to significant waste of resources. When $\alpha = 1$, that is, the linear capacity model and the hierarchical structure of the network are at the same level and have the same impact on the average failure scale of the network. When $\alpha < 1$, with the increase in β, CF rapidly declines. When $\beta > 0.2$, CF is reduced to a very small value. Adjusting initial load parameters to achieve the purpose of anticascade failure saves load capacity resources and reduces construction costs.

To further verify the rationality and feasibility of the cascading failure model, the cascading failure model based on an m-order adjacency matrix proposed in this paper is compared with the typical cascading failure model. The definition method of the initial load for traditional cascade failure model adopts degree and betweenness. Considering the different limited parameters α to comprehensively verify the model in this paper, the variation trend of the cascading invulnerability index CF with the tolerance parameter β is shown in Figure 6.

In Figure 6, it can be seen that the average failure scale CF decreases gradually with the increase of the parameters β in the six groups of different values of the parameter α, and the average failure scale in the proposed method drops faster than other methods, and the cascade failure resistance is stronger. When $\alpha < 1$, with the increase of parameters β, the load capacity of nodes increases and the load ability of nodes also increases, but among the three definition methods of the initial load, the average failure scale in the proposed method decreases the fastest, and the effect of anticascade failure is the best. When $\alpha \geq 1$, with the increase of parameters β, the average failure scale CF in the three methods decreases equivalently. Although the increase of parameters α and β will further increase the load capacity of the network and effectively improve the ability of anticascade failure, the increase of load capacity will increase the construction cost of the network greatly. Therefore, among the three definition methods of the initial load, the cascade failure model established in this paper is superior to the other two. It also shows that the initial load has a significant impact on cascade invulnerability of networks, that is, a reasonable definition of the initial load can effectively improve the cascade invulnerability of networks.

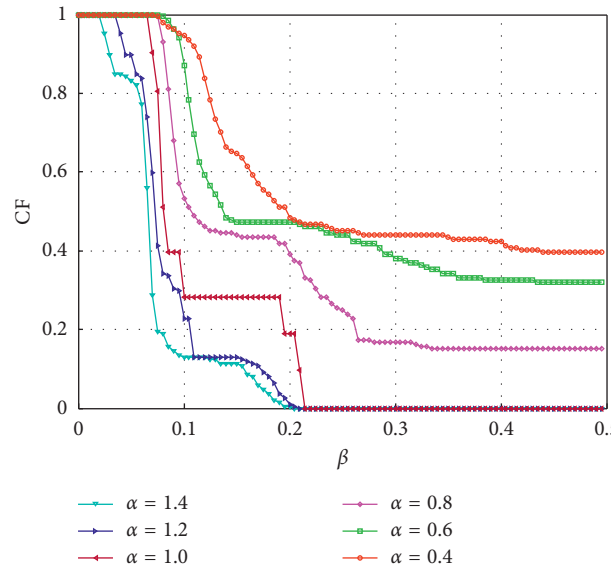

Figure 5: Influence of nonlinear parameter on the cascading invulnerability of the network.

At present, another index commonly used to measure the invulnerability of C2 networks is the survival rate of nodes. The formulas are as follows [28]:

$$G = \frac{N'}{N_0}. \tag{16}$$

Among them, N_0 is the total number of nodes in the network at the initial time and N' is the number of nodes working normally in the network after the cascade failure terminates at a certain time. Obviously, the larger the index and the smaller the cascading failure of network, the better the invulnerability of network.

In order to further analyze the superiority of the cascade failure model proposed in this paper, the survival rate of nodes G and average scale of failure CF are used as the cascaded invulnerability measure of C2 network. The cascade failure model proposed in this paper is compared with several typical cascade failure models of C2 network. The relationship between network survivability and attack ratio p is shown in Figure 7 under different cascading failure models. Among them, model I is the cascade failure model of C2 network established in this paper; model II defines the initial load based on the degree of node and adopts the nonlinear capacity model; model III defines the initial load based on the degree of node and adopts the linear capacity model; model IV defines the initial load based on betweenness and adopts the linear capacity model; model V defines the initial load based on the betweenness and uses the nonlinear capacity model; and model VI defines the initial load based on the combination of degree and betweenness and uses the nonlinear capacity model.

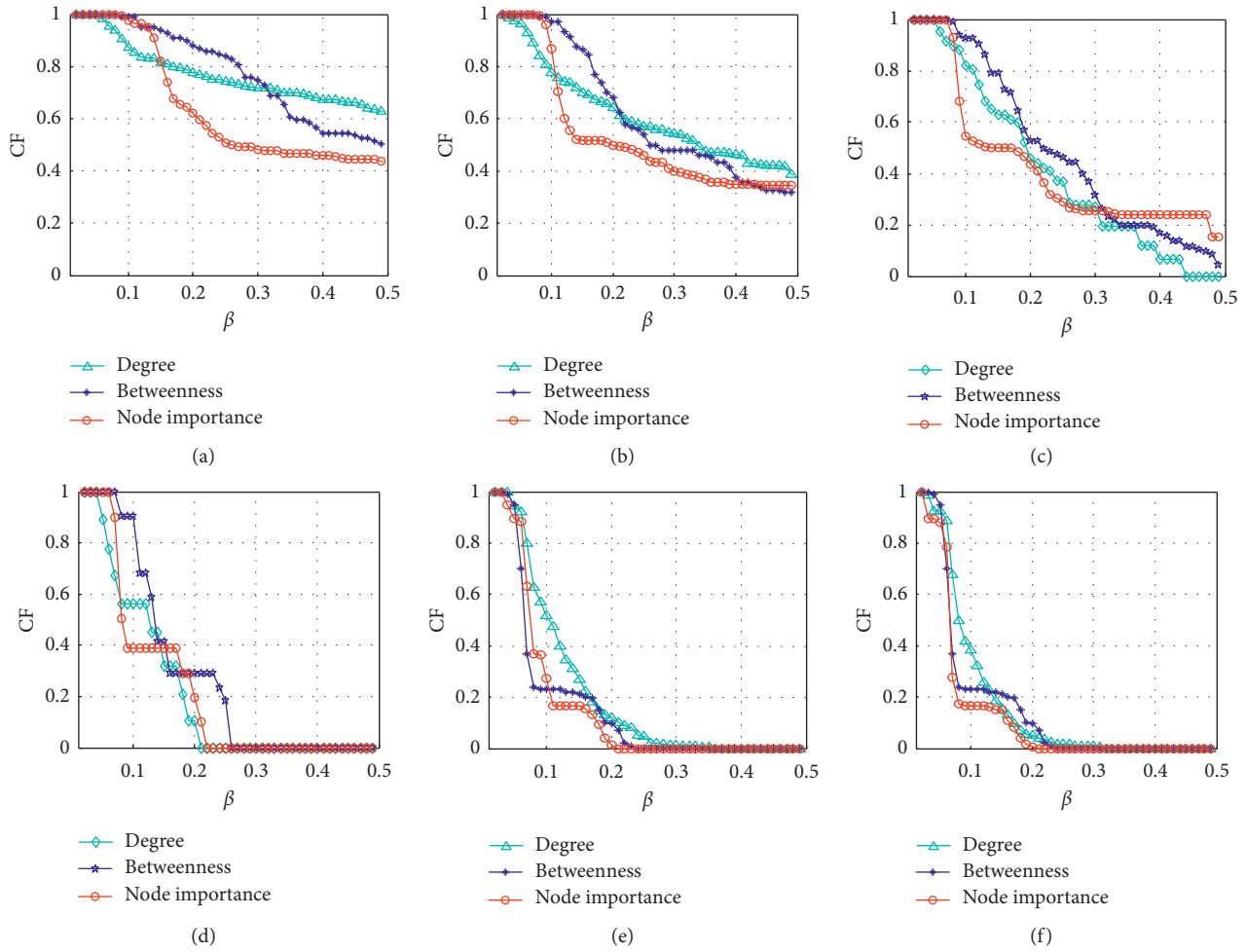

Figure 6: The comparison graph of cascading invulnerability with different limits. (a) $\alpha = 0.4$. (b) $\alpha = 0.6$. (c) $\alpha = 0.8$. (d) $\alpha = 1.0$. (e) $\alpha = 1.2$. (f) $\alpha = 1.4$.

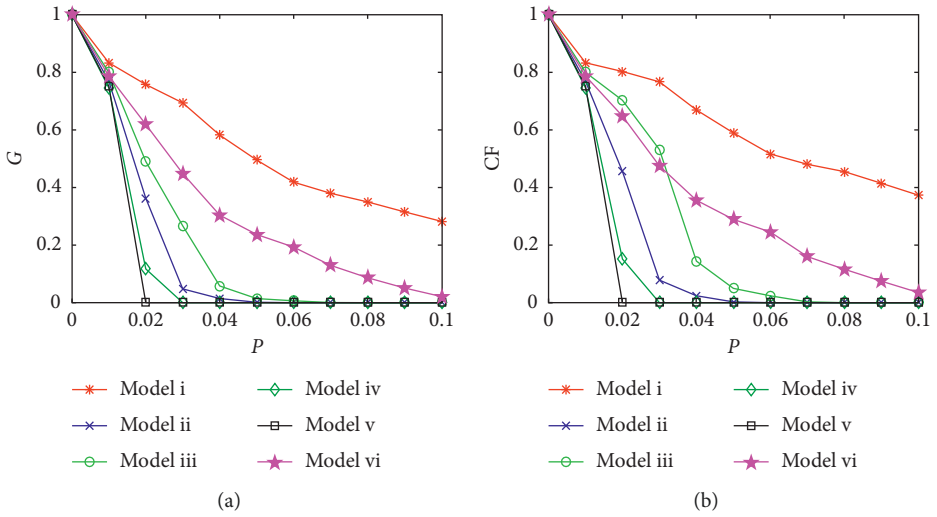

Figure 7: The influence of different cascading failure models on the C2 network invulnerability.

By comparing the cascade failure model proposed in this paper with other cascade failure models, the following conclusions can be drawn: (1) the invulnerability of C2 network decreases with the increase of the attack ratio p, regardless of the way of initial load definition and capacity model. (2) The network has the worst ability to resist cascading failures, when the initial load is defined by degree. Due to the influence of the hierarchical structure of C2 network, the high-level nodes are in the center of the network and have a large betweenness. The low-level nodes are at the edge of the network and have a small betweenness. The value of the betweenness of the nodes in the whole network varies greatly, which leads to the uneven distribution of the load and capacity of the nodes in the network. The whole network is easy to collapse when the network suffers targeted attacks. (3) The cascade model of C2 network proposed in this paper is more invulnerable than other models, because the definition of initial load considers not only the impact of the node on the network but also the impact of the neighbor nodes on the network. It can distinguish the initial load of the nodes more strictly than the traditional method, and its accuracy is relatively high. The above analysis also shows that the initial load and load capacity model have a significant impact on cascade invulnerability of the network, that is, a reasonable way of defining the initial load and load capacity model can effectively improve the cascade invulnerability of the network.

4. Conclusion

The cascading failure problem in C2 networks was studied in this paper, and a new cascading failure model based on an m-order adjacency matrix was established. In the process of constructing the cascading failure model, an initial load definition method based on the contribution degree of m-order neighboring nodes was proposed. The load definition utilized the degree and the combat link betweenness, including the importance of the node itself and the contribution degree of its m-order neighboring nodes. The nonlinear load capacity model was studied. Based on experimental simulation, the influence of model parameters on the cascading failure behavior of C2 networks is analyzed. The results are promising and indicate that the invulnerability of C2 networks can be enhanced by reasonably defining the initial load and adjusting the model's coefficients.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

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

Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant number 91338104 and the Defence Advance Research Foundation of China under Grant numbers 61400010303, 61401310101, and 61400010301.

References

[1] X. Song, W. Shi, G. Tan, and Y. Ma, "Multi-level tolerance opinion dynamics in military command and control networks," *Physica A: Statistical Mechanics and its Applications*, vol. 437, pp. 322–332, 2015.

[2] Y. S. Lan, K. Yi, and H. Wang, "Delay assessment method for networked C4ISR system architecture," *Systems Engineering & Electronics*, vol. 35, no. 9, pp. 1908–1914, 2013.

[3] H. G. Hwang, H. K. Kim, and J. S. Lee, "An agent based modeling and simulation for survivability analysis of combat system," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 16, no. 12, pp. 2581–2588, 2012.

[4] S. D. Li, L. X. Li, Y. Jia, and Y. X. Yang, "Identifying vulnerable nodes of complex networks in cascading failures induced by node-based attacks," *Mathematical Problems in Engineering*, vol. 2013, Article ID 938398, 10 pages, 2013.

[5] M. Liang, Z. Gang, and D. Wang, "A novel method for survivability test based on end nodes in large scale network," *KSII Transactions on Internet & Information Systems*, vol. 9, no. 2, pp. 620–636, 2015.

[6] J. Rak, "Measures of region failure survivability for wireless mesh networks," *Wireless Networks*, vol. 21, no. 2, pp. 673–684, 2015.

[7] S. Chattopadhyay, H. Dai, D. Y. Eun, and S. Hosseinalipour, "Designing optimal interlink patterns to maximize robustness of interdependent networks against cascading failures," *IEEE Transactions on Communications*, vol. 65, no. 9, pp. 3847–3862, 2017.

[8] J. Liu, Q. Xiong, and X. 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.

[9] D. H. Kim and A. E. Motter, "Resource allocation pattern in infrastructure networks," *Physics A: Mathematical and Theoretical*, vol. 41, no. 22, article 224019, 2008.

[10] L. Ding, V. C. M. Leung, and M. S. Tan, "Robustness of complex networks with both unidirectional and bidirectional links against cascading failures," *Modern Physics Letters B*, vol. 31, no. 27, article 1750252, 2017.

[11] Z. Zhang, W. An, and F. Shao, "Cascading failures on reliability in cyber-physical system," *IEEE Transactions on Reliability*, vol. 65, no. 4, pp. 1745–1754, 2016.

[12] H. Yu, Z. Liu, and Y. J. Li, "Using local improved structural holes method to identify key nodes in complex networks," in *Proceedings of Fifth International Conference on Measuring Technology and Mechatronics Automation*, pp. 1292–1295, Hong Kong, China, January 2013.

[13] C. Q. Fu, Y. Wang, and X. Y. Wang, "Research on complex networks' repairing characteristics due to cascading failure," *Physica A: Statistical Mechanics and its Applications*, vol. 482, pp. 317–324, 2017.

[14] R. R. Liu, L. Ming, and C. X. Jia, "Cascading failures in coupled networks: the critical role of node-coupling strength across networks," *Scientific Reports*, vol. 6, no. 1, article 35352, 2016.

[15] Y. M. Wang, S. Chen, C. S. Pan, and B. Chen, "Measure of invulnerability for command and control network based on mission link," *Information Sciences*, vol. 426, pp. 148–159, 2017.

[16] P. Paci, T. Colombo, and G. Fiscon, "SWIM: a computational tool to unveiling crucial nodes in complex biological networks," *Scientific Reports*, vol. 7, article 44797, 2017.

[17] K. Al, A. Dudin, V. Klimenok, and S. Dudin, "Generalized survivability analysis of systems with propagated failures," *Computers & Mathematics with Applications*, vol. 64, no. 12, pp. 3777–3791, 2012.

[18] H. J. Sun, H. Zhao, and J. J. Wu, "A robust matching model of capacity to defense cascading failure on complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 387, no. 25, pp. 6431–6435, 2008.

[19] E. Bompard, A. Estebsari, and T. Huang, "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.

[20] K. J. Kim, K. S. Kwak, and B. D. Choi, "Performance analysis of opportunistic spectrum access protocol for multi-channel cognitive radio networks," *Journal of Communications and Networks*, vol. 15, no. 1, pp. 77–86, 2013.

[21] H. Chen, J. Zhang, W. B. Du, J. M. Sallan, and O. Lordan, "Cascading failures with local load redistribution in interdependent Watts–Strogatz networks," *International Journal of Modern Physics C*, vol. 27, no. 11, article 1650125, 2016.

[22] H. R. Liu, Y. L. Hu, R. R. Yin, and Y. J. Deng, "Cascading failure model of scale-free topology for avoiding node failure," *Neurocomputing*, vol. 260, pp. 443–448, 2017.

[23] A. Shen, J. Guo, and Z. Wang, "Research on methods for improving robustness of cascading failures of interdependent networks," *Wireless Personal Communications*, vol. 95, no. 3, pp. 2111–2126, 2017.

[24] X. J. Wang, S. Z. Guo, L. Jin, and M. Chen, "Cascading failures mechanism based on betweenness-degree ratio distribution with different connecting preferences," *International Journal of Modern Physics C*, vol. 28, no. 4, article 1750052, 2017.

[25] D. X. Zhang, D. Zhao, Z. H. Guan, Y. H. Wu, M. Chi, and G. L. Zheng, "Probabilistic analysis of cascade failure dynamics in complex network," *Physica A: Statistical Mechanics and its Applications*, vol. 461, pp. 299–309, 2016.

[26] A. Moussawi, N. Derzsy, X. Lin, B. K. Szymansk, and G. Korniss, "Limits of predictability of cascading overload failures in spatially-embedded networks with distributed flows," *Scientific Reports*, vol. 7, no. 1, article 11729, 2017.

[27] X. Z. Peng, H. Yao, J. Du, Z. Wang, and C. Ding, "Load-induced cascading failures in interconnected networks," *Nonlinear Dynamics*, vol. 82, no. 1-2, pp. 97–105, 2015.

[28] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, no. 6, article 065102, 2002.

[29] D. H. Kim, B. J. Kim, and H. Jeong, "Universality class of the fiber bundle model on complex networks," *Physical Review Letters*, vol. 94, no. 2, article 025501, 2005.

[30] F. Xue, E. Bompard, T. Huang, L. Jiang, S. F. Lu, and H. Y. Zhu, "Interrelation of structure and operational states in cascading failure of overloading lines in power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 482, pp. 728–740, 2017.

[31] Z. Y. Jiang and J. F. Ma, "An efficient local cascade defense method in complex networks," *International Journal of Modern Physics C*, vol. 28, no. 3, article 1750031, 2017.

[32] Y. Moreno, J. B. Gómez, and A. F. Pacheco, "Instability of scale-free networks under node-breaking avalanches," *Europhysics Letters (EPL)*, vol. 58, no. 4, pp. 630–636, 2001.

[33] P. G. Sun and X. Ma, "Controllability and observability of cascading failure networks," *Journal of Statistical Mechanics Theory and Experiment*, vol. 2017, no. 4, Article ID 043404, 2017.

[34] X. E. Gao, K. Q. Li, and B. Chen, "Invulnerability measure of a military heterogeneous network based on network structure entropy," *IEEE Access*, vol. 6, pp. 6700–6708, 2017.

[35] M. Tian, X. Wang, Z. Dong et al., "Cascading failures in interdependent modular networks with partial random coupling preference," *Modern Physics Letters B*, vol. 31, no. 29, article 1750267, 2017.

[36] P. Li, B. H. Wang, H. Sun, P. Gao, and T. Zhou, "A limited resource model of fault-tolerant capability against cascading failure of complex network," *European Physical Journal B*, vol. 62, no. 1, pp. 101–104, 2008.

[37] Y. M. Wang, C. S. Pan, B. Chen, and D. P. Zhang, "Evolution model of weighted command and control network based on local world," *Systems Engineering and Electronics*, vol. 39, no. 7, pp. 1596–1603, 2017.