Optimization of robustness of network controllability against malicious attacks*

Xiao Yan-Dong(肖延东)†, Lao Song-Yang(老松杨), Hou Lv-Lin(侯绿林), and Bai Liang(白 亮)

College of Information Systems and Management, National University of Defense Technology, Changsha 410073, *China*

(Received 25 March 2014; revised manuscript received 26 May 2014; published online 24 September 2014)

As the controllability of complex networks has attracted much attention recently, how to design and optimize the robustness of network controllability has become a common and urgent problem in the engineering field. In this work, we propose a method that modifies any given network with strict structural perturbation to effectively enhance its robustness against malicious attacks, called dynamic optimization of controllability. Unlike other structural perturbations, the strict perturbation only swaps the links and keeps the in- and out-degree unchanged. A series of extensive experiments show that the robustness of controllability and connectivity can be improved dramatically. Furthermore, the effectiveness of our method is explained from the views of underlying structure. The analysis results indicate that the optimization algorithm makes networks more homogenous and assortative.

Keywords: robustness, network controllability, structure controllability

PACS: 89.75.Fb, 89.75.Hc, 02.30.Yy **DOI:** 10.1088/1674-1056/23/11/118902

1. Introduction

As the network systems appear around us at an increasing rate, dynamics in complex networks has become one of the most popular research fields.[1–4] For the past few decades, the dynamics has been studied on the underlying mechanisms of systems, such as, viruses spread,[3] rumor spread,[5] synchronization[2,6] and random walker.[7] The ultimate proof of our understanding of such systems and its basic principles is reflected in our ability to control them.[8] Questions concerning how to manage and control complex networks are important in science, engineering, and biology. Recently, the controllability of complex networks has become a hot topic,[8–11] the main point of which is applying the external signals to some nodes so that the system can achieve the desirable state in finite time. Controllability of complex networks with linear dynamics has been studied by Liu and Barabási, who proposed an efficient methodology to assess the controllability of real and manmade networks. According to Lin's structural controllability theorem[12] and the minimum inputs theorem,[8] Liu *et al.*[8] proposed the concept of the minimum set of driver nodes (N_{D}) which can maintain full control over the network. The nodes controlled directly by input signals are called driver nodes, which can be computed by maximum matching.[8] The controllability index N_{D} (the minimum number of driver nodes) was used as a measure of the difficulty to control a network. The network with high N_{D} means poor controllability. The main conclusions of Ref. [8] are that (i) the controllability of networks is mainly determined by the degree distributions of networks; (ii) the driver nodes tend to avoid the high-degree nodes. To further study this problem, many studies focused on the optimization of network controllability through the structural perturbations. Wang *et al.*[13] proposed a method to add the smallest number of links to optimize the network that can be fully controlled using only one control signal. Hou *et al.*[14] found that assigning the link direction is more practical and effective than that of reconstructing the network in improving the network controllability. Furthermore, other studies investigated the correlations between controllability and structure properties, such as, betweenness and closeness centrality,[15] and degree correlation coefficients.[33]

However, the destruction of a few individuals can affect the normal functions of networks and systems, while the systems are always confronted by node attacks or failure. For industry fields, i.e., electric power grids,[16] transportation systems[17] and communication networks[18] and the Internet,[19] maintaining their efficiency is a matter of the utmost importance. The cascading failure and intentional attacks can easily damage their functions, such as, the network controllability[20–24] and connectivity.[25] Therefore, it is of significance to propose a method to enhance the robustness of network control ability against attack or failure. Previous works mainly focused on the static optimization of network controllability (SOC) without considering node attacks or failure, which cannot improve its robustness effectively.[13,31]

In this paper, we analyze the evolution of network controllability with static optimization of network controllability (SOC), and find that it can improve the robustness before the attack process but cannot decrease the increased rate of driver nodes during the attack process. Next, we are concerned with

*Project supported by the National Natural Science Foundation of China (Grant No. 60902094) and the Military Science Foundation of China (Grant No. 2010JY0072-046).

†Corresponding author. E-mail: xiaoyandong08@gmail.com

© 2014 Chinese Physical Society and IOP Publishing Ltd

enhancing the robustness of network controllability against malicious attack, called dynamics optimization of controllability (DOC). We monitor the size of the driver nodes to estimate how the network controllability gets destroyed after some "important" nodes are removed step by step. Although there are many methods to measure the "importance" of nodes, we choose the most used maximal degree as the measure of node importance. Malicious attack means that the most important node is deleted at each attack step.

2. Basic index of complex networks

For the convenience of sequential analysis, some basic concepts of complex networks are introduced. We introduce the features that have strong correlations with the controllability of complex networks and abandon others have been proved to have no discernible impact, for instance, clustering coefficient and modularity.[33]

2.1. Network heterogeneity

The heterogeneity index of a network was defined according to the Lorenz curve and Gini coefficient originally used in microeconomics to describe income inequality.[27] Applied to networks, the heterogeneity index provides a measure of the average degree of inequality in a network. The index H is defined as[27]

$$H = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}|k_i - k_j|}{2N^2\langle k\rangle}, \tag{1}$$

where N is the total number of nodes and k_i labels the degree of the i-th node. Actually, the H considers the difference of every two degree values in a degree sequence. Apparently, $0 < H < 1$ and the larger index implies a higher level of heterogeneity. The $H = 0$ means a completely homogeneous network, where all nodes have the same degree. Heterogeneous networks are harder to control and they are less robust to intentional attacks.[8]

2.2. Network assortativity

A network is said to show the feature of assortativity if the nodes that have many connections tend to be connected to other nodes with many connections,[26,28] i.e., a preference for high-degree nodes to attach to other high-degree nodes. On the contrary, others show disassortativity-high-degree nodes attached to low-degree ones. If a network has perfect assortativity ($r = 1$), then all nodes connect only with nodes with the same degree. If the network has no assortativity ($r = 0$), then any node can randomly connect to any other node. If a network is perfectly disassortative ($r = -1$), all nodes will have to connect to nodes with different degrees.

Degree assortativity of directed networks has been defined by Newman as a Pearson correlation between the expected degree distribution and the joint degree distribution.[28] For the practical purpose of evaluating r on an observed network, Newman[29] rewrote the degree assortativity as follows:

$$r = \frac{\sum_i j_i k_i - L^{-1}\sum_i j_i \sum_i k_i}{\sqrt{[\sum_i j_i^2 - L^{-1}(\sum_i j_i)^2][\sum_i k_i^2 - L^{-1}(\sum_i k_i)^2]}}, \tag{2}$$

where j_i and k_i are the excess in-degree and out-degree of the nodes that the i-th link leads into and out of respectively, and L is the number of edges.

However, since nodes in directed networks have both in-degrees and out-degrees, classes of directed networks show common patterns across the four directed degree–degree correlation measures: $r(\text{in},\text{in})$, $r(\text{in},\text{out})$, $r(\text{out},\text{in})$, $r(\text{out},\text{out})$,[30] where the first element labels the degree of the source node of the directed link, and the second represents the degree of the target node. Let $\alpha,\beta \in \{\text{in},\text{out}\}$ index the degree type, and j_i^α and k_i^α be the α- and β- degrees of the source node and target node for link i. Then the directed assortativity using the Pearson correlation is defined as

$$r(\alpha,\beta) = \frac{L^{-1}\sum_i[(j_i^\alpha - \bar{j}^\alpha)((k_i^\beta - \bar{k}^\beta)]}{\sigma^\alpha\sigma^\beta}, \tag{3}$$

where L is the number of links in the network, j^α is the degree of the source node, and k^β is the degree of the target node; and $\bar{j}^\alpha = L^{-1}\sum_i j_i^\alpha$, $\sigma^\alpha = \sqrt{L^{-1}\sum_i (j_i^\alpha - \bar{j}^\alpha)^2}$; $\bar{k}^\beta$ and σ^β are similarly defined. The four directed assortativity types are shown in Fig. 1. Pósfai *et al.*[33] investigated that the driver nodes have linear, quadratic or independent correlations on the four degree correlation coefficients.

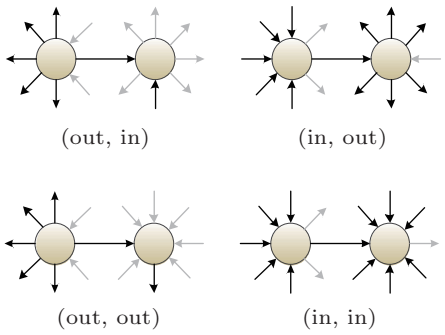


Fig. 1. (color online) The four directed degree–degree correlations in directed networks. The fuzzy directed links represent that they do not enter into the specific correlation.

3. Robustness of network controllability index

In real systems, when a fraction of power stations in the electricity network are malfunctioning due to either node cascade failures or malicious attacks, the whole network may be paralyzed because it is broken into several isolated parts. Therefore, the robustness of networks means that it maintains the mitigation ability so that it still has considerable connected components in the network after several malicious attacks. To avoid such a dramatic break-down and reduce the fragility of complex networks, a procedure proposed by Schneideret *et al.*[25] successfully optimizes the robustness of a network

against malicious attacks by exchanging only a small number of links. In particular, they introduce an index R as a unique measure to weigh the robustness of the network, which is defined as

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

where N is the number of nodes in the network, and $s(q)$ is the fraction of nodes in the largest connected component after removing qN nodes by malicious attack.

Actually, the controllability of networks has a strong correlation with the connectivity because the delivery of control signals relies on the connection between the pairs of nodes. Analogously, we also propose a robustness index CR to assess the evolution of controllability with the node removal, which is defined as

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

where $n_{\mathrm{D}}(q) \equiv N_{\mathrm{D}}(q)/N$ is the fraction of driver nodes in the remaining network after attacks. Therefore, the minimal number of driver nodes in the remaining network can evaluate the robustness of network controllability. Similar to the index R, if the CR is larger, it has better robustness of network controllability, because $N_{\mathrm{D}}(q)$ represents the minimum control price we should pay.

4. Methods

4.1. Static optimization of controllability

There are several methods through structural perturbations to optimize the controllability of networks without the process of node attacks or failure, called static optimization of controllability. We introduce two typical SOC methods, called adding minimum links (AML, see Fig. 3(c)) and rewiring redundant links (RRL), respectively. AML is the minimal cost of structural perturbations (only $N_{\mathrm{D}} - 1$ adding links) to control the network using only one control signal, which simply links the ending node of the control path to the starting node of the other control paths in proper sequence.[13] According to the introduction of the link category on network controllability, deleting a redundant link cannot increase the number of driver nodes, and adding a link may enhance the controllability of a network but never weaken the controllability of a network. If we keep the total number of links unchanged and only rewire some links, rewiring redundant links until there are no redundant links can also optimize the network controllability effectively.[31]

Consider an arbitrary network $G(V, E)$ with the minimum number of driver nodes being N_{D}. After improving the initial network through SOC, we present the change of network controllability with a malicious attack (attack the node with the largest degree in each step) in Fig. 2, where $n_{\mathrm{D}}(q)$ ($\equiv N_{\mathrm{D}}(q)/N$) is the fraction of minimum driver nodes $N_{\mathrm{D}}(q)$ after removing qN nodes in the ER network. We can see from Fig. 2 that the SOC can significantly optimize the network controllability when $q = 0$. What is noteworthy is that though the improved network has better controllability at the beginning, the increased rate of n_{D} does not have significant improvement during the process of a malicious attack. This result indicates that the advantage of the robustness of network controllability in the SOC network might stem from the better controllability at the beginning. With the process of a malicious attack, the network optimized by SOC cannot have any advantage of robustness for network controllability at all, that is, there exists another method of structural perturbations that can generate a network with more robustness of network controllability against intentional attacks. Moreover, even though the CR of SOC is larger than that of the initial networks, this dominant position may be caused by the different controllability at $q = 0$.

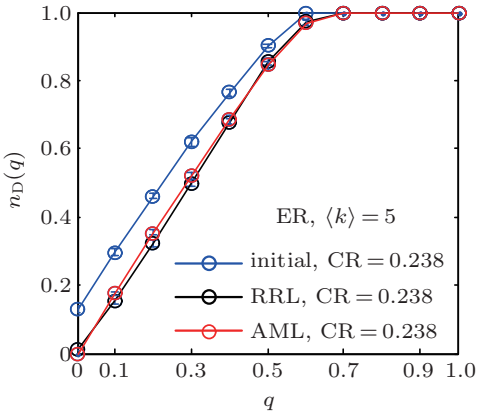


Fig. 2. (color online) Plot of the fraction of driver nodes $n_{\mathrm{D}}(q)$ after the removal of qN nodes. AML represents adding the directed link from the end of one control path to the start of another control path, while RRL is the method of rewiring the redundant links in the networks. The network size $N = 500$ and average degree $\langle k \rangle = 5$. Each data point result is obtained by averaging over 30 different realizations and all the error bars are small.

4.2. Dynamic optimization of controllability (DOC)

Node attacks and failure are common problems that always occur in real systems, i.e., electricity networks. However, to optimize the robustness of network controllability by only SOC would not cause noticeable improvements under a malicious attack. Therefore, we propose a method of dynamic optimization of controllability (DOC) because it evolves a heuristic algorithm in every step of structural perturbation.

In order to optimize the network robustness R, Schneider *et al.*[25] proposed a simple hill-climbing search to modify a network topology. Analogously, we can use the heuristic algorithm to optimize the robustness of network controllability. Note that the restriction to keep the degree of each node fixed is always important and of real significance in the modification of artificial systems, for example, the installation of power lines between a pair of power plants would skyrocket

costs and be impractical. In this paper, we follow the restriction to fix the in-degree and out-degree of each node when swapping the links. Hence, in the original network, we swap the connections of two randomly chosen links, that is, the directed links e_{ij} and e_{kl}, which point from node i to node j, and from node k to node l, become e_{il} and e_{kj} respectively (see Fig. 3(a)). Besides, in order to eliminate the ambiguity of the CR caused by the different $N_{\rm D}$ at the beginning, we firstly use AML to optimize the network controllability, which connects all the local control paths to a global control path containing all the nodes. So our optimizing process contains two steps: first using AML to achieve the complete controllability, and then increase the robustness index CR through link swapping. Unless stated, we will consider AML as SOC in what follows.

Now, we present an improved version of DOC under malicious attacks using simulated annealing.

(I) **SOC** Consider a network $G(V,E)$ (see Fig. 3(b)) and use AML to optimize the network controllability firstly, denoted as $G'(V,E')$ (see Fig. 3(c)).

(II) **Link mark** Mark the global control path as $\bar{E}$ (see red links and green links in Fig. 3(c)).

(III) **Link swap** Choose two pairs of directed links e_{ij} and $e_{kl} \in (E' - \bar{E})$ randomly, and delete the two selected links and add the e_{il} and e_{kj} links, denote the new network as $G^*(V,E')$.

(IV) **Acceptance probability** Calculate the acceptance probability p of the system as

$$p = \begin{cases} \exp\left[\dfrac{\mathrm{CR}(G^*) - \mathrm{CR}(G')}{T}\right], & \text{if } \mathrm{CR}(G^*) < \mathrm{CR}(G'), \\ 1, & \text{if } \mathrm{CR}(G^*) \geq \mathrm{CR}(G'). \end{cases}$$

Meanwhile, we define τ as the number of edge swap which satisfies $p = 1$.

(V) **Comparison** Generate a random number r from $U(0,1)$. If $r < p$, make $G' = G^*$, otherwise discard G^*. Return to Step (III).

(VI) **Stop** If the predefined amount of edge swaps ω is reached, the search is stopped. Here, we define the amount of edge swaps as $10|N|\langle k\rangle$.

The simulated annealing allows a network G^* with $\mathrm{CR}(G^*) < \mathrm{CR}(G')$ to be chosen with finite probability, where global optimization could be reached and inferior local results could be avoided. Furthermore, we decrease the temperature as a function of the number of edge swaps, by following the equation: $T(\tau) = 0.8^{\tau}$.

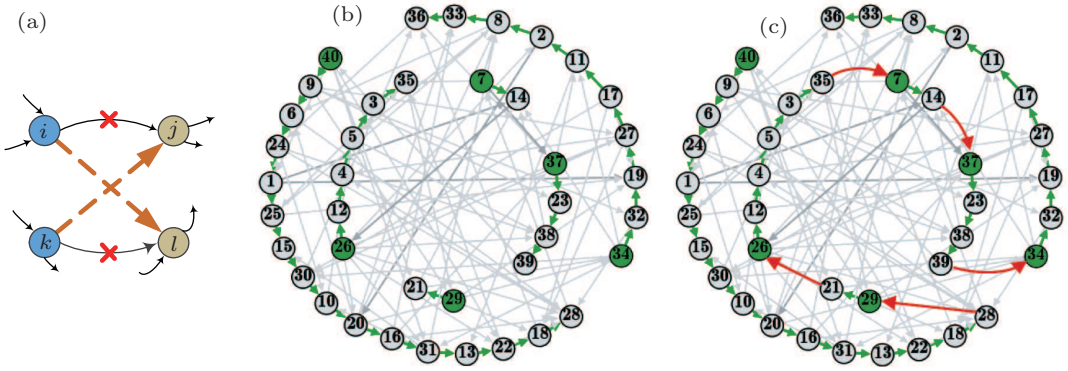


Fig. 3. (color online) Method for dynamic optimization of network controllability. (a) Swapping the two randomly chosen links, the links e_{ij} and e_{kl}, respectively become e_{il} and e_{kj} to fix the in- and out-degree of each node. (b) The initial network is generated by the ER model with $N = 40$ and $\langle k\rangle = 5$, and the green links represent the matching links. There are six local control paths in this network. (c) The typical SOC method, called adding minimum links. We add the red links to connect all the local control paths to a global control path.

5. Results and discussion

The procedure of DOC is starting from the generated ER and SF networks. The initial network is composed of $N = 500$ nodes and the average degree $\langle k\rangle = 5$. We also investigate whether our method can enhance the robustness of network connectivity after malicious attacks or not, because the connection of pairs of nodes also affects the network controllability. A plot of $n_{\rm D}(q)$ and $s(q)$ versus q under malicious attack is shown in Fig. 4. The "SOC" represents that the procedure of optimization only using the first step of the DOC. Therefore, we can compare the robustness of network controllability under malicious attack at the same level, eliminating the ambiguity of Fig. 2. In this plot, the curves indicate that the DOC obviously optimizes the robustness of network controllability under malicious attacks, at the same time it slows down the decrease speed of the strongly connected component in the network. More specifically, the CR and R of the ER network improved by DOC are 54.11% and 132.32% larger than that of the initial network respectively. Due to the links with direction, $s(q)$ can be easily and sharply damaged under malicious attacks. However, our method mitigates the damage of connectivity effectively.

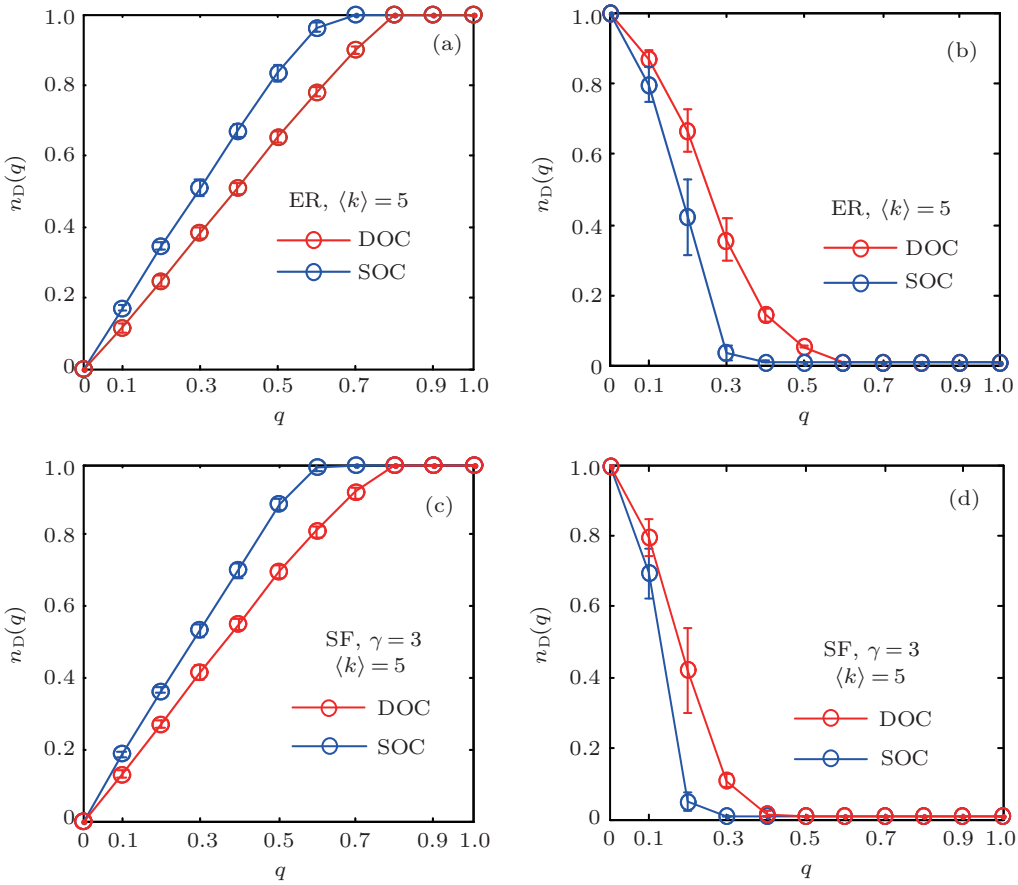


Fig. 4. (color online) Plot of the fraction of driver nodes $n_D(q)$ and the largest strong connected component size $s(q)$ after the removal of qN nodes. (a) and (b) ER network, (c) and (d) SF network with $\gamma = 3$. The initial network is composed of $N = 500$ and $\langle k \rangle = 5$. The results are averaged over 30 independent realizations.

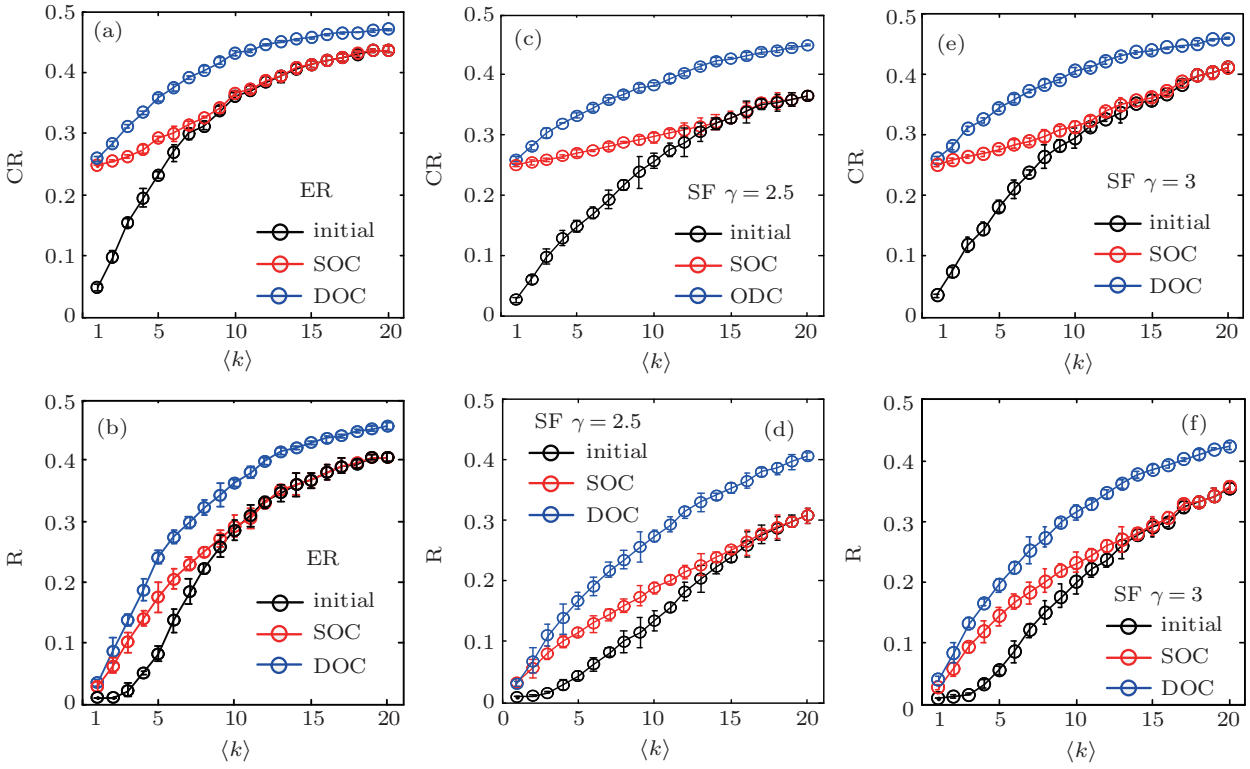


Fig. 5. (color online) CR and R as a function of $\langle k \rangle$ for DOC and SOC methods on ER networks ((a) and (b)), SF networks with $\gamma = 2.5$ ((c) and (d)), SF networks with $\gamma = 3$ ((e) and (f)). The initial network is composed of $N = 500$ and $\langle k \rangle = 5$. The results are averaged over 30 independent realizations.

Besides, we investigate the CR and R of networks with different average degrees $\langle k\rangle$ by the DOC as shown in Fig. 5. When the $\langle k\rangle$ is small, DOC can notably enhance the robustness for network controllability and connectivity against malicious attacks. Oppositely, with the increase of $\langle k\rangle$, the advantage of DOC is weakening and SOC cannot improve anymore. This is because the dense network itself has the ability to mitigate the damage caused by malicious attacks. Figure 5 also indicates that the CR of the ER network is larger than that of the SF network. These results stem from the different structural characters of networks. Compared to CR, the connectivity index R has the same tendency during the attack process. To deeply understand the function of DOC, we investigate some differences of structural characters between the initial and improved networks.

First, the network heterogeneity defined by Eq. (1) is considered. Since the results in Refs. [8] and [14] show that the degree of heterogeneity strongly influences the network controllability, we compare the network heterogeneity between the initial and improved networks, which are shown in Fig. 6. The decreases of $H_{\rm in}$ and $H_{\rm out}$ mean the improved network tends to be more homogeneous. We can obtain that the DOC dramatically decreases the in- and out-degree heterogeneity when the average degree is small. With the increase of $\langle k\rangle$, the difference of H between the initial network and the improved network gets smaller and smaller, eventually getting to be the same. As we know, the network becomes completely controllable with the increase of $\langle k\rangle$, thus it is unnecessary to optimize the controllability using SOC. On the other hand, it demonstrates that connecting the control paths is an efficient way to decrease heterogeneity, especially for sparse networks. After DOC, the degree distribution tends to be more homogenous. The network has fewer nodes with low degrees, especially for the network with small $\langle k\rangle$. It is because the larger the differences between the nodes' degrees are, the more the control costs. Moreover, figure 6 implies that the heterogeneity of the ER network is less than that of the SF network. This result also proves that the ER network is more robust for network controllability than the SF network. Besides, based on the experimental results, the heterogeneity of out-degree and in-degree have a similar changing trend, soi t is difficult to clearly identify which heterogeneity is more important for network controllability.

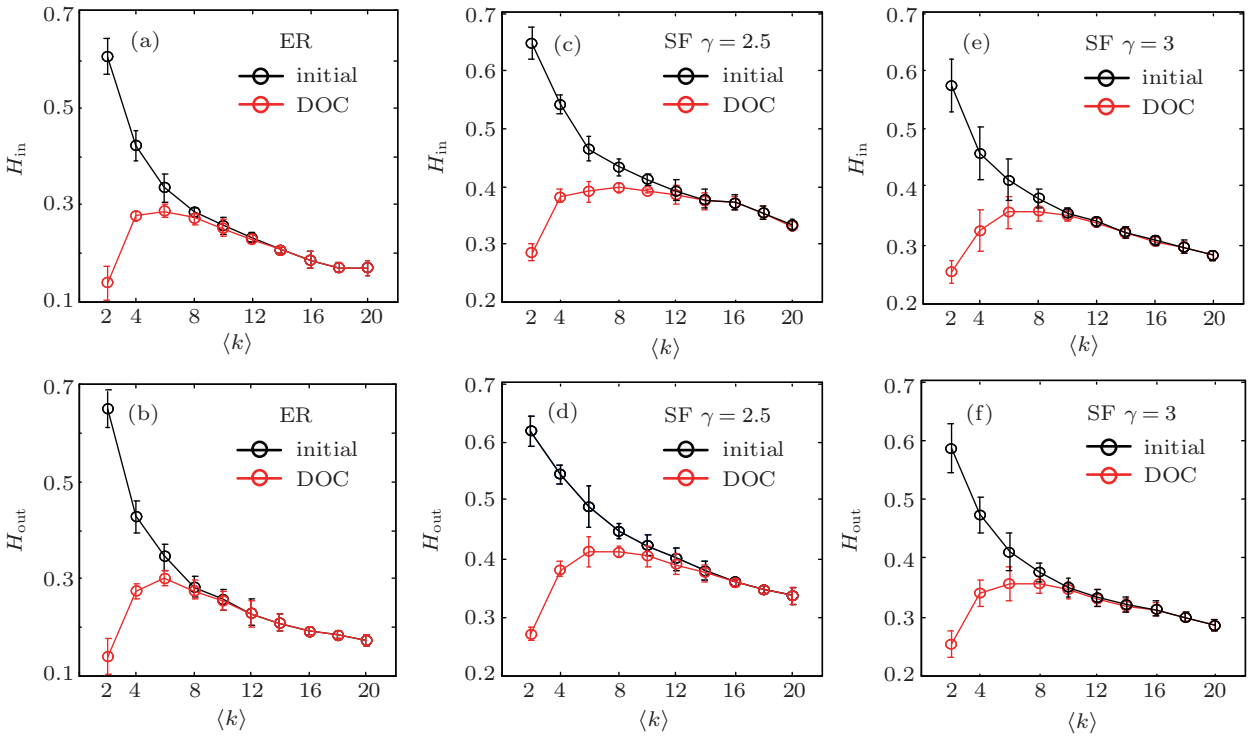


Fig. 6. (color online) $6H_{\rm in}$ and $H_{\rm out}$ as a function of $\langle k\rangle$ for DOC and initial on ER networks ((a) and (b)), SF networks with $\gamma = 2.5$ ((c) and (d)), SF networks with $\gamma = 3$ ((e) and (f)). The initial network is composed of $N = 500$ and $\langle k\rangle = 5$. The results are averaged over 30 independent realizations.

What is noteworthy is that the network heterogeneities of SOC and DOC have the same values because of the swapping restriction, that is, the structural perturbations cannot change the in- and out-degree of any single node (see the i-th node of Fig. 3 before and after the link swapping). Therefore, we need to demonstrate the reason why the DOC network has better robustness against intentional attacks. The degree–degree correlation (also called assortativity or disassortativity) is consid-

ered because the link swapping process changes the degree–degree correlations between the pairs of nodes. For example, these correlations between the i-th node and l-th node are different from that between the i-th node and the j-th node (see Fig. 3(a)). As we know, each node in directed networks has an in-degree and an out-degree, thus there are four correlation coefficients defined above: correlations between the source node's in- and out-degree, and the target node's in- and out-degree, such as, $r(\text{in},\text{in})$, $r(\text{in},\text{out})$, $r(\text{out},\text{in})$, $r(\text{out},\text{out})$. We investigate the assortativity coefficient defined by Eq. (2) and the directed degree–degree correlation of four different types defined by Eq. (3). We report our simulation results in Fig. 7. From Figs. 7(a)–7(c), the DOC increases the degree–degree correlation when it optimizes the robustness of network controllability. It means that the improved network has the tendency of transferring from disassortativity to assortativity. This is similar with the optimization of maintaining connectivity against malicious attacks,[25,32] which implies that changing the mixing pattern toward positive assortativity can enhance the robustness. However, although the improved networks change the feature of degree–degree correlations from a global structure, it needs to investigate the four directed degree correlations because Ref. [33] has indicated that they systematically affect network controllability. In Figs. 7(d)–7(f), the scatter plots show that all the $r(\alpha,\beta)(\alpha,\beta\in\{\text{in},\text{out}\})$ of DOC networks increase from negative to positive values. Especially for $r(\text{out},\text{in})$, it increases dramatically since the high correlations lower the number of driver nodes.[33] It is important for the networks with an assortativity coefficient to maintain the connectivity and controllability against malicious attacks, because once a node with the highest degree was attacked or failed, its neighbor node can replace it to maintain the functions normally.

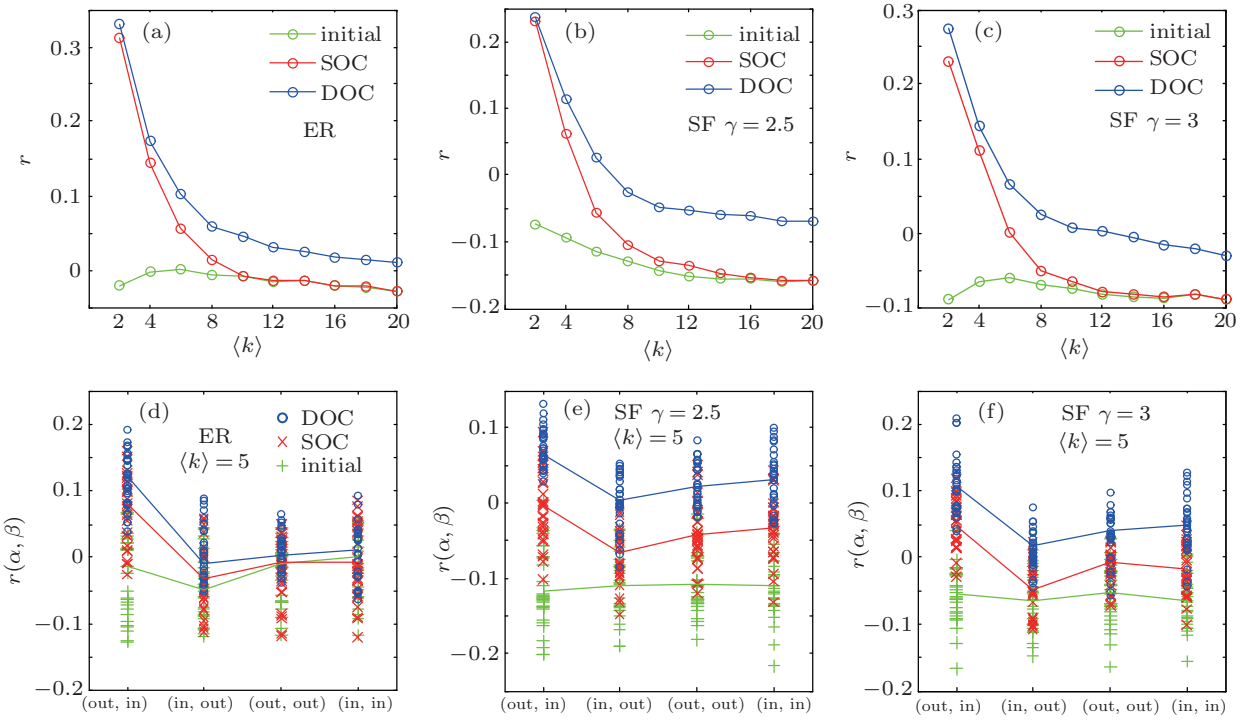


Fig. 7. (color online) Scatter plot of the robustness index CR as a function of ((a) and (b)) the degree-degree correlation r and ((c) and (d)) the four directed correlation $r(\alpha,\beta)(\alpha,\beta\in\{\text{in},\text{out}\})$ for initial and improved networks. The curves represent the average value of the four directed assortativities. All the modeled networks are $N=500$ and $\langle k\rangle=5$. The results are averaged over 30 independent realizations.

Besides, we further compare the robustness of links[8] on network controllability after applying our algorithm. In Ref. [8], the links are classified into three different types: critical, ordinary, and redundant. A link is critical if its absence increases the minimum number of driver nodes to maintain full control of the network; a link is redundant if its absence does not affect the current set of driver nodes; a link is ordinary if it is neither critical nor redundant. According to the different function of link categories, the absence of an ordinary link only changes the control configurations but the network is still controllable with the same number of driver nodes. The networks with high robustness must have more ordinary links. The link robustness of controllability is characterized by the number of ordinary links E_{O}, $e_{\text{O}}\equiv E_{\text{O}}/E$, where E is the total number of links and e_{O} is the fraction of ordinary links. Figure 8 shows the values of e_{O} in the DOC and SOC networks. It clearly shows that e_{O} in networks by DOC is larger than that by SOC, which implies that is why the networks improved by

DOC out perform SOC against malicious attacks. When $\langle k \rangle$ is medium, the result is especially obvious. These results also demonstrate that the DOC network can mitigate the destruction of controllability against edge removals.

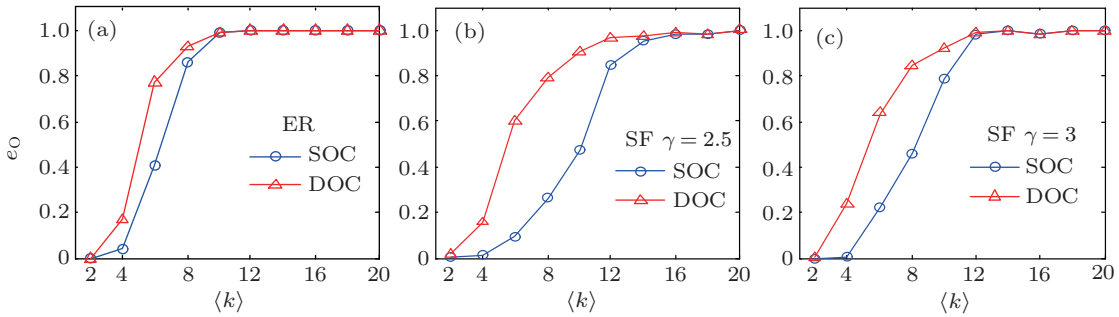


Fig. 8. (color online) Behavior of e_O as a function of $\langle k \rangle$ for the SOC and DOC methods on (a) ER network, (b) SF network with $\gamma = 2.5$, (c) SF network with $\gamma = 3$. The results are averaged over independent realizations.

6. Conclusion

Enhancing the robustness of network controllability and connectivity is of real significance. In this paper, we compare the robustness of networks controllability with static optimization of network controllability against malicious attacks; however, it can optimize the controllability efficiently but cannot mitigate the damage of controllability during the attack process. Therefore, we propose a method of dynamic optimization to improve the robustness of network controllability against malicious attacks. The optimization procedure uses the strict structural perturbation, which keep the in- and out-degree fixed. Moreover, through the views of underlying structure, we deeply analyze the effectiveness of our method and find that the improved networks tend to be homogenous and assortative. We further investigate the link robustness of controllability, and show that the network improved by DOC has higherlink robustness, which means this method can mitigate the destruction of controllability against edge and removals simultaneously. In summary, our method provides a practical and effective way to obtain the directed networks with high robustness of controllability.

References

[1] Barzel B and Barabási A L 2013 *Nat. Phys.* **9** 673
[2] Arenas A, Diaz-Guilera A, Kurths J, Moreno Y and Zhou C 2008 *Phys. Rep.* **469** 93
[3] Lloyd A L and May R M 2001 *Science* **292** 1316
[4] Liu Z B, Zhang H G and Sun Q Y 2010 *Chin. Phys. B* **19** 090506
[5] Moreno Y, Nekovee M and Pacheco A F 2004 *Phys. Rev. E* **69** 066130
[6] Wu J S, Jiao L C and Chen G R 2011 *Chin. Phys. B* **20** 060503
[7] Shen Y, Pei W J, Wang K and Wang S P 2009 *Chin. Phys. B* **18** 3783
[8] Liu Y Y, Slotine J J and Barabási A L 2011 *Nature* **473** 167
[9] Egerstedt M 2011 *Nature* **473** 158
[10] Müller F J and Schuppert A 2011 *Nature* **478** E4
[11] Sorrentino F, Bernardo M, Garofalo F and Chen G R 2007 *Phys. Rev. E* **75** 046103
[12] Lin C T 1974 *IEEE Trans. Autom. Contr.* **19** 201
[13] Wang W X, Ni X, Lai Y C and Grebogi C 2012 *Phys. Rev. E* **85** 026115
[14] Hou L L, Lao S Y, Liu G and Bai L 2012 *Chin. Phys. Lett.* **29** 108901
[15] Banerjee S J and Roy S 2012 arXiv:1209.3737
[16] Sole R V, Rosas-Casals M, Corominas-Murtra B and Valverde S 2008 *Phys. Rev. E* **77** 026102
[17] Motter A E and Lai Y C 2002 *Phys. Rev. E* **66** 065102
[18] Albert R, Jeong H and Barabási A L 2000 *Nature* **406** 378
[19] Buldyrev S V, Parshani R, Paul G, Stanley H E and Havlin S 2010 *Nature* **464** 1025
[20] Xiao Y D, Lao S Y, Hou L L and Bai L 2013 *Acta Phys. Sin.* **62** 180201 (in Chinese)
[21] Lv T Y, Piao X F, Xie W Y and Huang S B 2012 *Acta Phys. Sin.* **61** 170512 (in Chinese)
[22] Nie S, Wang X, Zhang H, Li Q and Wang B 2014 *PLoS ONE* 9e89066
[23] Pu C L, Pei W J and Michaelson A R 2012 *Physica A* **391** 4420
[24] Ruths J and Ruths D 2013 *Complex Networks IV* 185
[25] Schneider C M, Moreira A A, Andrade J S, Havlin S and Herrmann H J 2011 *Proc. Natl. Acad. Sci. USA* **108** 3838
[26] Newman M E 2003 *SIAM Rev.* **45** 167
[27] Hu H B and Wang X F 2008 *Physica A* **387** 3769
[28] Newman M E 2002 *Phys. Rev. Lett.* **89** 208701
[29] Newman M E 2003 *Phys. Rev. E* **67** 026126
[30] Foster J G, Foster D V, Grassberger P and Paczuski M 2010 *Proc. Natl. Acad. Sci. USA* **107** 10815
[31] Hou L L, Lao S Y, Bu J and Bai L 2013 *Proceedings of IEEE International Conference on Intelligent System Design and Engineering Applications* (Hong Kong) p. 709
[32] Wu Z X and Holme P 2011 *Phys. Rev. E* **84** 026106
[33] Pósfai M, Liu Y Y, Slotine J J and Barabási A L 2013 *Sci. Rep.* **3** 1067