An effective method to improve the robustness of small-world networks under attack*

Zhang Zheng-Zhen(张争珍)[a], Xu Wen-Jun(许文俊)[a], Zeng Shang-You(曾上游)[b], and Lin Jia-Ru(林家儒)[a]†

[a] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
[b] College of Electronic Engineering, Guangxi Normal University, Guilin 541004, China

(Received 21 September 2013; revised manuscript received 24 April 2014; published online 20 June 2014)

In this study, the robustness of small-world networks to three types of attack is investigated. Global efficiency is introduced as the network coefficient to measure the robustness of a small-world network. The simulation results prove that an increase in rewiring probability or average degree can enhance the robustness of the small-world network under all three types of attack. The effectiveness of simultaneously increasing both rewiring probability and average degree is also studied, and the combined increase is found to significantly improve the robustness of the small-world network. Furthermore, the combined effect of rewiring probability and average degree on network robustness is shown to be several times greater than that of rewiring probability or average degree individually. This means that small-world networks with a relatively high rewiring probability and average degree have advantages both in network communications and in good robustness to attacks. Therefore, simultaneously increasing rewiring probability and average degree is an effective method of constructing realistic networks. Consequently, the proposed method is useful to construct efficient and robust networks in a realistic scenario.

Keywords: small-world networks, robustness, network efficiency

PACS: 89.75.Fb, 89.75.Hc, 89.75.–k **DOI:** 10.1088/1674-1056/23/8/088902

1. Introduction

Complex networks have attracted much attention over the last decade. The milestones of the research on complex networks are the discoveries of small-world[1] and scale-free networks.[2] The primary characteristics of small-world networks regarding topology include short average distance between vertices and large clustering coefficient.[1] When used in network communications, small-world networks exhibit high global and local efficiencies.[3–5] In addition, when employed in network communications, small-world networks have other advantages, such as fast response, high coherent oscillation, and strong synchronization.[6,7] Many practical networks, including neural,[8–10] biological,[11] traffic,[12] social,[13] and communication networks,[14–16] have the two main characteristics of small-world networks.

Studies of transportation networks have shown that many transportation networks, such as the Indian railway network and the Boston subway,[5,17] have the properties of small-world networks. Numerous experimental studies have shown that, although there are many types of neural network in the brain, the primary pattern of neuronal connections in the brain is of the small-world type.[9,18] Some experimental studies show that some psychiatric disorders, such as Alzheimer's disease,[19] schizophrenia,[20] and attention-deficit/hyperactivity disorder,[21] are induced by the disruption or abnormality of small-world networks in the brain. Although the small-worldness reflects the global properties of brain functional networks, some experimental studies have shown that a hierarchical organization that can reflect both their local and global organization exists in the brain functional networks. The hierarchical organization of brain functional networks during visual tasks, which involve visual, sensory, and motor functions of the brain cortex, was analyzed,[22] and the modular architecture of the brain network was shown to correspond well to the anatomical organization of the cortex over different levels of hierarchy.[22] Furthermore, the consistency was found to become more pronounced at the vision, sensory, vision–temporal, and motor cortices during visual tasks, thus implying that the patterns of neural activities of brain cortex during a task are determined by the modular architecture of the brain, and the modular structure forms the physiological basis for the task.[22]

Small-world communication networks have attracted much attention. During the last decade, numerous small-world communication networks, such as telecommunication,[14,15] ad hoc,[16,23] P2P,[24,25] and wireless sensor networks,[26,27] have been proposed and investigated. Navigation of small-world communication networks was studied recently, and a

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61101117 and 61171100), the National Key Scientific and Technological Project of China (Grant Nos. 2012ZX03004005002 and 2013ZX03003012), the National High Technology Research and Development Program of China (863 Program, Grant No. 2014AA01A701), the Special Youth Science Foundation of Jiangxi Province of China (Grant No. 20133ACB21007), the Natural Science Foundation of Jiangxi Province of China (Grant Nos. 20132BAB201018 and 20132BAB201018), and the Fundamental Research Funds for the Central Universities, China (Grant No. BUPT2012RC0112).

†Corresponding author. E-mail: jrlin@bupt.edu.cn

© 2014 Chinese Physical Society and IOP Publishing Ltd

general scheme was proposed for navigating small-world networks in which existing networks are embedded into hidden metric space rather than adding links between vertices.[28] A navigation scheme for different types of small-world network can be established using a self-organized embedding algorithm. Therefore, the embedding algorithm is distributed and localized, thus differentiating it from previous algorithms. Navigability was shown to be enhanced only when networks exhibit strong small-world characteristics.[28] These results provide a profound insight into scalable routing in the Internet via a self-organized method in the absence of prior knowledge.[28]

Climate is considered to be a network of many dynamical systems, and graph theory is applied to a global data set to study its collective behavior.[29–32] A climate network is found to possess some properties of small-world networks. Further research showed that interaction between two interweaved subnetworks induces the overall dynamics. One subnetwork operates in the tropics whereas the other operates at higher latitudes. The equatorial subnetwork acts as an agent that establishes connections between the two hemispheres.[29–32] Although major differences exist between the two subsystems, both are small-world networks. The mid-latitude network is very similar to a scale-free network whereas the tropical one is almost a fully connected network. This unique architecture may lead to a new insight into the dynamics of the climate system.[29–32] Climate research based on complex networks has also been conducted by Chinese scholars.[33–35] A climate network of six climate indices of the North Pacific air–sea system during the last five decades was constructed, and synchronization and coupling of these indices were investigated.[33] Synchronization states are always followed by a reduction in coupling strength. Each synchronization state of the network is associated with abrupt phase or trend variations of North Pacific sea-surface temperature.[33] Specifically, abrupt climate change in the North Pacific air–sea system may be indicated by the synchronization and coupling of climate indices.[33] In another study, the spatial connection structural complexity of the circulation system and the influence of four teleconnection patterns are quantitatively described in terms of characteristic topology parameters of complex climate networks.[34] Research results show that teleconnections considerably shorten the mean shortest length of networks.[34] The topology of Chinese climate networks has been investigated using surface temperature data from 160 Chinese weather observations,[35] and the results show that the Chinese climate network exhibits a characteristic of regular networks with most vertices having the same number of edges and the absence of the so-called supervertices with a very large number of edges.[35]

Although numerous studies have been conducted on the robustness of small-world networks regarding network topology,[36] research on their robustness in terms of network efficiency has not yet been conducted thoroughly. Therefore, this aspect is extensively analyzed in this study. A small-world network having good robustness in terms of network efficiency will be an ideal model for constructing practical networks. In this study, three types of attack are chosen: intentional attack on the long-range edges, attack on the edges having the highest edge betweenness centrality, and attack on the vertices with the highest vertex betweenness centrality. The robustness of a small-world network is investigated under the above mentioned attacks. The robustness of the small-world network measured via global efficiency is shown to be improved monotonically by increasing the rewiring probability or the average degree under all three types of attack. The robustness of the small-world network measured using global efficiency can be significantly enhanced by simultaneously increasing rewiring probability and average degree. Furthermore, the increase in robustness achieved by increasing both rewiring probability and average degree is several times that achieved by increasing rewiring probability or average degree. Therefore, considering network efficiency and robustness, a small-world network with a relatively high rewiring probability and average degree is the ideal model for realistic networks. The information provided in this paper may be useful for the construction of future traffic, social, and communication networks.

2. Model

In 1998, Watts and Strogatz (WS) proposed the WS small-world network model and described its characteristics in the domain of network topology.[1] First, a regular network is constructed with N vertices and an average degree of k. The WS small-world network is then reconstructed by rewiring the network with probability p_{Rewire}.[1] Therefore, the number of long-range edges in the WS small-world network is $Nkp_{\text{Rewire}}/2$. On the basis of the WS small-world network, Newman and Watts (NW) proposed the NW small-world network model.[37] In the NW model, no edge is removed; however, long-range edges are added randomly. In order to preserve compatibility, the number of added long-range edges in the NW model is the same as that in the WS model.[37] In this model, the probability of adding a long-range edge (p_{Add}) in the NW small-world network is proportional to the rewiring probability (p_{Rewire}) in the WS small-world network. The total number of candidates for long-range edges is equal to $N(N-1)/2-Nk/2$. Therefore,

$$p_{\text{Add}} = \frac{Nkp_{\text{Rewire}}/2}{N(N-1)/2-Nk/2}.$$

Specifically, rewiring probability is also used to measure the small-world property of the NW small-world network. Since its introduction in 1998, the small-world model has been used

in numerous applications, especially in communication networks. In recent years, small-world wireless sensor networks (WSNs) have aroused extensive interest and thus developed quickly. In this study, they are chosen as the study samples. Construction of a small-world WSN is similar to that of an NW small-world network. In this study, a small-world WSN is constructed as follows.[38,39] In a 1000 mm $\times$1000 mm sensor field, 1600 sensors are uniformly deployed to form a regular grid network. Namely, in the regular grid network, the distance between two nearest sensors is 25 m. In a small-world WSN, there exist numerous low-end sensors (L-sensors) and a small set of powerful high-end sensors (H-sensors).[38,39] The H-sensors are distributed randomly in the regular grid network. The numbers of L- and H-sensors are denoted by $N_{\rm L}$ and $N_{\rm H}$, respectively. The sum of $N_{\rm L}$ and $N_{\rm H}$ equals 1600, i.e., $N_{\rm L}+N_{\rm H}=1600$. In order to reduce network cost and energy consumption, each L-sensor is a relatively weak device with relatively short transmission range. The H-sensor is a more powerful device and has two radios.[38,39] One radio of the H-sensor is used for communication with the L-sensors, and its transmission range, which is the same as that of the L-sensors, is relatively short. The other radio is used for communication among H-sensors, and its transmission range is chosen to be much longer (500 m). The transmission ranges of the L- and the H-sensors are denoted by $R_{\rm L}$ and $R_{\rm H}$, respectively. All the sensors in the small-world WSN communicate with one another by broadcasting in a relatively short communication range (i.e. $R_{\rm L}$), and this type of communication structures the regular graphs. Each H-sensor communicates with other H-sensors by unicasting, and this type of long-range edge communication induces the well known small-world effect.[38,39]

In the small-world WSN, the average degree (k) is determined by the transmission range of the L-sensors and is given by $k \simeq \pi R_{\rm L}^2/(25\times 25)$. The average number of neighboring H-sensors, which is the average number of H-sensors within the communication radius of a specific H-sensor, is denoted by $N_{\rm Neighbor_H}$. Because the ratio of the transmission area of each H-sensor to the whole sensor field is equal to $\pi R_{\rm H}^2/(1000\times 1000)$, i.e. $\pi/4$, $N_{\rm Neighbor_H}$ is approximately equal to $\pi N_{\rm H}/4$. The total number of all possible long-range edges among the H-sensors is a function of the total number of H-sensors ($N_{\rm H}$) and is denoted by $f(N_{\rm H})$. If the communication probability among neighboring H-sensors is denoted by $p_{\rm shortcut}$, the total number of all long-range edges in the small-world WSN is equal to $p_{\rm shortcut}f(N_{\rm H})$. Because $p_{\rm shortcut}f(N_{\rm H}) = Nkp_{\rm Rewire}/2$, $p_{\rm shortcut} = Nkp_{\rm Rewire}/2f(N_{\rm H})$.[38,39]

In their classical papers,[3–5] Latora and Marchiori described small-world characteristics in terms of network efficiency. The concept of network efficiency is restated here. An unweighted graph (G) with N vertices and K edges is considered, and it is assumed to be sparse, i.e. $N\times N$. In addition, G can be represented by an $N\times N$ connection matrix whose entry $a_{ij}=1$ if there is an edge connecting the ith and jth vertices; otherwise it is 0. An important coefficient of G is k_i, which denotes the number of edges connecting to the ith vertex, namely, the degree of the ith vertex. Because N vertices and K edges exist in G, the average value of k_i (i.e. the average degree of the whole network) is $k=2K/N$. Dijkstra's algorithm is used to find the shortest path between each pair of vertices (ith and jth vertices), and d_{ij} is the number of edges along the shortest path. If there is no path connecting the ith and jth vertices, $d_{ij}=+\infty$. Because the information transmission time between the ith and jth vertices is inversely proportional to d_{ij}, the corresponding network efficiency (ε_{ij}) can be given by $1/d_{ij}$. The global efficiency of G is given as

$$E_{\rm glob}(G)=\frac{\sum_{i\neq j\in G}\varepsilon_{ij}}{N(N-1)}=\frac{1}{N(N-1)}\sum_{i\neq j\in G}\frac{1}{d_{ij}}. \tag{1}$$

The global efficiency measures the network efficiency at the global scale and is the counterpart of the average distance.

The network efficiency of the subgraph G_i, which is the subgraph of the neighbors of the ith vertex, can also be evaluated. The local property of G can be characterized by the local efficiency ($E_{\rm loc}$), which is defined as

$$E_{\rm loc}=\frac{1}{N}\sum_{i,\in G}E_{\rm glob}(G_i), \tag{2}$$

where i is an arbitrary vertex in G. The local efficiency measures the network efficiency on a local scale and is the counterpart of the clustering coefficient. Because k, $E_{\rm loc}$ measures the fault tolerance of the system. Therefore, the characteristics of small-world networks can be generalized in terms of network efficiency, i.e. high global and local efficiencies.

In this study, attacks are carried out in three different ways. The first method involves the intentional removal of long-range edges. In the second method, the edges are removed one by one starting from the edge having the highest edge betweenness centrality.[36,40] In the third method, the vertices are removed one after another starting from the vertex having the highest vertex betweenness centrality.[36,40] The edge betweenness centrality ($C_{\rm B}(e)$) is defined as[36,40]

$$C_{\rm B}(e)=\sum_{i\neq j\in G}\frac{\sigma_{ij}(e)}{\sigma_{ij}}, \tag{3}$$

where σ_{ij} is the total number of shortest paths between the ith and j-th vertices, and $\sigma_{ij}(e)$ is the number of these paths including the edge e. Similarly, the vertex betweenness centrality ($C_{\rm B}(v)$) is defined as[36,40]

$$C_{\rm B}(v)=\sum_{i\neq j\in G}\frac{\sigma_{ij}(v)}{\sigma_{ij}}, \tag{4}$$

where $\sigma_{ij}(v)$ is the number of shortest paths between the ith and j-th vertices passing through the vertex v, and σ_{ij} is the same as in Eq. (3).

3. Results

First, we construct a small-world WSN with 1600 sensors and a specific average degree k. When $p_{\text{Rewire}} = 1$, the total number of H-sensors is chosen to be 1600.[38,39] According to $p_{\text{shortcut}} = Nkp_{\text{Rewire}}/2f(N_{\text{H}})$, p_{shortcut} is equal to $1600k/2f(1600)$. Therefore,

$$p_{\text{Rewire}} = \frac{2p_{\text{shortcut}}f(N_{\text{H}})}{1600k},$$

which implies that p_{Rewire} depends on N_{H}. The definite value of $f(N_{\text{H}})$ can be obtained by simulation. According to $k \simeq \pi R_{\text{L}}^2/(25 \times 25)$, k can be controlled using R_{L}. Moreover, the property of a small-world network is determined by k and p_{Rewire} if the number of vertices of the network is fixed.

In the first simulation, the number of vertices and rewiring probability are set to be $N = 1600$ and $p_{\text{Rewire}} = 0.05$, and values of k are chosen to be 10, 30, 50, and 70. The variations of global efficiency with average degree under the three types of attack are shown in Fig. 1. When k is a fixed value, the global efficiency of the network in which no edges or vertices are cut (E_0) is chosen as the denominator. The global efficiency of a network with a certain removed ratio p of edges or vertices (E_p) is then the numerator. Therefore, the normalized global efficiency (E_{Norm}) of the network with a specific removed ratio of edges or vertices (p) is defined as E_p/E_0. The results of E_{Norm} as a function of k and p are shown in Fig. 1. The greater the value of E_{Norm}, the better the robustness of the network is. As can be seen from Fig. 1, as k increases, E_{Norm} increases monotonically for a fixed p. For example, if the network is under the first type of attack and p is set to be 0.04, the values of E_{Norm} are chosen to be 0.671, 0.815, 0.886, and 0.938 for values of k of 10, 30, 50, and 70, respectively. If the network is under the second type of attack and $p = 0.06$, the values of E_{Norm} are 0.271, 0.411, 0.532, and 0.728 for values of k of 10, 30, 50, and 70, respectively. If the network is under the third type of attack and p is set to be 0.4, the values of E_{Norm} are 0.275, 0.698, 0.839, and 0.917 for values of k of 10, 30, 50, and 70, respectively. From the above analysis, it is clear that as k increases the robustness of the small-world network is monotonically enhanced.

Next, the effect of rewiring probability (p_{Rewire}) on the robustness of the small-world network is analyzed. The number of vertices in the small-world network is still set to be 1600, and k is set to be 40. Further, the values of p_{Rewire} are chosen to be 0.02, 0.04, 0.06, 0.08, and 0.1. Figure 2 shows the variations of E_{Norm} with the removed ratio of edges or vertices (p) for different values of p_{Rewire}. As can be seen, the robustness of the network is enhanced as p_{Rewire} increases. For example, if the network is under the first type of attack and the values of p_{Rewire} are set to be 0.06, 0.08, and 0.1, the values of the corresponding E_{Norm} are 0.844, 0.927, and 0.958 for $p = 0.05$. When the network is under the second type of attack and the values of p_{Rewire} are set to be 0.02, 0.04, 0.06, 0.08, and 0.1, the values of the corresponding E_{Norm} are 0.279, 0.37, 0.524, 0.805, and 0.884 for $p = 0.06$. If the network is under the third type of attack and values of p_{Rewire} are set to be 0.02, 0.04, 0.06, 0.08, and 0.1, the values of the corresponding E_{Norm} are 0.477, 0.657, 0.717, 0.781, and 0.828 for $p = 0.5$. In addition, figure 2(a) shows that an increase in p_{Rewire} can quasi-linearly enhance the robustness of the network under the first type of attack. If the long-range edges are all removed (i.e., $p = p_{\text{Rewire}}$), the values of E_{Norm} are 0.323, 0.314, 0.305, 0.291, and 0.284 for values of p_{Rewire} of 0.02, 0.04, 0.06, 0.08, and 0.1, respectively. Although p and p_{Rewire} increase from 0.02 to 0.1 (5 times), E_{Norm} decreases only slightly from 0.323 to 0.284.

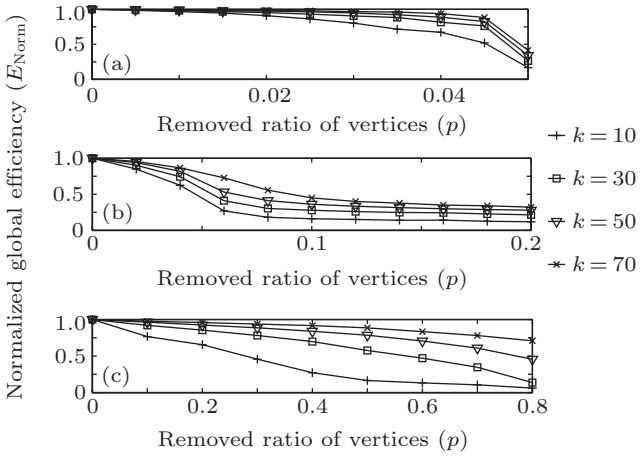


Fig. 1. Curves of normalized global efficiency versus removed ratio of edges or vertices for different values of k under the first (a), second (b), and third (c) types of attack.

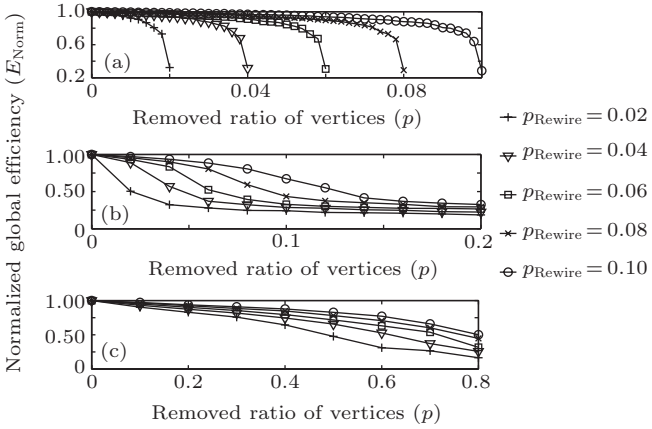


Fig. 2. Curves of normalized global efficiency versus the removed ratio of edges or vertices with different rewiring probabilities under the first (a), second (b), and third (c) types of attack.

According to the above analysis, the increase of either k or p_{Rewire} can improve the robustness of small-world networks. Next, we focus on the effectiveness of increasing both k and p_{Rewire}. When k and p_{Rewire} are fixed, the extreme case

in which all the long-range edges are removed is considered under the first type of attack. The global efficiency of the small-world network without any edges being cut is E_0, and the corresponding efficiency (i.e., $p = p_{\text{Rewire}}$) is E_{Rewire}. As a result, the normalized global efficiency E_{Norm} is given as E_{Rewire}/E_0. Based on the above analysis, the results of E_{Norm} as a function of k and p_{Rewire} are shown in Fig. 3(a). As can be seen, when $p = p_{\text{Rewire}}$ is a fixed value, E_{Norm} increases monotonically with increasing k. In other words, the robustness of the small-world network improves monotonically with increasing k, which is in accordance with the results shown in Fig. 1(a). When k is a fixed value and $p = p_{\text{Rewire}}$ is varied, E_{Norm} decreases very slowly with increasing p_{Rewire}, indicating that the robustness of the small-world network is enhanced quasi-linearly, which is in agreement with the results shown in Fig. 2(a). In addition, the joint effectivenesses of k and p_{Rewire} on network robustness are also shown in Fig. 3(a). For example, when $k = 10$ and $p_{\text{Rewire}} = 0.02$, $E_{\text{Norm}} = 0.216$. However, when $k = 100$ and $p_{\text{Rewire}} = 0.1$, E_{Norm} is 0.483. Although p and p_{Rewire} increase fivefold (from 0.02 to 0.1), the robustness of the latter network is much better than that of the former network.

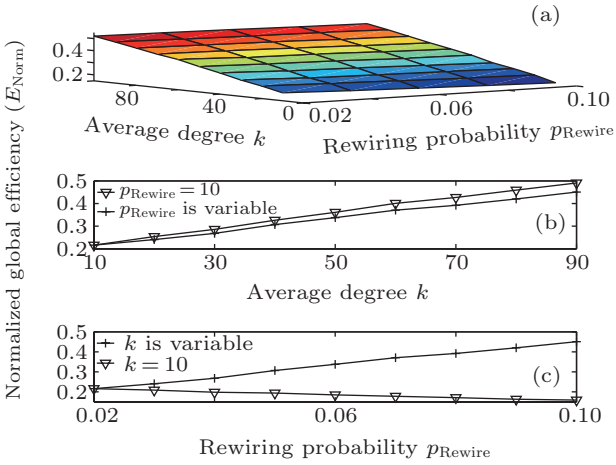


Fig. 3. (color online) Curves of (a) normalized global efficiency as a function of average degree and rewiring probability, (b) normalized global efficiency versus average degree, and (c) normalized global efficiency versus rewiring probability. Note that the pairs of k and p_{Rewire} of the curve marked by crosses are (10, 0.02), (20, 0.03), (30, 0.04), (40, 0.05), (50, 0.06), (60, 0.07), (70, 0.08), (80, 0.09), and (90, 0.1). In the extreme case, all the long-range edges are removed and $p = p_{\text{Rewire}}$.

To clearly show the combined effect of k and p_{Rewire} on network robustness, some results are selected from Fig. 3(a) and shown in Figs. 3(b) and 3(c). In Fig. 3(b), p_{Rewire} of the curve marked by triangles is set to be 0.02 whereas p_{Rewire} of the curve marked by crosses increases monotonically with increasing k. Therefore, the curve marked by triangles only shows the effect of k on the network robustness whereas the curve marked by crosses shows the combined effect of k and p_{Rewire}. As can be seen in Fig. 3(b), the maximum difference between the two curves is only 10%. For two pairs of k and p_{Rewire}, (90, 0.02) and (90, 0.1), E_{Norm} = 0.49 and 0.45, respectively. Although p and p_{Rewire} are increased fivefold (from 0.02 to 0.1), E_{Norm} is reduced by only 10%. Therefore, the combined effect of k and p_{Rewire} on network robustness is shown to be considerable. The curve marked by crosses in Fig. 3(c) shows the combined effect of k and p_{Rewire} on network robustness whereas the curve marked by triangles only shows the effect of p_{Rewire}. As can be seen, the difference between the two curves is increasing, thus indicating that the combined effect of k and p_{Rewire} on the network robustness is increasingly significant. When k = 10 and $p_{\text{Rewire}} = 0.1$, E_{Norm} is 0.159. However, when $k = 90$ and p_{Rewire} = 0.1, E_{Norm} is 0.45, which is an increase of 183%.

Next, another coefficient, which is the removed ratio of edges or vertices when the normalized global efficiency E_{Norm} is reduced to 0.8 ($p_{E_{\text{Norm}}=0.8}$), is introduced to measure the network robustness. The greater the value of $p_{E_{\text{Norm}}=0.8}$, the better the network robustness is. The results of $p_{E_{\text{Norm}}=0.8}$ versus p_{Rewire} and k are shown in Fig. 4. As can be seen, $p_{E_{\text{Norm}}=0.8}$ increases with increasing p_{Rewire} or k and is significantly increased with the combined increase of both. These results are in accordance with those of the above analysis. Some data from Fig. 4(a) are enumerated to confirm our conclusion. When $k = 10$ and $p_{\text{Rewire}} = 0.02$, $p_{E_{\text{Norm}}=0.8}$ is as small as 9.8×10^{-3}. When k is increased individually to 100 and $p_{\text{Rewire}} = 0.02$, $p_{E_{\text{Norm}}=0.8}$ increases to 1.95×10^{-2}. When p_{Rewire} is increased individually to 0.1 and $k = 10$, $p_{E_{\text{Norm}}=0.8}$ increases to 0.055. When both k and p_{Rewire} are increased to 100 and 0.1, respectively, $p_{E_{\text{Norm}}=0.8}$ increases significantly and is almost 0.095. Data from Figs. 4(b) and 4(c) also support our argument. For conciseness, they are not enumerated in the paper.

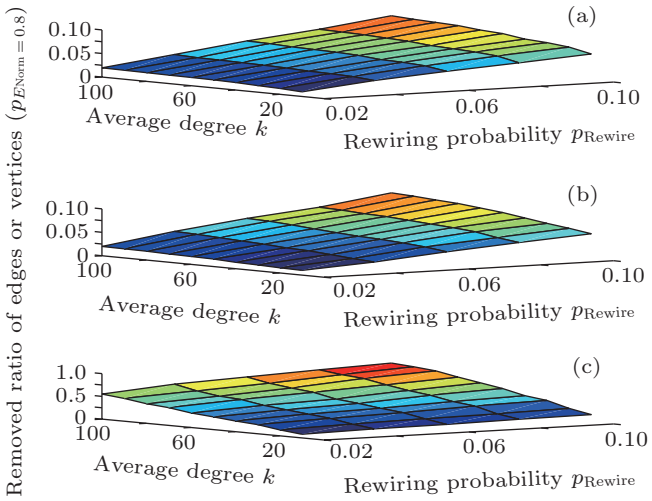


Fig. 4. (color online) Curves of the removed ratio of edges or vertices $p_{E_{\text{Norm}}=0.8}$ versus average degree and rewiring probability under the first (a), second (b), and third (c) types of attack.

As done from Figs. 3(b) and 3(c), some results are selected from Fig. 4 to clearly show the combined effect of av-

erage degree and rewiring probability. The data of Figs. 5(a) and 5(b) are selected from Fig. 4(a), and the data of Figs. 5(c) and 5(d) are selected from Fig. 4(b). The data of Figs. 5(e) and 5(f) are selected from Fig. 4(c). The individual effects of average degree and rewiring probability on network robustness are shown with the curve marked by triangles in Fig. 5, whereas the combined effect of k and p_{Rewire} is shown with the curve marked by crosses. The slopes of the curves in Fig. 5 are used to quantitatively measure these effects on network robustness. The combined effect of the average degree and rewiring probability on network robustness is found to be approximately eight, nine, and two times those of average degree under the first, second, and third types of attack, respectively. Furthermore, the combined effect of average degree and rewiring probability on network robustness is approximately two, two, and ten times those of rewiring probability under the first, second, and third type of attack, respectively. The above analysis shows that the combined increase of average degree and rewiring probability is advantageous to network robustness.

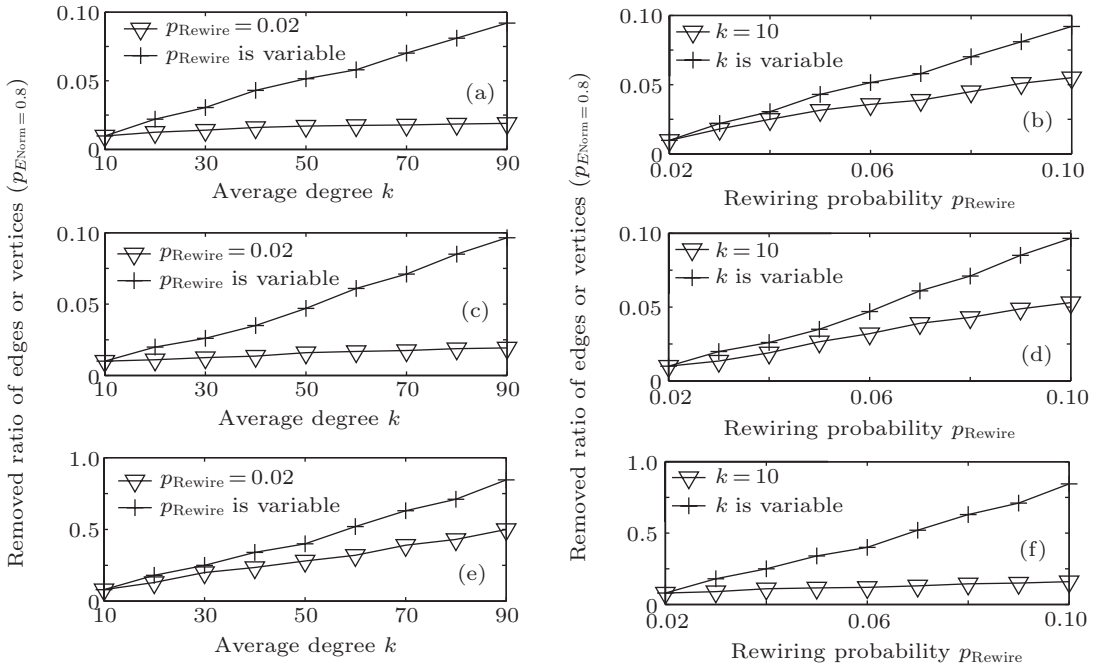


Fig. 5. Curves of $p_{E_{\text{Norm}}=0.8}$ versus k or p_{Rewire} under the (a), (b) first, (c), (d) second, and (e), (f) third type of attack (note that the pairs of k and p_{Rewire} of the curve marked by crosses are the same as those of the curve marked by crosses in Fig. 3).

From Figs. 1 and 2, we can see that the global efficiencies decrease rapidly under the first and second types of attack, but decrease slowly under the third type of attack. For example, if the number of vertices, rewiring probability, and average degree are set to be 1600, 0.02, and 40, respectively, and the removed ratio of edges or vertices is chosen to be 0.02, the global efficiencies decrease by 68, 50, and only 2% under the first, second, and third types of attack respectively. The long-range edges are known to play an important role in global efficiency. Therefore, when all the long-range edges are removed under the first type of attack, the global efficiency decreases considerably. Because long-range edges play a critical role in the shortest paths between vertices, the edges with the highest edge betweenness centrality are typically long-range edges. Therefore, the effect of the second type of attack on global efficiency is similar to that of the first type of attack, namely, the global efficiencies decrease rapidly under the first and second types of attack. Because the long-range edges are located randomly and quasi-uniformly in the entire network, the vertices with the long-range edges are also located randomly and quasi-uniformly in the entire network. Namely, there is no super-vertex with a very large number of long-range edges. Therefore, under the third type of attack, the number of long-range edges and global efficiency decrease slowly. Based on the above analysis, figure 6 shows the removed ratios of the long-range edges under the second and third types of attack when the number of vertices, rewiring probability, and average degree are set to be 1600, 0.02, and 40, respectively. As can be seen, under the second type of attack, the removed ratio of the long-range edges is as high as 95% when $p = 0.02$. We can also see in Fig. 6 that under the third type of attack, the removed ratio of the long-range edges reaches 95% only when the removed ratio of vertices is as high as 55%. Because the long-range edges are removed very quickly under the first and

second types of attack, the rewiring probability is assumed to play a more important role in network robustness than average degree, as shown in Fig. 5. Because the long-range edges are removed very slowly under the third type of attack, the rewiring probability is assumed to play a less important role in network robustness than average degree, which is also shown in Fig. 5.

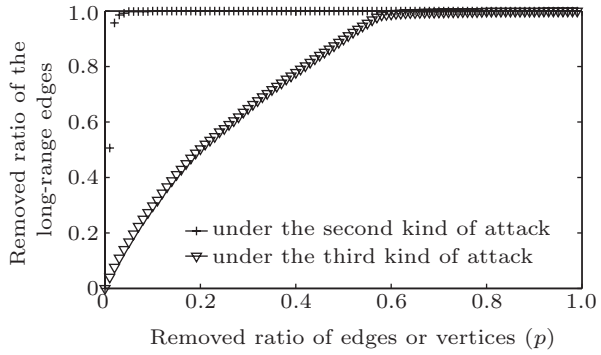


Fig. 6. Curves of removed ratio of long-range edges or vertices versus the removed ratio of edges or vertices under the second and third types of attack.

In previous studies, another coefficient S, which is the ratio of the size of the largest component to the size of the entire network, was introduced to measure network robustness.[36,41] In the following discussion, we compare the differences between network efficiency and the coefficient S to investigate the robustness of the small-world network. Because the complex network used in this study is an NW small-world network, the remaining network is still a regular network even though all the long-range edges are removed. Hence, the value of S is unity until all the long-range edges are removed. Therefore, we compare the differences between the network efficiency and S only under the second and third types of attack. The number of vertices, rewiring probability, and average degree are set to 1600, 0.05, and 40, respectively. The variations of $E_{\rm Norm}$ and S with different values of p under the second and third types of attack are shown in Figs. 7(a) and 7(b), respectively. As shown in Figs. 7(a) and 7(b), $E_{\rm Norm}$ and S decrease simultaneously in the attacking process, but there is a considerable difference between $E_{\rm Norm}$ and S. Even at the beginning of the attack, the value of $E_{\rm Norm}$ decreases considerably. The value of S decreases clearly until the removed ratios of edges and vertices reach 0.4 and 0.8, respectively. Because the network efficiency can reflect a slight variation in network topology, the value of $E_{\rm Norm}$ decreases considerably at the beginning of the attack. An observable variation in the value of S indicates that the network topology has a critical change; namely, the whole network has been divided into several subgraphs. Therefore, the value of S begins to exhibit visible variation only till the removed ratios of edges and vertices are very large.

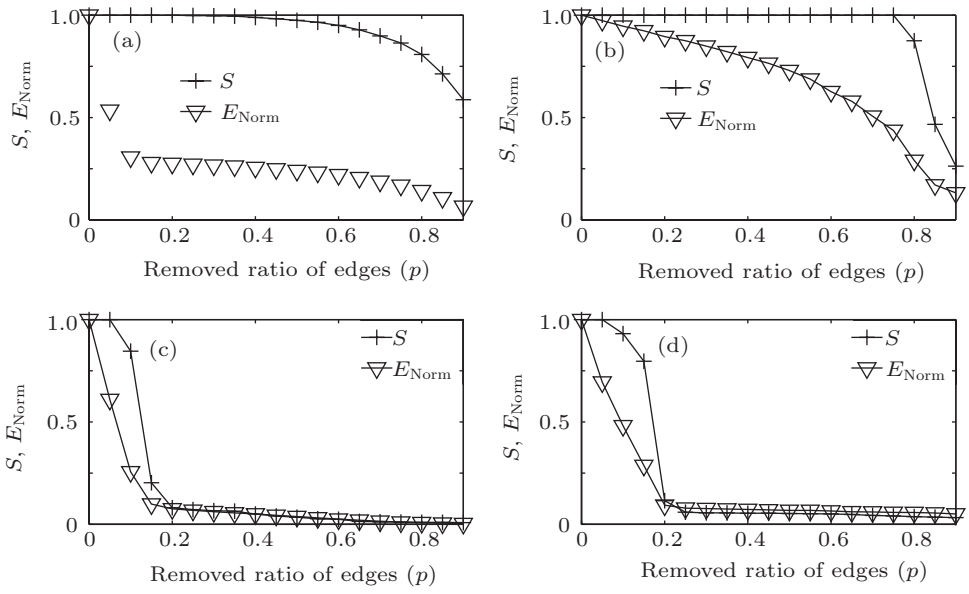


Fig. 7. Variations of $E_{\rm Norm}$ and S with p under the second (a) and third (b) types of attack for $k = 40$ and under the second (c) and third (d) types of attack for $k = 4$.

If the average degree is small, the whole network can easily be divided into numerous subgraphs under attack. Therefore, if the average degree is small, we assume that the value of S will have visible variation even at the beginning of attack. In order to confirm our assumption, the number of vertices and rewiring probability are still set to be 1600 and 0.05, respectively, but the average degree is reduced from 40 to 4. The variations of $E_{\rm Norm}$ and S with ratio value of p under the second and third types of attack are shown in Figs. 7(c) and 7(d), respectively. As can be seen, when p is as low as 0.1, the value of S has visible variation, thus confirming our assumption. In other words, because the variation of S reflects the

critical change in network topology, i.e. the whole network is divided into several subgraphs, the value of S can be used to measure network robustness only when the network is sparse. However, because network efficiency can reflect even a slight variation in network topology, it can be used to measure the robustness of any type of network, sparse or dense.

4. Conclusion and discussion

Small-world networks are known to have some advantages in network efficiency, such as high global and local efficiencies.[3–5] To be an ideal candidate for realistic networks, a small-world network also requires good robustness measured with network efficiency. Although the robustness of small-world networks has been studied extensively in terms of topology, its robustness in terms of network efficiency has not yet been fully investigated. In this study, the improvement in robustness of a small-world WSN is extensively analyzed under three different types of attack. The results show that under all three types of attack an increase in average degree or rewiring probability can monotonically enhance the robustness of the small-world WSN. Furthermore, the combined effect of average degree and rewiring probability on the network robustness is found to be considerable, and several times that of average degree or rewiring probability. Therefore, a small-world WSN with a relatively high average degree and rewiring probability has good robustness. Some realistic networks, such as neural, traffic, and communication networks, have good robustness measured by network efficiency,[9,12,41,42] primarily because they have both relatively high average degree and rewiring probability.

This study proves that increasing the average degree of the network can improve both network efficiency and robustness. For example, fully connected networks with $K = N(N-1)/2$ have the highest efficiency and robustness. However, the network cost is maximum, and it is extremely inefficient. In other words, improving both network efficiency and network robustness by only increasing average degree is not efficient. The intriguing topological structure of small-world networks can considerably enhance network efficiency; however, network robustness reduces significantly. Although the network robustness can be improved by increasing the rewiring probability, the effect is limited. It should also be noted that the small-world characteristics will be gradually lost with increasing rewiring probability. Namely, the rewiring probability of small-world WSN networks cannot be increased unlimitedly. Therefore, it is also not effective to improve both efficiency and robustness by only increasing rewiring probability. The results of this study show that the simultaneous increase of rewiring probability and average degree can significantly enhance the robustness of small-world WSN networks. Furthermore, with this type of construction, the network cost is relatively low and acceptable. On the basis of the above analysis, this study provides an effective method of constructing future networks, including communication, traffic, and social networks, by simultaneously considering efficiency, robustness, and cost.

References

[1] Watts D J and Strogatz S H 1998 *Nature* **393** 440
[2] Barabási A L and Albert R 1999 *Science* **286** 509
[3] Latora V and Marchiori M 2001 *Phys. Rev. Lett.* **87** 198701
[4] Latora V and Marchiori M 2003 *Eur. Phys. J. B* **32** 249
[5] Latora V and Marchiori M 2002 *Physica A* **314** 109
[6] Lago-Fernández L F, Huerta R, Corbacho F and Sigüenza J A 2000 *Phys. Rev. Lett.* **84** 2758
[7] Barahona M and Pecora L M 2002 *Phys. Rev. Lett.* **89** 054101
[8] Liang X et al. 2012 *PLoS One* **7** e32766
[9] Bullmore Ed and Sporns O 2009 *Nat. Rev. Neurosci.* **10** 186
[10] Tian L, Wang J, Yan C and He Y 2011 *NeuroImage* **54** 191
[11] Wagner A and Fell D A 2001 *Proc. R. Soc. Lond. B* **268** 1803
[12] Li S B, Wu J J, Gao Z Y, Lin Y and Fu B B 2011 *Acta Phys. Sin.* **60** 050701 (in Chinese)
[13] Sun K, Mao X M and Ouyang Q 2002 *Chin. Phys.* **11** 1280
[14] Onnela J P, Saramäki J, Hyvönen J, Szabó G, Lazer D, Kaski K, Kertész J and Barabási A L 2007 *Proc. Natl. Acad. Sci.* **104** 7332
[15] Schintler L A, Gorman S P, Reggiani A, Patuelli R, Gillespie A, Nijkamp P and Rutherford J 2005 *Networks and Spatial Economics* **5** 351
[16] Guidoni D L, Mini R A F and Loureiro A A F 2010 *Computer Networks* **54** 1266
[17] Sen P, Dasgupta S, Chatterjee A, Sreeram P A, Mukherjee G and Manna S S 2003 *Phys. Rev. E* **67** 036106
[18] Rubinov M and Sporns O 2010 *NeuroImage* **52** 1059
[19] Stam C J, Jones B F, Nolte G, Breakspear M and Scheltens Ph 2007 *Cerebral Cortex* **17** 92
[20] LiuY, Liang M, Zhou Y, He Y, Hao Y H, Song M, Yu C S, Liu H H, Liu Z N and Jiang T Z 2008 *Brain* **131** 945
[21] Wang L, Zhu C Z, He Y, Zang Y F, Cao Q J, Zhang H, Zhong Q H and Wang Y F 2009 *Hum. Brain Mapp.* **30** 638
[22] Zhuo Z, Cai S M, Fu Z Q and Zhang J 2011 *Phys. Rev. E* **84** 031923
[23] Brust M R, Ribeiro C H C, Turgut D and Rothkugel S 2010 35*th Annual IEEE Conference on Local Computer Networks* 144
[24] Hai Z and Sun X 2008 *IEEE Trans. Knowl. Data Eng.* **20** 1712
[25] Li M, Lee W, Sivasubramaniam A and Zhao J 2008 *IEEE Trans. Paral. Distrib. Sys.* **19** 735
[26] Zhu H, Luo H, Peng H, Li L and Luo Q 2009 *Chaos, Solitons and Fractals* **41** 1828
[27] Kulkarni R V, Förster A and Kumar G 2011 *IEEE Commun. Surv. Tut.* **13** 68
[28] Zhuo Z, Cai S M, Fu Z Q and Wang W X 2011 *New J. Phys.* **13** 053030
[29] Tsonis A A and Roebber P J 2004 *Physica A* **333** 497
[30] Bialonski S, Horstmann M T and Lehnertz K 2010 *Chaos* **20** 013134
[31] Gonges J F, Zou Y and Marwan N 2009 *The European Physical Journal Special Topics* **174** 157
[32] Steinhaeuser K, Ganguly A R and Chawla N V 2012 *Climate Dynamics* **39** 889
[33] Wang X J, Zhi R, He W P and Gong Z Q 2012 *Chin. Phys. B* **21** 029201
[34] Gong Z Q, Wang X J, Zhi R and Feng A X 2011 *Chin. Phys. B* **20** 079201
[35] Wang G L and Anastasios A T 2009 *Chin. Phys. B* **18** 5091
[36] Holme P, Kim B J, Yoon C N and Han S K 2002 *Phys. Rev. E* **65** 056109
[37] Newman M E J and Watts D J 1999 *Phys. Rev. E* **60** 7332
[38] Helmy A 2003 *IEEE Commun. Lett.* **7** 10
[39] Guidoni D L, Mini R A F and Loureiro A A F 2010 *Comput. Networks* **54** 1266
[40] Iturria-Medina Y, Sotero R C, Canales-Rodríguez E J, Alemán-Gómez Y and Melie-García L 2008 *NeuroImage* **40** 1064
[41] Albert R, Jeong H and Barabási A L 2000 *Nature* **406** 387
[42] Verma C K, Tamma B R, Manoj B S and Rao R 2011 *IEEE Commun Lett.* **15** 455