Physica A 427 (2015) 302–325

Contents lists available at ScienceDirect

Physica A

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

The cascading vulnerability of the directed and weighted network

Wei-Xin Jin [a,b,*], Ping Song [a,c], Guo-Zhu Liu [a], H. Eugene Stanley [d]

[a] *The State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System (CEMEE), Luoyang, 471003, China*

[b] *National Defense University, Beijing, 100091, China*

[c] *Xi-an Communication Institute, Xi-an, 710106, China*

[d] *Center for Polymer Studies and Department of Physics, Boston University, Boston, MA 02215, USA*

HIGHLIGHTS

- The cascading failures based on directed and weighted network is studied.
- The 'load-capacity' model of the directed and weighted network is built.
- The 'over-loading' and the 'short-loading' cascading failure models based on the directed and weighted network were built.
- The power exponent β of 'load-capacity' function should be taken value (0, 1) for a good robustness of the power law network.
- The power exponent β of loading function should be taken value (0, 3) for a good robustness of the Poisson network.

ARTICLE INFO

Article history:
Received 1 June 2014
Received in revised form 27 November 2014
Available online 10 February 2015

Keywords:
Directed and weighted network
Cascading failure
Model
Vulnerability

ABSTRACT

The cascading failure can bring a huge loss for most real-world networks; but, we cannot uncover fully the mechanism and law of the cascading events occurrence. Most networks in which the cascading failure occurred are based on the various 'flows', such as power, oils, and information; moreover, the same link degree of the different nodes likely contain the different meanings, where some are large pivotal nodes and some are mini switching centers. Thus, these networks must be described by the directed and weighted network model. Besides, the 'over-loading' cascading failures were more analyzed and studied; but the cascading failures caused by 'short-loading' were less studied relatively. However, for some directed networks, such as power grids, oil pipe nets, gas pipe nets and information networks, the large-scale failures of network nodes substantially could be induced by 'short-loading' in a such similar way as 'over-loading'. Based on the above reasons, in this paper, we first built the 'load-capacity' model of the directed and weighted network. Afterwards the 'over-loading' cascading failure model and the 'short-loading' cascading failure model based on the directed and weighted network were built. Meanwhile, applying the models to two typical real networks – Poisson distribution network and power law distribution network – intensive study and numerical analysis were carried out. Lastly, two classical networks simulation experiment results are provided. After the numerical and simulation analyses, we gained the following conclusions. For the power law network, the power exponent β of 'load-capacity' function should be taken value (0, 1) for a good robustness, and the minimum in-degree and out-degree should be increased respectively, meanwhile, the weight and the scaling exponents of the in-degree and the out-degree distributions

[*] Correspondence to: Department for Information Operations and Command Training, National Defense University, Beijing, 100091, China. Tel.: +86 10 66772287.
E-mail address: jwx773059@126.com (W.-X. Jin).

http://dx.doi.org/10.1016/j.physa.2015.02.035
0378-4371/© 2015 Elsevier B.V. All rights reserved.

should be increased synchronously in the interval (2, 3) for enhancing the resistibility of 'over-loading' and 'short-loading' failures. For the Poisson network, the power exponent β of loading function should be taken value (0, 3) for a good robustness, and the average weight and the average in-degree should be increased respectively restricting $2 < \beta < 3$ for enhancing the resistibility of 'over-loading' and 'short-loading' failures.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Dr. R. Albert et al., publishing in a 2000 NATURE article, 'Error and attack tolerance of complex networks' [1], pioneered the research for the vulnerability of complex networks. They found that, the scale-free network has high robustness for the accidental failure, but behaves extremely vulnerable for the deliberate attack. On the contrary, the vulnerability of exponential network has no significant difference for the accidental failure and deliberate attack. In the same year, D.S. Callaway et al. wrote in a physics journal PRL article, 'Network robustness and fragility: Percolation on random graphs' [2]. Using the generating function method presented in literature [3], they found the critical condition of the removed node proportion when the network with arbitrary degree distribution function was paralyzed for failures or deliberate attacks. In 2001, R. Cohen et al. wrote in a PRL article, 'Breakdown of the Internet under intentional attack' [4]. With the both analysis and simulation methods to verify each other, they proposed the quantitative relationship among the scaling exponent α ($\alpha \geqslant 2$), the scale of the maximum interconnection-group and the critical proportion of the removed nodes when the scale-free network ($p(k) \sim k^{-\alpha}$) was paralyzed as a result of deliberate attacks. They concluded that the bigger the scaling exponent was, the more vulnerable the network was in deliberate attack mode. Since 2002, some scholars such as A.E. Motter [5,6], Y. Lai [5,7], I. Dobson [8,9], P. Crucitti [10,11], H.J. Sun [12], and L.D. Dueňas-Osorio [13], have paid more attention to the cascading failure phenomenon of network and set to an in-depth study. They think that the cascading failure is the main reason of a large-scale break down of the real-world networks such as power grids and Internet. They found the cascading failure that is the individual node failure caused by disaster or contingency leads to the loading diversion from this failure node to others; the loading of the nodes accepted extra loading rise suddenly, which can cause over loading of some nodes then failures; this process progressed continually will finally lead to a large-scale break down of the network. Explaining and simulating this phenomenon, they proposed the loading and capacity models based on node betweenness [5–7,12], the redistribution model CASCADE based on stationary loading P [8,9], the time-varying model which represents the efficiency decline in proportion to over loading instead of removing the over loading nodes, and calculates loading and capacity by node betweenness [10,11], and the statistic model based on historical real-world data [13]. Above papers respectively concluded that the node attack based on maximum load should be the most easy way to cause the scale-free network to cascading paralysis [5,8,6,7,10,11,9] ; removing the minimum loading node can reduce the scale of paralysis to a certain extent [6]; the load capacity coefficient will greatly affect the efficiency decreasing speed of the cascading nodes [10]; and to enhance the robustness of the network, network engineers cannot just rely on increasing the capacities of nodes and load-edges, but need adjust the network topology structure [13]. However, all of the above-mentioned models need betweenness to calculate the node loading and capacity, and calculating betweenness must obtain the global topological information of the network, which is very difficult for large-scale networks (for instance many real-world networks). Therefore, since 2008, many scholars have attempted to explore the way to calculate the node loading and capacity by the local information of nodes, and build the loading and capacity calculation models based on the local information of nodes [14–16,13,17–19]. The above main calculation models include: the loading and capacity model based on the node degree power function [14,18], the edge-weight loading and capacity model based on the degree product power function of the two ends nodes [15], the loading and capacity model based on time-varying edge-weight power function [16], the loading and capacity model based on the product power of node degree and the degree sum of its secondary neighbors [17] or the degree sum power product of multilevel neighbors [19], etc. In this period, some scholars even use the physical models such as Ohm's law and Kirchhoff conservation law to research the cascading vulnerability of the large-scale network based on 'flow' like electric power [20–22]. They gained counter-intuition conclusion that the incremental increase of one edge's load capacity could expand the cascading vulnerability of the network.

In 2010, S.V. Buldyrev et al. published an article 'Catastrophic cascade of failures in interdependent networks' in NATURE. They analyzed for the first time the cascading vulnerability of the interconnected and interdependent networks by complex network method. They found the vulnerability characteristic of interdependent networks different from the single network. This characteristic is that for the accidental failure or deliberate attack, the wider the degree distribution of interdependent networks is, the more vulnerable the interdependent networks become. But for single network, the wider the degree is, the more robust the network becomes [23]. In 2012, Dr. J. Shao et al. wrote in a NATURE PHYSICS article 'Networks formed from interdependent networks'. In this paper, the vulnerabilities of two partially interdependent networks and more interdependent NoN (Network of Networks) were analyzed systematically. They also proposed the explicit function between the removed nodes proportion and the maximum interconnection-group scale of three typical NoN with similar star, tree or chain structure, which were composed of Erdös–Rényi network [24]. In 2013, Dr. X. Huang et al. designed a bank-network bipartite graph model based on bank and bank assets, and built a cascading failure model of the financial risk

Download English Version:

https://daneshyari.com/en/article/975033

Download Persian Version:

https://daneshyari.com/article/975033

Daneshyari.com