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 $(k_ik_j)^\theta$ 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.

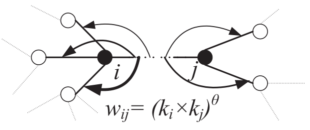

Fig. 1. Illustration of the load local preferential redistribution triggered by an edge-cut-based attack. Edge ij is broken and the load along it is redistributed to its neighboring edges. Among these neighbor edges, the one with the higher load will receive the higher extra load from the broken edge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