COMPLEX SYSTEM MODELING AND SIMULATION
ISSN 2096-9929 01/06 pp 1–14
Volume 4, Number 1, March 2024
DOI: 10.23919/CSMS.2023.0020

Cascading Failures in Power Grids: A Load Capacity Model with Node Centrality

Chaoyang Chen*, Yao Hu, Xiangyi Meng, and Jinzhu Yu

Abstract: Power grids, due to their lack of network redundancy and structural interdependence, are particularly vulnerable to cascading failures, a phenomenon where a few failed nodes—having their loads exceeding their capacities—can trigger a widespread collapse of all nodes. Here, we extend the cascading failure (Motter-Lai) model to a more realistic perspective, where each node's load capacity is determined to be nonlinearly correlated with the node's centrality. Our analysis encompasses a range of synthetic networks featuring small-world or scale-free properties, as well as real-world network configurations like the IEEE bus systems and the US power grid. We find that fine-tuning this nonlinear relationship can significantly enhance a network's robustness against cascading failures when the network nodes are under attack. Additionally, the selection of initial nodes and the attack strategies also impact overall network robustness. Our findings offer valuable insights for improving the safety and resilience of power grids, bringing us closer to understanding cascading failures in a more realistic context.

Key words: load capacity; complex network; node centrality; cascading failures; robustness of power grids

1 Introduction

Cascading failures have attracted substantial attention recently owing to their tremendous potential for harming the reliability and security of power systems[1, 2]. An instance of cascading failures took place in 2003 in Manhattan, New York, USA. As the first significant power loss occurred, additional significant northeastern United States cities experienced cascading failures[3].

To analyze cascading failures of power grids, Motter and Lai introduced the "load capacity" Motter-Lai (ML) model[1]. This model, which is based on the dynamic redistribution of network traffic, depicts cascading failure by assuming a linear connection between the load and capacity of nodes. Using the ML model, Li et al.[4] compared the effects of maximum load attacks and random attacks on different networks using the ML model, showing that under random attacks, most links and nodes fail at the beginning of cascading failure. Qi et al.[5] established an interaction model to examine the impact of interaction on the risk of cascading failure. Their results were verified using simulation data generated from the ORNL-PSerc-Alaska (OPA) model on an IEEE 118 node system. An essential technique for examining cascading failures in complex networks is the load capacity model. Researchers have studied the use of load capacity models in complex network cascading failures extensively during the last several decades. According to research, load capacity models may be used to anticipate the resilience and stability of the network as well as to accurately explain the failure process of network nodes[6–8]. Additionally, to better

• Chaoyang Chen and Yao Hu are with the Department of Information and Electrical Engineering, Hunan University of Science and Technology, Xiangtan 411100, China. E-mail: ouzk@163.com; 21010401004@mail.hnust.edu.cn.
• Xiangyi Meng is with the Department of Physics and Astronomy, Northwestern University, Evanston, IL 60208, USA. E-mail: xm@northwestern.edu.
• Jinzhu Yu is with the Department of Civil Engineering, University of Texas, Arlington, TX 22201, USA. E-mail: yujinzhu88@gmail.com.
∗ To whom correspondence should be addressed.

※ This article was recommended by Associate Editor Rui Wang.
Manuscript received: 2023-08-16; revised: 2023-09-27; accepted: 2023-10-25

accommodate various network[9–11] kinds and failure patterns, researchers have put out a number of revised load capacity models[12, 13].

One of the primary failure modes for networked systems is now cascading failures[14]. For example, in 2003, when the North American power grid failed, communication networks and control centers also failed, which in turn hindered decision making for power restoration. This example further highlights the importance of understanding cascading failures in complex systems. Cascading failure mechanisms can be loosely divided into two categories: structural and functional. Structural cascading failures consider visible or direct causal relationships between component failures[15–19]. As cascading failures are tied to load redistribution caused by intial failure, nodes with larger load capacities are normally more resilient to cascading failures, while nodes with smaller load capacities are more vulnerable[20]. Practically, each node of the power grid can have a different load capacity. Therefore, it is crucial to formulate practical models that explicitly consider the variety of load capacities of nodes. For example, the issue of redundant capacity, resulting from the varying strength of network interaction, has been carefully considered in real-world networks such as power grids and traffic networks[21]. In Ref. [22], a heuristic algorithm has been developed to identify vulnerable lines in power grids, aiming to balance the accuracy and efficiency of identification. The robustness of interdependent networks against degree-based deliberate attacks has also been thoroughly investigated[23], which has led to the proposal of counter-attack procedures involving the addition of links to improve interdependent network connectivity. As a subfield of dynamic modeling of complex systems, research on cascading failures in power networks might be considered[14]. In this field, researchers use various methods to describe and predict the behavior of complex systems, such as network science[24], nonlinear dynamics[25, 26], and stochastic processes[27]. The specifics of the research problem will determine the dynamic modeling techniques applied to cascading failure analysis in power networks[18].

The article thoroughly investigates the impact of crucial parameters on cascading failures and validates their effectiveness through simulation. The findings show that this approach may successfully evaluate cascading failures in a variety of networks, promoting the secure operation and increased resilience of power grids against catastrophic events. The main highlights of this article are as follows:

- **Proposing a node threshold calculation framework based on nonlinear load capacity:** Our contribution lies in proposing a model based on nonlinear load capacity, which is the fundamental framework for calculating node thresholds and promoting cascading failures simulation.
- **Observations from extensive model analysis:** Through meticulous analysis of the model, notable observations emerge. Particularly, downstream nodes exhibit susceptibility when confronted with attack nodes, signifying a cascading effect. For directed networks, the determination of the network load capacity parameter hinges on the maximum value among downstream nodes' load capacity parameters. Conversely, within undirected networks, the paramount parameter value arises as the highest among the load capacity parameters of neighboring nodes.
- **Enhancing resilience through tolerance parameter improvement:** A significant outcome of our study underscores that the enhancement of tolerance parameters directly correlates with the bolstering of resilience across all network types.
- **Unveiling threats to network robustness:** We compare random and target attacks and analyze the impact of initial failure nodes. By analyzing the attacks in the network, we can identify potential targets that targeted attacks exploit, thus posing a major threat to the overall security of the network.
- **Guiding predictive accuracy via a proposed general strategy:** The strategic approach we introduce, grounded in the load capacity model, emerges as a valuable tool for an analysis of cascading failures, thereby offering substantial guidance.

2 Methodology

2.1 Network model and network centrality

2.1.1 Network model

A complex network, $\mathcal{G}$, can be defined as a graph or graph-like structure that represents the constituent elements of a complex system as nodes and the pairwise relationships between them as links[28]. In this work, we demonstrate the proposed method on three synthetic complex network models:

(1) An Erdos-Renyi network (ER)[29].

(2) A Watts-Strogatz network (WS)[30].

(3) A Barabsi-Albert network (BA)[31].

The small-world property usually reflects the fact that the characteristic path length between points in the network is small, like that of an ER network, but the clustering coefficient of a WS network is substantial, similar to that of a regular network (such as a lattice). The scale-free feature, on the other hand, the scale-free characteristic demonstrates that the distribution of nodes' degree values follows a power law, with a small number of nodes in the network having large degree values and the majority of nodes having tiny degree values. Real-world networks often exhibit small-world and scale-free features. Furthermore, for comparison, we employed the network structure of the US power system. Table 1 displays the specifics of this network.

2.1.2 Network centrality

The importance of the nodes can be measured by the centrality of the network[18, 32]. Here, we adopt three centrality measures:

(1) Degree centrality[33, 34].

(2) Betweenness centrality[35].

(3) Closeness centrality[36].

Their formulas are

$$\mathrm{DC}_i = \frac{k_i}{N-1},\ i = 1,2,\ldots,N \tag{1}$$

$$\mathrm{BC}_i = \frac{1}{(N-1)(N-2)/2}\sum_{s\neq i\neq t}\frac{n^i_{st}}{g_{st}},\ i = 1,2,\ldots,N \tag{2}$$

$$\mathrm{CC}_i = \left(\frac{1}{N-1}\sum_{j=1}^{N} d_{ij}\right)^{-1},\ i = 1,2,\ldots,N \tag{3}$$

where k_i is the degree of the node i, and N is the number of nodes in the network. n^i_{st} indicates the number of the shortest paths passing through node i, g_{st} indicates the total number of the shortest paths between s and t, and d_{ij} is the geodesic distance between nodes i and j. The three network centrality measures' detailed explanations are shown in Table 2.

Table 1 Average centrality of each network.

Network	N	V	$\langle K\rangle$	$\langle B\rangle$	$\langle C\rangle$
BA	5000	10 025	4.0	8612.3	4.58×10^{-5}
WS	5000	10 000	4.0	43 305.2	1.12×10^{-5}
ER	5000	6222	2.5	16 158.4	1.70×10^{-5}
US	4941	6594	2.7	44 433.3	1.09×10^{-5}

Note: N denotes the number of nodes, V denotes the number of connected links, $\langle K\rangle$ denotes the average degree, $\langle B\rangle$ denotes the average betweenness, and $\langle C\rangle$ denotes the average closeness.

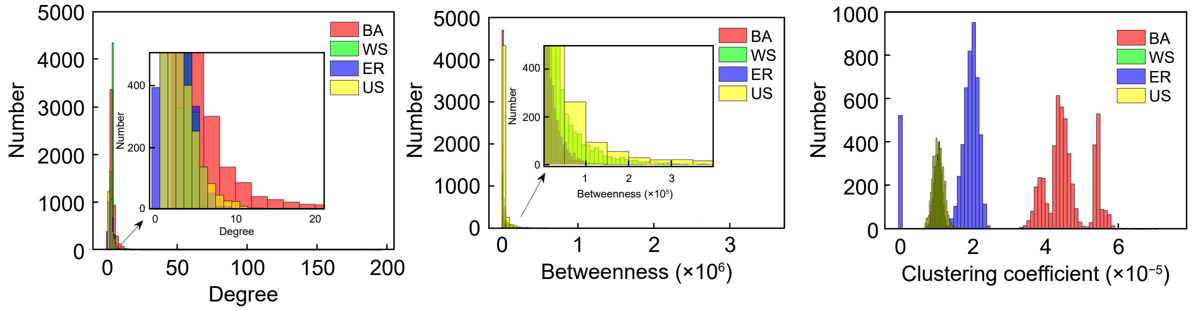
In this research, we create three complex network models, namely ER, WS, and BA networks, each of which contains 5000 nodes as detailed in Table 1. To further elucidate the distinctions in statistical properties of those networks, we conduct a comparative analysis of the degree centrality, betweenness centrality, and clustering coefficient centrality across four networks, as depicted in Fig. 1. As can be observed, in exceptional cases, networks may have a power-law distribution, signaling the presence of strongly coupled nodes or hubs. The centrality distribution indicates the relevance of the nodes in permitting communication and information transmission between the other nodes. Nodes with greater centrality of betweenness serve crucial roles in preserving efficient routes and are critical for network stability.

2.2 Load capacity model

A mathematical model for calculating a network's capacity for carrying load is known as the load capacity model. A network may crash if its load capacity is surpassed, which causes the network to become overloaded. The load capacity model is commonly used

Table 2 Network centrality detailed explanations.

Symbol	Equation	Description
DC_i	(1)	It is a widely used node centrality metric in network research, depending on the node's degree.
BC_i	(2)	Based on a node's connectivity with other nodes in the network, it is a measure of the node's value.
CC_i	(3)	Determine the significance of each node in the network by measuring its distance from other nodes.



(a) Degree distribution (b) Betweenness distribution (c) Clustering coefficient distribution

Fig. 1 Distributions of degree, betweeness, and clustering coefficient of four networks.

in the study of power grids, transportation systems, and other infrastructure networks to predict the probability of failure or overload under different load conditions. In our research, we propose a framework using a load capacity model for calculating the threshold value of each node in the grid and use it to model the cascading failure event. By contrasting the performance of different models, we intend to demonstrate the efficacy of the load capacity model in correctly predicting cascading failures.

2.2.1 Initial load

The cascading failure model allocates the initial load based on the importance of the node, typically using the degree or the betweenness approach[37, 38]. In a network composed of a set of nodes, it is possible to define the initial load based on the centrality of the complex network. For example, suppose that all nodes transmit the same data on the shortest path. In this case, the initial load of each node can be represented by its betweenness centrality, and the initial load of the node is considered to be closely related to the degree of the node. Assuming that all nodes will transmit the same amount of data on the shortest path, the betweenness centrality can be used to represent the initial load of each node. This can help to understand the impact of different load conditions on the network and predict the likelihood of overload or failure. The initial load can then be expressed by the intermediate centrality, which is given by

$$L_{1i} = \sum_{s\neq i\neq t} \frac{n^{i}_{st}}{g_{st}} \tag{4}$$

Alternatively, the initial load of each node can also be considered closely related to the degree of the node. This approach allows for a more accurate representation of the load capacity of each node in the network, as nodes with higher centrality and degree are likely to have a higher initial load due to their increased connectivity and importance within the network.

$$L_{2i} = \mathrm{DC}_i \times (N-1) = k_i \tag{5}$$

Note that in this article L_{1i} is used in the analysis of the toy network and IEEE power network while L_{2i} is used in complex network models.

2.2.2 Maximum capacity

The maximum capacity, sometimes referred to as the load-carrying capacity, is the greatest load that a node in a network can support before being overwhelmed. This capacity is an important factor in understanding the reliability and resilience of a network, as it determines the ability of the node to withstand different load conditions and continue to function properly. It is generally accepted that a node's maximum capacity is linearly related to its initial load[1]. However, in this study, we also consider nonlinear factors that can be considered using the following potential relationships among the maximum carrying capacity as well as the beginning load:

$$C = (1+\alpha)L^{\beta} \tag{6}$$

where the tolerance parameter α and the nonlinear parameter β determine the capacity. Note that as the initial load L increases, the capacity C must also increase. We picked five alternative connections, which are stated in Table 3. As an example between a node's maximum capacity (C) and beginning load (L), C_1 represents the initial linear model, and C_2 signifies the nonlinear model after load logarithmic reduction. C_3−C_5 denote the nonlinear load capacity models scaled through varying β values. The initial load and maximum load curves for C_1−C_5 are depicted in Fig. 2. Among the five curves, the blue curve (C_3) exhibits the most rapid increase with the increase in the initial load L.

2.3 Cascading failure model

Cascading failures occur when the breakdown of a

Table 3 Different load-capacity relationships (Eq. (6)).

Curvilinear	Equation	Relationship
C_1	$C = 1.3L$	Linear relationship
C_2	$C = 1.3L^{1.2}\log L$	Nonlinear relationship with a logarithmic correction
C_3	$C = 1.3L^{1.7}$	Superlinear relationship
C_4	$C = 1.3L^{1.2}$	(Less-)superlinear relationship
C_5	$C = 1.3L^{0.5}$	Sublinear relationship

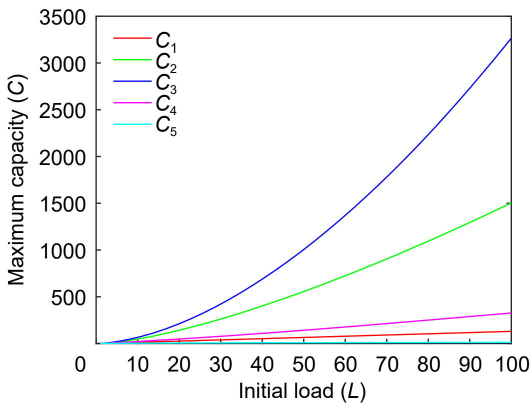


Fig. 2 Different load-capacity relationships, as defined in Table 3.

single part causes a chain reaction that may lead to the collapse of the whole system. These sorts of breakdowns are typically found in power grids and transportation networks[39]. Cascading failure models may be graph-based[40] or network flow models[5]. In this research, cascading failures are represented using the flow-based network model. In this approach, the load distribution of the failing node is defined by the load percentage of its nearby nodes. For example, if node j fails, the capacity given to its neighboring node i would be calculated as Eq. (7). After the failure of node i, its load will be moved to the nearby working nodes. If the load moved to nearby node j exceeds its capacity, node j will also fail. Consequently, the burden of node j will be further spread to its nearby operable nodes, possibly commencing a cascade failure process. In this procedure, the load transmitted from node i to node j, indicated by $\varDelta_{ij}$, can be computed as

$$\varDelta_{ij} = L_j \cdot \frac{L_i}{\sum\limits_{m \in \varGamma_j} L_m} \tag{7}$$

where $\varGamma_j$ represents the set of neighbors of node j, and L_m is the load of one of the neighbors.

The network robustness index is used to evaluate the capacity of the network to withstand cascading failures. When the network achieves a stable state, it is measured by the fraction of failing nodes. As such, a lower index indicates a higher level of robustness.

$$I = \frac{F}{N} \tag{8}$$

where N is the overall number of network nodes, and F denotes the number of failing nodes. The range of this index is from 0 to 1, where 0 indicates no node failures, and 1 indicates the fail of every nodes in this networks.

2.4 Theoretical analysis

Our theoretical analysis aims to determine how α and β affect the cascading failure. When one parameter is fixed, it is important to determine how the other parameters should be adjusted to curb cascading failures. Consider a weighted graph (network) represented as $G = (V, E, W)$. The primary characteristic of this network is its weight distribution $Q(w)$, which represents the probability of a specific edge having a weight of w. We can use Eq. (9) to calculate the weight w_{ij} between node i and node j:

$$w_{ij} = (k_i k_j)^{\theta} \tag{9}$$

θ can take any real values, but $\theta = 1$ is assumed here because according to Refs. [40, 41], $\theta = 1$ leads to the highest robustness of various networks.

The node load is transferred to the neighboring node. When $L_j + \varDelta_{ij} > C_j$, the neighbor j will also fail, and its load will be further distributed to the neighbor, which can cause the neighbor to fail. Therefore, according to Formula (10), we can calculate the case when node j does not fail.

$$L_j \times \left(\frac{L_i}{\sum\limits_{a \in \varGamma_j} L_a} + 1 \right) \leqslant (1+\alpha) \times L_j^{\beta} \tag{10}$$

The threshold for the happening of failure is given by

$$L_j \times \left(\frac{L_i}{\sum\limits_{a \in \varGamma_j} L_a} + 1 \right) = (1+\alpha) L_j^{\beta} \tag{11}$$

When α and β increase at the same time, the robustness of the network is enhanced, as indicated by the increase in the value on the right side of Eq. (11). However, when α and β increase unevenly, the conclusion may vary. It is possible to define a critical parameter value α^* that renders the network invalid, as suggested by Eq. (11). If the value of the stanza parameter α^* is lower than this critical value, the node fails.

When considering a weighted network, the load distribution should take into account the weights of the links. In the case of multiple nodes connected to a single node, the load transfer from node i to node j can be determined considering the ratio of the weights of the links between i and j to the sum of the weights of all the links between node i and its neighboring nodes. We define this ratio as the link compactness, which can be represented as follows:

$$c_{ij} = \frac{w_{ij}}{\sum\limits_{m,n} w_{mn}} \tag{12}$$

Using Eq. (12), we can derive Eq. (13) based on Eq. (11).

$$c_{ij} \times k_j \left(\frac{k_i}{\sum\limits_{a \in \varGamma_j} k_a} + 1 \right) = k_j^{\beta} (\alpha^* + 1) \tag{13}$$

When β increases, to maintain the validity of Eq. (13), the corresponding α should be reduced to maintain a critical state. If α does not change, there will be fewer nodes in the vulnerable stage, and the robustness of network as a whole will continue to improve with the increase of parameter β.

The existence of a threshold may also be referred to as the critical condition, which reflects the least cost to the network. However, it is vital to remember that each node has a separate threshold. If the overall resilience of the network is evaluated, the threshold should be the greatest value of all nodes. If the robustness of a certain node is evaluated, then the threshold of that node should be utilized. For a fixed β network, the α threshold is not fixed. As a result, the value of α may be changed to affect the network's resilience. The highest value of α^* for each node can be considered as the network's overall α^*, as shown in the following formula:

$$\alpha^* = \max_{i\in N} \alpha_i^* \tag{14}$$

Similarly, with a fixed α network, the threshold for β is not fixed. Therefore, we may adjust the value of β^*, and the overall β^* for all nodes can be defined as the greatest value of β^* for each node, as indicated in the following formula:

$$\beta^* = \max_{i\in N} \beta_i^* \tag{15}$$

3 Numerical Analysis

3.1 Toy network

We construct a toy network with 25 nodes and 30 links, as shown in Fig. 3. We apply the cascading failure approach outlined in Algorithm 1 to simulate the cascading failure on the toy network. We initialize the matrices LS_1 and LS_2 to store the node states, and the variable I represents the proportion of failed nodes. We calculate the variable CF using Eq. (16), where N_A denotes the number of initially attacked nodes.

For comparison, we select Nodes 11 and 17. By utilizing the model specified in Eq. (6) and following the principle of isolating a single variable, we fix the parameter values and employ the robustness parameter to analyze the network's robustness.

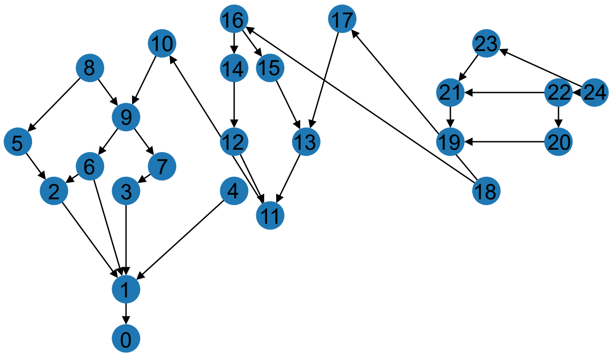


Fig. 3 Network topology with 25 nodes and 30 links.

Algorithm 1 Cascading failure simulation based on degree centrality

```
Initialize lists $\mathrm{LS}_1$ and $\mathrm{LS}_2$, variables $I$ and CF.
Append initial fail node to list $\mathrm{LS}_1$.
while $\mathrm{LS}_1$ is not empty do
  for each node in $\mathrm{LS}_1$ do
    for each neighbor of node do
      if increased load + initial load of neighbor > capacity of neighbor then
        if state of neighbor is “S” then
          Change state of neighbor to “F”.
          Append neighbor to list $\mathrm{LS}_1$.
        end if
      end if
    end for
    Update value of variable CF.
    Update value of variable $I$.
    Append node to list $\mathrm{LS}_2$.
    Remove node from list $\mathrm{LS}_1$.
  end for
end while
```

$$\mathrm{CF} = \frac{N_A}{F\times N} \tag{16}$$

To investigate the impact of parameter α on network robustness, we fix the value of β at 1.2. Figure 4 presents the simulation results of the attack at nodes 11 and 17, with α varying within a certain range. The CF parameter, which shows a similar pattern for both nodes, measures the impact of the first attack node

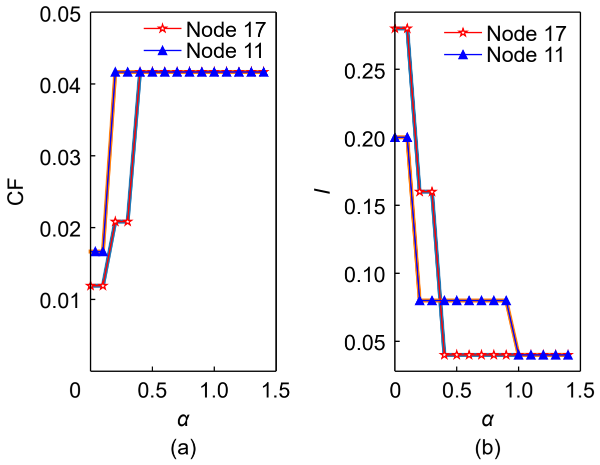


Fig. 4 Impact on network robustness of parameter α.

upon the network's overall robustness. As the tolerance parameter for the network α increases, the network's robustness improves. However, there is a distinction between Node 11 and Node 17. Node 11 remains relatively stable when α is set to 0.2, while Node 17 requires a value of 0.4 to maintain stability. This trend is also evident in the I parameter, which represents the proportion of node failures. Both parameters mutually support the observed trend.

We also investigate the impact of the parameter β on network robustness while keeping its value fixed at 0.2. The simulated results of the attack on Nodes 11 and 17 are shown in Fig. 5. It shows that as the network nonlinear parameter β increases, the network capacity steadily improves. When β reaches 1.2, the network already exhibits relatively good robustness. The CF parameter effectively captures the changes in network robustness associated with different values of β, reflecting the increasing trend of network robustness with varying β.

The visualization results of the impact of parameter β on the network robustness, specifically for attacks on Node 11, are depicted in Fig. 6. The graph provides a clear visualization of node failures, where red represents failed nodes and green represents surviving nodes. When attacking Node 11, it is evident that Node 10 is highly vulnerable. This vulnerability arises because the network is directed, and Node 10 is the only downstream node of Node 11. Consequently, when Node 11 is attacked, Node 10 exhibits a relatively vulnerable aspect. It is worth noting that improving the overall robustness of the network also contributes to protecting Node 10. However, focusing

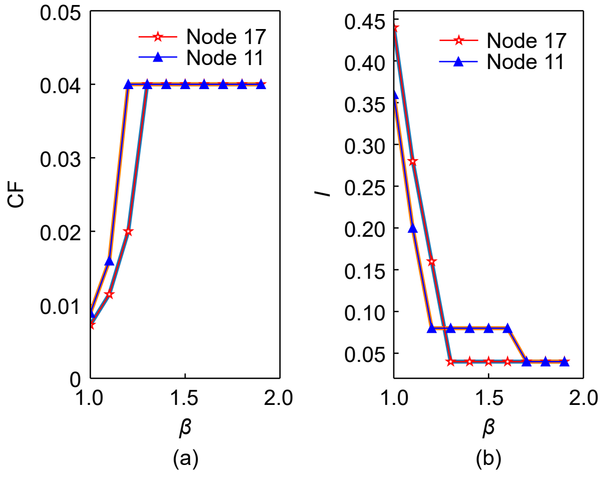
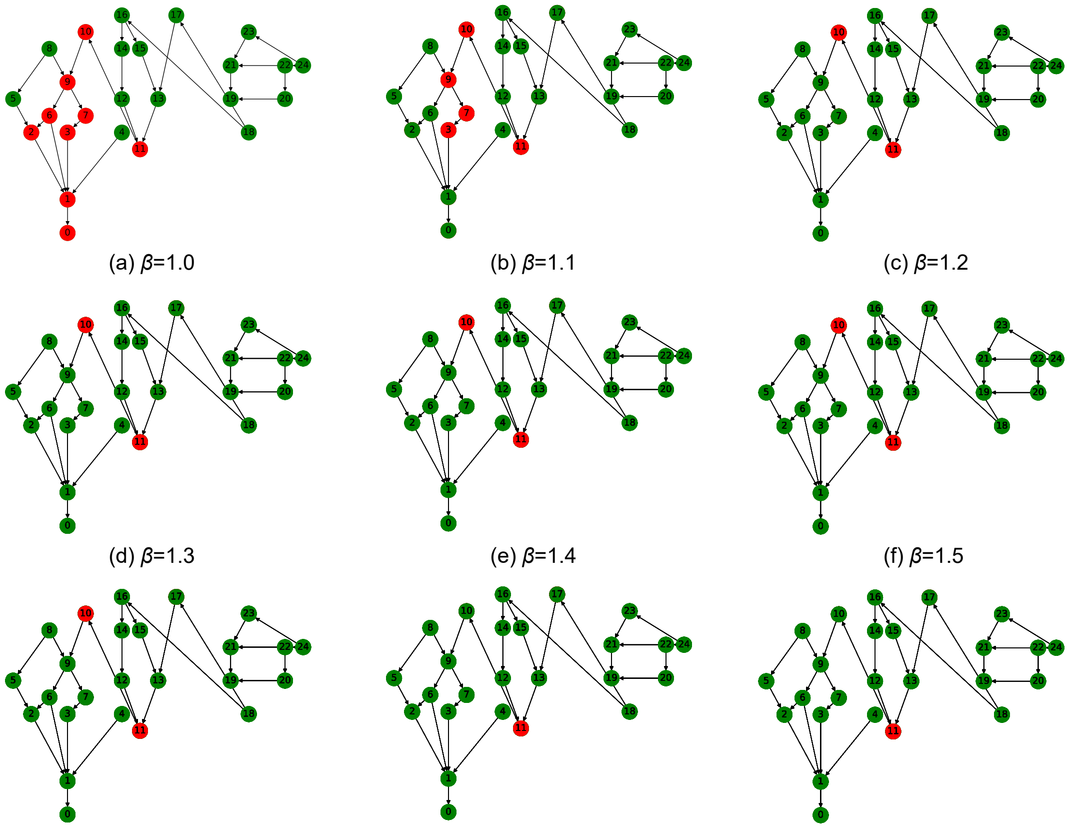


Fig. 5 Impact on network robustness of parameter β.



(a) β=1.0 (b) β=1.1 (c) β=1.2

(d) β=1.3 (e) β=1.4 (f) β=1.5

(g) β=1.6 (h) β=1.7 (i) β=1.8

Fig. 6 Cascading failure visualization with initial attack at Node 11.

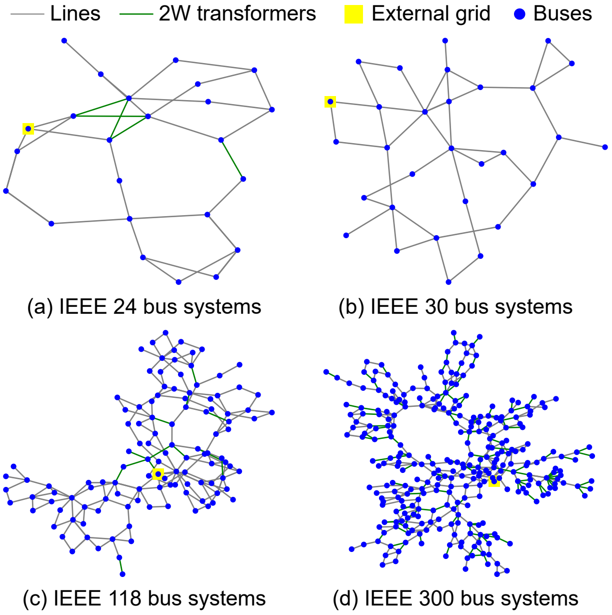
specifically on protecting Node 10 can significantly reduce costs and enhance efficiency. However, attacks are often unpredictable, and network topologies are subject to continuous change. In practice, protecting a single node can be challenging. However, modeling cascading failures based on centrality indicators of nodes proves to be effective in addressing such concerns.

From the visualization results in Fig. 6, we can also verify the correctness of Eqs. (14) and (15). Node 10 has a β^* value of 1.7, while Node 9 has a β^* value of 1.2. As this network is directed, Node 10 is the only downstream node of Node 11, so it is expected that Node 10 has a larger β^* value than Node 9. Generally, for directed networks, the β^* value of the network is the maximum value of all downstream nodes' β^* values, while for undirected networks, the β^* value of the network is the maximum value of all neighboring nodes' β^* values.

3.2 IEEE power networks

Next, we conduct numerical analysis using the IEEE 24, 30, 118, and 300 bus systems (Fig. 7). Each power grid can be modeled as a directed graph G with N nodes (substations) and K links (transmission lines).

In order to consider the impact of equipment outages on static security and develop expected adjustment plans for operational modes, power flow calculations are also taken into account in the power grid. When considering power flow calculations, the steps for cascading failures are as shown in Fig. 8.



(a) IEEE 24 bus systems (b) IEEE 30 bus systems

(c) IEEE 118 bus systems (d) IEEE 300 bus systems

Fig. 7 IEEE 24, 30, 118, and 300 bus systems.

The power flow[42, 43] equations are represented as follows:

$$\begin{cases} P_i = \mathrm{Re}\left[V_i I_i^*\right] = \mathrm{Re}\left[V_i \sum\limits_{j=1}^{N} Y_{ij}^* V_j^*\right], \\ Q_i = \mathrm{Im}\left[V_i I_i^*\right] = \mathrm{Im}\left[V_i \sum\limits_{j=1}^{N} Y_{ij}^* V_j^*\right] \end{cases} \tag{17}$$

where V_i represents the voltage of node i and I_i^* represents the current of node i. Y_{ij}^* represents the admittance of the link from node i to node j. Re represents the real part, and Im represents the imaginary part.

Using the proposed cascading failure algorithm, one can assess the connectivity and stability of the IEEE power networks after node failures, which can support the identification of vulnerabilities and the enhancement of network's robustness. The robustness metrics after cascading failures are depicted in Fig. 9. From Fig. 9, it is evident that the robustness metrics of these IEEE power grids decrease after cascading failures, indicating a certain impact on the grid's robustness. However, when comparing across different IEEE power networks, it can be observed that the cascading failures have the smallest impact on the IEEE 300 bus system.

3.3 US power grid

Now we extend our simulations to an actual large-scale system, which is the US power grid (Fig. 10). The formula for calculating the initial load is given by Eq. (4), which differs from the approaches used in the toy network and the IEEE power networks. Due to the random initialization of failed nodes, the simulations are run 20 times to obtain the average values of interest.

First, consider the effect of α tolerance values on the US power grid and the ER, WS, and BA networks on robustness. We find that, under random attacks, the ER and BA networks are more robust than the US power grid, while the WS network is worse (Fig. 11). The difference between their dependence on α suggests that the US power grid cannot simply be modeled as a synthetic network of one type but rather a mixture of network models with complex network properties such as randomness, small-worldness, and scale-freeness.

Next, fixing α, we investigate how different values of β affect the robustness (Fig. 12). We find that as the value of β increases, the invulnerability index of the

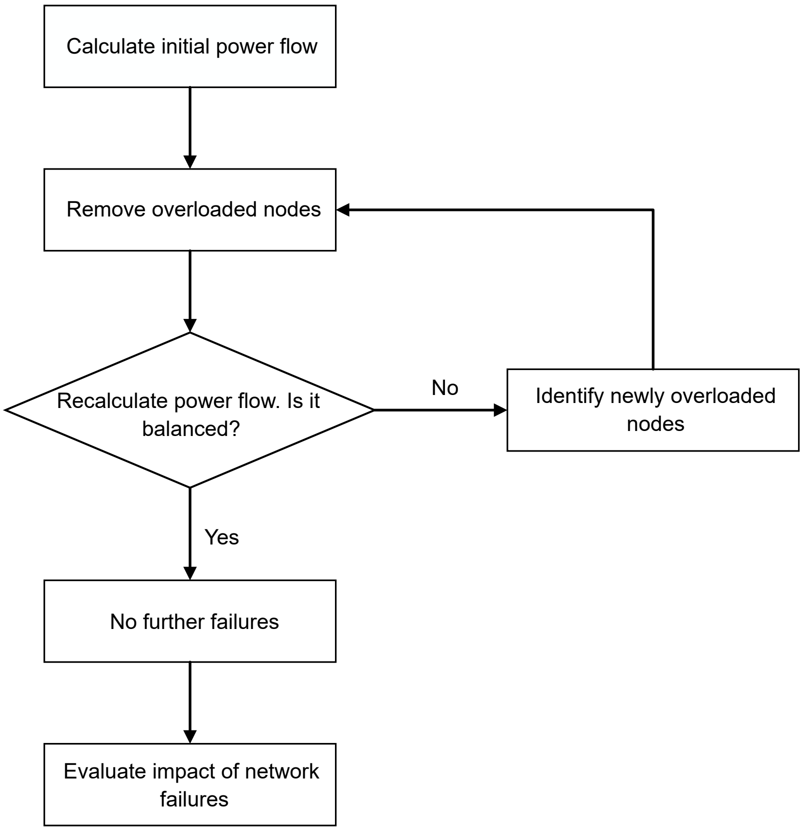
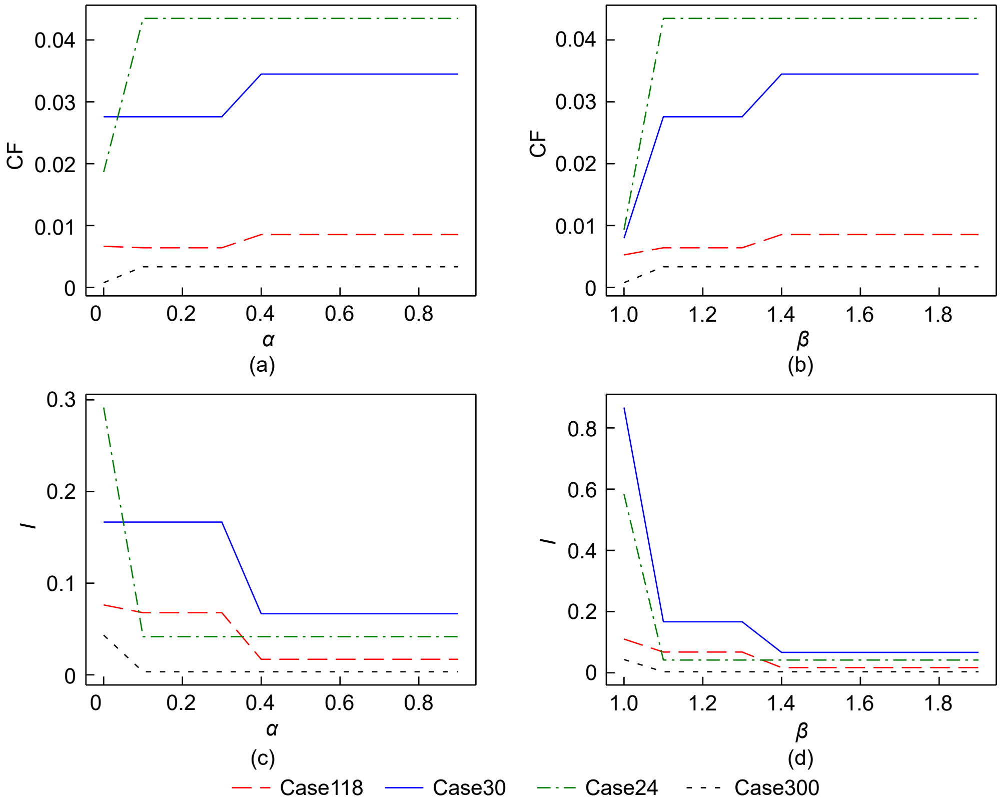

Calculate initial power flow
Remove overloaded nodes
Recalculate power flow. Is it balanced?
No
Identify newly overloaded nodes
Yes
No further failures
Evaluate impact of network failures

Fig. 8 Steps for cascading failures.



(a)

(b)

(c)

(d)

Fig. 9 Impact of parameters α and β on network robustness.

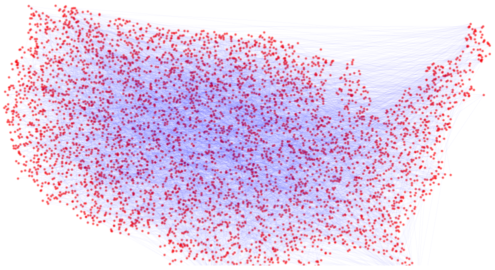


Fig. 10 US power network.

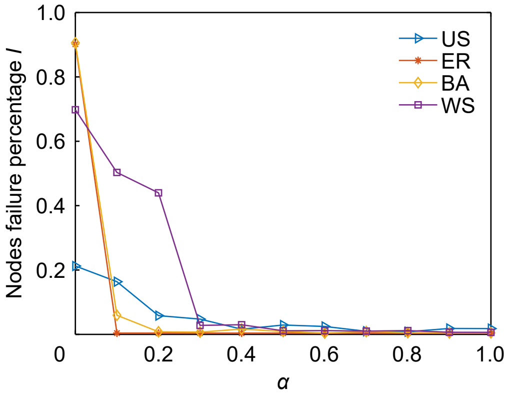


Fig. 11 Network robustness under random attacks.

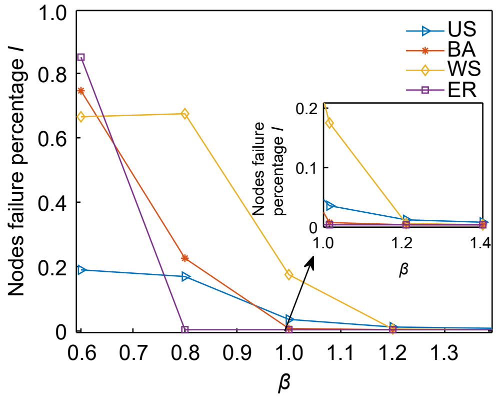


Fig. 12 Results of different values of β under random attacks.

network expands as the value increases, which shows that the network is becoming more resilient to cascading failures. It explains that the higher the value of β, the higher the maximal capacity of the nodes in the network, i.e., the more burden they can bear. Therefore, the network becomes more resistant to cascading failures. However, observe that if the value of β is too large, the maximal capacity of the nodes may become too high and thus become wasteful. As the cost of the network increases, it becomes challenging to compare the disparities between different networks.

We also study the resilience of the network to various sorts of attacks (random attacks and targeted attacks) and the influence of the initial number of assaulted nodes on cascade failures. α for the simulation is set at 0.3, and β is 1.2. Results are given in Fig. 13. The results disclose that intentional attack patterns have a considerable impact on the vulnerability of the network, whereas random attacks are comparatively less effective. However, as the number of initially assaulted nodes increases, the network’s resistance against random attacks diminishes. This is attributed to the increased occurrence of network failures triggered by the increased number of initially assaulted nodes. Different networks exhibit varying performance against different attack strategies. For instance, the BA network is highly vulnerable to targeted attacks, as disabling only 10 nodes can lead to network failure. However, the ER network demonstrates relative robustness. However, as the number of attacked nodes increases, most nodes in the network still experience failures. Furthermore, intentional attacks consistently demonstrate a more significant impact, regardless of the initial number of nodes. Following cascading failures, the network experiences substantial disruptions in connectivity, leading to a notable decline in overall robustness.

To comprehend the dynamic nature of cascading failures in the context of random and targeted attacks, we analyze the average number of unsuccessful nodes at each time step for distinct networks (Fig. 14). It is evident that cascading failures occur quite swiftly. Under targeted attacks, the US power grid exhibits a lower number of initial node failures compared to the WS and BA networks. This discrepancy arises from the lack of hubs in the US power grid, which are abundant in the WS and BA networks. Additionally, the BA network experiences a higher number of failed nodes in the first step, followed by a lower rate of failures in subsequent steps. Furthermore, in the case of random attacks, we observe that the WS network demonstrates a considerable number of failed nodes during the initial stages of cascading failures, with a progressive increase in the number of failed nodes in subsequent phases. Overall, these various networks showcase distinct characteristics regarding the quantity of failed nodes and the velocity of cascading failures.

4 Discussion and Conclusion

We offer a way to compute the threshold based on the load capacity of each node and use this approach to mimic the cascading failure process. To highlight the

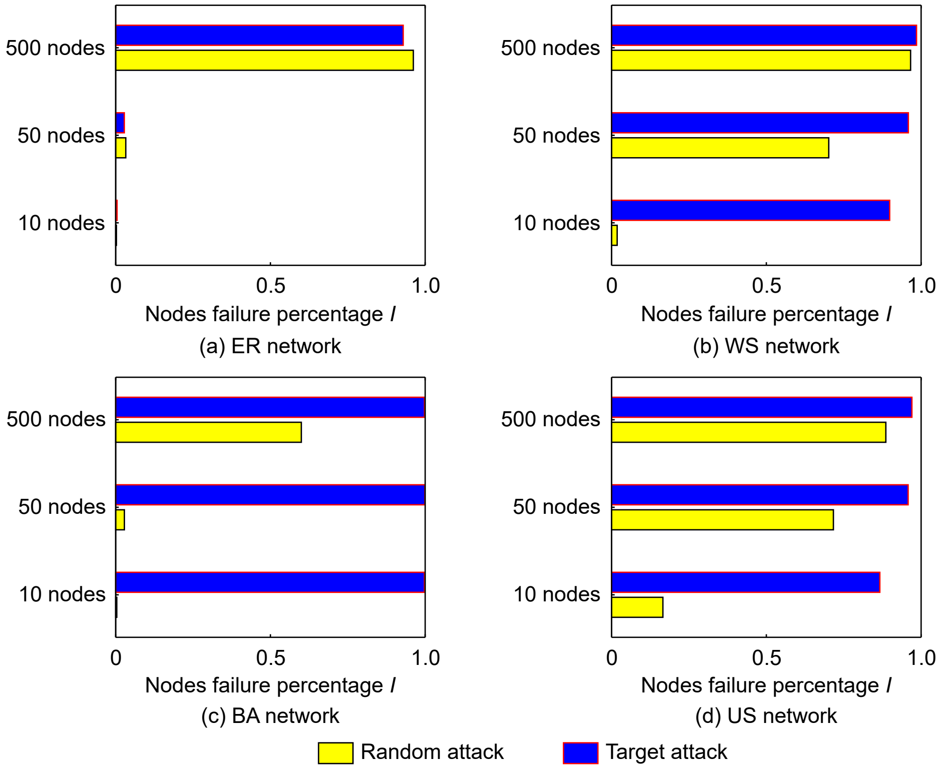


Fig. 13 **Impact of different attacks and numbers of initial attacked nodes on network robustness.**

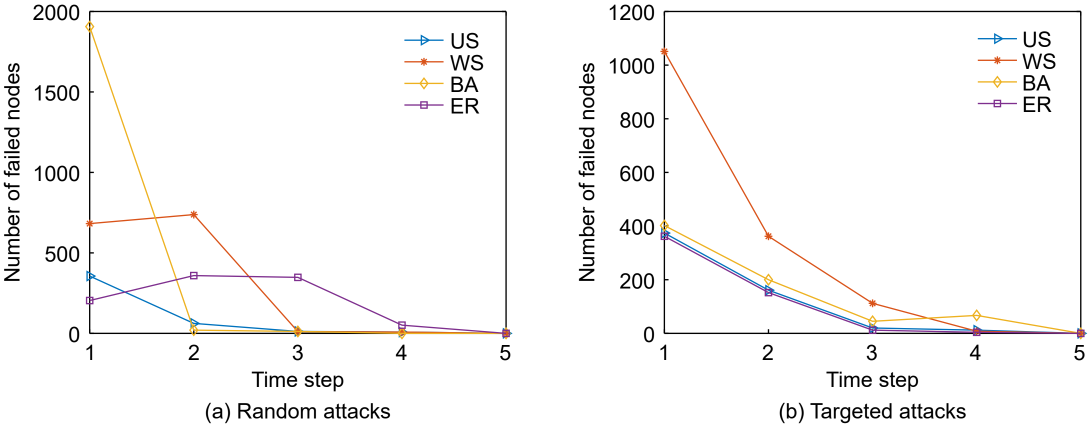


Fig. 14 **Average number of cascading failure nodes per step under random attacks and targeted attacks.**

contribution of this article to the cascading failure of power networks and showcase the advantages and characteristics of the proposed model, a comparison will be made with the article published the state-of-the-art progress made by Li et al.[8] in 2022. The comparison analysis will cover the highlights of the articles, the scope of theoretical research, the discussion of the load capacity model, and the discussion of the application of the cascading failure model to the network. The specific comparison will be presented in Table 4.

Through a comparative research on numerous networks, we show the usefulness of our technique in assessing the resilience of distinct network architectures. The suggested load capacity based technique allows us to explore the dynamic and evolutionary patterns of cascading failures within power networks. Based on the examination of the cascading process and resilience measures of diverse networks, we make the following findings:

(1) The robustness of all networks is improved when the tolerance parameter α is increased, except for the WS network, which has the worst robustness.

(2) Targeted attacks based on load can significantly

Table 4 Comparison of Ref. [8] and our proposed technique.

Item	Ref. [8]	Our proposed technique
Highlight	An elastic reinforcement strategy based on capacity redundancy to enhance network resilience during cascading failures and recovery processes, considering uneven node loads.	Main contents see article introduction.
Theoretical research scope	Selection process of reinforcement nodes.	We demonstrate the feasibility of utilizing our model to determine critical node thresholds.
Load capacity model discussion	Various initial load scenarios using a linear capacity model.	We conduct a thorough exploration of a nonlinear capacity model. This includes analyzing changes in maximum capacity across different parameter settings and considering diverse initial load scenarios under the nonlinear capacity model. We also perform threshold analysis for load model parameters in both directed and undirected networks.
Cascading failure model application	ER networks and BA networks.	We extend our model's application to ER, WS, and BA network topologies. We analyze conditions within a smaller "toy net" context and provide a comparative study within the IEEE power network. Additionally, we apply our model to the real US power grid network.
Additional aspect	Three optimized adaptable reinforcement strategies based on node capacity redundancy at different scales.	We delve into the impact of initial attack strategies and the number of targeted nodes on network robustness.

impact the robustness of the network. When attacking BA, WS, and US networks, attacking a small number of nodes can also significantly affect network robustness, which reminds us to pay attention to the identification and protection of key nodes

(3) Adding early nodes decreases the strength of the network against random assaults. Regardless of the number of starting nodes, purposeful assaults may severely impair the connection of the network and diminish its robustness.

(4) In general, the US network has fewer failure nodes compared to the small-world network. In the first stage, there are fewer failure nodes overall, but it takes longer for a failure to complete than in the BA network.

(5) Adjusting the value of β can improve the invulnerability index of the network and make it more resistant to cascading failures, but care must be taken to avoid making the value of β too large.

Our findings, such as the relative significance of downstream nodes in directed networks and the relatively robust nature of weighted power networks, can be used to support the mitigation of cascading failures and ensure secure operations in power grids. Furthermore, the results of this study can be leveraged to enhance the resilience and resistance of power grids against disasters.

Future studies can focus on the extension of nonlinear load capacity models to more complex network structures and real-world network scenarios. Furthermore, a better understanding of the variations among different nonlinear models can be achieved through further investigations, providing more robust evidence.

Acknowledgment

This work was supported by the National Key R&D Program of China for International S&T Cooperation Projects (No. 2019YFE0118700), National Natural Science Foundation of China (Nos. 62222306 and 61973110), Hunan Young Talents Science and Technology Innovation Project (No. 2020RC3048), and Natural Science Found for Distinguished Young Scholars of Hunan Province (No. 2021JJ10030).

References

[1] A. E. Motter and Y. C. Lai, Cascade-based attacks on complex networks, *Phys. Rev. E*, vol. 66, no. 6, p. 065102, 2002.

[2] P. Crucitti, V. Latora, and M. Marchiori, Model for cascading failures in complex networks, *Phys. Rev. E Stat. Nonlinear Soft Matter Phys.*, vol. 69, no. 4, p. 045104, 2004.

[3] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, et al., Causes of the 2003 major grid blackouts in North America and Europe, and

recommended means to improve system dynamic performance, *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, 2005.

[4] S. Li, L. Li, Y. Yang, and Q. Luo, Revealing the process of edge-based-attack cascading failures, *Nonlinear Dyn.*, vol. 69, no. 3, pp. 837–845, 2012.

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

[6] H. Chen, L. Zhang, Q. Liu, H. Wang, and X. Dai, Simulation-based vulnerability assessment in transit systems with cascade failures, *J. Clean. Prod.*, vol. 295, p. 126441, 2021.

[7] H. Liu, X. Chen, L. Huo, Y. Zhang, and C. Niu, Impact of inter-network assortativity on robustness against cascading failures in cyber–physical power systems, *Reliab. Eng. Syst. Saf.*, vol. 217, p. 108068, 2022.

[8] J. Li, Y. Wang, J. Zhong, Y. Sun, Z. Guo, Z. Chen, and C. Fu, Network resilience assessment and reinforcement strategy against cascading failure, *Chaos Solitons Fractals*, vol. 160, p. 112271, 2022.

[9] S. Liu, C. Yin, D. Chen, H. Lv, and Q. Zhang, Cascading failure in multiple critical infrastructure interdependent networks of syncretic railway system, *IEEE Trans. Intell. Transport. Syst.*, vol. 23, no. 6, pp. 5740–5753, 2022.

[10] J. Cumelles, O. Lordan, and J. M. Sallan, Cascading failures in airport networks, *J. Air Transp. Manag.*, vol. 92, p. 102026, 2021.

[11] H. Hao, Z. Ma, A. Wang, W. Xing, H. Song, P. Zhao, J. Wei, and S. Zheng, Modeling and assessing the robustness of the lithium global trade system against cascading failures, *Resour. Policy*, vol. 85, p. 103822, 2023.

[12] N. Wang, Z. Y. Jin, and J. Zhao, Cascading failures of overload behaviors on interdependent networks, *Phys. A Stat. Mech. Appl.*, vol. 574, p. 125989, 2021.

[13] X. Shi, W. Long, Y. Li, and D. Deng, Robustness of interdependent supply chain networks against both functional and structural cascading failures, *Phys. A Stat. Mech. Appl.*, vol. 586, p. 126518, 2022.

[14] Y. Tang, L. Li, and X. Liu, State-of-the-art development of complex systems and their simulation methods, *Complex System Modeling and Simulation*, vol. 1, no. 4, pp. 271–290, 2021.

[15] Y. Xia, W. Zhang, and X. Zhang, The effect of capacity redundancy disparity on the robustness of interconnected networks, *Phys. A Stat. Mech. Appl.*, vol. 447, pp. 561–568, 2016.

[16] L. Böttcher, M. Luković, J. Nagler, S. Havlin, and H. J. Herrmann, Failure and recovery in dynamical networks, *Sci. Rep.*, vol. 7, no. 1, p. 41729, 2017.

[17] C. Liu, D. Li, B. Fu, S. Yang, Y. Wang, and G. Lu, Modeling of self-healing against cascading overload failures in complex networks, *EPL Europhys. Lett.*, vol. 107, no. 6, p. 68003, 2014.

[18] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, A critical review of cascading failure analysis and modeling of power system, *Renew. Sustain. Energy Rev.*, vol. 80, pp. 9–22, 2017.

[19] B. Wu, T. Yuan, Y. Qi, and M. Dong, Public opinion dissemination with incomplete information on social network: A study based on the infectious diseases model and game theory, *Complex System Modeling and Simulation*, vol. 1, no. 2, pp. 109–121, 2021.

[20] D. S. Yang, Y. H. Sun, B. W. Zhou, X. T. Gao, and H. G. Zhang, Critical nodes identification of complex power systems based on electric cactus structure, *IEEE Syst. J.*, vol. 14, no. 3, pp. 4477–4488, 2020.

[21] C. Y. Chen, Y. Zhao, J. Gao, and H. E. Stanley, Nonlinear model of cascade failure in weighted complex networks considering overloaded edges, *Sci. Rep.*, vol. 10, no. 1, p. 13428, 2020.

[22] C. Y. Chen, Y. Zhou, Y. Wang, L. Ding, and T. Huang, Vulnerable line identification of cascading failure in power grid based on new electrical betweenness, *IEEE Trans. Circuits Syst. II*, vol. 70, no. 2, pp. 665–669, 2023.

[23] C. Y. Chen, Y. Zhao, H. Qin, X. Meng, and J. Gao, Robustness of interdependent scale-free networks based on link addition strategies, *Phys. A Stat. Mech. Appl.*, vol. 604, p. 127851, 2022.

[24] A. L. Barabási, Network science, *Phil. Trans. R. Soc. A.*, vol. 371, no. 1987, p. 20120375, 2013.

[25] W. Gong, Z. Liao, X. Mi, L. Wang, and Y. Guo, Nonlinear equations solving with intelligent optimization algorithms: A survey, *Complex System Modeling and Simulation*, vol. 1, no. 1, pp. 15–32, 2021.

[26] Z. Liao and S. Li, Solving nonlinear equations systems with an enhanced reinforcement learning based differential evolution, *Complex System Modeling and Simulation*, vol. 2, no. 1, pp. 78–95, 2022.

[27] L. Wang, Z. Pan, and J. Wang, A review of reinforcement learning based intelligent optimization for manufacturing scheduling, *Complex System Modeling and Simulation*, vol. 1, no. 4, pp. 257–270, 2021.

[28] W. Song, W. Zhang, J. Wang, L. Zhai, P. Jiang, S. Huang, and B. Li, Blockchain data analysis from the perspective of complex networks: Overview, *Tsinghua Science and Technology*, vol. 28, no. 1, pp. 176–206, 2023.

[29] P. Erdős and A. Rényi, On random graphs. I, *Publ. Math. Debrecen*, vol. 6, nos. 3&4, pp. 209–297, 1959.

[30] D. J. Watts and S. H. Strogatz, Collective dynamics of ‘small-world’ networks, *Nature*, vol. 393, no. 6684, pp. 440–442, 1998.

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

[32] W. Fan, Z. Liu, P. Hu, and S. Mei, Cascading failure model in power grids using the complex network theory, *IET Gener. Transm. Distrib.*, vol. 10, no. 15, pp. 3940–3949, 2016.

[33] M. E. J. Newman, Communities, modules and large-scale structure in networks, *Nat. Phys.*, vol. 8, no. 1, pp. 25–31, 2012.

[34] J. Zhang and Y. Luo, Degree centrality, betweenness centrality, and closeness centrality in social network, in

Proc. 2017 2nd Int. Conf. Modelling, Simulation and Applied Mathematics (*MSAM2017*), Bankog, Thailand, 2017, pp. 300–303.

[35] M. Barthélemy, Betweenness centrality in large complex networks, *Eur. Phys. J. B Condens. Matter*, vol. 38, no. 2, pp. 163–168, 2004.

[36] K. Okamoto, W. Chen, and X. Y. Li, Ranking of closeness centrality for large-scale social networks, in *Proc. Int. Workshop Frontiers in Algorithmics*, Changsha, China, 2008, pp. 186–195.

[37] D. L. Duan, Cascading failure of complex networks based on load local preferential redistribution rule, *Complex Systems and Complexity Science*, vol. 12, no. 1, pp. 33–39, 2015.

[38] J. W. Wang and L. L. Rong, A model for cascading failures in scale-free networks with a breakdown probability, *Phys. A Stat. Mech. Appl.*, vol. 388, no. 7, pp. 1289–1298, 2009.

[39] X. Wei, J. Zhao, T. Huang, and E. Bompard, A novel cascading faults graph based transmission network vulnerability assessment method, *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2995–3000, 2018.

[40] W. X. Wang and G. Chen, Universal robustness characteristic of weighted networks against cascading failure, *Phys Rev E Stat Nonlin Soft Matter Phys*, vol. 77, no. 2, p. 026101, 2008.

[41] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari, Cascaded failures in weighted networks, *Phys. Rev. E*, vol. 84, no. 4, p. 046114, 2011.

[42] J. Yan, Y. Tang, H. He, and Y. Sun, Cascading failure analysis with DC power flow model and transient stability analysis, *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 285–297, 2015.

[43] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. H. Hines, Dynamic modeling of cascading failure in power systems, *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2085–2095, 2016.

Chaoyang Chen received the PhD degree in control science and engineering from Huazhong University of Science and Technology, Wuhan, China in 2014. He is currently a professor at Hunan University of Science and Technology, Xiangtan, China. From 2015 to 2017, he served as a postdoctoral researcher at the School of Information Science and Engineering, Central South University, Changsha, China. From 2018 to 2019, he was a visiting researcher at the Polymer Research Center and Department of Physics, Boston University, Boston, MA, USA. His current research interests include networked control systems, complex networks and multi-agent systems, robust control, and related applications.

Xiangyi Meng received the BS degree from Peking University, Beijing, China in 2015, and the PhD degree from Boston University, Boston, MA, USA in 2020. He is currently serving as a research associate at the Department of Physics and Astronomy, Northwestern University, Evanston, IL, USA. His primary research interests encompass interdependent networks and cascading failures.

Yao Hu received the bachelor degree in mechanical and electronic engineering from Hunan University of Science and Technology, Xiangtan, China in 2021 and is currently pursuing the master degree in control science engineering at Hunan University of Science and Technology, China. Currently, his research focuses on complex networks, power networks, interdependent network modeling, and cascading failures analysis.

Jinzhu Yu received the bachelor and master degrees from Tongji University, Shanghai, China and the PhD degree in systems engineering from Vanderbilt University, NashVille, TN, USA. He is currently an assistant professor at the Department of Civil Engineering, University of Texas, Arlington, TX, USA. He previously served as a postdoctoral researcher at the Department of Computer Science and the Center for Network Technology, Rensselaer Institute of Technology, USA. His research interests include complex networks, interdependent networks, and cascading failures.