Physica A 424 (2015) 248–253

Contents lists available at ScienceDirect

Physica A

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

New attack strategies for complex networks

Tingyuan Nie [a,*], Zheng Guo [a], Kun Zhao [a], Zhe-Ming Lu [b]

[a] Communication & Electronic Engineering Institute, Qingdao Technological University, Qingdao 266033, China
[b] School of Aeronautics and Astronautics, Zhejiang University, Hangzhou 310027, China

HIGHLIGHTS

- We propose two new attack strategies based on both degree and betweenness.
- The proposed strategies are more efficient than the traditional ones (ID and RD).
- The WS small-world network behaves more sensitive to the proposed strategies.
- The attack efficiency of RDB and IDB strategy is improved by 20% and 40%.

ARTICLE INFO

Article history:
Received 13 September 2014
Received in revised form 12 December 2014
Available online 14 January 2015

Keywords:
Complex networks
Attack strategy
Invulnerability
Degree
Betweenness

ABSTRACT

The invulnerability of complex networks is an important issue in that the behavior of scale-free network differs from that of exponential network. According to the structural characteristics of the networks, we propose two new attack strategies named IDB (initial degree and betweenness) and RDB (recalculated degree and betweenness). The strategies are originated from ID (initial degree distribution) and RD (recalculated degree distribution) strategies in which attacks are based on initial structural information of a network. The probability of node removals depends on a new metric combining degree centrality and betweenness centrality. We evaluate the efficiency of the proposed strategies on one real-world network and three network models. Experimental results indicate that the proposed strategies are more efficient than the traditional ID and RD strategies. Specially, the WS small-world network behaves more sensitive to the proposed strategies. The attack efficiency of RDB strategy is improved by 20% to RD strategy, and IDB strategy is improved by 40% to ID strategy.

1. Introduction

In recent decades, complex networks have received much attention. A large number of complex systems in the real world and human society can be described as complex networks, ranging from biology to medicine, sociology and engineering. The nodes in a network represent individuals, while edges represent the relationship between individuals. One of the most important phenomena found in the literature is that some networks such as the World Wide Web [1], the Internet [2], airplanes networks [3], metabolic networks [4], protein–protein networks [5], and ecology networks [6,7], are different from exponential random networks [8]. All of them have a power-law degree distribution $P(k) \sim k^{-\gamma}$ with an exponent γ ranges in the scope of [2,3]. The essential feature of network with power-law degree distribution (so called scale-free network) is extremely heterogeneous.

* Correspondence to: Communication & Electronic Engineering Institute, Qingdao Technological University, No. 11, Fushun Road, Qingdao 266033, China. Tel.: +86 53268052206.
E-mail address: tynie@qtech.edu.cn (T. Nie).

http://dx.doi.org/10.1016/j.physa.2015.01.004
0378-4371/

In real life, a network or system is not always safe. The threats of complex networks may come from two aspects: random failure and attack. The random failure damages nodes (edges) with uniform probability, which can be seen as a simple abstraction of the successive error in a complex network. The attack damages nodes (edges) in the descending order of their importance in prerequisite of knowing the global information of the network. For the goal of protecting networks or systems against attacks or failures, enormous interest and effort has been devoted to the study of the invulnerability of complex networks. It shows that scale-free networks behave higher tolerant to failure but more vulnerable to attack than exponential networks [9–11].

In order to evaluate the invulnerability of complex networks, several measurements have been proposed. The popular one is the existence of the giant component [9–12]. In complex networks, the largest connected subgraph is known to have a size of the order of the entire network, and accordingly called "giant component" [12]. The network percolates if the giant component exists, indicating that the general connectedness of the network is maintained. Holme et al. used global efficiency to evaluate how well a system works before and after node removals [12,13]. Albert et al. used characteristic path length of the network to evaluate the robustness of complex networks [9,12]. Annibale et al. used the integrity to measure the resilience of network against attacks constrained by node degree dependent cost and limited resources [14]. Eckhoff and Mörters analyzed the invulnerability of scale-free networks from the variation of the asymptotic degree distribution, the largest degree, and the typical distance of the network [15].

The attack strategies to complex networks were proposed based on network information such as degree centrality [9–11,13,16], betweenness centrality [12,17,16], eigenvector [18,16], closeness centrality [16,19], entropy [20], second-degree neighbors [21], and so on. In them, Holme et al. studied the behavior of complex networks subject to attacks on nodes and edges. They proposed four different attack strategies: the initial degree distribution (ID) removal, the initial distribution of betweenness centrality (IB) removal, the recalculated degree distribution (RD) removal, and the recalculated betweenness centrality (RB) removal. They measured the invulnerability of complex networks using the relative size of the giant component and the average inverse geodesic length [12]. Due to different structural features and dynamics, the discrepancy of invulnerabilities of different complex networks is very large. The small-world networks have strong resilience against the frequently-used attack strategies, such as random attack, ID, IB, RD and RB strategies.

To explore the fragility of the complex network more deeply, we propose two new attack strategies based on the metric combining degree centrality and betweenness centrality. We use the average inverse geodesic length and the relative size of the giant component to evaluate the efficiency. Furthermore, we compare different behaviors of complex networks under the new proposed attack strategies.

2. Proposed attack strategies

Complex networks can be divided into exponential networks and scale free networks according to the degree distribution [22]. In the work, we use ER random network model [22], WS small-world network model [23,24], BA scale-free network model [25,26], and real-world power grid network [22] for the evaluation. The attack strategies are constructed based on local information or global information of the network [12,27,28]. It has shown that the invulnerability of networks behaves different to various attack strategies [29]. Notably, the WS small-world network behaves more robust to selective attacks due to its narrow degree distribution [30]. There are numerous vertices with the same degree which implies it may be inefficient using only one metric (degree) in the process. We show the correlation between the degree and the betweenness in Fig. 1. The range of betweenness distribution with the same degree for different networks diversifies. In order to improve the attack efficiency, we propose two new attack strategies that take into account both degree and betweenness, which are called IDB (initial degree and betweenness) strategy and RDB (recalculated degree and betweenness) strategy. We assign a value to each node, which represents the probability that a node becomes inactive under attacks. The definition is shown in formula (1).

$$\begin{aligned} p_{k_i} &= \left(\frac{k_i}{\sum_{i=1}^{N} k_i}\right)\alpha + \left(\frac{B_i}{\sum_{i=1}^{N} B_i}\right)\beta \\ p'_{k_i} &= \left(\frac{k'_i}{\sum_{i=1}^{N} k'_i}\right)\alpha + \left(\frac{B'_i}{\sum_{i=1}^{N} B'_i}\right)\beta. \end{aligned} \tag{1}$$

Here, p_{k_i}, p'_{k_i} represent the probabilities that a node be removed by IDB and RDB strategies, k_i, B_i, k'_i, B'_i are initial degree, initial betweenness, recalculated degree, and recalculated betweenness. In our methods, attacks are based on the first order (degree centrality), then the second order (betweenness centrality). We set two coefficients α, β for degree centrality and betweenness centrality to adjust their importance. We will show the meaning of the coefficients in latter experiment. Thus