Robustness of scale-free networks under re-wiring operations

S. Xiao[1], G. Xiao[1], T.H. Cheng[1], S. Ma[2], X. Fu[3] and H. Soh[3]

[1] *Division of Communication Engineering, School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798. Email: XiaoShi, egxxiao, ethcheng@ntu.edu.sg*
[2] *Epidemiology and Disease Control Division, Ministry of Health, Singapore 169854. Email: Stefan_MA@moh.gov.sg*
[3] *Institute of High Performance Computing, Agency for Science, Technology and Research (A*STAR), Singapore 138632. Email: fuxj, sohsh@ihpc.a-star.edu.sg*

PACS 89.75.Fb – Structures and organization in complex systems
PACS 89.60.Gg – Impact of natural and man-made disasters
PACS 89.20.Hh – World Wide Web, Internet

Abstract. - Scale-free networks have strong tolerance against random failures yet are fragile under intentional attacks. Existing results show that the network robustness can also be affected by its correlation profile. Specifically, scale-free networks with larger assortativity coefficients generally tend to be more robust against intentional attack. In this letter, we reveal some interesting different observations. By proposing a simple rewiring method which does not change any nodal degree, we show that network robustness can be steadily enhanced at a slightly *decreased* assortativity coefficient. The tolerance against random failures meanwhile remains largely unaffected. Such observations demonstrate the more complicated relationship between network robustness and its assortativity level, as well as some new possibilities of network enhancement and protection.

Introduction. – Many real-life networks display a power-law degree distribution with heavy-tailed statistics, which are called scale-free networks [1, 2]. Extensive research efforts have been made to study the robustness of such networks [3–6]. One of the most important results is that while scale-free networks are strongly tolerant against random failures, they are fragile under *intentional attack* which crashes down networks nodes in a decreasing order of their nodal degrees [3].

The fragileness of the scale-free networks under the intentional attack comes from their heavy-tailed property, causing loss of a large number of links when a hub node is crashed. The heavy loss of network links quickly makes the network to be sparsely connected and then fragmented. A random failure, on the other hand, usually removes a low-degree node. The network connectivity therefore would not be severely impaired.

It has been found that the robustness of the scale-free networks under intentional attack can be affected by several different factors:

Exponent γ. It is proven that the fragileness only exists in scale-free networks with exponents smaller than 3 [5]. However, most of the real-life scale-free networks have their exponents within this range;

Density of connections (measured by the average nodal degree) [7]. Networks having the same exponent may have different densities of connections. Those with higher densities have stronger robustness (and usually higher costs as well);

Assortative mixing [8], which measures the probability that a hub node is connected to another hub node. It is known that most social networks are assortative mixed where hub nodes tend to connect to hub nodes; whereas most communication and biological networks are disassortative where hub nodes tend to connect to low-degree nodes. The most important exception is probably the assortative-mixed model of the Internet on router level [9]. In [8], the assortative coefficient was introduced as

$$\frac{M^{-1}\sum_i j_i k_i - [M^{-1}\sum_i \frac{1}{2}(j_i+k_i)]^2}{M^{-1}\sum_i \frac{1}{2}(j_i^2+k_i^2) - [M^{-1}\sum_i \frac{1}{2}(j_i+k_i)]^2}, \qquad (1)$$

where M is the total number of edges, and j_i and k_i are the degrees of the nodes at each end of the i-th edge. A positive coefficient value reflects an assortative mixed network model, while a negative value reflects a disassortative one. It is shown that for a given nodal-degree distribution, assortative-mixed networks generally speaking are more robust than disassortative ones [8, 10]. Exceptions however do exist. By conducting random link rewiring in a

few real-life networks, it is shown in [10] that with certain values of clustering coefficient, occasionally stronger robustness can be achieved at a lower assortativity level.

In this letter, we focus on revealing the more complicated relationship between network robustness and assortativity. Specifically, we show that by proper link rewiring which does not change any nodal degree, in random uncorrelated networks or random correlated networks (defined in the following section) satisfying some simple conditions stronger network robustness can be steadily achieved at a slightly lower assortativity level. The observations also suggest some new possibilities of network enhancement and protection.

Random networks and their robustness. – A few different random network models have been proposed in literature. The most commonly studied one is the well-known Erdős-Rényi model [11]. Another model which also has been extensively studied is the *generalized random graph* [12,13], which are random in every respect except for the nodal degree distribution. In other words, to define such a network, it only needs to be given the distribution $P(k)$, which denotes the probability that a node has a degree k.

The generalized random graph has been further extended to introduce degree correlation [14]. Specifically, in a directed network, let e_{jk} denote the probability that a directed edge goes from a node with an out-degree j to a node with an in-degree k. Such definition can be extended to an undirected network by simply replacing each undirected edge by two directed ones leading in opposite directions [15]. Note that in some studies, e_{jk} denotes the probability that the *excess* degrees of the two end nodes of a randomly chosen link are j and k, respectively (e.g., [8,15,16]). In this letter, we adopt the former definition.

To differentiate network models generated by generalized random graph and its extended version, we term them as *random uncorrelated* and *random correlated* networks respectively.

It is well known that in random uncorrelated networks where loops of connected nodes can be neglected, they lose their global connectivities when [4]

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} < 2, \tag{2}$$

where $\langle k \rangle$ denotes the average of nodal degrees and $\langle k^2 \rangle$ the average of the squares of nodal degrees. This equation actually also applies to random correlated networks where loops can be neglected. In fact, the derivation of Eq. (2) in [4] does not depends on any non-correlation assumption. As an alternative approach, below we derive Eq. (2) by explicitly including e_{jk} into equations.

In random correlated networks where loops can be ignored, a giant component starts to emerge when a node i connected to a node j in a spanning cluster is also connected to at least one other node. Hence [4]

$$\langle k_i | i \leftrightarrow j \rangle = \sum_{k_i} k_i P(k_i | i \leftrightarrow j) = 2, \tag{3}$$

where k_i denotes the degree of node i and $P(k_i|i \leftrightarrow j)$ the conditional probability that node i has a degree k_i given that it is connected to node j. Same as that in [4], we have

$$P(k_i | i \leftrightarrow j) = P(i \leftrightarrow j | k_i) P(k_i) / P(i \leftrightarrow j), \tag{4}$$

where $P(i \leftrightarrow j)$ denotes the probability that two randomly chosen nodes i and j are connected to each other.

Define $P(i \leftrightarrow j | k_i, k_j)$ as the conditional probability that two nodes i and j are connected given that their nodal degrees are k_i and k_j, respectively. We have

$$P(i \leftrightarrow j | k_i, k_j) = \begin{cases} \frac{k_i \cdot e_{k_i k_j}}{q_{k_i} \cdot N \cdot P(k_j)}, & k_i \neq k_j, \\ \frac{k_i \cdot e_{k_i k_i}}{q_{k_i} \cdot [NP(k_i) - 1]}, & k_i = k_j. \end{cases} \tag{5}$$

Here N denotes the number of nodes in the network, and

$$q_{k_i} = \sum_{k_j} e_{k_i k_j}.$$

Note that $\frac{e_{k_i k_j}}{q_{k_i}}$ denotes the conditional probability that an edge is connected to a degree-k_j node given that it is connected to a degree-k_i node. $\frac{k_i \cdot e_{k_i k_j}}{q_{k_i}}$ therefore calculates the expected number of degree-k_j nodes connected to a degree-k_i node. Based on (5), we have

$$\begin{aligned} P(i \leftrightarrow j | k_i) &= \frac{1}{N-1} \Big[(NP(k_i) - 1) P(i \leftrightarrow j | k_i, k_i) \\ &\quad + \textstyle\sum_{k_j, k_j \neq k_i} NP(k_j) P(i \leftrightarrow j | k_i, k_j) \Big] \\ &= \frac{k_i}{N-1} \Big[\frac{e_{k_i k_i}}{q_{k_i}} + \textstyle\sum_{k_j, k_j \neq k_i} \frac{e_{k_i k_j}}{q_{k_i}} \Big] \\ &= \frac{k_i}{N-1}. \end{aligned} \tag{6}$$

Finally,

$$\begin{aligned} P(i \leftrightarrow j) &= \textstyle\sum_{k_i} P(i \leftrightarrow j | k_i) P(k_i) \\ &= \frac{\sum_{k_i} k_i \cdot P(k_i)}{N-1} \\ &= \frac{\langle k \rangle}{N-1}. \end{aligned} \tag{7}$$

From Eqs. (3), (4), (6) and (7), we shall then have Eq. (2) holds in random correlated networks.

Rewiring method. – Under intentional attack, network nodes with highest degrees in the original network are removed one after another. When there are multiple nodes with the same degree in the original network, one of them is randomly removed. The procedure is repeated until the network is crashed, or in other words, until

$$\kappa \equiv \frac{\langle k^2 \rangle_T}{\langle k \rangle_T} < 2, \tag{8}$$

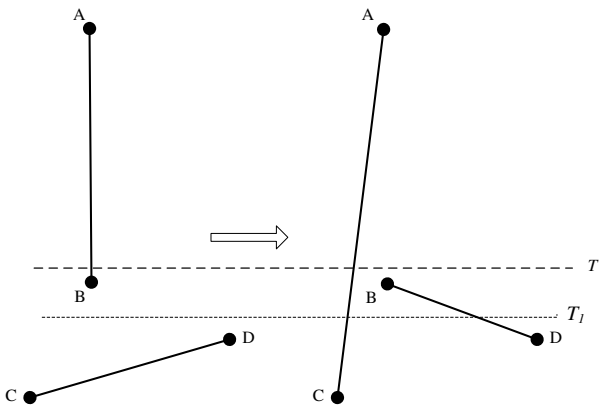

Fig. 1: An illustration of the rewiring operation.

where T denotes the degree of the last removed node in the original degree, $\langle k\rangle_T$ is the average of nodal degrees once the network has been crashed, and $\langle k^2\rangle_T$ the average of the squares of nodal degrees at that time [18]. Hereafter we term such a network just crashed by the intentional attack as a *post-attack network*.

The proposed rewiring method repetitively applies the rewiring operation in the original network as follows:

Divide the nodes with degrees strictly lower than T into two non-overlapping parts, with degrees $\{1, 2, \cdots, T_1\}$ and degrees $\{T_1+1, T_1+2, \cdots, T-1\}$ respectively.

Denote the degree of a certain node i as k_i. Randomly choose two links A-B and C-D which satisfy the condition that

$$k_A > T > k_B > T_1 \geq \max(k_C, k_D). \tag{9}$$

If there are no links A-C and B-D, the rewiring operation replaces links A-B and C-D with links A-C and B-D as long as such does not generate a loop. An example of the rewiring operation is illustrated in Fig. 1.

The rewiring operation obviously does not change any nodal degree. It changes a random network into another one with the same $P(k)$ but different probability distributions $\{e_{jk}\}$. Consider its effects on the average nearest neighbor degree, defined as the average degree of all the neighbors of the nodes with a certain degree k [17]. For nodes with degrees higher than T_1 in the original network, the average nearest neighbor degree is decreased, while for the other nodes, it is increased. In the example case in Fig. 1, it can be observed that the average nearest neighbor degree is decreased for nodes A and B, and increased for nodes C and D.

In this letter, we evaluate the simple case in which nodes A to D are randomly selected as long as their degrees satisfy Eq. (9) and the rewiring does not generate a loop. The optimal rewiring method which achieves the best network robustness without changing any nodal degree remains as an open problem which is out of scope of this letter.

Analysis. – For each node i with a certain degree k_i in the original network, the k_i links attached to it can be categorized into two groups, those connecting to nodes which have been removed when network is crashed, and those connecting to nodes remaining in the post-attack network. Denoting the number of links belonging to these two groups as k_i^+ and k_i^- respectively, we have

$$k_i = k_i^+ + k_i^-. \tag{10}$$

Now we analyze the influence of the rewiring operations. As we can see in Fig. 1, since node A will be removed during attack, the rewiring operations actually replace link C-D with link B-D in the post-attack network. We calculate how the value of $\langle k^2\rangle / \langle k\rangle$ changes in the post-attack network. The value of $\langle k\rangle$ apparently does not change in the post-attack network. As to the value of $\langle k^2\rangle$, it is changed by

$$(k_B^-+1)^2+(k_C^--1)^2-(k_B^-)^2-(k_C^-)^2 = 2(k_B^--k_C^-)+2. \tag{11}$$

In random uncorrelated networks, since $k_B > k_C$, we have that

$$E(k_B^-) > E(k_C^-), \tag{12}$$

where $E(\cdot)$ denotes the expected value of all the nodes involved. In random correlated networks with positive correlation between k_i and k_i^- where $k_i < T$, or in other words,

$$E(k_i^-) > E(k_j^-), \quad \text{where}\, T > k_i > k_j, \tag{13}$$

we shall still have

$$E(k_B^-) > E(k_C^-).$$

In both cases, we have that the expected value of $\langle k^2\rangle / \langle k\rangle$ is increased. With a large enough number of rewiring operations, $\langle k^2\rangle / \langle k\rangle$ may be pushed up to be higher than 2, allowing the emergence of a giant component. Therefore statistically the rewiring operations enhance the network robustness.

We then show that the proposed rewiring method slightly decreases network assortativity coefficient. According to Eq. (1), each rewiring operation changes the value of the network assortativity coefficient by

$$\begin{aligned} &\tfrac{1}{K}\left(k_A \times k_C + k_B \times k_D - (k_A \times k_B + k_C \times k_D)\right) \\ &= \tfrac{1}{K}(k_C - k_B)(k_A - k_D). \end{aligned} \tag{14}$$

where K is a positive constant number. From Eq. (9), $k_A - k_D > 0$, $k_C - k_B < 0$. Therefore, the value of Eq. (14) is negative. The overall network assortativity coefficient is decreased. Such effects can also be observed from the fact that the rewiring operations decrease the average nearest neighbor degrees of high-degree nodes, and increase them for low-degree nodes, as we have pointed out earlier in the section of "Rewiring method".

To summarize, we showed that the proposed rewiring method enhances network robustness in random uncorrelated networks as well as random correlated networks satisfying Eq. (13) while decreasing their assortativity.

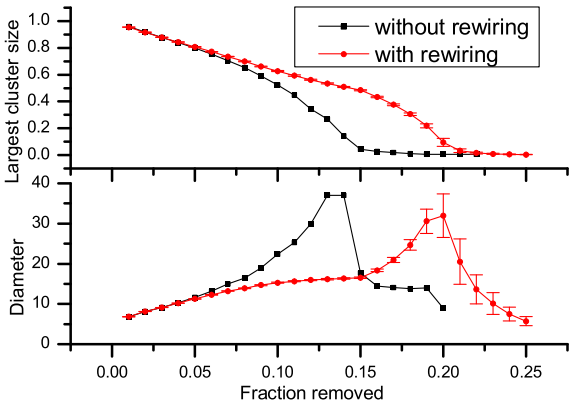

Fig. 2: Simulation results of intentional attack on the random scale-free network where exponent equals to 2.5.

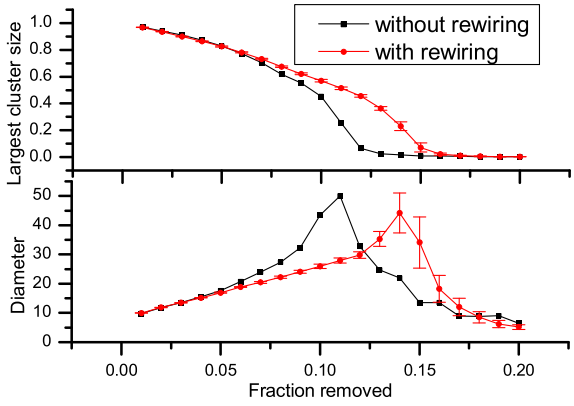

Fig. 3: Simulation results of intentional attack on the random scale-free network where exponent equals to 3.

Simulation results and discussions. – As that in most existing studies [3–7,18–23], we evaluate the robustness of a network by measuring its (i) largest cluster size, defined as the number of nodes in the biggest connected component versus the number of nodes in the original network; and (ii) cluster diameter, i.e., the average length of the shortest paths between all the node pairs in the largest cluster.

We present the simulation results on two random scale-free networks generated by adopting the algorithm proposed in [17], with exponent values of 2.5 and 3, respectively. In both networks, there are 10,000 nodes. The minimum nodal degree is 2 and the cutoff nodal degree is 400. Calculations show that the two networks have assortativity coefficient values of -0.0146 and -0.0062, respectively. This means that both networks are slightly disassortive, which matches what has been discussed in [17]. To carry out rewiring operations, in the former network, $T = 6$ and we set $T_1 = 3$, while in the latter one, $T = 5$ and $T_1 = 3$. We test network robustness when the maximum numbers of 2920 and 1084 rewiring operations have been carried out in the two networks respectively.

The simulation results for the case under intentional attack are reported in Fig. 2 and Fig. 3, in which we show the biggest cluster size and the cluster diameter in the two networks before and after rewiring operations, respectively. For each network, 100 independent realizations have been carried out. The figures show the average values of all the realizations and the error bars. If we regard a network as being crashed once $\langle k^2 \rangle / \langle k \rangle < 2$, the percentage of the network nodes that have to be removed to crash the network (hereafter termed as *threshold* of crash (TOC)) is increased from 15% to 26% in the first network and from 13% to 16% in the second one. Also, we see that most of time during the attack until the network is crashed, the cluster diameter is smaller after rewiring. Note that when networks are attacked to be highly sparsely connected, there is a large range of standard error in network diameter. This is not a surprise: different connection patterns of a small number of relatively high-degree (e.g., degree-4) nodes and a large number of low-degree (mostly degree-1 and degree-2) nodes can make big differences to network diameter.

Fig. 2 and Fig. 3 evidently show that the rewiring method enhances network robustness in scale-free networks with different exponent values. And the enhancements are more significant when more link pairs are rewired.

We then evaluate whether the rewiring operations affect the network tolerance against random failures. Figs. 4-5 show that most of time no major changes are made, except that the cluster diameter may be slightly different.

For the interest of potential applications, we also test a real-life router-level Internet model which contains 192,244 nodes and 609,066 links [24]. Our calculations show that it is indeed an assortative-mixing network with an assortativity coefficient value of 0.02498. In this network, $T = 6$ and we set $T_1 = 3$. A total of 26,017 link pairs can be rewired. Since it is prohibitively time-consuming to carry out 100 realizations on such a large network, only 10 realizations have been conducted and the average results are shown in Fig. 6. It can be seen that though the router-level Internet is not strictly a random network, the rewiring operations nevertheless significantly enhance the network robustness: the TOC value is increased from 27% to 34%.

It is known that recalculated intentional attack which removes the largest-degree node in the *remaining* network is more efficient in crashing down scale-free networks than the one based on nodal degrees in the original network [25]. We carry out numerical simulations for testing the effects of rewiring under such attack. Due to limited space, only the results for the random scale-free network with exponent value of 2.5 are presented in Fig. 7, while the conclusions hold in all the other networks we have simulated. It can be observed that the rewiring method can still significantly enhance network robustness though the TOC values

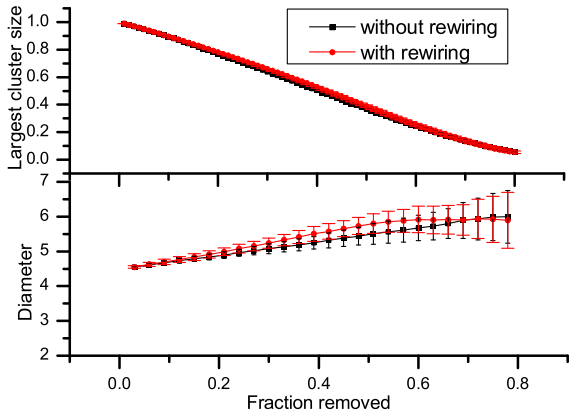

Fig. 4: Simulation results of random failure on the random scale-free network where exponent equals to 2.5.

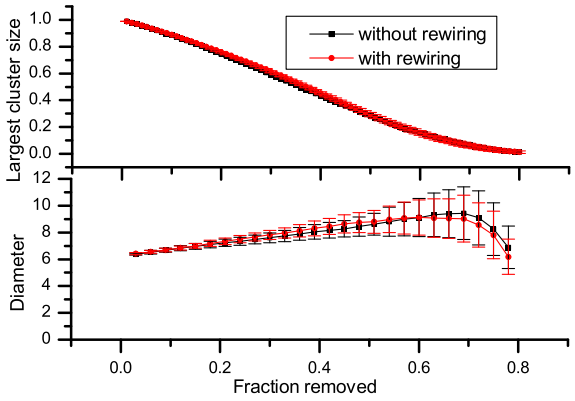

Fig. 5: Simulation results of random failure on the random scale-free network where exponent equals to 3.

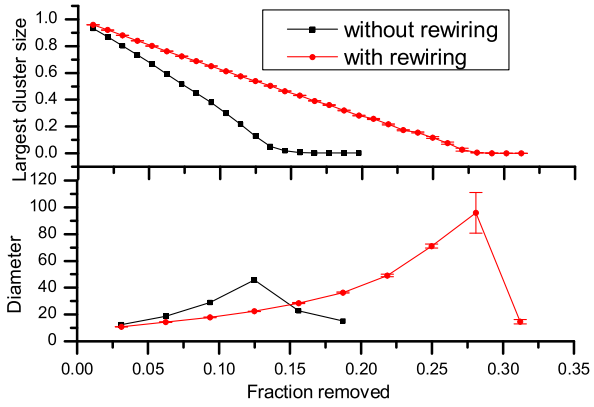

Fig. 6: Simulation results of intentional attack on the router-level Internet model.

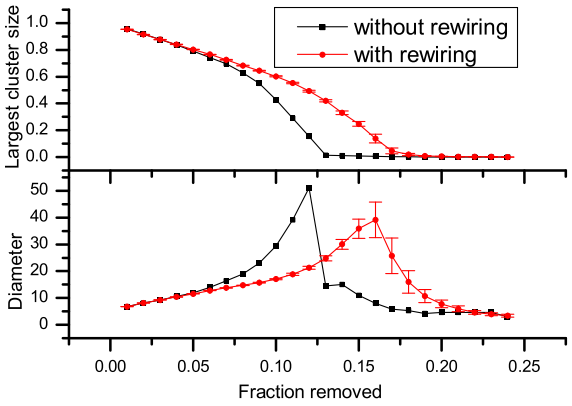

Fig. 7: Simulation results of recalculated intentional attack on the random scale-free network where exponent equals to 2.5.

with or without rewiring both become lower than those under original degree-based intentional attack. Specifically, the TOC value is increased from 13% to 21%. Theoretical analysis on the case of recalculated intentional attack will be carried out in our future research.

Finally, note that assortativity level is indeed decreased by the rewiring operations. According to our calculations, after the rewiring, the assortativity coefficient is slightly decreased from -0.0146 to -0.0268 in the first model, and from -0.0062 to -0.0114 in the second one. In the router-level network model, the coefficient value is decreased from 0.02498 to 0.02406.

Conclusion. – In this letter, we proposed a simple rewiring method which enhances network robustness without changing any nodal degree. Interesting observation is that it slightly decreases network assortativity coefficient. The rewiring method meanwhile does not significantly affect network tolerance against random failure. Such observations reveal the more complicated relationship between network robustness and assortativity level, and some new possibilities of enhancing network robustness by properly interconnecting the low-degree nodes.

The best rewiring method remains as an open problem, which will be of our future research interest.

* * *

This work is supported in part by Singapore A*STAR grant BMRC 06/1/21/19/457.

REFERENCES

[1] Bornholdt S., *Handbook of Graphs and Networks: From the Genome to the Internet*, edited by Schuster H. G. (Wiley-VCH) 2003.

[2] Ben-Naim E. and Frauenfelder H., *Complex Networks*, edited by Toroczkai Z. (SpringerVerlag Berlin Heidelberg) 2004.

[3] Albert R., Jeong H. and Barabási A.-L., *Nature*, **406** (2000) 378.
[4] Cohen R., Erez K., ben-Avraham D. and Havlin S., *Phy. Rev. Lett.*, **85** (2000) 4626.
[5] Cohen R., Erez K., ben-Avraham D. and Havlin S., *Phy. Rev. Lett.*, **86** (2001) 3682.
[6] Paul G., Sreenivasan S. and Stanley H. E., *Phy. Rev. E*, **72** (2005) 056130.
[7] Beygelzimer A., Grinstein G. M., Linsker R. and Rish I., *Physica A*, **357** (2005) 593.
[8] Newman M. E. J., *Phys. Rev. Lett.*, **89** (2002) 208701.
[9] Echenique P., Gómez-Gardeñes J., Moreno Y. and Vázquez A., *Phy. Rev. E*, **71** (2005) 035102.
[10] Holme P. and Zhao J., *Phy. Rev. E*, **75** (2007) 046111.
[11] Erdős P. and Rényi A., *Publ. Math.(Debrecen)*, **6** (1959) 290.
[12] Newman M. E. J., Strogatz S. and Watts D., *Phys. Rev. E*, **64** (2001) 026118.
[13] Molloy M. and Reed B., *Combinatorics Probab. Comput.*, **7** (1998) 295-305.
[14] Callaway D. S., Hopcroft J. E., Kleinberg J. M., Newman M. E. J. and Strogatz S. H., *Phys. Rev. E*, **64** (2001) 041902.
[15] Newman M. E. J., *Phys. Rev. E*, **67** (2003) 026126.
[16] Newman M. E. J., *SIAM Review*, **45** (2003) 167-256.
[17] Catanzaro M., Boguñá M. and Pastor-Satorras R., *Phys. Rev. E*, **71** (2005) 027103.
[18] Valente A. X. C. N., Sarker A. and Stone H. A., *Phy. Rev. Lett.*, **92** (2004) 118702.
[19] Shargel B., Sayama H., Epstein I. R. and Bar-Yam Y., *Phys. Rev. Lett.*, **90** (2003) 068701.
[20] Paul G., Tanizawa T., Havlin S. and Stanley H. E., *Eur. Phys. J. B*, **38** (2004) 187-191.
[21] Rezaei B. A., Sarshar N. and Roychowdhury V. P., *arxiv:cond-mat/0504185*, (2005) .
[22] Xiao S., Xiao G. and Cheng T. H., *IEEE Commun. Mag.*, **46** (2008) 146.
[23] Albert R. and Barabási A.-L., *Rev. of modern physics*, **74** (2002) 47.
[24] *http://www.caida.org/data*, (2003) .
[25] Holme P., Kim B. J., Yoon C. N. and Han S. K., *Phy. Rev. Lett.*, **65** (2002) 056109.