Chaos, Solitons & Fractals 57 (2013) 35–40

Contents lists available at ScienceDirect

Chaos, Solitons & Fractals

Nonlinear Science, and Nonequilibrium and Complex Phenomena

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

Improving the network robustness against cascading failures by adding links

Xian-Bin Cao, Chen Hong, Wen-Bo Du *, Jun Zhang

School of Electronic and Information Engineering, Beihang University, Beijing 100083, PR China

ARTICLE INFO

Article history:
Received 24 May 2013
Accepted 6 August 2013
Available online 3 September 2013

ABSTRACT

In this paper, we explore the network robustness against cascading failures by adding links to the underlying network structure. Three link-adding strategies are compared, including random linking strategy (RLS), high-betweenness linking strategy (HBS), and low-polarization linking strategy (LPS). It is found that HBS is more effective than RLS to enhance the network robustness against cascades while the network exhibits the strongest robustness under LPS. Moreover, the effect of the total cost of link-adding is investigated. As the total cost grows, the advantage of LPS becomes more evident. Our work would be helpful for the design of networked systems.

1. Introduction

Modern human societies are greatly dependent on infrastructure systems such as power grids, the Internet, communication systems and transportation networks. However, the disastrous incidents in these crucial networks may lead to large-scale collapses and serious economic consequences [1,2]. In these realistic networks supporting the flow of physical quantities, the breakdown of a single node or link will cause the redistribution of physical flows over the surviving nodes or links [3], and then some nodes or links will fail if they are overloaded. The process is propagated until there are no overloaded nodes or links [4–7]. Therefore, an unexpected triggering event may result in the collapse of the entire network. Such behavior is called "avalanche" or "cascading failures" [8–16].

Due to the importance of robustness against cascades to many realistic complicated systems, the study of cascade defense and control strategy to improve network robustness has attracted a lot of interest in recent years [17–24]. To improve the robustness of networks against cascades, one method is to design efficient load redistribution strategies while the other is to make appropriate changes to the underlying network structure. Designing efficient load redistribution strategies [24–26] can be considered as "soft" strategies, because it does not change any network structure. Making changes to network topological structure [27–32] can be considered as "hard" strategies.

A number of "soft" strategies have been intensively investigated in previous literatures [24–26]. Schäfer et al. [24] proposed a proactive method to improve the robustness of heterogeneously loaded networks against cascading failures. The key of this method is to carefully use the load-based lengths of the flow paths. By picking only those flow paths with the lowest load-based lengths, the previously heterogeneous load distribution of the network changes into a more homogeneous one, then the network robustness is greatly improved. Zhao et al. [25] proposed a navigation strategy which combines the traditional shortest path information and the degree of the vertices. The results show that the navigation strategy performs well in cascade defense without damaging the network efficiency. Wang et al. [26] study the cascading failures on weighted complex networks by proposing a local weighted flow redistribution rule. On the other hand, there are also some "hard" strategies have been studied. Motter [19] proposed a simple reactive defense control strategy: after a single node or link failure, the intentional further

* Corresponding author. Tel.: +86 15801515627.
E-mail addresses: wenbodu@buaa.edu.cn, wenbodu@mail.ustc.edu.cn (W.-B. Du).

0960-0779/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.chaos.2013.08.007

shutdown of selected lowly loaded nodes or highly loaded links can significantly restricts the propagation of cascading failures. Wu et al. [29] considered how the link-removal strategies (flow-based removal, betweenness-based removal and mix-based removal) affect the damage of cascading failures. It is shown that the mix-based removal can reduce the damage of cascade and delay the time of network breakdown.

Actually, adding links to existing networks before the onset of the cascading can also improve the ability of networks to defense cascading failures. Some previous studies have found that adding links can remarkably improve the dynamic behaviors on complex networks, such as information traffic [33], epidemic spreading [34,35]. Because of the cost, adding links is not practical than closing some selective links after the onset of cascades. However, in the design of initial networks (i.e., before the onset of cascades), the effect of different link-adding strategies can be different. It is valuable to find an optimal link-adding strategy which can maximally improve the initial network robustness against cascading failures. Thus in this paper, we compared three link-adding strategies: random linking strategy (RLS), high-betweenness linking strategy (HBS), and low-polarization linking strategy (LPS). It is found that HBS can enforce the robustness of networks against cascading failures more remarkably than RLS while the strongest network robustness is achieved by LPS.

The paper is organized as follows. In the next section we demonstrate the cascading model and link-adding strategies in detail. In Section 3, simulation results and correspondent theoretical analysis are provided. Finally, the work is summarized in Section 4.

2. The model

2.1. Network model

Since many real-world networks have been found to be scale-free, such as the Internet, WWW, metabolic networks [36,37] and airline routes [38]. Following common practices [39–44], we use the well-known Barabási–Albert (BA) model [45] in this paper. The BA model is generated by two general mechanisms (i.e., growth and preferential attachment) which exist in many real-life systems. At the original step, we start from a small amount of m_0 fully connected nodes and the network increases by adding a new node at each time step. This new node is connected preferentially to m ($m \leqslant m_0$) old ones in such a way that the probability of connecting to an existing node is proportional to the old node's degree. The BA scale-free network exhibits a power-law degree distribution, which consists of many low-degree nodes connected by a few high-degree nodes.

2.2. Cascading model

Firstly, we need a metric to measure the network robustness against cascading failures. We use the relative size $G = N'/N$ of the giant component to measure the extent of disconnection of the network, where N' is the size of the giant component after cascades and N is the initial network size. High G values correspond to robust networks, while low G values represent vulnerable networks.

Many previous studies have shown that the load of a node scales with its degree as [20,46–49]:

$$L_i \sim k_i^{\beta}, \tag{1}$$

where k_i is the degree of node i, and β relies on topological elements [20,46–48]. For the BA networks, $\beta \approx 1.6$ [46–48] and thus we set $\beta = 1.6$ in the following context. The node capacity is the maximum load that the node can handle, i.e., each node has a finite ability to process the load [9,19]:

$$C_j = (1+\alpha)L_j, \tag{2}$$

where α ($\alpha \geqslant 0$) is a tolerance parameter, and L_j is the load of node j in the initial network. Obviously, the tolerance parameter α denotes the ability of nodes to handle the load thereby resisting the flow perturbations. The larger the value of α is, the higher the security margin is. It is well known that the critical value of α is also an important metric of network robustness against cascades [49–51]. It is found that the cascade-induced breakdown of the scale-free network exhibits a phase transition phenomenon [50,51]. When $\alpha > \alpha_c$, the global cascading failure will not emerge. While in the case of $\alpha < \alpha_c$, the giant component disappears, reflecting the whole network collapses and the global cascading failure emerges. Thus, the critical point α_c is the lowest value of secure ability to avoid global cascading failures. Obviously, the smaller the value of α_c is, the more robust against cascades the network is.

The initial breakdown can occur at any node in the network. However, the eventual scale of damages must be greater when a heavily loaded node is broken [9]. In our model, we choose the worst case which the highest-load node is initially broken [9] and the local weighted flow redistribution rule [26,49] is adopted. The local weighted flow redistribution rule can be widely used in many real networked systems, such as transportation networks, communication systems and computer networks. For example, in the computer networks, if a server is broken, the load of the server could be redistributed to its nearest-neighbors. It is reasonable to preferentially distribute more loads to those higher-capacity neighbors to avoid further overloads. The load of the failed node i, denoted by F_i, will be directed to its non-failed nearest neighbors. The additional load ΔF_j received by the neighboring node j is proportional to its weight given by k_j^{θ}:

$$\Delta F_j = F_i \frac{k_j^{\theta}}{\sum_{l \in \Gamma_i} k_l^{\theta}}, \tag{3}$$

where θ ($\theta \geqslant 0$) is a tunable parameter, and Γ_i is the set of neighboring nodes of node i.

For node j, which is a neighbor of the failed node i, if $F_j + \Delta F_j > C_j$, then node j is collapsed, and node j and its links will be deleted simultaneously, inducing redistribution of the load of $F_j + \Delta F_j$ and potentially further breakdown of other fragile nodes. This process is continued until an equilibrium is finally obtained, i.e., when there are no more casualties. At the final stage, the current relative size of the giant component G is calculated.