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.

© 2016 Elsevier B.V. All rights reserved.

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/© 2016 Elsevier B.V. All rights reserved.

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.

The robustness measure R only takes targeted attacks on nodes into consideration. In Ref. [9], Zeng et al. extended the robustness measure R to evaluate network robustness against link attacks and proposed the link-robustness R_l

$$R_l = \frac{1}{M}\sum_{P=1}^{M} s(P) \tag{2}$$

where M is the number of edges and $s(P)$ is the fraction of nodes in the largest connected cluster after removing P links. The normalization factor $\frac{1}{M}$ also ensures that the robustness of network with different sizes can be compared. The larger the value of R_l is, the more robust the network is against malicious link attacks.

The existing results show that scale-free networks are strongly tolerant against random failures, while they are vulnerable under malicious attacks [4]. Therefore, in this paper, we just take malicious attacks into account in experiments to analyze the network robustness under continuous topological changes. Respectively, the robustness R is calculated based on high degree adaptive attack on nodes, where the node with highest degree is removed in each attack. And the link-robustness R_l is calculated based on the highest edge-betweenness attack strategy on edges.

3. Iterative attack and defense model

A network can be represented as a graph $G = (V, E)$, where $V = \{1, 2, 3, \ldots, N\}$ is the set of nodes, and $E = \left\{e_{ij} | i, j \in V, i \neq j\right\}$ is the set of M links. In this paper, the undirected and unweighted networks are considered.

In the framework of iterated attack and defense [12], an attacker's goal is to maximize the disruption to the network while a defender tries to minimize it. In this paper, we assume that the attacker and the defender have sufficient ability to destroy or repair the network. Unlike Kim and Anderson's model [14], we allow the defender rewires the existing edges in the network; it means that both the total number of nodes and edges remain invariant, while the network topologies do change. The network topology is changed by only one removal and one addition of node or edge. Here, we introduce the following strategies of removal and addition on nodes and edges. The performance of each strategy is measured by changes of the size of *LCC* in Section 4.

3.1. Attack and defense on nodes

In an attack phase, we assume that one node with degree n selected from the graph according to attack strategies is removed, while n edges connecting the node with the remaining nodes are also removed. In a defense phase, a new node is added to connect to m existing nodes selected according to defense strategies, where m is the average degree of the original graph. If $m < n$, each $n - m$ remaining edge is connected from a selected node to another selected node following defense strategies, neither creates self-connections nor double connections. If $m \geq n$, only n edges of the added node are linked to n existing nodes. For $n = 0$, a new node immediately becomes an isolated node after it is added. This is applied to all following defense strategies.

3.1.1. Attack strategies

(1) Random removal: Select a node randomly from the network.
(2) High-degree removal: Select the node with the highest degree from the network.
(3) High-centrality removal: Select the node with the highest node-betweenness centrality from the network. Betweenness centrality $b_n(u)$ is calculated for node u as the proportion of shortest paths between all node pairs in the graph that pass through u.

$$b_n(u) = \sum_{s\neq u, t\neq u\in V} \frac{\sigma_{s,t}(u)}{\sigma_{s,t}} \tag{3}$$

where $\sigma_{s,t}$ is the total number of shortest paths from source node s to destination node t, and $\sigma_{s,t}(u)$ is the number of shortest paths from source node s to destination node t which actually pass through node u.

3.1.2. Defense strategies

(1) Random replenishment: add a new node to the network such that the node is connected with m new edges to m randomly selected different nodes.
(2) Preferential replenishment: add a new node to the network such that the node is connected with m new edges to m different nodes with the probability proportional to their degree (*i.e.,* the node is connected to an existing node u with the probability $p(u) = d(u) / \sum_{v\in V} d(v)$ where $d(u)$ is node u's degree).
(3) Balanced replenishment: add a new node to the network such that the node is connected with m new edges to m different nodes with the probability proportional to their node-betweenness centrality (*i.e.,* the node is connected to an existing node u with the probability $p(u) = (b_n(u) + \varepsilon)^{-1} / \sum_{v\in V} (b_n(v) + \varepsilon)^{-1}$ where $b_n(u)$ is node u's betweenness centrality and ε is a very small positive constant to prevent division by zero).

We use NA^{random}, NA^{degree} and $NA^{central}$ to represent random removal, high-degree removal and high-centrality removal attack strategies on nodes. ND^{random}, ND^{prefer} and $ND^{balance}$ represent random replenishment, preferential replenishment and balanced replenishment defense strategies on nodes.

3.2. Attack and defense on edges

In real-world networks, edge attacks are another type of normal targeted attacks, which needs less attack cost and is easily executed for attackers. Generally speaking, the failure rate on edges is higher than it on nodes, so the replenishment on edges are also of great importance. We assume that only one edge selected according to the given strategies is removed in an attack phase, and a new edge will be added into the network following the given strategies in a defense phase.

3.2.1. Attack strategies

(1) Random removal: Select an edge randomly from the network and remove it.
(2) High-degree removal: Select the edge with the largest degree product from the network and remove it. The degree product of an edge is simply calculated by multiplying the degree of the nodes in the two ends of the edge (*i.e.,* the degree product D of the edge e_{ij} is: $D = d_i \times d_j$, where d_i and d_j are the degree of the nodes in two ends of edge e_{ij}).
(3) High-centrality removal: Select the edge with the highest edge-betweenness from the network and remove it. The edge-betweenness of an edge is the fraction of shortest paths that pass through it (*i.e.,* the edge-betweenness $b_e(e_{lk})$ of edge e_{lk} is

$$b_e(e_{lk}) = \sum_{s \neq t \in V} \frac{\sigma_{s,t}(e_{lk})}{\sigma_{s,t}} \tag{4}$$

where $\sigma_{s,t}$ is the total number of shortest paths from source node s to destination node t, and $\sigma_{s,t}(e_{lk})$ is the number of shortest paths from source node s to destination node t which actually pass through edge e_{lk}).

3.2.2. Defense strategies

(1) Random replenishment: Select two nodes randomly and add a new edge between them, neither create self-connections nor double connections.
(2) Preferential replenishment: Select two nodes according to the probability proportional to their degree (*i.e.,* the probability of selecting node u is $p(u) = d(u) / \sum_{v \in V} d(v)$), and add a new edge between them, neither create self-connections nor double-connections.
(3) Balanced replenishment: Select two nodes according to the probability proportional to their node-betweenness centrality (*i.e.,* the probability of selecting node u is $p(u) = (b_n(u) + \varepsilon)^{-1} / \sum_{v \in V} (b_n(v) + \varepsilon)^{-1}$), and add a new edge between them, neither create self-connections nor double-connections.

We use EA^{random}, EA^{degree} and $EA^{central}$ to represent random removal, high-degree removal and high-centrality removal attack strategies on edges. ED^{random}, ED^{prefer} and $ED^{balance}$ represent random replenishment, preferential replenishment and balanced replenishment defense strategies on edges.

4. Experiments

In this section, we selected four different synthetic networks and two real-world networks to test the iterative attack and defense model introduced in Section 3 for evaluating the performance of attack/defense strategies. And then the evolution of robustness of networks in terms of R and R_l is analyzed under four continuous topological changes.

4.1. Topologies

Topologies have been proposed to show different characteristics in terms of degree distribution and average node degree, which are related to the robustness of networks. The random networks (G_{ER}) have been obtained using the Erdős–Rényi model [16], small-world network ($G_{WS}^{2,0.5}$ – 2 is the initial neighbors and 0.5 is the connecting probability) using the Watts and Strogatz model [17] and scale-free networks (G_{BA}^{2}, G_{BA}^{4} – we denote G_{BA}^{x} as the Barabási–Albert network where each new node is connected to x existing nodes) using the Barabási–Albert model [15]. Two real-world networks are the US air transportation systems (G_{AIR}) [18] and the electrical power grid in part of western European (mainly Portugal and Spain) (G_{Power}) [19].

The properties of the four different synthetic and two real-world network topologies are summarized in Table 1. Given a graph $G = (V, E)$, $|V|$ is the total number of nodes, $|E|$ is the total number of edges, and $d(G)$ is the average degree of G.

In this paper, each experiment on these six types of networks is independently conducted over 10 runs, and the number of iterative attack and defense is set to 1000 rounds. Since the experimental results have randomness, the results should be averaged over multiple independent runs. Our purpose is to analyze the performance of each strategy. The result of

Table 1
Properties of network topologies.

Network	$\|V\|$	$\|E\|$	$d(G)$
G_{ER}	303	550	3.63
$G_{WS}^{2,0.5}$	301	700	4.65
G_{BA}^{2}	300	597	3.98
G_{BA}^{4}	300	1190	7.98
G_{Power}	217	320	2.94
G_{AIR}	332	2126	12.81

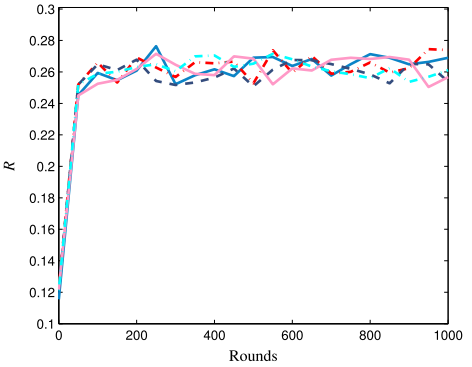

Fig. 1. Changes in robustness R of 5 independent runs on G_{BA}^{2}.

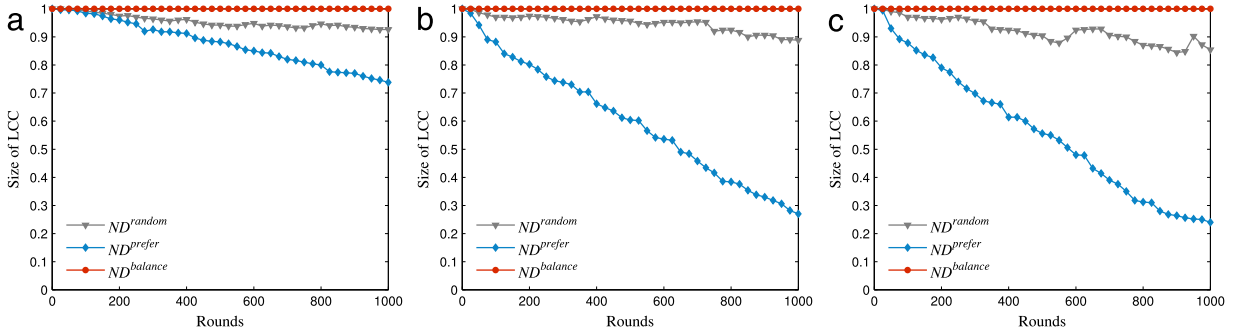

Fig. 2. Changes in size of *LCC* by different attack and defense strategies on nodes over rounds. (a) NA^{random}. (b) NA^{degree}. (c) $NA^{central}$. $ND^{balance}$ is the best defense strategy against node attacks. As for attack strategy, NA^{degree} and $NA^{central}$ are more destructive than NA^{random}.

current round is associated with its previous round. In each experiment, the performance of attack/defense strategy should be evaluated by all results over 1000 iterative rounds, so it is not suitable to average the results over multiple runs. For example, in the experiments on G_{BA}^{2}, the attack strategy is NA^{degree} and the defense strategy is $ND^{balance}$. Changes in robustness R of 5 independent experiments are shown in Fig. 1. As can be seen, the five curves of robustness R are similar with each other and they have similar fluctuations over 1000 iterative rounds. Other experiments have similar characteristics. Therefore, in the following experiments, we randomly selected the result of one run from 10 independent runs to show the performance of each strategy.

4.2. Performance of attack/defense strategies

In this paper, one of our interests is to find the best attack/defense strategies on both nodes and edges. The detail of each strategy is introduced in Section 3, in which we keep the number of nodes and edges be invariant. By observing changes of the size of *LCC*, we validate the performance of each attack/defense strategy on G_{BA}^{2} with 500 nodes and 997 edges. Figs. 2 and 3 show the results. At each round, the size of *LCC* is normalized by dividing by the total number of nodes in the initial network.

As shown in Fig. 2, only $ND^{balance}$ has a good performance against node attacks NA^{random}, NA^{degree} or $NA^{central}$ since the size of *LCC* is unchanged during 1000 rounds while ND^{random} and ND^{prefer} are not effective, since the size of *LCC* has been decreased from the beginning of iterated attack and defense process. Especially, ND^{prefer} is the worst strategy among all

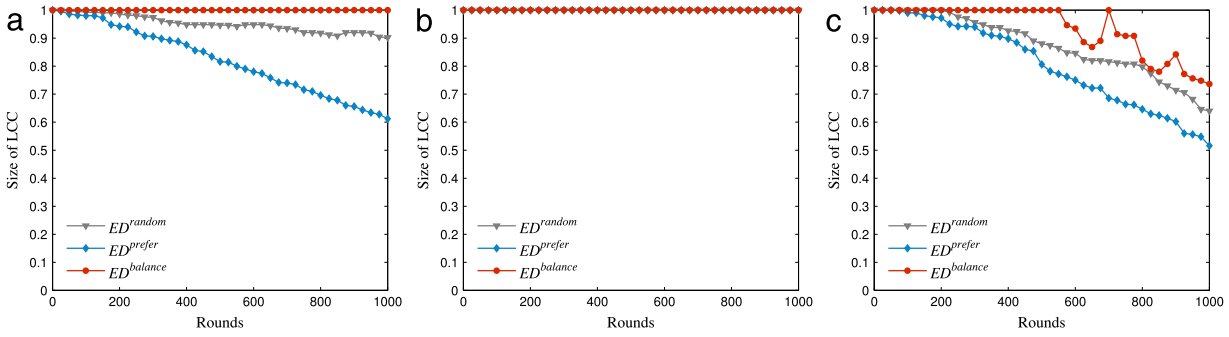

Fig. 3. Changes in size of *LCC* by different attack and defense strategies on edges over rounds. (a) EA^{random}. (b) EA^{degree}. (c) $EA^{central}$. $ED^{balance}$ also shows a good performance against edge attacks EA^{random} and EA^{degree}. Interestingly, EA^{degree} is a harmless edge attack strategy.

Table 2
Best attack and defense strategies for networks.

Target	Best attack	Best defense
Node	NA^{degree}, $NA^{central}$	$ND^{balance}$
Edge	EA^{random}, $EA^{central}$	$ED^{balance}$

defense strategies. From the curves of ND^{prefer} against NA^{random}, NA^{degree} and $NA^{central}$ in Fig. 2, we can see that NA^{degree} and $NA^{central}$ perform better than NA^{random} in the attack phase.

From Fig. 3 we can see that $ED^{balance}$ is comparatively effective against edge attacks EA^{random}, EA^{degree} or $EA^{central}$, while the performance of ED^{random} and ED^{prefer} is worse—the size of *LCC* decreases as the number of iterative rounds increases. In Fig. 3(b), all defense strategies perform well against edge attack EA^{degree}. It can be explained that the edge attack following degree product EA^{degree} is a harmless edge attack strategy while EA^{random} and $EA^{central}$ are destructive. And during iterative rounds, $EA^{central}$ causes cascading failures—the size of *LCC* suddenly falls by one third at about the 500th round. In real-world systems, it may lead to more accidental damage in the case of unprepared.

Based on the analysis of the performance of each attack/defense strategy above, we summarize the best attack/defense strategies for networks in Table 2.

4.3. Evolution of network robustness

The robustness R and link-robustness R_l, introduced in Section 2, can evaluate the friability of networks against malicious node and edge attacks, while the size of *LCC* cannot show these detailed information about network robustness. In this paper, another research purpose is to study how the attack/defense strategy affects the network robustness through analyzing the changes in terms of R and R_l.

According to the best attack/defense strategies shown in Table 2, we classify these four different combinations of best attack/defense to simulate continuous topological changes on nodes and edges: (1) high-degree attack and balanced defense on nodes (NA^{degree}–$ND^{balance}$); (2) high-centrality attack and balanced defense on nodes ($NA^{central}$–$ND^{balance}$); (3) random attack and balanced defense on edges (EA^{random}–$ED^{balance}$); (4) high-centrality attack and balanced defense on edges ($EA^{central}$–$ED^{balance}$).

In general, the network robustness increases as the network density increasing, and fully connected networks are the most robust networks. Therefore, our experiments are designed on networks with different densities, shown in Table 1. The experimental results are shown in Figs. 4–9.

From these figures we can see that $ND^{balance}$ performs well against node attack NA^{degree} or $NA^{central}$ in all networks—the size of *LCC* remains unchanged during 1000 rounds. And from the curves of R we find $ND^{balance}$ is perfect for enhancing R against NA^{degree} and $NA^{central}$. The values of R of $G_{WS}^{2,0.5}$ just remain unchanged (see Fig. 5(b)), while the values of R of other networks increase (see Fig. 4(b), Figs. 6(b)–9(b)). The robustness R signifies the ability of network against malicious attacks on nodes, so this conclusion can explain why $ND^{balance}$ always performs well on maintaining network connectivity against node attacks during 1000 rounds.

However, as shown in the curves of R_l, we can find $ND^{balance}$ is not sufficiently effective against node attacks NA^{degree} or $NA^{central}$ in many network topologies. The values of R_l decrease during 1000 rounds (see Figs. 4(c), 6(c), and 7(c)) and are remained in $G_{WS}^{2,0.5}$ (see Fig. 5(c)). It means that $ND^{balance}$ cannot change the weakness of these networks against malicious edge attacks. But $ND^{balance}$ performs excellently on two real-world networks (see Figs. 8(c) and 9(c)), in which the values of R_l are almost doubled.

Interestingly, we find the curves of NA^{degree}–$ND^{balance}$ are similar with those of $NA^{central}$–$ND^{balance}$ on all networks no matter in terms of the size of *LCC*, R or R_l. It is justified that NA^{degree} and $NA^{central}$ have similar attacking ability on nodes. For an attacker, either NA^{degree} or $NA^{central}$ is an effective node attack strategy which can be selected to destroy networks.

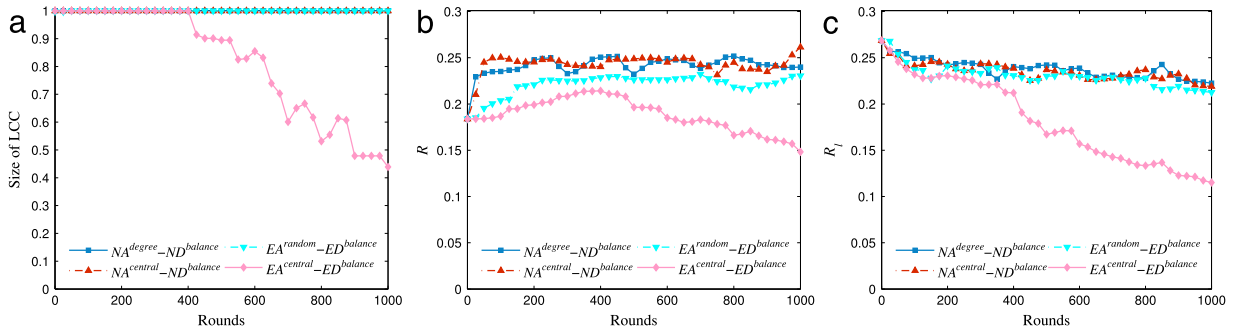

Fig. 4. Experimental results on random network G_{ER}: changes in the size of *LCC*, R and R_l under four continuous topological changes. While $ED^{balance}$ is performed against $EA^{central}$, the size of *LCC* begins falling off at about the 400th rounds. Balanced replenishment increases R, but R_l has been decreased over iterative rounds.

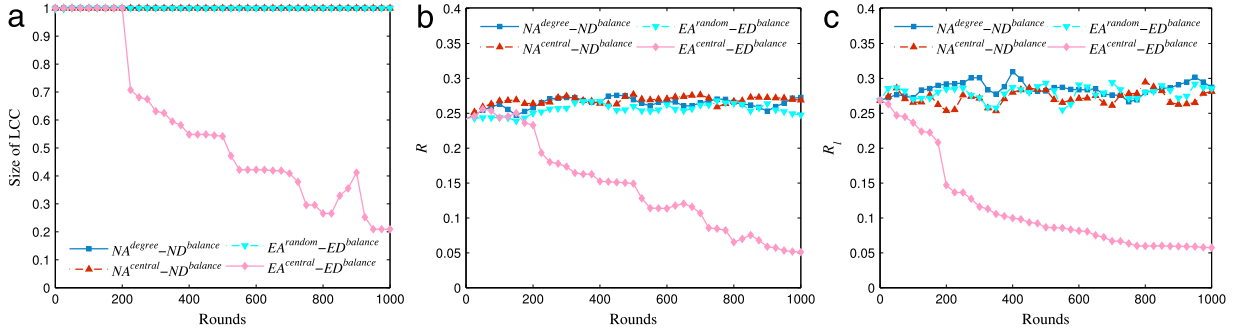

Fig. 5. Experimental results on small-world network $G_{WS}^{2,0.5}$: changes in the size of *LCC*, R and R_l under four continuous topological changes. The values of R and R_l remain almost unchanged. Balanced replenishment $ED^{balance}$ performs miserably against $EA^{central}$.

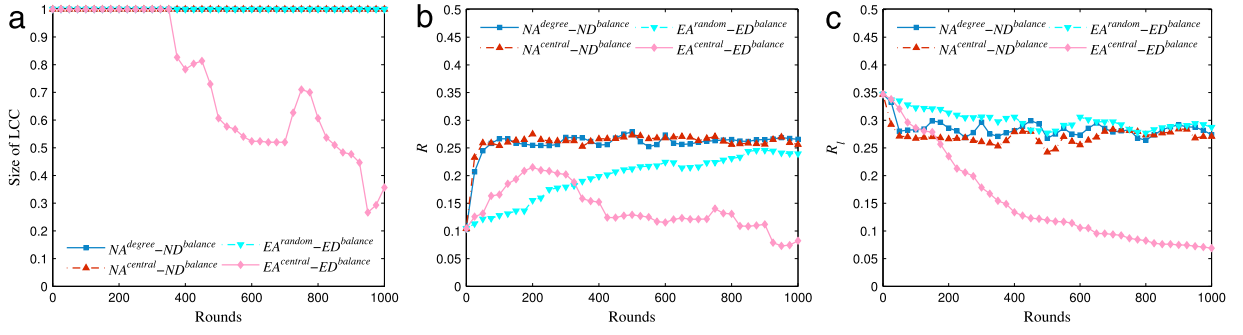

Fig. 6. Experimental results on scale-free network G_{BA}^{2}: changes in the size of *LCC*, R and R_l under four continuous topological changes. The values of R are doubled within 50 rounds. Meanwhile, the values of R_l decrease quickly.

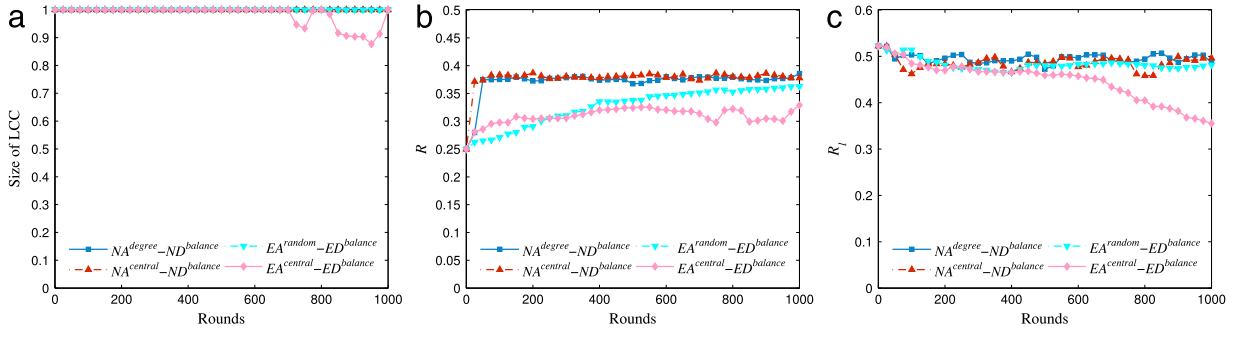

Fig. 7. Experimental results on scale-free network G_{BA}^{4}: changes in the size of *LCC*, R and R_l under four continuous topological changes. The values of R rapidly increase, but the values of R_l decrease slightly. Because of high link density of G_{BA}^{4}, the damage of $EA^{central}$ becomes less evident.

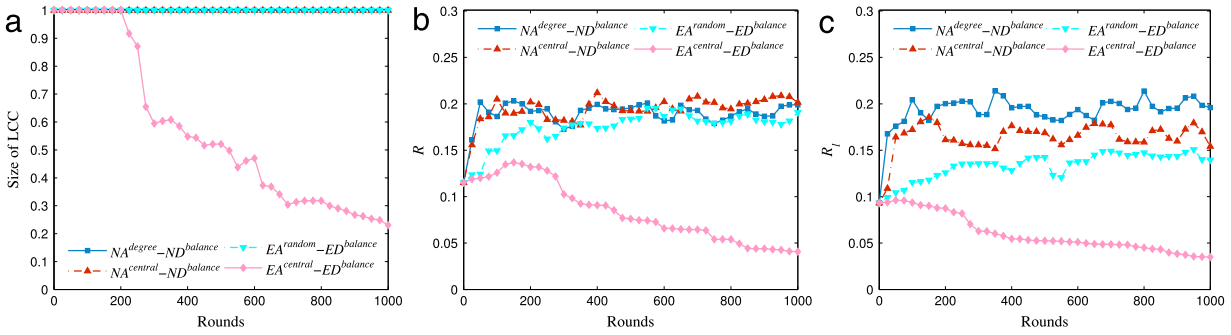

Fig. 8. Experimental results on power-grid network G_{Power}: changes in the size of *LCC*, R and R_l under four continuous topological changes. Due to the low link density, this network is sensitive to attacks on nodes or edges, and the fluctuations of results are large. At the macro level, both R and R_l have been improved.

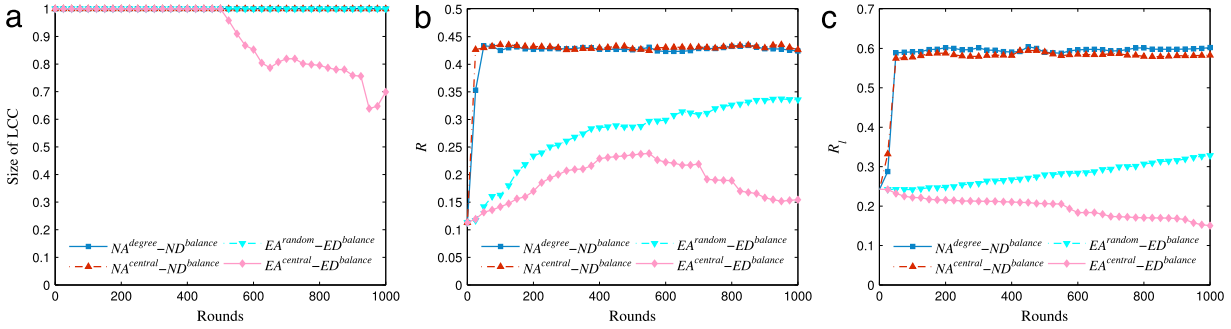

Fig. 9. Experimental results on US-air transportation network G_{AIR}: changes in the size of *LCC*, R and R_l under four continuous topological changes. Although balanced replenishment is still not perfect against $EA^{central}$, both the values of R and R_l are doubled.

As for the edge attack and defense, it is observed that $ED^{balance}$ performs well against EA^{random}, but is not perfect against $EA^{central}$—the size of *LCC* suddenly falls off after certain rounds on all network topologies. From Figs. 4(b)–9(b) we can see that $ED^{balance}$ can increase R against EA^{random} during 1000 rounds, and even against $EA^{central}$, R also increases until the size of *LCC* begins falling off at some round. The main reason is that R is defined based on the size of *LCC*. On the side of attackers, it is obvious that $EA^{central}$ is more malicious than EA^{random}.

To maintain network connectivity against malicious edge attacks, a possible approach is to increase R_l of networks. Unfortunately, the best defense strategy $ED^{balance}$ cannot increase R_l against $EA^{central}$ on all networks during 1000 rounds. For example, against $EA^{central}$, although network G_{ER} begins being disconnected at about the 400th round (see Fig. 4(a)), R_l is decreased from the beginning of the iterative process (see Fig. 4(c)). And even if $ED^{balance}$ is used to defend against EA^{random}, R_l still falls off on many networks topologies (see Figs. 4(c), 6(c) and 7(c)). This is the reason why $ED^{balance}$ cannot remain the size of *LCC* be unchanged.

Finally, we summarize the evolution of network robustness based on the best attack and defense strategies on nodes and edges in Table 3, where "↑" means increasing, "↓" means decreasing and "−" means unchange. For example, when the network is under edge attack $EA^{central}$ and defense $ED^{balance}$, R increases and R_l decreases.

5. Conclusions

Based on the framework of iterative attack and defense in Ref. [12] and the modified iterative model in Ref. [14], we extend existing models to an iterative attack and defense model on edges. Two well-known network robustness measures: R and R_l are employed to analyze the performance of each attack/defense strategy and the evolution of network robustness, while the size of the largest connected cluster cannot distinguish the resilience of networks against node and edge attacks.

Through intensive experiments on various different types of networks, we find that the balanced defense strategy of connecting nodes with low-centrality is effective to maintain network connectivity. This strategy can increase the robustness R of networks during iterative rounds. But the balanced defense cannot enhance the link-robustness R_l. So, the balanced defense is not perfect to fight against malicious edge attacks. Significantly, on two real-world networks, this defense strategy can be effective enough to increase the network robustness against both intentional node and edge attacks. On the side of attackers, both high-degree attack and high-centrality attack are effective node attack strategies to destroy connectivity and the best edge attack is removing edges with the highest edge-betweenness.

Table 3
Evolution of network robustness under best attack and defense strategies.

Network	Target	Best attack	Best defense	R	R_l
G_{ER}	*Node*	NA^{degree}, $NA^{central}$	$ND^{balance}$	↑	↓
	Edge	$EA^{central}$	$ED^{balance}$	↑	↓
$G_{WS}^{2,0.5}$	*Node*	NA^{degree}, $NA^{central}$	$ND^{balance}$	–	–
	Edge	$EA^{central}$	$ED^{balance}$	–	↓
G_{BA}^{2}	*Node*	NA^{degree}, $NA^{central}$	$ND^{balance}$	↑	↓
	Edge	$EA^{central}$	$ED^{balance}$	↑	↓
G_{BA}^{4}	*Node*	NA^{degree}, $NA^{central}$	$ND^{balance}$	↑	↓
	Edge	$EA^{central}$	$ED^{balance}$	↑	↓
G_{Power}	*Node*	NA^{degree}, $NA^{central}$	$ND^{balance}$	↑	↑
	Edge	$EA^{central}$	$ED^{balance}$	↑	↓
G_{AIR}	*Node*	NA^{degree}, $NA^{central}$	$ND^{balance}$	↑	↑
	Edge	$EA^{central}$	$ED^{balance}$	↑	↓

Acknowledgments

This work is partially supported by the Outstanding Young Scholar Program of National Natural Science Foundation of China (NSFC) under Grant 61522311, the General Program of NSFC under Grant 61271301, the Overseas, Hong Kong & Macao Scholars Collaborated Research Program of NSFC under Grant 61528205, the Research Fund for the Doctoral Program of Higher Education of China under Grant 20130203110010, and the Fundamental Research Funds for the Central Universities under Grant K5051202052.

References

[1] H. Jeong, B. Tombor, R. Albert, Z.N. Oltvai, A.-L. Barabási, The large-scale organization of metabolic networks, Nature 407 (6804) (2000) 651–654.
[2] R. Albert, I. Albert, G.L. Nakarado, Structural vulnerability of the North American power grid, Phys. Rev. E 69 (2) (2004) 025103.
[3] S.N. Dorogovtsev, J.F. Mendes, Evolution of Networks: From Biological Nets to the Internet and WWW, Oxford University Press, 2013.
[4] R. Albert, H. Jeong, A.-L. Barabási, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382.
[5] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Resilience of the Internet to random breakdowns, Phys. Rev. Lett. 85 (21) (2000) 4626.
[6] R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Breakdown of the Internet under intentional attack, Phys. Rev. Lett. 86 (16) (2001) 3682.
[7] C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Mitigation of malicious attacks on networks, Proc. Natl. Acad. Sci. 108 (10) (2011) 3838–3841.
[8] P. Buesser, F. Daolio, M. Tomassini, Optimizing the robustness of scale-free networks with simulated annealing, in: Adaptive and Natural Computing Algorithms, Springer, 2011, pp. 167–176.
[9] A. Zeng, W. Liu, Enhancing network robustness against malicious attacks, Phys. Rev. E 85 (6) (2012) 066130.
[10] M. Zhou, J. Liu, A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks, Physica A 410 (2014) 131–143.
[11] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, H.E. Stanley, Optimization of network robustness to waves of targeted and random attacks, Phys. Rev. E 71 (4) (2005) 047101.
[12] R. Anderson, S. Nagaraja, The topology of covert conflict, at WEIS, 2006.
[13] R. Axelrod, W.D. Hamilton, The evolution of cooperation, Science 211 (4489) (1981) 1390–1396.
[14] H. Kim, R. Anderson, An experimental evaluation of robustness of networks, IEEE Syst. J. 7 (2) (2013) 179–188.
[15] A.-L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[16] P. Erdős, A. Rényi, On the evolution of random graphs, Publ. Math. Inst. Hung. Acad. Sci. 5 (1960) 17–61.
[17] D.J. Watts, S.H. Strogatz, Collective dynamics of 'small-world' networks, Nature 393 (6684) (1998) 440–442.
[18] V. Batagelj, A. Mrvar, Pajek datasets. Available at: http://vlado.fmf.uni-lj.si/pub/networks/data/.
[19] Q. Zhou, J.W. Bialek, Approximate model of European interconnected system as a Benchmark system to study effects of cross-border trades, IEEE Trans. Power Syst. 20 (2) (2005) 782–788.
[20] S. Trajanovski, J. Martín-Hernández, W. Winterbach, P. Van Mieghem, Robustness envelopes of networks, J. Complex Netw. 1 (1) (2013) 44–62.
[21] T. Tanizawa, S. Havlin, H.E. Stanley, Robustness of onionlike correlated networks against targeted attacks, Phys. Rev. E 85 (4) (2012) 046109.
[22] J. Wu, M. Barahona, Y.-J. Tan, H.-Z. Deng, Spectral measure of structural robustness in complex networks, IEEE Trans. Syst. Man Cybern. A 41 (6) (2011) 1244–1252.
[23] B. Zheng, H. Wu, W. Du, W. Shu, J. Qin, The robustness of scale-free networks under edge attacks with the quantitative analysis. ArXiv Preprint: arXiv:1211.3238.
[24] H.J. Herrmann, C.M. Schneider, A.A. Moreira, J.S. Andrade Jr., S. Havlin, Onion-like network topology enhances robustness against malicious attacks, J. Stat. Mech. Theory Exp. 2011 (01) (2011) P01027.