Physica A 444 (2016) 458–465

Contents lists available at ScienceDirect

Physica A

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

Research on invulnerability of the random scale-free network against cascading failure

Rong-Rong Yin [a,b], Bin Liu [a,b,*], Hao-Ran Liu [a,b], Ya-Qian Li [c]

[a] *College of Information Science and Technology, Yanshan University, Qinhuangdao 066004, Hebei, People's Republic of China*

[b] *The Key Laboratory of Special Optical Fiber and Optical Fiber Sensing of Hebei Province, Yanshan University, Qinhuangdao 066004, Hebei, People's Republic of China*

[c] *Institute of Electrical Engineering, Yanshan University, Qinhuangdao 066004, Hebei, People's Republic of China*

HIGHLIGHTS

- The new cascading failure model of random scale-free network is established.
- The threshold of node capacity triggering the cascading failure is obtained.
- The relationship between capacity threshold and network's parameters is deduced.
- Invulnerability against cascading failure increases with parameters increasing.

ARTICLE INFO

Article history:
Received 16 April 2015
Received in revised form 8 July 2015
Available online 10 September 2015

Keywords:
Random scale-free network
Cascading failure
Power exponent
Critical threshold

ABSTRACT

The effect of structure parameters of random scale-free network on the network invulnerability for cascading failure is investigated by establishing a cascading failure model of random scale-free network based on node degree and analyzing the effect of node capacity on the cascading failure. The node capacity threshold is thus obtained. Furthermore, the relationship between the threshold of node capacity and the structure parameters of the network (the number of added edges per time slot and the power exponent) is established. The experimental results show that the structure parameters of the network are positively correlated with the network invulnerability for cascading failure. The more the number of added edges at a time and higher the power exponent, the stronger the network invulnerability for cascading failure.

1. Introduction

With the development of random scale-free network, network invulnerability has become a hot topic of research. It is defined as the ability of the network to continue working when it suffers random failures or intentional attacks [1]. Network invulnerability can be classified into static invulnerability and dynamic invulnerability, and the difference between the two depends on whether the failure node or edge can lead to failure of other nodes or edges. Because the nodes and edges of the real network carry the load, the failure of one link or part of the nodes causes load redistribution, which in turn could lead to failure of other nodes. Then, a further load redistribution will result in cascading failure [2]. The dynamic invulnerability is also known as cascading failure invulnerability [3]. Therefore, research on the cascading failure model of random scale-free network has practical significance, because it could reveal the dynamic invulnerability mechanism of network.

[*] Corresponding author at: College of Information Science and Technology, Yanshan University, Qinhuangdao 066004, Hebei, People's Republic of China.
E-mail address: liubin@ysu.edu.cn (B. Liu).

http://dx.doi.org/10.1016/j.physa.2015.08.017
0378-4371/© 2015 Published by Elsevier B.V.

In the study of static invulnerability, Albert et al. [4] proposed a well-known Barabási–Albert (BA) model by focusing on the influence of topological structure on the network invulnerability. In the BA model, there are few key nodes with high degrees, and most nodes have low degrees. This property makes the network robust to random failures, but vulnerable to intentional attacks. In the study of cascading failure invulnerability, Motter et al. [5] proposed a load–capacity model by studying the dynamic characteristics of the network invulnerability. In this model, the initial node load is betweenness, and the node capacity is proportional to the initial node load. Cascading failure is reduced by removing the nodes with low degrees. Wang et al. [6] proposed a cascading failure model based on the distribution strategy of the local load. This model requires only the local load information, and thus it has low complexity. Ren et al. [7] proposed another cascading failure model, in which load redistribution was based on the remaining capacity of nodes. This model makes full use of the network resources, which improves the network invulnerability. Li et al. [8] suggested that the node with high degree could effectively increase the ability of the network to resist cascading failure when more load was applied. Schafer et al. [9] proposed that network invulnerability could be increased by reducing the total network load. All the aforementioned studies on cascading failure invulnerability are also based on the BA model, but they are not conformed to the real network because the power exponent of the BA model is a constant. In order to resolve this problem, Yin et al. [10] proposed a cascading failure model based on the variable load and the fixed capacity of the node, and they achieved the critical value of load for the cascading failure of network. Simultaneously, the effect of the structure parameters of the random scale-free network (degree distribution coefficient and power exponent) and network invulnerability on simulation experiment was analyzed.

In this study, on the basis of a new cascading failure model, the effect of the structure parameters of the random scale-free network on the network invulnerability for cascading failure is further studied theoretically. In Section 2, construction of a new cascading failure model of random scale-free network is described, and the threshold of node capacity is obtained. The smaller the threshold is, the stronger the invulnerability of the network. By analyzing the mathematical model constructed based on the threshold, one can find that the number of newly added edges at a time and the power exponent influence the threshold. In Section 3, the relationship between the two network structure parameters (number of newly added edges at a time and power exponent) and the network invulnerability is investigated using the topology model with an adjustable power exponent. The results obtained reveal that the structure parameters of the network are proportional to the network invulnerability for cascading failure. This provides the theoretical reference to enhance the network invulnerability from the perspective of topological structure.

2. Analysis of invulnerability of random scale-free network

In a random scale-free network, when a node fails, unprocessed data will be redistributed to its neighbor nodes. In order to maintain the network flow and avoid network congestion, the neighbor nodes with high capacity will be redistributed with more unprocessed data. Thus, the initial load of node is set to be a function of node degree. Therefore, the cascading failure model is proposed using the load preferential redistribution principle of failure node. As a consequence, the network parameters, which can influence network invulnerability, could be found.

Cascading failure model based on the function of node degree

The network topology is described as an undirected graph, where $V = \{v_1, v_2, \dots, v_n\}$ is a set of nodes and $E = \left\{e(v_i, v_j)\right\}$ is a set of edges. Let k_i $(1 \le k_i \le N)$ denote the node degree of v_i, where N is the total number of nodes in the network. The average node degree in the network is denoted as $\langle k\rangle$.

Let us assume that in the initial stage of the network, load of each node is less than its capability, and the network is steady. However, when a node fails, it will redistribute the load to neighbor nodes. However, when the neighbor node is not able to handle this additional load, it will also fail, which in turn will lead to the failure of other nodes, resulting in cascading failure. Therefore, the model will be described in three aspects: initial node load [11], load redistribution rule, and node capacity.

The initial node load: For any node i in the network with initial load L_i, the function of node degree k_i is defined as follows [12]:

$$L_i = {k_i}^{\alpha}, \tag{1}$$

where α is an adjustable parameter, which controls the initial load of node in the network. With an increase of α, the difference of load among different nodes increases; thus, load distribution is more uneven.

Principle of load redistribution: The load of j is redistributed to its neighbor nodes based on preferential principle, and the node load redistribution principle is described as

$$\prod_{j} \frac{{k_i}^{\alpha}}{\sum\limits_{n\in\Gamma_j} {k_n}^{\alpha}}, \tag{2}$$

where n is the neighbor node of the failed node j and Γ_j is the set of node j's neighbor nodes. According to the principle of load redistribution, additional load ΔL_{ij}, which the node i receives from j, can be obtained by

$$\Delta L_{ij} = L_j \frac{{k_i}^{\alpha}}{\sum\limits_{n\in\Gamma_j} {k_n}^{\alpha}}. \tag{3}$$