Enhancing network robustness against malicious attacks

An Zeng and Weiping Liu

Phys. Rev. E **85**, 066130 — Published 27 June 2012

DOI: 10.1103/PhysRevE.85.066130

Enhancing network robustness for malicious attacks

An Zeng* and Weiping Liu
Department of Physics, University of Fribourg, Chemin du Musée 3, CH-1700 Fribourg, Switzerland

In a recent work [Proc. Natl. Acad. Sci. USA 108, 3838 (2011)], the authors proposed a simple measure for network robustness under malicious attacks on nodes. With a greedy algorithm, they found the optimal structure with respect to this quantity is an onion structure in which high-degree nodes form a core surrounded by rings of nodes with decreasing degree. However, in real networks the failure can also occur in links such as dysfunctional power cables and blocked airlines. Accordingly, complementary to the node-robustness measurement (R_n), we propose a link-robustness index (R_l). We show that solely enhancing R_n cannot guarantee the improvement of R_l. Moreover, the structure of R_l-optimized network is found to be entirely different from that of onion network. In order to design robust networks resistant to more realistic attack condition, we propose a hybrid greedy algorithm which takes both the R_n and R_l into account. We validate the robustness of our generated networks against malicious attacks mixed with both nodes and links failure. Finally, some economical constraints for swapping the links in real networks are considered and significant improvement in both aspects of robustness are still achieved.

PACS numbers: 89.75.Fb,89.75.Hc,05.10.-a

I. INTRODUCTION

The security of the infrastructure in modern society is of great importance. Systems like Internet, power grids, transportation and fuel distribution networks need to be robust and capable of surviving from random failures or intentional attacks [1]. Many processes taking place on networks might be significantly influenced if the network structures are damaged [2, 3]. Examples of such processes in nature and society include epidemic spreading [4, 5], synchronization [6–8], random walks [9, 10], traffic [11, 12] and opinion formation [13, 14]. Therefore, the robustness for different network structures was intensively studied in the past decade [15–19]. It is also revealed that the shortest path [20] and graph spectrum [21, 22] can be employed to estimate the network robustness. Moreover, interdependent network [23, 24] is proposed to model the catastrophic cascade of failures in real systems.

In a recent work, a new measure for network robustness under malicious attack on nodes is proposed [25]. This measurement, which we call node-robustness in this paper, considers the size of the largest component during all possible malicious attacks, namely $R_n = \frac{1}{N}\sum_{q=1/N}^{1} S(q)$, where N is the number of nodes in the network and $S(q)$ is the relative size of giant component (i.e., the fraction of nodes in the largest connected cluster) after removing qN largest degree nodes. The normalization factor $1/N$ makes robustness of networks with different sizes comparable. A robust network is generally corresponding to a large R_n value. With this measurement, a greedy algorithm is designed to enhance the node-robustness in real systems and large improvement is observed even though a small number of links are modified. Moreover, the optimal structure for node-robustness is found to be an onion structure in which high-degree nodes are highly connected with rings of nodes with decreasing degree surrounding. Lately, a simple method was also proposed to generate such robust onion networks [26].

However, the analysis in ref. [25] is only based on the targeted attacks on nodes. In reality, failures can happen in connections between nodes as well [18]. For example, the power cables can be dysfunctional and some airlines can be blocked due to the terrible weather or terrorist attacks. In this paper, we propose a link-robustness index (R_l) to measure the ability of network to resist link failures. We find that solely enhancing R_n cannot always improve R_l and the network structure for optimal R_l is far different from the onion network. In addition, we find the graph spectrum index [21, 22] only measures the robustness against attack on nodes but cannot reflect link-robustness of networks. In order to design robust networks resistant to different kinds of malicious attacks, we propose a greedy algorithm aiming for both R_n and R_l improvement. To validate the robustness of the resultant networks, we examined them against more realistic attack strategy which combines both nodes and links failure. Since the manipulation of real network always confronts certain economical constraints, we took these requirements into consideration in our method and some significant improvement in both R_l and R_n are still obtained. Finally, our study suggests that robustness improvement strongly depends on the considered attack strategy. Therefore, each real system should have its own optimal structure for robustness according to the attack it receives.

II. LINK-ROBUSTNESS OF NETWORKS

Since a robust network should be able to resist the most destructive attack, we begin our analysis by com-

* an.zeng@unifr.ch

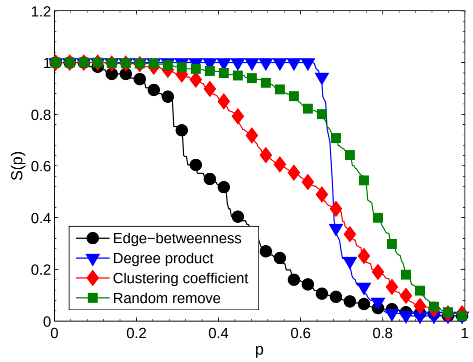

FIG. 1. (Color online) The change of the relative size of the giant component $S(p)$ with the fraction of links p removed by different strategies in BA networks. The BA networks are with $N = 100$ and $\bar{k} = 6$. The results are averaged over 100 independent realizations.

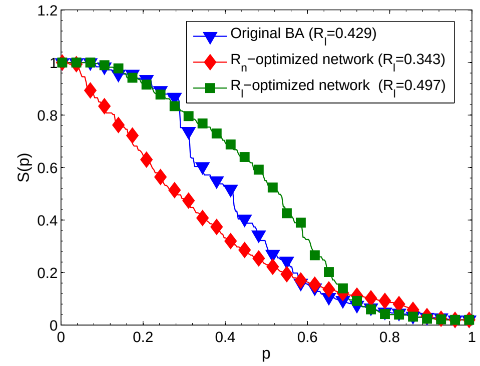

FIG. 2. (Color online) The R_l of BA networks with $N = 100$ and $\bar{k} = 6$, the corresponding R_n-optimized and R_l-optimized networks. The results are averaged over 100 independent realizations.

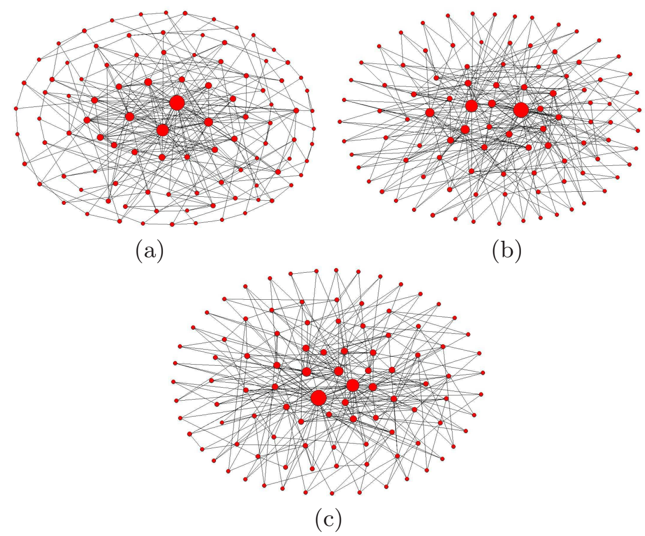

FIG. 3. (Color online) Simple examples of (a) the R_n-optimized network (the onion network), (b) R_l-optimized network (the urchin network) and (c) hybrid-optimized network. The size of the nodes is proportional to their degree. Both networks are obtained by using the corresponding greedy algorithm in a BA model with $N = 100$ and $\bar{k} = 6$.

paring the harmfulness caused by different malicious attack strategies on links. The most destructive attack is supposed to destroy the most "important" links in the networks. Like ref. [25], we monitor the size of giant component to estimate how the network gets destroyed after these "important" links are removed step by step. There are many methods to measure the "importance" of links, here we mainly consider three indexes to identify the most important link to delete. The indexes include edge-betweenness, link clustering coefficient and degree product. The edge-betweenness of a link is the fraction of shortest paths that pass through it [27]. In this strategy, the link with the highest edge-betweenness is removed in each step. The link cluster coefficient is the number of triangles to which a given link belongs, divided by the number of triangles that might potentially include it, given the degrees of the adjacent nodes [28]. In this strategy, the link with the lowest link cluster coefficient is removed in each step. Degree product of a link is simply calculated by multiplying the degree of the nodes on the two ends of the link. In this strategy, the link with the largest degree product is removed in each step. Moreover, we also use the random link removal as a benchmark for comparison. In order to simulate a more harmful strategy, we apply a dynamical approach in which the "importance" of the links (i.e. edge-betweenness, link clustering coefficient and degree product) are recalculated after each link removal during the attack [25].

Fig. 1 reports how the relative size of the giant component $S(p)$ changes with the fraction of links p removed by different strategies in a Barabasi-Albert (BA) network model [29]. Obviously, the most destructive strategy is the one based on the edge-betweenness since $S(p)$ decreases most quickly. Links with high betweeness usually have many shortest paths passing through. Cutting these links will force a large number of nodes to look for other alternative shortest path to communicate with each other. Gradually, the highest edge-betweenness link will be in the only path connecting many nodes. At this time, cutting this link will isolate these nodes. Interestingly, though the degree-based node attack strategy can make a severe damage to the network, cutting the links connecting high degree nodes leads to even less harmful effect than the random removal method to the network connectivity. This is reasonable because the hubs can be strongly connected with each other, and this is well known as the rich-club phenomenon [30].

Based on the analysis above, we will use edge-betweeness as our link removal strategy throughout the paper. Accordingly, we also propose a link-robustness index (R_l) based on the highest edge-betweenness attack

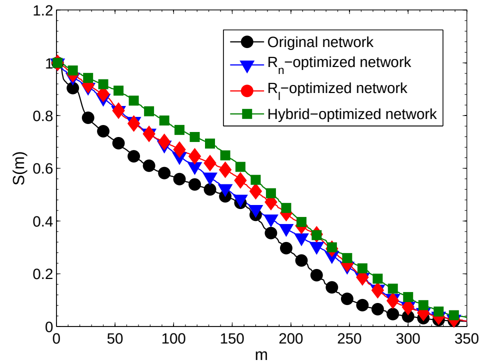

FIG. 4. (Color online) The change of the relative size of giant components S with attack step m when different networks are attacked by the mixed strategy. The original network is USAir and the fraction of node failure f is set as 0.5. The results are averaged over 100 independent realizations.

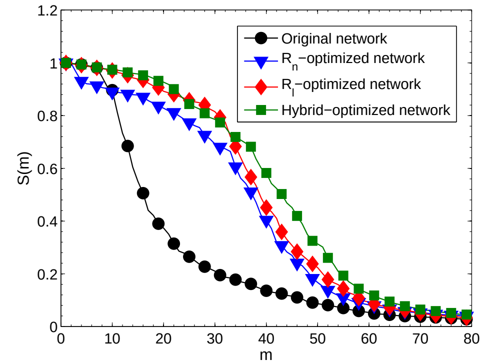

FIG. 5. (Color online) The change of the relative size of giant components S with attack step m when different networks are attacked by the mixed strategy. The original network is Grid and the fraction of node failure f is set as 0.5. The results are averaged over 100 independent realizations.

strategy as

$$R_l = \frac{1}{E}\sum_{p=1/E}^{1} S(p), \tag{1}$$

where E is the total number of links. This measure captures the network response to any fraction of link removal. Apparently, if a network is robust against link attack, its R_l should be relatively large. We remark that similar index has been designed for suppressing the spread of epidemics recently [31].

In ref. [25], it is found that the most robust structure for node attack is the onion-like network which is corresponding to the topology with maximum R_n. However, it is still unclear whether this structure is tolerant to the link attack as well. We therefore report the R_l in BA networks and the corresponding onion networks in Fig.2. Interestingly, despite the onion networks are resistant to malicious node attack, they are weaker than the original BA networks with respect to the intentional link attack. More specifically, the R_l in onion networks is 19.9% lower than the BA model (For detail value, see Table I). One typical onion network is shown in Fig. 3(a). As we can see, nodes with almost the same degree are connected to form a layer and different layers relays on several links to communicate. Since the edge-betweenness of these intra-layer links are relatively high, they will be removed early when the network is attacked on links. Consequently, some isolated layers can be quickly formed, which makes the onion structure sensitive to the link attack.

Therefore, it is necessary to design a structural manipulating method to enhance the link-robustness for networks. Since changing the degree of a node is commonly assumed to be particular more expensive than changing the connections, we keep invariant the degree of each node in our algorithm. Starting from an original network, we swap the connections of two randomly chosen edges, i.e., we randomly select two edges ab and cd (which connect node a with node b, and node c with node d, respectively), then change them to ad and bc only if $R_l^{\rm new} > R_l^{\rm old}$. We then repeat this procedure with another randomly chosen pair of edges until no further substantial improvement is achieved for a given large number of consecutive swapping trials (Here, we set it as 10^4).

Actually, the link swapping greedy algorithm has been commonly applied to achieve the optimal or near-to-optimal network functions such as node-robustness [25], immunization [31], synchronization [32], and so on. In our case, though we cannot guarantee this algorithm will obtain the global optimum, we have checked that the results from this algorithm are relatively stable in different swap trials. Moreover, it yields similar results as that obtained by the simulated annealing algorithm in improving link-robustness.

In Fig. 2, we can clearly see that the R_l can be significantly improved by the algorithm. Compared to the original BA network, R_l can be increased by 15.8% (See Table I for detail value). In Fig. 3(b), we also show the structure of the R_l-optimized network. Different from the "Onion" network obtained in [25], the R_l-optimized network shows roughly the prickles-covered "Urchin" structure in which no obvious community exists and nodes with small degree are not inclined to connect to each other but mainly attach to the nodes with higher degree. In this way, each pair of nodes has many paths to communicate with one another. So that the network can stay connected even many highest edge-betweenness links are removed.

III. IMPROVING ROBUSTNESS IN REAL NETWORKS

In real systems, the failures can actually happen in not only nodes but also links. For example, heavy snow can

TABLE I. Properties in the different networks: Node-robustness index (R_n), Link-robustness index (R_l), the spectrum of the adjacency matrix (λ_1/λ_2), degree assortativity (r), average shortest path length ($\langle d\rangle$) and clustering coefficient ($\langle C\rangle$).

Network	Algorithm	R_n	R_l	λ_1/λ_2	r	$\langle d\rangle$	$\langle C\rangle$
	Original	0.201	0.429	1.856	-0.181	2.576	0.142
BA	R_n-optimized	0.352	0.343	2.579	0.158	2.828	0.117
	R_l-optimized	0.200	0.497	1.891	-0.162	2.584	0.137
	Hybrid-optimized	0.219	0.491	1.898	-0.153	2.583	0.133
	Original	0.110	0.244	2.382	-0.208	2.738	0.625
USAir	R_n-optimized	0.293	0.245	5.054	-0.148	2.875	0.280
	R_l-optimized	0.111	0.319	2.631	-0.315	2.492	0.480
	Hybrid-optimized	0.196	0.298	3.018	-0.237	2.593	0.429
	Original	0.111	0.093	1.122	0.001	6.588	0.123
Grid	R_n-optimized	0.240	0.173	1.404	0.356	6.128	0.015
	R_l-optimized	0.125	0.248	1.192	0.019	4.974	0.024
	Hybrid-optimized	0.161	0.237	1.272	0.110	5.017	0.031

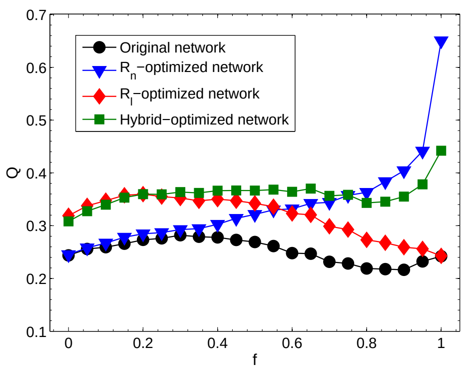

FIG. 6. (Color online) The Q value of different networks when f changes from 0 to 1. The original network is USAir. The results are averaged over 100 independent realizations.

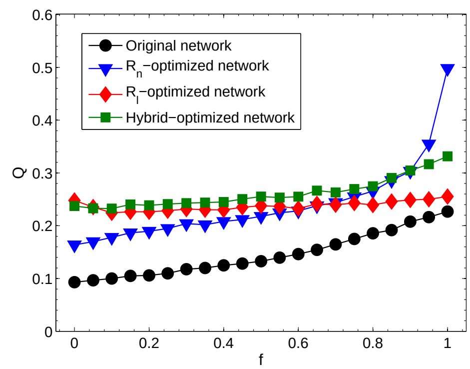

FIG. 7. (Color online) The Q value of different networks when f changes from 0 to 1. The original network is Grid. The results are averaged over 100 independent realizations.

break some power cables and aircraft mechanical problem can block certain airlines. Therefore, when designing the robust networks, we should take both R_n and R_l into account. In order to achieve this objective, we propose a hybrid greedy algorithm to manipulate the network structure for better robustness. Different from the process in the previous section, we swap the connections of two randomly chosen edges only if both R_n and R_l are improved. The swapping process stops if there is no improvement in a certain number of consecutive swapping trials which is set as 10^4 here.

Besides the BA network model, we further consider two real systems: (1) USAir: the network of US air transportation system [33], which contains 332 airports and 2126 airlines. (2) Grid: an electrical power grid in a part of western Europe (mainly Portugal and Spain) [34], with nodes representing generators, and links corresponding to the high-voltage transmission lines between them. This network contains 217 nodes and 320 links. Both real networks are well connected and without any isolated component.

For each network mentioned above, we obtained the corresponding R_n-optimized, R_l-optimized and Hybrid-optimized networks by the greedy algorithms and the related results are given in Table I. As we can see from the BA model and USAir network, optimizing R_n cannot guarantee the improvement of R_l and optimizing R_l cannot always increase R_n neither. However, the hybrid method can improve both R_n and R_l from the original networks. More specifically, the R_n and the R_l are increased respectively by 78.2% and 22.1% in the USAir network. In the Grid network, the improvement of R_n is 46.4% and the increment of R_l can reach even 154.8%. Compared with R_n-optimized and R_l-optimized networks, the hybrid-optimized networks do not have advantage in single aspect of robustness, but they are kept with a reasonable balance between R_n and R_l.

The spectrum of adjacency matrix, namely the ratio of largest and second largest eigenvalues λ_1/λ_2, was formerly used to characterize network robustness [21, 22]. However, we observe that the spectrum index has certain positive correlation with R_n but has no obvious relation to R_l. Therefore, it actually only represents the node-robustness but cannot reflect the network robustness for link attack. The topology properties of the resultant networks are also analyzed. The result in Table I shows that the hybrid-optimized networks usually have larger assortativity, smaller average shortest path length and lower cluster coefficient than the original networks. It has been revealed that the optimal structure for R_n is the onion structure in which nodes with almost the same degree are connected, so the most significant feature for R_n-optimized network is the large assortativity. For the aspect of R_l, the most destructive attack strategy is based on the highest load (edge-betweenness), so the less significant the community structure is, the higher R_l will be. Consequently, the robust network against to the link attack should be with small average shortest path length and small cluster coefficient. Unlike the onion networks, the R_l-optimized networks usually do not have a large assortativity, which explains why the onion networks do not have a high R_l. For the resultant networks from the hybrid algorithm, they will finally carry these topology properties from both R_n-optimized and R_l-optimized networks. One example of the hybrid-optimized network is shown in Fig. 3(c). The structure is between the "Onion" network and "Unchin" network. Although the hybrid-optimized network looks like an "Unchin" network, it still has some links connecting the nodes with small degree.

Since the attacks in nodes and links can happen simultaneously, one interesting aspect to consider is to see how the networks in Table I react to the attack combining node failures and link failures. Accordingly, we design a mixed attack strategy in which the largest degree nodes will be removed with probability f and the links with highest edge-betweenness will be cut with probability $1-f$. The procedure goes on until the size of the giant component reaches 0. We first set $f = 0.5$ as an example and report in Fig. 4 and 5 the performance of the networks in Table I. The results show that the hybrid-optimized networks preserve the giant component most effectively.

We then consider the mixed attack process with f varying from 0 to 1. When $f = 0$, the process is just pure highest load (edge-betweenness) attack on links. When $f = 1$, it returns to the largest degree attack on nodes. Here, we are mainly interested in the situation where $0 < f < 1$. In order to estimate in which range of f the hybrid-optimized network has advantage, we generalize the definition of robustness to a quantity Q in the mixed attack process,

$$Q = \frac{1}{M}\sum_{m=1}^{M} S(m), \tag{2}$$

where M is the total number of steps to reduce the size of giant component to 0. Q measures how tolerant a network against the malicious attack (which can be nodes attack, link attack or mixed). According to Eq. (2), $Q = R_l$ when the $f = 0$ and $Q = R_n$ when $f = 1$.

The Q value of the networks in Table I under different f are reported in Fig. 6 and 7. Obviously, the original networks performs worst under any f. The R_n-optimized networks can indeed improve the Q value when f is large. However, they do not have too much advantage when f is small. More specifically, in the USAir network (see Fig. 6), the R_n-optimized network has almost the same Q when f is smaller than 0.4. The R_l-optimized network can significant improve the Q value when f is small, but Q drops nearly back to the original network level when f is large. The similar trend can be observed also in the Grid network (Fig. 7). These phenomena indicate that the R_n-optimized network is very sensitive to link attack while the R_l-optimized network is fragile when attacked by nodes. The hybrid-optimized networks, however, perform very stable under different attack situations (i.e., different f), which suggests that the hybrid-optimized network is a much more reliable structure in reality, especially when the fraction of node and link failure is unknown. In addition, compared to the R_n-optimized and R_l-optimized networks, the hybrid-optimized network can even enjoy a higher Q value in certain range of f ($0.2 \le f \le 0.75$ in the USAir network and $0.1 \le f \le 0.9$ in the Grid network). In other words, when the network is attacked by both links and nodes, the hybrid-optimized network seems to be the most robust structure.

Finally, we consider some economical constraint on improving the robustness in the real system. First of all, the total length (geographically calculated) of links cannot be exceedingly large. Secondly, the number of changes of links should be relatively small. Therefore, for reconstructing the real networks like USAir and Grid, we add two more constraints to the greedy algorithm: the swap of two links is only accepted if the total geographic length of edges does not increase, and both R_n and R_l are increased more than certain values (denoted as ΔR_n and ΔR_l) [35]. With the strong constraints, R_n and R_l of real networks can still be significantly improved. Specifically, with only 3.9% links changed, the R_n and R_l of the USAir network can be respectively increased by 56% and 17% (R_n: from 0.110 to 0.172. R_l: from 0.244 to 0.285). In the Grid network, the R_n can be improved by 23% (from 0.111 to 0.136) and the R_l can be improved by 20% (from 0.093 to 0.112) with only 6.9% links changed.

IV. CONCLUSION

How to enhance the robustness of networks is an important topic, which is related to protecting the real system from random failures and malicious attacks. In the former literatures, most of the works focused on proposing methods to improve the network robustness for the attack on nodes. However, the connections between nodes can be also damaged due to some unexpected accidents, which requires us to take the link failure into account when designing robust networks. In this paper, based on the highest load attack strategy, we propose the link-robustness index to estimate how the network can resist to the most destructive targeted attack on links. Moreover, we designed a hybrid greedy algorithm to enhance both node-robustness and link-robustness. When attacked by the strategy combining node and link failure, the resultant networks from the hybrid method outperform the networks from solely improving either R_n or R_l. Finally, some economical constraints are considered when enhancing the robustness of real networks and some significant improvement are observed.

As shown in our results, different attack strategies require different optimal network structures to be tolerant to the damage. From the practical point of view, the hybrid method can create a reliable network which is generally robust to the attack mixed with node failures and link failures. In reality, the probability of the node failure and link failure can hardly be known especially when the systems receive malicious attacks. Since the hybrid-optimized networks perform very stable under different attack situations, they can be the most suitable structures when designing real systems. Finally, we remark that many possible extensions of this work can be done in the future. For example, there is a family of problems where the goal is to minimize the robustness to design effective immunization strategy [31, 36] and the hybrid immunization on both links and nodes can be considered in this case. Moreover, link failure should be also taken into consideration when studying the interdependent networks and the idea of hybrid-optimized method can be extended to design a robust structure for interdependent systems.

ACKNOWLEDGEMENT

We would like to thank Yi-Cheng Zhang, Ciulio Cimini, Chi Ho Yeung and Xiao-Pu Han for helpful suggestions. This work is supported by the Swiss National Science Foundation (No. 200020-132253).

[1] R. Albert, H. Jeong, A.-L. Barabasi, Nature **406**, 378 (2000).
[2] R. Guimera and M. Sales-Pardo, Proc. Natl. Acad. Sci. USA **106**, 22073 (2009).
[3] A. Zeng and G. Cimini, Phys. Rev. E **85**, 036101 (2012).
[4] R. Pastor-Satorras and A. Vespignani, Phys. Rev. Lett. **86**, 3200 (2001).
[5] M. Kitsak, L. K. Gallos, S. Havlin, F. Liljeros, L. Muchnik, H. E. Stanley and H. A. Makse, Nature Phys. **6**, 888 (2010).
[6] A. Arenas, A. Diaz-Guilera, J. Kurths, Y. Moreno, and C.-S. Zhou, Phys. Rep. **469**, 93 (2008).
[7] A. Zeng, S.-W. Son, C. H. Yeung, Y. Fan and Z. Di, Phys. Rev. E **83**, 045101(R) (2011).
[8] A. Zeng, Y. Hu and Z. Di, Europhys. Lett. **87**, 48002 (2009).
[9] J. D. Noh and H. Rieger, Phys. Rev. Lett. **92**, 118701 (2004).
[10] M. Rosvall and C. T. Bergstrom, Proc. Natl. Acad. Sci. U.S.A. **105**, 1118 (2008).
[11] G. Li, S. D. S. Reis, A. A. Moreira, S. Havlin, H. E. Stanley and J. S. Andrade, Jr., Phys. Rev. Lett. **104**, 018701 (2010).
[12] H. Yang, Y. Nie, A. Zeng, Y. Fan, Y. Hu and Z. Di, Europhys. Lett. **89**, 58002 (2010).
[13] M. Bartolozzi, D. B. Leinweber and A. W. Thomas, Phys. Rev. E **72**, 046113 (2005).
[14] C. Castellano, S. Fortunato and V. Loreto, Rev. Mod. Phys. **81**, 591 (2009).
[15] D. S. Callaway, M. E. J. Newman, S. H. Strogatz and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).
[16] R. Cohen, K. Erez, D. ben-Avraham and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).
[17] B. Shargel, H. Sayama, I. R. Epstein and Y. Bar-Yam, Phys. Rev. Lett. **90**, 068701 (2003).
[18] E. Estrada, Eur. Phys. J. B **52**, 563 (2006).
[19] A. A. Moreira, J. S. Andrade Jr., H. J. Herrmann and J. O. Indekeu, Phys. Rev. Lett. **102**, 018701 (2009).
[20] V. Latora and M. Marchiori, Phys. Rev. Lett. **87**, 198701 (2005).
[21] M. Fiedler, Czech Math. J. **23**, 298 (1973).
[22] S. Hoory, N. Linial, and A. Wigderson, Bull. New Ser. Am. Math. Soc.43, 439 (2006).
[23] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley and S. Havlin, Nature **464**, 1025 (2010).
[24] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, Phys. Rev. E **83**, 065101(R) (2011).
[25] C. M. Schneider, A. A. Moreira, J. S. Andrade, Jr., S. Havlin and H. J. Herrmann, Proc. Natl. Acad. Sci. U.S.A. **108**, 3838 (2011).
[26] Z.-X. Wu and P. Holme, Phys. Rev. E **84**, 026106 (2011).
[27] M. Girvan and M. E. J. Newman, Proc. Natl. Acad. Sci. USA **99**, 7821 (2002).
[28] F. Radicchi, C. Castellano, F. Cecconi, V. Loreto, D. Parisi, Proc. Natl. Acad. Sci. **101**, 2658 (2004).
[29] A.-L. Barabasi and R. Albert, Science **286**, 509 (1999).
[30] V. Colizza, A. Flammini, M. A. Serrano and A. Vespignani, Nature Phys. **2**, 110 (2006).
[31] C. M. Schneider, T. Mihaljev, S. Havlin and H. J. Herrmann, Phys. Rev. E **84**, 061911 (2011).
[32] M. Brede, Eur. Phys. J. B **74**, 217 (2010).
[33] V. Batageli and A. Mrvar, Pajek Datasets, available at http://vlado.fmf.uni-lj.si/pub/networks/data/default.htm
[34] Q. Zhou, J. W. Bialek, IEEE T. Power Syst. **20**, 782 (2005).

[35] In the USAir network, $\Delta R_n = 5{\cdot}10^{-4}$ and $\Delta R_l = 5{\cdot}10^{-4}$. In Grid network, $\Delta R_n = 10^{-3}$ and $\Delta R_l = 5 \cdot 10^{-4}$
[36] C. M. Schneider, T. Mihaljev, H. J. Herrmann, arxiv:1112.2957 (2011).