Physica A 451 (2016) 623–631

Contents lists available at ScienceDirect

Physica A

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

Evolution of network robustness under continuous topological changes

Liangliang Ma, Jing Liu *, Boping Duan

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

HIGHLIGHTS

- The iterative attack/defense model on links is proposed.
- The performance of different attack/defense strategy is intensively evaluated.
- High-degree and high-centrality attacks are effective node attack strategies.
- The best edge attack is removing edges with the highest edge-betweenness.
- Connecting low centrality nodes can increase R, but cannot enhance R_l.

ARTICLE INFO

Article history:
Received 12 May 2015
Received in revised form 24 November 2015
Available online 8 February 2016

Keywords:
Network robustness
Iterative attacks and defenses
Malicious attacks

ABSTRACT

Many networks in reality face a dynamic iteration of attacking and defending, in which attackers and defenders take turns to destroy and replenish networks. The framework of iterative attacking and defending has been introduced, and Kim and Anderson gave an iterative model with much finer granularity and empirically studied three attack/defense strategies on nodes. However, in real-world networks, the failure can also occur on links. We therefore extend the iterative attack/defense strategies to links and apply the robustness measure R and the link-robustness R_l to evaluate the performance of each attack/defense strategy. Through intensive experiments on several well-known networks, the defense strategy of connecting nodes with low-centrality is effective enough to maintain network connectivity and increase the network robustness R against targeted node attacks, but it cannot enhance the link-robustness R_l against malicious link attacks during the iterative rounds. Significantly, on two real-world networks, this strategy is perfect for simultaneously enhancing the robustness R and the link-robustness R_l.

1. Introduction

In modern society, the security and resilience of real-world networks is of great importance. Systems such as Internet, electrical power grids, and transportation systems often suffer from failures and attacks [1–3]. Albert et al. in Ref. [4] modeled selective attacks on networks in which an attacker targets high-order nodes to destroy the connectivity. Many existing literatures theoretically and numerically studied network robustness against random failures or targeted attacks in the single-shot case [5–10]. As well-known, Schneider et al. [7] proposed the robustness measure R against malicious node attacks based on the percolation theory and Zeng et al. [9] extended R to the link-robustness R_l against malicious link attacks. And Tanizawa et al. [11] focused on the network topology and obtained that the network with a bimodal degree distribution has strong robustness against simultaneous targeted and random node attacks.

* 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.2016.01.088
0378-4371/

However, many networks in reality face a dynamic iteration of attacking and defending, in which attackers and defenders take turns to destroy and replenish networks. In Ref. [12], Anderson et al. introduced the framework of repeated attack and defense based on the evolutionary game theory [13]. The attacker's goal is to destroy network connectivity, which can be evaluated by the size of the largest connected cluster (LCC) in the networks, while the defender's aim is to rebuild network and increase the robustness of network [12]. Kim et al. in Ref. [14] extended the repeated model by introducing the cost required to perform network operations and empirically studied three attack and defense strategies on nodes. Kim's iterative attack and defense operation is defined as follows: at each attack round, an attacker removes the existing n nodes from network according to his attack strategy, then, at each defense round, a defender adds n nodes to network according to his defense strategy. Through analyzing the changes in terms of the size of LCC, which sort of attack/defense strategies might be effective was investigated. However, Kim's work [14] has three shortcomings.

(1) Only the iterative attack and defense on nodes were modeled, and the situation in which failures or attacks occur on links was ignored. In many networks, enhancing tolerance against malicious node attacks cannot guarantee the improvement of the robustness against link attacks [9].
(2) The size of LCC was used to investigate which strategy is more effective. The size of LCC can only evaluate network connectivity in a simple way, while recent advances about network robustness have provided a lot of effective robustness measures [7–9].
(3) The link density of networks is allowed to be decreased during iterative rounds. However, when the link density is changed, the robustness is definitely changed. In real-world networks, it is better to keep both the number of nodes and links be unchanged. For example, links in air-transportation networks represent airlines which are related to the actual requirement of transportation. If some airlines are canceled without giving other choices, the real requirement may not be satisfied.

To cope with the above points, in this paper, we studied three attack/defense strategies on nodes and three attack/defense strategies on links, and propose a modified iterative model, in which both the total number of nodes and links are kept invariant. One of our objectives is to find the best attack and defense strategies on nodes or edges. By analyzing the changes in the size of LCC, we validate the performance of attack/defense strategies on Barabási–Albert scale-free network [15]. The experimental results show that the best strategy of edge replenishment for maintaining network connectivity is adding edges between two nodes with low centrality; either high-degree attack or high-centrality attack is effective node attack strategy and the best edge attack is removing edges with the highest edge-betweenness.

Another objective is to study how attack/defense strategies affect the network robustness through observing changes in the robustness R and the link-robustness R_l of networks. We classify four iterative models to simulate continuous topological changes and test them on four different synthetic networks and two real-world networks topologies with different density: Erdős–Rényi random network [16], Watts and Strogatz small-world network [17], two Barabási–Albert scale-free networks [15], and two real-world networks [18,19]. The results show that the strategy of connecting low centrality nodes can increase the tolerance of network against malicious node attacks, but cannot enhance the network robustness against malicious link attacks. Significantly, in two real-world networks, this defense strategy can be effective enough to increase the network robustness against both intentional node attacks and link attacks.

The rest of this paper is organized as follows. Section 2 presents the details of two well-known robustness measures. The iterative attack and defense model is introduced in Section 3. The experiments on the performance of attack/defense strategies and the evolution of network robustness are given in Section 4. Finally, conclusions are given in Section 5.

2. Network robustness measures

The network robustness of various real-life systems is of great importance and has been studied intensively in the past decades [20–24]. Many existing works proposed a lot of metrics of robustness, such as the critical fraction p_c [5,6], the robustness R [7], the link-robustness R_l [9], natural connectivity [22] et al. The robustness measures widely used are designed based on the percolation theory, including the robustness R and the link-robustness R_l, and these well-known measures will be employed to analyze the evolution of network robustness in this work. Thus, the details of these robustness measures are first introduced as follows.

In Ref. [7], Schneider et al. considered the size of the largest component during all possible malicious attacks and proposed the robustness measure R

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

where N is the number of nodes in the network and $s(Q)$ is the fraction of nodes in the largest connected cluster after removing Q nodes. The normalization factor $\frac{1}{N}$ ensures that the robustness of networks with different sizes can be compared. The larger the value of R is, the more robust the network is against malicious node attacks.