Hindawi
Security and Communication Networks
Volume 2018, Article ID 6254876, 7 pages
https://doi.org/10.1155/2018/6254876

Research Article

A Novel Load Capacity Model with a Tunable Proportion of Load Redistribution against Cascading Failures

Zhen-Hao Zhang,[1] **Yurong Song**,[2] **Lingling Xia**,[3] **Yin-Wei Li**,[1] **Liang Zhang**,[3] **and Guo-Ping Jiang**[2]

[1]*School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, China*
[2]*School of Automation, Nanjing University of Posts and Telecommunications, Nanjing, China*
[3]*Department of Computer Information and Cyber Security, Jiangsu Police Institute, Nanjing, China*

Correspondence should be addressed to Yurong Song; songyr@njupt.edu.cn

Received 10 April 2018; Accepted 13 May 2018; Published 7 June 2018

Academic Editor: Lu-Xing Yang

Defence against cascading failures is of great theoretical and practical significance. A novel load capacity model with a tunable proportion is proposed. We take degree and clustering coefficient into account to redistribute the loads of broken nodes. The redistribution is local, where the loads of broken nodes are allocated to their nearest neighbours. Our model has been applied on artificial networks as well as two real networks. Simulation results show that networks get more vulnerable and sensitive to intentional attacks along with the decrease of average degree. In addition, the critical threshold from collapse to intact states is affected by the tunable parameter. We can adjust the tunable parameter to get the optimal critical threshold and make the systems more robust against cascading failures.

1. Introduction

Cascading failures are ubiquitous phenomena in real life and often occur in many networks such as power grids, Internet, and transportation systems. In 2003, the largest power outage took place in North America, which just resulted from a broken-down power plant in Ohio [1]. Traffic paralysis of south China caused by storm in 2008 and Internet congestions [2] are typical examples of cascading failures as well. These incidents seriously affect people's life and threaten the stability of society. Therefore, more and more researchers come to investigate the issue from different perspectives.

There are several kinds of traditional models on researching cascading failures, respectively, known as the load capacity model [3], the double value impact model [4], the optimal power flow approach model [5], the sand pile model [6], the coupled map lattice model [7], and so on. Load capacity model [3] (ML model) proposed by Motter and Lai shows that, for such networks, where loads can redistribute to other nodes, intentional attacks can lead to a cascade of overload failures, which can in turn cause the entire or a substantial part of the network to collapse. To be more practical and reduce the collapse scale, scholars have put forward many cascading failures model based on ML model. Zhou et al. [8] deem that degrees of nodes in networks can to some extent reflect the processing ability and let nodes with both higher loads and larger degrees acquire more extra capacities. Sun et al. [9] propose a new matching model of capacity by developing a profit function to defence cascading failures on artificially created scale-free networks and the real network structure of the North American power grid. Fang et al. [10] investigate the cascading failures in directed complex networks and make a load redistribution rule of average allocation. Chen et al. [11] propose a nearest neighbours load redistribution model, where load of broken nodes is allocated to nearest neighbours according to their degrees. Wang et al. [12] propose a local load redistribution model. They adopt the initial load of node to be $L_j = \beta k_j^\alpha$ and the load redistribution proportion to be $P_{ji} = \beta k_i^\alpha / \sum_{n\in\Omega_j} \beta k_n^\alpha$, where

Ω_j denotes the neighbors set of broken node j. Wang et al. [13] consider that not all overload nodes will be removed from networks due to some effective measures to protect them and propose a new model with a breakdown probability. Also, they propose a new method considering neighbours' degrees for initiating loads, where the initial load of a node j is $L_j = (k_j \times (\sum_{m\in\Omega_j} k_m))^\alpha$ and the load redistribution proportion is $P_{ji} = (k_i \times (\sum_{m\in\Omega_i} k_m))^\alpha / \sum_{n\in\Omega_j}(k_n \times (\sum_{f\in\Omega_n} k_f))^\alpha$. Peng et al. [14] propose a renewed cascading failures model. In this model, the initial loads are defined as a nonlinear function of the generalized betweenness which is $L_j = (1+q)B_j^\alpha$. The redistribution strategy is $P_{ji} = B_i^\alpha / \sum_{n\in\Omega_j} B_n^\alpha$. The numeric value of betweenness centrality is proportional to that of degree with power exponent [2, 15, 16], so the definition of initial loads is substantially a nonlinear function of degree. Generally, we can conclude that initial loads are all defined as a function of degree. And the load redistribution proportion can be seen as a function of initial loads, where $P_{ji} = f(L_i)/\sum_{n\in\Omega_j} f(L_n)$ and $f(L_i) = L_i$. Actually, the load redistribution proportion [8–14] depends on the initial loads that reflect the load processing ability to some extent. Duan et al. [17, 18] explore the critical thresholds of scale-free networks against cascading failures and spatiotemporal tolerance after a fraction of nodes attacked with a tunable load redistribution model that can tune the load redistribution range and heterogeneity of the broken nodes. The initial load is assumed as $L_j = \rho k_j^\tau$. The redistribution strategy is global. They make l_{ji} denote the distance between broken node j and intact node i. The redistribution proportion is $P_{ji} = l_{ji}^{-\theta} k_i^\beta / \sum_{n\in\Omega_j} l_{jn}^{-\theta} k_n^\beta$. Likewise, the initial loads are defined as a function of degree, and the redistribution proportion can be concluded as a function of $P_{ji} = y(l_{ji}) f(L_i)/\sum_{n\in\Omega_j} y(l_{jn}) f(L_n)$, where $f(*)$ is a function of initial loads with a power exponent β/τ. And $y(*)$ is a function of distance, where $y(x) = x^{-\theta}$. Extending the redistribution range can improve the system robustness against cascading failures undoubtedly. However, this strategy is sometimes unpractical. Long distance load redistribution strategy costs too much in practical application and has high time complexity in computation. Recently, some scholars [19] pay attention to the application of load capacity model in information warfare and propose a cascading failures model for command and control networks with hierarchy structure.

The above scholars are devoted to improving robustness of networks from various points of view and have considered degree, betweenness, path length, and so on. However, scholars have not adopted clustering coefficient [20] into modelling cascading failures. Some researchers have recently investigated the effect of clustering coefficient [20] in the propagation of cascading failures. Zheng et al. [21] find that scale-free networks with larger clustering coefficient are sensitive and are prone to suffering from cascading failures. Ding et al. [22] explore the cascading failures in interconnected weighted networks and draw a conclusion that networks with smaller mean clustering coefficient have stronger ability to resist cascading failures. Eisenberg et al. [23] analyze the topology and resilience of the South Korea power grid. They discover that the power grid has a low efficiency and a high clustering coefficient, implying that highly clustered structure does not necessarily guarantee a functional efficiency of a network. Based on the error and attack tolerance analysis evaluated with efficiency, they find that the South Korea power grid is vulnerable to random or degree-based attacks. Likewise, Monfared et al. [24] investigate the structural properties of power transmission of Iran. The clustering coefficient displayed by Iranian power grid is much larger than that of corresponding random networks. Similarly, after studying the largest connected component of the network, they conclude that the power grid is vulnerable against cascading failures.

In this paper, we propose a novel load capacity model by considering clustering. The load redistribution strategy in our model is a kind of nearest neighbour redistribution methods, where the broken nodes allocate loads to their one-leap neighbours. We introduce a tunable parameter α to govern the strength of load redistribution proportion. By taking the robustness quantified as the critical threshold β_m, where a phase transition takes place from collapse to intact states, we investigate the relation between α and β_m on ER random graph networks [25], BA scale-free networks [26], WS small-world networks [20], North American power grid, and autonomous systems (AS) subnet topology. The simulation of the intentional attacks on a single node shows the nonmonotonic and nonlinear effect between the two parameters. We can control parameter α to adjust the proportion of load redistribution, thus reaching the optimal robustness of networks. Our simulations also suggest that networks with large average degree may be robust under the intentional attacks in our model, and highly clustered networks with the same degree distribution cannot guarantee the robustness. By contrast with another nearest neighbours load redistribution model [14], we verify the better performance of our model. Our model may further the research of controlling and defence against cascading failures in complex networks, which is constructive in designing infrastructure networks, such as power grid, logistics network systems, and communication networks.

2. Cascading Failures Model

For simplicity, we assume that the network is at the static state initially where the initial load of each node is less than its capacity and there are no broken nodes. After removal of one single node caused by intentional attacks, the balance among nodes will be changed. Therefore, the loads of the broken nodes will be redistributed to other nodes. In this paper, these nodes are one-leap neighbours of broken nodes. If some of these nodes do not have enough capacity to handle the extra load from the broken nodes, they will break down afterwards. In turn, these newly generated broken nodes will continue to allocate loads to their normal neighbours, triggering a collapse of partial nodes or even the whole network. This is the process of cascading failures under the frame of load capacity model [3].

Table 1: Relevant parameters of networks. N and M denote the numbers of nodes and links, respectively. $< k >$ denotes the average degree.

Name	N	M	$< k >$	Name	N	M	$< k >$
BA1	1000	2000	4	ER4	1000	5000	10
BA2	1000	3000	6	WS1	1000	2000	4
BA3	1000	4000	8	WS2	1000	3000	6
BA4	1000	5000	10	WS3	1000	4000	8
ER1	1000	2000	4	WS4	1000	5000	10
ER2	1000	3000	6	Power grid	4941	6594	2.67
ER3	1000	4000	8	AS	4158	13422	6.456

Here, we let the initial load of node j be a function of degree. The definition of the initial load of node j is as follows:

$$L_j^0 = \rho \left[k_j \times \left(\sum_{m \in \tau_j} k_m \right) \right], \quad j = 1, 2, \ldots N. \tag{1}$$

N is the number of nodes in the network. k_j is the degree of node j. ρ is a constant parameter that characters the strength of initial loads. τ_j is the set of node j's neighbours. The capacity of a node is the maximal load that the node can manage under the normal operation. The definition is as follows:

$$C_j = (1 + \beta) L_j^0. \tag{2}$$

β ($\beta \geq 0$) is the tolerance parameter. Generally, the tolerance parameter reveals the node's ability of defence against cascading failures. Evidently, the larger it is, the more robust the network is. However, improving the ability of tolerance at all costs is not reasonable. Here, we aim to seek the minimal β that we define as critical threshold β_m to get a balance between costs and robustness. Undoubtedly, reducing the critical threshold as much as possible is our ambition.

Considering that clustering coefficient plays a negative role in the propagation of cascading failures [21–24] and initial loads reflect the load processing ability to some extent [8–14, 17, 18], we make our redistribution strategy as follows:

$$P_{ji} = \frac{\left(g(cc_i) f\left(L_i^0\right) \right)^\alpha}{\sum_{n \in \Omega_j} \left(g(cc_n) f\left(L_n^0\right) \right)^\alpha}. \tag{3}$$

$$L_i \longleftarrow L_i + L_j \times P_{ji}. \tag{4}$$

The term cc_i denotes the clustering coefficient [20] of node i. The definition of clustering coefficient [20] of node i is as follows. E_i denotes the number of links among node i's neighbours. k_i is the degree of node i.

$$cc_i = \frac{2E_i}{k_i (k_i - 1)} \tag{5}$$

Function $f(*)$ is proportional to initial loads and in this paper we adopt the function $f(L_i^0) = L_i^0$ [12–14]. The function $g(cc_i)$ characters the negative effect of clustering coefficient [21–24] and is a decreasing function of clustering coefficient. When a node is broken, the neighbours will be redistributed the loads of the broken node. If the adjacent node has a higher clustering coefficient, it will be redistributed fewer loads from the broken node. We here adopt a simple exponential function, namely, $g(cc_i) = e^{-cc_i}$, a decreasing function of clustering coefficient. Actually, we can apply a more complicated form of $g(cc_i)$. However, a more complicated form of $g(cc_i)$ adds little value to characterize the effect of clustering coefficient but increases the computing complexity. In reality, the results and perspectives of our research are not limited by a specific function of clustering coefficient. Ω_j denotes the set of intact neighbours of node j. Here, node i is an element of the set. When node j breaks down, it will allocate its loads to intact neighbours at the certain proportion of P_{ji}. After getting the extra loads of node j, node i will break down if the updated loads exceed its capacity ($L_i > C_i$). In turn, node i will allocate its loads to intact neighbours, just as (3) and (4). The process will stop until the whole network breaks down or there are no newly generated broken nodes. The parameter α ($\alpha \geq 0$) is tunable. By controlling parameter α, we can adjust the proportion of load redistribution to reach the optimal robustness of networks at the lowest cost.

3. Simulations

In this section, we first investigate the relation between α and β_m on ER random graph networks [25], BA scale-free networks [26], WS small-world networks [20], North American power grid, and autonomous systems (AS) subnet topology. The average degrees of artificial networks are, respectively, four, six, eight, and ten. Fifty networks of the same average degree are generated, and the simulations are implemented in each network. Average results are shown in this paper. Relevant parameters of networks are shown in Table 1.

As triggered by the intentional attacks on a single node, cascading failures may probably spread to a certain scale. We calculate the proportion (see (6)) of broken nodes in the whole network to characterize the scale of cascading failures.

$$P = \frac{n_b}{N} \tag{6}$$

N denotes the number of nodes. n_b denotes the number of broken nodes. There is no doubt that if the tolerance parameter β is equal to zero, the proportion P is always equal to one. In this paper, we intend to attack the nodes of the largest degree and the node of the largest initial load. In

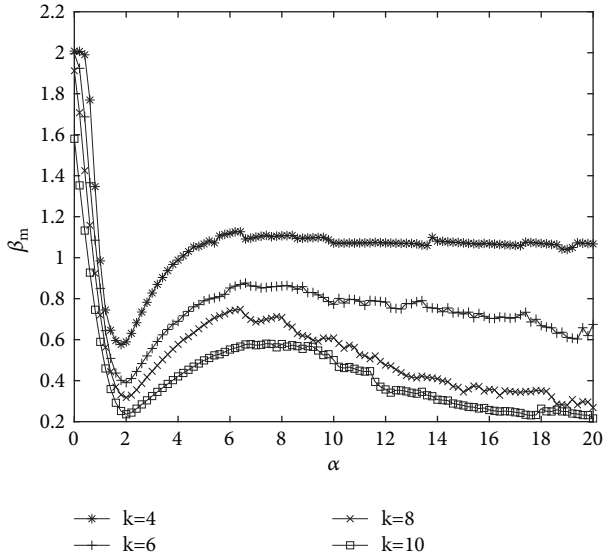

Figure 1: The relation between α and β_m in BA networks.

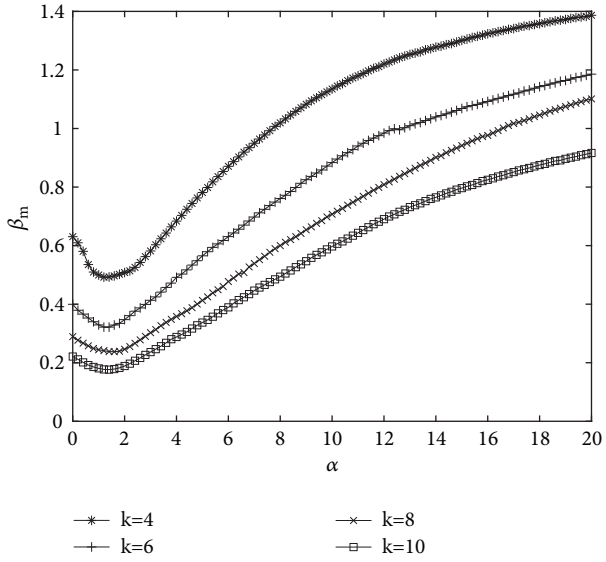

Figure 2: The relation between α and β_m in WS networks.

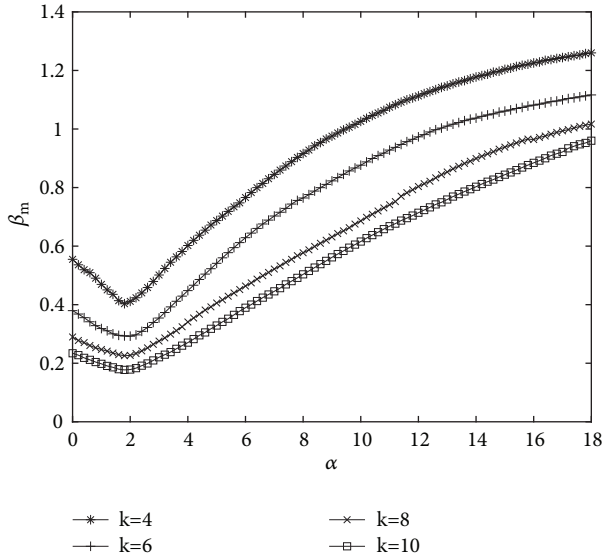

Figure 3: The relation between α and β_m in ER networks.

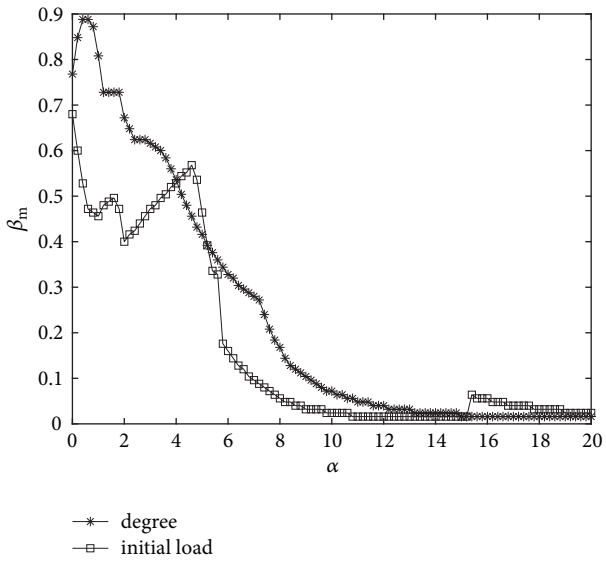

Figure 4: The relation between α and β_m in North American power grid after attacking the nodes of the largest degree and initial loads.

North American power grid, nodes of the largest degree and initial load are, respectively, No. 2554 and No. 4346. In other networks, the node of the largest degree is the same as the node of the largest initial load.

We then attack the above nodes in each network, and the relations between α and β_m are shown in Figures 1–5.

In Figures 1–5, each α corresponds to a critical threshold β_m. It is well known that the larger tolerance parameter β costs more. Therefore, we aim to seek the minimal tolerance parameter under the condition that the network is robust. We can get that optima for four BA networks are around $\alpha = 2$, where the minimum β_m exists. From Figure 1, we can also see that curves tend to be stable when $\alpha > 14$. This is easy to explain. When α is large enough, there is no numerically striking difference among the proportions of redistribution with the change of α, so the curves become stable. When scrutinizing the simulations of BA networks, we discover that β_m (s) are getting smaller with the increase of average degree, indicating that the network is getting robust in our model. If the average degree increases, the scope of load redistribution is actually extended. This situation reduces the probability that neighbours of broken nodes continue to get broken. Hence, the network gets robust with the increase of average degree in our model. When α approaches zero, we can see that β_m (s) of BA networks are evidently larger than those of WS and ER networks. This phenomenon is caused by the heterogeneity of scale-free networks. In BA networks, the heterogeneity of degree distribution makes the initial loads of some nodes large apparently. Therefore, the

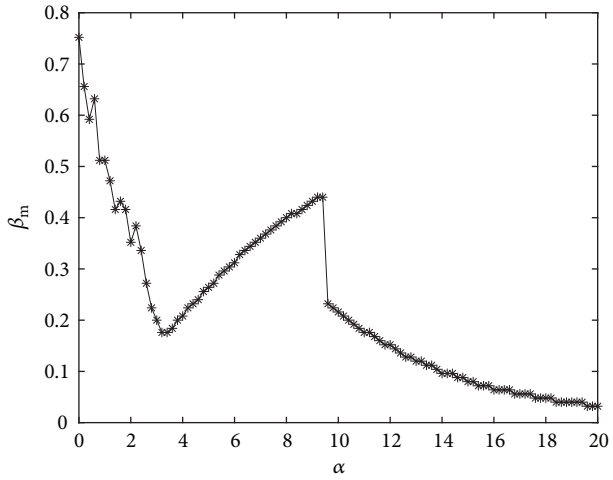

Figure 5: The relation between α and β_m in AS network.

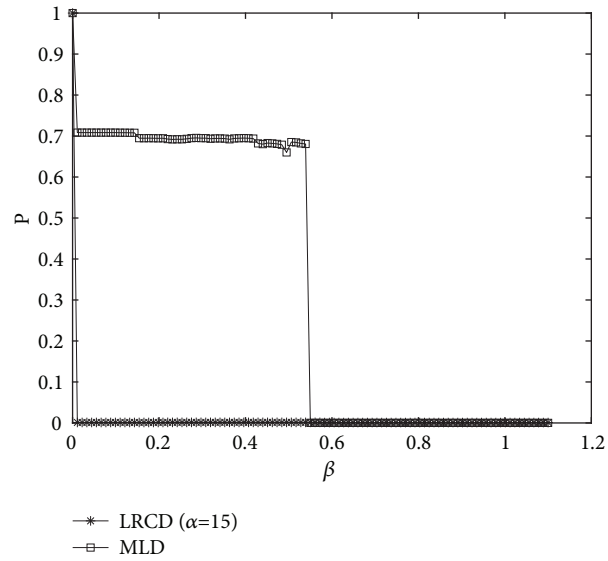

Figure 6: Attacking power grid based on the largest degree and initial load. LRCD (load redistribution based on clustering coefficient and degree) denotes our model. MLD denotes the nearest neighbours load redistribution model [14].

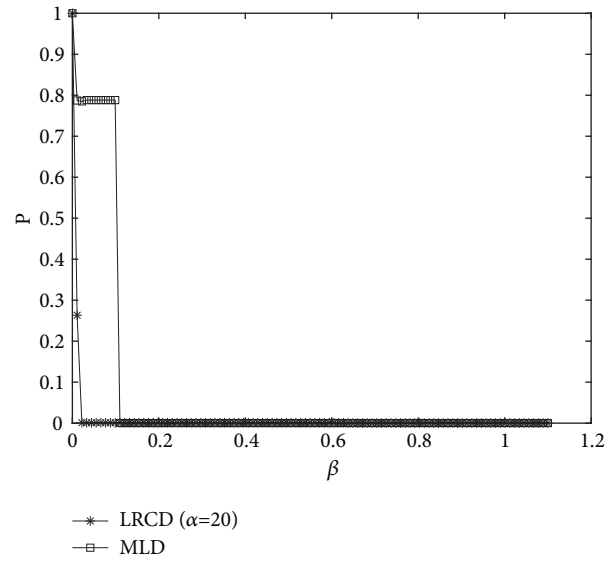

Figure 7: Attacking AS network. LRCD (load redistribution based on clustering coefficient and degree) denotes our model. MLD denotes the nearest neighbours load redistribution model [14].

minimal tolerance parameter β_m ought to be large enough to guarantee the robustness of networks when nodes of the largest degree and the largest initial load are attacked. Compared with critical thresholds of WS and ER networks with the same average degree, β_m of BA networks is smaller at the stable state. Similarly, the heterogeneity of scale-free networks contributes to the phenomenon. The broken nodes of BA networks have more neighbours than those of WS and ER networks, which means that there are more nodes to be redistributed loads from broken nodes. Therefore, the minimal tolerance parameter β_m (s) can be smaller.

The optima for WS networks and ER networks are, respectively, around $\alpha = 1.5$ and $\alpha = 2$. We may also discover a phenomenon that β_m (s) get smaller along with the increase of average degree, indicating that the WS and ER networks are getting robust in our model. Remarkably, the degree distributions of WS and ER networks are both Poisson distribution, and β_m (s) denoting the gentle pieces of curves of WS networks are not strikingly different from those of corresponding ER networks. Even β_m (s) of WS networks are sometimes larger than those of ER networks. Although WS network has the character of high clustering, it cannot guarantee the robustness of networks with the same degree distribution. This finding is coincident with the former research [21–24].

Figures 4-5 indicate that two curves of power grid and that of AS network topology do not have remarkable regularities but all present the declining trends. The optima are around $\alpha = 15$ and $\alpha = 20$, respectively. Figures 4-5 show the simulations on the real networks. Real networks are different from artificial networks, and their statistical characters are sometimes not technically subject to the corresponding network models. Therefore, the simulation curves are sometimes not smooth and sudden change may appear.

The above studies on the relation between α and β_m are from the macro perspective. To verify the better performance of our model, we will next concentrate on the relation between P and β to investigate the propagation process of cascading failures from the microscopic level. We compare our model with another nearest neighbour load redistribution model [14] on American power grid and autonomous systems (AS), using optimal α corresponding to minimal β_m. The simulations are shown in Figures 6-7.

From the simulations, we can see that β_m of our model is smaller, which means that our model decreases the critical threshold and makes it easier to acquire the robustness of networks. Dramatically, when applying our model into real networks, such as North American power grid and

autonomous systems, shown in Figures 6-7, we find that the phase transition from collapse to intact states takes place more quickly. Therefore, our model is more practical in applications and may inspire researchers to design more robust infrastructure systems against cascading failures when faced with the intentional attacks.

4. Conclusions

Nowadays, defence against cascading failures is a vital research, which contributes to operation of power grid, information security, efficiency of logistics networks, and so on. A novel load capacity model by considering clustering is proposed in this paper, aiming to get a smaller critical threshold and improve the robustness of networks. With the help of Monte Carlo simulations, the effectiveness of our model can be verified through comparison with a famous nearest neighbour load redistribution model [14]. The simulations suggest that our model is more practical in applications and may inspire researchers to design more robust infrastructure systems against cascading failures.

Data Availability

The North American power grid and autonomous systems (AS) subnet topology data used to support the findings of this study have been deposited in the website http://snap.stanford.edu/. ER random graph networks, BA scale-free networks, and WS small-world networks used to support the findings of this study are generated by the methods cited in [16, 24, 25].

Conflicts of Interest

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

Acknowledgments

This research has been supported by the National Natural Science Foundation of China (Grants [61672298], [61373136], and [61374180]), the National Social Science Foundation of China (Grant [13BTQ046]), and the High-Level Introduction of Talent Scientific Research Start-up Fund of Jiangsu Police Institute (Grant [JSPI17GKZL403]).

References

[1] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 69, no. 2, Article ID 025103, 2004.

[2] K.-I. Goh, B. Kahng, and D. Kim, "Universal behavior of load distribution in scale-free networks," *Physical Review Letters*, vol. 87, no. 27, Article ID 278701, 2001.

[3] M. E. J. Newman, S. Forrest, and J. Balthrop, "Email networks and the spread of computer viruses," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 66, no. 3, Article ID 035101, 4 pages, 2002.

[4] D. J. Watts, "A simple model of global cascades on random networks," *Proceedings of the National Acadamy of Sciences of the United States of America*, vol. 99, no. 9, pp. 5766–5771, 2002.

[5] I. Dobson, J. Chen, J. S. Thorp, B. A. Carreras, and D. E. Newman, "Examining criticality of blackouts in power system models with cascading events," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS '02)*, vol. 2, p. 63, January 2002.

[6] K. Goh, D. Lee, B. Kahng, and D. Kim, "Sandpile on scale-free networks," *Physical Review Letters*, vol. 91, no. 14, Article ID 148701, 2003.

[7] X. F. Wang and J. Xu, "Cascading failures in coupled map lattices," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 70, no. 5, Article ID 056113, 2004.

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

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

[10] X. Fang, Q. Yang, and W. Yan, "Modeling and analysis of cascading failure in directed complex networks," *Safety Science*, vol. 65, pp. 1–9, 2014.

[11] W. X. Wang and G. Chen, "Universal robustness characteristic of weighted networks against cascading failure," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 77, no. 2, Article ID 026101, 2008.

[12] J.-W. Wang and L.-L. Rong, "Cascading failures on complex networks based on the local preferential redistribution rule of the load," *Acta Physica Sinica*, vol. 58, no. 6, pp. 3714–3721, 2009.

[13] J.-W. Wang and L.-L. Rong, "A model for cascading failures in scale-free networks with a breakdown probability," *Physica A: Statistical Mechanics and Its Applications*, vol. 388, no. 7, pp. 1289–1298, 2009.

[14] X. Z. Peng, H. Yao, J. Du, Z. Wang, and C. Ding, "Invulnerability of scale-free network against critical node failures based on a renewed cascading failure model," *Physica A: Statistical Mechanics and Its Applications*, vol. 421, pp. 69–77, 2015.

[15] K. I. Goh, B. Kahng, and D. Kim, "Packet transport and load distribution in scale-free network models," *Physica A: Statistical Mechanics & Its Applications*, vol. 318, no. 1-2, pp. 72–79, 2003.

[16] M. Barthélemy, "Betweenness centrality in large complex networks," *The European Physical Journal B*, vol. 38, no. 2, pp. 163–168, 2004.

[17] D.-L. Duan, X.-D. Ling, X.-Y. Wu, D.-H. Ouyang, and B. Zhong, "Critical thresholds for scale-free networks against cascading failures," *Physica A: Statistical Mechanics and Its Applications*, vol. 416, pp. 252–258, 2014.

[18] C. C. Lv, S. B. Si, and D. L. Duan, "Dynamical robustness of networks against multi-node attacked," *Physica A: Statistical Mechanics & Its Applications*, vol. 471, pp. 837–844, 2017.

[19] X. Gao, D. Zhang, K. Li, and B. Chen, "A cascading failure model for command and control networks with hierarchy structure," *Security and Communication Networks*, vol. 2018, Article ID 6063837, 14 pages, 2018.

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

[21] J.-F. Zheng, Z.-Y. Gao, and X.-M. Zhao, "Clustering and congestion effects on cascading failures of scale-free networks,"

Europhysics Letters. EPL, vol. 79, no. 5, Article ID 58002, 5 pages, 2007.

[22] C. Ding, H. Yao, J. Du, X. Peng, Z. Wang, and J. Zhao, "Cascading failure in interconnected weighted networks based on the state of link," *International Journal of Modern Physics C*, vol. 28, no. 3, 2017.

[23] D. H. Kim, D. A. Eisenberg, Y. H. Chun, and J. Park, "Network topology and resilience analysis of South Korean power grid," *Physica A: Statistical Mechanics & Its Applications*, vol. 465, pp. 13–24, 2017.

[24] M. A. S. Monfared, M. Jalili, and Z. Alipour, "Topology and vulnerability of the iranian power grid," *Physica A: Statistical Mechanics and Its Applications*, vol. 406, pp. 24–33, 2014.

[25] P. Erdös and A. Rényi, "On the evolution of random graphs," *Publication of the Mathematical Institute of the Hungarian Academy Ofences*, vol. 38, no. 1, pp. 17–61, 2012.

[26] A.-L. Barabasi and R. Albert, "Emergence of scaling in random networks," *American Association for the Advancement of Science: Science*, vol. 286, no. 5439, pp. 509–512, 1999.