Analysis of Robustness of Complex Networks based on Optimization Theory

Yu Sun, Peiyang Yao, Dongdong Shui, Yun Zhong

Information and Navigation College, Air Force Engineering University, China

*suny.z@qq.com

Keywords: complex network; robustness; network structure; optimization

Abstract. The analysis of robustness of complex networks tries to find out the relation between the structure of a complex network and its robustness performance, which will be beneficial to some work such as network design. The robustness measurement of a complex network is defined at first to evaluate its robustness performance. Then a framework is put forward for robustness analysis of complex networks. The framework analyzes the impacts of structural parameters of a complex network on its robustness by comparing the network structures and its robustness performance before and after optimization. These network structural parameters include the degree distribution, the average clustering coefficient, the network efficiency and so on. An optimization method based on the variable neighborhood search method is developed to solve the network optimization problem appearing in the framework. Finally, through the application of this analytical framework, it is found that if the degree of nodes in a complex network tends to be consistent, then the upper bound of the robustness measurement of the network will increase. In addition, the regression relationships between the robustness measurement and some structural parameters of the network, such as the average clustering coefficient, the network efficiency and so on, will become evident.

1 Introduction

Since Albert et al. pointed out that the scale-free network is very vulnerable under a deliberate attack [1][2], how to improve the robustness of complex networks has gradually attracted attentions of people [3][4]. Network structure determines the function of the network. Only in depth study of the impact that the structure of a complex network has on the its robustness, can we be more efficient in designing and optimizing networks with the goal to improve their robustness. Robustness analysis of complex networks is just to explore the relationship between the structure of a complex network and its robustness performance through analytical or experimental methods.

In early research, the seepage theory was often used to calculate the critical node removal ratio which would result in the phase transition of a complex network. Then, the impact of the degree distribution of a network had on its robustness would be measured through the comparison of critical node removal ratios of networks with different degree distributions [5][6][7]. But there still existed problems in those researches. One was that the definition of the critical state of network, which indicated the occurrence of the phase transition, was not suitable for every kinds of network [8]. The other was that the critical node removal rate of a network under intentional attack could not be calculated accurately by the seepage theory [9]. Thus, adopting the experimental way to analyze the robustness of complex networks becomes more and more popular. Wu et al. thought the robustness of a network came from the redundancy of edges in the network, then on that basis proposed a robustness measurement of complex networks, which was named natural connectivity, and further analyzed the effect that the degree distribution, small-world feature and degree correlation of a network had on its robustness with the robustness measurement [10][11]. Hu et al. measured the robustness of a network with indexes such as the size of the largest connected component and the average shortest path length [12]. And a result concluded from the comparison of robustness of random networks, small-world networks and scale-free networks was that the robustness of small-world networks was best. Schneider et al. regarded the average size of the largest connected component of a network under attack as the measurement of its robustness. It was

found that under the condition of the deliberate attack, the robustness of the network having the "onion" structural characteristic was better within the networks featured by power-law degree distribution [13][14][15]. The influence of some other structural parameters, such as the clustering coefficient, the assortativity coefficient, on the robustness of a network was studied with similar robustness measurement in [16].

If the number of nodes and edges in a network is decided, then structural parameters of the network are related with each other. In other words, if one structural parameter of the network is changed, then other structural parameters will vary. Thus, it is difficult to apply the idea of controlling variables in experiments of analyzing the influence of one structural parameter of a network has on its robustness. As a result, some conclusions made from experiments may be inaccuracy. However, although structural parameters of a network are related to each other, their impact on the structure of the network is not the same. It is generally believed that the degree distribution of a network can affect the structure more heavily than other structural parameters [17]. So it is regarded as a low-order feature of a complex network. In addition, a set constituted by all complex networks having the same number of nodes and edges and the same degree distribution is classified to an one-order zero-model in statistical research on properties of networks, which also shows the fundamental influence that the degree distribution of a network has on its structure [18]. Therefore, this paper assumes that the degree distribution is the main factor that affects the robustness of a complex network. Since the degree distribution does not completely determine the structure of a network, the robustness of the network may still change if some other structural parameters of the network vary. Thus, the degree distribution of a network can only determine the upper limit of robustness performance of the network. Then, what kind of degree distribution will maximize the upper limit of robustness performance of a network? If the degree distribution of a network is given, what are the relationships between the robustness and other structural parameters of the network? Trying to answer these problems is the main content of this paper.

This paper will define the robustness measurement of complex networks first, then design a robustness analysis framework of complex networks based on optimization theory and finally analyze the relationship between the structure of a complex network and its robustness with the use of this framework.

2 Robustness Measurement of Complex Networks

The robustness of a complex network usually refers to the ability of the network to maintain its basic functions under the condition that the network encounters the failure of nodes or edges. There are two ways to measure the robustness of a network. One is using some relative simple features of the network whose state under attack will be simulated. These features include the size of the largest connected component, the critical node removal ratio and so on. The other is using some relative complex indicators defined based on the initial structure of the network. These indicators include toughness, integrity, tenacity, node connectivity, degree distribution entropy, network efficiency, algebraic connectivity, natural connectivity and so on. Due to simplicity and intuitivism, the former way has been used widely [19][20]. Compared to the former way, no one of indicators defined in the latter way is fully proved to be effective in measuring the robustness of a complex network. Therefore, the former way is adopted in this paper.

Suppose there are N nodes in a complex network. If the nodes in the network suffer failure one by one, then the change of the size of the largest connected component of the network is shown in Fig. 1.

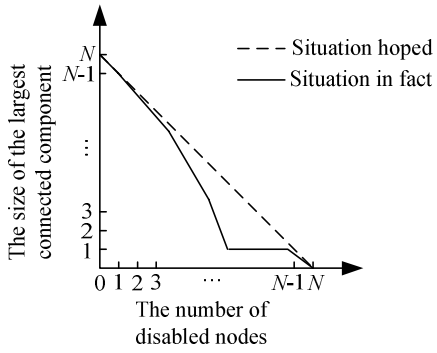


Figure 1. Change of the size of the largest connected component.

In Fig. 1, the area encircled by the solid line and the coordinate axis is denoted by S' and the area encircled by the dotted line and the coordinate axis is denoted by S. Then an index suggested to be used to measure the robustness of the network [21] is defined as

$$R = \frac{S'}{S} = \frac{1}{N^2}(2\sum_{q=0}^{N} S(q) - N) \qquad (1)$$

where $S(q)$ represents the size of the largest connected component after q nodes suffer failure. According to the definition, the R satisfies $0 < R \le 1$. The larger the R is, the better the robustness of the network is. The index R is linearly related to the robustness measurement proposed in [13][14][15] but it is more intuitive in measuring the robustness of a complex network.

Before the robustness measurement R of a complex network is calculated, the attack mode ready for the network such as random node attack, degree priority node attack et al. should be known. The value of the robustness measurement of a network is different when the network is faced with different network attack modes. Unfortunately, the attack mode which a network will suffer is uncertain in real environment. Thus, the robustness of a network should be evaluated comprehensively based on its robustness performance under different attack modes. The idea of [9] adopted the weighted summation of values of robustness measurement calculated according to different attack modes for a network. However, an attacker is always tries to find the most efficient attack mode to destroy a network. Thus, the minimum of values of robustness measurement is chosen to evaluate the robustness of the network in this paper. Suppose the set constituted by all possible attack modes for a network is $AT = \{at_1, at_2, \ldots\}$ where at_i represents the number i type of attack mode. If $R(at_i)$ is the value of robustness measurement calculated by formula (1) with the attack mode at_i, then the comprehensive robustness measurement of the network is defined as

$$R^{\mathrm{I}} = \min_{at_i \in AT} R(at_i). \qquad (2)$$

Considering that the random node attack, degree priority node attack and betweenness priority node attack are commonly used attack modes, this paper constructs the set AT with these three kinds of attack modes.

3 Framework for Robustness Analysis of Complex Networks

The structural parameters of a network, such as the degree distribution, the average clustering coefficient and the shortest path length et al., determine the structure of the network together under the condition that the number of nodes and the number of edges of the network are decided. Since the degree distribution of a network has relatively large impact on the structure of the network [17], the influence that the degree distribution has on the upper bound of the robustness measurement of the network needs to be analyzed first. The effect that other structural parameters of the network have on its robustness is analyzed then with a fixed degree distribution. The framework proposed for robustness analysis of complex networks is shown in Fig. 2.

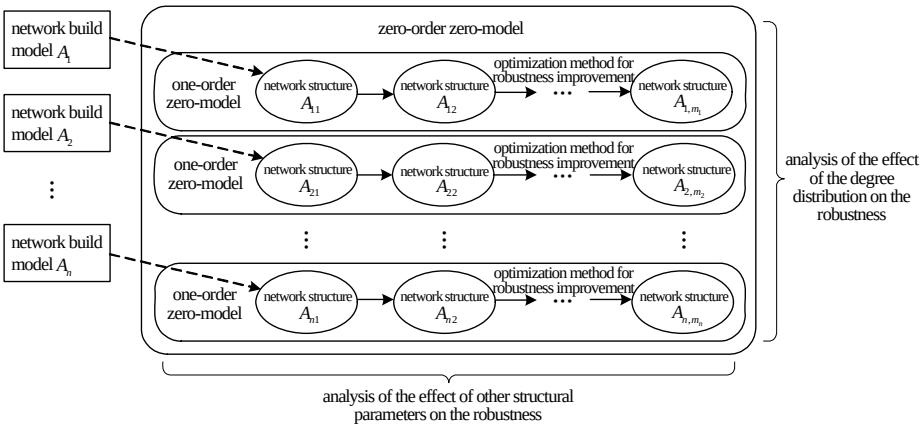


Figure 2. The framework for robustness analysis of complex networks.

In Fig. 2, the zero-order zero-model is a set constituted by all the networks having the same number of nodes and edges. An one-order zero-model is a subset of the zero-order zero-model [18]. That is, networks in an one-order zero-model not only have the same number of nodes and edges, but also have the same degree distribution. The framework generates complex networks whose degree distributions are different through a variety of network build models first. Then it improves the robustness of these networks based on the optimization theory. Robustness improvement of a network is carried out within the one-order zero-model of the network. The largest value of robustness measurement of the network is regarded as the upper bound of the robustness measurement of the network which has a fixed degree distribution. By comparing the upper bounds of robustness measurement of networks whose degree distribution are different, the framework analyzes the effect of the degree distributions on the robustness of a network. The optimization model established for the robustness improvement of a network is as below

$$\max R^{\mathrm{I}} \qquad s.t.\begin{cases} N \text{ is const}; \\ M \text{ is const}; \\ p(k) \text{ is const}; \end{cases} \qquad (3)$$

where R^{I} is the robustness measurement calculated by formula (2); N is the number of nodes in the network; M is the number of the edges in the network; $p(k)$ is the probability of the occurrence of the event that the degree of a node is k. The optimization method for robustness improvement in the framework is used to solve the model. Since the degree distribution of a network remains the same during the process of the robustness improvement of the network, the effect of other structural parameters on the robustness of the network can be analyzed then.

4 Optimization Method for Robustness Improvement of Complex Networks

The methods to search better structures which result in better robustness performance of a network include simulated annealing, tabu search and so on. The difficulty of applying these methods to solve the model in formula (3) is how to set the parameters of these methods, such as how to control the temperature drop in the simulated annealing and how to decide the length of the tabu list in the tabu search. Compared with these methods, the variable neighborhood search is easy to be used for the way to set its parameters is simple [23]. Thus, the optimization method for robustness improvement of complex networks is designed based on the variable neighborhood search in this paper.

The operation of reconnecting nodes while keeping their degree the same is adopted to remain the degree distribution of a network during the robustness improvement of the network. In detail, the operation choose two edges in a network, then reconnect nodes which are linked to the edges, which is show in Fig. 3.

Through this operation, new structures of a network can be obtained. The k-order neighborhood of the structure X of a network is denoted by $NH_k(X)$ which is a set constituted by structures that can be generated through k operations on the X.

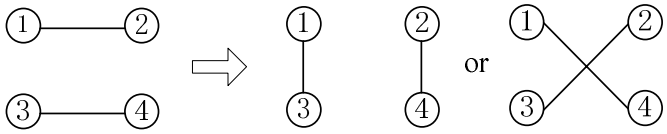


Figure 3. Rewiring nodes while keeping their degree fixed.

The idea of the robustness optimization method based on the variable neighborhood search is as below. Suppose a network is given and the structure of the network is noted as X. Then search in the $NH_1(X), \bigcup_{l=1}^{2} NH_l(X), \ldots, \bigcup_{l=1}^{l_{\max}} NH_l(X)$ to find which structure will improve the robustness of the network. If a better structure X' is found, then search the neighborhood of X'. Repeat the above steps until no better structures can be found during continuous several iterations. The detailed steps of the optimization method for robustness improvement are as follows.

Step 1. Initialize a network. The structure of the network is noted as X. Set the parameters $l_{\max}, c_{\max}$.

Step 2. Set a counter $c \leftarrow 1$.

Step 3. Whether $c \le c_{\max}$? If yes, set a counter $l \leftarrow 1$ and go to step 4. If not, the search process ends and input the structure X.

Step 4. Whether $l \le l_{\max}$? If yes, go to step 4.1. If not, set $c \leftarrow c+1$ and return to step 3.

Step 4.1. Select a structure X' from $\bigcup_{k=1}^{l} NH_k(X)$ randomly.

Step 4.2. Whether $R^1(X') \ge R^1(X)$? If yes, set $X \leftarrow X', l \leftarrow 1, c \leftarrow 1$. If not, set $l \leftarrow l+1$. Return to step 4.

The problem of how to set parameters $l_{\max}, c_{\max}$ in step 1 is discussed as below. Suppose there are two networks A and B. The number of nodes in A and B is N, the number of edges in them is M and the degree distributions of A and B are the same. Then the structure of A can change to be the same with that of B through less than M operations which reconnect nodes in A while keeping their degree fixed. That is, the set $\bigcup_{l=1}^{M} NH_l(X_A)$ where X_A represents the structure of A contains the structures of all the networks who has N nodes , M edges and a same degree distribution with that of A. Thus, the $l_{\max}$ in step 1 can be set to the number of edges in the initial network so that the structure of any one network in the one-order zero-model of the initial network will be explored with a probability which must not be zero. In step 3, that the formula $c = c_{\max} + 1$ holds means the method dose not found a better structure after continuous $l_{\max} \cdot c_{\max}$ iterations. If the search process will be ended after continuous m iterations during which a better structure is not found, then the $c_{\max}$ should be set to an integer that is not smaller than $m / l_{\max}$ where the m is usually set to 10000.

5 Relationship Between Structures and Robustness of Complex Networks

This section analyzes the robustness of complex networks with the proposed framework. The input information of the framework includes types of zero-order zero-models of complex networks, types of network build models and structural parameters of networks. The information of types of zero-order zero-models of networks is shown in Table 1 where the network size represents the number of nodes in a network and network density represents the ratio of the number of edges to the number of nodes in a network.

The information of network build models is shown in table II. The small-world network model is realized through the operation of reconnecting nodes in a nearest neighbor ring network. The probability of

reconnection is 0.1 in this paper. Since the probability is small, the degree of each node in a network generated by the small-world model is still relatively consistent [24].

Table I. Zero-order zero-modle of networks

number	1	2	3	4	5	6	7	8	9
network size	50	50	50	100	100	100	200	200	200
network density	2	3	4	2	3	4	2	3	4

Table II. Networks build models

type	nearest neighbor ring network model	random network model	small-world network model	scale-free network model
degree distribution of networks generated	single point distribution	Poisson distribution	exponential distribution	power-law distribution

Commonly used structural parameters of a network include average clustering coefficient, network efficiency, natural connectivity and algebraic connectivity. The average clustering coefficient reflects the degree of collectivization among nodes in a network [25]. If the number of nodes in a network X is N, then the average clustering coefficient (CC) is defined as

$$CC = \frac{1}{N}\sum_{i \in X} \frac{2e_i}{g_i(g_i - 1)} \qquad (4)$$

where g_i is the degree of node i and e_i is the number of edges that are between neighbor nodes of node i.

The network efficiency (NE) reflects the distance between the nodes in the network [26], which is defined as

$$E = \frac{1}{N(N-1)} \sum_{i,j \in X, i \neq j} \frac{1}{d_{ij}} \qquad (5)$$

where d_{ij} is the number of edges in the shortest path between node i and node j. If there is no one path between node i and node j, then $d_{ij} = \infty$.

The natural connectivity (NC) reflects the degree of redundancy of edges in the network [11], which is defined as

$$NC = \ln(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}) \qquad (6)$$

where $\lambda_1, \lambda_2, \ldots, \lambda_N$ are the N characteristic solutions of the adjacency matrix of the network.

The algebraic connectivity (AC) reflects the community property of the network [27], whose value is the second smallest characteristic solution of the Laplace matrix corresponding to the network.

Firstly, the influence of the degree distribution on the robustness of a network is analyzed according to the framework. The results are shown in Figure 4 in which the data are average values from a variety of experiments.

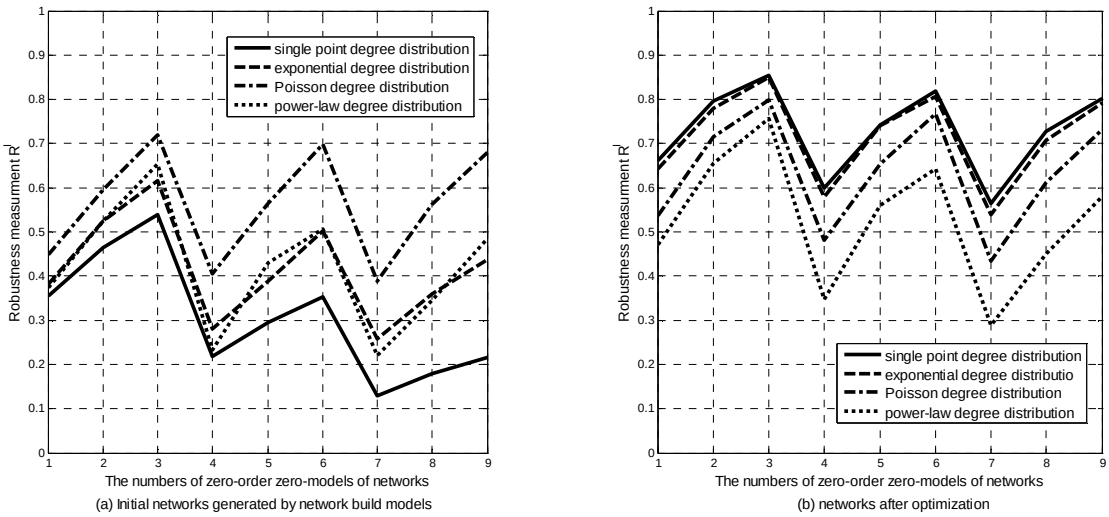


Figure 4. Impact of degree distribution on robustness of networks.

From the Fig. 4(a), it can be seen that the robustness of networks with Poisson degree distribution is the best, the robustness of networks with exponential degree distribution and power-law degree distribution follows and the robustness of networks with single point degree distribution is the worst. After optimization, robustness of all the networks is improved. It can be seen in Fig. 4(b) that the robustness of networks with single point degree distribution is the best, the robustness of networks with exponential degree distribution and Poisson degree distribution follows and the robustness of networks with power-law degree distribution is the worst. This phenomenon indicates that the closer the degree distribution of a network is to the single point distribution, the larger the upper bound of the robustness measurement of the network is.

The next work is to analyze the effects of other structural parameters on the robustness of networks. It is found that there exist significantly regression relationships between the robustness of a network with the single point degree distribution and its structural parameters, which are shown in Fig. 5 (Due to space limit, results in the zero-order zero-models of the number 5 and 8 in Table I are given). The regression relationships between the robustness of a network with the exponential degree distribution and its structural parameters are not very evident as shown in Fig. 6. In addition, no obvious relationships can be found between structural parameters and the robustness of networks with Poisson degree distribution and power-law degree distribution, which are shown in Fig. 7 and Fig. 8. All parameters in the figures have been normalized.

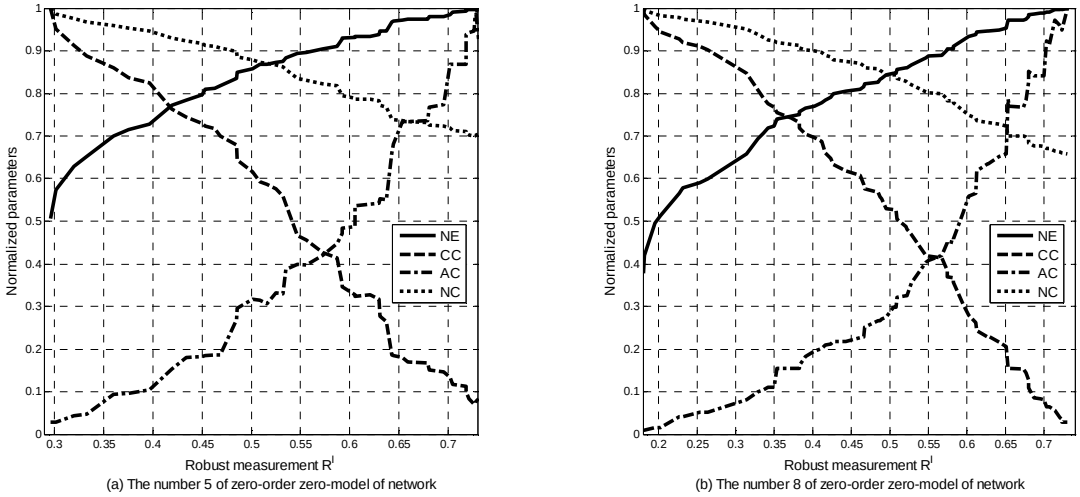
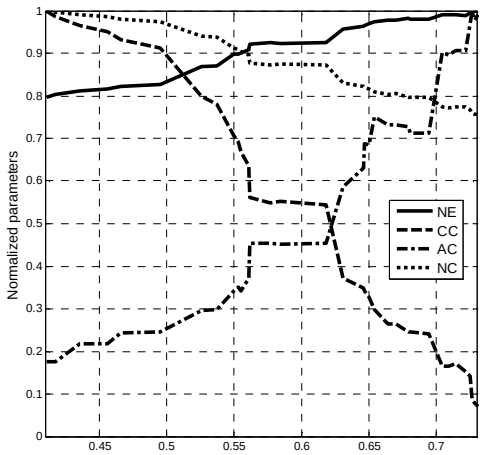
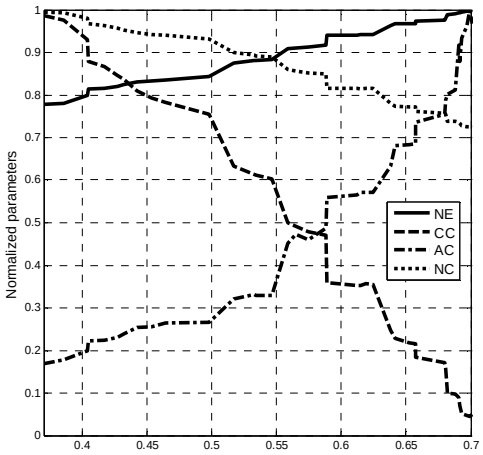


Figure 5. Networks with one-point degree distribution.



(a) The number 5 of zero-order zero-model of network



(b) The number 8 of zero-order zero-model of network

Figure 6. Networks with exponential degree distribution.

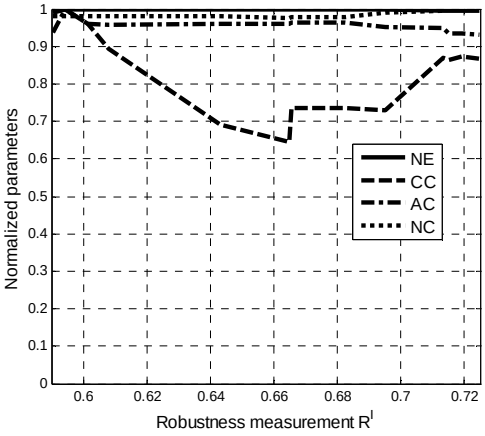


Figure 7. Networks with Poisson degree distribution.

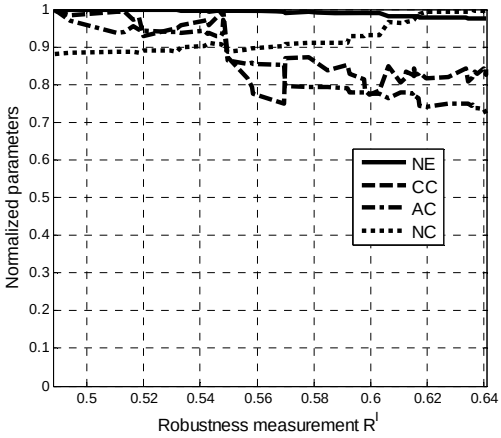


Figure 8.Networks with power-law degree distribution

The results indicate that the more consistent the degree of each node in a network is, the more evident the regression relationships between the robustness of the network and its structural parameters, such as the average clustering coefficient, the network efficiency et al., is. It is usually considered that the larger the natural connectivity of a network is, the better the robustness of the network is [11]. But the results in Fig. 5 and Fig. 6 show the viewpoint is not always right, which demonstrate the complexity of complex networks once again.

6 Discussion

A conclusion is made in Section 5 that the closer the degree distribution of a network is to the single point distribution, the larger the upper bound of the robustness measurement of the network is. Suppose there are N nodes and M edges in a network X. The quotient and the remainder of M divided by N are noted as Q and S separately. If S is zero, then the degree distribution of the structure of X can be design to the single point distribution with the purpose to increase the upper bound of the robustness measurement of X. If S is not zero , which means that the degree distribution of the structure of X will not be the single point distribution, then the strategy for increasing the upper bound of the robustness measurement of X is to make the degree of each node in X as same as possible. The method to realize the strategy is as follows. First construct a nearest neighbor ring network of which the number of nodes is N and the number of edges is M. Then select $N-S$ nodes in the network randomly and delete the edges between the nodes chosen and

their anticlockwise first neighbor node. Finally, a network having N nodes and M edges is gained, which is shown in Fig. 9. Through this method, the degree of every node in the network is not larger than $2Q+2$ and not smaller than $2Q$. That is, the degree distribution of the structure of the network is two-peak distribution or three-peak distribution. Valente et al. pointed out that a network with two-peak degree distribution or three-peak degree distribution had better robustness performance [7]. Thus, the correctness of the conclusion made in this paper is demonstrated to a certain degree based on [7].

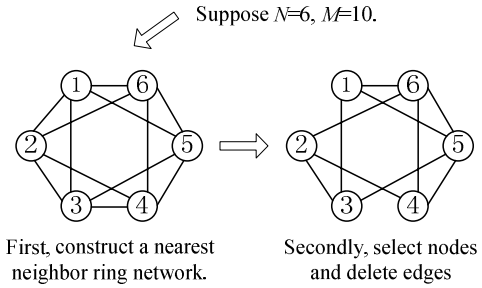


Fig. 9. Construction method.

7 Conclusions

This paper analyzes the relationship between the structures of complex networks and their robustness. The main work of this paper is as follows. First, we improve the robustness measurement of a complex network based on the analysis of the disadvantages of traditional robustness measurements. Then, we propose a framework for robustness analysis of complex networks based on optimization theory. The framework evaluates the influence of the degree distribution and other structural parameters of a network on its robustness within the zero-order zero-model and one-order zero-model of this network. Thirdly, we design the robustness optimization method based on the variable neighborhood search and discuss the way to set the parameters of this method. The method is not only simple to use but also can solve robustness optimization problem of complex networks well. Finally, through the framework proposed, it is found that the more consistent the degree of each node in a network is, the larger the upper bound of the robustness measurement of the network is. In addition, the more consistent the degree of each node in a network is, the more evident the regression relationships between the robustness of the network and its structural parameters, such as the average clustering coefficient, the network efficiency et al., are. These findings have positive referenced significance for network design et al.

References

[1] R. Albert, H. Jeong and A. L. Barabasi. 2000. Error and attack tolerance of complex networks, Nature, 406: 378-382.

[2] A. L. Baralasi. 2009. Scale-free networks: A decade and beyond, Science, 325: 412-413.

[3] E. M. Adilson and T. Zoltan. 2007. Introduction: Optimization in networks, Chaos, 17(2): 1-3.

[4] A. Gutfraind. 2012. Handbook of optimization in complex networks: Theory and applications, Springer, New York.

[5] T. Tanizawa, G. Paul and R. Cohen et al. 2005. Optimization of network robustness to waves of targeted and random attacks, Physical Review E: Statistical, Nonlinear, and Soft Matter Physics, 71(4): 1-4.

[6] G. Paul, S. Sreenivasan and S. Havlin et al. 2006. Optimization of network robustness to random breakdowns, Physica A: Statistical Mechanics and its Applications, 370(2): 854-862.

[7] A. X. C. N. Valente, A. Sarkar and H. A. Stone. 2004. Two-peak and three-peak optimal complex networks, Physical Review Letters, 92(11): 118702-1-118702-4.

[8] R. Cohen, K. Erez and D. Ben-Avraham et al. 2000. Resilience of the internet to random breakdowns, Physical Review Letters, 85(21): 4626-4628.

[9] G. Paul, T. Tanizawa and S. Havlin et al. 2004. Optimization of robustness of complex networks, European Physical Journal B, 38(2): 187-191.

[10] J. Wu, M. Barahona and Y. J. Tan et al. 2010. Natural connectivity of complex networks, Chinese Physics Letters, 27(7): 078902.

[11] J. Wu, M. Barahona and Y. J. Tan et al. 2011. Spectral measure of structural robustness in complex networks, IEEE Transactions on Systems, Man and Cybernetics – Part A, 41(6): 1244-1252.

[12] Z. Hu and P. K. Verma. 2011. Topological resilience of complex networks against failure and attack, In the 5th IEEE International Conference on Advanced Telecommunication Systems and Networks, 1-6.

[13] C. M. Schneider, A. A. Moreira and J. S. Andrade et al. 2011. Mitigation of malicious attacks on networks, Proceedings of the National Academy of Sciences, 108(10): 3838-3841.

[14] V. H. P. Louzada, F. Daolio and H. J. Herrmann et al. 2013. Smart rewiring for network robustness, Journal of Complex Networks, 1(2): 150-159.

[15] V. H. P. Louzada, F. Daolio and H. J. Herrmann et al. 2015. Propagation phenomena in real world networks, Springer, New York.

[16] D. Kasthurirathna, M. Piraveenan and G. Thedchanamoorthy. 2014. On the influence of topological characteristics on robustness of complex networks, Journal of Artificial Intelligence and Soft Computing Research, 3(2): 1-16.

[17] S. Maslov, K. Sneppen and A. Zaliznyak. 2004. Detection of topological patterns in complex networks: correlation profile of the internet, Physica A: Statistical and Theoretical Physics, 333: 529-540.

[18] M. Gjoka, M. Kurant and A. Markopoulou. 2013. 2.5K-graphs: From sampling to generation, In the 32nd IEEE Conference on Computer Communications, 1968-1976.

[19] P. Holme, B. J. Kim and C. N. Yoon et al. 2002. Attack vulnerability of complex networks, Physical Review E: Statistical, Nonlinear, and Soft Matter Physics, 65(5): 1-14.

[20] M. Bellingeri, D. Cassi and S. Vincenzi. 2014. Efficiency of attack strategies on complex model and real-world networks, Physica A: Statistical Mechanics and its Applications, 414: 174-180.

[21] M. Piraveenan, G. Thedchanamoorthy and S. Uddin et al. 2013. Quantifying topological robustness of networks under sustained targeted attacks, Social Network Analysis and Mining, 3(4): 939-952.

[22] Y. Jiang and Y. B. Wang. 2013. Analysis of attack and defense strategies on complex networks, In the International Conference on Sensor Network Security Technology and Privacy Communication System, 58-62.

[23] E. K. Burke and G. Kendall. 2006. Search methodologies: Introductory tutorials in optimization and decision support techniques, Springer, New York.

[24] A. Barrat and M. Weigt. 2000. On the properties of small-world network models, The European physical journal B, 13(3): 547-560.

[25] R. Albert and A. L. Barabbsi. 2002. Statistical mechanics of complex networks, Reviews of Modern Physics, 74: 47-97.

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

[27] M. Fiedler. 1973. Algebraic connectivity of graphs, Czechoslovak Mathematical Journal, 23(98): 298-305.