Safety Science 49 (2011) 807–812

Contents lists available at ScienceDirect

Safety Science

journal homepage: www.elsevier.com/locate/ssci

Robustness of the western United States power grid under edge attack strategies due to cascading failures

Jian-Wei Wang [a,b,*], Li-Li Rong [b]

[a] School of Business Administration, Northeastern University, Shenyang 110004, PR China
[b] Institute of Systems Engineering, Dalian University of Technology, Dalian 116024, PR China

ARTICLE INFO

Article history:
Received 31 August 2009
Received in revised form 26 August 2010
Accepted 18 October 2010
Available online 9 March 2011

Keywords:
Cascading failure
Attack strategy
Load
Critical threshold
Power grid

ABSTRACT

Power systems are the basic support of modern infrastructures and protecting them from random failures or intentional attacks is an active topic of research in safety science. This paper is motivated by the following two related problems about cascading failures on power grids: efficient edge attack strategies and lower cost protections on edges. Applying the recent cascading model by adopting a local load redistribution rule, where the initial load of an edge ij is $(k_i k_j)^\theta$ with k_i and k_j being the degrees of the nodes connected by the edge, we investigate the performance of the power grid of the western United States subject to three intentional attacks. Simulation results show that the effects of different attacks for the network robustness against cascading failures have close relations with the tunable parameter θ. Particularly, the attack on the edges with the lower load in the case of $\theta < 1.4$ can result in larger cascading failures than the one on the edges with the higher load. In addition, compared with the other two attacks, a new attack, i.e., removing the edges with the smallest proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge, usually are prone to trigger cascading failures over the US power grid. Our findings will be not only helpful to protect the key edges selected effectively to avoid cascading-failure-induced disasters, but also useful in the design of high-robustness and low-cost infrastructure networks.

1. Introduction

The problem of stability of infrastructure networks (Tomas, 2007; Koos, 2008; Leonardo and Srivishnu, 2009), especially in the context of the power grid, has recently attracted a great deal of attention in recent years. Power systems play, together with transportation networks and the Internet, indispensable roles in modern society. However, for the past decade, many countries have suffered from serious blackouts and the frequency of large-scale blackouts all over the world has not decreased, in spite of technological progress and huge investments in system reliability and security. For instance, the Western North American blackouts in July and August 1996, and the major power blackout on August 14, 2003, which lasted up to 4 days in various parts of the eastern USA, not only caused traffic congestion, but also affected many other critical infrastructures. These severe incidents have been attributed to cascading behaviors, i.e., one typical feature of blackouts where even though intentional attacks and random failures emerge very locally, the entire network can be largely affected, even resulting in global collapse. Therefore, a great effort is necessary to investigate the emergent behaviors of cascading failures and to further study the control and defense of cascading failures.

Taking into account the intrinsic dynamics of the load of physical quantities in the network, a number of important aspects of cascading failures have been discussed in the literature and many valuable results have been found, including the load model of cascading failures (Crucitti et al., 2004; Wang and Chen, 2008; Wang and Xu, 2004; Wang and Rong, 2009; Goh et al., 2001; Sandro et al., 2008), avalanche size distributions (Moreno et al., 2002; Goh et al., 2003), the cascade control and defense strategy (Simonsen et al., 2008; Motter, 2004; Ash and Newth, 2007), the performance of the network under cascade-based attacks (Motter and Lai, 2002; Wang et al., 2008; Wang and Rong, 2008; Zhao et al., 2004; Zhao et al., 2005; Ricard et al., 2008), cascading failures in real networks (Albert et al., 2004; Dusko et al., 2006; Wu et al., 2007,), and so on. The vital importance of the power systems to real life motivates the study on the salient features of cascading failures. Albert et al. (2004) studied the power grid from a network perspective and determined its ability to transfer power between generators and consumers when certain nodes are disrupted. Leonardo and Srivishnu (2009) studied the effect of cascading failures in the risk and reliability assessment of complex infrastructure systems. Motter and Lai (2002) proposed a load model and demonstrated

* Corresponding author at: School of Business Administration, Northeastern University, Shenyang 110004, PR China. Tel.: +86 024 83672631.
E-mail address: wdut@yahoo.cn (J.-W. Wang).

0925-7535/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2010.10.003

that the heterogeneity of the western US power transmission grid made them particularly vulnerable to attacks in that a large-scale cascade might be triggered by disabling a single key node. Ricard et al. (2008) explored the fragility of the European power grid under the effect of selective node removal. In all cited studies above, the most existing works focused only on the cascading failures induced by the node overload breakdown rather than by the edge overload failure. However, we believe that cascading failures on edges are as important for the network security as those on nodes, even more important owing to some flow or load generally transmitted by the edges of networks, and therefore deserve a careful investigation.

In view of the importance of the study of attacks on real-life networks, which can be used either for protection in many infrastructure networks, e.g., in an electrical power grid, or for destruction in the spread of rumors and the control of epidemic diseases, the aim of this paper is to investigate the roles of different edges in the cascading propagation on real-life networks. Identifying the most important edges, breaking of which would make the whole network malfunction, one can effectively protect the network to avoid cascading failures and build attack-robust networks. Generally speaking, the edges with the highest load play the most important roles, however, is this really true? In view of this, applying a recently cascading load model proposed by Wang and Chen (2008) in which a new strategy of the load local preferential redistribution rule is put forward to reflect real-life networks, we compare the effects of and three intentional attacks for the network robustness against cascading failures on the US power grid. Considering the effect of the attacked edge for its connecting edges, we proposed a new attack strategy, namely, the attack on the edge with the lowest average capacity of its connecting edges. By numerical simulations, we obtain the relation between the most efficient attack strategies and the tunable parameter in the cascading model. Our findings may be useful in protecting the most importance edges to avoid cascading-failure-induced disasters on the US power grid.

2. The edge load model

Large-scale blackouts in most cases are usually due to the concurrent malfunction of a large number of transmission lines often triggered by an initial disturbance or event. When a power line fails, the load it carried before the fault will be shifted to the neighboring lines. If the malfunction line has a relatively small load, its failure may not bring about the subsequent overload failures. However, when the load at a line is relatively large, its removal is likely to affect significantly load at other lines and can cause a cascade of failures with consequences on the whole electric system. Therefore, the main purpose of our study is to investigate the effects of the different lines to the network robustness against cascading failures and to identify the key line being prone to trigger universal cascading failures.

Our study on attack strategies is based on a recently cascading load model originally proposed in Wang and Chen (2008), and we briefly summarize this model first. Wang and Chen assume the initial load of an edge ij to $(k_i k_j)^\theta$, θ is a adjustable parameter which controls the strength of the initial load of the edge, and k_i and k_j are the degrees of nodes i and j, respectively. This assumption is supported by empirical evidence of real network (Wu et al., 2008; Sergey et al., 2010). Moreover, Holme et al. (2002) shows that the betweenness[1] of an edge has positive correlation with the product form of node degrees at both ends of the edge. In this sense, their assumption on the initial load of an edge is in accordance with the previous load-based model but has practical convenience. The load along the broken edge ij will be redistributed to the neighboring edges connecting to the ends of ij (see Fig. 1, Wang and Chen, 2008). The additional load ΔF_{im} received by edge im is proportional to its initial load, i.e., $\Delta F_{im} = F_{ij} w_{im} / \left(\sum_{a \in \Gamma_i} w_{ia} + \sum_{b \in \Gamma_j} w_{jb} \right)$, where Γ_i and Γ_j are the sets of neighboring nodes of i and j, respectively. If edge ij does not receive additional load before being broken, $F_{ij} = w_{ij}$. Considering that the edge capacity on real-life networks, i.e., the maximum load that the edge can transmit, is generally limited by cost, it is natural to assume that the capacity C_{ij} of an edge ij is proportional to its initial load L_{ij}, i.e., Tw_{im}, where the constant $T > 1$ is a threshold parameter. If $F_{im} + \Delta F_{im} > Tw_{im}$, then im will be broken and induce further redistribution of load $F_{im} + \Delta F_{im}$ and potentially further edge breaking.

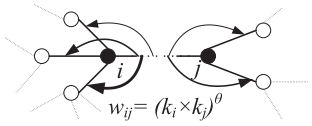

Fig. 1. Illustration of the load local preferential redistribution triggered by an edge-cut-based attack. Edge ij is broken and the load along it is redistributed to its neighboring edges. Among these neighbor edges, the one with the higher load will receive the higher extra load from the broken edge (Wang and Chen, 2008).

3. Analysis of three attack strategies

To investigate the roles of the different edges on the cascading propagation, we propose two special attack strategies. Generally speaking, the removal of the edge with the highest load can result in larger cascading failures than that of the edge with the lowest load, however, is this really true? Motivated by that question and considering the effect of the removal of a single edge for its neighboring edges, we analyze the local characteristics of a breakdown edge (see Figs. 2 and 3 for illustrations).

(1) Attack on the edges with the lowest load (LL). By studying the different attack strategies, we aim at answering the question that the protection of what edges can more efficiently control the cascading propagation. In the original study of the attack vulnerability of complex networks, only the attack strategies on the nodes or the edges with the highest load have been considered. Therefore, a natural question is that why we propose this attack strategy. In fact, in Wang et al. (2008) and Wang and Rong (2008, 2009) we have investigated the effects of the nodes with the lowest load for the network robustness against cascading failures and found that the nodes with the lowest load also played vital roles in the cascading propagation. Inspired by the previous studies, in Fig. 2 we analyze the effect of the edge removal for its neighboring edges. As can been seen from Fig. 2, by comparing the value of the capacity parameter T we find that the malfunction of the edge with the lower load is easier to cause overloading of the neighboring edges of the failed edge than that of the edge with the higher load. In view of this, the detailed investigation to this attack strategy can also be ignored. In this attack strategy, we first calculate the load on each edge and then continually select the edges in the ascending order of their load (if some edges happen to have the same lowest load, we randomly choose one of them).

[1] The betweenness of an edge can be obtained by counting the number of geodesics going it. More precisely, the betweenness b_{ij} of an edge ij, sometimes referred to also as load, is defined as: $b_{ij} = \sum_{m,n \in N, m \neq n} n_{mn}(ij)/n_{mn}$, where n_{mn} is the number of shortest paths connecting m and n, while $n_{mn}(ij)$ is the number of shortest paths connecting m and n and passing through ij.

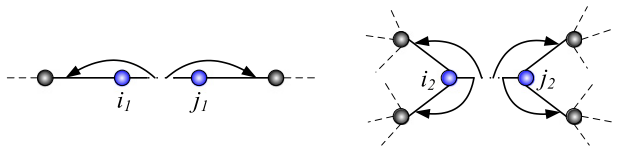

Fig. 2. Comparison of the effects of the malfunctions of the edge i_1j_1 with the lower load and the edge i_2j_2 with the higher load for their neighboring edges. For example, to avoid the further breakdowns of the neighboring edges, it is found when $\alpha = 1$ that the lowest values of the capacity parameter T are 1.5 and 1.1875 in two cases of the removals of the edges i_1j_1 and i_2j_2, respectively, and the LL is more easy to lead to cascading failures.

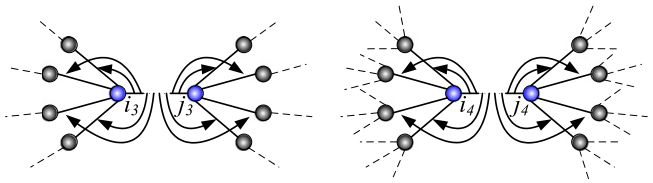

Fig. 3. Illustration for the effect of the proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge for cascading failures. For example, to avoid the further breakdowns of the neighboring edges of the attacked edge, we find when $\alpha = 1$ that the lowest values of the capacity parameter T are 1.3125 and 1.1563 in two cases of the removals of the edges i_3j_3 and i_4j_4, respectively. Therefore, the SPC is more efficient because the proportion between the total capacities of the neighboring edges of and the capacity of i_3j_3 is smaller than that of i_4j_4.

(2) Attack on the edges with the smallest proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge (SPC). The birth of this new attack can be explained by taking into account the characteristic of the load local redistribution after the edge fails. According to the load redistribution rule and the definition of the uniform T, the proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge plays a vital role in the control the cascading propagation. In Fig. 3, we can see that the malfunction of the edge i_3j_3 with the lower proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge can be more likely to trigger the overload of its neighboring edges than that of the edge i_4j_4. Therefore, the relative total capacities of the neighboring edges of the failed edge is more important in the study on attack strategies. Similar to the LL, in this attack strategy we will continually select the edges in the ascending order of the proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge (if some edges happen to have the same proportion, we randomly choose one of them).

(3) Attack on the edges with the highest load (HL). The important role played by the edges with the highest load in cascading failures has been widely investigated. By the comparison between the HL and other two attacks, we aim at providing the most efficient protection strategy to avoid the cascading propagation in the whole network. The removal rule of this attack is to select the edges in the descending order of load in the network and then to remove edges one by one starting from the edge with the highest load (if some nodes happen to have the same highest load, we randomly choose one of them).

As an example we consider the power grid of the western United States (Watts and Strogatz, 1998) which has 4941 nodes and 6594 edges. We neglect the details of the electromagnetic processes and focus only on the universal cascading phenomenon of the grid subject to the intentional attacks. By comparing three attacks, our aim is to demonstrate that the structure of an electric

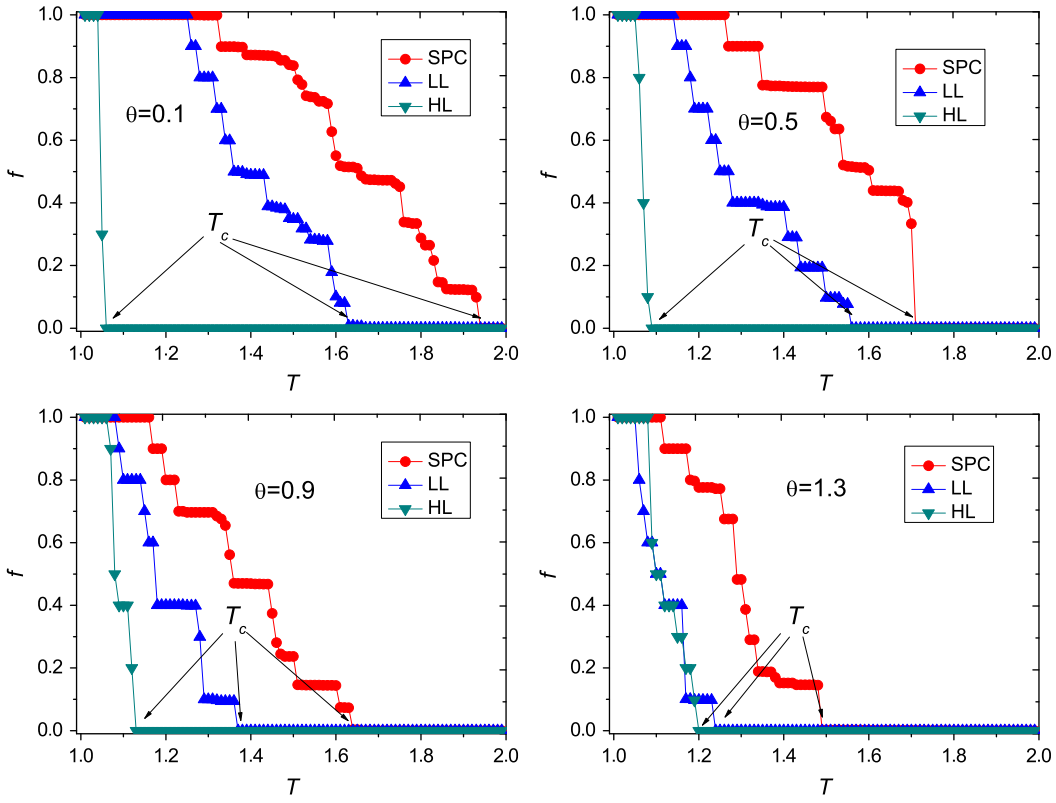

Fig. 4. Cascading failures with $\theta = 0.1$, 0.5, 0.9, and 1.3 in the power grid of the western United States, as triggered by three attack strategies, i.e., the HL, the LL, and the SPC. The data are averages over 30 realizations.

power grid can give us important information on the vulnerability of the system under cascading failures.

The damage caused by a cascade is quantified in terms of the number of broken edges after the cascading process is over. We use f_{ij} to denote the avalanche size induced by removing edge ij and calculate the consequence after every attacked edge fails. It is evident that $0 \leqslant f_{ij} \leqslant e-1$, where e represents the number of edges in the network. Without loss of generality, we assume the normalized avalanche size, i.e., $f = \sum_{ij \in A} f_{ij}/(N_A(e-1))$, where A and N_A represents the set and the number of edges attacked, respectively.

We choose 10 edges as the attacked objects and each curve is averaged over 30 realizations. We perform numerical simulations with θ = 0.1, 0.5, 0.9, and 1.3. In Fig. 4, we can observe that the responses of the power grid to three attacks display threshold-like behaviors. This crossover behaviors can be explained by the role of the parameter T in the load model. T is a capacity threshold parameter and its value decides the capacity of each edge dealing with the extra load. Thus, in the case of the fixed value of θ, for a sufficiently small value of T the malfunction of an arbitrary edge can trigger the universal cascading failures of the whole network because the capacity of each node is limited; while for a sufficiently big value of T no cascading failures occur and the system maintains its normal and efficient functioning because all edges have the larger extra capacities to handle the load. Thus, with the increase of T there should be a crossover behavior of the system from large scale breakdown to no breakdown, going through small scale ones. This phenomenon has been observed in Fig. 4. Interesting, in many previous studies on cascading failures (Wang and Chen, 2008; Wang et al., 2008; Wang and Rong, 2008, 2009), quantifying the network robustness by the crossover behavior of the capacity parameter has been widely applied to many networks. In order to have a better comparison among three attacks, we also adopt this crossover behavior to quantify the network robustness, i.e., the critical threshold T_c, at which a phrase transition occurs from normal state to collapse. Apparently, the bigger the value of T_c, the more efficient the attack strategy.

It is original expected the HL may be prone to trigger a cascade of overload failures capable of disabling the network almost entirely than other two attacks. However, by comparing the values of T_c induced by three attacks, we find, surprisingly, that the bigger cascades can be more likely to be triggered by the LL or the SPC than by the HL in the case of $\theta \leqslant 1.3$, as shown in Fig. 4. Fig. 4 indicates in the case of $\theta \leqslant 1.3$ that the most efficient attack is the SPC, the second and the last are the LL and the HL, i.e., the disruption degree order is SPC > LL > HL (the inequality SPC > LL means that the SPC is more likely to trigger cascading failures than the LL). Our finding has an important implication that it can provide guidance in protecting some edges selected effectively to avoid cascading-failure-induced disasters according to the different cases in real-life networks. In addition, as θ increases from 0.1 to 1.3, another interesting observation is that the difference between the HL and the LL is smaller and smaller. Thus a natural question arises: does there exist the value θ at which the effects of two attacks are almost identical?

To address this problem, we further compare the effects of three attacks for the network robustness in the range of $\theta > 1.3$. As can been seen from Fig. 5, it is easy to find in the case of $\theta = 1.4$ that obtaining T_c originating from the HL and the LL are almost the same. When $\theta = 1.4$, the disruption degree order is SPC > LL = HL. As θ increases, T_c obtained by the HL is bigger than that by the LL. Therefore, when $2.1 \geqslant \theta > 1.4$, the disruption degree order is SPC > HL > LL. In the range of $\theta \leqslant 2.1$, we observe that the difference between the HL and SPC is smaller and smaller. In Fig. 6, we further explore three attacks in the range of $\theta > 2.1$ and find when $\theta = 2.2$ that the order does not change; while when $\theta = 2.3$

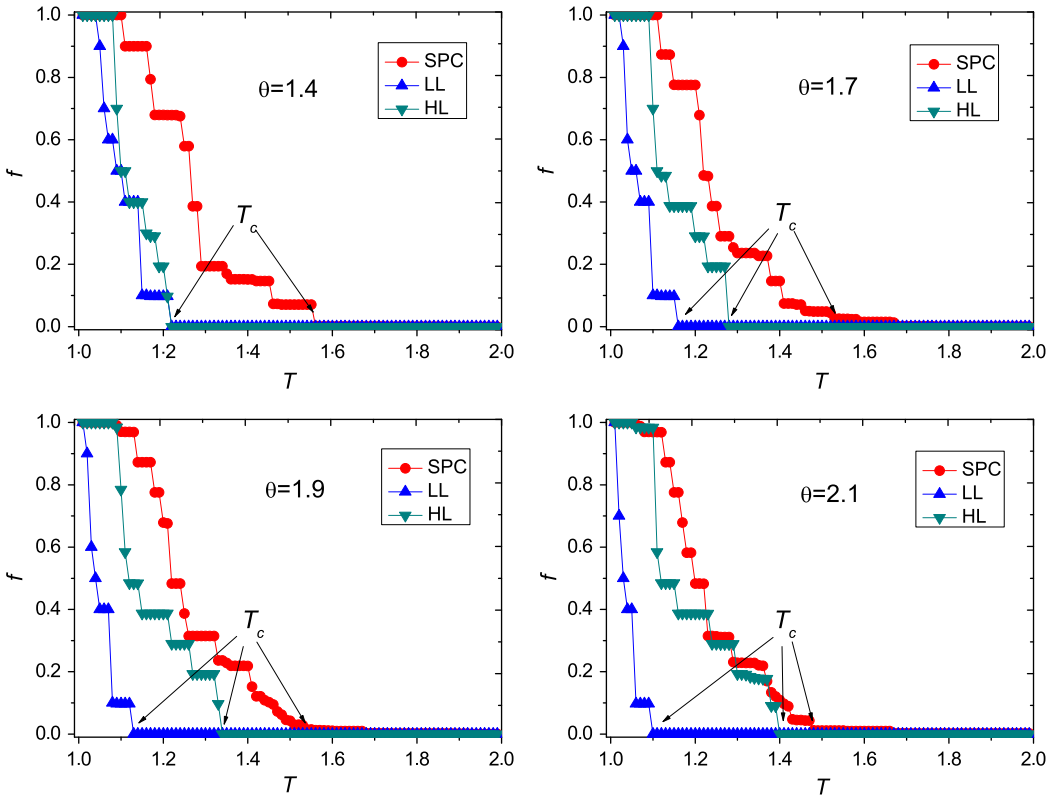

Fig. 5. Cascading failures with $\theta = 1.4$, 1.7, 1.9, and 2.1 in the power grid of the western United States. The data are averages over 30 realizations. The legends and other parameters are the same as Fig. 4.

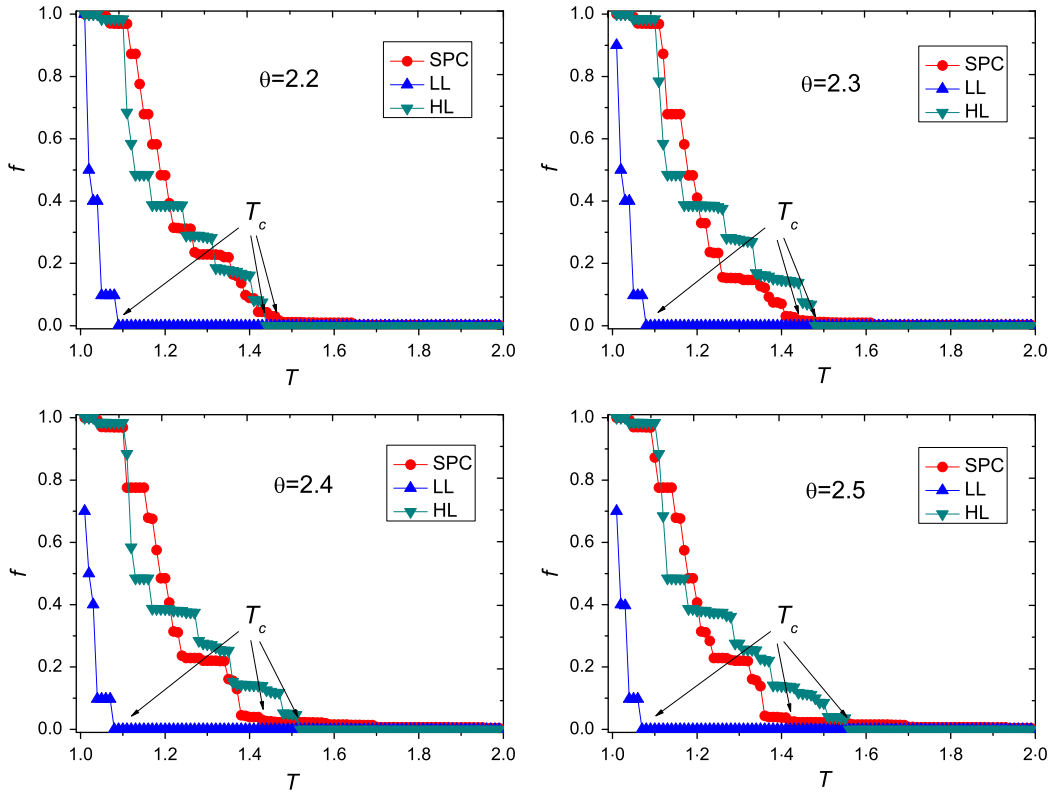

Fig. 6. Cascading failures with $\theta = 2.2$, 2.3, 2.4, and 2.5 in the power grid of the western United States. The data are averages over 30 realizations. The legends and other parameters are the same as Fig. 4.

the order is adjusted to HL > SPC > LL. To better comparing the effects of three attacks for the network robustness against cascading failures, we plot a function between T_c and θ, as shown in Fig. 7. Fig. 7 shows that there exists a switching point in comparing the effects of the HL and the LL when $\theta = 1.4$. Additionally, we also find that the network robustness has a negative correlation with θ under the HL (i.e., the estimate critical threshold T_c is positive correlation with θ); while the network robustness has a positive correlation with θ under the LL. For the SPC, the distribution of the smaller proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge leads to the relation uncertainty between T_c and θ. The inverted "V" curve of the SPC in Fig. 7 when $1.3 \leqslant \theta \leqslant 1.5$ can be explained by Fig. 8

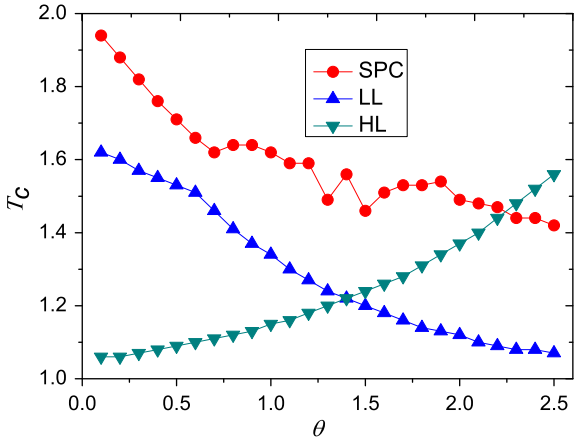

Fig. 7. Relation between the critical threshold T_c and the parameter θ under three attacks

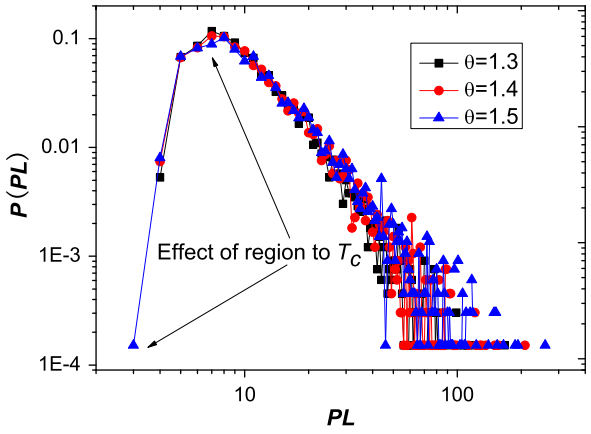

Fig. 8. Probability distribution $P(PL)$ as a function of the proportion PL between the total capacities of the neighboring edges of and the capacity of every edge in the power grid of the western United States. According to the load local redistribution rule, the region of the smaller PL has an important impact on the critical threshold T_c. In fact, the smallest PL with $\theta = 1.3$, 1.4, and 1.5 leads to the inverted "V" curve of the SPC in Fig. 7.

plotting a function between the proportion between the total capacities of the neighboring edges of and the capacity of every edge in the power grid and its probability distribution.

4. Conclusion

Maximizing robustness and minimizing cost are common objectives in the design of power grid networks. In this paper, based on the recently proposed load model of cascade, we investigate cascading failures induced by the intentional edge attacks in

the power grid of the western United States. In many previous studies about cascading failures, the classic intentional attack is usually defined as the attack based on the biggest degree or the highest load, while the lowest load attack is ignored. Considering the impact of the local characteristics of a breakdown edge on the cascading propagation, we propose two new attack strategies, i.e., the attack on the edges with the lowest load and the attack on the edges with the smallest proportion between the total capacities of the neighboring edges of and the capacity of the attacked edge. Numerical simulations show that the local characteristics of a breakdown edge has an important impact on the effects of intentional attacks in different parameter circumstances. Such insights, we believe, should be useful in further studies in the important area of network security and will be helpful for developing effective attacking/protecting strategies for future power systems.

So far, we have only focused on cascading failures induced by intentional attacks in the limited case of a single, non-interacting network. In fact, electrical blackouts frequently result from a cascade of failures between interdependent networks (Sergey et al., 2010), and the problem has been dramatically exemplified by the several large-scale blackouts that have occurred in recent years (Rosato, 2008). To this end, our future study will focus on the cascade dynamical aspect of errors and attacks on interdependent networks.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant No. 70771016.

References

Albert, R., Albert, I., Nakarado, G.L., 2004. Structural vulnerability of the North American power grid. Physical Review E 69, 025103. R.

Ash, J., Newth, D., 2007. Optimizing complex networks for resilience against cascading failure. Physica A 380, 673–683.

Crucitti, P., Latora, V., Marchiori, M., 2004. Model for cascading failures in complex networks. Physical Review E 69, 045104.

Dusko, P.N., Lan, D., Daniel, S.K., 2006. Criticality in a cascading failure blackout model. Electrical Power and Energy Systems 28, 627–633.

Goh, K.-I., Kahng, B., Kim, D., 2001. Universal behavior of load distribution in scale-free networks. Physical Review Letters 87 (27), 278701.

Goh, K.-I., Lee, D.-S., Kahng, B., et al., 2003. Sandpile on scale-free networks. Physical Review Letters 91, 148701.

Holme, P., Kim, B.J., Yoon, C.N., et al., 2002. Attack vulnerability of complex networks. Physical Review E 65, 056109.

Koos, V.D.B., 2008. Critical infrastructures and responsibility: a conceptual exploration. Safety Science 46, 1137–1148.

Leonardo, D.-O., Srivishnu, M.V., 2009. Cascading failures in complex infrastructure systems. Structural Safety 31, 157–167.

Moreno, Y., Gómez, J.B., Pacheco, A.F., 2002. Instability of scale-free networks under node-breaking avalanches. Europhysics Letters 58 (4), 630.

Motter, A.E., 2004. Cascade control and defense in complex networks. Physical Review Letters 93, 098701.

Motter, A.E., Lai, Y.C., 2002. Cascade-based attacks on complex networks. Physical Review E 66, 065102.

Ricard, V.S., Martí, R.C., Bernat, C.M., et al., 2008. Robustness of the European power grids under intentional attack. Physical Review E 77, 026102.

Rosato, V. et al., 2008. Modelling interdependent infrastructures using interacting dynamical models. International Journal of Critical Infrastructures 4, 63–79.

Sandro, M., Jesús, G.-G., Vito, L., et al., 2008. Scaling breakdown in flow fluctuations on complex networks. Physical Review Letters 100, 208701.

Sergey, V.B., Roni, P., Gerald, P., et al., 2010. Catastrophic cascade of failures in interdependent networks. Nature 464, 1025–1028.

Simonsen, I., Buzna, L., Peters, K., et al., 2008. Transient dynamics increasing network vulnerability to cascading failures. Physical Review Letters 100, 218701.

Tomas, H., 2007. Critical infrastructure and systemic vulnerability: towards a planning framework. Safety Science 45, 415–430.

Wang, W.X., Chen, G.R., 2008. Universal robustness characteristic of weighted networks against cascading failure. Physical Review E 77, 026101.

Wang, J.W., Rong, L.L., 2008. Effect attack on scale-free networks due to cascading failures. Chinese Physics Letters 25, 3826.

Wang, J.W., Rong, L.L., 2009. Cascade-based attack vulnerability on the US power grid. Safety Science 47, 1332–1336.

Wang, J.W., Rong, L.L., 2009. A model for cascading failures in scale-free networks with a breakdown probability. Physica A 388, 1289–1298.

Wang, X.F., Xu, J., 2004. Cascading failures in coupled map lattices. Physical Review E 70, 056113.

Wang, J.W., Rong, L.L., Zhang, L., et al., 2008. Attack vulnerability of scale-free networks due to cascading failures. Physica A 387, 6671.

The raw data used in "Collective dynamics of 'small-world' networks" by Watts, D.J., Strogatz, S.H., 1998. Nature. describing the US power grid.

Wu, J.J., Sun, H.J., Gao, Z.Y., 2007. Cascading failures on weighted urban traffic equilibrium networks. Physica A 386, 407.

Wu, J.J., Sun, H.J., Gao, Z.Y., 2007. Cascading failures on weighted urban traffic equilibrium networks. Physica A 386, 407.

Wu, Z.X., Peng, G., Wang, W.X., et al., 2008. Cascading failure spreading on weighted heterogeneous networks. Journal of Statistical Mechanics, P05013.

Zhao, L., Park, K., Lai, Y.C., 2004. Attack vulnerability of scale-free networks due to cascading breakdown. Physical Review E 70, 035101. R.

Zhao, L., Park, K., Lai, Y.C., et al., 2005. Tolerance of scale-free networks against attack-induced cascades. Physical Review E 72, 025104.