Physica A 392 (2013) 2257–2264

Contents lists available at SciVerse ScienceDirect

Physica A

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

Mitigation strategies on scale-free networks against cascading failures

Jianwei Wang *

School of Business Administration, Northeastern University, Shenyang 110819, PR China

ARTICLE INFO

Article history:
Received 12 August 2012
Received in revised form 13 November 2012
Available online 9 January 2013

Keywords:
Cascading failure
Complex network
BA network
Mitigation strategy

ABSTRACT

According to the dynamic characteristics of the cascading propagation, we introduce a mitigation mechanism and propose four mitigation methods on four types of nodes. By the normalized average avalanche size and a new measure, we demonstrate the efficiencies of the mitigation strategies on enhancing the robustness of scale-free networks against cascading failures and give the order of the effectiveness of the mitigation strategies. Surprisingly, we find that only adopting once mitigation mechanism on a small part of the overload nodes can dramatically improve the robustness of scale-free networks. In addition, we also show by numerical simulations that the optimal mitigation method strongly depends on the total capacities of all nodes in a network and the distribution of the load in the cascading model. Therefore, according to the protection strength for scale-free networks, by the distribution of the load and the protection price of networks, we can reasonably select how many nodes and which mitigation method to efficiently protect scale-free networks at the lower price. These findings may be very useful for avoiding various cascading-failure-induced disasters in the real world and for leading to insights into the mitigation of cascading failures.

1. Introduction

Cascading failures induced by random failure or intentional attacks are common phenomena and can occur in many of the real-world networks including transportation networks, the Internet, the power grid, computer networks, and so on, which make up the cornerstone of modern society. In these networks, the failure of one or a few nodes can influence the entire network, often resulting in large-scale collapse in the whole network, for example, the largest blackout in US history took place on 14 August 2003 [1], the Western North American blackouts in July and August 1996 [2], and Internet collapse [3,4] caused by congestion.

Therefore, to avoid or at least reduce the cascading propagation, by studying the dynamic evolving mechanism of cascading failure in real-world networks, a number of important aspects of cascading failures have been discussed and many valuable results have been obtained in the literature including the models for describing cascade phenomena [5–13], the cascade control and defense strategies [14–20], cascading failures in real networks [21–28], the attack strategies [29–35], the robustness of coupled networks [36–45], and so on. In all studies cited above, most works on cascading failures focused only on the cascading modeling or how to protect a variety of networks. Thus far, to obtain the optimal robustness of networks against cascading failures, there are few works about the mitigation mechanism on the overload node and selecting what type of and how many nodes to adopt the mitigation strategy. However, in many infrastructure networks, for instance, traffic networks, the power grid, or the Internet, when the load on a node exceeds its capacity, there exist some measures (traffic

* Tel.: +86 411 81258693.
E-mail addresses: wdut@yahoo.cn, jwwang@mail.neu.edu.cn.

0378-4371/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
doi:10.1016/j.physa.2013.01.013

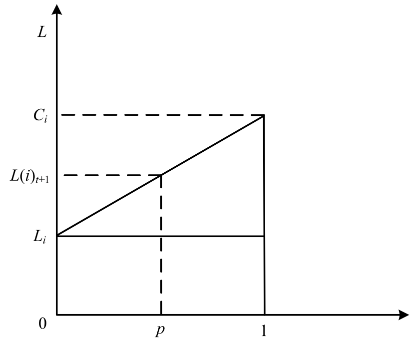

Fig. 1. The scheme illustrates the relation between the load $L(i)_{t+1}$ on node i at $t+1$ time and the random number p after node i adopted the mitigation strategy redistributes some load.

police can ease traffic flow on traffic networks) or replacement equipment to maintain its normal and efficient function to avoid the cascading propagation. Moreover, under the limitation of the total protection cost in realistic networks, the choice of the mitigation strategy on some key nodes is very important. Therefore, we will consider two above aspects and intend to fill this gap.

To this end, we address the optimal defense against cascading failures on scale-free networks. According to the cascading evolving process in real-life networks and the characteristics of the cascading model, we introduce a simple efficient mitigation mechanism for an overload node and develop two new methods to select nodes to adopt the mitigation strategy. By the normalized average avalanche size and the new unique robustness measure, we numerically investigate the efficiencies of the different mitigation strategies on enhancing the robustness of Barabási–Albert [46] scale-free networks against cascading failures. We demonstrate that with relatively minor modifications to the redistribution rule of the load on the overload nodes can significantly improve the network robustness against cascading failures. We compare the efficiencies of the different mitigation strategies and obtain how to select the key node to adopt the mitigation strategy according to some parameters in the cascading model. We hope these findings might shed some light on the mitigation and control of cascade failures and its propagation in real-world networks.

The rest of this paper is organized as follows: in Section 2 we describe the new mitigation strategy. In Section 3 we numerically investigates the effect of the mitigation strategy on improving the network robustness against cascading failures. Finally, some summaries and conclusions are shown in Section 4.

2. The mitigation strategy

In previous cascading models, the removal mechanism that the overload node will immediately fail is widely adopted. However, in the real-world networks, to avoid the propagation of cascading-failure-induced disasters, due to some protection measures or replacement equipments the overload nodes will be not removed from the network, and can redistribute some of the load on them to its neighboring nodes to maintain their normal and efficient functions. We know of little study that has attempted to model the above dynamic evolving mechanism to discuss the cascading phenomenon. To this end, we develop a mitigation strategy to fill this gap. For simplicity, we apply our method to a cascading model proposed in Refs. [5,8]. Our aim is to examine the effectiveness of the mitigation strategy and to find a better method to suppress cascading failures. In the cascading model, the initial load L_i of node i with the degree k_i is defined as $L_i = k_i^{\alpha}$, where $\alpha(> 0)$ is a tunable parameter which controls the strength of the initial load of node i. The capacity C_i of node i is proportional to its initial load and is defined as $C_i = (1+\beta)L_i$, where the parameter β is the tolerance parameter characterizing the tolerance of the network against cascading failures. After node i fails, the additional load ΔL_{ji} received by node j among its neighboring nodes is proportional to its initial load, i.e., $\Delta L_{ji} = L_i L_j / \sum_{m\in\Gamma_i} L_m$, where Γ_i represents the set of all neighboring nodes of node i.

Next, we in detail describe our mitigation strategy. In traffic networks, when a traffic intersection saturates, the traffic police can ease traffic flows to maintain its normal and efficient function. However, due to the restraints of some protection resources and some objective conditions, the node once again overloads may be removed from the network. Therefore, suppose that a node in a network at most adopt once mitigation strategy and mark the number that node i adopt the mitigation strategy by δ_i, i.e., for any node i in a network, $\delta_i \le 1$. We will choose some of the nodes to protect them by the mitigation strategy, and set $\xi_i = 1$ if node i can adopt the mitigation, otherwise set $\xi_i = 0$. Thus a next question arises: how to redistribute the load on an overload node with the mitigation strategy. To avoid the malfunction of the node and consider the limitation of the mitigation strategy, we think that after adopting the mitigation strategy, the load on the node should be lower than its capacity and be higher than its initial load. Thus, taking into account two above aspects, at $t+1$ time we define the load $L(i)_{t+1}$ on node i that adopt the mitigation strategy at t time as $L(i)_{t+1} = L_i + p(C_i - L_i)$ (see Fig. 1), where $L(i)_{t+1}$ represents the load on node i at $t+1$ time and the parameter p represents a random number in 0 and 1. Therefore, at t time the redistributed load $\Delta L_{i,t}$ by the node i adopted the mitigation strategy is defined as $\Delta L_{i,t} = L(i)_t - L_i - p(C_i - L_i)$