Physica A 457 (2016) 129–137

Contents lists available at ScienceDirect

Physica A

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

The dynamic correlation between degree and betweenness of complex network under attack

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

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

HIGHLIGHTS

- The paper verifies network robustness through variants of the characteristics.
- The decaying of betweenness in the process of attack is different to that of degree.
- Dynamic betweenness-degree correlation for scale-free network obeys a power-law.
- The betweenness-degree correlation for small-world network presents irregularly.

ARTICLE INFO

Article history:
Received 2 November 2015
Received in revised form 22 January 2016
Available online 4 April 2016

Keywords:
Complex networks
Betweenness centrality
Betweenness-degree correlation
Network attack
Invulnerability

ABSTRACT

Complex networks are often subjected to failure and attack. Recent work has addressed the resilience of complex networks to either random or intentional deletion of nodes or links. Here we simulate the breakdown of the small-world network and the scale-free network under node failure or attacks. We analyze and discuss the dynamic correlation between degree and betweenness in the process of attack. The simulation results show that the correlation for scale-free network obeys a power law distribution until the network collapses, while it represents irregularly for small-world network.

1. Introduction

In recent decades, complex networks have received an increasing amount of attention. A large number of complex systems can be described as complex networks, as shown by many real-world examples ranging from biology to medicine, sociology and engineering [1,2]. Scientists try to explore structural features and dynamics of real-world systems in recent years [1,3]. Many networks possess unique structural properties such as scale-free [4] and small-world attributes [5].

The scale-free networks such as the World Wide Web (WWW) [4,6], Internet [7], metabolic networks [8], and protein networks [9], display an unexpected degree of robustness. Their connectivity distribution decays as a power-law degree distribution $P(k) \propto k^{-\gamma}$ with an exponent γ that commonly ranges between 2 and 3 [10]. Network with a power-law degree distribution is extremely heterogeneous.

The exponential networks are characterized by a $P(k)$ distribution that is peaked at an average $\langle k\rangle$ and decays exponentially for large k. The exponential networks [11,5] leads to a fairly homogeneous network, in which each node has approximately the same number of links, $k \approx \langle k\rangle$.

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

http://dx.doi.org/10.1016/j.physa.2016.03.075
0378-4371/© 2016 Elsevier B.V. All rights reserved.

The performance of the complex network relies on the robustness against failure or attacks. The failure (also called random attack) removes nodes/edges with uniform probability, as simple and successive error in a network. The (intentional) attack removes nodes/edges in a descending order of their importance, usually targets the most important components in the network.

It is proved the essential to study the invulnerability of the complex network. In the literature, a lot of helpful conclusions based on robustness measurements have been proposed. The scale-free network is tolerant to failure but vulnerable to intentional attack, while a small fraction of node/edge deletion can make the small-world network lost the functionality [12–15].

Many measurements are therefore proposed to evaluate the vulnerability of the complex network. A frequently used measurement is the existence of the giant component [12–16]. The giant component is a connected component of a given network that contains a constant fraction of the entire vertices. The attack to a network can be exactly mapped to a standard percolation process. A network percolates and keeps general connected when the giant component exists. The critical percolation fraction f_c at which the system practically falls apart is observed in Ref. [12]. For exponential networks, $f_c \approx 0.28$, while for scale-free networks, $f_c \approx 0.18$. The average inverse geodesic length l^{-1} and the clustering coefficient C are proposed to measure the efficiency of the network [16,17]. The definitions are shown as follows.

$$l^{-1} = \left\langle \frac{1}{d(v,w)} \right\rangle = \frac{1}{N(N-1)} \sum_{v \in V} \sum_{w \neq v \in V} \frac{1}{d(v,w)'}$$

$$C(G) = \frac{1}{N} \sum_{i \in G} C_i, \quad C_i = \frac{\#\ \text{edge in}\ G_i}{k_i(k_i-1)/2}. \tag{1}$$

Another measurement is the diameter d which indicates the interconnectedness of a network, defined as the average length of the shortest paths between any two nodes in the network [12,16]. He et al. used the total connectedness as the criterion of network breakdown [18].

This question of the importance of nodes in a network is thus of primary interest since it concerns crucial subjects such as networks resilience to attacks [3–5] and also immunization against epidemics [6].

The degree is a local quantity which does not reflect accurately the importance of a node in the network. The betweenness is a global indicator because it is determined by its capability to provide efficient paths between separated regions of the network. It is essential to reveal how the global centrality depends on the local centrality. Moreover, the betweenness centrality is more calculation-complicated than the degree centrality. If there is correlation between them, one may approximately estimate the betweenness from the degree. So it is meaningful to identify the correlation between the degree and the betweenness.

To make betweenness centrality practically computable, several approximation algorithms have been proposed. The methods are based on random-walk [19], neighbor-information [20], or sampling [21,22]. In them, some methods are related to degree information [20], and others are not [19,21,22].

The scale-free network shows clear signs of correlation between the degree and the betweenness. As network becomes more clustered, the correlation is very difficult to conclude because the degree distribution is narrow [16]. Barthélemy pointed out that betweenness centrality in a scale-free network is increasing with connectivity as a power law with an exponent $\eta \geq 2$ [23].

As mentioned, a mass of work have addressed to estimate the robustness of complex networks. The correlation between the degree and the betweenness is also investigated. However, does the correlation still exist when the complex network suffers from attack? If exists, how the correlation changes dynamically in the process of attacks?

In this paper, we estimate the invulnerability of complex network through the variant of degree and betweenness. The correlation between degree and betweenness is also investigated when the fraction of the network is removed gradually.

The paper is organized as follows. In Section 2 we introduce the networks to be estimated. In Section 3 we discuss the correlation between the degree and the betweenness when networks under failure or attack. In Section 4, we draw the conclusions.

2. Networks

Different algorithms have been proposed for the study of different geometric properties of complex networks. A lot of network models are generated based on the algorithms, in which two generic models, the Barabási–Albert (BA) model for the scale-free network and the Watts–Strogatz (WS) model for the small-world network have been widely studied.

2.1. Barabási–Albert model of scale-free network

In real-world, a lot of networks have a power-law distribution of degree, manifesting a scale-free nature of the network. The usually used BA model for scale-free network is defined as follows [4,6].

- Initial condition: to start with the network consists of m_0 vertices and no edges.
- Growth: one vertex v with m edges is added in each step.

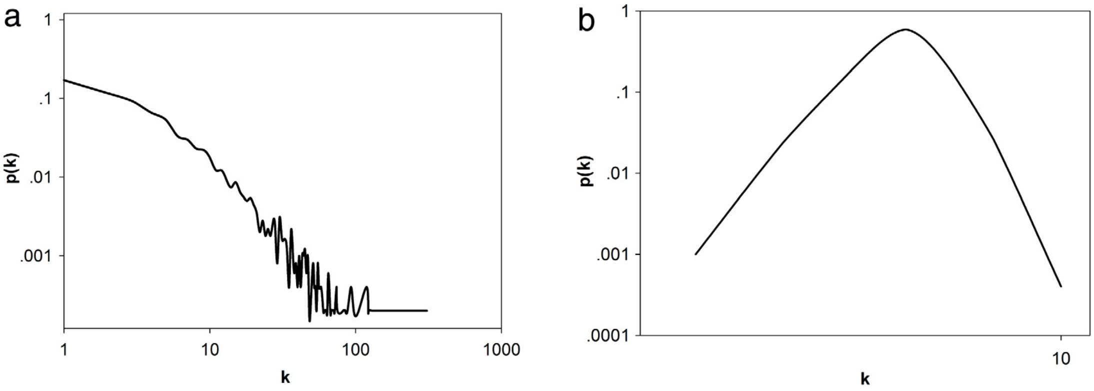

Fig. 1. Degree distribution curve for (a) BA scale-free network with $N = 10\,000$ nodes (log–log scale) and (b) WS small-world network with $N = 10\,000$ nodes (linear-log scale).

- Preferential attachment: an edge is added to an old vertex with the probability proportional to its degree. Concretely, the probability P_u for a new vertex v to be attached to u is: $P_u = \frac{k_u}{\sum_{w \in V} k_w}$.

The growth step is repeated $(N - m_0)$ times to construct a network with the size of N, for each growth step the preferential attachment step is repeated m times. The described BA model has been shown to generate the scale-free network with the logarithmically increasing average geodesic length with size N.

The curve in Fig. 1(a) shows an approximate straight line in a log–log plot, which indicates the BA network has a power-law degree distribution.

2.2. Watts–Strogatz model of small-world network

Milgram showed that real social networks are rich in short paths in 1967, which is known as "six degrees of separation". Many real-world networks have short average path length and high cluster coefficient, comparable to that of random networks, is called small-world phenomenon. The structural properties of small-world network are somehow in between regular and random networks. Watts and Strogatz introduced the WS model constructing small world network [5].

We use the original random rewiring algorithm to construct an undirected and unweighted Watts–Strogatz network [5]. Considering a ring graph with N nodes each connected to its m-nearest neighbors, one should choose a node and one of the edges to connect with its neighbors. Then, this edge is reconnected to a node randomly chosen over the graph with probability P, provided that the duplication of edges and self-loops are forbidden. This process is repeated until all nodes and their non-rewired edges are met. For the value of P in (0, 1), the resulting network has short characteristic path length and high clustering coefficient and the average degree will be $\langle k \rangle = 2$ m.

The degree distribution of WS network obeys a Poisson distribution, as shown Fig. 1(b). The distribution indicates that the WS network is a single scale network [24].

3. Correlation between degree and betweenness

In this section, we estimate the invulnerability of complex networks and try to explore the dynamic correlation between the degree and the betweenness in the process of failure or attacks.

3.1. Attack strategies

Usually, failure removes the randomly selected nodes. Instead, attack removes the most important nodes intentionally according to a certain criterion. We consider four different criteria once used in Ref. [18] to determine the importance of the node.

- ID removal: is based on the initial degree distribution;
- IB removal: is based on the initial betweenness distribution;
- RD removal: is based on the recalculated degree distribution at each step;
- RB removal: is based on the recalculated betweenness at each step.

Notably, the criterion in RD strategy and RB strategy is recalculated in all connected subnetworks.

3.2. Basic concepts

In this work, we use the following basic concepts to evaluate the robustness of complex networks.

The degree k_v of v is defined as the number of edges that connected to this node.

$$k_v = \sum_u a_{vu}. \tag{2}$$

The betweenness counts the fraction of shortest paths going through a given node.

$$B_i = \sum_{j \neq l \neq i} \left[N_{jl}(i)/N_{jl} \right] \tag{3}$$

where N_{jl} is the total number of shortest paths from node v_j to node v_l and $N_{jl}(i)$ is the number of shortest paths from v_j to v_l going through v_i. Notably, the shortest path exists only when two nodes locate in the same connected component. In this paper, the calculation of betweenness refers to the connected sub-network.

The betweenness centrality g is derived by rescaling the betweenness by $(N-1)(N-2)/2$ to get a number in the interval of [0, 1].

$$g = 2B_i/(N-1)(N-2). \tag{4}$$

The correlation between the betweenness and the degree $B(k) \sim k$ shows the correlation that the average betweenness of all the nodes with a degree k how changes with the value k.

3.3. Invulnerability and correlation discussion

In the simulation, the node removal fraction is set to 0.01. Namely, one percent of nodes will be removed at each attack step. The degree and the betweenness are then calculated based on current structure of the network. At the beginning of attack, only some single nodes break apart. At f_c, the network practically falls apart, the main cluster breaking into small pieces, leading the size of the giant component to be zero. In other words, all the nodes of the network at f_c are isolated. The emphasis of this work is to investigate the variants of degree and betweenness in the process of attack. For convenience, we consider the network is destroyed completely when the maximal degree close to zero.

3.3.1. Scale-free network

We generated a scale-free network with $N = 10\,000$ nodes by using BA model. The network begins with an initial connected network of $m_0 = 5$ nodes. New nodes are added to the network one at a time. Each new node is connected to $m = 3$ existing nodes with a probability that is proportional to the number of links that the existing nodes already have.

We implemented failure, ID, RD, IB, and RB five attack strategies on the network. In Fig. 2, we plot the characteristics (maximal degree, average degree, maximal betweenness, and average betweenness) of the scale-free network as functions of the fraction N_r/N of removed nodes. Because the values for the average degree and the average betweenness are too small to observe, we plot a sub-figure embedded in upper-right. We calculate the critical fraction from simulation data. The f_c for failure, ID, RD, IB, and RB are showed as 0.87, 0.36 0.22, 0.53, and 0.17, separately. From the curves shown in the Fig. 2, the harm of attack strategies behaves in such order: RB > RD > ID > IB > failure. The maximum degree and the maximum betweenness in intentional attacks decay more rapidly than failure, which indicates the scale-free network behaves robust to failure and vulnerable to intentional attacks. The observation is consistent to previous works [12,16].

Notably, the maximal degree and the maximal betweenness under intentional attacks decrease rapidly when removal fraction exceeds 0.02. The curve of the maximal betweenness centrality emerges a "spike" in the process of attack. The reason of this phenomenon can be explained as follows. The network is split into much smaller components when some nodes are removed. The betweenness of a node probably increases abruptly because the shortest paths via the node maybe increase due to the deletion of some important nodes. In addition, the number of the shortest paths may decrease when the size of the separated component shrinks. This further leads to the increasing of the betweenness centrality, as defined in formula (3).

Barthélemy proved that betweenness centrality (BC) has a power-law degree distribution which shows how the betweenness centrality depends on the connectivity [23]. The relation is shown as the following formula.

$$g \sim k^{\eta}. \tag{5}$$

We study the correlation between the betweenness and the degree shown in formula (5) is satisfied or not in the process of attacks. In Fig. 3, we plot the curves with different removal fractions for different attack strategies. For the scale free network, we can see that the correlation between the betweenness and the degree still obeys a power-law distribution except small violations for failure and IB attack. The slope of each curve is approximately the same, which indicates the betweenness-degree correlation keeps the power-law distribution in the process of attack. Notably, the correlation keeps well even if the removal fraction achieves 0.8 in failure, as shown in Fig. 3(a). The phenomenon reflects the strong robustness of scale free network to random attack from another viewpoint.

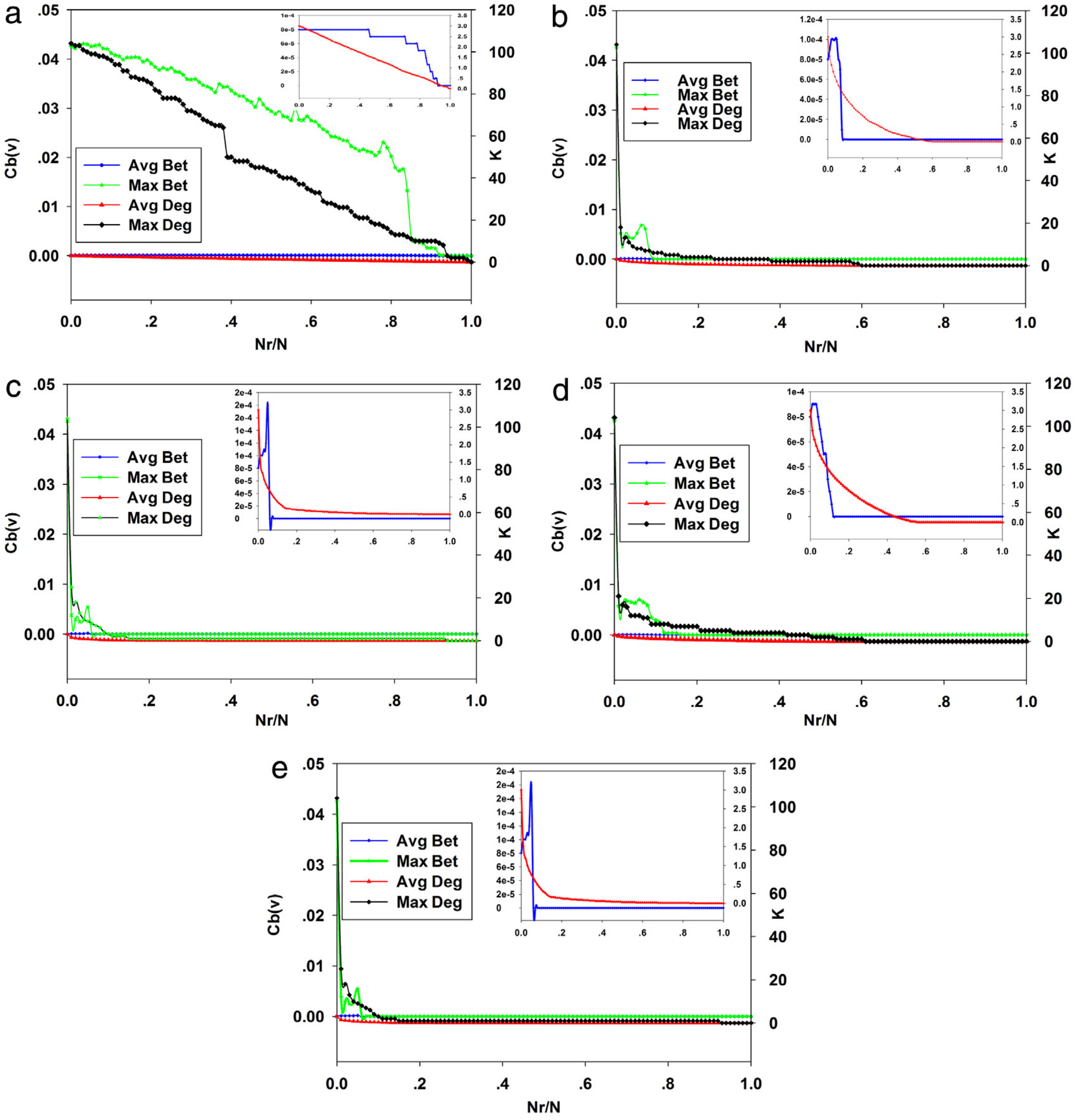

Fig. 2. Failure and attack tolerance for BA scale-free network with $N = 10\,000$ nodes. The attacks were based on (a) failure, (b) ID, (c) RD, (d) IB, and (e) RB strategies. We plot the characteristics of the scale-free network as functions of the fraction N_r/N of removed nodes. It shows double vertical axes, the left is betweenness centrality, and the right is degree.

The result shows that scale-free network behaves robust to failures while vulnerable to intentional attacks due to the homogeneous property. The correlation between the betweenness and the degree in scale-free network obeys a power-law distribution until the network collapses.

3.3.2. *Small-world network*

We also generated a small-world network using the WS model with $N = 10\,000$, $r = 4$, and $p = 0.01$. We implemented the same attacks on the network. In Fig. 4, we plot the characteristics (maximal degree, average degree, maximal betweenness, and average betweenness) of the WS network as functions of the fraction N_r/N of removed nodes.

Unlike failure, the maximal degree decays rapidly at the beginning of attacks and decays evenly in the sequential process. The average degree decays approximately linearly in the whole attack process. This is because that the degree distribution in the WS network is very narrow (in the experiment it ranges from 1 to 28), a fraction node removal results in an even degree decreasing. However, if some fractions are deleted by chance or intentionally, it probably forms bridge nodes. This causes the maximal betweenness and the average betweenness dramatically increases and appear a peak, then decay rapidly. The network lost the small-world property when a certain number of nodes are removed.

The fraction N_r/N need to collapse the small-world network for RD attack is 0.81, while for other attacks is 100%. It indicates the RD attack is a relatively efficient attack strategy to the WS network.

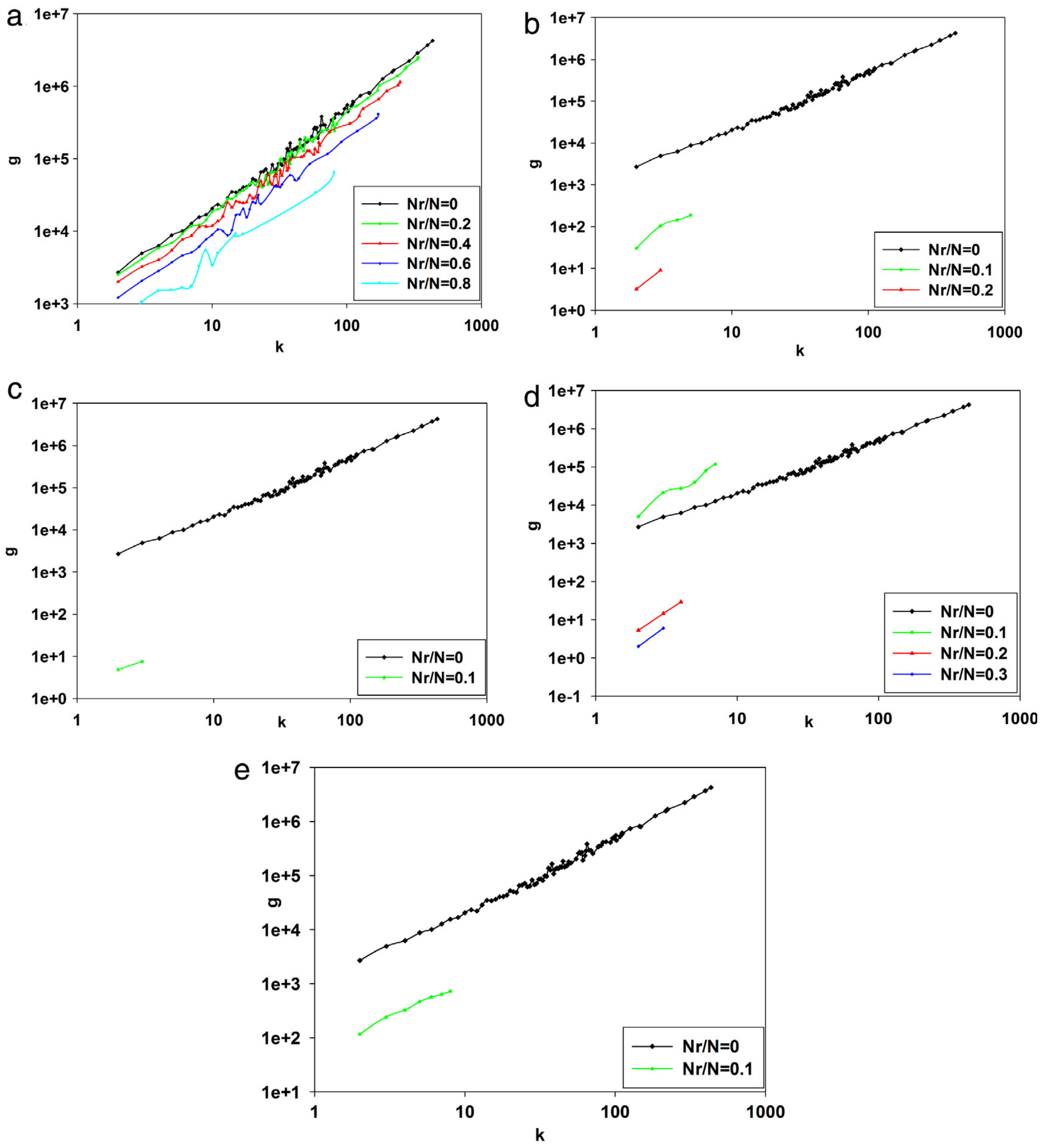

Fig. 3. The correlation between the degree and the betweenness for BA scale-free network with $N = 10\,000$ nodes. The attacks were based on (a) failure, (b) ID, (c) RD, (d) IB, and (e) RB strategies. We draw curves with different fractions $^{N_r}/_N$ are removed.

Limited to our knowledge, there is no detailed research on the correlation between degree and betweenness for the small-world network in the literature. We explore the dynamic correlation of the WS network through simulations. As shown in Fig. 5, the correlation between the degree and the betweenness represents irregularly. In the initial curve ($^{N_r}/_N = 0$), there is a break point is at the integer of $\kappa = \sum_i k_i P(k_i)$. The initial value of κ is 8 (the black diamond curve), it becomes smaller when the removed fraction increases. In cases of Random, ID and RD, the curves maintain the initial shape for a period. In cases of IB and RB, the curves lost the property rapidly. It indicates the higher efficiency of IB and RB strategies.

The simulation result shows that the small-world network is more robust to perturbations than the scale free network. However, the deletion of important nodes will damage the network functionality dramatically. The WS Network with a greater than expected number of hubs will have a greater fraction of nodes with high degree, and consequently the degree distribution will be enriched at high degree values. The heavy-tailed distribution makes the correlation between the degree and the betweenness is rather difficult to observe in the region of high degrees. The properties representing in small-world network should be further investigated in future work.

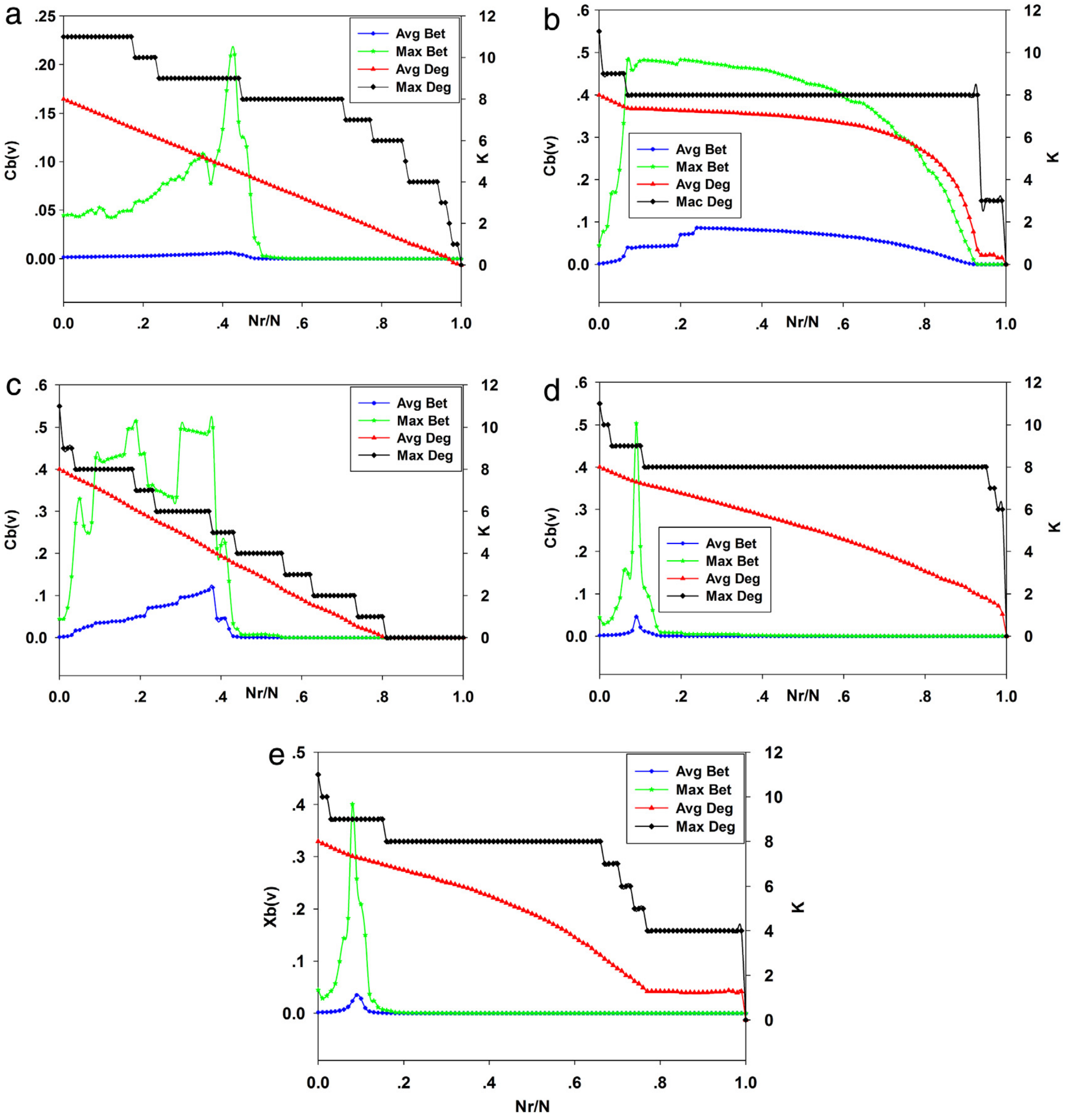

Fig. 4. Failure and attack tolerance for WS exponential network with $N = 10\,000$ nodes and $p = 0.01$. The attacks were based on (a) failure, (b) ID, (c) RD, (d) IB, and (e) RB strategies. We plot the characteristics of the scale-free network as functions of the fraction N_r/N of removed nodes. It shows two axes vertically, left is centrality of betweenness, right is degree.

4. Conclusions

In this paper, we investigated the invulnerability of the small-world network and the scale-free network through the changes of degree and betweenness in the process of attacks. We provided a new method to verify the invulnerability of complex networks through the variant of the characteristics (maximal degree, average degree, maximal betweenness, and average betweenness). The decaying of betweenness in the process of attack is different to that of degree. It decays fast, then emerges a spike, and converges to zero in the end. We simulated the *dynamic* correlation between degree and betweenness in the process of attacks. The results show that the dynamic correlation for scale-free network obeys the power-law distribution until the network collapses, and the betweenness-degree correlation keeps almost the same power-law slope in the process of attack. The correlation in the small-world network initially presents segment distribution with a break point of integer κ. The small-world property is lost gradually in the process of attack, and the phenomenon behaves more intensively on the strategies based on betweenness.

From the simulation, we concluded that the small-world network is more robust than the scale free network and the strategies based on betweenness are more efficient than that of other strategies. We proved the consistent fact from a new

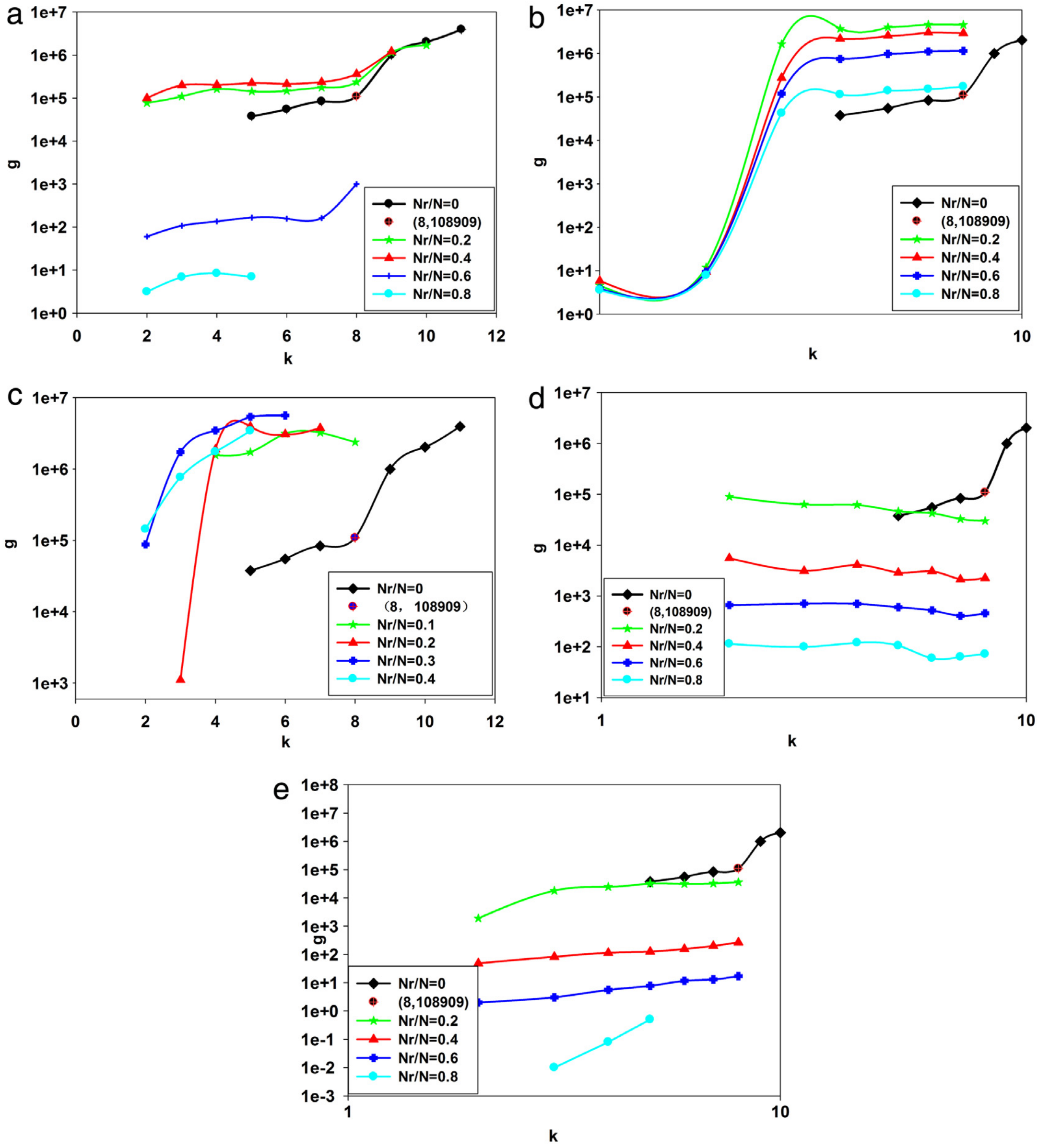

Fig. 5. The correlation between the degree and the betweenness for WS exponential network with $N = 10\,000$ nodes and $p = 0.01$. The attacks were based on (a) failure, (b) ID, (c) RD, (d) IB, and (e) RB strategies. We draw curves with different fractions N_r/N are removed. The axis is in a linear-log scale.

viewpoint. We hope the contribution of the work is helpful to understand the robustness of complex network from another viewpoint, although some works should be deeply conducted in the future.

Acknowledgments

Project 61572269 supported by NSFC. This work was supported by the Qingdao Fundamental Research Fund under Grant No. 13-1-4-164-jch. A Project of Shandong Province Higher Educational Science and Technology Program (No. J14LN25).

References

[1] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.U. Hwang, Phys. Rep. 424 (2006) 175.
[2] S.H. Strogatz, Nature 410 (2001) 268.
[3] M.E.J. Newman, A. Barabási, D.J. Watts (Eds.), The Structure and Dynamics of Networks, Princeton Univ. Press, Princeton, NJ, 2006.
[4] A.L. Barabási, R. Albert, Science 286 (1999) 5009.
[5] D.J. Watts, S.H. Strogatz, Nature 393 (1998) 440.

[6] R. Albert, H. Jeong, A.L. Barabási, Nature 401 (1999) 130.
[7] M. Faloutsos, P. Faloutsos, C. Faloutsos, Comput. Commun. Rev. 29 (1999) 251.
[8] H. Jeong, B. Tombor, R. Albert, Z.N. Oltvai, A.L. Barabási, Nature 407 (2000) 651.
[9] H. Jeong, S.P. Mason, A.L. Barabási, Z.N. Oltvai, Nature 411 (2001) 41.
[10] S.N. Dorogovtesev, J.F.F. Mendes, Evolution of Networks, Oxford University Press, Oxford, 2003.
[11] P. Erdös, A. Rényi, Publ. Math. Inst. Hung. Acad. Sci. 5 (1960) 17.
[12] R. Albert, H. Jeong, A.-L. Barabási, Nature 406 (2000) 378.
[13] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, Phys. Rev. Lett. 85 (2000) 4626.
[14] R. Cohen, K. Erez, D. ben-Avraham, S. Havlin, Phys. Rev. Lett. 86 (2001) 3682.
[15] D.S. Callaway, M.E.J. Newman, S.H. Strogatz, D.J. Watts, Phys. Rev. Lett. 85 (2000) 5468.
[16] P. Holme, B. Kim, C. Yoon, S. Han, Phys. Rev. E 65 (2002) 056109.
[17] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Physica A 320 (2003) 622.
[18] S. He, S. Li, H. MA, Physica A 388 (2009) 2243.
[19] M.E.J. Newman, Social Networks 27 (2003) 39.
[20] P.L. Szczepański, T.P. Michalak, T. Rahwan, International Conference on AAMAS, 2012, p. 239.
[21] M.H. Chehreghani, Comput. J. 57 (2013) 1489.
[22] D.A. Bader, S. Kintali, K. Madduri, M. Mihail, Lecture Notes in Comput. Sci. 4863 (2007) 124.
[23] M. Barthélemy, Eur. Phys. J. B 38 (2004) 163.
[24] L.A.N. Amaral, A. Scala, M. Barthélémy, H.E. Stanley, Proc. Natl. Acad. Sci. USA 97 (2000) 11149.