Physica A 460 (2016) 139–151

Contents lists available at ScienceDirect

Physica A

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

Robustness of single and interdependent scale-free interaction networks with various parameters

Shuai Wang, Jing Liu *

Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, Xidian University, Xi'an 710071, China

HIGHLIGHTS

- Robustness of scale-free networks with various parameters is systematically studied.
- Robustness measures against malicious and random attacks are compared.
- Robustness of interdependent networks is also studied.
- Positive correlation exists in robustness against node attacks and parameters.
- The positive correlation also exists in interdependent networks.

ARTICLE INFO

Article history:
Received 22 September 2015
Received in revised form 27 January 2016
Available online 6 May 2016

Keywords:
Scale-free network
Robustness
Assortativity
Scaling exponent

ABSTRACT

The robustness of scale-free networks has attracted increasing attentions recently. It has been shown that scale-free networks are tolerant to random failures but fragile under malicious attacks. However, most existing studies focus on scale-free networks with fixed exponent (around 3) and assortativity (around 0), and the relationship between robustness and these parameters has not been studied systematically. Therefore, in this paper, we study the change of robustness along with different parameters, including scaling exponent and assortativity, of scale-free networks; moreover, the robustness of interdependent networks is also studied. In the experiments, synthetic single scale-free networks with varying scaling exponents are constructed and adjusted to fix assortativity. Several measures are adopted to estimate the robustness of networks under malicious and random attacks. Then, interdependent networks with varying parameters are constructed and their robustness against malicious attacks is studied. The results show that there is a positive correlation between robustness against node attacks and the scaling exponent as well as assortativity, and the positive correlation also exists in interdependent networks.

1. Introduction

The topology of interaction networks has been widely employed in modeling of systems with complex structures [1,2]. One of the significant properties of a network is the tolerance to failures or attacks, namely the robustness. In daily life, we have witnessed many cases like failure on part of financial networks may cause economic crises or the breakdown of some routers in the Internet leads to interruption in a large area etc. It is important to keep a networked system operative even when failures occur, which is significant to power grid, the gene networks, and so on. Therefore, the research of network robustness is practical and meaningful.

* Corresponding author.
E-mail addresses: neouma@mail.xidian.edu.cn, neouma@163.com (J. Liu).

http://dx.doi.org/10.1016/j.physa.2016.04.035
0378-4371/

In practice, systems with power-law degree distribution are quite common. As Adamic et al. stated in Ref. [4], as an important part of complex networks, the scale-free network [2,3] depicting power-law feature has attracted much attention. Previous studies show that scale-free topology has strong toleration to random attacks compared with other models. But when the attack is intentional, i.e. attack the most important member (node or edge) of the network, scale-free networks may crash down in a short time. In fact, scale-free networks have an evident feature of hubs-existing, which means a small part of nodes could have much higher degree than others. Under malicious attacks, the crash of hubs causes much loss in connectivity, and the network will get separated quickly. The scaling exponent (α) is the parameter to evaluate the degree distribution of specific network, and the probability of a vertex having degree k is $p(k) \propto k^{-\alpha}$. Previous studies show that α lies in the range $2 < \alpha < \infty$ in natural systems, and various networks may possess different α [5]. A preferential attachment method proposed by Barabási–Albert (BA model) [2,3] is popular in constructing networks with power-law degree distribution.

For further describing the structure of networks, the propensity of similar degree vertices connected is referred as the assortativity (r) [6]. If r is positive, nodes with almost the same degree are inclined to make connections, and vice versa. In most of previous studies, scale-free networks were generated using the BA model, which generates the networks with fixed parameters $\alpha \approx 3$ and $r \approx 0$. Limited by this model, the correlation between the robustness and those parameters is still unclear. Therefore, in this paper, we focus on the robustness of scale-free networks with different α and r, and both malicious and random attacks are studied.

In our daily life, a large system often contains several networks, which are associated with each other. For example, the shutdown of power station led to the failure of the Internet communication, which in turn caused further breakdown of power stations on 28 September, 2003, Italy [7]. In fact, practical networks often present much dependency on one another. Buldyrev et al. proposed the model of interdependent networks in Ref. [7] and mainly focused on random failures on nodes. Besides the robustness on single networks, in this paper, we also study the effect of network parameters on the robustness of independent networks. Different scale-free networks with various parameters are constructed as interdependent pairs, and the malicious nodal attacks are studied.

In the experiments, we find both single and interdependent scale-free networks with higher scaling exponents and assortativity tend to perform more robust against malicious nodal attacks. When malicious attacks are conducted on edges, both parameters do not show clear relationship with robustness. Due to the excellent resistance to random failures of scale-free networks, the change of network parameters has little effect on the robustness against random attacks.

The rest of this paper is organized as follows. Section 2 introduces the measures of robustness on single and interdependent networks. Section 3 gives the generation method of scale-free interaction networks. Experiments are shown in Sections 4 and 5. Discussions and conclusions are presented in Section 6.

2. Robustness measures

Usually, a network is robust if it still keeps functional under attacks, either random or malicious. There are many ways to define robustness of a network, and connectivity was core to define robustness in early studies, such as the graph connection [8], super connectivity [9] and conditional connectivity [10], but proved to be unilateral. Recently, the fraction of maximum cluster after attacking has become the basis for defining the robustness. Schneider et al. proposed the well-known robust measure R in terms of the critical fraction of attacks on nodes [11], which was extended to attacks on edges by Zeng et al. in Ref. [12]. In addition, betweenness centrality [13,14] is also a common-used measure of robustness.

In single scale-free networks, we conduct malicious and random attacks. As to malicious attacks, both of nodes and edges are considered in the experiments. The degree and betweenness centrality are adopted to evaluate the importance of attacked targets. For random attacks, node-random as well as edge-random is adopted, the measures are calculated individually.

2.1. Measures for single networks

A scale-free network can be represented as a graph $G = (V, E)$, where $V = \{1, 2, 3, \ldots, N\}$ is the set of N nodes, and $E = \{e_{ij} | i, j \in V, i \neq j\}$ is the set of M links. In terms of degree, we focus on node degree first, which is equal to the number of links a node connects to. Malicious attacks are conducted in a decreasing order of node degree. The measure R is defined as,

$$R = \frac{1}{N} \sum_{Q=1}^{N} s(Q) \tag{1}$$

where Q stands for the number of nodes being attacked, and $s(Q)$ stands for the fraction of the largest connected component after removing Q nodes. The normalization factor $1/N$ ensures networks with different nodes could be compared.

Based on the node degree, if e_{ij} is the link between vertex i and vertex j, then k_{ij} is the edge degree of e_{ij}

$$k_{ij} = \sqrt{k_i \times k_j} \tag{2}$$