Front. Comput. Sci., 2017, 11(4): 568–584
DOI 10.1007/s11704-016-6108-z

RESEARCH ARTICLE

A comparative study of network robustness measures

Jing LIU (✉), Mingxing ZHOU, Shuai WANG, Penghui LIU

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

Abstract The robustness is an important functionality of networks because it manifests the ability of networks to resist failures or attacks. Many robustness measures have been proposed from different aspects, which provide us various ways to evaluate the network robustness. However, whether these measures can properly evaluate the network robustness and which aspects of network robustness these measures can evaluate are still open questions. Therefore, in this paper, a thorough introduction over attacks and robustness measures is first given, and then nine widely used robustness measures are comparatively studied. To validate whether a robustness measure can evaluate the network robustness properly, the sensitivity of robustness measures is first studied on both initial and optimized networks. Then, the performance of robustness measures in guiding the optimization process is studied, where both the optimization process and the obtained optimized networks are studied. The experimental results show that, first, the robustness measures are more sensitive to the changes in initial networks than to those in optimized networks; second, an optimized network may not be useful in practical situations because some useful functionalities, such as the shortest path length and communication efficiency, are sacrificed too much to improve the robustness; third, the robustness of networks in terms of closely correlated robustness measures can often be improved together. These results indicate that it is not wise to just apply the optimized networks obtained by optimizing over one certain robustness measure into practical situations. Practical requirements should be considered, and optimizing over two or more suitable robustness measures simultaneously is also a promising way.

Keywords scale-free network, malicious attack, robustness measure, hill climbing algorithm

1 Introduction

Most interacting systems in nature and society can be modeled as complex networks with the components of systems being represented as nodes and the relationships between components being represented as edges [1–3]. Network properties, such as small-world property [4], scale-free property [5,6] and robustness [7–27], have attracted increasing attention. The robustness, which evaluates the capability of networks in resisting failures or attacks on some parts of networks, has drawn extensive attention in recent years, because the breakdown of many real-world networks caused by the failure on a small number of nodes or links led to considerable economic losses in the past, such as the breakdown of Chinese power line network caused by the bad weather [21], and the effect of economic network spreading to the world caused by the subprime mortgage crisis of America [24].

To study the network robustness, suitable measures are needed to evaluate the robustness. Recently, many robustness measures have been proposed from different aspects. One important factor in designing measures is attacks, which can be either random or malicious. In random attacks [8], each node or edge is removed with the same probability. While in malicious attacks [12,14], one popular way is to sequentially remove the most important node or edge at each attack, and the importance of remaining nodes or edges is re-calculated.

Received February 22, 2016; accepted September 29, 2016

E-mail: neouma@163.com

This process repeats until only isolated nodes are left in the network. In the following text, a thorough introduction over attacks and existing measures is first given.

Random networks [28], small-world networks [4] and scale-free networks [5,6] are widely studied complex network models. Because the scale-free network (SFN) model well matches with real-world networks, it attracts much more attention. Moreover, SFNs are much more interesting because it has been proved in [11,12] that SFNs are robust in defending random attacks, but fragile in defending malicious attacks. Therefore, we focus on studying the robustness of SFNs in this paper.

In fact, there are two main functions of robustness measures; that is, evaluate the robustness of networks and guide the optimization process as optimization objectives to find more robust networks. To evaluate the robustness of networks, the measures should be sensitive to changes in networks. Thus, to validate whether a robustness measure can evaluate the network robustness properly, the sensitivity of these measures is first studied on both initial and optimized networks, where the optimized networks are obtained by optimizing initial networks using a hill climbing algorithm and taking robustness measures as objectives.

Different robustness measures may guide the optimization algorithms to find different types of robust networks. That is to say, the optimized networks may be robust in terms of the objective measures, but fragile in terms of other measures. In [14], Schneider et al. proposed a robustness measure R based on simulating malicious node attacks. Later, Zeng et al. [15] extended R to evaluate malicious edge attacks, which is labeled as R_l. Moreover, Zeng et al. [15] also found that R and R_l contradict with each other; that is, the network which is robust evaluated by R is fragile evaluated by R_l.

Therefore, it is meaningful to analyze the robustness of optimized networks in terms of measures that have not been used as objective functions. We further studied the performance of robustness measures in guiding the optimization process. Both the optimization process and the optimized networks are studied. To enhance the network robustness, adding edges or adjusting the topology of network without changing the degree distribution and the connectivity of each node are considered. The way of adding edges tends to spend more cost in real applications, thus, the way of adjusting topology is much more attractive. Schneider et al. [14] and Zeng et al. [15] optimized network topologies by designing a hill climbing method and a hybrid-optimized method, respectively. Thus, in this paper, the hill climbing method in [14] is used to optimize the robustness through adjusting topologies without changing the degree distribution and the connectivity of each node.

The rest of this paper is organized as follows. Section 2 introduces a uniform framework of malicious attacks, and Section 3 introduces robustness measures systematically. Section 4 studies the sensitivity of these measures on randomly generated and optimized networks. The performance of robustness measures in guiding the optimization process is studied in Section 5. Finally, conclusions are given in Section 6.

2 Uniform framework of malicious attacks

A network can be represented as a graph $G = (V, E)$, where $V = \{1, 2, \ldots, N\}$ is the set of nodes, and $E = \{e_{ij} | i, j \in V, i \neq j\}$ is the set of M links. In this paper, undirected and unweighted networks are considered. Synthetic SFNs with different sizes are generated using the well-known Barabási-Albert model (BA model) [1,5]. The BA model starts from a small clique (a completely connected graph) of N_0 nodes. At each successive time step, a new node is added and connects to M_0 different existing nodes, where M_0 is smaller than N_0. When a new node is connected to an existing node, the probability of choosing an existing node is proportional to its degree. This high preferential attachment situation has been observed in many real networks.

The attack on nodes or edges can be random or malicious. In random attacks, each node or edge is removed with the same probability. While in malicious attacks, the most important nodes or edges are removed first. There are several ways to define the importance of nodes or edges, such as betweenness centrality and closeness centrality.

In existing studies on malicious attacks, High Degree Adaptive Attack on nodes (HDA) [14] and High Betweenness Centrality Attack on edges (HBA) [15] are used. In HDAs, the node with the largest degree is always removed, and in HBAs, the edge with the largest betweenness centrality [29,30] is always removed. In fact, in addition to node degree and betweenness centrality, the importance of nodes or edges can also be evaluated by other factors, such as edge degree and closeness centrality [31–33].

Therefore, a unified framework of malicious attacks can be defined based on the importance of nodes or edges, which is labeled as High Importance Adaptive Attack (HIA). In HIAs, the importance of nodes or edges is first calculated and the current most important node or edge is removed. Then, the importance of left nodes or edges is re-calculated again, and the current most important node or edge is removed. This process is repeated until only isolated nodes are left. Next, three types of importance of nodes and edges are introduced, and then six types of malicious attacks combining with these importance are described in detail.

The node degree is equal to the number of nodes that a node connects to, and the edge degree is defined as follows [22],

$$k_{ij} = \sqrt{k_i \times k_j}, \quad i \neq j \in V, e_{ij} \in E, \tag{1}$$

where k_i and k_j represent the degree of nodes i and j, respectively. The larger the node degree or edge degree of a node is, the more important this node or edge is.

The node betweenness centrality and the edge betweenness centrality are defined as the fraction of shortest paths passing through nodes or edges [29,30], which are given in Eqs. (2) and (3),

$$c_l^B = \sum_{i \neq j \in V} \frac{P_{ij}^l}{P_{ij}}, \quad l \in V, \tag{2}$$

$$c_{e_{kl}}^B = \sum_{i \neq j \in V} \frac{P_{ij}^{e_{kl}}}{P_{ij}}, \quad e_{ij} \in E, \tag{3}$$

where c_l^B represents the betweenness of node l, P_{ij} represents the number of shortest paths between nodes i and j, and P_{ij}^l represents the number of shortest paths between nodes i and j and passing through l. $c_{e_{kl}}^B$ represents the betweenness of edge e_{kl}, and $P_{ij}^{e_{kl}}$ represents the number of shortest paths between nodes i and j and passing through e_{kl}. The higher the betweenness of a node or edge is, the more important this node or edge is.

The nodal closeness centrality is defined as the average length of shortest paths from a node to all other nodes [31–33], and the edge closeness centrality is defined as follows,

$$c'^C_i = \frac{1}{N-1} \sum_{j \in V} d_{ij}, \quad i \neq j \in V, \tag{4}$$

$$c'^C_{e_{ij}} = \sqrt{c'^C_i \times c'^C_j}, \quad i \neq j \in V, e_{ij} \in E, \tag{5}$$

where c'^C_i and $c'^C_{e_{ij}}$ represent the closeness centrality of node i and edge e_{ij}, respectively. d_{ij} is the length of the shortest path between nodes i and j. In fact, the node closeness centrality describes whether a node can be easily reached. The smaller the closeness centrality is, the easier a node or edge can be reached; that is, the more important this node or edge is.

Because the network may be disconnected after being attacked, the length of shortest paths between two nodes may be infinite. Thus, the calculation of node and edge closeness centrality is revised as follows,

$$c_i^C = \frac{1}{N-1} \sum_{j \in V} \frac{1}{d_{ij}}, \quad i \neq j \in V, \tag{6}$$

$$c_{e_{ij}}^C = \sqrt{c_i^C \times c_j^C}, \quad i \neq j \in V, e_{ij} \in E. \tag{7}$$

In this way, the larger the closeness centrality is, the more important a node or edge is.

Based on the above importance measures, six kinds of malicious attacks are given as follows,

A_1: Attack nodes based on the nodal degree. This attack is the same with the HDA [14], and renamed as *high degree adaptive node attack* (NA_{HDA}) here.

A_2: Attack edges based on the edge degree. This attack is named as *high degree adaptive link attack* (LA_{HDA}).

A_3: Attack nodes based on the node betweenness centrality. This attack is named as *high betweenness centrality adaptive node attack* (NA_{HBCA}).

A_4: Attack edges based on the edge betweenness centrality. This attack is the same with the HBA [15], and renamed as *high betweenness centrality adaptive link attack* (LA_{HBCA}) here.

A_5: Attack nodes based on the node closeness centrality. This attack is named as *high closeness centrality adaptive node attack* (NA_{HCCA}).

A_6: Attack edges based on the edge closeness centrality. This attack is named as *high closeness centrality adaptive link attack* (LA_{HCCA}).

3 Robustness measures

The early research on robustness measures was mainly based on connectivity, which can be traced back to 1970 [34–36]. After that, several analytical studies on network robustness from the viewpoint of random graph theory were proposed [8–11]. Taking the critical fraction of attacks and realistic cases into consideration, widely used robustness measures based on the percolation theory were proposed [14–16]. Another remarkable kind of robustness measures is designed based on the eigenvalue of network matrix [17,37,38]. Next, we classify the robustness measures into four groups, and introduce them in detail, respectively.

3.1 Robustness measures based on connectivity

In 1970, Frank et al. [34] analyzed the survivability of networks using the basic concept of graph connectivity. However, the graph connectivity only partly reflects the ability of graphs to retain certain degree of connectedness under deletion. Thus, other improved measures were introduced, such as super connectivity [35] and conditional connectivity [36].

Although these improved measures consider both the cost of damaging a network and the extent to which the network is damaged, the computational cost in calculating these measures for general graphs is too high. So here, only the vertex and edge connectivity are introduced.

The edge connectivity, labeled as $\upsilon(G)$, is the minimum number of edges which must be removed from a connected graph in order to disconnect it. Let $\upsilon_{s-t}(G)$ be the number of edges which must be removed to disconnect nodes s and t, then the edge connectivity is defined as

$$\upsilon(G) = \min_{s,t \neq s \in V} \{\upsilon_{s-t}(G)\}. \tag{8}$$

According the above definition, it is not difficult to find that the larger the value of $\upsilon(G)$ is, the more robust the network is, because more edges need to be removed to disconnect networks. However, the value is not larger than the minimum node degree in the network, so the value of this measure cannot be changed too much through adjusting the network topology without changing the degree distribution and each nodal degree.

The node connectivity, being similar with the edge connectivity, is the minimum number of nodes which must be removed from a connected graph in order to disconnect it. Let $\omega(G)$ be the node connectivity of network G, and $\omega_{s-t}(G)$ be the minimum number of nodes which must be removed to disconnect nodes s and t. Thus,

$$\omega(G) = \min_{s,t \neq s \in V \wedge e_{st} \notin E} \{\omega_{s-t}(G)\}. \tag{9}$$

According to the definition, $\omega(G)$ is not defined in a full connected graph. The larger the value of $\omega(G)$ is, the more robust the graph is, because more nodes need to be removed to disconnect the graph. A remarkable result of these two robustness measures is that $\omega_{s-t}(G) \leqslant \upsilon_{s-t}(G)$ for any s and t ($s \neq t \in V, e_{st} \notin E$), so $\omega(G) \leqslant \upsilon(G)$ [39]. Thus, the value of this measure cannot be changed too much through adjusting the topology without changing the degree distribution and each nodal degree.

3.2 Robustness measures based on random graph theory

In 2000, Albert et al. [8] studied the network robustness from the viewpoint of random graph theory. They proposed a statistical measure, namely, the critical removal fraction of vertices (edges) for the disintegration of networks, to characterize the structural robustness of complex networks. The disintegration of networks is measured in terms of network performance. The most common performance measurements include the diameter, the size of the largest component, the average path length, and communication efficiency [40]. For some special networks, the critical removal fraction can be obtained analytically [8–11]. Here, the critical removal fractions against random and targeted attacks are introduced in detail.

The critical fraction against random attacks is labeled as p_c^r. According to [9], p_c^r for any degree distribution $P(k)$ is calculated as

$$p_c^r = 1 - \frac{1}{\kappa_0 - 1}, \tag{10}$$

where κ_0 is equal to $\langle k^2 \rangle / \langle k \rangle$, $\langle k \rangle$ is the average nodal degree of the original network, and $\langle k^2 \rangle$ is the average of square of nodal degree. The larger the value of p_c^r is, the more robust the network is. If the degree distribution and each nodal degree are unchanged, then κ_0 is unchanged.

The critical fraction against targeted attacks is labeled as p_c^t. In [11], p_c^t is defined against NA_{HDA}. After the node with the largest degree is removed, the degree distribution needs to be re-calculated. In fact, according to the definition in [11], we can calculate p_c^t for graphs with any degree distributions through simulating the attacking process. Attack the node with the largest degree, check the condition of networks, and repeat this process until the left network is disconnected, then p_c^t is obtained. The larger the value of p_c^t is, the more robust the network is. However, being different from p_c^t, p_c^t may change a lot if it is calculated through simulation.

3.3 Robustness measure R and its extensions

In 2011, Schneider et al. [14] pointed out that the robustness measure in terms of the critical fraction of attacks at which the system completely collapses, the percolation threshold, may not be useful in many realistic cases. These measures, for example, ignore the situations in which the network suffers from a significant damage, but still keeps its integrity. Thus, they proposed a unique robustness measure R, which considers the size of the largest component against malicious node attacks [14],

$$R = \frac{1}{N} \sum_{Q=1}^{N} s(Q), \tag{11}$$

where $s(Q)$ is the fraction of nodes of the largest connected component after removing Q nodes. The normalization factor $1/N$ 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.

Since the original R only considers the attacks on nodes, Zeng et al. extended it to consider the attacks on links in [15] as follows,

$$R_l = \frac{1}{M}\sum_{P=1}^{M} s(P), \tag{12}$$

where $s(P)$ is the fraction of nodes in the largest connected component after removing P links. The normalization factor $1/M$ 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.

Instead of keeping track of the size of largest connected subgraph, Louzada et al. [16] focus on the communication efficiency [40] of networks after each attack, and proposed a new measure, namely, integral efficiency of network, which is labeled as *IntE*,

$$IntE = \frac{1}{N}\sum_{Q=1}^{N} E(Q), \tag{13}$$

where $E(Q)$ is the communication efficiency of networks after removing Q nodes. The normalization factor $1/N$ also ensures that the robustness of networks with different sizes can be compared. The larger the value of *IntE* is, the more robust the network is. $E(0)$ is the communication efficiency of original networks, which can be calculated as [40]:

$$E(G) = \frac{1}{N(N-1)}\sum_{i\neq j\in G}\zeta_{ij} = \frac{1}{N(N-1)}\sum_{i\neq j\in G}\frac{1}{d_{ij}}, \tag{14}$$

where ζ_{ij} is the communication efficiency between vertices i and j which is defined to be inversely proportional to the shortest distance: $\zeta_{ij} = 1/d_{ij}$. When there is no path between i and j, $d_{ij} = +\infty$ and $\zeta_{ij} = 0$.

Combining R_l with *IntE*, the communication efficiency can be also tracked for malicious link attacks, which extends the measure as follows,

$$IntE_l = \frac{1}{M}\sum_{P=1}^{M} E(P), \tag{15}$$

where $E(P)$ is the communication efficiency of network after removing Pedges, and is calculated through Eq. (13). The normalization factor $1/M$ also ensures that the robustness of networks with different sizes can be compared. The larger the value of $IntE_l$ is, the more robust the network is.

3.4 Robustness measures based on eigenvalue

A remarkable group of robustness measures are those based on the eigenvalue of network Laplacian matrix or adjacent matrix. Here, two robustness measures, namely, algebraic connectivity, which is based on the eigenvalue of Laplacian matrix, and natural connectivity, which is based on the eigenvalue of adjacent matrix, are introduced in detail.

The algebraic connectivity, $a(G)$, is the second smallest eigenvalue of the Laplacian matrix. Fiedler [37] showed that the magnitude of the algebraic connectivity reflects how well connected the overall graph is and Merris in [38] gave a survey of the vast literature on algebraic connectivity.

$$\alpha(G) = \lambda_2, \lambda_1 \leqslant \lambda_2 \leqslant \lambda_3 \leqslant \cdots \leqslant \lambda_N, \tag{16}$$

where λ_i, $i = 1, 2, 3, \ldots, N$ are the eigenvalue of Laplacian matrix of graph G.

However, the algebraic connectivity is too coarse to capture important features of structural robustness of complex networks [17]. Thus, Wu et al. [17] proposed the natural connectivity, which characterizes the redundancy of alternative routes in a network by quantifying the weighed number of closed walks of all lengths. The natural connectivity can be regarded as an average eigenvalue that changes strictly monotonically with the addition or deletion of edges.

$$\overline{\lambda} = \ln\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right), \tag{17}$$

where λ_i is the ith eigenvalue of the graph adjacency matrix. Given the number of vertices, the empty graph has the minimum *natural connectivity* and the complete graph has the maximum *natural connectivity*. So the lager the value of $\overline{\lambda}$ is, the more robust the network is.

Next two sections focus on analyzing the above nine robustness measures. First, their sensitivity is analyzed on randomly generated and optimized networks through adding or deleting edges. Second, the performance of these measures in guiding the optimization process is systematically studied.

4 Sensitivity of robustness measures

Whether a robustness measure can give an accurate evaluation of network robustness is of great importance. To evaluate the robustness, the measures should be sensitive to the change in networks. In general, if an edge is added to a network, the robustness should be improved, or at least unchanged, and if an edge is removed from a network without changing the connectivity, the robustness should be decreased. Thus, in this section, the sensitivity of above measures is studied on BA networks [1,5] and optimized networks, whose robustness is improved by a hill climbing method, by adding and deleting edges to and from these networks. When optimized networks are attacked or their robustness is improved, the robustness measures should reflect these changes.

Different strategies in adding or deleting edges may have different effects on the robustness. Thus, four strategies of adding and deleting edges are considered, namely random strategy, rich-rich strategy, poor-poor strategy, and rich-poor strategy, which were also used in [17]. In the random strategy, an edge is selected randomly. In the rich-rich strategy, edges are sorted decreasingly according to $k_i \times k_j$, where k_i and k_j are the degree of the two end nodes of an edge, and the edge is selected in this order. In the poor-poor strategy, edges are sorted increasingly according to $k_i \times k_j$, and selected in this order. In the rich-poor strategy, edges are sorted decreasingly according to $|k_i - k_j|$, and selected in this order.

The *adding edge process* is executed as follows,

1) Calculate the robustness of the given network G_0;
2) Select an edge using one of the four strategies, add the selected edge to G_0, and re-calculate the robustness of G_0;
3) Repeat Step 2 until the maximum number of edges need to be added is reached;
4) Conduct Steps 1–3 for ten times to calculate the average values to reduce the bias.

The *deleting edge process* is similar to the *adding edge process*, and the only difference lies in Step 2: "Select an edge using one of the four strategies, and delete the selected edge from G_0; if the connectivity of G_0 is not affected, then re-calculate the robustness of G_0; otherwise, reject the deletion and repeat Step 2."

In the following experiments, initial networks are generated using the BA model, where $N = 100$ and $\langle k \rangle \approx 4$. In order to optimize the BA networks, the hill climbing algorithm (HCA) [14,15] is used to improve the robustness of initial networks without changing the degree distribution and the degree of each node. The HCA starts from an initial network, repeatedly swaps a pair of edges, and accepts the swapping only when the robustness is improved. The details of HCA are summarized in the hill climbing algorithm.

Next, the sensitivity of $\upsilon(G)$, $\omega(G)$, p_c^r, p_c^t, R, R_l, $IntE$, $\alpha(G)$, and $\overline{\lambda}$ are studied on both randomly generated networks and optimized networks, which are generated using p_c^t, R, R_l, $IntE$, $\alpha(G)$, and $\overline{\lambda}$ as the optimization objectives.

4.1 Sensitivity of robustness measures on randomly generated networks

In this experiment, the sensitivity of robustness measures $\upsilon(G)$, $\omega(G)$, p_c^r, p_c^t, R, R_l, $IntE$, $\alpha(G)$, and $\overline{\lambda}$ are studied on randomly generated networks. For each robustness measure, four different strategies in selecting edges are used and the maximum number of selected edges is set to 50. For p_c^t, R, and $IntE$, the NA_{HDA} is used in calculating their values. The results are showed in Fig. 1, where the negative values of the x-coordinate means the number of removed edges and the positive values means the number of added edges.

```
Algorithm  Hill climbing algorithm
Input:
    $G_0$: Initial network;
Output:
    $G^*$: Optimized network;
$G^* \leftarrow G_0$;
Calculate the robustness of $G^*$ according to the optimization objective,
namely, a certain robustness measure;
while (termination criteria are not satisfied) do
  Randomly select two existing edges $e_{ij}$, $e_{kl}$ from $G^*$, which satisfy the
  condition that $e_{ik}$, $e_{jl}$ are not in $G^*$;
  Delete $e_{ij}$, $e_{kl}$ from $G^*$ and add $e_{ik}$, $e_{jl}$ to $G^*$;
  Calculate the robustness of $G^*$ according to the optimization objective;
  if (the robustness of $G^*$ is not improved) then
    Delete $e_{ik}$, $e_{jl}$ from $G^*$ and add $e_{ij}$, $e_{kl}$ back to $G^*$;
  end if
end while
```

As it can be seen, these measures show different responses to the changes in networks. $\upsilon(G)$ and $\omega(G)$ almost fail to reflect the changes incurred by the rich-rich strategy, and their ability to reflect the changes incurred by the three other strategies is also very limited. p_c^r shows a sensitive response to all the four strategies, but for the poor-poor strategy, the value of p_c^r decreases with the increasing of number of edges. In fact, no matter how an edge is added, this measure always removes nodes with the same probability. Thus, this measure can reflect the changes incurred by all the four strategies. p_c^t shows a different performance with p_c^r, and is more positively sensitive to the poor-poor strategy. Because this measure always removes the node with the largest degree, the edges added between nodes with smaller degree can stay in the networks for long time, and contribute more to the sensitivity than those connecting nodes with larger degree.

R only reflects the changes incurred by the poor-poor and random strategies, while R_l reflects the changes incurred by all the four strategies. $IntE$ is similar to R, and is more sensitive to the poor-poor and random strategies, while $a(G)$ is similar to R_l. $\overline{\lambda}$ increases with the increasing of the number of edges incurred by all the four strategies. Being similar to the difference between p_c^r and p_c^t, the difference between R, $IntE$ and R_l, $a(G)$, $\overline{\lambda}$ is also due to the way in removing nodes or edges in calculating these measures. Moreover, since R and $IntE$ are calculated after the network changes to isolated nodes, but not like p_c^t, which is calculated only after the network is disconnected, they are also sensitive to the random strategy.

4.2 Sensitivity of robustness measures on optimized networks

The HCA is used to optimize the BA networks with 100 nodes and $\langle k \rangle \approx 4$. During the optimization process, p_c^t, R, R_l, $IntE$, $\alpha(G)$, and $\overline{\lambda}$ are respectively used as the optimization objectives. Then, six types of optimized networks are obtained. For each type of optimized networks, the sensitivity of above robustness measures is analyzed and the results are show in Figs. 2–7.

Figure 2 shows the response of the measures other than p_c^t is similar to that in Fig. 1. p_c^t shows a little decreasing tendency when the edges are added using the rich-rich strategy.

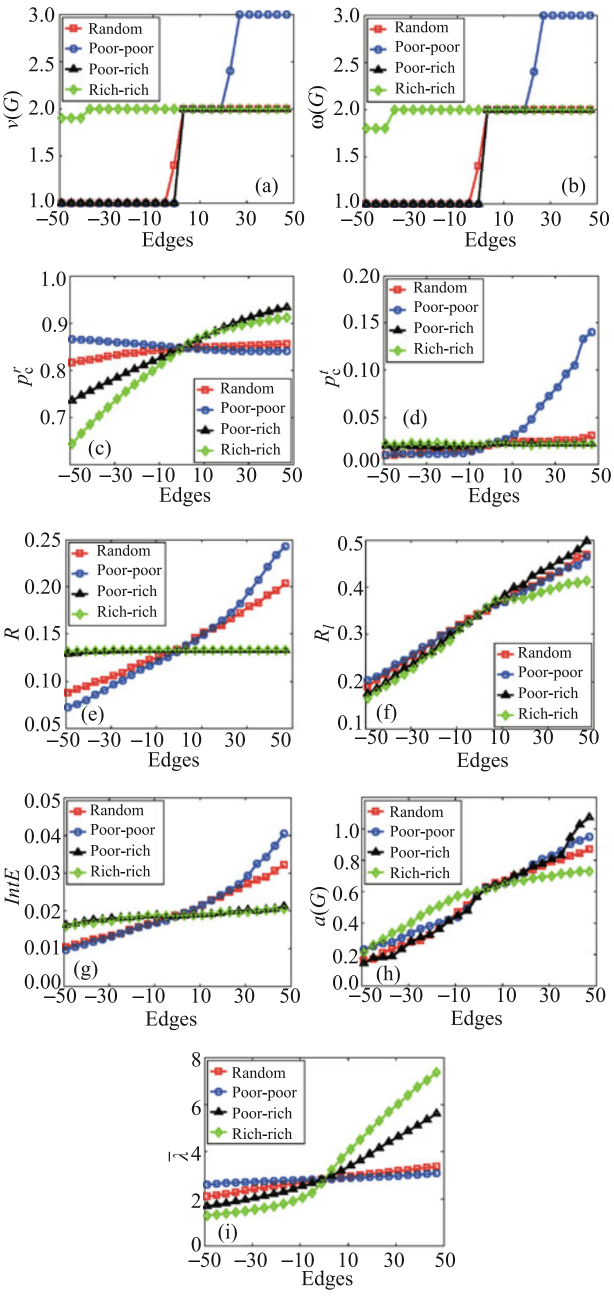


Fig. 1 The sensitivity of robustness measures on randomly generated BA networks. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) $IntE$; (h) $\alpha(G)$; (i) $\overline{\lambda}$

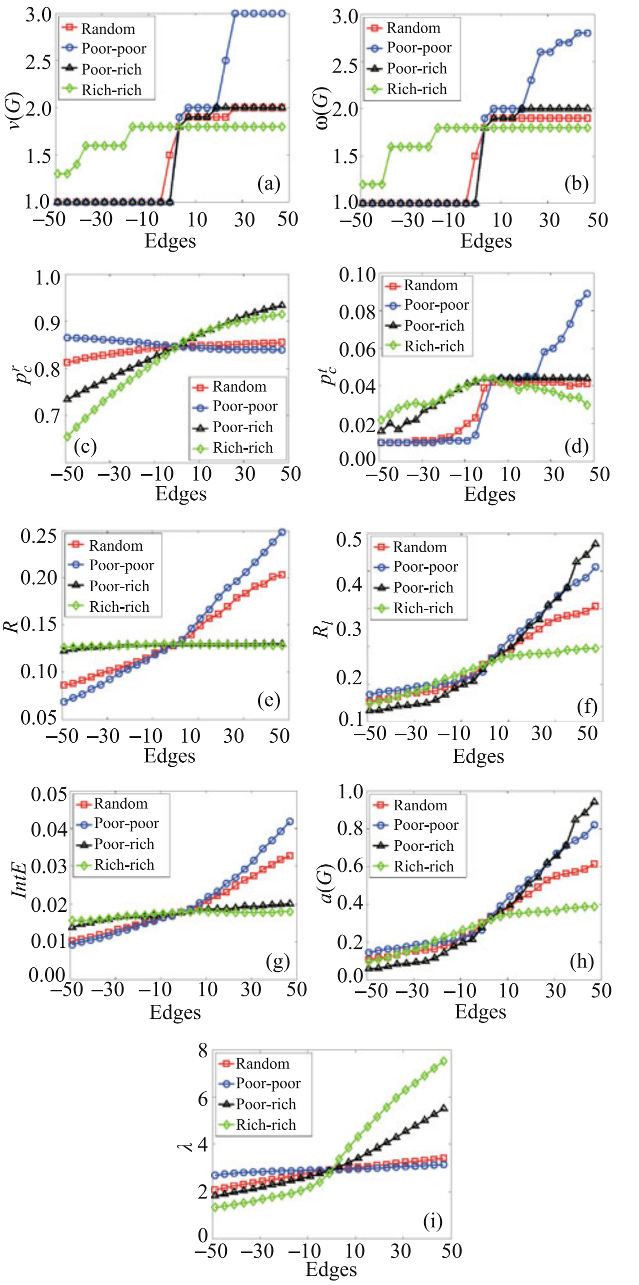


Fig. 2 The sensitivity of robustness measures on optimized networks obtained using p_c^t as the optimization objective. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) $IntE$; (h) $\alpha(G)$; (i) $\overline{\lambda}$

This is mainly because the networks used here is already optimized in terms of p_c^t, but the rich-rich strategy destroys the optimized network topology to certain extent.

Figures 3(d) and 3(e) show that adding edges cause a little decreasing of robustness when random and rich-rich strategies are used, and the poor-poor strategy results in the same phenomenon in Fig. 3(e). However, with the increasing of number of edges, the decreased robustness can increase back as we expected. Since the network topology is already optimized in terms of R, the adding edges may destroy the topology, but the decreased topology can be compensated by adding enough edges.

Figure 4 shows that the decreasing of robustness is only found in Fig. 4(f). Because LA_{HBCA} is considered for this type of optimized networks in calculating R_l, other types of optimized networks are not affected. Since R_l takes every edge into account, the effect is extended to all the four strategies, especially the rich-rich one.

From Fig. 5 we find no significant changes in terms of

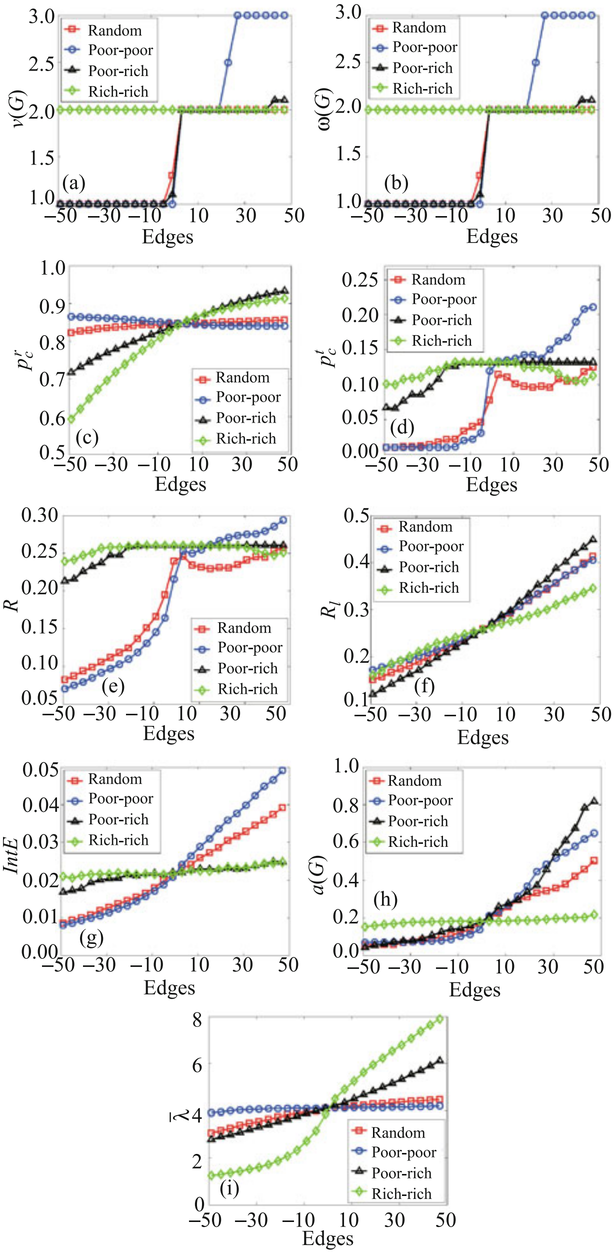


Fig. 3 The sensitivity of robustness measures on optimized networks obtained using R as the optimization objective. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) $IntE$; (h) $\alpha(G)$; (i) $\overline{\lambda}$

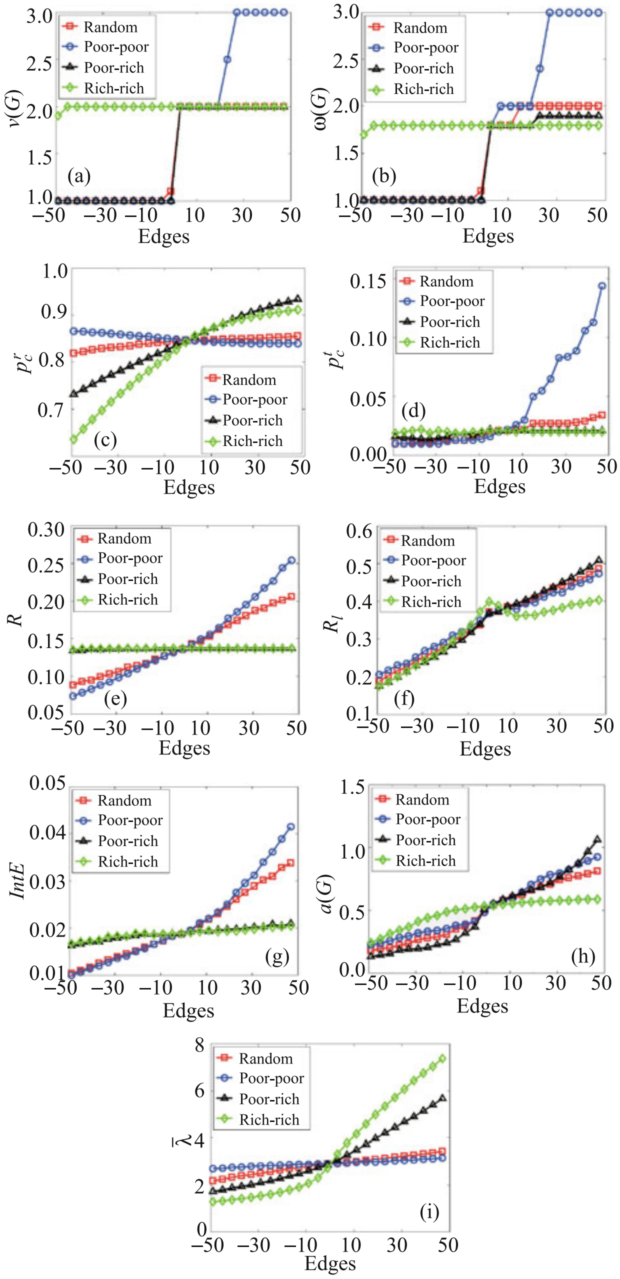


Fig. 4 The sensitivity of robustness measures on optimized networks obtained using R_l as the optimization objective. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) $IntE$; (h) $\alpha(G)$; (i) $\overline{\lambda}$

IntE, but p_c^t in the random and rich-rich strategies and R in the random strategy are affected. This is because when evaluating *IntE*, instead of using the size of largest connected subgraph in R or the connectivity of largest component in p_c^t, the attack procedure considers NA_{HDA}, and preserves the communication efficiency of networks.

From the results showed in Fig. 6 we find that $a(G)$ is affected a lot because it decreases much faster when deleting edges and increases much slower when adding edges compared with the results on randomly generated networks. However, $a(G)$ can still evaluate the robustness well as excepted without too much fluctuation.

Figure 7 shows this extreme situation affects $\upsilon(G)$, $\omega(G)$ and $a(G)$ a lot but not too much to itself and others. The changes appears in $\upsilon(G)$, $\omega(G)$ and $a(G)$ when deleting edges may be caused by the high centralization when optimizing $\overline{\lambda}$. Also, this effect can be compensated through adding edges, too.

From the above sensitivity analysis on optimized networks we can see that the optimized network in one aspect can take

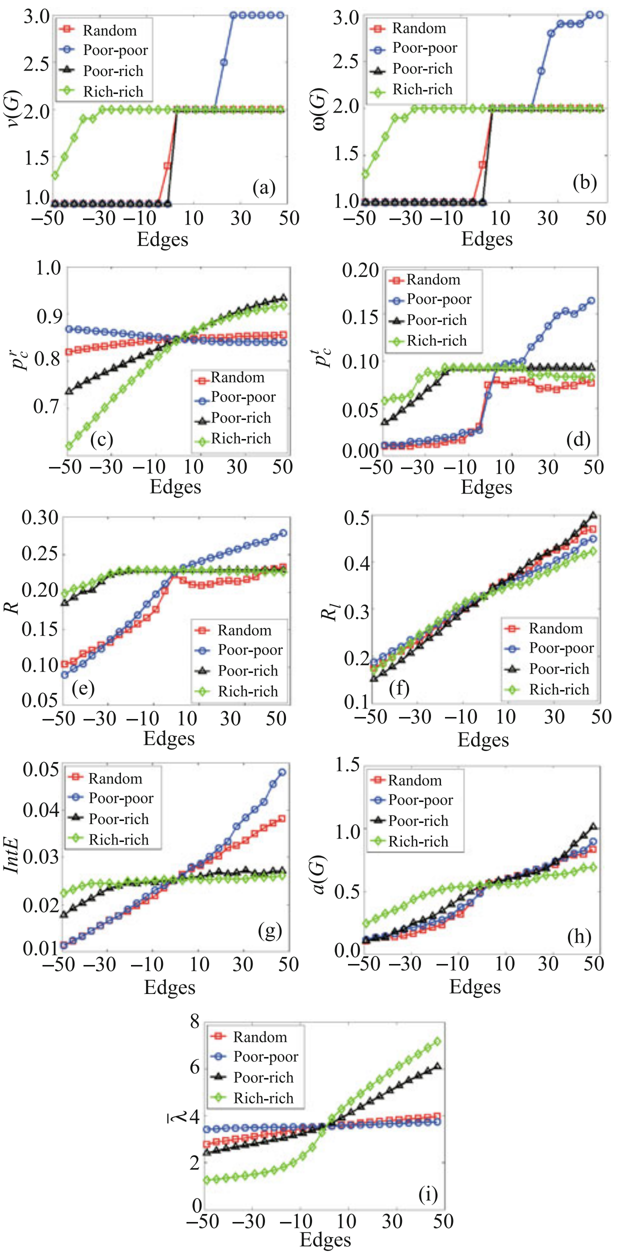


Fig. 5 The sensitivity of robustness measures on optimized networks obtained using *IntE* as the optimization objective. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) *IntE*; (h) $\alpha(G)$; (i) $\overline{\lambda}$

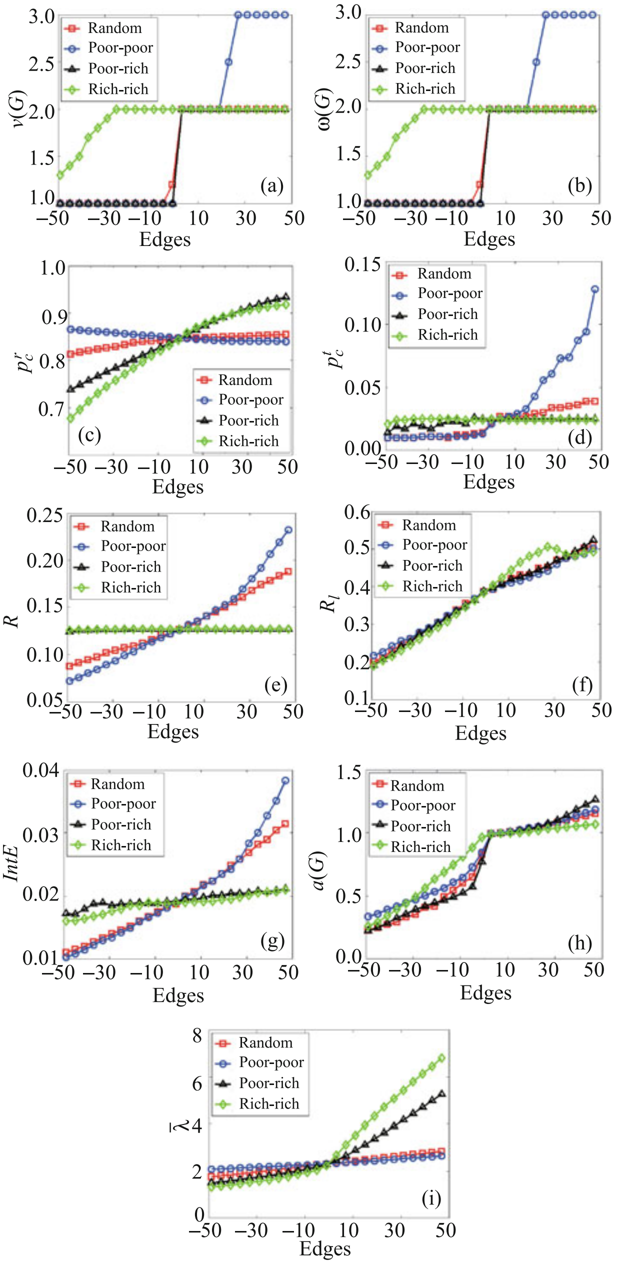


Fig. 6 The sensitivity of robustness measures on optimized networks obtained using $a(G)$ as the optimization objective. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) *IntE*; (h) $\alpha(G)$; (i) $\overline{\lambda}$

the network topology into fully use, and adding edges may destroy this fully optimized topology. Moreover, on these optimized networks obtained by optimizing the single objective, adding edges may increase the robustness slowly, but deleting edges may decrease the robustness quickly. This effect may be extended to the robustness measure which is closely related to the optimized robustness measure.

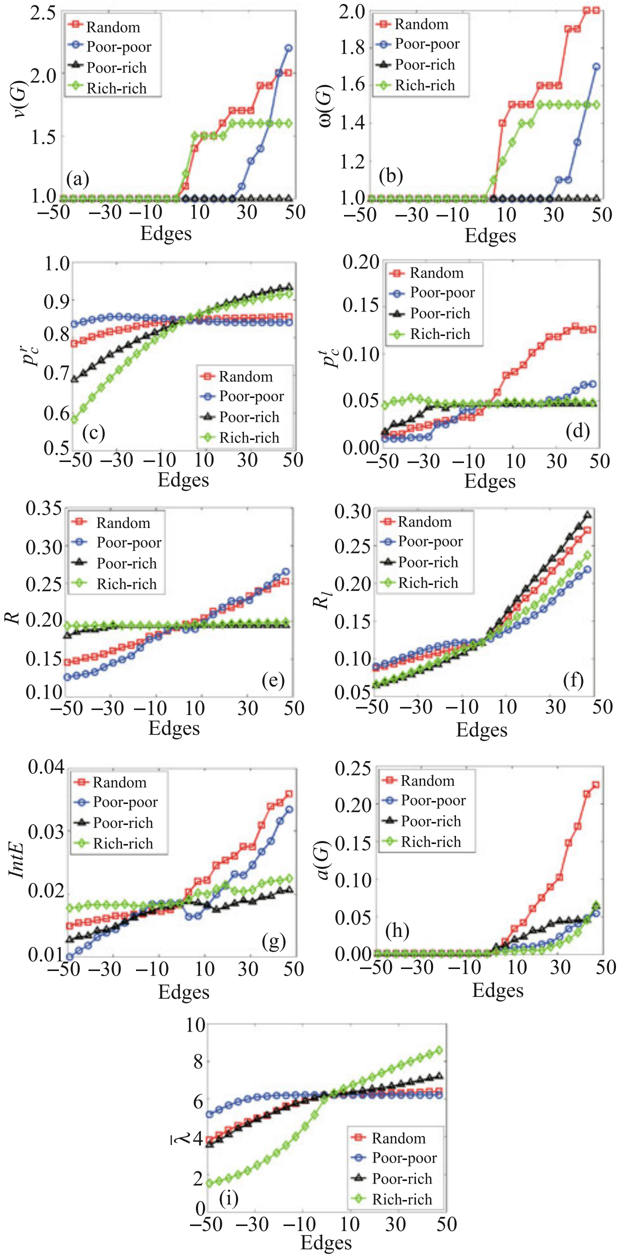


Fig. 7 The sensitivity of robustness measures on optimized networks obtained using $\overline{\lambda}$ as the optimization objective. The results are averaged over ten independent runs. (a) $\upsilon(G)$; (b) $\omega(G)$; (c) p_c^r; (d) p_c^t; (e) R; (f) R_l; (g) $IntE$; (h) $a(G)$; (i) $\overline{\lambda}$

5 Performance of robustness measures in guiding the optimization process

Another major function of robustness measures is to guide the optimization process as an optimization objective to find more robust networks. This section focuses on studying of the performance of these measures in this aspect. Three groups of experiments are conducted, where the first one focuses on the optimization process and the two others focus on the optimized networks. The first experiment studies how the importance network characteristics, like average shortest path and assortativity, change during the optimization process. In the second experiment, the above six types of optimized networks are evaluated by $\upsilon(G)$, $\omega(G)$, p_c^r, p_c^t, R, R_l, $IntE$, $a(G)$, and $\overline{\lambda}$ to see whether the networks which are robust in terms of certain measures are robust in terms of other measures. In the third experiment, the robustness of above optimized networks against the six malicious attacks introduced in Section 2 is studied.

5.1 Change of network characteristics during the optimization process

In this experiment, to study how robustness measures guide the optimization process, the networks obtained during the optimization process are recorded, and their two important characteristics, namely, average shortest path length and assortativity, are studied, because they can reflect network topologies, which are defined in Eqs. (18) and (19), respectively.

$$D(G) = \frac{1}{N(N-1)} \sum_{i \neq j} d_{ij}, \tag{18}$$

$$\gamma = \frac{M^{-1} \sum_{i=2}^{N} \sum_{j=1}^{i} a_{ij} k_i k_j - \left[M^{-1} \sum_{i=2}^{N} \sum_{j=1}^{i} \frac{1}{2} a_{ij} \left(k_i + k_j \right) \right]^2}{M^{-1} \sum_{i=2}^{N} \sum_{j=1}^{i} \frac{1}{2} a_{ij} \left(k_i^2 + k_j^2 \right) - \left[M^{-1} \sum_{i=2}^{N} \sum_{j=1}^{i} \frac{1}{2} a_{ij} \left(k_i + k_j \right) \right]^2}, \tag{19}$$

where d_{ij} is the shortest path length between nodes i and j, k_i is the degree of node i, M is the total number of edges. a_{ij} is the value of the element in the adjacency matrix A_{ij}, which is defined as

$$a_{ij} = \begin{cases} 1, & \text{if } e_{ij} \in E; \\ 0, & \text{otherwise}. \end{cases} \tag{20}$$

The networks obtained during the optimization process are recorded when the initial networks are optimized by HCA and using p_c^t, R, R_l, $IntE$, $a(G)$, and $\overline{\lambda}$ as the optimization objectives for 3×10^4 steps. During the optimization process, many networks with the same robustness may be generated, and only networks with different robustness are recorded. The relationships between the average shortest path length and these measures of the recorded networks are shown in Fig. 8, while those between the assortativity and these measures are shown in Fig. 9, both of which are averaged over ten independent runs.

Figure 8 shows when R and $\overline{\lambda}$ increase, the average shortest path length increases dramatically. However, for the four other measures, the average shortest path length just changes slightly. Thus, in the process of optimizing R and $\overline{\lambda}$, the shortest path is sacrificed. In the process of optimizing $IntE$, the average shortest path length first increases and then decreases, and during the process of optimizing R_l, it is almost not changed.

Figure 9 shows that the changing of assortativity with robustness measures has diversity. For R, $IntE$ and $\overline{\lambda}$, the assortativity increases dramatically, for $a(G)$, it decreases, and for R_l, it is almost unchanged. Combining with the results in Figs. 8 and 9, we can see when we use the robustness measures to improve the network robustness, some network characteristics may be sacrificed, and these network characteristics can be taken as important information to indicate whether an existing type of robust networks is suitable for practical applications. Thus, to generate a robust network, network characteristics should be well balanced considering practical requirements.

5.2 Robustness of optimized networks in terms of different robustness measures

In this experiment, the six types of optimized networks are evaluated by $\upsilon(G)$, $\omega(G)$, p_c^r, p_c^t, R, R_l, $IntE$, $a(G)$, and $\overline{\lambda}$ to see whether networks robust in terms of certain measures are robust in terms of other measures. To be convenient, the six types of optimized networks are labeled as $G_x(x = 1, 2, \ldots, 6)$, which correspond to optimized networks obtained by using p_c^t, R, R_l, $IntE$, $a(G)$, and $\overline{\lambda}$ as optimization objectives, respectively. Moreover, we compare the experimental results on networks with different numbers of nodes to show the effect of network size on the optimization of robustness measures. The number of fitness evaluations for each optimization of the robustness measure is set to be 3×10^4, and ten independent runs are conducted. The results are reported in Fig. 10.

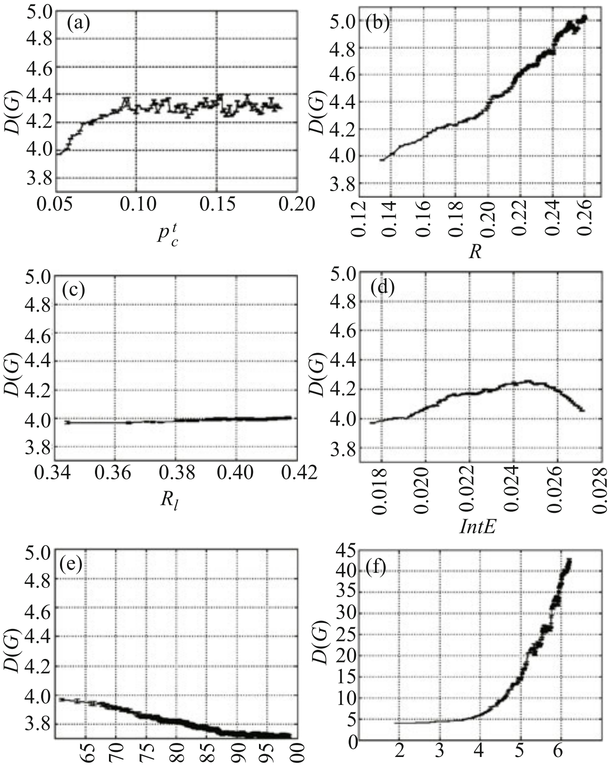


Fig. 8 The relationships between the average shortest path length and the robustness measures of networks obtained during the optimization process. The results are averaged over 10 independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

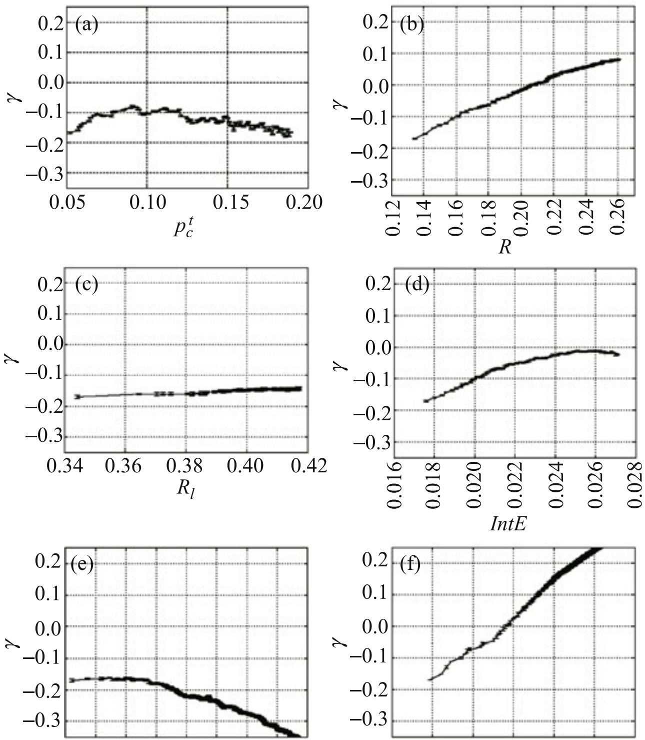


Fig. 9 The relationships between the assortativity and the robustness measures of networks obtained during the optimization process. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

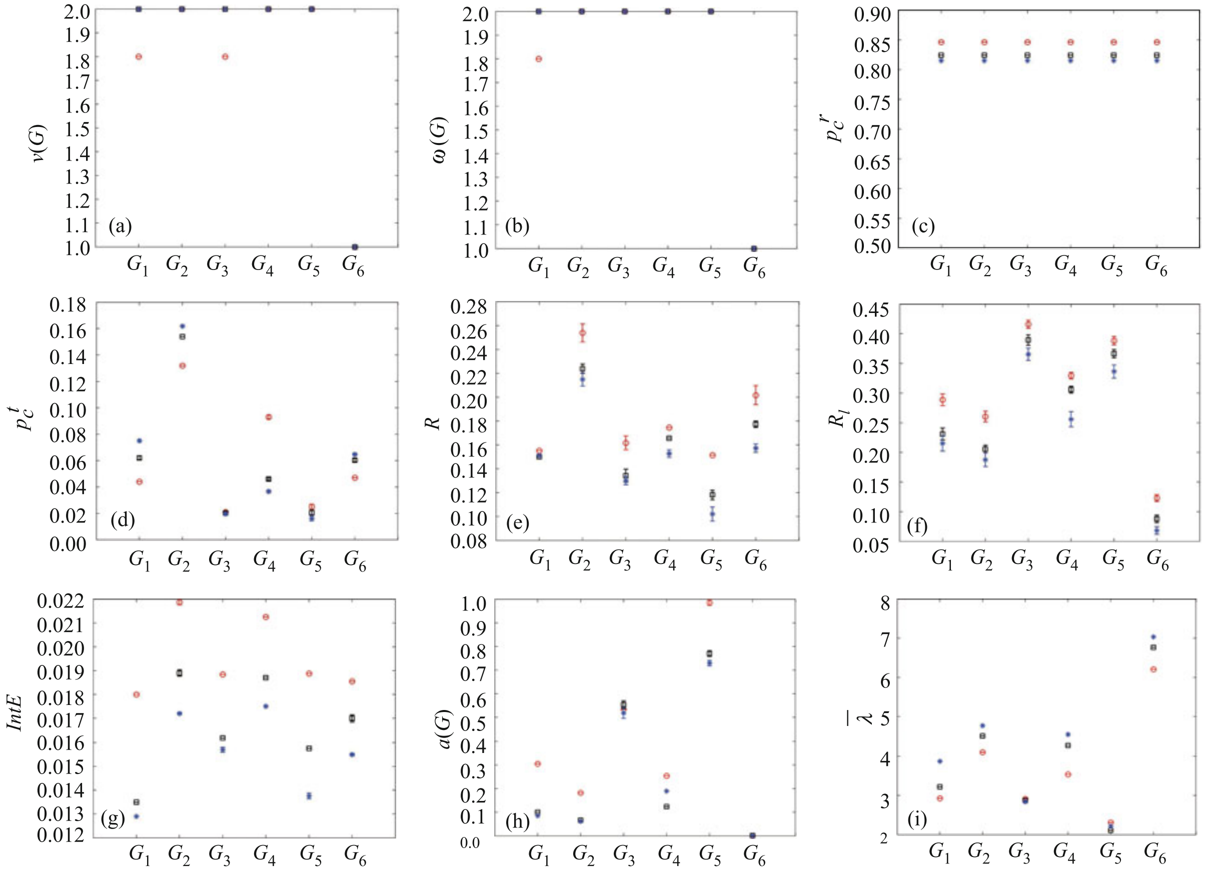


Fig. 10 The values of robustness measures of different optimized networks (The labels $G_1 - G_6$ denote p_c^t, R, R_l, $IntE$, $a(G)$, and $\overline{\lambda}$, respectively. In this figure, circles represent the results of networks with 100 nodes, squares represent those with 300 nodes and asterisks represent those with 500 nodes)

From Fig. 10 we can see that the optimized networks are not robust in every aspect. Figures 10(a), 10(b), 10(f), and 10(h) show that these optimized networks are not robust in terms of $\overline{\lambda}$. p_c^r only depends on the degree distribution, so the optimization without changing the degree distribution cannot affect it. Figures 10(d), 10(e) and 10(g) show almost similar phenomena, because all of them are defined on the basis of NA_{HDA}. In terms of network sizes, networks with different numbers of nodes show similar performances in the optimization processes. Thus, in following sections, to save the computational cost, we mainly focus on studying the networks with 100 nodes.

5.3 Robustness of optimized networks against malicious attacks

In order to study the capability of optimized networks against malicious attacks, the six types of malicious attacks defined in Section 2 are used to attack the optimized networks, and after each attack, the largest connected subgraph and the communication efficiency of left graphs are calculated. The results in terms of the largest connected subgraph against the three node and link attacks are respectively shown in Figs. 11 and 12.

Figure 11 show that G_2, G_4 and G_6 have better performance when suffering from NA_{HDA}, because G_2 and G_4 are obtained by optimizing networks against NA_{HDA}. G_6 is more fragile against NA_{HBCA} and NA_{HCCA}. Figure 11(a), 11(c) and 11(e) show that most optimized networks perform poorly when suffering from malicious attacks that they are not designed to. In fact, we can see that the three node attacks, NA_{HDA}, NA_{HBCA} and NA_{HCCA}, are almost equally malicious to all the optimized networks.

Figure 12 shows that LA_{HBCA} is always the most malicious one, and that an optimized network may be terribly fragile when suffering from some malicious attacks, such as LA_{HBCA} to G_6 showed in Fig. 12(f). Fig. 12(c) and (e) show that G_3 and G_5 have a good performance in defending LA_{HBCA}, which is consistent with the results in Fig. 10(f).

The results in terms of the communication efficiency against the three node attacks are shown in Fig. 13 and those against the three link attacks are shown in Fig. 14. As it can be seen from Fig. 13, NA_{HCCA} performs similar with NA_{HBCA}

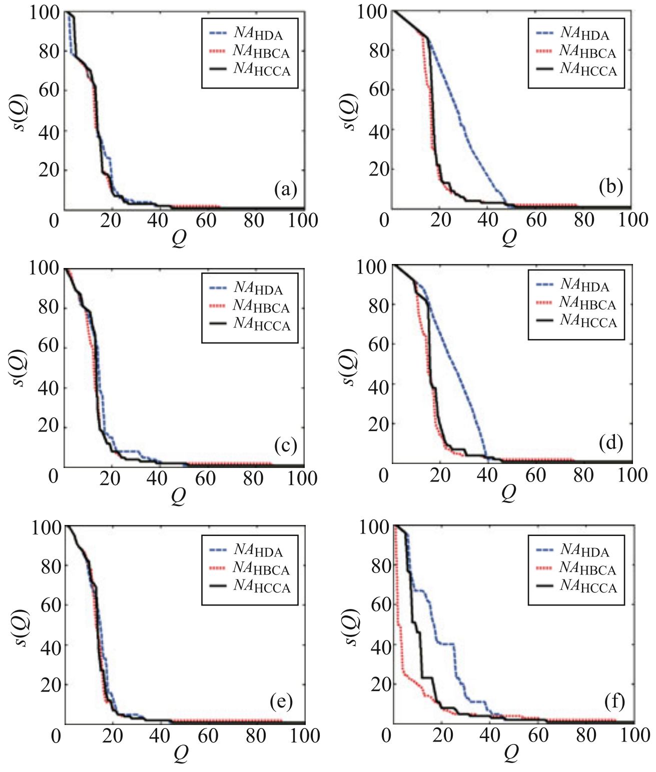


Fig. 11 The change of the size of largest connected subgraphs of optimized networks in the process of node attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

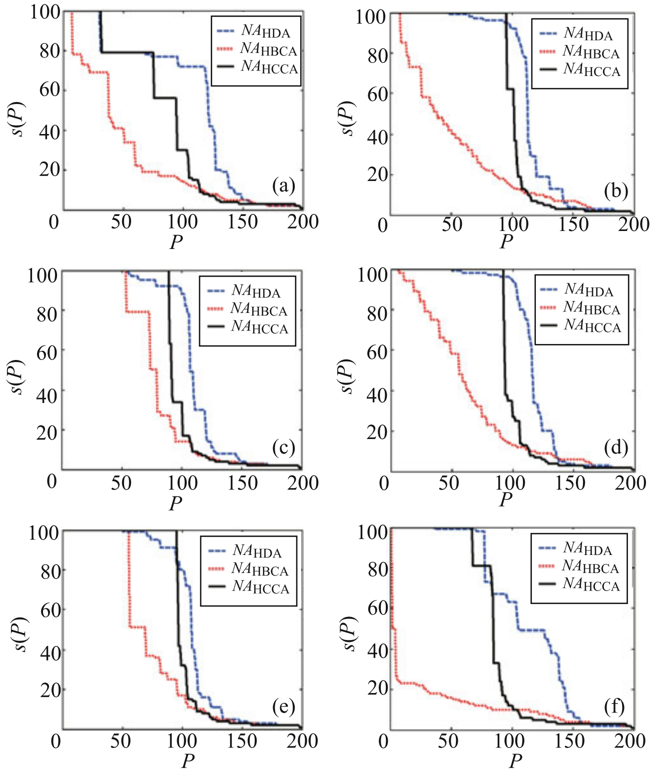


Fig. 12 The change of the size of largest connected subgraphs of optimized networks in the process of link attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

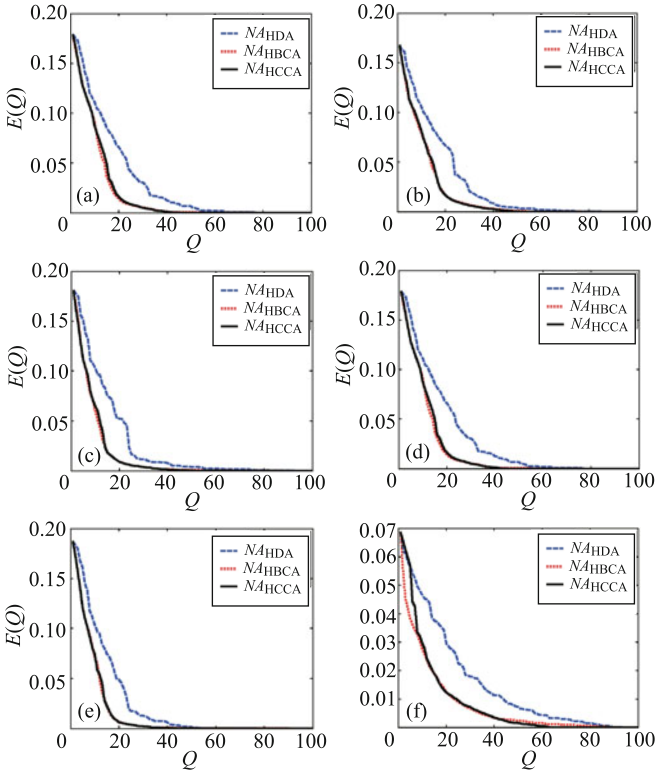


Fig. 13 The change of the communication efficiency of optimized networks in the process of node attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

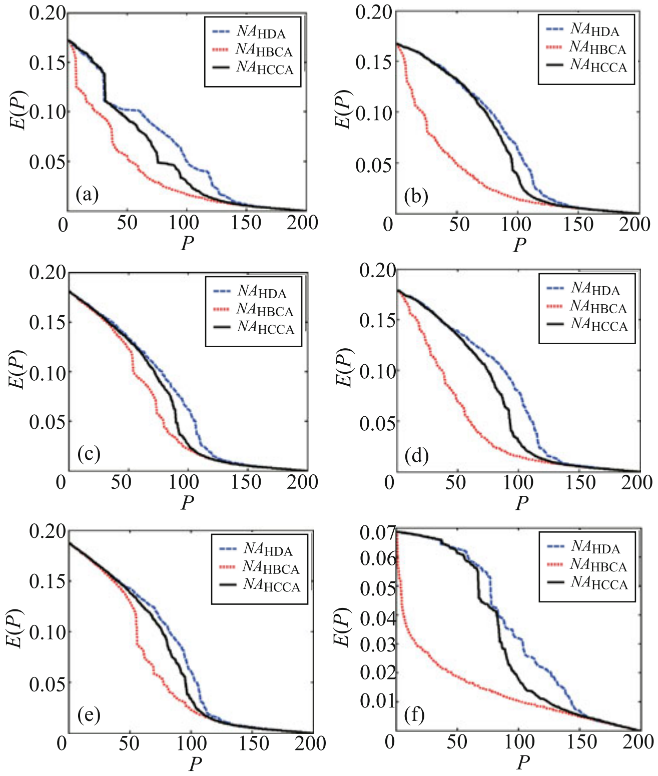


Fig. 14 The change of the communication efficiency of optimized networks in the process of link attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

and presents more destruction than NA_{HDA}. Figure 14 shows that LA_{HBCA} is the most malicious edge attack compared with LA_{HDA} and LA_{HCCA}.

From Figs. 11–14, we have two important observations: 1) If we need a network which has strong ability in defending a certain type of malicious attacks, the better way to generate such a network is to optimize the network using the corresponding robustness measures as the optimization objective. 2) NA_{HCCA} and NA_{HBCA} have similar malicious effects and show higher damage ability than NA_{HDA} in most situations, and LA_{HBCA} seems to be the most malicious link attack in all situations.

5.4 Application on real networks

In this section, we conduct experiments on the real-world network, namely, WU Power Grid network [41], to show the potential applications in reality. The network consists of 217 nodes and 320 edges, modeled from the west Europe power network where the nodes represent generators and links represent high-voltage transmission lines between them. First, the change of average shortest path length and assortativity in the process of optimizing by HCA and using p_c^t, R, R_l, $IntE$, $a(G)$, and $\overline{\lambda}$ as the optimization objectives for 3×10^4 steps are reported in Figs. 15 and 16.

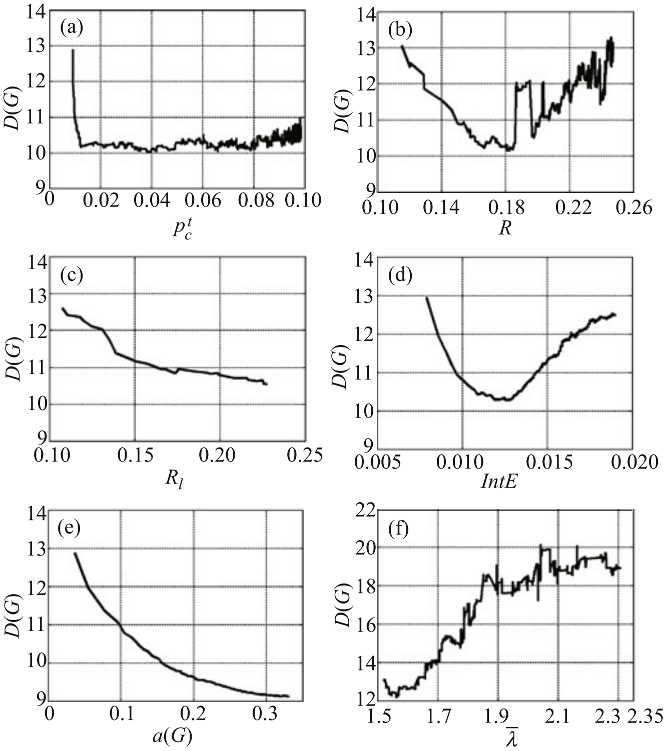


Fig. 15 The change of average shortest path length during optimization on the WU Power Grid network. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

The results in Figs. 15 and 16 show similar trends with those on the above synthetic networks. Furthermore, we record the size of largest connected subgraphs and communication efficiency in the optimized networks guided by different measures in Figs. 17–20. As it can be seen, similar conclusions with those on the above synthetic networks can also be obtained.

6 Conclusions

In this paper, systematic comparative analyses on nine robustness measures are conducted from multiple viewpoints. Both the sensitivity of these measures to the changes in robustness and their performance in guiding the optimization process to find more robust networks are studied. The studied measures show different sensitivities to the changes in robustness, where $\upsilon(G)$ and $\omega(G)$ almost fail to reflect the changes and the seven other measures can show the changes to different extents.

The experiments on optimized networks were conducted. The changes of network functionalities during the optimization process are determined by the optimization objectives. For example, the average shortest path length changes a lot

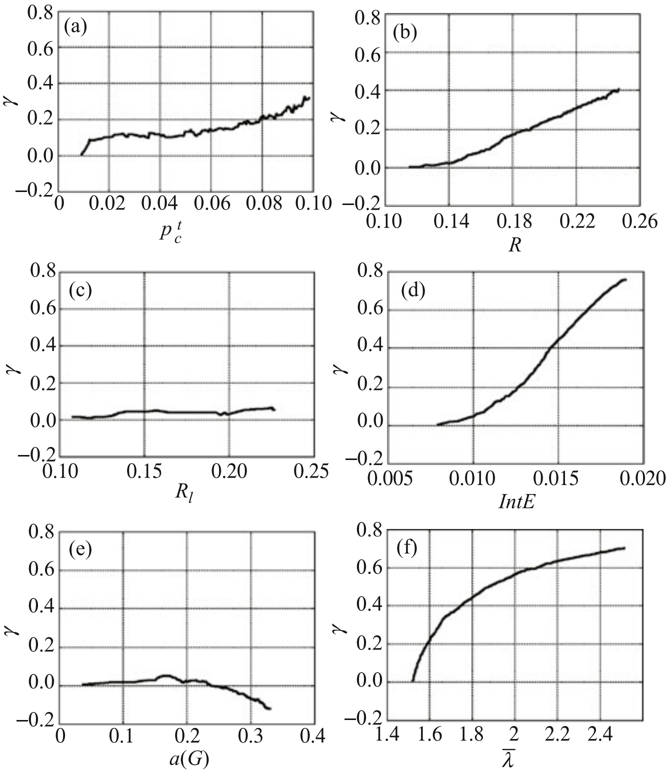


Fig. 16 The change of assortative coefficient during optimization on the WU Power Grid network. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

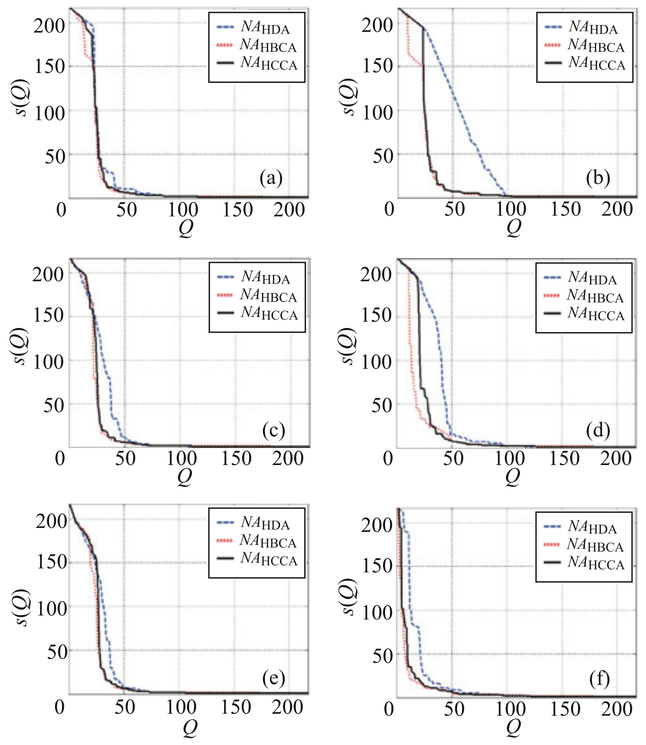


Fig. 17 The change of the size of largest connected subgraphs of optimized WU Power Grid network in the process of node attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

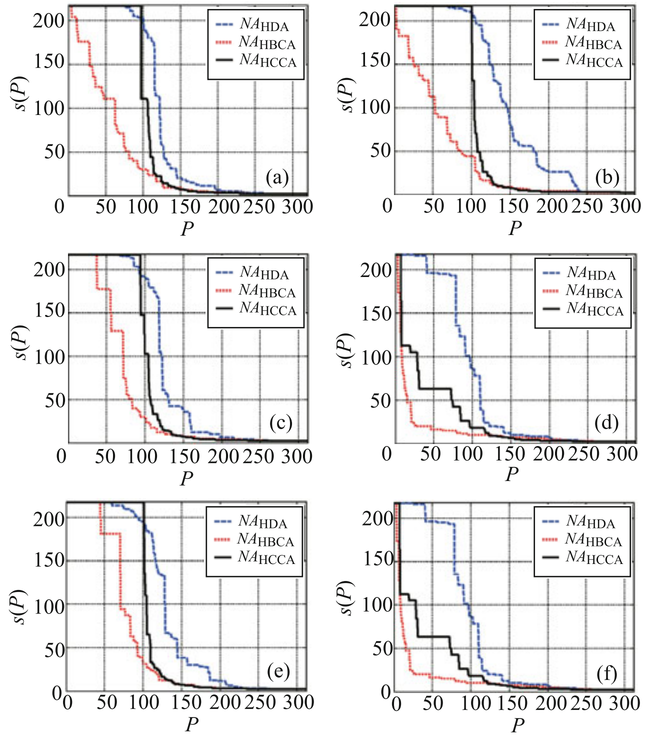


Fig. 18 The change of the size of largest connected subgraphs of optimized WU Power Grid network in the process of link attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

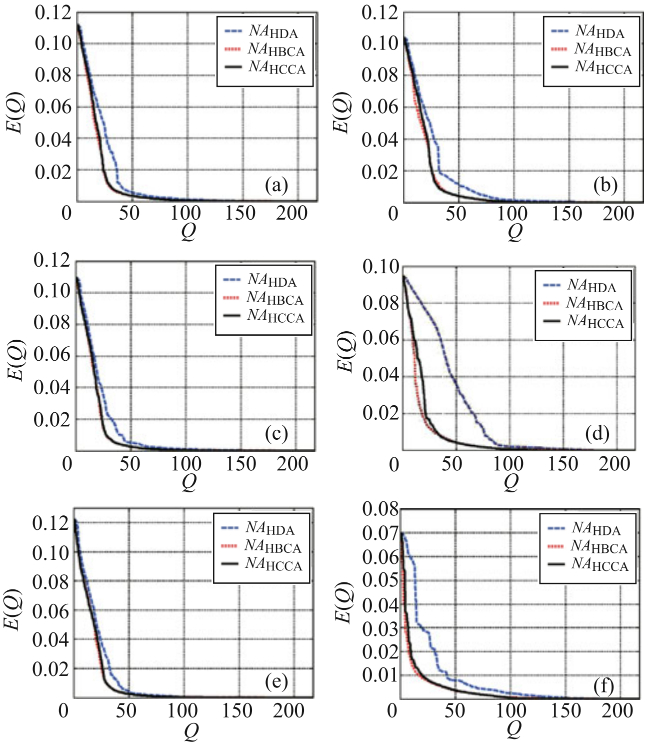


Fig. 19 The change of the communication efficiency of optimized WU Power Grid network in the process of node attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

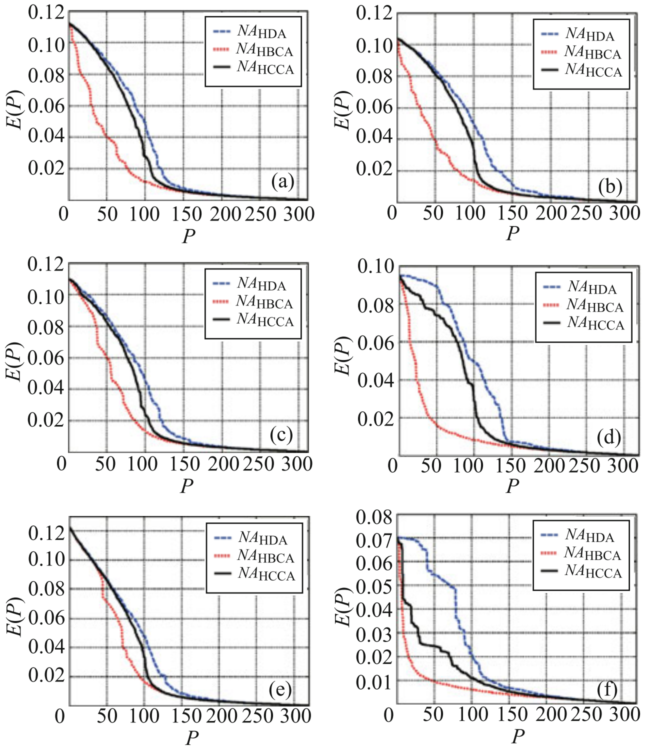


Fig. 20 The change of the communication efficiency of optimized WU Power Grid in the process of link attacks. The results are averaged over ten independent runs. (a) p_c^t; (b) R; (c) R_l; (d) $IntE$; (e) $a(G)$; (f) $\overline{\lambda}$

when optimizing R, $IntE$, $a(G)$, and especially $\overline{\lambda}$. Among these changes, R, p_c^t and $\overline{\lambda}$ seem to sacrifice the average shortest path length to improve themselves. A very interesting phenomenon is that the optimization over these three measures always causes a slight increasing of network assortativity.

A robust network in terms of certain robustness measure may be fragile in terms of other measures, especially when these measures are uncorrelated or negatively correlated with each other. However, if the robustness measures are closely correlated with each other, they can often be improved together.

These results indicate that it is not simple to apply a robust network into practical situations, and there are many network characteristics that need to be considered and balanced. During the optimization process, taking more suitable robustness measures into consideration is a promising way to generate more robust networks.

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

References

1. Albert R, Barabási A L. Statistical mechanics of complex networks. Reviews of Modern Physics, 2002, 74(1): 47
2. Newman M E J. The structure and function of complex networks. SIAM Review, 2003, 45(2): 167–256
3. Dorogovtsev S N, Mendes J F F. Evolution of Networks: from Biological Nets to the Internet and WWW. Oxford: Oxford University Press, 2013
4. Watts D J, Strogatz S H. Collective dynamics of small-world networks. Nature, 1998, 393(6684): 440–442
5. Barabási A L, Albert R. Emergence of scaling in random networks. Science, 1999, 286(5439): 509–512
6. Adamic L A, Huberman B A. Power-law distribution of the World Wide Web. Science, 2000, 287(5461): 2115
7. Gao J, Buldyrev S V, Havlin S, Stanley H E. Robustness of a network of networks. Physical Review Letters, 2011, 107(19): 195701
8. Albert R, Jeong H, Barabási A L. Error and attack tolerance of complex networks. Nature, 2000, 406(6794): 378–382
9. Paul G, Sreenivasan S, Stanley H E. Resilience of complex networks to random breakdown. Physical Review E, 2005, 72(5): 056130
10. Callaway D S, Newman M E J, Strogatz S H, Watts D J. Network robustness and fragility: percolation on random graphs. Physical Review Letters, 2000, 85(25): 5468–5471
11. Cohen R, Erez K, Ben-Avraham D, Havlin S. Resilience of the Internet to random breakdowns. Physical Review Letters, 2000, 85(21): 4626–4628
12. Cohen R, Erez K, Ben-Avraham D, Havlin S. Breakdown of the Internet under intentional attack. Physical Review Letters, 2001, 86(16): 3682–3685
13. Paul G, Tanizawa T, Havlin S, Stanley H E. Optimization of robustness of complex networks. The European Physical Journal B Condensed Matter and Complex Systems, 2004, 38(2): 187–191
14. Schneider C M, Moreira A A, Andrade J S, Havlin S, Herrmann H J. Mitigation of malicious attacks on networks. Proceedings of National Academy of Sciences of the United States of America, 2011, 108(10): 3838–3841
15. Zeng A, Liu W. Enhancing network robustness against malicious attacks. Physical Review E, 2012, 85(6): 066130
16. Louzada V H P, Daolio F, Herrmann H J, Tomassini M. Generating robust and efficient networks under targeted attacks. In: Król D, Fay D, Gabryś B, eds. Propagation Phenomena in Real World Networks. Intelligent System Reference Library, Vol 85. Springer International Publishing, 2015, 215–224
17. Wu J, Barahona M, Tan Y J, Deng H Z. Spectral measure of structural robustness in complex networks. IEEE Transactions on Systems Man and Cybernetics Part A: Systems and Humans, 2011, 41(6): 1244–1252
18. Ma L, Liu J, Duan B, Zhou M. A theoretical estimation for the optimal network robustness measure R against malicious node attacks. Europhysics Letters, 2015, 111: 28003
19. Louzada V H P, Daolio F, Herrmann H J, Tomassini M. Smart rewiring for network robustness. Journal of Complex Networks, 2013, 1(2): 150–159
20. Buesser P, Daolio F, Tomassini M. Optimizing the robustness of scale-free networks with simulated annealing. In: Proceedings of International Conference on Adaptive and Natural Computing Algorithms. 2011, 167–176
21. Zhou M, Liu J. A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks. Physica A: Statistical Mechanics and its Applications, 2014, 410: 131–143
22. Holme P, Kim B J, Yoon C N, Han S K. Attack vulnerability of complex networks. Physical Review E, 2002, 65(5): 056109
23. Qin J, Wu H, Tong X, Zheng B. A quantitative method for determining the robustness of complex networks. Physica D: Nonlinear Phenomena, 2013, 253: 85–90
24. Zhou M, Liu J. A two-phase multi-objective evolutionary algorithm for enhancing the robustness of scale-free networks against multiple malicious attacks. IEEE Transactions on Cybernetics, 2017, 47(2): 539–552
25. Duan B, Liu J, Zhou M, Ma L. A comparative analysis of network robustness against different link attacks. Physica A: Statistical Mechanics and its Applications, 2016, 448: 144–153
26. Ma L, Liu J, Duan B. Evolution of network robustness under continuous topological changes. Physica A: Statistical Mechanics and its Applications, 2016, 451: 623–631
27. Tang X, Liu J, Zhou M. Enhancing network robustness against targeted and random attacks using a memetic algorithm. Europhysics Letters, 2015, 111(3)
28. Bollobás B. Modern Graph Theory. New York: Springer Science & Business Media, 1998

29. Brandes U. On variants of shortest-path betweenness centrality and their generic computation. Social Networks, 2008, 30(2): 136–145

30. Estrada E, Higham D J, Hatano N. Communicability betweenness in complex networks. Physica A: Statistical Mechanics and its Applications, 2009, 388(5): 764–774

31. Bonacich P. Some unique properties of eigenvector centrality. Social Networks, 2007, 29(4): 555–564

32. Hage P, Harary F. Eccentricity and centrality in networks. Social Networks, 1995, 17(1): 57–63

33. Borgatti S P. Centrality and network flow. Social Networks, 2005, 27(1): 55–71

34. Frank H, Frisch I T. Analysis and design of survivable network. IEEE Transactions on Communication Technology, 1970, 18(5): 501–519

35. Bauer D, Boesch F, Suffel C, Tindell R. Connectivity extremal problems and the design of reliable probabilistic networks. The Theory and Application of Graphs, 1981, 89–98

36. Harary F. Conditional connectivity. Networks, 2983, 13(3): 346–357

37. Fiedler M. Algebraic connectivity of graphs. Czechoslovak Mathematical Journal, 1973, 23(98): 298–305

38. Merris R. Laplacian matrices of graphs: a survey. Linear Algebra Applications, 1994, 197: 143–176

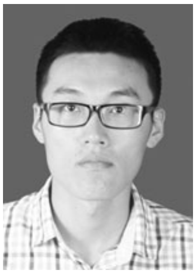
39. Boesch F, Frisch I T. On the smallest disconnecting set in a graph. IEEE Transactions on Circuit Theory, 1968, 15(3): 286–288

40. Latora V, Marchiori M. Efficient behavior of small-world networks. Physical Review Letters, 2001, 87(19): 198701

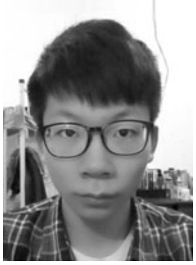
41. Zhou Q, Bialek J W. Approximate model of European interconnected system as a benchmark system to study effects of cross-border trades. IEEE Transactions on Power Systems, 2005, 20(2): 782–788

Jing Liu is an awardee of the NSFC Excellent Young Scholars Program in 2015. She received the BS degree in computer science and technology and the PhD degree in circuits and systems from Xidian University (XDU), China in 2000 and 2004, respectively. In 2005, she joined XDU as a lecturer, and was promoted to a full professor in 2009. From 2007 to 2008, she was a post-doctoral research fellow with the University of Queensland, Australia, and from 2009 to 2011, she was a research associate with the University of New South Wales - Canberra, Australia. She is currently a full professor with the Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, XDU. Her research interests include evolutionary computation, complex networks, fuzzy cognitive maps, multiagent systems, and data mining. She is the associate editor of IEEE Trans. Evolutionary Computation.

Mingxing Zhou received the BS degree in intelligence science and technology from Xidian University (XDU), China and the MS degree in circuits and systems from the Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, XDU in 2013 and 2016, respectively. His research interests include evolutionary algorithms, complex networks, and data mining.



Shuai Wang received the BS degree in intelligence science and technology from Xidian University (XDU), China in 2015. Now, he is pursuing the PhD degree in circuits and systems from the Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, XDU. His research interests include complex networks and evolutionary algorithms.



Penghui Liu received the BS degree in physics from Xidian University (XDU), China in 2015. Now, he is pursuing the MS degree in circuits and systems from the Key Laboratory of Intelligent Perception and Image Understanding of Ministry of Education, XDU. His research interests include complex networks and evolutionary games.