Eur. Phys. J. B (2016) 89: 186
DOI: 10.1140/epjb/e2016-60845-8

THE EUROPEAN PHYSICAL JOURNAL B

Regular Article

Optimization of controllability and robustness of complex networks by edge directionality

Man Liang[1,2], Suoqin Jin[1,2], Dingjie Wang[1,2], and Xiufen Zou[1,2,a]

[1] School of Mathematics and Statistics, Wuhan University, Wuhan 430072, P.R. China
[2] Computational Science Hubei Key Laboratory, Wuhan University, Wuhan 430072, P.R. China

Received 26 October 2015 / Received in final form 7 January 2016
Published online 5 September 2016

Abstract. Recently, controllability of complex networks has attracted enormous attention in various fields of science and engineering. How to optimize structural controllability has also become a significant issue. Previous studies have shown that an appropriate directional assignment can improve structural controllability; however, the evolution of the structural controllability of complex networks under attacks and cascading has always been ignored. To address this problem, this study proposes a new edge orientation method (NEOM) based on residual degree that changes the link direction while conserving topology and directionality. By comparing the results with those of previous methods in two random graph models and several realistic networks, our proposed approach is demonstrated to be an effective and competitive method for improving the structural controllability of complex networks. Moreover, numerical simulations show that our method is near-optimal in optimizing structural controllability. Strikingly, compared to the original network, our method maintains the structural controllability of the network under attacks and cascading, indicating that the NEOM can also enhance the robustness of controllability of networks. These results alter the view of the nature of controllability in complex networks, change the understanding of structural controllability and affect the design of network models to control such networks.

1 Introduction

In recent decades, complex networks have attracted much attention in science and engineering fields [1,2]. Numerous studies on the structure and dynamics of complex networks have been performed to understand the properties of complex networks. These studies have led to notable achievements in many areas, such as pinning control, synchronization and cascading [3–15]. One of the most important aspects of complex networks lies in our ability to control them. There are many excellent studies about the controllability of complex networks governed by linear dynamics [16–19]. Structural controllability was proposed to offer a general framework for controlling directed networks with arbitrary structures while ignoring the configurations of link weights [17]. Liu et al. [17] developed a minimum input theory to investigate the ability to efficiently steer a complex network from any initial state toward any desired state and revealed that the minimum number of driver nodes (N_D) is determined by the set of maximum matching. The N_D refers to the number of control signals applied to an arbitrary set of nodes to bring the system under control, qualitatively. Therefore, it is meaningful to optimize the minimum driver nodes of complex networks.

[a] e-mail: xfzou@whu.edu.cn

Several methods have been proposed to optimize the controllability of complex networks. Wang et al. [20] optimized network controllability by connecting the fewest number of edges between isolated control paths, thus, a network can be controlled using only one control signal. Based on the node residual degree, Hou et al. [21] proposed a method to enhance network controllability by appropriately assigning link direction. Xiao et al. [22] constructed a switching network, found its maximum independent set and obtained the minimum driver nodes and the fewest number of edges that must be modified for optimal control while conserving entire topology. To decrease the time complexity, they classified edges into three categories based on directions: critical edge directions, redundant edge directions and intermittent edge directions. They then demonstrated that the existence of more critical edge directions implies not only a lower cost for modifying inappropriate edges but also better controllability [23]. Finally, they proposed a method called edge orientation by critical directions (EOCD) to generate more critical edge directions. The EOCD method achieves near-optimal controllability. Compared to adding edges, it is more applicable and economical to change the direction of edges. However, the effects of edge directionality on network controllability have not been completely investigated.

Generally, systems are always confronted with attacks and cascading. For example, in the internet, a node denotes some information, an overload corresponds to congestion, and an attack on several nodes may cause a collapses [24]. The vulnerability of systems under various attacks and cascading has been a significant issue in studies of complex networks [25–27]. The removal of nodes generally changes the distribution of shortest paths, leading to a global redistribution of loads over the entire network and destroying some control routes. Therefore, we need to consider how to maintain network controllability during an attack. Wang et al. [28] proposed a greedy approach by swapping connections to maintain structural controllability; however, this method has high computational complexity; and cannot be applied to large-scale networks. For an arbitrary network, we consider whether we can properly organize the edge direction of a complex network to not only optimize network controllability but also optimize network robustness.

To address these problems, this study proposes a new edge orientation method (NEOM) based on residual degree without changing network topology and directionality. By comparing the results with the original networks and networks constructed by EOCD in two random graph models (i.e., the Erdös-Rényi (ER) model and scale-free (SF) model) and several real systems, we demonstrate that our approach is an effective and competitive method for improving the structural controllability of complex networks. Numerical simulations show that our method is near-optimal in optimizing structural controllability. Furthermore, we show that our method can maintain the structural controllability of the network under attack and cascading. According to their roles in minimum driver node set, these nodes are classified into three categories: critical, redundant and intermittent. We show that our method is likely to generate more redundant nodes, and fewer critical and intermittent nodes. Moreover, using our method, the characteristic path-length becomes longer and assortativity becomes greater than in the original network. Finally, we applied the NEOM to several realistic networks to demonstrate its efficiency.

2 Preliminaries

2.1 Structural controllability

Given a network $G = (V, E)$ of N nodes, we start our study with a linear, time-invariant dynamical system described as follows:

$$\dot{x}(t) = Ax(t) + Bu(t), \quad (1)$$

where $x(t) \in R^N$ is the state of N nodes at time t, and $u(t) \in R^M$ is the time-dependent input vector imposed by the controller. Here, $A \in R^{N\times N}$ stands for the adjcency matrix of the system, and $B \in R^{N\times M}$ describes the control matrix. The system (1) can denote as (A, B) and is controllable if and only if Kalman's controllability matrix

$$C = (B, AB, A^2B, \dots, A^{N-1}B) \quad (2)$$

has full rank. Therefore, to fully control the network, we need to choose the right B and $u(t)$ to make C have full rank. However, Kalman's controllability condition (2) is difficult to apply, because it is not easy to compute rank (C) when C is a large-scale matrix. Fortunately, structural controllability can be used to solve the problem. The system (A, B) is called structurally controllable if it is possible to fix the free parameters in A, B to certain values so that the obtained system (A, B) is controllable in the usual sense, i.e., rank $(C) = N$ [17]. The maximum matching algorithm can be used to identify the minimum numbers of driver nodes.

2.2 Cascading failure

Cascading failure of complex network is defined as one or a few nodes or links failure (or attack, removal) which can trigger the failure of other nodes or other links through the interconnected relations, and it will cause the successive effect and lots of nodes failure, ever the collapse of the whole network. Cascading failure occurs widely in many systems, including power grids, the Internet and transportation. Thus, the analysis of cascading failure plays an important role in the vulnerability of complex networks. The related research can help us attain a comprehensive understanding of robustness and reliability of complex networks.

The load on a node is defined as the total number of shortest paths in network passing through the node [24]. The capacity of a node is the maximum load that the node can handle. Because the capacity is subject to cost, it is natural to assume that the capacity C_j of node j is proportional to its initial load L_j [24]:

$$C_j = (1 + c)L_j, \quad j = 1, 2, \dots, N, \quad (3)$$

where the constant $c > 0$ is the tolerance parameter and N is the size of the network. In this study, we chose $c = 0.15$. When node j is attacked or removed, i.e., the edges that connected to the node j is removed, the loads on all nodes of network will then be redistributed. If the loads of some nodes in a network are more than their capacity, we call these nodes as overloaded nodes. Simultaneously, we consider the corresponding nodes as the failed nodes and its edges are removed from the network. In turn, this causes a new redistribution of loads and subsequent failures. The process continues until there are no overloaded nodes.

3 Using the NEOM to improve the structural controllability and its robustness of complex networks

3.1 Description of the proposed NEOM

Complex network systems are always confronted by attacks and cascading failures that can easily damage their normal functions. For many industries, such as the Internet and power grids, the attacks and cascading failures can easily cause a great deal of damage. Maintaining their

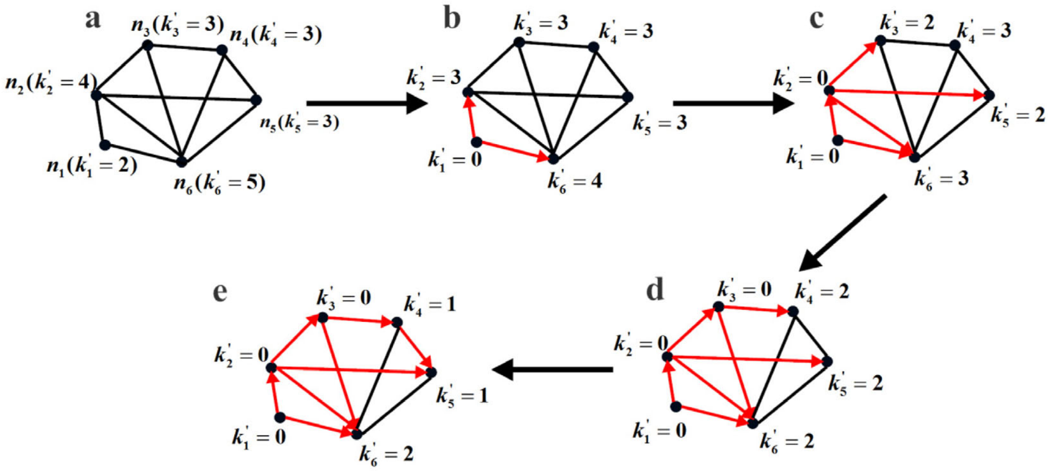

Fig. 1. A schematic of the proposed NEOM. Given a directionality $\alpha = 0.8$: (a) consider an undirected network with $N = 6$ nodes and 10 edges. Each node i is given the residual degree k'_i, which represents the number of undirected edges of node i. The black and red lines represent undirected and directed edges, respectively. (b) Choose the node with the smallest residual degree as the target node, i.e., n_1, and find its neighbors, i.e., n_2 and n_6. Assign the outgoing direction from target node n_1 to its neighbors. Meanwhile, the residual degree of n_2 and n_6 is reduced by one and the residual degree of target node becomes zero, i.e., $k'_1 = 0$. (c) Then, n_2 is the smallest residual degree node among the neighbors of n_1, so we choose n_2 as the new target node, find its neighbors n_3, n_5, n_6, and repeat step (b). (d) Because the sum of the residual degree of n_3 and that of n_5 in the previous steps are equal, we randomly choose n_3 or n_5 as a new target node. Here we choose n_3 as the target node, find its neighbors n_4, n_6, and repeat step (b). (e) Now, n_4 is the new target node. Although $k'_4 = k'_6 = 2$ in step (d), the sum of residual degree of n_4 is smaller than that of n_6 in the previous steps, so we choose n_4 as the new target node, find its neighbors n_5, n_6, and repeat step (b). However, we find that the number of directed links (#9) is greater than expected ($\#10 \times 0.8 = 8$), so we sort the neighbor nodes (i.e., n_5, n_6) by descending residual degree, i.e., n_6, n_5, and then we turn the directed edge ($n_4 \to n_6$) to undirected edge ($n_4 - n_6$). Thus, all the directions are determined.

efficiency during such threats is a matter of the utmost importance; therefore, enhancing network robustness and controllability is of great significance.

The directedness of complex networks plays an important role in emerging dynamical behaviors [29–32]. For example, as a network gains more directed arcs, its small-world behavior becomes weaker: The path length increases and the clustering coefficient becomes smaller. Structural changes related to the changing bidirectional edges to unidirectional arcs are naturally expected to be reflected in the dynamic properties of the network system [29]. So it is also necessary to keep the directionality of complex networks unchanged.

The edge directions of network play an important role in optimizing the controllability of complex networks. Based on the residual degree k', we propose a new edge orientation method (NEOM) to optimize the controllability of complex networks without changing the entire network topology and directionality.

Consider an undirected network $G\ (V, E)$. We change edges from undirected to directed using a given probability of α [29–32]. When $\alpha = 0$, the network is identical to undirected network. However, when $\alpha = 1$, all edges in the network become directed. For a given directionality, the NEOM is described as follows:

Step 1. Consider an undirected network. Each node is given a residual degree (the number of undirected links of that node), denoted as k'.

Step 2. Choose the node with the smallest residual degree in the network as the target node, denoted as node i. If there are multiple such nodes, we choose the one with the smallest sum of its residual degree in all the previous iterations.

Step 3. Assign the outgoing direction from the selected node to its neighbors whose residual degrees are nonzero. Thus, the residual degree of the selected node becomes zero and the residual degree of each node of those neighbors is reduced by one.

Step 4. If all directed links are determined, then stop. If all directed links are less than expected, we proceed to step 5. Otherwise, we count the number of the redundant directed links, denoted as m. Then, we sort the neighbor nodes by descending residual degree and denote them as $i_1, i_2, \ldots, i_l$ (where $l > m$). Afterwards, change the links between node i and $i_1, i_2, \ldots, i_m$ from directed to undirected, then stop.

Step 5. Choose the smallest k' in the neighbors as the new target node. If k' equals zero, jump to step 2; otherwise, jump to step 3. To further explain the proposed NEOM, the schematic of a simple network with size $N = 6$ is shown in Figure 1. This framework illustrates how to optimize the controllability of complex networks without changing the entire network topology and directionality.

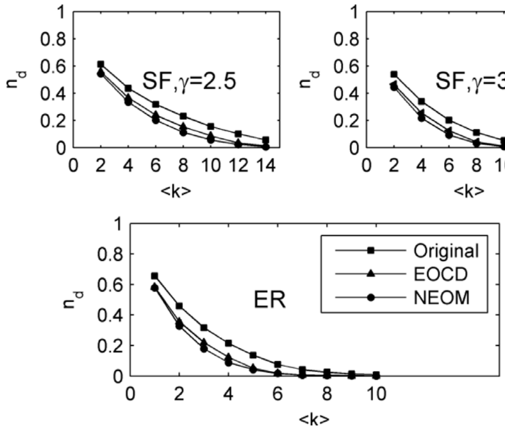

Fig. 2. The controllability of the original, NEOM and EOCD networks (network constructed by NEOM and EOCD, respectively), which are represented by square, circle and triangle, respectively, as a function of $\langle k \rangle$. Each data point is an average of 10 independent runs; the error bars represent the standard deviation.

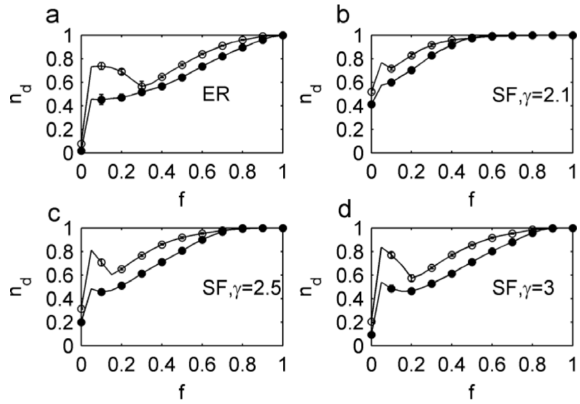

Fig. 3. The fraction of driver nodes as a function of removal fraction f under intentional attack and cascading based on node betweenness. (a) ER network, (b) SF network with $\gamma = 2.1$, (c) SF network with $\gamma = 2.5$, (d) SF network with $\gamma = 3$. The open and solid symbols represent the original network and the NEOM network, respectively.

3.2 The NEOM can improve the structural controllability of complex networks

To illustrate the efficiency of the NEOM, we compare it with EOCD which is a near-optimal method. We use a static model [33] to build a scale free (SF) network and note that when $\gamma \to \infty$, this model is equivalent to the ER model (see detailed description in [17]). Compared to the orginal network using ER and SF models with different average degrees and power laws, Figure 2 shows that NEOM is effective and competitive for improving the structural controllability of complex networks. Moreover, compared to EOCD, which is a near-optimal method in optimize the controllability of complex network [23], NEOM is clearly more efficient-which means that the NEOM is also near-optimal.

3.3 The NEOM can enhance the robustness of controllability of complex networks

The function of systems will be affected by the removal of a few nodes in the network. For example, a node attack on a circuit network can affect the current supply; sometimes the current load can paralyze the whole network. Cascading failures and intentional attacks can easily damage network functionality; therefore, it is meaningful to propose a method to enhance the robustness of the controllability of complex networks against attacks and cascading failures.

For a given network, the robustness can be improved in many ways. Adding edges without any other restrictions would be feasible, but it is impractical because the cost of each network edge cannot be ignored. Under this constraint, Wang et al. [28] propose to swap connections to maintain the structural controllability of complex networks. However, this method has high computational complexity. Therefore, it is not suitable for large-scale networks.

Schneider et al. [34] proposed the following measure by considering the size of the largest component of an undirected network against malicious attacks:

$$R = \frac{1}{N} \sum_{q=1/N}^{1} s(q), \tag{4}$$

where N is the number of vertices and $s(q)$ is the fraction of vertices in the largest component of the undirected network after attacks on qN nodes. Here, R is normalized by $1/N$ so that the robustness of networks with different sizes can be compared.

Analogously, Xiao et al. [35] proposed a robustness index CR to assess the evolution of controllability by node removal:

$$CR = \frac{1}{N} \sum_{q=1/N}^{1} (1 - n_d(q)), \tag{5}$$

where $n_d(q)$ is the fraction of minimum driver nodes in the remaining network after attacking qN nodes. A larger CR means that the robustness of network controllability is better.

To investigate the robustness of controllability of a NEOM network (network constructed by NEOM), in our numerical experiments, we use ER and SF ($\gamma = 2.1$, 2.5 and 3) networks with network size $N = 1000$, $\langle k_{in} \rangle = \langle k_{out} \rangle = 3$ as the example. Throughout our study, we assume that vertices are attacked according to their high-betweenness. Other attack strategies can also be used.

As shown in Figure 3, compared to the original network, the NEOM network requires fewer driver nodes to achieve the target states after attacks on qN nodes (where $1/N \leqslant q \leqslant 1$). According to the definition of CR, the NEOM can enhance the robustness of controllability (as shown in Fig. 4). Besides, our method keeps the topology and directionality unchanged, making it more practicable than CR for swapping connectivity.

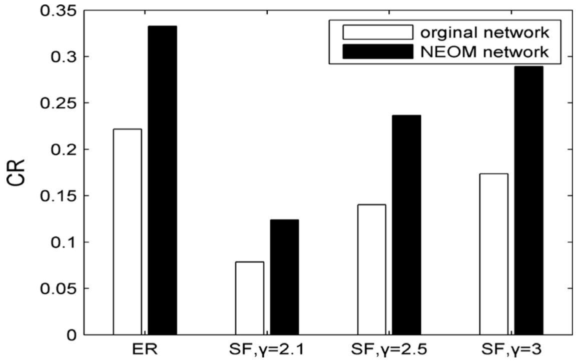

Fig. 4. The robustness index *CR* of NEOM network and original network. All these in turn are ER network, SF network with $\gamma = 2.1$, SF network with $\gamma = 2.5$ and SF network with $\gamma = 3$. The open and solid symbols represent the original network and NEOM network, respectively.

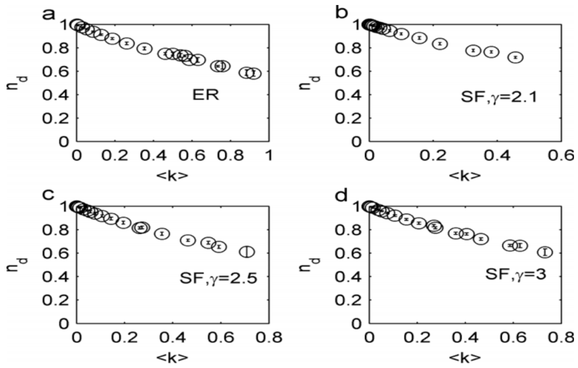

Fig. 5. The fraction of driver nodes as a function of the average degree of a network after an intentional attack and cascading based on node betweenness. (a) ER network, (b) SF network with $\gamma = 2.1$, (c) SF network with $\gamma = 2.5$, and (d) SF network with $\gamma = 3$.

Then, we study the number of failed edges to explain why the number of driver nodes of the NEOM network after attack and cascading is smaller than that of the original network. For the ER network, the number of driver nodes of the network [17] is given by:

$$n_d \approx e^{-\frac{\langle k \rangle}{2}}. \tag{6}$$

Equation (6) shows that the number of driver nodes is negatively correlated with the average degree of the network for ER network. To further investigate the relationship between them after an intentional attack and cascading, we used a network with size $N = 1000$, and $\langle k \rangle = 3$ as an example to perform numerical simulations. Our results demonstrated that the number of driver nodes is indeed negatively correlated with the average degree of the network after intentional attack and cascading, as shown in Figure 5. At the beginning, we construct the NEOM network without changing the topology and directionality, so the number of edges in the NEOM network is the same as that of the original network. As shown in Figure 6, after an attack on the f $(0 < f < 1)$ fraction of nodes, the number of failed edges in NEOM network is less than the

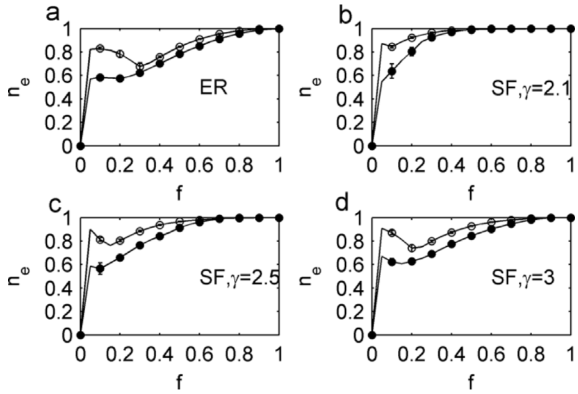

Fig. 6. The fraction of failed edges as a function of removing the fraction f nodes under an intentional attack and cascading based on high-betweenness. (a) ER network, (b) SF network with $\gamma = 2.1$, (c) SF network with $\gamma = 2.5$, and (d) SF network with $\gamma = 3$. The open and solid symbols represent the original network and the NEOM network, respectively.

original network. The smaller the number of failed edges is, the greater the average degree is, which means that the number of driver nodes of the NEOM network is smaller than that of original network. The same reasons apply to the SF network.

4 Effect of the NEOM on network characteristics

To investigate the feature difference between the NEOM network and the original network, we studied the changes in three categories of nodes. According to their roles in the minimum driver node set (MDS), these nodes are classified into three different types: 'critical' that is a part of MDSs, 'redundant' that is not in any MDSs, and 'intermittent' that is neither critical nor redundant [17]. The minimum driver nodes are composed of critical nodes and parts of intermittent nodes.

We randomly generated 1000 ER and SF networks and then reconstructed the networks by using the NEOM. To determine whether the features between the original network (O) and the NEOM network (N) were significantly different, we performed a non-parametric one-tailed Wilcoxon rank sum test and used the p-value of that test as a measure of the difference in the two networks. As shown in Figure 7, the number of three categories of nodes in the NEOM network are separately significantly different from those in original network, causing all the p-values to approach zero. Figure 7 also shows that the NEOM is more likely to produce more redundant nodes, but fewer critical and intermittent nodes (the p-values were: critical nodes: $p = 3.4142\text{e-}23$, redundant nodes: $p = 8.8296\text{e-}82$, and intermittent nodes: $p = 1.8734\text{e-}73$).

In addition to these changes in node types, compared to the original network, the NEOM can also influence some topology characteristics. We measure two quantitative indexes as follows: (i) the characteristic path length l [20], defined by $l^{-1} = \sum_{i \neq j} d_{ij}^{-1} / N(N-1)$, where d_{ij} means

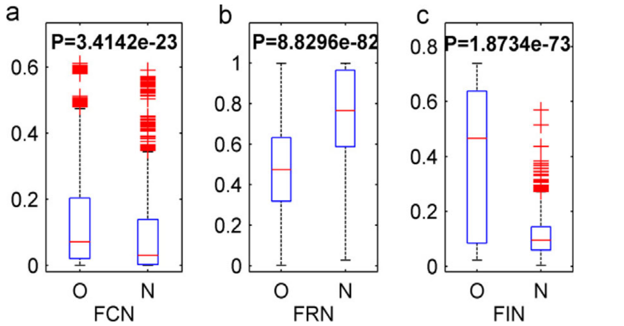

Fig. 7. Comparison of three different types of nodes between the original network (O) and networks constructed by the NEOM (N). We randomly generate 1000 ER and SF networks with $2 \leqslant \langle k \rangle \leqslant 14$, $\gamma = 2, 1, 2.5, 3$ and 3.5. All the networks were of size $N = 1000$; (a) represents the fraction of critical nodes (FCN); (b) the fraction of redundant nodes (FRN), and (c) the fraction of intermittent nodes (FIN). p-values are from a one-tailed Wilcoxon rank sum test.

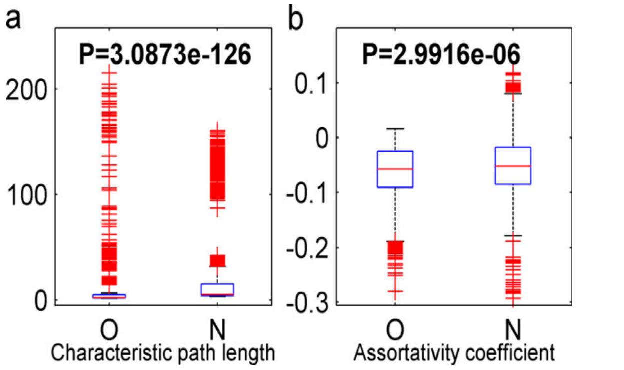

Fig. 8. Comparison of the characteristic path length and assortativity coefficient between the original network (O) and NEOM network (N) with $2 \leqslant \langle k \rangle \leqslant 14$, $\gamma = 2, 1, 2.5, 3$ and 3.5. All networks were of size $N = 1000$.

the shortest path length starting from node i to node j, and (ii) the assortativity coefficient defined as [36]:

$$r = \frac{M \sum_i l_i k_i - [M^{-1} \sum_i \frac{1}{2}(l_i + k_i)]^2}{M^{-1} \sum_i \frac{1}{2}(l_i^2 + k_i^2) - [M^{-1} \sum_i \frac{1}{2}(l_i + k_i)]^2}, \quad (7)$$

where l_i and k_i are the degrees of the nodes at the ends of the ith edges with $i = 1, \ldots, M$.

The assortativity coefficient of a network depends on the fact that nodes with many connections tend to be connected to other nodes with many connections, i.e., there is a greater preference for high-degree nodes to be connected to other high-degree nodes than for high-degree nodes to be attached to ones of lower-degree. When $r = 1$, all nodes connect only with nodes of the same degree; when $r = 0$, any node can randomly connect to any other node, and when $r = -1$, all nodes must connect to nodes with different degrees.

We randomly generate ER and SF networks with $2 \leq \langle k \rangle \leq 14$, $\gamma = 2.1$, 2.5, 3 and 3.5. All networks were of size $N = 1000$. Figure 8a describes the changes in characteristic path length of the networks, while Figure 8b describes the change of the assortativity coefficient

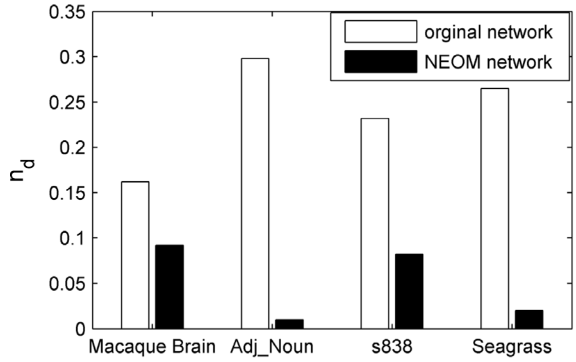

Fig. 9. The controllability of the NEOM network and original network. All these in turn are Macaque brain, Adj_Noun, s838 network and Segrass network. The open and solid symbols represent the original network and NEOM network, respectively.

of the networks. The p-value of the test is used as a measure of the difference. Because both p-values are far less than 0.01, the changes of characteristic path length and assortativity coefficients of networks are significantly different. As Figure 7 shows the path length becomes longer and assortativity becomes greater than that of the original network.

5 Application of the NEOM to several real networks

Finally, we apply the NEOM to four real networks[1]: (1) The macaque brain network consists of 383 hierarchically organized regions spanning cortex, thalamus, and basal ganglia. It includes 6,602 directed long-distance connections. (2) In the Adj_Noun network, the nodes represent the most commonly occurring adjectives and nouns in the novel David Copperfield by Charles Dickens, and edge connects a pair of nodes that appear adjacent to one another at any point in the book. (3) The s838 network is an electric circuit. In this network, the nodes represent logic gates and flip-flops and edges represent directed electronic transmission paths. (4) The seagrass network is the predatory interactions among species. A directed link of the network is drawn from the prey to the predator. As shown in Figure 9, compared to the original network, the NEOM network needs fewer driver nodes. Figure 10 also indicates that the structural controllability of NEOM network is better than that of the original network under attacks and cascading failures, which means that NEOM network is more robust than the real networks (as shown in Fig. 11). Thus, the NEOM cannot only apply to random models, but also real network models.

6 Discussion

Our understanding of natural or technological systems depends upon our ability to control them. Robustness

[1] http://boseinst.ernet.in/soumen/Network_Controllability_Datasets.html

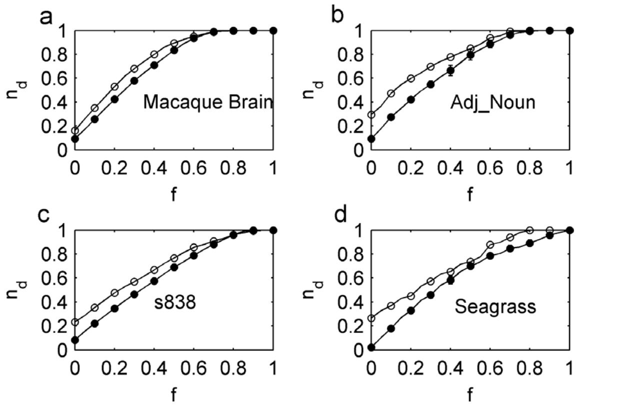

Fig. 10. The fraction of driver nodes of real systems as a function of removing fraction f under an intentional attack and cascading. (a) Macaque brain network, (b) Adj_Noun network, (c) Seagrass network, and (d) s838 network. The open and solid symbols represent the original network and the NEOM network, respectively.

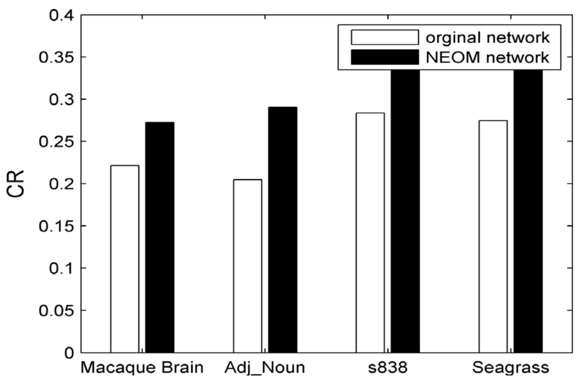

Fig. 11. The robustness index *CR* of NEOM network and original network. All these in turn are Macaque brain, Adj_Noun, s838 network and Segrass network. The open and solid symbols represent the original network and NEOM network, respectively.

implies the degree of continuing functionality of a network under intentional attacks and cascading failures. Many methods have been proposed to optimize the controllability or robustness of complex networks, such as adding edges, or assigning edges properly. Compared to adding edges, it is of more practical significance to reveal the directional effects on the controllability and robustness of complex networks. In this work, we propose a new method for constructing a network without changing its topology and directionality and find that both controllability and robustness can be optimized simultaneously. By comparing the results with those of previous methods in two random graph models, i.e., ER model and SF model, we demonstrate that our proposed approach is not only near-optimal in optimizing structural controllability, but also can maintain that the controllability under intentional attacks and cascading failures. According to the definition of robustness of controllability, we show that this method can enhance the robustness of controllability. An additional feature of our method is that it can improve both the average path length and assortativity. This is significant in designing of network models to control such networks.

Many real-world networks are coupled into multiplexed communication networks and are nonlinear systems, whereas all results in this paper are discussed in reference to isolated networks and linear systems; therefore our future work will involve our method to the real-world systems. Moreover, more and more attentions has been given to observability, target control, control energy and other significant problems [37–43]; therefore it is necessary to determine the relationship between directness and those dynamic processes.

Author contribution statement

X.F.Z. designed the study; M.L., S.Q.J. and D.J.W. performed the research and analyzed data; M.L. and X.F.Z. wrote and revised the manuscript. All authors reviewed the manuscript.

The authors thank the anonymous reviewers for their helpful comments and suggestions. This work was supported by the Major Research Plan of the National Natural Science Foundation of China (Nos. 91230118 and 91530320).

References

1. D.J. Watts, S.H. Strogatz, Nature **393**, 440 (1998)
2. A.L. Barabasi, R. Albert, Science **286**, 509 (1999)
3. M. Newman, A.-L. Barabasi, D.J. Watts, *The structure and dynamics of networks* (Princeton University Press, State of New Jersey, 2006)
4. S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.-U. Hwang, Phys. Rep. **424**, 175 (2006)
5. J.Y. Tan, X.F. Zou, Int. J. Bifurc. Chaos **23**, 1350180 (2013)
6. X.F. Wang, G. Chen, Physica A **310**, 521 (2002)
7. L. Donetti, P.I. Hurtado, M.A. Munoz, Phys. Rev. Lett. **95**, 188701 (2005)
8. Y.Y. Li, X.F. Zou, Sci. China. Inf. Sci. **59**, 070102 (2016)
9. C.M. Gray, P. Konig, A.K. Engel, W. Singer, Nature **338**, 334 (1989)
10. Y. Moreno, M. Nekovee, A.F. Pacheco, Phys. Rev. E **69**, 065102 (2004)
11. J.D. Noh, H. Rieger, Phys. Rev. Lett. **92**, 118701 (2004)
12. J.Y. Tan, X.F. Zou, Comput. Math. Methods Med. **2015**, 386235 (2015)
13. S.Q. Jin, L.L. Niu, G. Wang, X.F. Zou, Int. J. Bifurc. Chaos **25**, 1540007 (2015)
14. S.Q. Jin, Y.Y. Li, R.G. Pan, X.F. Zou, Sci. Rep. **4**, 3799 (2014)
15. Y.Y. Li, S.Q. Jin, L. Lei, Z.S. Pan, X.F. Zou, Sci. Rep. **5**, 9283 (2015)
16. C.T. Lin, IEEE. Trans. Automat. Contr. **19**, 201 (1974)
17. Y.Y. Liu, J.J. Slotine, A.L. Barabasi, Nature **473**, 167 (2011)
18. T. Nepusz, T. Vicsek, Nat. Phys. **8**, 568 (2012)
19. J. Ruths, D. Ruths, Science **343**, 1373 (2014)
20. W.X. Wang, X. Ni, Y.C. Lai, C. Grebogi, Phys. Rev. E **85**, 026115 (2012)

21. L.L. Hou, S.Y. Lao, G. Liu, L. Bai, Chin. Phys. Lett. **29**, 108901 (2012)
22. Y.D. Xiao, S.Y. Lao, L.L. Hou, L. Bai, Phys. Rev. E **90**, 042804 (2014)
23. Y.D. Xiao, S.Y. Lao, L.L. Hou, M. Small, L. Bai, Plos One **10**, e0135282 (2015)
24. A.E. Motter, Y.C. Lai, Phys. Rev. E **66**, 114 (2002)
25. C.L. Pu, W.J. Pei, A. Michaelson, Physica A **391**, 4420 (2012)
26. S. Nie, X. Wang, H. Zhang, Q. Li, B. Wang, Plos One **9**, e89066 (2014)
27. J. Ruths, D. Ruths, *Robustness of network controllability under edge removal* (Springer, Berlin, 2013)
28. B.B. Wang, L. Gao, Y. Gao, Y. Deng, Europhys. Lett. **101**, 58003 (2013)
29. S.M. Park, B.J. Kim, Phys. Rev. E **74**, 026114 (2006)
30. S.W. Son, B.J. Kim, H. Hong, H. Jeong, Phys. Rev. Lett. **103**, 228702 (2009)
31. G. Bianconi, N. Gulbahce, A.E. Motter, Phys. Rev. Lett. **100**, 2239 (2008)
32. G. Zamora-Lopez, V. Zlatic, C. Zhou, H. Stefancic, J. Kurths, Phys. Rev. E **77**, 119 (2008)
33. K.I. Goh, B. Kahng, D. Kim, Phys. Rev. Lett. **87**, 455 (2001)
34. C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Proc. Natl. Acad. Sci. USA **108**, 3838 (2011)
35. Y.D. Xiao, S.Y. Lao, L.L. Hou, L. Bai, Chin. Phys. B **23**, 118902 (2014)
36. M.E.J. Newman, Phys. Rev. Lett. **89**, 111 (2002)
37. Y.Y. Liu, J.J. Slotine, A.L. Barabasi, Proc. Natl. Acad. Sci. USA **110**, 2460 (2013)
38. J. Gao, Y.-Y. Liu, R.M. D'Souza, A.-L. Barabási, Nat. Commun. **5**, 5415 (2014)
39. D.J. Wang, S.Q. Jin, F.X. Wu, X.F. Zou, Adv. Complex. Syst. **18**, 1550018 (2015)
40. S.Q. Jin, L.L. Niu, G. Wang, X.F. Zou, Int. J. Bifurc. Chaos **25**, 1540007 (2015)
41. Y.B. Wang, J.Y. Tan, F. Sadre-Marandi, J.G. Liu, X.F. Zou, Math. Biosci. **262**, 198 (2015)
42. X.F. Zou, L.L. Niu, S.Q. Jin, J. Jiangxi Norm. Univ. (Nat. Sci. Ed.) **39**, 7 (2015)
43. G. Yan, G. Tsekenis, B. Barzel, J.J. Slotine, Y.Y. Liu, A.L. Barabasi, Nat. Phys. **11**, 779 (2015)