Physica A 388 (2009) 1731–1737

Contents lists available at ScienceDirect

Physica A

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

Edge-based-attack induced cascading failures on scale-free networks

Jian-Wei Wang *, Li-Li Rong

Institute of Systems Engineering, Dalian University of Technology, 2 Ling Gong Road., Dalian 116024, Liaoning, PR China

ARTICLE INFO

Article history:
Received 3 October 2008
Received in revised form 26 December 2008
Available online 20 January 2009

PACS:
89.75.Hc
89.75.-k
89.75.Fb

Keywords:
Cascading failure
Scale-free network
BA network
Attack
Breakdown probability

ABSTRACT

Most previous existing works on cascading failures only focused on attacks on nodes rather than on edges. In this paper, we discuss the response of scale-free networks subject to two different attacks on edges during cascading propagation, i.e., edge removal by either the descending or ascending order of the loads. Adopting a cascading model with a breakdown probability p of an overload edge and the initial load $(k_i k_j)^\alpha$ of an edge ij, where k_i and k_j are the degrees of the nodes connected by the edge ij and α is a tunable parameter, we investigate the effects of two attacks for the robustness of Barabási–Albert (BA) scale-free networks against cascading failures. In the case of $\alpha < 1$, our investigation by the numerical simulations leads to a counterintuitive finding that BA scale-free networks are more sensitive to attacks on the edges with the lowest loads than the ones with the highest loads, not relating to the breakdown probability. In addition, the same effect of two attacks in the case of $\alpha = 1$ may be useful in furthering studies on the control and defense of cascading failures in many real-life networks. We then confirm by the theoretical analysis these results observed in simulations.

1. Introduction

Complex networks [1] such as the Internet, the electrical power grid, and the transportation networks, are an essential part of modern society. Network robustness [1–13] subject to random or intentional attacks has been one of the most central topics in network safety. Therefore, cascading failures on complex networks have been highly concerned and widely investigated.

Cascading failures refer to the subsequent failure of other parts of a network induced by the failure of or attack on only a few nodes (or edges). It can happen in many infrastructure networks. Some famous accidents, such as the largest blackout in US history took place on 14 August 2003 [14], the Western North American blackouts in July and August 1996 [15,16], and the Internet collapse caused by congestion [5,17], are believed by some researchers to be typical examples of cascading failures.

Some aspects of cascading failures in complex networks have been discussed in literature, including the cascade control and defense strategy [14,18–22], the model for describing cascade phenomena [23–29], the analytical calculation of capacity parameter [26,27,30–33], and so on. However, in all studies cited above, most previous works on cascading failures only consider attacks on nodes rather than on edges. Attacks on edges are as important for the network security as those on nodes, and therefore deserve a careful investigation.

Following a recent work of Wang and Chen [26], we also assume the initial load of an edge ij to be $(k_i k_j)^\alpha$ with k_i and k_j being the degrees of the nodes connected by the edge, where α is a tunable parameter and governs the strength of the edge load. Since there exist a certain degree monitoring and control in most real-life complex networks, not all overloaded edges will be removed from networks. Therefore, we propose a new concept, i.e., the breakdown probability of an overload

* Corresponding author. Tel.: +86 411 81258693.
E-mail address: wdut@yahoo.cn (J.-W. Wang).

0378-4371/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.physa.2009.01.015

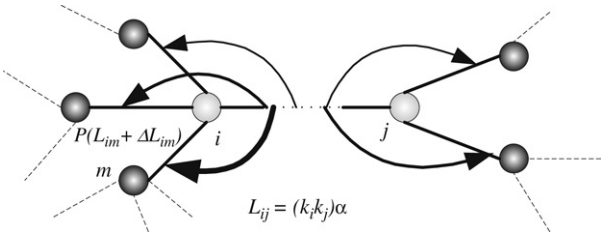

Fig. 1. The scheme illustrates the load redistribution triggered by an edge-cut-based attack and the removal mechanism with the breakdown probability $P(L_{im} + \triangle L_{im})$ of a neighboring edge im of the breakdown edge ij.

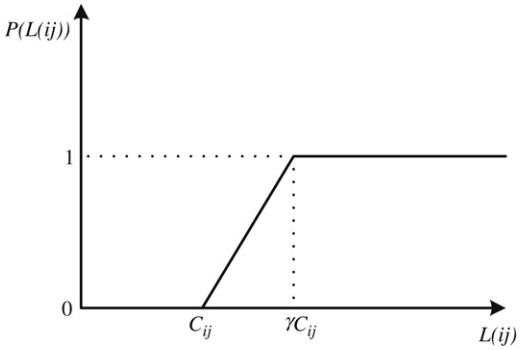

Fig. 2. Illustration of the relation between the removal probability $P(L(ij))$ and the load $L(ij)$ of an edge ij.

edge, by which we describe the removal mechanism of an overload edge. Adopting two attacks on edges, we investigate cascading reaction behaviors on the Barabási—Albert (BA) [34] modeling networks. We numerically find some interesting and counterintuitive results in the cascading model, of which one unexpected finding is that attacking the edges with the lowest loads is more harmful than attacking on the ones with the highest loads in the case of $\alpha < 1$. In addition, we verify these results by theoretical analysis.

The rest of this paper is organized as follows: in Section 2, we describe the cascading model in detail. The effects of two attacks for network robustness are discussed based on BA networks in Section 3. In Section 4, the numerical simulations are verified by theoretical analysis. Finally, some summaries and conclusions are shown in Section 5.

2. The model

Here we focus on cascading failures triggered by the removal of a single edge. If an edge has a relatively small load, its removal will not cause major changes in the balance of loads, and subsequent overload failures are unlikely to occur. However, when the load at an edge is relatively large, its removal is likely to affect significantly loads at other edges and possibly to start a sequence of overload failures and eventually a large drop in the network performance.

We assume the initial load of an edge ij to be $L_{ij} = (k_i k_j)^{\alpha}$ with k_i and k_j being the degrees of the nodes connected by the edge. The additional load ΔL_{im} received by edge im after the collapse of an edge ij is proportional to its initial load, i.e., $\Delta L_{im} = L_{ij} L_{im}/(\sum_{a\in\Gamma_i} L_{ia} + \sum_{b\in\Gamma_j} L_{jb})$, where Γ_i and Γ_j represent the sets of the neighboring nodes of the node i and j, respectively. Since edge capacity on real-life networks is generally limited by cost, it is natural to assume that the capacity C_{ij} of an edge ij is proportional to its initial load for simplicity: $C_{ij} = \beta L_{ij}$, where the constant $\beta(\geq 1)$ is a tolerance parameter. In our study, to accord with the positive proportion correlation between the initial load of an edge ij and $k_i k_j$, we set $\alpha > 0$. Fig. 1 illustrates the effect of an edge-cut-based attack for its neighboring edges.

In most real-life networks, owing to a certain protection strategy, an overloaded edge is not always removed. Therefore, we propose a new concept of the breakdown probability of an overload edge to reflect the removal mechanism. Taking the limit of the protection capacity into account, we assume that an edge ij has a removal threshold, i.e., the removal probability $P(L(ij))$ of the overload edge ij is equal to 1 when $L(ij) \geq \gamma C_{ij}$, where $L(ij)$ represents the load of the edge ij and $\gamma(\geq 1)$ is a tunable parameter. The expression of the breakdown probability $P(L(ij))$ of an edge ij reads (See Fig. 2),

$$P(L(ij)) = \begin{cases} 0, & C_{ij} > L(ij) \\ \dfrac{L(ij) - C_{ij}}{\gamma C_{ij} - C_{ij}}, & C_{ij} \leq L(ij) < \gamma C_{ij} \\ 1, & \gamma C_{ij} \leq L(ij). \end{cases} \tag{1}$$

In our cascading model, the damage caused by attacking a single edge ij is quantified in terms of the avalanche size S_{ij}, namely, the number of broken edges after the cascading process is over. It is evident that $0 \leq S_i \leq N_{edge} - 1$, where N_{edge} denotes the