Physica A 448 (2016) 144–153

Contents lists available at ScienceDirect

Physica A

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

A comparative analysis of network robustness against different link attacks

Boping Duan, Jing Liu [*], Mingxing Zhou, Liangliang Ma

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

HIGHLIGHTS

- Analyses of network link robustness maintaining the number of edges are conducted.
- Four types of networks are used as the initial networks.
- Measures for optimized networks starting from different initial ones are similar.
- Topologies of optimized networks may be different.
- Optimized networks obtained by one link attack may not robust against other ones.

ARTICLE INFO

Article history:
Received 6 January 2015
Received in revised form 10 October 2015
Available online 23 December 2015

Keywords:
Network robustness
Robustness measures
Link attacks

ABSTRACT

Recently, the study of optimizing network robustness has attracted increasing attentions, and the constraint that every node's degree cannot be changed is considered. Although this constraint maintains the node degree distribution consistently in order to reserve the structure of networks, it makes the network structure be lack of flexibility since many network structure always transform in the modern society. Given this consideration, in this paper, we analyze the robustness of networks through setting a new constraint; that is, only the number of edges should be unchanged. Then, we use the link-robustness index (R_l) as the measure of the network robustness against either random failures or intentional attacks, and make a comparative analysis of network robustness against different types of link attacks. Moreover, we use four types of networks as initial networks, namely scale-free networks, random networks, regular networks, and small-world networks. The experimental results show that the values of robustness measures for the optimized networks starting from different initial networks are similar under different link attacks, but the network topologies may be different. That is to say, networks with different topologies may have similar robustness in terms of the robustness measures. We also find that the optimized networks obtained by one link attack may not robust against other link attacks, sometimes, even weaker than the original networks. Therefore, before building networks, it is better to study which type of link attacks may happen.

1. Introduction

The infrastructure of complex systems plays a significant role in our daily life such as airports, power grids, transportation systems, World Wide Wed, and disease control systems, which make the life of people more convenient and glorious. These infrastructures can be modeled by networks with complex topologies [1–4], however, they may suffer from assaults

[*] Correspondence to: P.O. Box 224, Xidian University, Xi'an 710071, China. Tel.: +86 29 88202661.
E-mail addresses: neouma@mail.xidian.edu.cn, neouma@163.com (J. Liu).

http://dx.doi.org/10.1016/j.physa.2015.12.045
0378-4371/© 2015 Elsevier B.V. All rights reserved.

that are random or intentional [5]. Many processes happening in networks could be severely impacted if the network structures are injured [6,7]. A lot of examples of such processes in nature and society involve the spread of epidemics [8,9], synchronization [10–12], random walks [13,14], traffic [15,16], and opinion formation [17,18]. Therefore, the robustness of different network structures has been studied intensively in the past decade [19–28].

Recently, a measure (R) [29] to evaluate the robustness of networks is widely used, which was designed for malicious attacks on nodes. Nodes and edges are two major components in networks. Many existing studies focused on improving the robustness of networks against node attacks. The optimized network structure embrace higher robustness than the original one, but cannot make sure that the robustness of structures is better than the original one against malicious link attacks. We know that nodes and edges are equally important. In Ref. [30], a new measure (R_l) under link attacks was proposed. In this paper, we re-name R as R_n to represent node attacks. Most of the existing work on improving network robustness requires that the degree of each node is kept unchanged. However, in reality, sometimes we only need to keep the number of edges and nodes be unchanged.

Therefore, in this paper, we relax the requirement that the degree of each node is kept unchanged, and use the requirement that the number of nodes and links should be kept unchanged instead. We use R_l to evaluate the robustness of networks against three link attacks, and four types of networks are studied, including scale-free networks, small-world networks, random networks, and regular networks. In order to construct robust networks for each of these four types of networks which can be robust against different link attacks, we also design a simple heuristic method to optimize R_l. The experimental results show that the values of R_l for the optimized networks starting from different initial networks are similar under different link attacks, but the network topologies may be different. We also find that the optimized networks obtained by one link attack may not robust against other link attacks, sometimes, even weaker than the original networks.

The rest of this paper is organized as follows. In the next section, we describe the robustness measures and the link attacks used. Section 3 reports the experimental results. Finally, Section 4 summarizes the work in this paper.

2. Robustness measures and link attacks

In Ref. [29], Schneider et al., adapting from the percolation theory, proposed a measure R to evaluate the network robustness against node attacks. R takes the size of the largest connected component into account during the process of removing nodes,

$$R = \frac{1}{N}\sum_{P=1}^{N} S(P) \tag{1}$$

where $S(P)$ denotes the fractions of nodes in the largest connected cluster after P nodes are removed, and N is the number of nodes in the network.

Based on R, in Ref. [30], Zeng et al. proposed a measure (R_l) to evaluate the robustness of networks against link attacks,

$$R_l = \frac{1}{E}\sum_{Q=1}^{E} S(Q) \tag{2}$$

where E denotes the number of edges in the network, and $S(Q)$ is the fractions of nodes in the largest connected cluster after Q links are removed. In fact, R and R_l are defined similarly, however, the types of robustness they evaluate are different. Next, we use R_l to study the network robustness against link attacks, and re-label R as R_n to stand for node attacks.

To build a robust network, of course, it should have a strong ability to endure the most destructive attack. In terms of link attacks, the most destructive attack is the one breaking the "key" links. As indicated in Ref. [27], we detect the size of the giant component to estimate how the network is ruined after these "key" links are removed one by one. Here, we mainly choose three commonly used link attacks to carry out experiments, i.e., the random edge attack (RnE), the edge-betweenness attack (EB), and the degree product attack (DP). RnE denotes that all edges are treated equally and chosen randomly to attack. The edge-betweenness of a link means that the fraction of shortest paths that pass through it [31]. In this strategy, the edge with the highest edge-betweenness is removed in each step. The degree product of an edge is simply computed by multiplying the degree of the two end nodes. In this strategy, the link with the largest degree product is removed in each step. We study the change of the relative size of the giant component $S(Q)$ with the fraction of links Q removed by different strategies on four types of networks in Fig. 1.

As can be seen, for these networks, the most destructive strategy is the EB attack because $S(Q)$ decreases much faster in this case. Removing these links will force a large number of nodes to look for other shortest path to communicate with each other. Gradually, the link with the highest edge-betweenness will be in the only path connecting many nodes. At this time, cutting this link will isolate these nodes, and the network will be destructed completely. In the BA, ER, and small-world networks, the damage caused by the DP is more serious than the RnE, however, the contrary is the case in the regular networks. Therefore, before building networks, we should put emphasis on the EB attack. Of course, sometimes we should consider which type of link attacks may happen according the current state.