IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 24, 2019, accepted December 7, 2019, date of publication December 12, 2019,
date of current version December 31, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2959122

Mitigation Strategy for the Cascading Failure of Complex Networks Based on Node Capacity Control Function

TIAN-CHI TONG[1], YUAN JIANG[1], YI ZHOU[1], XIAO-QIANG ZHUANG[2], WEI-BAI DUAN[1], AND XU PENG[1]

[1]School of Information Engineering, Nanchang Hangkong University, Nanchang 330063, China
[2]Han's Laser Technology Industry Group Company, Ltd., Shenzhen 518000, China

Corresponding author: Yuan Jiang (jiangyuan@nchu.edu.cn)

This work was partially supported by National Natural Science Foundation of China (No. 61663030, No. 61663032), Natural Science Foundation of Jiangxi Province (No. 20142BAB207021), the Foundation of Jiangxi Educational Committee (No. GJJ150753), the Open Fund of Key Laboratory of Image Processing and Pattern Recognition of Jiangxi Province (Nanchang Hangkong University) (No. TX201404003), Key Laboratory of Nondestructive Testing (Nanchang Hangkong University), Ministry of Education (No. ZD29529005) and the reform project of degree and postgraduate education in Jiangxi (No. JXYJG-2017-131).

ABSTRACT A single node failure capacity control function taking into account attack strength, attack times, control node load intensity and the degree of attacked node is proposed in this paper to mitigate the cascading failure of complex networks under random attack. An optimal probability allocation mechanism of redundant resources is established by targeting the load of each neighbor node. Then, the node failure capacity control function and allocation mechanism are used to define the phase transition critical factor and robustness indicator that used the attack strength, control node load intensity and the degree of attacked node as the parameters. Based on the above analysis, the phase transition critical factor model of degree distribution of scale-free network and random network is derived, and the dynamic change law between the parameters and phase transition critical state as well as robust performance of classical network and real network is analyzed. The theoretical and experimental results show that in the controllable region, the smaller the degree of attacked node, the greater the control node load intensity and the more difficult the phase transition critical state to be achieved, and the better the effect of mitigating cascading failure. Besides, the robustness of the network with cascading failure is mutually affected by the control node load capacity, the degree of attacked node and phase transition critical factor within a certain range, which thus embarks on a new perspective to mitigate the failure.

INDEX TERMS Cascading failure, node failure capacity control function, phase transition critical factor.

I. INTRODUCTION

Almost all infrastructure networks in the real world can be regarded as complex networks, such as power grid [1]–[5], communication network [6], transportation network [7]–[9] and the Internet [10], etc., in which there are a large number of nodes connecting to each other as well as links transmitting information and energy. As the information transfer station with storage capacity in the network, the node load is inevitably attacked by the external world during the operation, causing a series of dynamic losses in a network, i.e. cascading failure of complex networks [11]–[13]. When a network is subject to random or deliberate attacks from the external world, some nodes become invalid in the target network, which leads to the redistribution of the node load and the loss of input-output ability of some redistributed node load due to exceeding the load capacity. The failure of these nodes may cause the failure of other nodes through the redistribution. This kind of network chain reaction is called cascading failure, which is significant for making mitigation strategy for network cascading failure, especially for the application of mitigation strategy in the actual network and social network [14]–[17]. Based on the previous research results, we are aware that the ability of each node in the network to bear extra load is limited [18], [19], and grasping node control redundant resources [20]–[23], improving the instantaneous critical state threshold when the network structure is destroyed, optimizing network system parameters and

The associate editor coordinating the review of this manuscript and approving it for publication was Daniel Benevides Da Costa.

adjusting the topological framework of information network are conducive to improving mitigation strategy for cascading failure. Therefore, studying the topology dynamic evolution process of network with cascading failure in external attack environment as well as the node failure capacity control function based phase transition critical factor and other indicators can better mitigate the negative influence of cascading failure.

It is necessary to build the cascading failure model of complex networks and make load redistribution principle before studying the dynamic mechanism of cascading failure and developing the corresponding mitigation strategy. In 2002, Motter and Lai investigated cascading failure based on overload mechanism and proposed the load-capacity model [20]. They defined that the node capacity was directly proportional to the initial load. Motter's load-capacity model was improved in [21], where it was put forward that the higher the initial load is, the larger the extra redundant resources obtained. Lehmann et al proposed a random load redistribution method [24], which depended on the load of the attacked nodes and the distribution was non-uniform and random. Another study [25] proposed to define load local redistribution proportion coefficient Δ by using the degree of the node and the load distribution range of the control failure node as parameters based on the load-capacity model, and a cascading failure model was established by effectively adjusting the range and heterogeneity of load redistribution. The real-time processing capacity index of nodes was defined in [26], and the weight was used as the extra load distribution ratio, and each adjacent node bore the load of failed nodes according to the normalized weight value. In study [27], to better explain the strategy for repairing node failure, large load nodes bore more redistributed load on the basis of shared load. A research report tracked the real-time load state of nodes and took state of adjacent nodes an important index to improve the classical redistribution method [28], and the cascading failure under the probability distribution of load increment and redistribution was analyzed. The overload coefficient reflecting the node's ability to bear extra load, as well as the residual coefficient and failure probability parameter describing the load born by the nodes after the load distribution were introduced in [19], which helped to build the dynamic model close to the actual network failure.

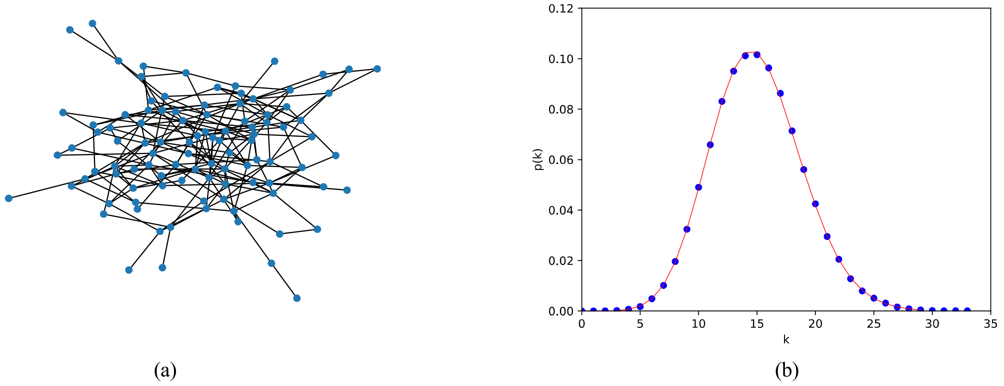
On the basis of the cascading failure model of the overload mechanism, the dynamic behaviors affecting the cascading failure of network nodes was measured, especially the critical state of network where neighbor nodes fail successively due to destroying some nodes, so as to explore how each parameter affected the relationship between the network critical state and network robustness, as well as how to mitigate the failure. Dobson et al. derived the capacity critical value for generating the power-law cascading failure network scale [29]. According to the adjustment control strategy, structural characteristics and network tolerance under three different load redistribution strategies, the corresponding critical model of tolerance coefficient was derived in [24]. Duan proposed to take the node importance index [30] as the critical condition of triggering cascading failure based on the degree of oscillation of node load within the distribution range. Another study [31] obtained the load limit of scale-free network under large-scale cascading failure by setting the critical value of the maximum connected branch which met the minimum application degree of the network in the case of random node failure. Peng et al. analyzed the load adjustment parameters, and studied the network node failure based on the attack threshold of network under external attack [32]. Researchers derived the critical value of the maximum connected branch based on the probability generating function of node failure, and concluded that the large scale cascading failure of scale-free networks could be avoided when the node load was lower than its load limit [18].

This paper is based on the load-capacity model with adjustable parameters. However, most of the previous studies fail to explore the critical conditions and robustness of cascading failure based on node failure capacity control function by considering the attack strength, the degree of attacked nodes and the ability to bear load in different network topologies. In view that any node may be attacked regardless of the importance of the nodes under the external random attack mode, this paper adopts the classic load-node degree correlation function model, follows the newly-defined optimal probability distribution mechanism of neighbor nodes to redistribute the load, and redefines a new node failure capacity control function with various constraints. Besides, the phase transition critical function θ_c and new robustness indicator $R(T)$ are introduced. Two classical network topologies—ER (Erdos-Renyi) random network and BA (Barabasi-Albert) scale-free network are introduced in this paper, and two actual network topologies—ARPA network and CERNET network are used as experimental objects to derive the analytic expression of phase transition critical factor of classical network topologies. The experimental results show that the indicator is effective and feasible. This indicator is used to analyze the dynamic evolution mechanism of node's successive failure and to make strategy to mitigate the cascading failure of the network, and it also helps to improve the robustness of the complex network by moderately weakening the phase transition critical factor. This paper provides strategies for mitigating the damages of cascading failure of complex network under the external random attack mode from the perspective of parameter optimization.

II. TOPOLOGY MODEL OF COMPLEX NETWORK

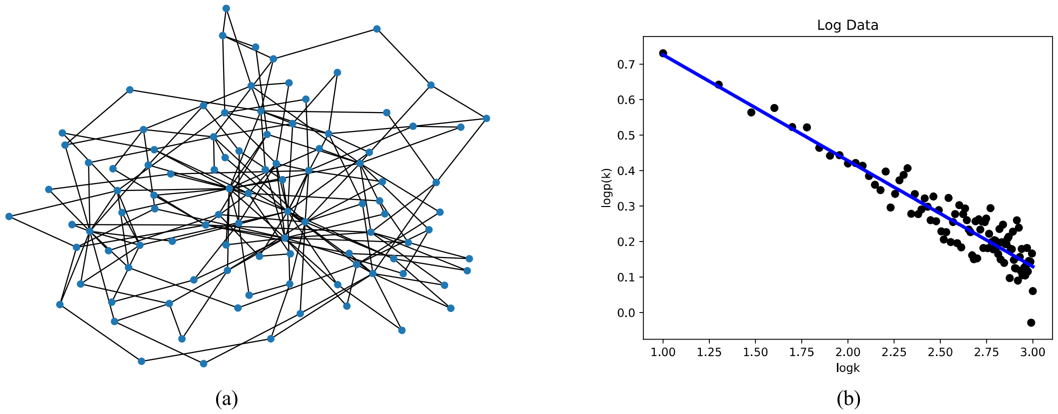
A. TWO CLASSICAL COMPLEX NETWORKS

ER random network [33] and BA scale-free network [34] are common classical complex networks, where the important information contained in a single node and a single edge in the overall structure of the network is revealed. ER random network is a complex random network model that is commonly studied. The compilation environment pycharm is



(a) (b)

FIGURE 1. Characteristics of ER random network. (a) Network topology model (b) Degree distribution.



(a) (b)

FIGURE 2. Characteristics of BA scale-free network. (a) Network topology model (b) Degree distribution.

imported into module networks to build ER random network with 100 nodes and the random edge connection probability of 0.035, as shown in Fig. 1(a). And the degree distribution of ER random network obeys the Poisson distribution, as shown in Fig. 1(b) [33], and it is expressed by[33]:

$$p(k) = \binom{N}{k} p^k (1-p)^{N-k} \approx e^{-\langle k \rangle} \frac{\langle k \rangle^k}{k!} \tag{1}$$

where $\langle k \rangle$ is the average degree and k is the degree of node.

Different from ER random network, the degree distribution of topology of BA scale-free network is not uniform, and the degree distribution function has power-law form, in which few nodes have a high degree while most nodes have a small degree. Once the nodes with a high degree and great importance are attacked, the network paralyzes immediately. The number of initial network nodes is set to be $m_0 = 8$, the number of new edges generated when each new node is introduced is $m = 5$, and the growing network scale is $N = 100$. Assuming that the nodes form a complete graph, the BA scale-free network topology model is constructed, as shown in Fig. 2(a), and the degree distribution of BA scale-free network is as follows [34]:

$$p(k) = ck^{-\lambda} \tag{2}$$

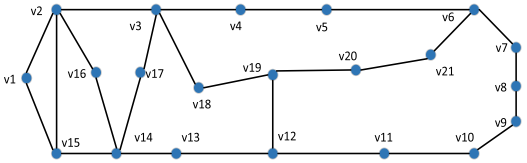


FIGURE 3. ARPA network topology model.

where c is the parameter and λ is the power exponent of the BA scale-free network. The degree distribution of the logarithmic coordinates is shown in Fig. 2(b) [34].

B. TWO ACTUAL COMPLEX NETWORKS

Most of the networks in the real world are irregular in structure and degree distribution. In this paper, two actual networks in real life are studied, which are ARPA network and CERNET network. ARPA network topology is a backbone network topology, mainly used to study the characteristics and properties of the network at present. It is composed of 21 nodes and 23 links, with an average degree between 2 and 3, and its topology model [35] is shown in Fig. 3. CERNET network is the backbone of China's education and scientific research computer network, which consists of 36 nodes and 49 links, with the maximum degree value of 9 and the minimum degree value of 1. Its topology model [36] is shown in Fig. 4.

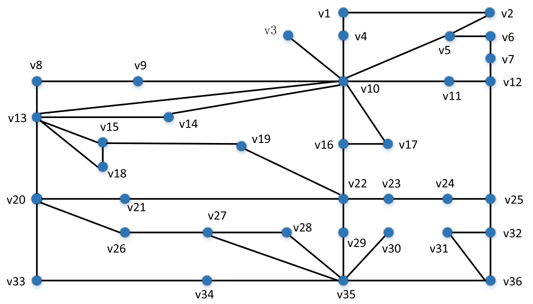


FIGURE 4. CERNET network topology model.

III. OPTIMAL PROBABILITY DISTRIBUTION MECHANISM BASED ON NEIGHBOR NODE LOAD

When describing the cascading failure in the past, the node's failure state was usually directly removed, but in the real world, the load of the attacked nodes is regarded to be distributed to the nodes in the neighbor set according to a certain distribution principle. The network studied in this paper is an unweighted network, where the cascading failure is to utilize the change of complex network topology changes to simulate the successive failure of nodes in the network under external attack based on the dynamic characteristics of the network. Assuming a actual network with N nodes, the load of each node is less than its original capacity at the initial stage, which means the whole network is in a stable state; with the intensity and frequency of external attacks gradually increasing, the attacked node j loses its load capacity and information transmission ability gradually and becomes a failed node, and then the load it bore is distributed to the neighboring unaffected part or intact node i according to certain distribution principle. If the total load of neighbor nodes after increase exceeds their own capacity, they become failed and cannot bear the extra load, and load will be redistributed again, leading to load change of other nodes in the network and thus large-scale cascading failure, as shown in Fig. 5. Therefore, the cascading failure mechanism of complex networks needs to be described from node capacity, node load and the distribution principle of extra redundant resources.

The node load refers to the amount of information carried by a node at a certain time. Based on the correlation between the load and the degree of the node, assuming that the initial load of the attacked node j at the initial stage is $l_j^{(0)}$ and the degree of it is k_j, the initial load is defined as [30]:

$$l_j^{(0)} = \ell k_j^{\tau} \tag{3}$$

where ℓ and τ are two parameters of control node load intensity.

In general, in cascading failure models of many actual networks, with the load objects determined, such as the actual power network, traffic network and Internet, there is a certain correlation between the load and the degree of each node, and the larger the degree of the node, the greater the load it carries. It is reasonable to utilize this dimensionless "structural load" to study the failure propagation process of complex networks under disturbance and the vulnerability of the whole network after attack.

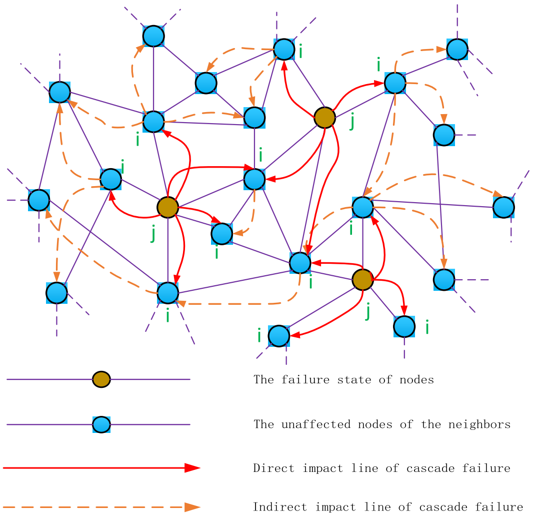

i
j
The failure state of nodes
The unaffected nodes of the neighbors
Direct impact line of cascade failure
Indirect impact line of cascade failure

FIGURE 5. Evolution of Multi-node failure after attack.

In the actual networks, the ability of each node to bear extra load is usually limited by technical and economic factors, and the relationship between load and capacity is studied according to "capacity on-demand". For this reason, due to the limited supply of hardware resources and the influence of harsh environment, the node capacity is controlled by α_j under appropriate conditions. The capacity of the node C_j is defined to be directly proportional to the initial load $l_j^{(0)}$ [25], i.e

$$C_j = (1 + \alpha_j) \times l_j^{(0)} \tag{4}$$

where $j = 1, 2, \cdots, N$, and $\alpha_j > 0$ is node failure capacity control function, indicating the ability of a node to bear extra load to further control the total amount of redundant resources ΔC of the node. It will be introduced in detail in the next chapter.

However, in the actual environment, the node capacity is limited by its own resources, and it cannot obtain the supply energy instantaneously from the external world when the network is subjected to the sudden random attack, so the upper limit of the node capacity has a fixed threshold. The node capacity is redefined as:

$$C_j = \begin{cases} \left(1 + \alpha_j\right) \times l_j^{(0)} & C_j < C_{\max} \\ \psi & C_j = C_{\max} \end{cases} \tag{5}$$

where ψ is the fixed threshold of node capacity.

The total amount of redundant resources ΔC of all nodes in a network is positively correlated with the initial load and capacity control coefficients of each attacked node, which is defined as:

$$\Delta C = \sum\nolimits_{j \in \Omega_j} \alpha_j \times l_j^{(0)} \tag{6}$$

When the network is subjected to the random attack from the external world and the set of attacked nodes $\Omega_j = \{j\,|j = 1, 2, \cdots, N\}$ is destroyed, the total amount of redundant resources is directly transferred to the neighbor nodes of the failed nodes in the network through the adjacent links that transmit information in a certain distribution way. The initial load of the nodes can reflect the ability of the node to process information under the normal operation of the steady-state network, and the larger the initial load, the stronger the node's ability to processing information flowing through it and the more the extra redundant resources to be distributed. This distribution idea is defined as the optimal probability distribution mechanism based on the neighbor node load, that is, the probability distributed to the neighbor intact nodes i is defined as:

$$\prod_i = \frac{\ell k_i^{\tau}}{\sum_{i\in\Omega_i} \ell k_i^{\tau}} \tag{7}$$

where $\Omega_i = \{i\,|i = 1, 2, \cdots N - j\}$ is the intact node set. The proportion α_{ji} of the load of attacked node j distributed to the neighbor intact node i is described as:

$$\alpha_{ji} = \prod_i \alpha_j \tag{8}$$

The redundant resources that are distributed to the neighbor intact node i from the node j are defined as:

$$\Delta C_i = \alpha_{ji} \times l_j^{(0)} \tag{9}$$

Its initial load is distributed to the neighbor intact node i according to the proportion α_{ji}, which results in an update of load of node i.

When the network is under the random attack, a node j quickly fails when attacked, and its load is transferred to partially or entirely intact node, which will result in the failure of this node if the sum of the received load ΔC_i and its own load l_i exceeds its original capacity C_i, that is, $l_i + \Delta C_i > C_i$. The load is distributed to other intact nodes according to the optimal probability distribution mechanism of neighbor node load at the same time, and cascading failure repeats, which leads to the failure of other nodes until the load of the remaining nodes of the network does not exceed their capacities.

IV. NETWORK PHASE TRANSITION CRITICAL INDEX AND ROBUSTNESS BASED ON NODE FAILURE CAPACITY CONTROL FUNCTION

In general, once the actual networks are attacked randomly by the external world in real life, the nodes with self-protection ability and the communication links between nodes are damaged to different degrees. The stronger the attack strength, the more serious the damage. Only the failure of nodes subjected to random attack is considered in the process of cascading failure of complex network in this paper. Therefore, it is necessary to focus on the degree of gradual change of the node load and the influence of attack times and attack strength on the dynamic response of large-scale cascading failure. The attack strength [37] is defined as:

$$\mu = T \times \gamma \tag{10}$$

where T is the attack times and γ is the strength coefficient, indicating the damage degree of each attack to the target.

The capacity of the attacked node j is limited by the external attack times T, the coefficient of attack strength γ, the degree of the node itself and the control load strength parameter τ. The node failure capacity control function is defined as:

$$\alpha_j = \alpha_j\left(T, \gamma, k_j\right) = \beta \frac{T\gamma k_j^{\tau}}{\left\langle k_j^{\tau}\right\rangle} \quad \left(C_j < \psi\right) \tag{11}$$

The distribution of redundant resources is controlled at the same time, and β is the distribution parameter.

$$\left\langle k_j^{\tau}\right\rangle = \frac{1}{N}\sum_{j=1}^{N} k_j^{\tau} = \int_{k_{\min}}^{k_{\max}} k^{\tau} p\left(k\right) dk \tag{12}$$

where $p\left(k\right)$ is the degree distribution of network topology. Based on the optimal probability distribution mechanism of model in the random attack environment, to avoid a series of successive cascading failures, $l_i + \Delta C_i < C_i$ should be met.

To better explore the failure process of any node in random attack, a new indicator θ_c, i.e. the phase transition critical factor is introduced, which is a threshold for measuring whether the network topology jumps violently after the node is attacked. Because the larger the phase transition critical factor is, the more likely each node is to fail, resulting in topology collapse, and cascading failure is more likely to happen. When the intact nodes in the network have strong ability to bear extra load, the successive failure of nodes can be effectively controlled and the system can keep working normally, so that further damage to the global network can be avoided. At this time, the network phase transition trend does not reach the topology structure of the original network maintained by the phase transition critical factor, so the topology phase transition does not happen and it maintains at the steady state; otherwise, the intact nodes fail successively, the network phase transition breaks through the whole network topology constant structure maintained by the critical factor, each node gradually fails, and the network vulnerability gradually increases.

Assuming that the intact node i is in a critical state when receiving extra redundant resources, its capacity is directly proportional to the network phase transition critical factor, i.e.

$$C_{ic} = \theta_c \times l_i \tag{13}$$

In the critical state of network topology phase transition, based on (9) and (13), we have

$$l_i + \alpha_{ji} l_j = \theta_c l_i \tag{14}$$

According to (7), (8) and (11), equation (14) is re-expressed as:

$$\frac{\beta T\gamma k_j^{2\tau}}{\left\langle k_j^{\tau}\right\rangle \sum_{i\in\Omega_i} k_i^{\tau}} = \theta_c - 1 \tag{15}$$

Based on the above-mentioned situations, the randomness of external attacks and the direct or indirect correlation between nodes make the ability of node to bear load seriously affected, and the network topology weakened. To better study the overall damage degree and vulnerability under random attack reflected by the successive failure of network nodes, the effectiveness $R(T)$ of information transmission of the whole network after T attacks are adopted to measure the robustness of network dynamic phase transition scale under the cascading failure model, which is defined as [37]:

$$\begin{aligned} R(T) &= \frac{H(T)}{H(0)} \\ &= \frac{N'(T) \times \sum\limits_{i=1}^{N'(T)} k_i(T)}{N \times \sum\limits_{i=1}^{N} k_i} \end{aligned} \tag{16}$$

where $H(T)$ is the efficiency of information transmission between nodes in the network after T attacks, $N'(T)$ is the number of nodes that have not failed in the network after T attacks, $k_i(T)$ is the node degree after the N^{th} attack, and N is the total number of nodes in the network initially. When subjected to a certain number of attacks, the smaller the effectiveness $R(T)$ of the information transmission between nodes with communication ability, the greater the impact of cascading failure on the topology connectivity and information transmission efficiency, and the weaker the robustness; otherwise, the larger $R(T)$, the smaller the impact of cascading failure on the topology connectivity and information transmission efficiency, the stronger the robustness, and the smaller the cascading failure scale.

When the phase transition critical factor θ_c of network topology decreases gradually, although there is external random attack, the node failure at this can cannot change the network topology, so the system still operates well with good function, and the robustness $R(T)$ is gradually enhanced, which is enough to maintain the normal work of the network. Besides, the network robustness function $R(T)$ will gradually change with the corresponding parameters. When the phase transition critical factor θ_c increases gradually, each node collapses too frequently, and the network robustness function $R(T)$ gradually weakens until it tends to 0.

V. ANALYTIC SOLUTION OF CLASSICAL NETWORK PHASE TRANSITION CRITICAL FACTOR

To explore the gradual evolution of topology structures of BA scale-free network and ER random network under random attack, the destructive power and influence of network resisting cascading failure under the phase transition critical condition controlled by each parameter. Putting (10) in (15), we have:

$$\frac{\beta\mu k_j^{2\tau}}{\left\langle k_j^{\tau}\right\rangle \sum_{i\in\Omega_i} k_i^{\tau}} = \theta_c - 1 \tag{17}$$

According to the conditional probability, we have:

$$\sum_{i\in\Omega_i} k_i^{\tau} = \sum_{k_{\min}}^{k_{\max}} k_j p\left(k' \left| k_j\right.\right) k'^{\tau} \tag{18}$$

where $p(k' \left| k_j\right.)$ is the conditional probability of degree k' of the node neighboring the attacked node j with the degree of k_j.

In degree-independent network, we have:

$$p\left(k' \left| k_j\right.\right) = k' p\left(k'\right) / \langle k\rangle \tag{19}$$

According to (19), equation (18) is simplified into:

$$\begin{aligned} \sum_{i\in\Omega_i} k_i^{\tau} &= \frac{k_j}{\langle k\rangle} \sum_{k_{\min}}^{k_{\max}} p\left(k'\right) k'^{\tau+1} \\ &= \frac{k_j \left\langle k^{\tau+1}\right\rangle}{\langle k\rangle} \end{aligned} \tag{20}$$

Based on the degree distribution of BA scale-free network, i.e. (2), and putting it in (12), we obtain:

$$\begin{aligned} \left\langle k_j^{\tau}\right\rangle &= \int_{k_{\min}}^{k_{\max}} k^{\tau} c k^{-\lambda} dk \\ &= \frac{c}{\tau - \lambda + 1}\left[k_{\max}^{\tau-\lambda+1} - k_{\min}^{\tau-\lambda+1}\right] \end{aligned} \tag{21}$$

Make the maximum degree $M = k_{\max}$ and the minimum degree $m = k_{\min}$, according to study [16], $M = mN^{(\lambda-1)^{-1}}$, $\langle k\rangle = 2m$, $c = (\lambda - 1) m^{\lambda-1}$ in the scale-free network, and therefore,

$$\left\langle k_j^{\tau}\right\rangle = \frac{(\lambda - 1) m^{\tau}}{\tau - \lambda + 1}\left[N^{\frac{\tau-\lambda+1}{\lambda-1}} - 1\right] \tag{22}$$

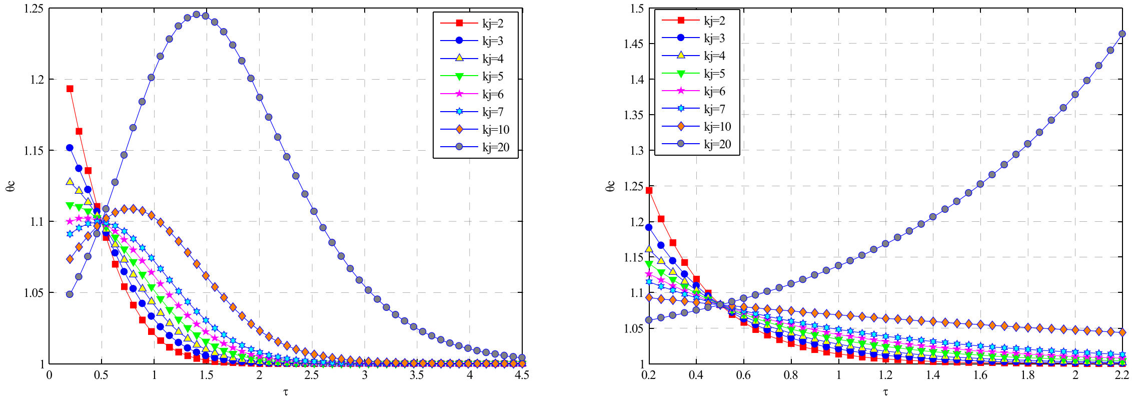
Then, the phase transition critical factor in the BA scale-free network can be expressed as:

$$\theta_c = 1 + \frac{2\beta\mu k_j^{2\tau-1}(\tau - \lambda + 1)(\tau - \lambda + 2)}{m^{2\tau}(\lambda - 1)^2\left(N^{\frac{\tau-\lambda+1}{\lambda-1}} - 1\right)\left(N^{\frac{\tau-\lambda+2}{\lambda-1}} - 1\right)} \tag{23}$$

BA scale-free network itself is to support the whole network with some nodes with large degrees as the key points. Due to the randomness of external attacks, when the nodes with the degree of k_j attacked is the important node, its load-bearing capacity cannot resist the external strength, and θ_c gradually increases, resulting in the change of topology structure and gradually worsening operation of the whole network. Besides, the network topology change performance is also influenced by the external attack strength, the scale-free power index of the whole network, and the ability of the failure node to bear load, etc.

The degree distribution of the ER random network is shown as (1), and then we have:

$$\begin{aligned} \left\langle k_j^{\tau}\right\rangle &= \sum_{k_{\min}}^{k_{\max}} k^{\tau} e^{-\langle k\rangle}\frac{\langle k\rangle^{k}}{k!} \\ &= \langle k\rangle \sum_{I=0}^{\tau-1}\binom{\tau-1}{I}\left\langle k^{I}\right\rangle \end{aligned} \tag{24}$$



(a) (b)

FIGURE 6. Influence of parameter τ on the phase transition critical factors of two classical networks. (a) BA scale-free network (b) ER random network.

Similarly,

$$\left\langle k^{\tau+1}\right\rangle = \langle k\rangle \sum_{I=0}^{\tau}\binom{\tau}{I}\left\langle k^{I}\right\rangle \tag{25}$$

The phase transition critical factor of ER random network can be expressed as:

$$\theta_c = 1 + \frac{\beta\mu k_j^{2\tau-1}}{\langle k\rangle \sum\limits_{I=0}^{\tau-1}\binom{\tau-1}{I}\left\langle k^{I}\right\rangle \sum\limits_{I=0}^{\tau}\binom{\tau}{I}\left\langle k^{I}\right\rangle} \tag{26}$$

The iterative calculation result of (26) is relatively complicated. Based on the homogeneity of ER random network, $\langle k^{\tau}\rangle$ can be approximately seen as $\langle k\rangle^{\tau}$, and then analytic (19) of network phase transition critical factor is directly simplified into:

$$\theta_c = 1 + \frac{\beta\mu k_j^{2\tau-1}}{\langle k\rangle^{2\tau}} \tag{27}$$

Similar to the BA scale-free network, the degrees of nodes in ER random network are generated according to the Poisson distribution law. Some nodes have large degrees, and the external attack strength and other parameters have a great influence on the critical phase transition of the network topology.

VI. SIMULATION EXPERIMENT AND RESULTS ANALYSIS

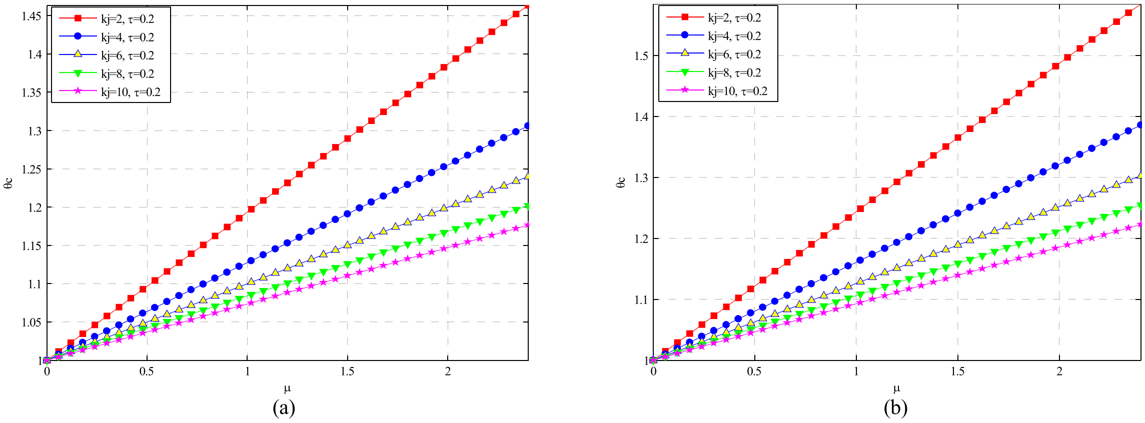
In order to test the accuracy and reliability of the mitigation strategy proposed in this paper, two groups of experiments are carried out to compare and analyze. One is to take BA scale-free network and ER random network as objects to study cascading failure. By analyzing the changes of parameters such as control node load intensity, attack strength and the degree of attacked node, the influence of external random attack on the robustness $R(T)$ and the phase transition critical factor θ_c of the network is studied, so as to prove the accuracy of the mitigation strategy for cascading failure. The other is to take ARPA network and CERNET network in the real world as objects and to simulate the cascading failure process of these two networks by using the strategy proposed in this paper, so as to verify the practicability and reliability of the mitigation strategy proposed.

A. SIMULATION EXPERIMENT AND ANALYSIS OF TWO CLASSIC NETWORKS

In the cascading failure model of two classical networks constructed in this paper, the input parameters of the model mainly includes distribution parameter β, attack strength μ, degree of attacked node k_j, power index λ, control node load intensity τ, network scale N, minimum degree of node m and average degree of network $\langle k\rangle$. Therefore, based on ER random network and BA scale-free network architecture, through controlling these parameters, the behavior mechanism and restriction factors of network under random attack are analyzed, and how to adjust them to mitigate the harm of repeated failure is explored in this simulation.

1) INFLUENCE OF CONTROL NODE LOAD INTENSITY ON CASCADING FAILURE OF TWO CLASSICAL NETWORKS

The control node load intensity τ is an important indicator to represent the initial load of actual networks, and it affects the load-bearing capacity of each initial node in the network, as well as the distribution strength of nodes in the network space structure at the initial time. When subjected to the external random attack, the cascading failure mode is generated. For the BA scale-free network, the network scale is defined to be $N = 100$, minimum degree to be $m = 1$, distribution coefficient to be $\beta = 1$, attack strength to be $\mu = 1$ and power exponent to be $\lambda = 2.1$. For ER random network of the same scale, the distribution coefficient is defined to be $\beta = 1$, attack strength to be $\mu = 1$ and the average degree to be $\langle k\rangle = 12.06$. According to two kinds of cascading failure mechanism models, mainly through the analysis of how the control node load intensity τ reflects its correlation with cascading failure when the degree k_j of attacked node changes, the simulation results are shown in Fig. 6.



(a) (b)

FIGURE 7. Influence of parameter μ on the phase transition critical factors of two classical networks ($\tau = 0.2$). (a) BA scale-free network (b) ER random network.

We can observed from Fig. 6 that the control node load intensity τ has a great influence on the phase transition critical factor θ_c of the network topology. In ER random network, when the degree k_j of the attacked nodes is small, the phase transition critical factor θ_c decreases with the increase of parameter τ, and its convergence to 1 gradually slows down until divergence with the increase of k_j. It is easy to understand. The nodes with enhanced ability to bear load in the network have greater ability to resist external disturbance, so the network topology is less likely to fail. However, when the nodes with larger degrees are attacked by the external world, their neighbor nodes are greatly affected by it. Hence, no matter how the node controls its load, the structure distribution of the network will inevitably change, leading to large-scale failure.

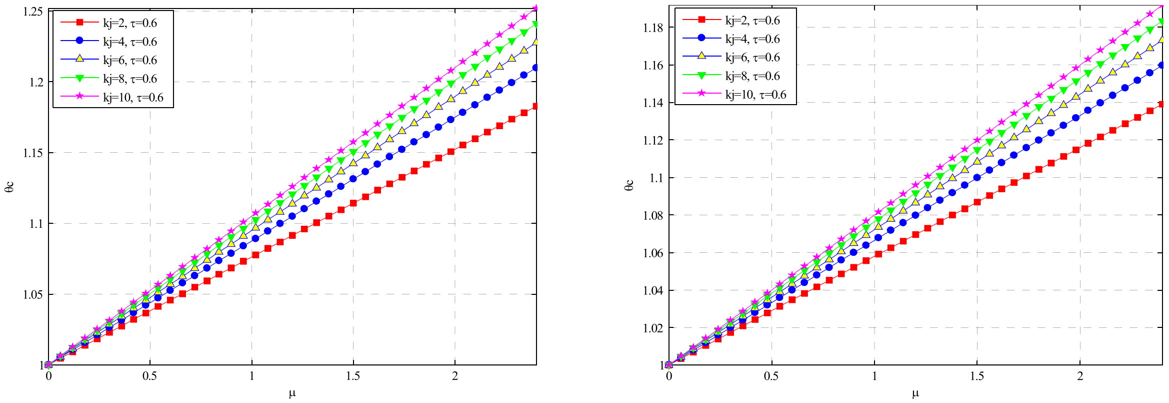
In BA scale-free network, the phase transition critical factor θ_c also decreases with the increase of parameter τ, and its convergence to 1 gradually slows down until divergence with the increase of k_j. However, when the degree k_j of the attacked nodes is large, the phase transition critical factor θ_c first increases and then decreases with the increase of parameter τ due to the heterogeneity of BA network. Hence, to some extent, continuously strengthening the load-bearing capacity does not necessarily improve the invulnerability of the network. The smaller the degree of attacked node k_j, the larger the control load strength τ and the less likely the topological phase transition of cascading failure to occur, which mitigate the adverse situation to some extent.

We can learn by further observation and analysis of Fig. 6 that curves intersect at the same point with coordinate of approximately (0.5,1.1). When $0.2 \leq \tau < 0.5$, θ_c decreases with the increase of k_j; When $\tau \geq 0.5$, θ_c increases with the increase of k_j, and $\theta_c = 1.1$ is the value of the critical state.

2) INFLUENCE OF ATTACK STRENGTH ON THE CASCADING FAILURE OF TWO CLASSICAL NETWORKS

In order to explore the influence of attack strength μ on the change of network topology under the external random attack, we make the distribution coefficient $\beta = 1$, network scale $N = 100$, minimum degree $m = 1$, average degree $\langle k \rangle = 12.06$ and power index $\lambda = 2.1$. Different values of attack strength μ are taken to study the change of damage degree of network topology when the attacked nodes j with different node degrees k_j under different attack strength in two classical networks. We can learn from the simulation test in Fig. 6 that $\tau = 0.5$ is an important critical factor affecting the network phase change structure. Therefore, this simulation test includes two mitigation strategies: strategy 1 with $\tau = 0.2$ when $0.2 \leq \tau < 0.5$, and strategy 2 with $\tau = 0.6$ when $\tau \geq 0.5$. The simulation results of strategy 1 with $\tau = 0.2$ are shown in Fig. 7, and the simulation results of strategy 2 with $\tau = 0.6$ are shown in Fig. 8.

In strategy 1, when the network structure and nodes are not attacked by the external world, $\theta_c = 1$ and the network operates normally. Whether it is BA scale-free network or ER random network, with the increase of attack strength, the damage to the attacked nodes aggravates in the network. At the same time, the number of failed nodes increases continuously because of the load factor transferred through links between nodes, and the phase transition critical factor θ_c of the network topology increases, further triggering the cascading failure of the whole network structure. When the nodes have same capacity τ to bear load, it is the nodes with smaller degree, not the nodes with larger degree that intensify the change of the phase transition critical state of network topology, and when the degree increases gradually, the difference of the network topology change between the curves is gradually reduced. That is to say, the nodes with higher degree are less sensitive to the change of network topology. For this difference, BA scale-free network test results are consistent with those of ER random network. By comparing the data of the nodes of the same degree in two figures of Fig. 7, it can be seen that the nodes of the same degree are more likely to fail successively in BA network than in ER random network under the same attack strength, which reflects the advantage of heterogeneity of degree distribution of nodes in BA scale-free network.



(a) (b)

FIGURE 8. Influence of parameter μ on the phase transition critical factors of two classical networks ($\tau = 0.6$).

Similarly, the phase transition critical factors of two network topologies in strategy 2 with $\tau = 0.6$ are positively correlated with the external random attack strength μ. However, under the premise that the attack strength is constant and the node control load capacity is large, the greater the degree of the attacked nodes, the greater the importance for the network structure, and the faster the failure speed of the network, which leads to failure of the communication between network nodes. It is observed by the test and simulation results that the change state of BA scale-free network and ER random network is the same. When the load-carrying capacity of the node reaches a certain value, the key to restrict the cascading failure is the construction mechanism of the initial network. The nodes of the same degree are more likely to fail successively in the BA network than in the ER random network.

3) INFLUENCE OF PHASE TRANSITION CRITICAL FACTOR AND CONTROL NODE LOAD INTENSITY ON THE ROBUSTNESS OF TWO CLASSICAL NETWORKS

Robustness measures the ability of a network structure to resist damage after being disturbed and attacked by the external world, and it is represented by $R(T)$ in this experiment. The network scale is defined to be $N = 100$, distribution coefficient to be $\beta = 1$, attack times to be $T = T_0 = 100$, the proportion of attacked nodes to be 0.05, attack strength to be $\mu = 1$, minimum degree to be $m = 1$, power index to be $\lambda = 2.1$ and the average degree to be $\langle k \rangle = 12.06$. And then experiment 1 is conducted to study the influence of the phase transition critical factor θ_c on the robustness of two classical networks; experiment 2 is carried out to study the influence of control node load intensity τ on the robustness of two classical networks. Experiment 1 explores the correlation between the parameter θ_c and the robustness under the strong and weak load-bearing capacity of the attacked nodes, and the simulation results are shown in Fig. 9.

We can observe from Fig. 9 that the phase transition critical factor θ_c of the network topology is negatively correlated to the robustness indicator $R(T_0)$ no matter whether the load-bearing capacity of the nodes is low ($\tau = 0.4$) or high ($\tau = 0.6$). In the stage of $1 \leq \theta_c < 1.2$, the decline speed of ER network curve and BA network curve is fast first and then slows down gradually, while in the stage of $1.2 \leq \theta_c < 1.7$, the decline speed of two curves is slow first and then fast, and there are fluctuations in the decline process. Finally the robustness converges to $R(T_0) = 0$, which means the network topology nodes are completely failed. We can observe that the degree of attack nodes in the two networks is the same, and when two networks is in the same phase transition critical state, compared with ER random network, the BA scale-free network structure has poor robustness and is easier to trigger the cascading failure of neighbor nodes. Besides, in the same network topology framework, the nodes with higher degree have poorer ability to maintain the network communication and resist damage under external attack, that is, the nodes with higher degree have poorer robustness. The simulation results of experiment 2 are shown in Fig. 10.

We can observe from Fig.10 that whether the phase transition critical factor is on the left side ($\theta_c = 1.05$) of the key point or on the right side ($\theta_c = 1.12$) of the key point, in the topology framework of two networks, the load-bearing capacity τ of the node is positively correlated to the robustness. In the stage of $0.2 \leq \tau < 0.64$, the curves of the two network structures first rise rapidly and then slowly, while in the stage of $\tau \geq 0.64$, the rising of the curves slows down first and then speeds up gradually, and there are some fluctuations until the robustness converges to $R(T_0) = 1$. It can also be seen that the degree of attack nodes in the two networks is the same, and when the two nodes have the same load-bearing capacity, compared with ER random network, the BA scale-free network has good robustness and is not easier to trigger the cascading failure of neighbor nodes. Besides, whether it is the BA scale-free

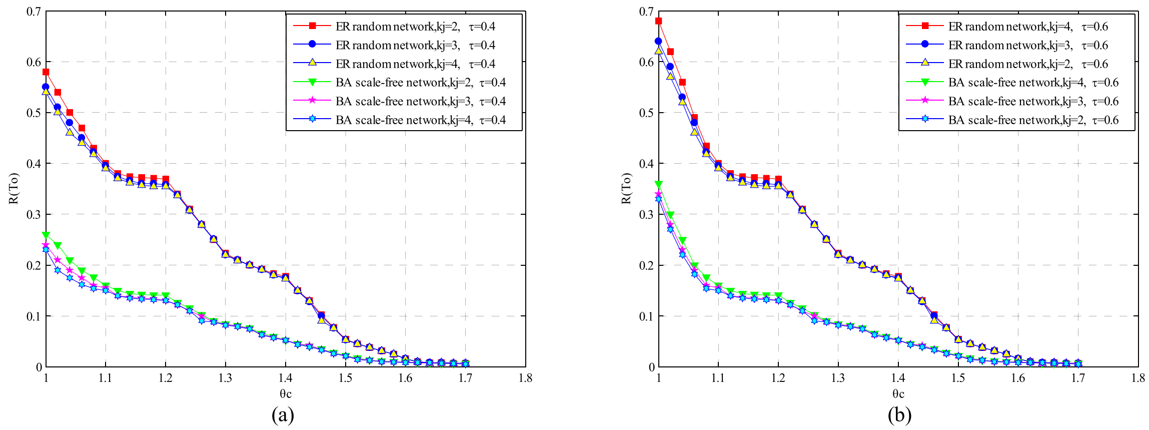


FIGURE 9. Influence of parameter θ_c on the robustness of two networks at different levels of τ. (a) $\tau = 0.4$ (b) $\tau = 0.6$.

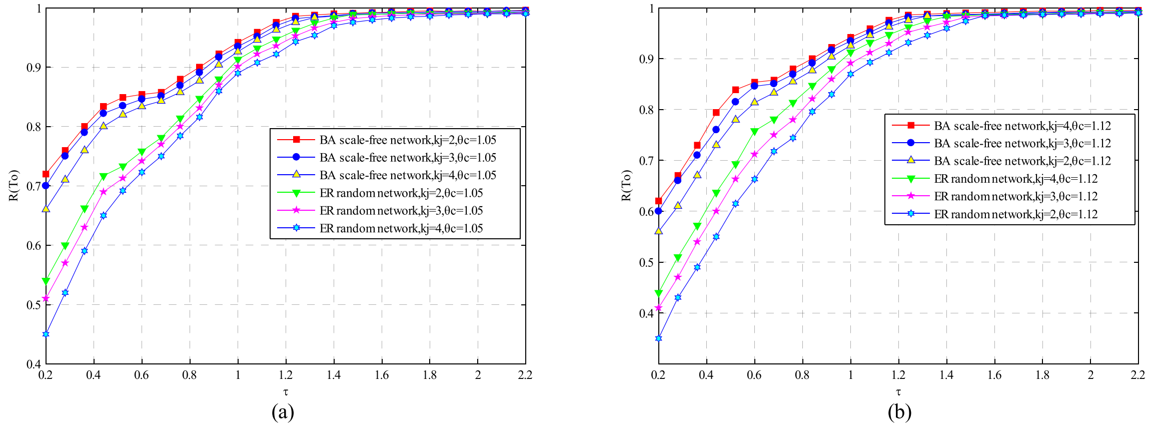


FIGURE 10. Influence of parameter τ on the robustness of two networks at different levels of θ_c. (a) $\theta_c = 1.05$ (b) $\theta_c = 1.12$.

network or the ER random network, when the nodes have the same capacity in handling the load, the higher degree the nodes have, the poorer the robustness of the corresponding network is, and the more likely the cascading failure between neighbor nodes is to happen. In the simulation experiments, the dynamic correlation between the influence parameters and the phase transition critical state as well as the robustness of the network system has well confirmed the conclusion of the theoretical analysis.

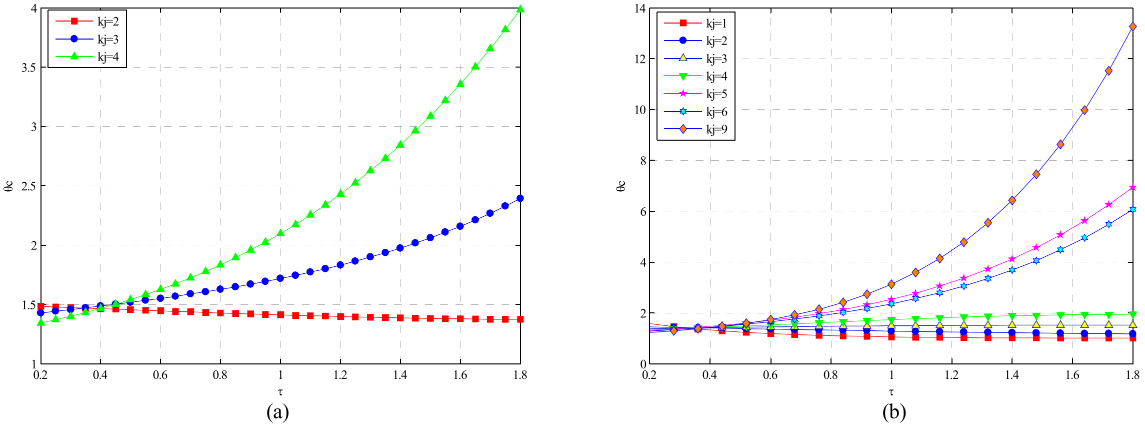
B. SIMULATION EXPERIMENT AND ANALYSIS OF TWO ACTUAL NETWORKS

However, classic network topology structures with regular characteristics, such as BA network and ER network, are not common in real world. Whether the mitigation strategy based on node failure capacity control function proposed in experiment 1 is applicable to actual networks or not, as well as its practicability and reliability need to be verified by ARPA network and CERNET network. In experiment 2, the node degree values of ARPA network topology are 2, 3 and 4 respectively, and the node degree values of CERN network topology are 1, 2, 3, 4, 5, 6 and 9 respectively.

1) INFLUENCE OF CONTROL NODE LOAD INTENSITY ON THE CASCADING FAILURE OF TWO ACTUAL NETWORKS

Similar to experiments of the classical network, as the main index, the control node load intensity τ affects both the load of each initial node in the network and the distribution density of nodes in the network spatial structure. The network scale the two actual networks is 21 and 36 respectively, their distribution coefficient is $\beta = 1$ and their attack strength is $\mu = 1$. Through analyzing how control node load intensity τ reflects its correlation with the cascading failure when the degree of attacked nodes changes, the simulation results are shown in Fig. 11.

We can observe from Fig.11 that whether it is ARPA network or CERNET network, the control load strength parameter τ is not always negatively correlated to the network phase transition critical factor θ_c. It can be known from the ARPA network topology model that it has relatively simple structure and scale, and the nodes with k_j of 3 and 4 account for $1/3$, and these nodes are located in the important hub of the spatial structure model. When attacked, the node with large degree certainly will disturb its neighbor nodes seriously, and no matter how the node strengthens its load



(a) (b)

FIGURE 11. **Influence of parameter τ on the phase transition critical factors of two actual networks. (a) ARPA network (b) CERNET network.**

strength parameters, the structure distribution of the network will inevitably change, which will lead to a large-scale collapse. For nodes with smaller k_j, reasonably increasing the load strength parameters of nodes improves the ability of the whole network to resist external disturbances. Similarly, the structure model of CERNET network is relatively simple, and when a small number of nodes with k_j of 4, 5, 6 and 9 are failed, with the increase of τ, τ is positively correlated with θ_c. And only when parameter τ of the nodes with smaller k_j increases, it is difficult to break through the whole network topology constant structure maintained by the critical factor, so that the cascading failure is not easy to occur.

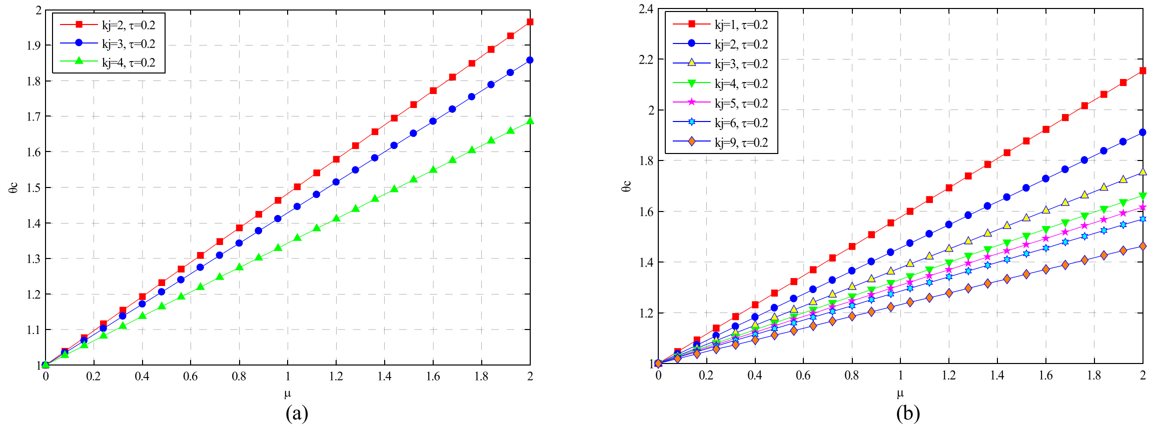
Through further observation and analysis of Fig.11, we can observe that the phase transition critical factor curves of regular networks such as BA network and ER network converge to different points. In the ARPA network, the curves with k_j of 2, 3 and 4 intersect in the area of $\tau \in [0.343{,}0.448]$. When $0.2 \leq \tau < 0.343$, the smaller the degree of attacked node, the larger the θ_c value. When $\tau \geq 0.448$, the smaller the degree of attacked node, the smaller the θ_c value. Similarly, the curves with different k_j values intersect in the area of $\tau \in [0.315, 0.435]$. When $0.2 \leq \tau < 0.315$, the smaller the degree of attacked node, the larger the θ_c value. When $\tau \geq 0.435$, the smaller the degree of the attacked node, the smaller the θ_c value. Therefore, $\tau \in [0.343, 0.448]$ of ARPA network and the corresponding $\theta_c \in [1.465{,}1.479]$ as well as $\tau \in [0.315{,}0.435]$ of CERNET network and the corresponding $\theta_c \in [1.387{,}1.421]$ are the critical areas of dynamic changes of four cascading failures. In order to prevent the interference to the following experiment caused by parameters in the critical area, fixed values $\tau = 0.2, 0.8$, $\theta_c = 1.42, 1.48$ of ARPA network and $\theta_c = 1.38, 1.45$ of CERNET network are set.

Based on the above analysis, parameter τ has the same influence on the two actual networks as on the BA scale-free network and ER random network studied in Fig. 6, that is, for the attacked node with smaller degree k_j, appropriate increase of control load strength τ can effectively mitigate a series of damages caused by cascading failure.

2) INFLUENCE OF ATTACK STRENGTH ON THE CASCADING FAILURE OF TWO ACTUAL NETWORKS

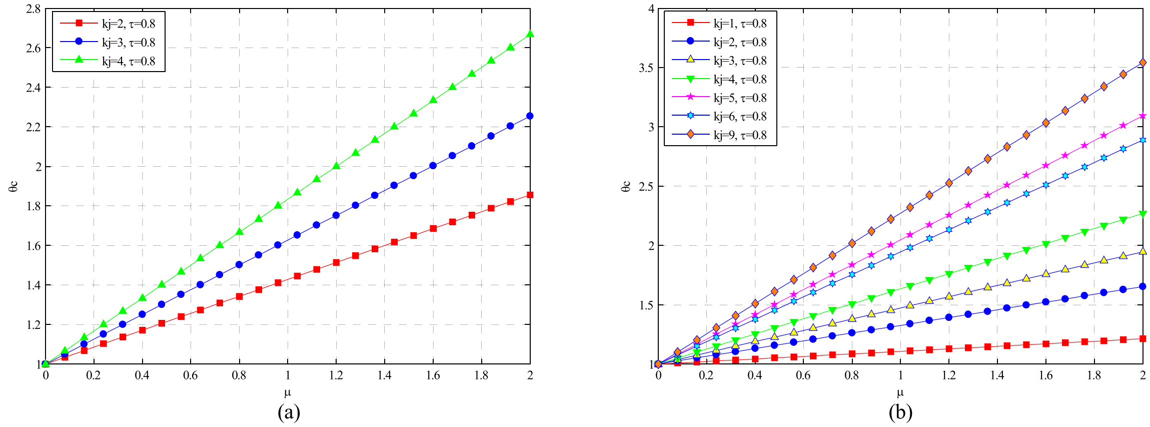
In order to explore the influence of external attack strength μ on the change of network topology, the distribution coefficient is set to be $\beta = 1$, and different μ values are taken to analyze and study the change of extent of damage to network topology when the attacked node j with the degree of k_j in two actual networks is under different attack strength. It can be seen from the simulation results in Fig. 11 that two mitigation strategies are established through fixed values. The simulation results of strategy 1 with $\tau = 0.2$ and strategy 2 with $\tau = 0.8$ are shown in Fig. 12 and Fig. 13 respectively.

In strategies 1 and 2, whether it is ARPA network or CERNET network, with the increase of attack strength under random attack, the damage of the attacked nodes in the network increases sharply, and the phase transition critical factor θ_c of the network topology also increases. In strategy 1, for the attacked node with small degree, when the control load strength τ is small, the attacked node with large degree is more likely to increase the change of phase transition critical state and cause a series of network damage. However, in strategy 2 with $\tau = 0.8$, the attacked node with large degree is more likely to show the network vulnerability with the increase of attack strength μ. The reason for this is that when τ is small, it is the node itself resists cascading failure, whoes characteristics such as the load of the node itself have a certain ability to delay damage against random attacks, and the larger the degree of attacked node, the better the effect of resisting network cascading failure, while when τ is large, the attacked node with small degree has greater ability to mitigate failure than the attacked node with large degree. It is the same with the simulation results and analysis of the influence of parameter μ on the phase transition critical factors of BA network and ER network in Fig. 7 and Fig. 8.



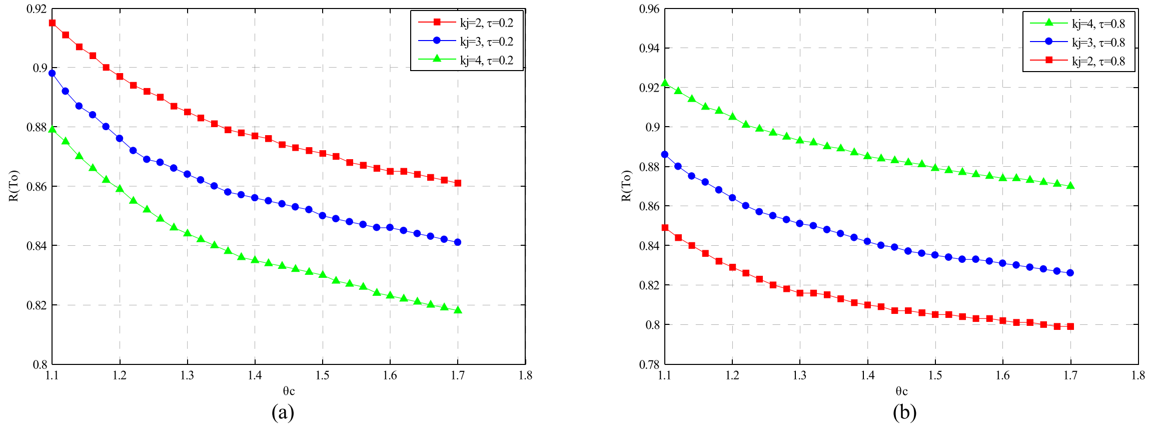
(a) (b)

FIGURE 12. Influence of parameter μ on the phase transition critical factors of two actual networks ($\tau = 0.2$). (a) ARPA network (b) CERNET network.



(a) (b)

FIGURE 13. Influence of parameter μ on the phase transition critical factors of two actual networks ($\tau = 0.8$). (a) ARPA network (b) CERNET network.



(a) (b)

FIGURE 14. Influence of parameter θ_c on the robustness of ARPA network at different levels of τ. (a) $\tau = 0.2$ (b) $\tau = 0.8$.

3) INFLUENCE OF PHASE TRANSITION CRITICAL FACTOR AND CONTROL NODE LOAD INTENSITY ON THE ROBUSTNESS OF TWO ACTUAL NETWORKS

To further determine the reliability and authenticity of the influence of phase transition critical factor and load strength on the network robustness, the distribution coefficient is set to be $\beta = 1$ and attack strength to be $\mu = 1$ in this experiment, and $R(T)$ represents the robustness of the network after T attacks. Because the total number of nodes and the link size of ARPA network and CERNET network are small,

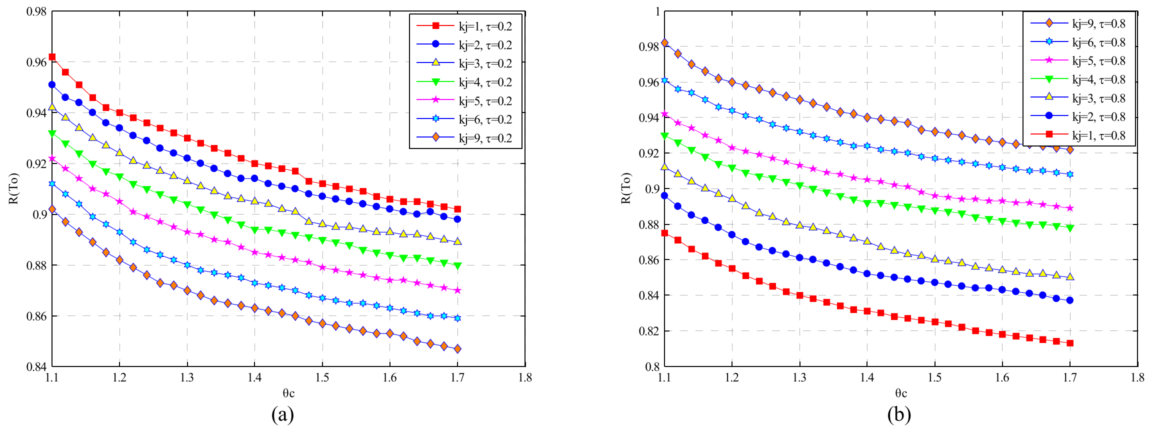


FIGURE 15. Influence of parameter θ_c on the robustness of CERNET network at different levels of τ. (a) $\tau = 0.2$ (b) $\tau = 0.8$.

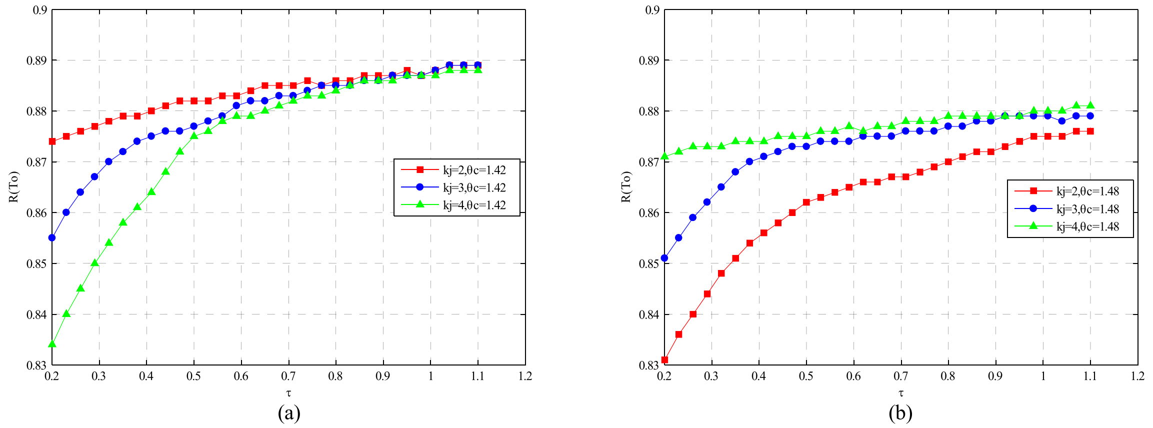


FIGURE 16. Influence of parameter τ on the robustness of ARPA network at different levels of θ_c. (a) $\theta_c = 1.42$ (b) $\theta_c = 1.48$.

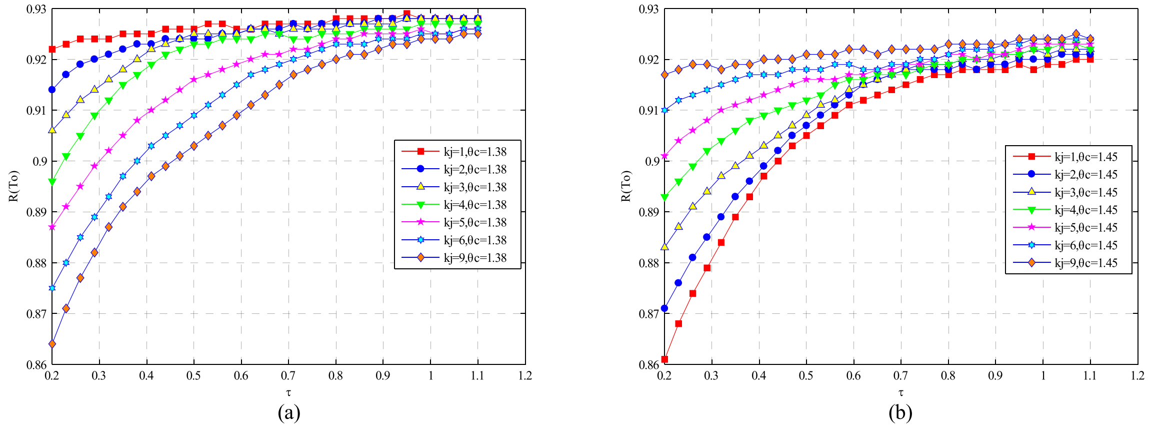


FIGURE 17. Influence of parameter τ on the robustness of CERNET network at different levels of θ_c. (a) $\theta_c = 1.38$ (b) $\theta_c = 1.45$.

a certain proportion of random attack may cause instantaneous collapse of the network, which is not conducive to studying the robustness law under various parameters in depth. Hence, attack times is set to be $T = T_0 = 1$. In this section, experiments 1 and 2 study the influence of phase transition critical factor θ_c on the robustness of two actual networks at different levels of τ, as shown in Fig. 14 and 15. Experiments 3 and 4 study the influence of control node load intensity τ on the robustness of two actual networks at different levels of θ_c, as shown in Fig. 16 and 17.

We can observe from Fig. 14 and 15 that whether parameter τ of ARPA network and CERNET network is located at the left side or right side of the critical area, the critical state factor θ_c is always negatively correlated to the robustness at this time. Under the condition that the critical state of phase transition remains unchanged, when the control load strength τ is small ($\tau = 0.2$), the $R(T_0)$ of two networks decrease with the increase of k_j, and when the control load strength τ is large ($\tau = 0.8$), the $R(T_0)$ of two networks increases with the increase of k_j. It is consistent with the results of the experiment in Fig. 9.

We can observe from Fig. 16 and 17 that whether it is ARPA network or CERNET network, when the critical state factor θ_c is at a high level or a low level, τ is always positively correlated to $R(T_0)$. When θ_c is at a low level ($\theta_{\mathrm{c}} = 1.38, 1.42$), with the increase of τ value, the attacked node with small degree has stronger ability to resist damage than the node with large degree. When θ_c is at a high level ($\theta_{\mathrm{c}} = 1.45, 1.48$), the overall robustness reflected when the node with large degree is attacked is good. Therefore, the appropriate comprehensive control of load strength τ and θ_c values promotes the network to maintain its functional attributes as much as possible under the random attack, so as to mitigate the cascading failure of the network. The correctness of the mitigation strategy proposed in this paper is verified by comparing the results of experiment in Fig. 10.

VII. CONCLUSION

The cascading failure models of classical and actual networks under the external random attack are constructed based on the optimal probability distribution mechanism of neighbor node load and the node failure capacity control function, and through controlling the changes of important parameters in the model, the corresponding indexes are used to analyze the cascading failure mechanism of each node of the network and their influence on some characteristics of cascading failure model. The mains conclusions are summarized as follows.

1) Theoretical analysis and simulation results show that the analytic evolution model of node failure constructed based on two classical networks and two actual networks as well as the cascading failure model based on the optimal probability allocation mechanism are reasonable, which has provided a theoretical basis for the study of the cascading failure mechanism and the making of mitigation strategies of complex networks in real world.

2) The adjustable parameter τ influences the phase transition critical factor θ_c of the network with different topology structures and different degrees of attacked nodes, thus intensifying the network cascading failure. No matter what topology structure a network has, when τ is small, θ_c decreases with the increase of parameter k_j; when τ is large, θ_c increases with the increase of parameter k_j. Therefore, when the actual networks are attacked randomly by the external world, the network failure can be mitigated by comprehensively adjusting the network structure, control node load intensity τ and the degree of attacked node, so as to minimize the damage.

3) Under a certain control node load intensity τ, the attack strength μ is positively correlated with the phase transition critical factor θ_c of the network. When μ is small, θ_c of two classical networks and two actual networks decreases with the increase of the degree of attacked node, and the network structure is relatively stable; when μ is large, θ_c of the classical networks and the actual networks increase with the increase of the degree of attacked node, and the network structure is more likely to be damaged. If the nodes have low ability to control load in the actual networks, the node with larger degree can used as the communication network node, and vice versa, so as to mitigate the damage caused by cascading failure of the nodes in the whole network.

4) The robustness of communication network with cascading failure is limited by control node load intensity τ and phase transition critical factor θ_c in a certain range. When τ is constant, the robustness function $R(T)$ is negatively correlated with θ_c; when θ_c is constant, the robustness function $R(T)$ is positively correlated with τ. And under the condition of same θ_c, when τ is large, the network with large k_j are more robust than the network with small k_j; similarly, under the condition of same τ, when θ_c is large, the robustness of the network with large k_j is stronger than that of the network with small k_j. Therefore, to improve the robustness of the actual communication network and mitigate the cascading failure, within the possible scope of adjustment, the two mitigation strategies are proposed. Strategy 1: take the attacked node with smaller degree as the node in the actual network, and appropriately reduce the parameter τ to make θ_c as small as possible; or for the network with attacked node with large degree, appropriately increase the parameter τ to make θ_c as small as possible. Strategy 2: for the network with attacked node with large degree, increase the parameter τ moderately to make θ_c as large as possible; for the network with attacked node with small degree, increase the parameter τ moderately to make θ_c as small as possible.

Of course, the model constructed in this paper is an improvement and in-depth study of the cascading failure models of classical networks and actual networks under the random attack mode of complex networks by the external world. In reality, complex network facilities are often subjected to deliberate attack or random-deliberate attack, while most of the topology structures of actual networks are more complex and larger in scale. Furthermore, to simplify the discussion, this paper takes the approximation in the minimum degree, distribution parameter, attack strength as well as the homogeneity of $\langle k^{\tau} \rangle$ in the cascading failure model of ER random network, which is an idealized case. Therefore, the mitigation strategy for cascading failure of real-world complex networks such as the dependent network will be further improved next.

REFERENCES

[1] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," *Eur. Phys. J. B-Condensed Matter Complex Syst.*, vol. 46, no. 1, pp. 101–107, Jul. 2005.

[2] H. Huang and X.-C. Wu, "Comparison of security and stability standards of transmission network in China and EU&USA," *Autom. Electric Power Syst.*, vol. 38, no. 1, pp. 127–133, Jan. 2014.

[3] D.-Q. Wei, X.-S. Luo, and B. Zhang, "Analysis of cascading failure in complex power networks under the load local preferential redistribution rule," *Phys. A, Stat. Mech. Appl.*, vol. 391, no. 8, pp. 2771–2777, Apr. 2012.

[4] F. F. Wu and P. P. Varaiya, "Smart grids with intelligent periphery: An architecture for the energy Internet," *Engineering*, vol. 1, no. 4, pp. 436–446, Dec. 2015.

[5] M. Rohden, D. Jung, S. Tamrakar, and S. Kettemann, "Cascading failures in ac electricity grids," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 94, no. 3, Sep. 2016, Art. no. 032209.

[6] C. Zhang, F.-M. Zhang, Y. Wang, and H.-S. Wu, "Method to analyses the robustness of aviation communication network based on complex networks," *Syst. Eng. Electron.*, vol. 37, no. 1, pp. 180–184, Jan. 2015.

[7] J.-J. Wu, H.-J. Sun, and Z.-Y. Gao, "Cascading failures on weighted urban traffic equilibrium networks," *Physica A, Stat. Mech. Appl.*, vol. 386, no. 1, pp. 407–413, Dec. 2007.

[8] Y. Qian, B. Wang Y. Xue, J. Zeng, and N. Wang, "A simulation of the cascading failure of a complex network model by considering the characteristics of road traffic conditions," *Nonlinear Dyn.*, vol. 80, nos. 1–2, pp. 413–420, Apr. 2015.

[9] H.-Y. Liu, Y.-B. Lv, B.-S. Liu, Q. Li, and W.-J. Lv, "Cascading failure resistance of urban rail transit network," *J. Transp. Syst. Eng. Inf. Technol.*, vol. 18, no. 5, pp. 82–87, Oct. 2018.

[10] S.-M. Chen, S.-P. Pang, and X.-Q. Zhou, "An LCOR model for suppressing cascading failure in weighted complex networks," *Chin. Phys. B*, vol. 22, no. 5, pp. 626–631, Mar. 2013.

[11] L. Huang, Y.-C. Lai, and G. Chen, "Understanding and preventing cascading breakdown in complex clustered networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 78, no. 3, Sep. 2008, Art. no. 036116.

[12] M. Ouyang, Z.-Z. Pan, H. Liu, and L.-J. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Phys. A, Stat. Mech. Appl.*, vol. 396, no. 2, pp. 204–211, Feb. 2014.

[13] J.-C. Zhao, D.-Q. Li, H. Sanhedrai, R. Cohen, and S. Havlin, "Spatio-temporal propagation of cascading overload failures in spatially embedded networks," *Nature Commun.*, vol. 7, Jan. 2016, Art. no. 10094.

[14] C.-Q. Yi, Y.-Y. Bao, J.-C. Jiang, and Y.-B. Xue, "Mitigation strategy against cascading failures on social networks," *China Commun.*, vol. 11, no. 8, pp. 37–46, Aug. 2014.

[15] H. Nasrin, and A. Mehrdad, "A mitigation strategy for the prevention of cascading trust failures in social networks," *Future Gener. Comput. Syst., Int. J. eSci.*, vol. 94, pp. 564–586, May 2019.

[16] J.-J. Qi, K. Sun, and S.-W. Mei, "An interaction model for simulation and mitigation of cascading failures," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 804–819, Mar. 2015.

[17] J. Wang, N.-D. Yang, Y.-L. Zhang, and Y. Song, "Development of the mitigation strategy against the schedule risks of the R&D project through controlling the cascading failure of the R&D network," *Phys. A, Stat. Mech. Appl.*, vol. 508, pp. 390–401, Oct. 2018.

[18] H.-R. Liu, M.-D. Cui, R.-R. Yin, Y.-H. Xu, and Q.-Y. Wang, "Mitigation strategy for scale-free network against cascading failures," *Control Decis.*, vol. 33, no. 6, pp. 1087–1092, Jun. 2018.

[19] Y.-C. Hao, C.-B. Li, and L. Wei, "Cascading failure model of complex networks considering overloaded nodes," *Syst. Eng. Electron.*, vol. 40, no. 10, pp. 2282–2287, Oct. 2018.

[20] A. E. Motter and Y. C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 66, no. 6, Jan. 2003, Art. no. 065102.

[21] B. Wang and B. J. Kimeom, "A high-robustness and low-cost model for cascading failures," *Europhys. Lett.*, vol. 78, no. 4, pp. 8001–8005, Apr. 2007.

[22] 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," *Eur. Phys. J. B*, vol. 62, no. 1, pp. 101–104, Mar. 2008.

[23] B. Guo, L.-N. Wang, Y. Li, and F.-R. Zhou, "Study on network cascading failures based on load-capacity model," *J. Comput. Res. Develop.*, vol. 49, no. 12, pp. 2529–2538, Dec. 2012.

[24] J. Lehmann and J. Bernasconi, "Stochastic load-redistribution model for cascading failure propagation," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 81, no. 3, Mar. 2010, Art. no. 031129.

[25] D.-L. Duan, J. Wu, H.-Z. Deng, F. Sha, X.-Y. Wu, and Y.-J. Tan, "Cascading failure model of complex networks based on tunable load redistribution," *Syst. Eng. Theory Pract.*, vol. 33, no. 1, pp. 203–208, Jan. 2013.

[26] Z.-Q. Liang, D.-L. Fu, and Y. Deng, "A load redistribution strategy based on dynamic information in cascading process," *Comput. Eng. Sci.*, vol. 39, no. 9, pp. 1638–1644, Sep. 2017.

[27] C.-Q. Fu, Y. Wang, K. Zhao, and Y.-J. Cao, "Complex networks under dynamic repair model," *Phys. A, Stat. Mech. Appl.*, vol. 490, no. 3, pp. 323–330, Jan. 2018.

[28] G.-Q. Cheng, Y.-Z. Lu, M.-X. Zhang, and J.-C. Huang, "Node importance evaluation and network vulnerability analysis on complex network," *J. Nat. Univ. Defense Technol.*, vol. 39, no. 1, pp. 120–127, Feb. 2017.

[29] L. Dobson, B. A. Carreras, and D. E. Newman, "A probabilistic loading-dependent model of cascading failure and possible implications for blackouts," *Syst. Sci.*, vol. 65, no. 1, pp. 6–9, Jan. 2003.

[30] D.-L. Duan and R.-J. Zhan, "Evolution mechanism of node importance based on the information about cascading failures in complex networks," *Acta Phys. Sinica*, vol. 63, no. 6, Mar. 2014, Art. no. 068902.

[31] R.-R. Yin, B. Liu, H.-R. Liu, and Y.-Q. Li, "Dynamic fault-tolerance analysis of scale-free topology in wireless sensor networks," *Acta Phys. Sinica*, vol. 63, no. 11, Jun. 2014, Art. no. 110205.

[32] X. Peng, H. Yao, J. Du, Z. Wang, and C. Ding, "Invulnerability of scale-free network against critical node failures based on a renewed cascading failure model," *Phys. A, Stat. Mech. Appl.*, vol. 421, no. 3, pp. 69–77, Mar. 2015.

[33] P. Erdös and A. Rényi, "On random graphs," *Pub. Math., Debrecen*, vol. 6, pp. 290–297, Jan. 1959.

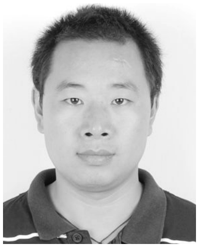
[34] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, 1999.

[35] X.-P. Zhang, Y.-S. Li, G. Liu, and L. Wang, "Evaluation method of importance for node in complex networks based on importance contribution," *Complex Syst. Complex. Sci.*, vol. 11, no. 3, pp. 26–33, Sep. 2014.

[36] Y. Sun, P.-Y. Yao, J.-Y. Zhang, and K. Fu, "Node attack strategy of complex networks based on optimization theory," *J. Electron. Inf. Technol.*, vol. 39, no. 3, pp. 518–524, Mar. 2017.

[37] L.-B. Ma, P. Guo, and J. Zhao, "Node protection capability based survivability assessment method for command and control system network," *Syst. Eng. Electron.*, vol. 39, no. 7, pp. 1524–1531, Jul. 2017.

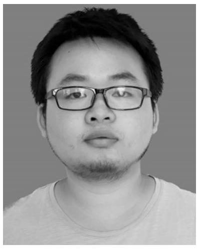
TIAN-CHI TONG received the B.S. degree in automation from the Henan University of Urban Construction, China, in 2016. He is currently pursuing the M.Sc. degree in control engineering with Nanchang Hangkong University, China. His research interest includes the cascading failures and simulation analysis of complex networks.



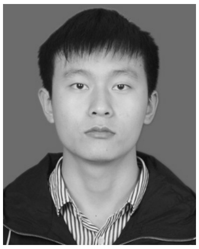
YUAN JIANG received the B.Sc. degree from the Changsha University of Science and Technology, China, in 2004, the M.Sc. degree from Guangxi Teachers Education University, China, in 2007, and the Ph.D. degree in control theory and control engineering from Shandong University, China, in 2010. From September 2018 to September 2019, he was a Visiting Scholar with the University of Chinese Academy of Sciences. He is currently an Associate Professor with the School of Information Engineering, Nanchang Hangkong University, China. His research interests include the cascading failures of complex networks, nonlinear and adaptive control design, disturbance rejection, output regulation, and flight control of helicopter.

YI ZHOU will receive the B.S. degree in automation from Nanchang Hangkong University, China, in 2020. Her research direction is cascading failure of complex networks.

XIAO-QIANG ZHUANG received the B.S. degree in mechanical engineering and automation from Wuyi University, China, in 2015. He is currently working as an Engineer with Han's Laser Technology Industry Group Company, Ltd. His research interests include the laser micromachining technology, finite element analysis of mechanical structure, and the cascading failures and simulation analysis of complex networks.



WEI-BAI DUAN received the B.S. degree in electronic information science and technology from Nanchang Hangkong University, China, in 2018, where he is currently pursuing the M.Sc. degree in technology of computer application. His research interests include simulation analysis of complex networks and pose estimation.



XU PENG received the B.S. degree in computer science and technology from the Wuhan University of Science and Technology City College, China, in 2019. He is currently pursuing the M.Sc. degree in technology of computer application with Nanchang Hangkong University, China. His research interests include neural networks and deep learning.