Physics Letters A 372 (2008) 5778–5782

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Dynamics of load entropy during cascading failure propagation in scale-free networks

Z.J. Bao [a], Y.J. Cao [a,b,*], L.J. Ding [a], Z.X. Han [a], G.Z. Wang [a]

[a] College of Electrical Engineering and National Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China
[b] College of Electrical and Information Engineering, Hunan University, Changsha 410082, China

ARTICLE INFO

Article history:
Received 14 May 2008
Received in revised form 26 June 2008
Accepted 10 July 2008
Available online 22 July 2008
Communicated by A.R. Bishop

Keywords:
Scale-free network
Load entropy
Cascading failures
Dynamics
Load distribution

ABSTRACT

In this Letter, we introduce the concept of load entropy, which can be an average measure of a network's heterogeneity in the load distribution. Then we investigate the dynamics of load entropy during failure propagation using a new cascading failures load model, which can represent the node removal mechanism in many real-life complex systems. Simulation results show that in the early stage of failure propagation the load entropy for a larger cascading failure increases more sharply than that for a smaller one, and consequently the cascading failure with a larger damage can be identified at the early stage of failure propagation according to the load entropy. Particularly, load entropy can be used as an index to be optimized in cascading failures control and defense in many real-life complex networks.

1. Introduction

Recently, it has been shown that many large-scale real complex networks display a free-scale feature [1,2], such as the Internet, the power transmission grid, and metabolic networks, etc., with power-law degree distribution [3,4]: $P(k) \sim k^{-\gamma}$, where k is the number of links of a randomly chosen node in the network and γ is the scaling exponent. The work by Albert et al. demonstrated that scale-free networks possess the robust-yet-fragile property, in the sense that they are robust against random failures of nodes but fragile to intentional attacks [5]. Large cascading events observed in many real large-scale infrastructure networks just prove Albert's conclusion. For instance, on 10 August 1996 when a 1300-mW electrical line in southern Oregon sagged in the summer heat, a chain reaction that cut power to more than 4 million people in 11 Western States is initiated [6,7]. In October 1986 during the first documented Internet congestion collapse, the speed of the connection between the Lawrence Berkeley Laboratory and the University of California at Berkeley dropped by a factor 100 [8,9].

Because of the ubiquity of scale-free networks, as well as the increasing catastrophes with severe long-term consequences surrounding us, induced by cascading failures, the security of scale-free networks, i.e., how failures or attacks affect the integrity and operation of the networks has been of great interest [10–22]. In the previous research, the cascade events are extensively studied by using two kinds of models, one is the cascading failures load model [10–13,18,19,23,24] and another is the susceptible-infected-recovered (SIR) model [20–22]. In Ref. [10], a simple mechanism was proposed to incorporate the dynamics of load in both random and scale-free networks, by introducing a cascading model based on the intrinsic flows of physical quantities in the network. By using the load model, Ref. [11] investigated a phase-transition phenomenon in terms of the key parameter characterizing the node capacity. Based on the previous work, Lai et al. derived an upper bound for the capacity parameter, above which the network is immune to cascading breakdown [12]. A model and mechanism for overload breakdown in growing networks has been considered by Holme and Kim [13], in which these authors focused on overloads caused by the growth of the network. The cascading failures in scale-free coupling map lattices have been studied by Wang et al. [14,15]. More recently, Wu et al. discussed the dynamics of cascading failures in urban traffic networks, from the edge overloading to the malfunctioning of node [16,17]. In Refs. [20,21], epidemic spreading in scale-free networks is investigated by proposing a modified susceptible-infected-recovered (SIR) model, and a conclusion is drawn that the density of the recovered individuals shows a threshold behavior. By using a SIR model, rumor propagation in complex networks is studied analytically and numerically, with emphasis on the relationship between the network topological structure and the number of the total final infected

* Corresponding author at: College of Electrical Engineering and National Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China. Tel.: +86 571 87952702; fax: +86 571 87951625.
E-mail address: yjiacao@zju.edu.cn (Y.J. Cao).

0375-9601/$ – see front matter
doi:10.1016/j.physleta.2008.07.034

nodes [22]. The pioneering work on cascade control and defense has made many significant achievements [23], which suggest that an intentional removal of network elements right after the initial attack can drastically reduce the size of the cascade.

Many studies show that the heterogeneity in the load distribution makes the system vulnerable to cascading failures [23,24]. However, to our knowledge no research focused on how to quantify the heterogeneity of node loads. Inspired by the work of Wang et al., who introduced the entropy of the degree distribution in scale-free networks [25], we propose the concept of load entropy to characterize a network's heterogeneity in the load distribution and develop a new cascading failures load model, which can represent the overloaded node removal mechanism common to many real-life complex systems, and then investigate the dynamical evolving properties of load entropy during the failure propagation. Numerical simulations show the relationship between the dynamics of load entropy and the damage size of cascading failures, by which large cascades can be recognized at the early stage of failure propagation.

2. A new cascading failure load model representing the real overloaded nodes removal mechanism

We assume that the time scale for cascading failures is much smaller than the time scale in which the network grows, and hence the growth of network is not considered in the study of cascading failures.

In many realistic situations the flow of physical quantities in the network, as characterized by the loads on nodes, is important. For a given network, suppose that at each time step one unit of a physical quantity (so-called a packet), which can be information, energy, etc., is exchanged between every pair of nodes and transmitted along the shortest path connecting them. The load $L_i(t)$ on node i at time t is the total number of shortest paths passing through i. If there is more than one shortest path connecting two nodes, the packet is divided evenly at each branching point. Each node is characterized by a capacity defined as the maximum load that node can handle. In man-made networks, the capacity is severely limited by cost. Following Ref. [10] we assume the capacity C_i of node i to be proportional to its initial load $L_i(0)$:

$$C_i = (1+\alpha)L_i(0), \quad i = 1, 2, \ldots, N, \tag{1}$$

where the constant $\alpha \geqslant 0$ is the tolerance parameter and N is the number of nodes.

The initial removal of a node, in general, changes the distribution of shortest paths. The load at a particular node can then change. If it increases and exceeds the capacity, the corresponding node is prone to malfunction. As a result, a new redistribution of loads occurs, and thus may lead to a new round of nodes failure. This step-by-step process is so-called a cascading failure. If a relatively important node is attacked, the cascading failures can propagate and shutdown a considerable fraction of the whole network [10].

We consider that in most real-life complex networks a certain quantity of instantaneous node overload is permissible and the node malfunction is mainly caused by the accumulative effect of overload. For instance, in traffic transmission networks, the temporary congestion of a crossing, which results from a small occasional incident and can be solved soon, usually has no distinct effect on the normal operation of the whole network. The same case can also be observed in the Internet. At the same time, there exists a certain monitoring and control in many large-scale infrastructure networks. Once the node overload is detected, some effective measures are taken within the response time to decrease the capacity constraint violation and even make the node load less than its capacity. However, in the most previous cascading failures models, the simple and unreasonable strategy of immediate removal of an instantaneously overloaded node is widely adopted, without considering the real-life overloaded node removal mechanism described above. Therefore, we introduce a new strategy of the overloaded node removal to reflect many real-life complex networks.

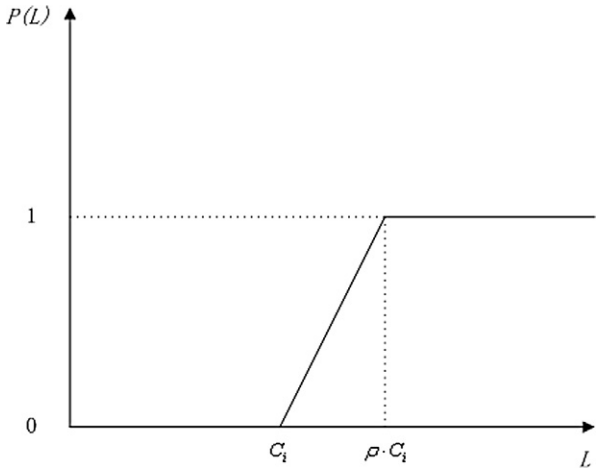

Fig. 1. The removal probability $P(L)$ of node i, which load L lasts for time T.

It is assumed that the removal probability $P(L)$ of a node, which load L lasts for a period of time T, is shown in Fig. 1 and the probability density of $P(L)$ obeys uniform distribution in the interval $[0, T]$. The parameter T has some relation to the response time of the complex systems. The parameter $\rho(\rho > 1)$, shown in Fig. 1, may be different for various networks and in the simulations we choose $\rho = 1.5$. At each time t, the following iterative rule is adopted:

$$p_i(t) = \begin{cases} p_i(t-1) + P(L_i(t))/T & \text{if } L_i(t) > C_i, \\ 0 & \text{if } L_i(t) \leqslant C_i, \end{cases} \quad i = 1, \ldots, N, \tag{2}$$

where $p_i(t)$ is the removal probability of node i at time t, $L_i(t)$ is the load of node i at time t and $P(L_i(t))$ can be obtained from Fig. 1.

In this way, after an initial removal of a node caused by an attack, at each time the loads of all nodes are calculated and then the nodes which will be removed from the network are determined by comparing a random $\beta \in (0, 1)$ and the malfunction probability derived by Eq. (2). When the loads of all nodes are not larger than their corresponding capacity, a cascading failure stops. The damage caused by a cascade is quantified in terms of the relative size G of the largest connected component

$$G = N'/N, \tag{3}$$

where N and N' are the numbers of nodes in the largest component before and after the cascade respectively.

3. Dynamics of load entropy during cascading failure propagation

A simple but essential reason for the vulnerability of scale-free networks to cascading failures is its heterogeneous load distribution. Heterogeneity can be measured by entropy [26,27]. The load level of node i at time t is expressed as

$$R_i(t) = \frac{L_i(t)}{C_i}. \tag{4}$$

In order to generate the load entropy, M successive intervals are defined as $[0, u), [u, 2*u), \ldots, [(M-1)*u, M*u)$ and it is