Safety Science 50 (2012) 443–447

Contents lists available at SciVerse ScienceDirect

Safety Science

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

Attack vulnerability of self-organizing networks

Jianhua Zhang [a,*], Xiaoming Xu [a,b,c], Liu Hong [a], Shuliang Wang [a], Qi Fei [a]

[a] Department of Control Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074, PR China
[b] University of Shanghai for Science and Technology, Shanghai 200093, PR China
[c] Shanghai Academy of System Science, Shanghai 200093, PR China

ARTICLE INFO

Article history:
Received 24 July 2010
Received in revised form 18 August 2011
Accepted 15 October 2011
Available online 8 November 2011

Keywords:
Self-organizing networks
Power grids
Cascading failures
Vulnerability

ABSTRACT

There are several self-organizing networks in the real world, and these networks severely affect the development of the modern society. This paper investigates the vulnerability of self-organizing networks subject to malicious attacks according to a new framework. Assuming the initial load of node i as $L_i = \alpha k_i + (1-\alpha)\sum_{j\in\Gamma_i} k_j$ with k_i and Γ_i being the degree and the set of neighbor nodes of the node i, where α is a tunable parameter and control the strength of the initial loads of nodes. The node with the maximum degree is considered as the attacked node, and with the changes of the parameter α, cascading failures will be investigated in this paper. Local redistribution rule has been adopted to study the cascading breakdowns of the US power grid and *IEEE*-118 networks. Additionally, the capacity of the node i is defined as $C_i = (1+\beta)L_i$, the critical threshold β_c of the US power grid and *IEEE*-118 networks will be obtained from the evolutional process of cascading failures. Finally, an optimal design of US power grid network is given in this paper.

1. Introduction

Networked infrastructures are more and more important in the modern society, such as power grid networks, internets, pipelines, and aviation networks. These networks are lifelines of our daily lives, and the safeties of these networks seriously affect the economic development, so we must pay more attention to the safeties of networked infrastructures. Networked infrastructure is a branch of the complex networks, and the related researches originate from the complex networks which have attracted increasing attention in recent decades. Complex networks are abstracted from the real networks, Watts and Strogaze (1998) discovered the small-world network and investigated the characteristics of small-world network, and Newman and Watts (1999) gave another model of small-world network. Barabasi and Albert (1999) proposed the scale-free network, and described the basic properties of the network. Random network originated from the random graph proposed by Erdos and Rényi (1960). These three networks are the basic networks of complex networks, and many scholars have investigated them in the past several decades (Strogatz, 2001; Albert et al., 2000). Additionally, there are many other networks, such as regulation networks, coupled networks, star networks, and hierarchical networks.

According to the past investigations on the complex networks, complex network theory has become more and more mature. Graph theory has been applied in complex networks to study the behaviors and properties of networks when the networks encounter the internal interruptions and external attacks. And most researchers are interested in investigating the cascading failures of complex networks, which is because that the cascading failures can cause huge damages to the modern society, especially the self-organizing networks.

In the modern society, we know that electricity network is the self-organizing network and it has significant impact on the society. It is known that if the generations blackout, we could not imagine the results of this event. For instances, if there is a blackout in a region, the plants will be closed, the household electric appliances lose its functions and traffic congestion will occur in this region, therefore the blackout events will result in huge economic losses to the society. So the safety of power grid networks is the most important issue. Many scholars have investigated the properties of the power grid networks and the reliability and vulnerability were studied in the past several years (Motter and Lai, 2002; Kinney et al., 2005; Carreras et al., 2002; Dobson et al., 2007; Albert et al., 2004; Chassin and Posse, 2005; Crucitti et al., 2004). Meanwhile, some researchers have investigated the characteristics of power grids subject to natural disasters (Duenas-Osorio and Vemuru, 2009; Winkler et al., 2010), such as hurricanes, earthquakes and snow disasters. Meanwhile the cascading failures of pipeline networks were also studied in the past, and many characteristics were obtained by the pioneers (Ouyang et al., 2009; Carvalho et al., 2009). The other properties of complex networks were investigated by researchers from all over the world. Wang

* Corresponding author. Tel./fax: +86 027 87540084.
E-mail address: zhangjianhua@smail.hust.edu.cn (J. Zhang).

0925-7535/$ - see front matter Crown Copyright © 2011 Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.ssci.2011.10.005

and Xu (2004) investigated the cascading failures of coupled map lattices. Wang et al. (2006) studied the oscillations of complex networks. Geographical effects of the complex networks were also discussed by many researchers (Huang et al., 2006; Hayashi, 2006). And many papers introduced the different properties of complex networks (Chen et al., 2007; Buzna et al., 2007; Bompard et al., 2009; Zio and Piccinelli, 2010).

The paper is organized as follows. Section 2 gives the model of self-organizing networks, and the dynamical process of cascading failures and the load redistribution rule after intentional attack are given in this section. The simulation results are given and the critical thresholds of tolerate parameter can be obtained in Section 3. Section 4 gives an optimal design on the US power grid and the optimal values of the parameters can be obtained. Finally, conclusion is given in Section 5.

2. The model

In the previous studies, the initial load of a node of the network was assumed according to the degree and the betweenness of the node, and the load redistribution after the attacks followed the shortest path in the whole networks. However, the load redistribution rules after attacks can be designed according to the given regulations and the other rules. Wang et al. (2008) investigated fault propagations of the weighted heterogeneous networks by employing a local weighted load redistribution rule when a node was removed from the network, and the initial load and the load capacity of node i were assumed as k_i^θ and ck^θ, respectively. Wang and Chen (2008) studied the universal robustness characteristic of weighted networks by employing a local weighted flow redistribution regulation with the weight of the edge ij being $(k_i k_j)^\theta$, where k_i is the degree of the node i. Wang and Rong (2009) introduced a weighted framework with the initial load and the capacity of a node were designed as $L_i = \left[k_i \sum_{j\in\Gamma_i} k_j\right]^\theta$ and cL_i respectively, and investigated the vulnerability of the US power grid. In all existing literatures, there are no scholars who designed the linear summation of the node degree and the degrees of its neighbor nodes as the initial load of the node to investigate the cascading failures of self-organizing networks.

In this section, graph theory is applied to abstract the self-organizing networks, and we can obtain the interrelations about the components of networked infrastructure. For any graph $G = \langle V, E\rangle$, $V = \{1,2,3,\ldots,N-1,N\}$ is the set of vertices, $E = \{ij\}$ is the set of edges. We assume the initial load and the load capacity of the node i being $L_i = \left[\alpha k_i + (1-\alpha)\sum_{j\in\Gamma_i} k_j\right]$ and $(1+\beta)L_i$ respectively, where $0 < \alpha < 1$, $\beta > 0$, k_i and Γ_i being the degree and the set of the neighbor nodes of the node i. Here we consider the cascading failures triggered by attacking a single node of self-organizing network. If the node has a small initial load, the removal cannot trigger the disastrous results, so the networks can recover from the load redistribution. However, if the deleted node has a large load, the local redistribution will trigger cascading breakdowns over the networked systems and lead to serious consequences, eventually result in the entire network collapsing.

Motivated by the above analyses and the ideas of the literatures (Wang et al., 2008; Wang and Rong, 2009), we discuss a novel model of cascading failures by adopting local load-redistribution regulation, that is to say, if a node collapses, the load of this node will be redistributed to its neighbor nodes according to the proposed rules. In this paper, the framework is given in the following:

R_1: Different from the previous papers, we assume the initial load of the node of self-organizing network being the interdependent linear summation of the node degree and the degrees of its neighbor nodes (two step degrees (Wu and Fang, 2008)), so the initial load L_i of the node i can be defined as follows

$$L_i = \left[\alpha k_i + (1-\alpha)\sum_{j\in\Gamma_i} k_j\right] \tag{1}$$

where α is a tunable parameter, and Γ_i is the set of the neighbor nodes of the node i. It is known that the load of a node is associated with its degree and the degrees of its neighbor nodes in some actual networked infrastructures, so this hypothesis is reasonable in some cases.

R_2: If a node is removed from the network, its load will be redistributed to its neighbor nodes according to local redistribution rule, the redistributed probability as following

$$P(i \to j) = \frac{k_j}{\sum_{\Gamma_i} k_m} \tag{2}$$

where Γ_i is the set of the neighbor nodes of the node i, this is the load redistribution rate to its neighbor node j when the node i is removed from the network.

R_3: Under the assumptions R_1 and R_2, the additional load from the attacked node i to its neighbor node j is proportional to the degree of the node j, and the load incremental is as follows:

$$\Delta L_{ij} = L_i \frac{k_j}{\sum_{m\in\Gamma_i} k_m} \tag{3}$$

We know that each node of the networked infrastructures has a capacity threshold which is the largest load that the node can tolerate. It is known that the load capacity of the node in actual network is limited by the cost of the node, so we assume that the load capacity C_i of the node i is proportional to its initial load, precisely $C_i = (1+\beta)L_i$, $i = 1,2,\ldots,N$, where $\beta > 0$ is called the tolerance parameter which can characterize the resistance to the intentional attacks and natural disasters. Because of the limitation of the capacity, when the node i malfunctions, the load of node i will be redistributed to its neighbor nodes, so the load of neighbor node j of the node i becomes $L_j + \Delta L_{ij}$, if $L_j + \Delta L_{ij} \leqslant C_j$, the whole network can restore balance. If $L_j + \Delta L_{ij} > C_j$, the node j will also collapse, which will lead to further redistributing the load $L_j + \Delta L_{ij}$ of node j, this may result in the other breakdowns, therefore the cascading failures occur. For example, the North America blackout in August of 2003 was caused by an untrimmed tree which was too close to high voltage transmission lines in the Midwest, this failure caused redistributing power flow and resulted in large scale cascading failures in North America. The visualization of the local load-redistribution rule is illustrated in Fig. 1.

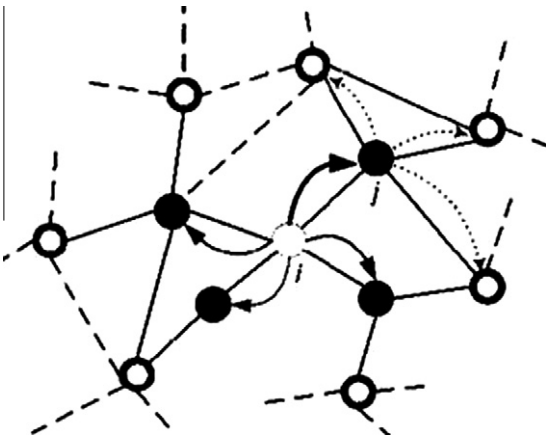

Fig. 1. The schematic diagram of load redistribution after the breakdown of node i.

3. Simulation results

In this section, we introduce the cascading process of self-organizing networks subject to malicious attacks, and discuss the robustness and vulnerability of the networks. We investigate the global connectivity of the proposed networks and obtain critical thresholds of the tolerate parameter of networks. We propose a parameter to measure the global connectivity, which is defined as follows

$$R = 1 - \frac{N'}{N} \tag{4}$$

where N and N' are the numbers of the nodes which can maintain the normal operations before and after cascading breakdowns in the whole network, R is the residual rate of nodes after cascading failures. The US power grid network and *IEEE*-118 network will be applied to simulate the cascading processes and illustrate the vulnerability of the self-organizing networks subjected to malicious attacks. The largest degree node-based attack is adopted to investigate the cascading phenomenon of the US power grid network with 4941 nodes and 6594 edges and *IEEE*-118 network with 118 nodes and 179 edges. If there are some nodes have equivalent degrees, we choose the node with the highest betweenness, which is the number of shortest paths passing through the node, as the removed node. If these two aspects are equivalent, we randomly select a node from them as the attacked node.

Fig. 2 characterizes the behaviors of cascading breakdowns of *IEEE*-118 network with different tunable parameter α. Fig. 2 illustrates that with the increase of the parameter α, the critical threshold of tolerance parameter β becomes smaller and smaller. According to Fig. 2, the cascading breakdowns of *IEEE*-118 network triggered by the largest degree node can result in serious results, so this node is one of the most important nodes of network, and the safety of this node must be considered and protected. Fig. 3 introduces the properties of cascading breakdowns of the US power grid. From Fig. 3, we know that the larger the tolerance parameter β is, the easier the cascading failures occur and the smaller the tunable parameter α is, the easier the cascading failures occur. This phenomenon of the US power grid is identical to *IEEE*-118 network, that is to say, with the decrease of parameter α, the probability of cascading breakdowns becomes larger and larger, and the critical threshold of the tolerate parameter becomes larger and larger. In terms of Figs. 2 and 3, we can declare that *IEEE*-118 network and the US power grid network are very vulnerability subjected to intentional attacks. We know that the smaller the critical threshold is, the better the robustness is, so Figs. 2 and 3 show that with the

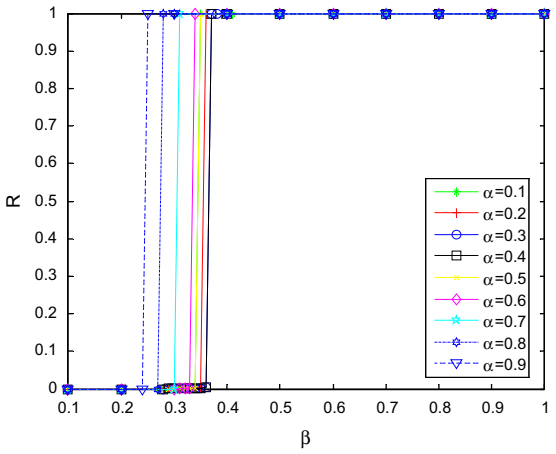

Fig. 3. The illustration of cascading breakdowns of US power grid network.

increase of the parameter α, the critical threshold β becomes smaller and smaller, so the robustness and reliability of the self-organizing networks become better and better.

From Eq. (1), we know that with the increase of the parameter α, the initial load of node i decreases, and according to Figs. 2 and 3, we can declare that with the increase of initial load, the probability of cascading breakdowns decreases according to the proposed scheme. Meanwhile, there is an interesting phenomenon which is that the number of breakdown nodes oscillates when the value of parameter β approaches its critical threshold, that is to say, in several small interval about tolerance parameter β, with the increase of β, the number of the crumbled nodes can increases in the US power grid network. This phenomenon illustrates that there are many very complicated characteristics in the large self-organizing networks.

The critical thresholds β_c of *IEEE*-118 and the US power grid networks are portrayed in Fig. 4 which shows that the critical threshold β_c of the US power grid network is larger than that of *IEEE*-118 network, which illustrates that the larger the network is, the easier the cascading failures occur. And it is obvious that the critical thresholds β_c have a trend to decrease with the increase of the tunable parameter α. Integrating with above analysis, we know the critical thresholds become smaller and smaller with the decrease of the initial loads of nodes in the networks. The critical threshold β_c is the most important parameter of network which can give the smallest value of tolerance parameter β. So we can declare that the

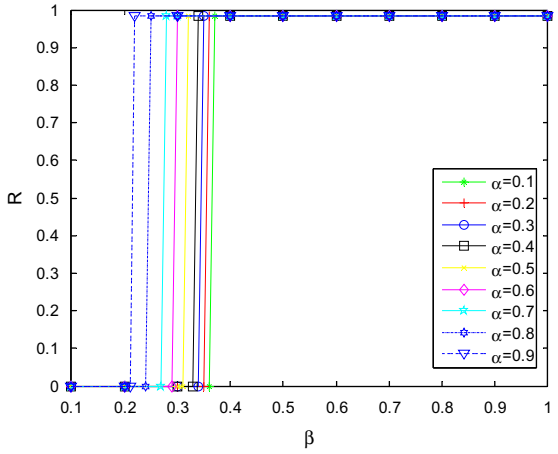

Fig. 2. The illustration of cascading breakdowns of *IEEE*-118 network.

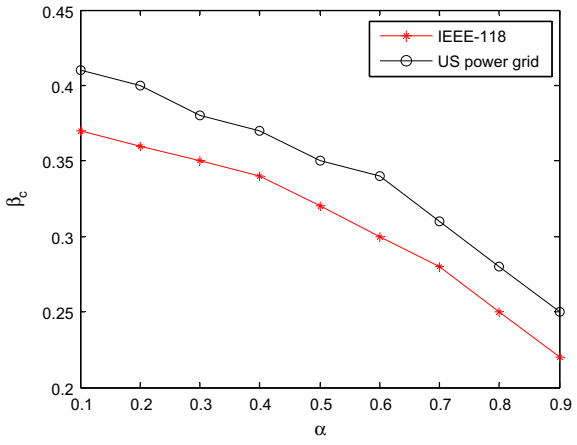

Fig. 4. The properties of critical threshold β_c versus α.

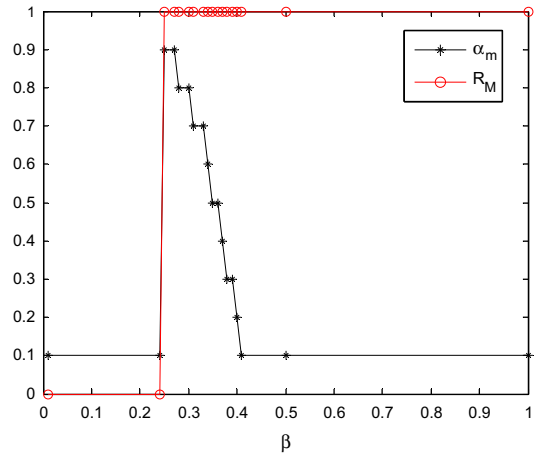

Fig. 5. The optimal values of scheme (5) versus β.

critical threshold of tolerance parameter of networks can control all the properties of network.

4. Optimal design of the US power grid network

From the definitions of the initial load and capacity of the node of the self-organizing networks, we know that the initial load of node increases with the decrease of the parameter α, and the capacity of the node increases with the increase of initial load of the node, so the capacity of the node becomes larger with the decrease of the parameter α. Figs. 3 and 4 show that the critical threshold β_c decreases with the increase of the parameter α, that is to say, the smaller the initial load of the node is, the smaller the critical threshold β_c is. However, we hope that the node can tolerate more load in the real networks and the load of the node can be designed before operations, so the optimal design must be given increasing concerns. In this section, we give an optimal design about the US power grid network. In order to reduce the probability of cascading failures, we assume the initial loads of nodes of the US power grid network being the largest initial loads of nodes, as follows

$$\begin{cases} \min\ \alpha \\ \max\ R \\ \beta \in (0,1] \\ \alpha \in \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9\} \end{cases} \tag{5}$$

Fig. 5 illustrates that the smallest value of parameter α_m severely changes from 0.1 to 0.9, at the same time, R_M rapidly changes from 0 to the largest value 0.9996. From the point $\beta = 0.27$, the parameter α starts to decrease until the initial state $\alpha = 0.1$. In order to make the nodes have the largest initial loads, we construct the optimal design (5), and the optimal values of the parameters are obtained in Fig. 5. The program (5) gives the largest loads of nodes, that is to say, the nodes have the largest load capacities according to the proposed model. Meanwhile, we know the capacities of nodes depend on the costs of nodes, so the optimal design can be used to enhance the robustness and reliability of networked infrastructures. Fig. 5 illustrates that there are no cascading failures in the US power grid network as long as the tolerance parameter $\beta \geqslant 0.25$.

5. Conclusion

This paper investigates the vulnerability of the self-organizing networks subjected to malicious attacks. Local load-redistribution rule is adopted to redistribute the load from the removed node to its neighbor nodes. From the proposed schemes, we investigate the cascading breakdowns of self-organizing networks, *IEEE*-118 and the US power grid networks are chosen as the examples to illustrate the effectiveness and the feasibility of the proposed model. Simulation results show that cascading failures of self-organizing networks can easily occur when the network encounter the malicious attacks and cascading breakdowns will cause huge damages to the modern society. So the safety of the networks must be paid more attention and we should take some measures to enhance the security and robustness of the networks. In order to improve the reliability and robustness of the networks, we give an optimal design about the US power grid network to enhance the resistance and robustness of the network.

Acknowledgements

This work is jointly supported by National Natural Science Foundations of China (61004088 and 60903174), the Key Foundation for Basic Research from Science and Technology Commission of Shanghai (09JC1408000), the Aeronautic Science Foundation of China (20100157001), the Fundamental Research Funds for the Central Universities, HUST: 2010QN016, 2010MS017 and the Fund of Key Lab for Image Processing and Intelligent Control (20093).

References

Albert, R., Jeong, H., Barabasi, A.L., 2000. Attack and error tolerance in complex networks. Nature 406, 378.
Albert, R., Albert, I., Nakarado, G.L., 2004. Structural vulnerability of north American power grid. Physical Review E 69 (2), 025103.
Barabasi, A.L., Albert, R., 1999. Emergence of scaling in random networks. Science 286, 509.
Bompard, E., Napoli, R., Xue, F., 2009. Analysis of structural vulnerability in power transmission grids. International Journal of Critical Infrastructure Protection 2, 5.
Buzna, L. et al., 2007. Efficient response to cascading disaster spreading. Physical Review E 75, 056107.
Carreras, B.A. et al., 2002. Critical points and transitions in an electric power transmission model for cascading failure blackouts. Chaos 12 (4), 985.
Carvalho, R. et al., 2009. Robustness of trans-European gas networks. Physical Review E 80, 016106.
Chassin, D.P., Posse, C., 2005. Evaluating north American electric grid reliability using the BA network model. Physica A: Statistical Mechanics and its Applications 355, 667.
Chen, M. et al., 2007. A new deterministic complex network model with hierarchical structure. Physica A: Statistical Mechanics and its Applications 385, 707.
Crucitti, P., Latora, V., Marchiori, M., 2004. A topological analysis of the Italian electric power grid. Physica A: Statistical Mechanics and its Applications 338, 92.
Dobson, I. et al., 2007. Complex systems analysis of series of blackouts: cascading failure, critical points, and self-organization. Chaos 17, 026103.
Duenas-Osorio, L., Vemuru, S.M., 2009. Cascading failures in complex infrastructure systems. Structural Safety 31, 157.
Erdos, P., Rényi, A., 1960. On the evolution of random graphs. Publications of the Mathematical Institute of the Hungarian Academy of Sciences 5, 17.
Hayashi, Y., 2006. Geographical effects on the path length and the robustness in complex networks. Physical Review E 73, 066113.
Huang, L., Yang, L., Yang, K.Q., 2006. Geographical effects on cascading breakdowns of scale-free networks. Physical Review E 73, 036102.
Kinney, R. et al., 2005. Modeling cascading failures in North American power grid. European Physical Journal B: Condensed Matter and Complex Systems 46, 101.
Motter, A.E., Lai, Y.C., 2002. Cascade-based attacks on complex networks. Physical Review E 66, 065102(R).
Newman, M.E.J., Watts, D.J., 1999. Renormalization group analysis of small world network model. Physics Letters A 263, 341.
Ouyang, M. et al., 2009. Effects of redundant systems on controlling the disaster spreading in networks. Simulation Modelling Practice and Theory 17, 390.
Strogatz, S.H., 2001. Exploring complex networks. Nature 410, 268.
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., 2009. Cascade-based attack vulnerability on US power grid. Safety Science 47, 1332.
Wang, X.F., Xu, J., 2004. Cascading failures in coupled map lattices. Physical Review E 70, 056113.
Wang, X.G., Lai, Y.C., Lai, C.H., 2006. Oscillations of complex networks. Physical Review E 74, 066104.

Wang, J.W. et al., 2008. Attack vulnerability of scale free networks due to cascading failures. Physica A: Statistical Mechanics and its Applications 387, 6671.
Watts, D.J., Strogaze, S.H., 1998. Collective dynamics of 'small world' network. Nature 393, 440.
Winkler, J. et al., 2010. Performance assessment of topologically diverse power systems subject to hurricane events. Reliability Engineering and System Safety 95, 323.
Wu, Z.H., Fang, H.J., 2008. Cascading failures of complex networks based on two-step degree. Chinese Physics Letters 25 (10), 3822.
Zio, E., Piccinelli, R., 2010. Randomized flow model and centrality measure for electrical power transmission network analysis. Reliability Engineering and System Safety 95, 379.