Hindawi
Journal of Sensors
Volume 2021, Article ID 8820413, 12 pages
https://doi.org/10.1155/2021/8820413

Research Article

Power Grid-Oriented Cascading Failure Vulnerability Identifying Method Based on Wireless Sensors

Shudong Li[1], **Yanshan Chen**[2], **Xiaobo Wu**[3], **Xiaochun Cheng**[4] and **Zhihong Tian**[1]

[1]*Cyberspace Institute of Advance Technology, Guangzhou University, Guangzhou 510006, China*
[2]*School of Economics and Statistics, Guangzhou University, Guangzhou 510006, China*
[3]*School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China*
[4]*School of Science and Technology, Middlesex University, London, UK*

Correspondence should be addressed to Shudong Li; lishudong@gzhu.edu.cn and Xiaobo Wu; happywxb@gzhu.edu.cn

Received 24 April 2020; Revised 28 August 2020; Accepted 22 May 2021; Published 28 June 2021

Academic Editor: Iftikhar Ahmad

In our paper, we study the vulnerability in cascading failures of the real-world network (power grid) under intentional attacks. Here, we use three indexes (B, K, k-shell) to measure the importance of nodes; that is, we define three attacks, respectively. Under these attacks, we measure the process of cascade effect in network by the number of avalanche nodes, the time steps, and the speed of the cascade propagation. Also, we define the node's bearing capacity as a tolerant parameter to study the robustness of the network under three attacks. Taking the power grid as an example, we have obtained a good regularity of the collapse of the network when the node's affordability is low. In terms of time and speed, under the betweenness-based attacks, the network collapses faster, but for the number of avalanche nodes, under the degree-based attack, the number of the failed nodes is highest. When the nodes' bearing capacity becomes large, the regularity of the network's performances is not obvious. The findings can be applied to identify the vulnerable nodes in real networks such as wireless sensor networks and improve their robustness against different attacks.

1. Introduction

Nowadays, people's daily life is increasingly dependent on electricity, but the failures and blackout happened in the electricity system has resulted in heavy losses and a huge impact on people's lives. There are a lot of famous examples like the massive power failure on the West Coast of United States in September 2011, the breakdown of Ukraine's electricity system under malicious attacks and the blackout in New York city in July 2019, and the massive power failure on the U.S. West Coast in 2019. Therefore, to this day, the research on the power grid is still hot. The current research on network robustness mainly includes these aspects: research based on power grid structure, analysis based on cascading effects, how to identify network attacks, and how to defend network attacks.

In terms of structural analysis, Huang [1] et al. (2013) used the theory of complex networks and obtained the distribution of risk energy along the path in the vulnerability analysis of cascading faults considering branch structures. Based on graph theory technology, Correa [2] et al. (2013) obtained the applicability conclusion of the graph theory method for the vulnerability of power grids by comparing the physical flow model and the statistical indicators of scale-free graphs. Based on the normalization effect of neighboring nodes and the weight distribution of nodes in the network, Wang [3] et al. (2014) studied the different roles of low-load and high-load nodes and the relationship between some parameters in the network and the strongest level of robustness. Finally, through numerical simulation, they obtained the parameter values corresponding to the model at the strongest level of robustness. Ouyang [4] et al. (2014) used the betweenness based-model (BBM), direct current power flow model (DCPFM), and purely topological model(PTM) to study network robustness under intentional attacks based on betweenness, degree, importance, and maximum traffic. Yang [5] et al. (2015) discussed the relationship between community structure and network robustness and proposed

a three-step strategy to improve network robustness while maintaining the degree distribution and the structure of the network community.

In terms of analysis based on cascading effects, considering the traffic load, Tan [6] et al. (2015) used the Barabasi-Albert scale-free network and interdependent Erdos-Renyi random graph to research the effect of the coupling mode on the cascade effect. Through research, Erdos-Renyi random graphs are fragile and robust. However, the interdependent Barabasi-Albert scale-free network is vulnerable to intentional attacks and the random attacks. These results are similar for interdependent communication networks and power grids, for the nonvulnerability under intentional attacks and the actual interdependent system. Cai [7] et al. (2016) analyzed the complex effects of cascading faults by modeling the interdependence between power systems and dispatch data networks. Their simulation results show that under random attacks, the probability of catastrophic failure of the power grid combined with the mesh structure is higher than that with a double-star structure; while under intentional attacks, the transmission performance of the mesh network is better than that of the double-star structure. Hai-PengRen [8] et al. (2016) proposed a new load distribution for the cascade effect and a node removal rule, that is, in the opposite direction of the flow, removing the first overload node, and then the network distributes the load and continues cascading process. This method has proven to suppress large-scale cascading failures. According to the maximum flow theory, Wenli [9] et al. (2016) proposed a model of cascading failure. Their results show that the node load distribution has a great impact on the cascading dynamics and the tolerance parameter threshold. Kornbluth [10] et al. (2018) use the node's betweenness centrality as the load to research the cascading effect of the network when the node's load is overloaded. They study the functional relationship between the initial attack and the number of surviving nodes at the end of the cascade PF strength under different tolerance values in Erdös-Renyi graphs and random regular graphs.

In terms of how to identify network attacks, Yan [11] et al. (2017) analyzed the vulnerability of the transmission network under sequential topology attack and proposed a method based on Q-learning. This method can identify the critical attack sequence considering the dynamic behavior of the physical system. Wang [12] et al. (2017) developed a smart search method based on state-space pruning to identify incidents of cyber attacks. They used the stochastic chemistry method and particle swarm optimization algorithm and took the IEEE system as an example to verify the efficiency and of the method. Lei [13] et al. (2020) proposed a distributed iterative positioning algorithm based on the abandonment strategy of the sensor relative to its neighbor's center of gravity coordinates. The algorithm uses relative distance calculations to locate the data packet loss through the neighbor's communication link. And they accurately locate the sensor through this algorithm. Daniel [14] et al. (2020) proposed an algorithm that shows the relationship between the variance of the attacker's signal and how far away the nodes are, which solves the problem of constructing a centralized and distributed version of Nesterov with the best fixed parameters.

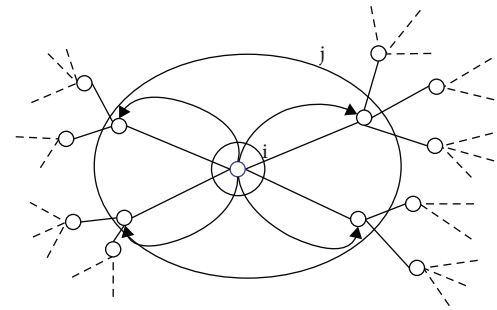

Figure 1: The evolution process of cascading faults in the network model.

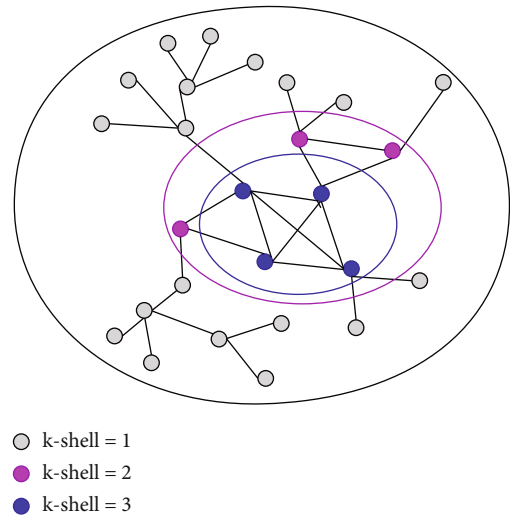

Figure 2: The definition of k-shell. Removing all the nodes with degree 1 and repeating this step until there are no nodes with degree 1 in the grid. Then, define their value of k-shell as 1 ($k-\text{shell}=1$), which is the outer circle in the figure. Next, continue to remove the node with a degree of 2. As described above, the k-shell value of the removed nodes is defined as 2 ($k-\text{shell}=2$), which is circle 2. Similarly, the k-shell values of all points are obtained.

In terms of how to defend network attacks, Zheng [15] et al. (2014) proposed a weighting strategy for edges, that is, designing the path length of the edge as the product of the clustering coefficients of the edge nodes and calculating the corrected neutrality center of the edge and applying it as a weight to the cascade model. It is found that the weighting scheme based on the modified betweenness centrality makes the three networks of the modular network, scale-free network, and small-world network all better than the original betweenness centrality networks that are more robust against edge attack. Liu [16] et al. (2015) found two ways to reduce the system vulnerability: (1) protect nodes with high degree and (2) increase the degree of correlation between networks. Guo [17] et al. (2017) proposed a vulnerability analysis method using the Cyber-Physical Power System (CPPS) model composed of the physical layer, network layer, and network physical interface and used this method to calculate

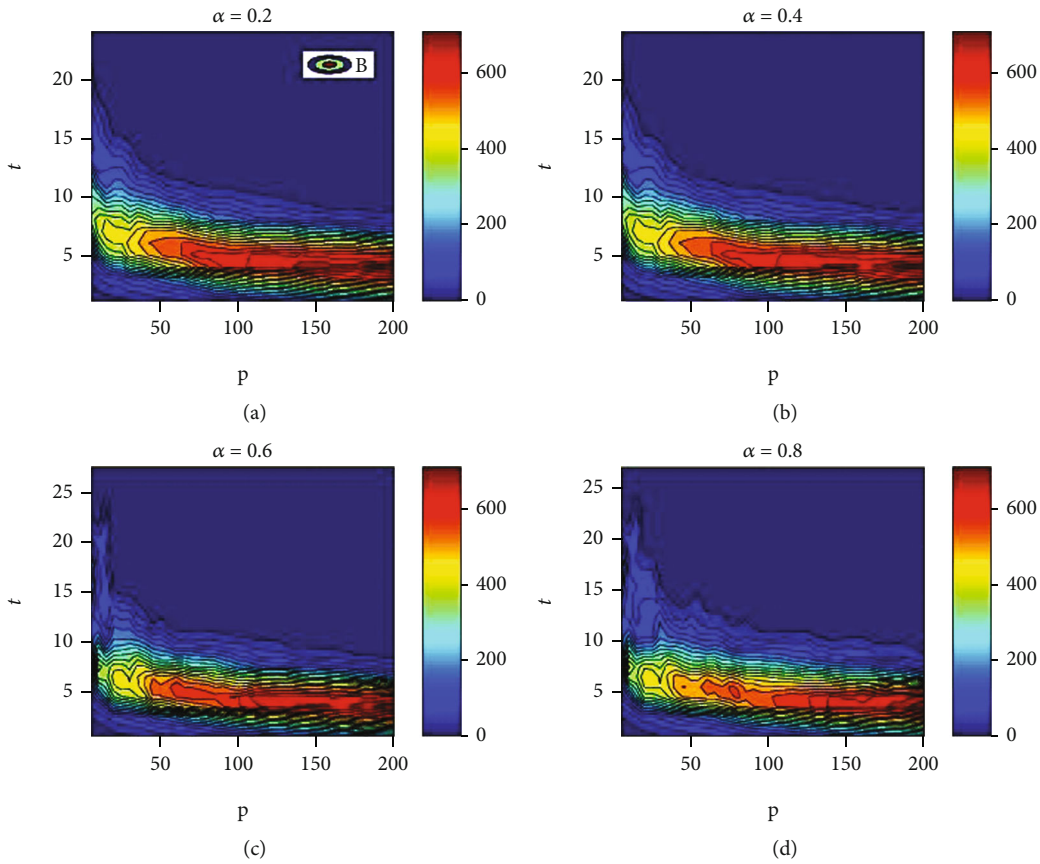

Figure 3: Under *B* attack, the figure shows how many nodes failed in the network (color shades) at time *t* (axis *Y*) when *p* nodes were attacked (axis *X*), where the range of p is 5 to 200, with an interval of 5 nodes. (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

the performance index of the model before and after the cascade failure. By comparing different attack strategies and interface strategies, they concluded that CPPS should protect high-indexed nodes and is more vulnerable to malicious attacks. Wang [18] et al. (2018) proposed a strategy to defend against cyber attacks by studying electronic computing physical systems (ECPSs). Besides, they also provided a weight adjustment strategy to work out the problem of unbalanced current caused by the split event. In the paper, their assessment of vulnerability has five aspects: robustness, economic cost, degree of damage, fragile equipment, and trigger points. Ma [19] et al. (2019) proposed a scale-free network model that can more effectively control the propagation of cascading faults. In their model, the connection load of any two nodes is defined, taking into account the degree and intermediateness of the nodes. Irshaad [20] et al. (2019) combined cognitive dynamic and state estimation systems in the smart network and proposed a new SG metric: entropy state. The manager achieves the goal of improving the entropy state by reconfiguring the weights of the sensors in the grid and dynamically optimizing the state estimation process. And CDS is the best choice for monitoring systems.

It can be seen from the above literature review that scholars understand the network structure and cascading effects and use sensors to identify attacks and defend them. In this article, we default to the identification of sensors and attach importance to defense to protect high-load nodes. However, rather than studying structural defenses, we value the impact of the network after an attack. We recorded not only the number of nodes in the network that crashed but also the speed and time of the crash. Because we believe that under the technical recognition of sensors, understanding the law of network collapse is of great practical significance for future defenses.

We break this article into three sections. In Section I, we will introduce the load distribution model of the network. In Section II, we will show three attacks. In Section III, we will list some indicators to show the extent to which the network is crashing. In Section IV, we will present the results graphically and analyze them. Finally, we will give the conclusion.

2. Results and Discussion

2.1. The Cascading Failure Model

2.1.1. Load Distribution Model. It can be seen from multiple studies that the load of a node is often estimated by the node's betweenness centrality [21, 22]. Therefore, in our paper, we set the betweenness centrality of the node as its load.

In reality, when a node is crashed by an attack, its load is distributed to other nodes in the network [23]. There are two distribution methods, global distribution and local

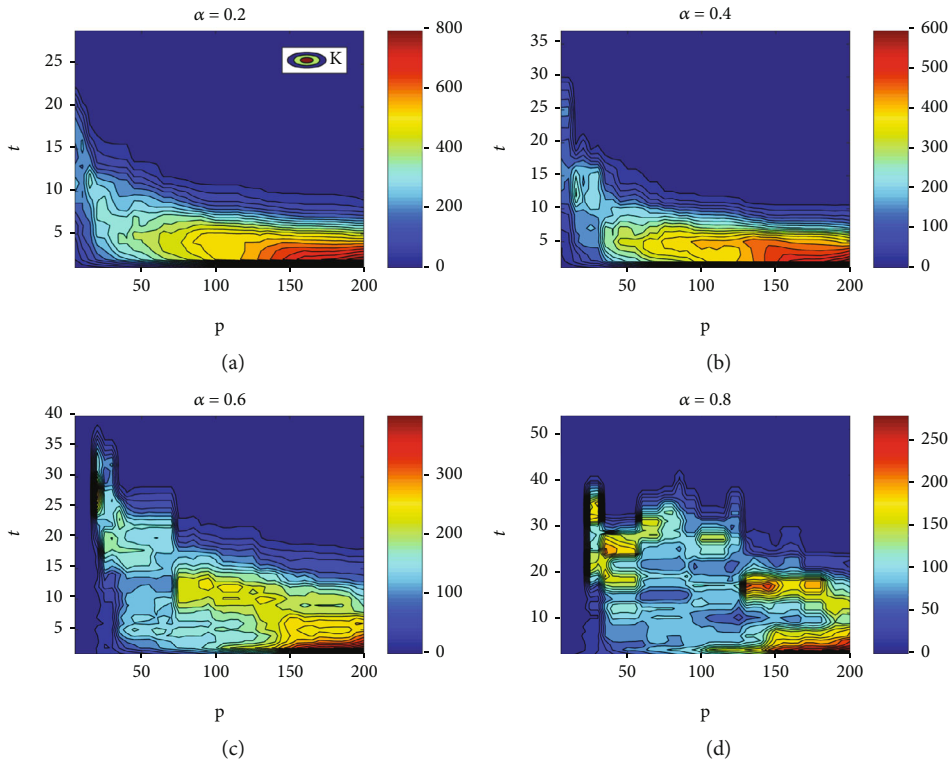

Figure 4: Under K attack, the figure shows how many nodes failed in the network (color shades) at time t (axis Y) when p nodes were attacked (axis X), where the range of p is 5 to 200, with an interval of 5 nodes. (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

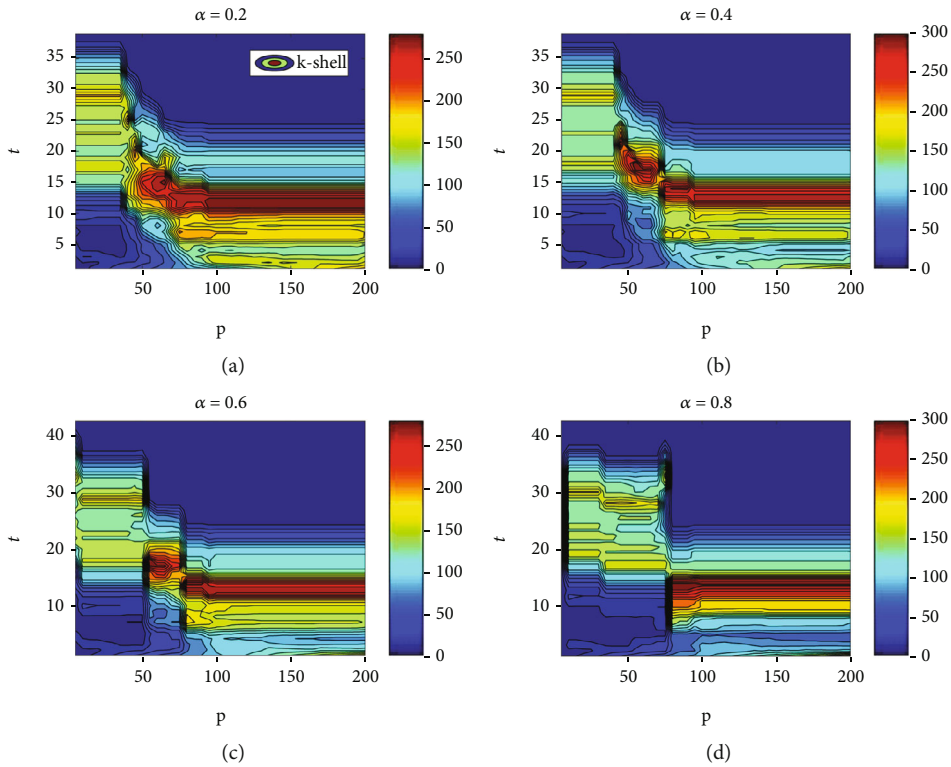

Figure 5: Under k-shell attack, the figure shows how many nodes failed in the network (color shades) at time t (axis Y) when p nodes were attacked (axis X), where the range of p is 5 to 200, with an interval of 5 nodes. (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

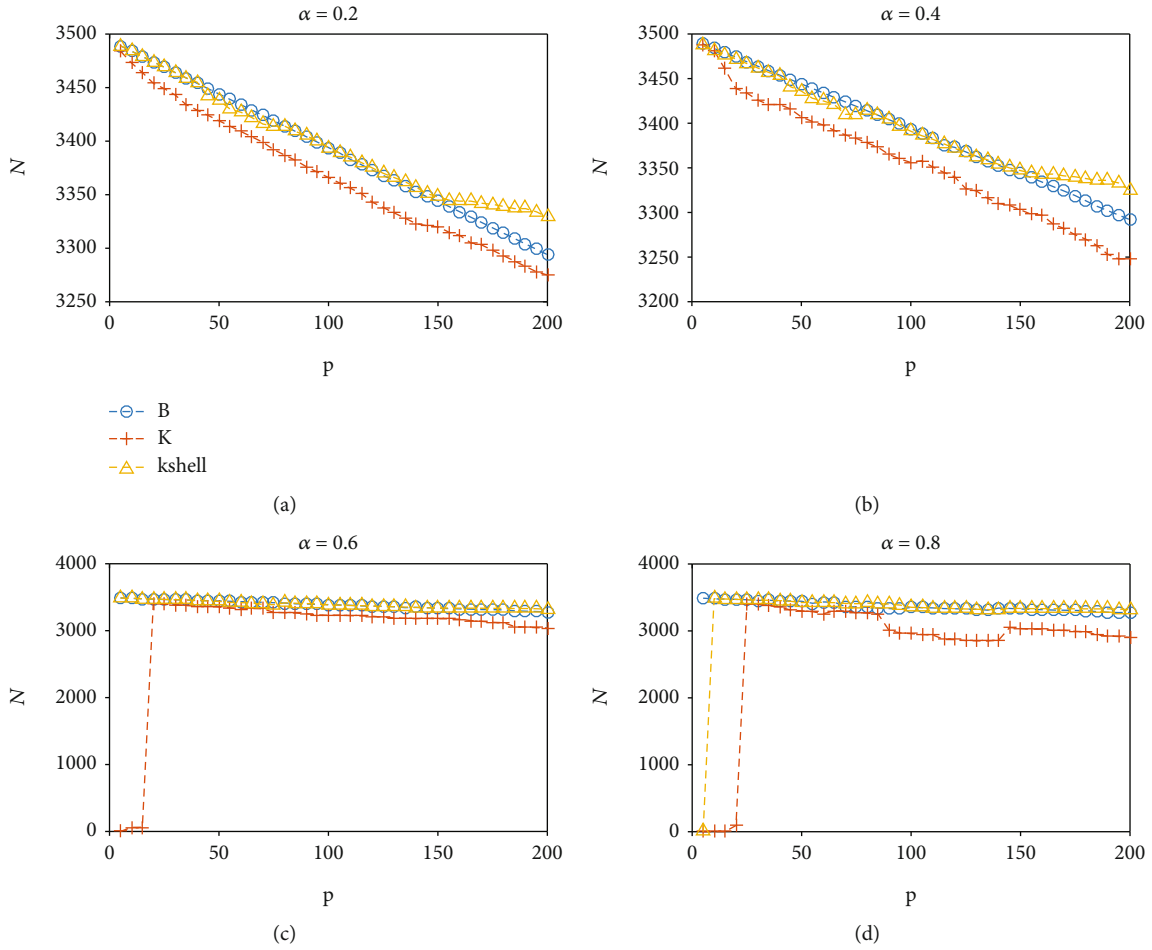

FIGURE 6: Under three attack strategies, the total number of the failed nodes N (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

distribution. Global distribution seems to be more comprehensive, but in actual research, global distribution calculation is huge, and in global distribution, the load is distributed in inverse proportion to the distance. On the contrary, distributing load to neighboring nodes is effective and reasonable. On the one hand, it can show the level after the collapse of the network. On the other hand, calculations are greatly reduced. Local distribution is not single, for example, using game theory [24]. Consequently, we adopt the local distribution method of node load distribution to its neighboring nodes after a node fails in this article, which is more suitable for research.

As shown in Figure 1, when the node i crashes, it allocates its own load to its neighboring node set j in a certain form. When a node is a neighboring node that exceeds its maximum load, the node fails and continues to be distributed to its neighboring nodes, which results in the cascade effect. Until the assigned nodes in the network do not exceed the maximum load, the process of cascading faults stops [25].

2.1.2. Cascade-Related Indicators. To measure the cascading effect of the network, you need to define some relevant indicators.

First of all, as mentioned above, we define the initial load (L) of node i [26] as the node's betweenness centrality (B).

$$L_i(0) = B_i. \tag{1}$$

Secondly, define the maximum load (C) that the node can withstand [27]. The definition is as follows:

$$C_i = (1 + \alpha)L_i(0). \tag{2}$$

In the formula, α is a tunable parameter, ranging from 0 to 1, indicating the performance of the nodes [28]. The larger the value of α, the better the load-carrying capacity of the node.

The next is how to distribute. At time t, as node i failed, its neighboring node k increases the load (ΔL_k) as

$$\Delta L_k(t) = \frac{B_i}{\sum B_j} L_i(t-1), \tag{3}$$

where k is any node of set j. The load distributed from the node i is added to each neighboring node. If the one of neighboring nodes exceeds its maximum load, the node fails [29].

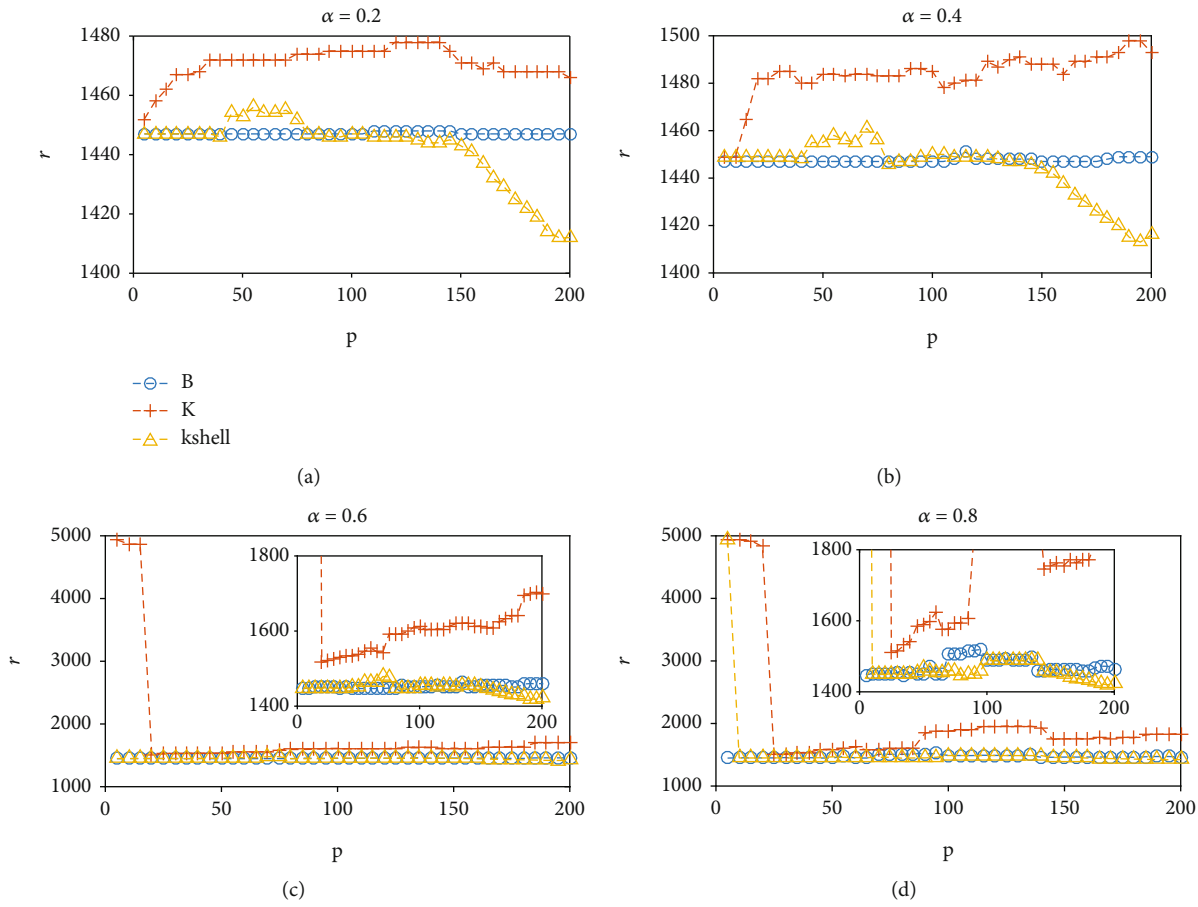

Figure 7: Under three attack strategies, the number of remaining nodes r (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

2.1.3. Simulated Attack Model. In general, our model is to achieve intentional attacks in reality by selecting high-load nodes to attack. After being attacked, the attacked node will distribute its load to neighboring nodes, that is, using the previous load distribution model. When any neighboring node's load exceeds its capacity, it will collapse and continue to distribute its load, thus form a series of chain reactions [30, 31]. And we will simulate this process through a computer to get our final conclusion.

2.2. Three Attack Strategies. We examine the survivability of the network under intentional attacks [32] in this article. Under intentional attacks, important nodes in the network will be attacked. Important nodes are often measured by the node's betweenness centrality, degree [33], k-shell [34] value, etc. Therefore, we study three attacks that sort these three metrics in descending order to attack. The three attacks are as follows:

(1) Betweenness attack (B attack): based on the above-mentioned distribution method, we sort all nodes in descending order of the betweenness centrality, then attack the top nodes

(2) Degree-based attack (K attack): The nodes to be attacked are arranged in descending order of degrees, and the rest are the same as the betweenness-based attack

(3) k-shell-based attack: keep the other conditions the same and arrange the attacked nodes in descending order according to the value of k-shell. For the definition of k-shell, see the Figure 2 below

Attack the nodes according to these three attacks, and then through certain indicators [35], we can see the degree of network collapse. Next, we will introduce the evaluation indicators.

2.3. Evaluation Indicators. Obviously, the degree of network collapse [36, 37] is bound up with the number of nodes that fail. The quantity available is an important indicator. On the other hand, due to the cascading effect, the moments when different nodes fail are not necessarily the same. Therefore, we must first define the time of the cascade. With quantity and time, we naturally think of another indicator—speed. Below, we will explain these three indicators in detail.

(1) Time: As for the time, we define the time of the attack as the moment 0 ($t = 0$), the time of the neighboring nodes fail caused by the attacked nodes as the moment 1($t = 1$), and so on to define the cascade moment. In addition, what we can get from this is

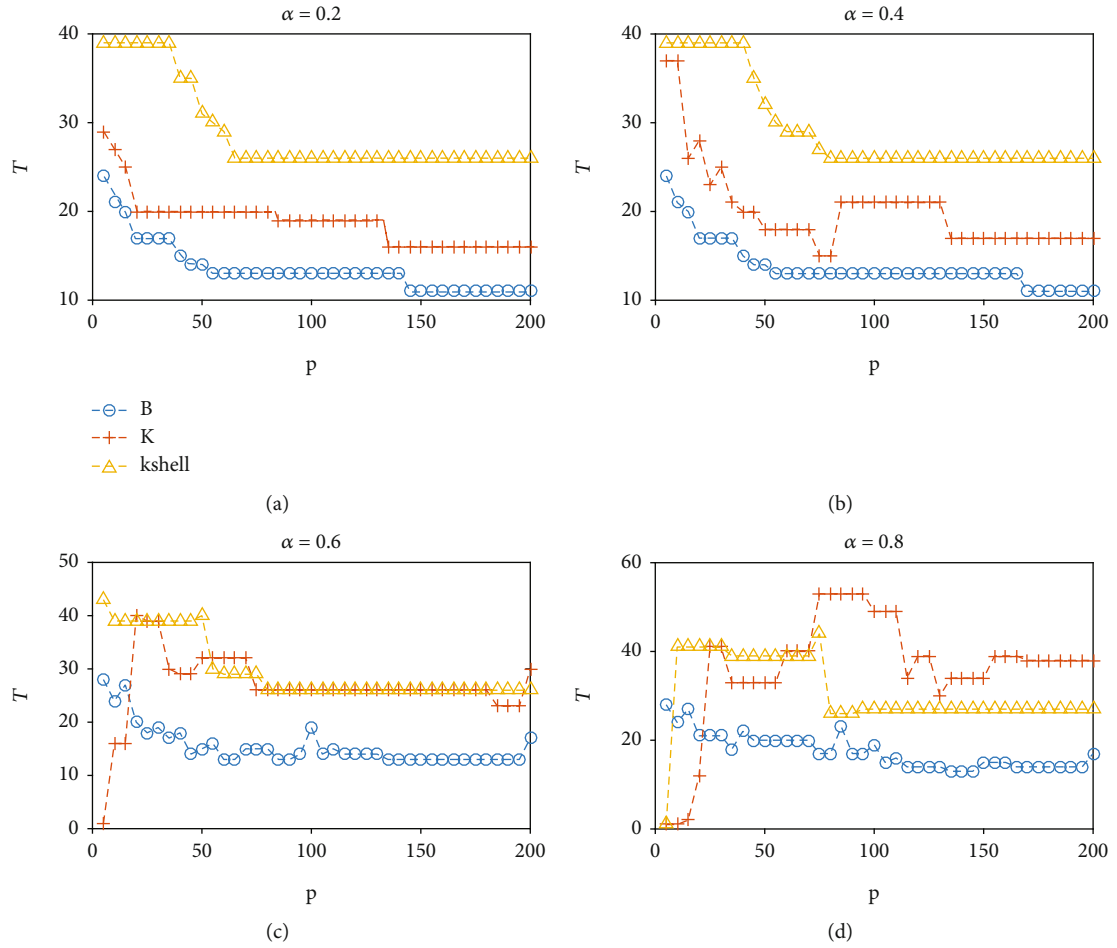

FIGURE 8: Under three attack strategies, the persistent time of cascade T (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6. (d) is an image with α equal to 0.8.

that the last moment recorded is the time (t) used for the cascade effect

(2) The number of failed nodes: Aiming to analyze the collapse of the network in the cascade effect process, we count the nodes that fail at different times (n (t)). By adding these numbers, we can get the total number of nodes that fail, calculated as follows:

$$N = \sum_{t=1}^{T} n(t). \tag{4}$$

(3) The number of noncrashed nodes: Knowing the total number of nodes (M) in the power grid and the number of failure nodes, we can easy to calculate the nodes that did not fail, excluding the number of nodes that have attacked (p), calculated as follows:

$$r = M - N - p. \tag{5}$$

(4) Speed of cascade: Speed is the quotient of quantity (N) and time (t). Here, the time it takes for the cascade effect to start and end. The quantity (N) here refers to the total number of nodes that fail. The specific formula is as follows:

$$v = \frac{N}{T}. \tag{6}$$

All in all, it is easy to know that the total number of failure nodes shows the degree of network collapse, and time and speed show the effects of different attacks. Then, based on these indicators, from the results, we can detect the effect of the cascade effect of the network under different attack conditions.

3. Result Analysis

Based on the previous model and evaluation indicators, we test it using the U.S. grid as an example. This power grid is a network with 4941 nodes and 6,594 edges. Here, we assume

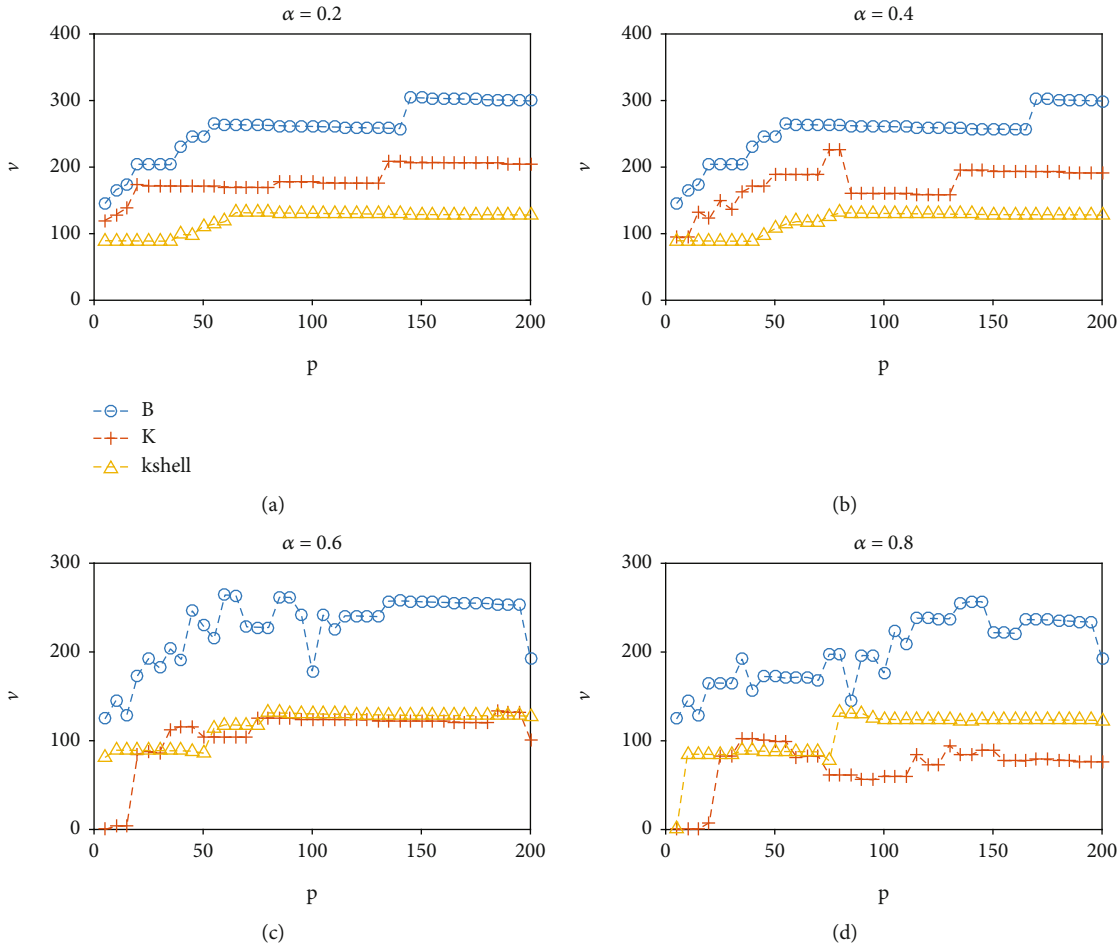

FIGURE 9: Under three attack strategies, the speed of cascade effect V (axis Y) is after attacking p nodes (axis X). (a) is an image with α equal to 0.2. (b) is an image with α equal to 0.4. (c) is an image with α equal to 0.6,.(d) is an image with α equal to 0.8.

that the edges of the network [38] are unweighted, and the distribution of the load is undirected.

3.1. Preliminary Analysis. As mentioned above, we will record the number of nodes that fail at each moment in the cascade effect. Therefore, we will initially display it in a three-dimensional graph.

Through the adjustment of α and the adjustment of attack modes, we can have different results. Among them, we will find some novel conclusions. Next, we will present them in turn.

As can be seen from the vertical perspective of Figure 3, under the B attack, the number of nodes in the cascade effect increases with time, showing a trend of increasing first and then decreasing. From the horizontal perspective, as the number of attacked nodes increases, so does the number of collapse nodes in the cascade effect. And it can be roughly seen that with the increasing of the number of attacked nodes, the total time of the cascade effect generally decreases.

Next, we use the same distribution method to perform the same operation on nodes sorted by degree (K). The result is shown in Figure 4.

It can be seen from Figure 4 that the horizontal and vertical images are roughly the same as the B attacks, but in the K attack, when the node performance is good, that is, when α is large, attacking a few important nodes has little impact on the entire network.

At last, we use the k-shell to measure the importance that is sorted by k-shell, attack the node with a large value of k-shell, and use the same distribution method to record the number of failure nodes, as shown in Figure 5.

It can be seen from Figure 5 that the image in the horizontal and vertical directions is roughly the same as the two modes, but compared to the previous two attack mode, this attack mode has a large time span and shows a fault phenomenon, as shown in Figure 5(a). The first 40 attacked nodes and less than 40 show roughly the same effect on the network, but when the number of attack nodes is greater than 40, the result of the attack is significantly different. This may be related to the point ordering with the same k-shell value.

3.2. Advanced Analysis. When α is determined, in a three-dimensional graph, we can know the time of the crash (t) and the number of crashed nodes at different times (n (t)) and compare the network crashes that attacked different numbers of nodes. However, we do not know whether the final total number of crashed nodes (N) still has such

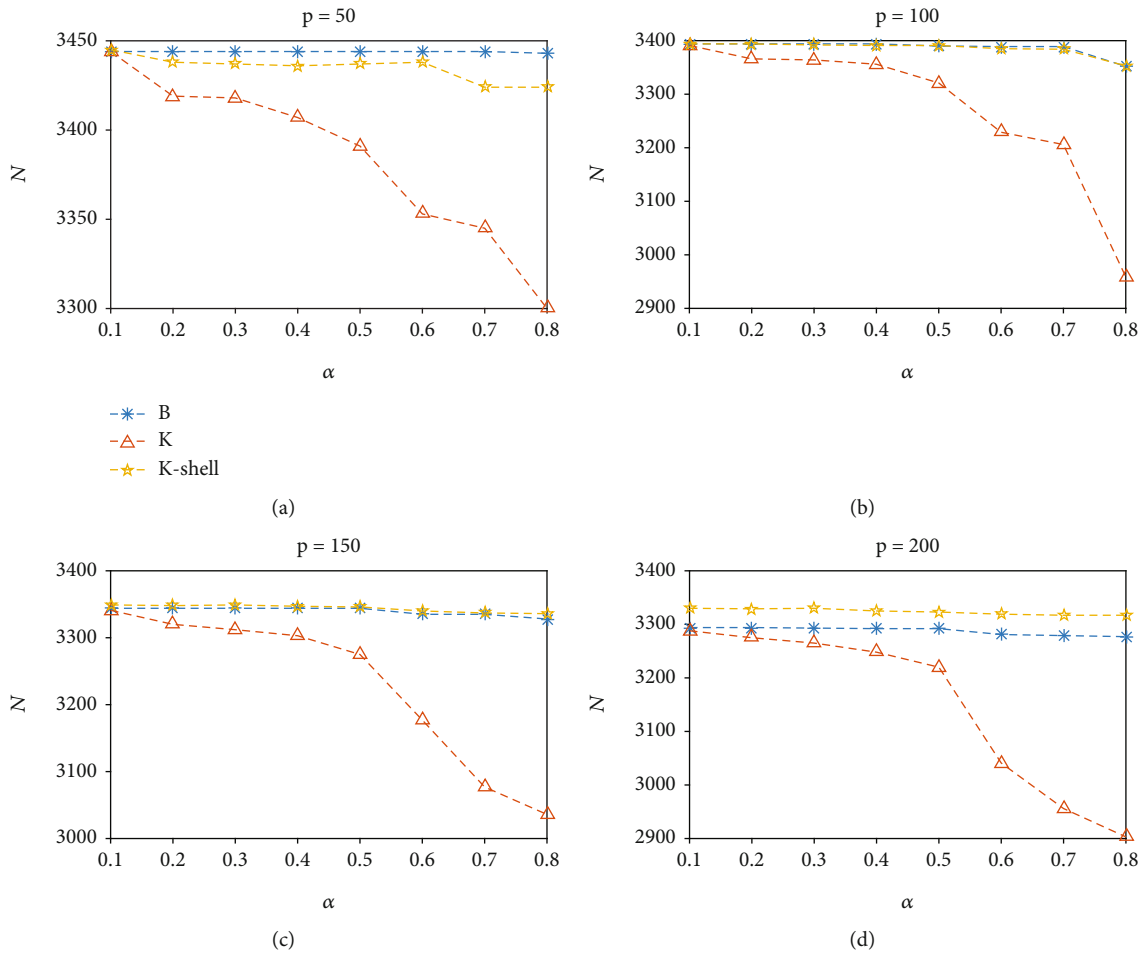

Figure 10: The total number of the failure nodes N (axis Y) is with different α (axis X). (a) is an image with attacking 50 nodes. (b) is an image with attacking 100 nodes. (c) is an image with attacking 150 nodes. (d) is an image with attacking 200 nodes.

regularity. Therefore, we introduce a two-dimensional graph to depict the total number of crashed nodes. In addition, we also depict time and speed accordingly.

From (a) and (b) of Figure 6, we see a strange phenomenon, and the more attacked nodes, the fewer the number of failed nodes. This is counterintuitive. However, there is a possible reason to explain this phenomenon; that is, the node that was attacked at the beginning is closely related to the nodes that are added later. The load allocated by the previous crashed node causes the subsequent node to fail. On how to answer this question, we draw a graph of the number of nodes without fail [39] (Figure 7). It turns out that for both the k-shell and the B attack, this explanation is feasible. As for how to explain the K attack, at this time, we should consider the phenomenon that the neighboring nodes fail at the same time, and the load cannot be distributed. Whether it is caused by one or both, we can conclude that, based on the previous model, increasing the number of attack nodes does not necessarily lead to an increase in network crash, especially for the B attack.

From Figures 6 and 7, we have not reached a good conclusion. However, from a time and speed perspective, we found good results. It can be seen from Figures 8 and 9 that when α is small, the speed and time of collapse reflect a better law. As the number of attacked nodes increases, the time spent by cascade effect decreases, and the speed of collapse increases. In addition, among the three attacks, the B attack has the shortest time and the fastest speed, followed by the K attack. When α is greater than or equal to 0.6, the volatility of the data is larger, and the law is not very obvious, but it can still be seen that the B attack is more destructive to the power grid.

From this, we reasonably guess that the size of the alpha has an effect on the number of nodes that fail. To do this, we set α as the independent variable [40], set the number of failure nodes as the dependent variable, and plot the results as follows.

It can be seen from Figure 10 that as the value of α increases, the number of failure nodes decreases. But as for the B attack and the K attack, the reduction trend is not obvious. Nevertheless, some phenomena can be found from them. As you can see from Figure 10(a), that when attacking 50 nodes, no matter how large α, the number of nodes fail by the betweenness-based attack is greater than the k-shell attack. However, when the number of attacks increased, there was almost no difference in the number of failure nodes by the two modes. When the number of attacked nodes is 200, the number of failure nodes by the k-shell attack is greater

than that of the B attack. On the other hand, the number of failure nodes in the network is closely related to the load capacity of the nodes for the K attack. In this case, improving the node's performance is very effective to ensure network security.

4. Conclusions

Through the above studies, we can draw some preliminary conclusions about the cascade effect. The specific conclusions will be listed in the following points.

(1) From the preliminary analysis, it can be roughly seen that at any time t, as the number of attacked nodes increases, so does the number of failure nodes, and the total crash time decreases

(2) However, Figures 6 and 7 show that the increase in the number of attacked nodes does not result in an increase in the total number of crashed nodes and a decrease in the number of noncrashed nodes. Based on the data of the number of crashed and noncrashed nodes, compared with the three attack methods, B attack is affected more

(3) Combined with the crash time and crash speed, it can be seen that the B attack has the fastest crash speed and the shortest crash time. Therefore, it can be known that in the B attack mode, the robustness of the network is the lowest, especially when α is small

(4) Improving the load-carrying capacity of a node is a good protection measure. Judging from the results, the load-carrying capacity of nodes has more influence on the degree of network collapse than the number of attack nodes, especially in K attack

(5) When the alpha is small, the cascading effect takes less time and is faster than the k-shell under the K attack. However, the number of failure nodes under the K attack is less than that of k-shell. Therefore, we cannot conclude that the K attack is stronger. If it is assumed that there is no way to intervene before the cascade effect stops, then the k-shell attack can be considered stronger

(6) When α is large and there are many attacked nodes, based on our model, our conclusions above may no longer be applicable

In the above conclusions, the results have revealed the topological vulnerability of cascade in the power grid systems under different attacks and could be used to design the robust topology of wireless sensor networks [41, 42]. The understanding of the process of network collapse is conducive to better erection and use of sensor detection. Under certain measures, this is a favorable measure to deal with the network cascade effect. But for other real networks [43–48], the results are maybe different. So, we will study the vulnerability in other real-world networks with considering the community structure [49] in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

S.L., Y.C., X.W., Z.T., and X.C. declare no conflicts of interest that are directly related to the submitted work.

Authors' Contributions

Shudong Li and Yanshan Chen contributed equally to this work.

Acknowledgments

This research was funded by the Key R&D Program of Guangdong Province (No. 2019B010136003), NSFC (Nos. U1803263 and 61672020), Project of Shandong Province Higher Educational Science and Technology Program (No. J16LN61), National Key Research and Development Program of China (No. 2019QY1406), and Guangdong Province Universities and Colleges Pearl River Scholar Funded Scheme (2019).

References

[1] X. C. Huang, H. Qi, X. P. Zhang, L. F. Lu, and Y. Y. Hu, "Analysis on power grid vulnerability considering cascading failure of branch," *Applied Mechanics and Materials*, vol. 433-435, pp. 1254–1257, 2013.

[2] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," *Electric Power Systems Research*, vol. 101, pp. 71–79, 2013.

[3] J. Wang, C. Zhang, Y. Huang, and C. Xin, "Attack robustness of cascading model with node weight," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 37–48, 2014.

[4] M. Ouyang, L. Zhao, Z. Pan, and L. Hong, "Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks," *Physica A: Statistical Mechanics and its Applications*, vol. 403, pp. 45–53, 2014.

[5] Y. Yang, Z. Li, Y. Chen, X. Zhang, and S. Wang, "Improving the robustness of complex networks with preserving community structure," *PLoS One*, vol. 10, no. 2, article e0116551, 2015.

[6] F. Tan, Y. Xia, and Z. Wei, "Robust-yet-fragile nature of interdependent networks," *Physical Review E*, vol. 91, no. 5, 2015.

[7] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 530–538, 2016.

[8] H.-P. Ren, J. Song, R. Yang, M. S. Baptista, and C. Grebogi, "Cascade failure analysis of power grid using new load distribution law and node removal rule," *Physica A: Statistical Mechanics and its Applications*, vol. 442, pp. 239–251, 2016.

[9] W. Fan, S. Huang, and S. Mei, "Invulnerability of power grids based on maximum flow theory," *Physica A: Statistical Mechanics and its Applications*, vol. 462, pp. 977–985, 2016.

[10] Y. Kornbluth, G. Barach, Y. Tuchman, B. Kadish, G. Cwilich, and S. V. Buldyrev, "Network overload due to massive attacks," *Physical Review E*, vol. 97, no. 5, 2018.

[11] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 200–210, 2017.

[12] M. Wang, Y. Xiang, and L. Wang, "Identification of critical contingencies using solution space pruning and intelligent search," *Electric Power Systems Research*, vol. 149, pp. 220–229, 2017.

[13] L. Shi, Q. C. Liu, J. L. Shao, and Y. Cheng, "Distributed localization in wireless sensor networks under denial-of-service attacks," *IEEE Control Systems Letters*, vol. 5, pp. 493–498, 2021.

[14] D. Silvestre, J. P. Hespanha, and D. Silvestre, "Resilient desynchronization for decentralized medium access control," *IEEE Control Systems Letters*, vol. 5, pp. 803–808, 2020.

[15] Y. Zheng, F. Liu, and Y.-W. Gong, "Robustness in weighted networks with cluster structure," *Mathematical Problems in Engineering*, vol. 2014, Article ID 292465, 8 pages, 2014.

[16] X. Liu, H. Peng, and J. Gao, "Vulnerability and controllability of networks of networks," *Chaos, Solitons& Fractals*, vol. 80, pp. 125–138, 2015.

[17] J. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," *Energies*, vol. 10, no. 1, p. 87, 2017.

[18] Y. Wang, G. Yan, and R. Zheng, "Vulnerability assessment of electrical cyber-physical systems against cyber attacks," *Applied Sciences*, vol. 8, no. 5, p. 768, 2018.

[19] J. Ma and Z. Ju, "Cascading failure model of scale-free networks for avoiding edge failure," *Peer-to-Peer Networking and Applications*, vol. 12, no. 6, pp. 1627–1637, 2019.

[20] M. I. Oozeer and S. Haykin, "Cognitive dynamic system for control and cyber-attack detection in smart grid," *IEEE Access*, vol. 7, pp. 78320–78335, 2019.

[21] A. E. Motter, T. Nishikawa, and Y.-C. Lai, "Range-based attack on links in scale-free networks: are long-range links responsible for the small-world phenomenon?," *Physical Review E*, vol. 66, no. 6, 2002.

[22] A. E. Motter, "Cascade Control and Defense in Complex Networks," *Physical Review Letters*, vol. 93, no. 9, 2004.

[23] M. Li, Y. Sun, H. Lu, S. Maharjan, and Z. Tian, "Deep reinforcement learning for partially observable data poisoning attack in crowdsensing systems," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6266–6278, 2020.

[24] C. Liu, H. Guo, Z. Li, X. Gao, and S. Li, "Coevolution of multigame resolves social dilemma in network population," *Applied Mathematics and Computation*, vol. 341, pp. 402–407, 2019.

[25] P. Zhu, X. Wang, S. Li, Y. Guo, and Z. Wang, "Investigation of epidemic spreading process on multiplex networks by incorporating fatal properties," *Applied Mathematics and Computation*, vol. 359, pp. 512–524, 2019.

[26] M. Zheng, S. Li, D. Lu, W. Wang, X. Wu, and D. Zhao, "Structural vulnerability of power grid under malicious node-based attacks," *Communications in Computer and Information Science*, vol. 1123, pp. 446–453, 2019.

[27] X. (. J.). du, M. Zhang, K. Nygard, S. Guizani, and H. H. Chen, "Self-healing sensor networks with distributed decision making," *International Journal of Sensor Networks*, vol. 2, no. 5/6, pp. 289–298, 2007.

[28] S. Li, D. Zhao, X. Wu, Z. Tian, A. Li, and Z. Wang, "Functional immunization of networks based on message passing," *Applied Mathematics and Computation*, vol. 366, article 124728, 2020.

[29] Z. Tian, C. Luo, J. Qiu, X. du, and M. Guizani, "A distributed deep learning system for web attack detection on edge devices," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1963–1971, 2020.

[30] H. Zhang, C. Zhai, G. Xiao, and T. C. Pan, "An optimal control approach to identifying the worst-case cascading failures in power systems," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 2, pp. 956–966, 2019.

[31] H. Zhang, C. Zhai, G. Xiao, and T. C. Pan, "Identifying critical risks of cascading failures in power systems," *IET Generation, Transmission & Distribution*, vol. 13, no. 12, pp. 2438–2445, 2019.

[32] H. Yang, S. Li, X. Wu, H. Lu, and W. Han, "A novel solutions for malicious code detection and family clustering based on machine learning," *IEEE Access*, vol. 7, no. 1, pp. 148853–148860, 2019.

[33] R. Yin, X. Yin, M. Cui, and Y. Xu, "Node importance evaluation method based on multi-attribute decision-making model in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, 14 pages, 2019.

[34] Z. Yi, X. Wu, and F. Li, "Ranking spreaders in complex networks based on the most influential neighbors," *Discrete Dynamics in Nature and Society*, vol. 2018, Article ID 3649079, 6 pages, 2018.

[35] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, 2020.

[36] X. Du, M. Rozenblit, and M. Shayman, "Implementation and performance analysis of SNMP on a TLS/TCP base," in *2001 IEEE/IFIP International Symposium on Integrated Network Management Proceedings. Integrated Network Management VII. Integrated Management Strategies for the New Millennium (Cat. No. 01EX470)*, pp. 453–466, Seattle, WA, USA, May 2001.

[37] Y. Li, S. Li, Y. Chen, P. He, X. Wu, and W. Han, "Electric power grid invulnerability under intentional edge-based attacks," in *Dependability in Sensor, Cloud, and Big Data Systems and Applications*, vol. 1123 of Communications in Computer and Information Science, , pp. 454–461, Springer, 2019.

[38] P. Zhu, X. Wang, D. Jia, Y. Guo, S. Li, and C. Chu, "Investigating the co-evolution of node reputation and edge-strategy in prisoner's dilemma game," *Applied Mathematics and Computation*, vol. 386, p. 125474, 2020.

[39] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3901–3909, 2020.

[40] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *2008 IEEE International Conference on Communications*, Beijing, China, 2008.

[41] L. Wu, X. Du, W. Wang, and B. Lin, "An out-of-band authentication scheme for Internet of Things using blockchain technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, Hawaii, USA, March 2018.

[42] X. Huang and X. Du, "Achieving big data privacy via hybrid cloud," in *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 512–517, Toronto, Ontario, Canada, May 2014.

[43] D. Zhao, L. Wang, Z. Wang, and G. Xiao, "Virus propagation and patch distribution in multiplex networks: modeling,

analysis and optimal allocation," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1755–1767, 2019.

[44] D. Zhao, G. Xiao, Z. Wang, L. Wang, and L. Xu, "Minimum Dominating set of multiplex networks: definition, application and identification," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–15, 2020.

[45] S. D. Li, D. N. Lu, X. B. Wu, W. Han, and D. Zhao, "Enhancing the power grid robustness against cascading failures under node-based attacks," *Modern Physics Letters B*, vol. 35, no. 9, article 2150152, 2021.

[46] D. Zhao, S. Yang, X. Han, S. Zhang, and Z. Wang, "Dismantling and vertex cover of network through message passing," *IEEE Transactions on Circuits & Systems II-Express Briefs*, vol. 67, no. 11, pp. 2732–2736, 2020.

[47] K. Huang, Z. Wang, and M. Jusup, "Incorporating latent constraints to enhance inference of network structure," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 466–475, 2020.

[48] W. B. Du, X. L. Zhou, M. Jusup, and Z. Wang, "Physics of transportation: Towards optimal capacity using the multilayer network framework," *Scientific Reports*, vol. 6, no. 1, p. 19059, 2016.

[49] S. D. Li, L. Y. Jiang, X. B. Wu, W. H. Han, D. Zhao, and Z. Wang, "A weighted network community detection algorithm based on deep learning," *Applied Mathematics and Computation*, vol. 401, no. 7, Article ID 126012, 2021.