Physica A 391 (2012) 4420–4425

Contents lists available at SciVerse ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Robustness analysis of network controllability

Cun-Lai Pu [a,b,c,*], Wen-Jiang Pei [b], Andrew Michaelson [d]

[a] School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, People's Republic of China
[b] School of Information Science and Engineering, Southeast University, Nanjing 210096, People's Republic of China
[c] Center for Complex Network Research, Department of Physics, Northeastern University, Boston, MA 02115, USA
[d] Department of Bioengineering, Northeastern University, Boston, MA 02115, USA

ARTICLE INFO

Article history:
Received 1 September 2011
Received in revised form 7 April 2012
Available online 24 April 2012

Keywords:
Network controllability
Robustness
Cascade failure

ABSTRACT

Structural controllability, which is an interesting property of complex networks, attracts many researchers from various fields. The maximum matching algorithm was recently applied to explore the minimum number of driver nodes, where control signals are injected, for controlling the whole network. Here we study the controllability of directed Erdös–Rényi and scale-free networks under attacks and cascading failures. Results show that degree-based attacks are more efficient than random attacks on network structural controllability. Cascade failures also do great harm to network controllability even if they are triggered by a local node failure.

1. Introduction

Complex networks, composed of interacting individual nodes abstracted from natural or technological systems, have received great attention from scientific communities in past decades [1–5]. Advances have focused on network topological characteristics and network dynamics [6–15]. However, the ultimate goal for studying complex networks is not only to explore underlying principles of complex systems, but also to learn how to control them more efficiently [16–30]. It is difficult to control a complex system due to the unknown architecture of the system and the complex dynamics rules that govern the time-dependent interactions between the components. Recent advances in structures of complex networks stimulate the research in efficient control of large complex systems. Yang et al. [18] found in the contact process dynamics spreading can be maximized when the contact probability is chosen to be inversely proportional to the node degree. Zhang et al. [19] obtained the transmission efficiency of scale-free networks can be dramatically enhanced by kicking out the edges linking to nodes with large betweenness. Wang and Chen [20] demonstrate that, in scale-free networks it is more efficient to choose the large-degree nodes rather than the small-degree nodes as controllers in order to achieve a desired stabilization of the network. Li et al. [21] developed a virtual control strategy in which the pinned nodes virtually control other dynamical nodes with links between them, and found that after the pinned nodes were stabilized, the whole network is virtually broken into parts. It is more important to study the control of a system in the absence of key nodes and links. Motter [22] obtained that a selective further removal of nodes, right after the initial attack or failure, can prevent the cascading failures from propagating through the entire network. Motter et al. [23] showed that in metabolic networks of single-cell organisms, some mutants that are unable to grow due to perturbations caused by genetic or epigenetic defects can be turned into viable organisms through additional gene deletions. Sahasrabudhe and Motter [24] found that the consequence of the extinction

[*] Corresponding author at: School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, People's Republic of China.
E-mail addresses: pucunlai@gmail.com, pucunlai@yahoo.cn (C.-L. Pu).

0378-4371/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.physa.2012.04.019

of one species can often be compensated by the concurrent removal or population suppression of other specific species in complex food webs. Moreover, Cornelius et al. [25] obtained that compensatory perturbations are effective even when they are limited to a small percentage of all nodes in the network and that they are much more effective when limited to the largest-degree nodes.

Structural controllability defined and studied by Lin [26] shows some connections between control theory and graphs. Liu et al. [16] applied the theory of structural controllability to a large number of large networks structures by assuming the nodes have no dynamics. Liu et al. [16] also developed analytical tools to explore the minimum number of driver nodes, in which control signals are injected to control the whole network. They found that the number of driver nodes needed for control of a network mainly depends on the degree distribution of the network. Also sparse inhomogeneous networks are the most difficult to control.

Previous work [31,32] has indicated that scale-free networks, which describe numerous infrastructural networks, do not typically break into pieces by random node failures, which is an extreme robustness rooted in the inhomogeneous network topology. However, scale-free networks are vulnerable to attacks, and even the absence of a tiny fraction of the most connected nodes will break the network into pieces. In general, an attack or failure will have more devastating consequences when the dynamics of flow in the network is properly accounted for, leading to the emergence of cascading failures [27,22]. The removal of nodes, either by random breakdown or intentional attacks, leads to a global redistribution of loads over the entire network. This redistribution may increase the load on particular nodes and links beyond their capacity, triggering a cascade of overload failures.

Based on the advances in network controllability and network robustness, we are dedicated to investigating the robustness of network controllability, which could be taken as a new property of complex networks, in function of the magnitude and mode of the attack, including random failures, target failures, and cascading failures. Strategies to compensate for the perturbations of the networks as in Ref. [22] are not the focus in this paper.

2. Controllability of networks

According to the control theory, a system is controllable if it can be driven from any initial state to any desired final state by probable variable inputs [28]. Here we consider linear systems and assume that individuals in the systems have no intrinsic dynamics. Then the linear control systems are described by the following state equation as Ref. [28]:

$$\dot{\mathbf{x}}(t) = A\mathbf{x}(t) + B\mathbf{u}(t) \tag{1}$$

where $\mathbf{x}(t) = \{x_1(t), x_2(t), \dots, x_N(t)\}^T$, which is the state of a system of N nodes at time t. A is the $N \times N$ adjacency matrix of the network representing the system. In this matrix, elements are the interaction strengths between individual nodes. B is the $N \times M$ input matrix, which identifies the nodes where the input signals are imposed. The input signal vector $\mathbf{u}(t) = \{u_1(t), u_2(t), \dots, u_M(t)\}^T$ is a time-dependent input signal vector. The state of each node at each time step is controlled by the linear combination of the elements of the input vector. The system defined by Eq. (1) is controllable, which is possible if and only if the $N \times NM$ controllability matrix:

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

has full rank, which is $\mathrm{rank}(C) = N$. This controllability rank condition is given by Kalman et al. [29] and Kalman [30]. The mathematical condition for system controllability indicates that, to fully control the network, we need to choose the right B and $\mathbf{u}(t)$ (the right number of signals and right nodes where the signals are imposed) so that $\mathrm{rank}(C) = N$. The critical and interesting question is how do we find out the minimum number $M(M < N)$ of different signals that offer full control over the network? However, Kalman's theory is only feasible for small networks, while for large real networks, it is very hard to compute the rank of C, since C is a incredibly large matrix. Fortunately, Liu et al. [16] proved that the minimum number of nodes (known as driver nodes in their paper), where the control signals are injected to control the whole network, can be found out in the 'maximum matching' of the network. In graph theory, the maximum matching of a directed network is the maximum set of links that do not share start or end nodes, and a node is matched if it is the end of a directed link in the maximum matching set, otherwise the node is unmatched. There might be many different maximum matchings of a directed network, but the numbers of unmatched nodes in every maximum matching are the same. We can bring a system to a certain state by just imposing control signals on the unmatched nodes or driver nodes in any one of the maximum matchings of the corresponding network. Therefore, by using the maximum matching algorithm we find out all the driver nodes in a directed network. Fig. 1 is an example of the maximum matching of a small directed network.

3. Network controllability under vulnerability

Here we investigate the behavior of network controllability under two different kinds of attacks: single-node attack and cascading failure. For simplicity's sake, we assume that when a node is attacked, its edges are removed from the network, but the node itself is still in the network, so the size of the network is unchanged after attacks. Here we study network controllability based on two kinds of networks: directed Erdös–Rényi (DER) [33] and directed scale-free (DSF) [34] networks. Usually, the network controllability is supposed to decrease after attacks, which is reflected in the increase of number of

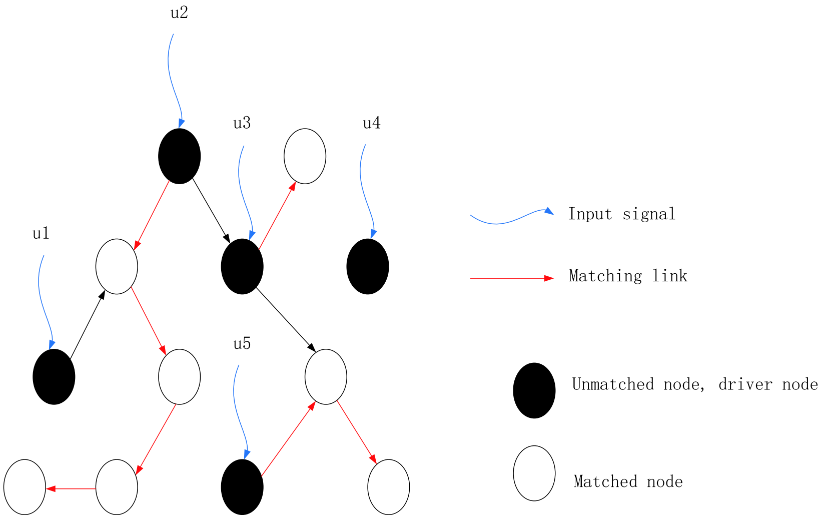

Fig. 1. A small example of maximum matching and network control. The driver nodes are found out by maximum matching.

driver nodes needed for controlling the network. Therefore, we measure the number of driver nodes n_D at each time step during the attacks and the increment of driver nodes Δn_D after attacks. We did not consider methods of defense against the attacks presented here. However, as shown in Ref. [22], defense strategies are very important and need further research.

3.1. Single-node attack

In this part, we study robustness of network controllability under random attacks, as well as degree-based attacks. In random attacks, at each time step we randomly attack a node, and then calculate the number of driver nodes. In degree-based attacks, at each time step we attack the node with the largest degree, and then calculate the number of driver nodes. Fig. 2 shows the results for number of driver nodes n_D with an increase of time step T during the attack processes. We see generally n_D increases with T, which means we need ever increasing control signals for controlling the whole network with the continuing attacks. This is to say the network controllability is decreasing after attacks. Degree-based attacks are more efficient in attacking the network controllability rather than random attacks both in the DER and DSF networks. With the increase of time step, the efficiency of the two kinds of single-node attacks goes further, and finally the degree-based attacks take less time to destroy the total controllability of the network than the random attacks. The reason is the degree-based attacks have more edges removed from the network at each time step, which indicates that most likely more matched links are removed in the degree-based attacks at each time step, compared to that of the random attacks. As a result, the network controllability decreases faster which reflects in the need for more control signals or driver nodes to control the network. Moreover, we obtain from Fig. 2 that the DER networks are more robust than the DSF networks in aspects of network controllability, which confirms the results in Ref. [16], where it is shown that the DER network is much easier to control since it needs a small number of driver nodes compared to other networks.

3.2. Cascading failure attack

Due to the complex topology of the network, breakdown on a global scale can be triggered by local failures through the cascading mechanism. We focus on cascades triggered by the removal of the node with the largest load [35,36] in the network. The load $B_i(t)$ on node i at time t is the total number of the shortest paths passing through i at time t. Each node is characterized by a capacity defined as the maximum load that node can handle. We assume the capacity C_i of node i to be proportional to its initial load $B_i(0)$ [27]:

$$C_i = cB_i(0), \quad i = 1, 2, \ldots, N \tag{3}$$

where $c(\geq 1)$ is the tolerance parameter of the network. The removal of the node with the largest load changes the distribution of shortest paths, and thus the load distribution. Load on some nodes may increase and become larger than their capacity. When this situation occurs, the overloaded nodes fail and all their edges are removed from the network. The failures of these overloaded nodes result in a new distribution of load on nodes. Again some nodes may fail in the network. The cascading failures continue until there are no overloaded nodes in the network. The cascading failures may stop after a few time steps, but they may also propagate and shutdown a considerable fraction of the network. We show the results of cascading failure attacks on network controllability for each time step in Fig. 3. At the first step n_D increases slightly, then from steps 2 to 5, n_D increases abruptly, after step 6 n_D increases very slightly until step 9 when the cascading failure

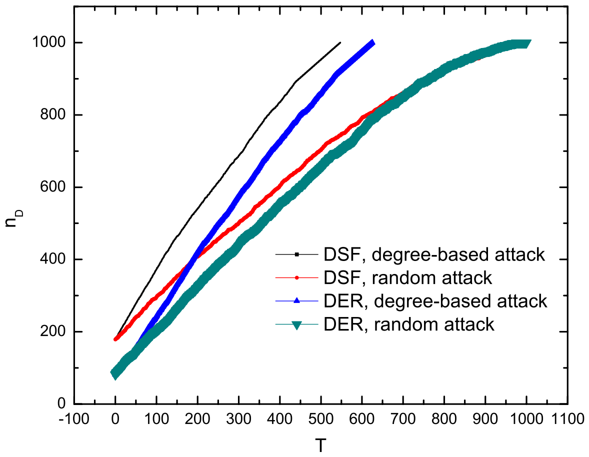

Fig. 2. Number of driver nodes n_D vs. time step T in single-node attacks. In the original network before attacks, the number of nodes is $N = 1000$, and the average node degree is $\langle k \rangle = 6$. The power law parameter is $\gamma_{in} = \gamma_{out} = 3$ in the DSF networks. Each data point is the average of 50 independent runs.

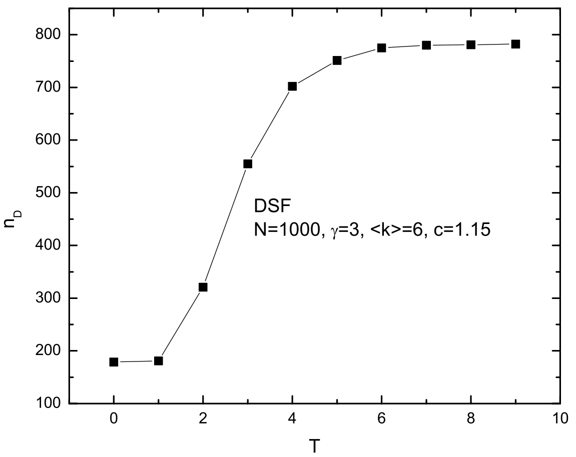

Fig. 3. Number of driver nodes n_D at each time step T in the cascading failure process. Each data point is the average of 10 independent runs.

process ends. n_D then increases 4 times after the cascading failure attack. This indicates the controllability of the network is reduced to 25% after the cascading failure attack. Fig. 3 is an example which shows the whole process of the cascading failure attack on network controllability. The degree of influence of cascading failure attacks on network controllability strongly dependents on the network topology and the tolerance parameter c.

Then we measure the addition of driver nodes Δn_D before and after the cascading failure attacks for the DSF and DER networks. In Fig. 4(a) and (b), Δn_D decreases significantly with the increase of c at first, and then it tends to stabilize. When c is very small, Δn_D is relatively large, and this means cascading failures damage the network connectivity and controllability greatly. When c is large enough ($c > 2$ in Fig. 4(a) and (b)), the network controllability is not affected at all, since the cascading failure is not likely to happen in this case. Moreover, we see from Fig. 4(a) that, the bigger γ, the larger Δn_D when c is small enough, but the smaller Δn_D in the wide range of c. When c is miniscule, the cascading failure damages the connectivity of the network significantly, no matter what γ is. Since n_D is relatively small in homogeneous networks, Δn_D is relatively larger after the cascading failure attacks. However, when c is large enough, the cascading failure just damages parts of the network, which is even less in homogeneous networks. In other words, network homogeneity contributes to the robustness of network controllability against cascading failures in the wide range of c. From Fig. 4(b) we see, when c is small enough, the cascading failure damages the network controllability significantly. Since n_D is relatively small in networks with more links, n_D increases more after the cascading failure attack. However, in the wide range of c, more links are better for the network controllability against cascading failures. Fig. 4(c) are the results for the DER networks which have the same conclusion as Fig. 4(b).

From Fig. 5, we see Δn_D increases with $\langle k \rangle$ at first, then decreases with $\langle k \rangle$ both in the DSF networks and DER networks. The reason for this is that when $\langle k \rangle$ is small, the connectivity of the network is relatively sparse, and the cascading failure is unlikely to occur, or just happens in a small part of the network. As a result, the damage of the network controllability is not obvious. When $\langle k \rangle$ is large, the network has more links, which means the network is more robust to cascading failures.

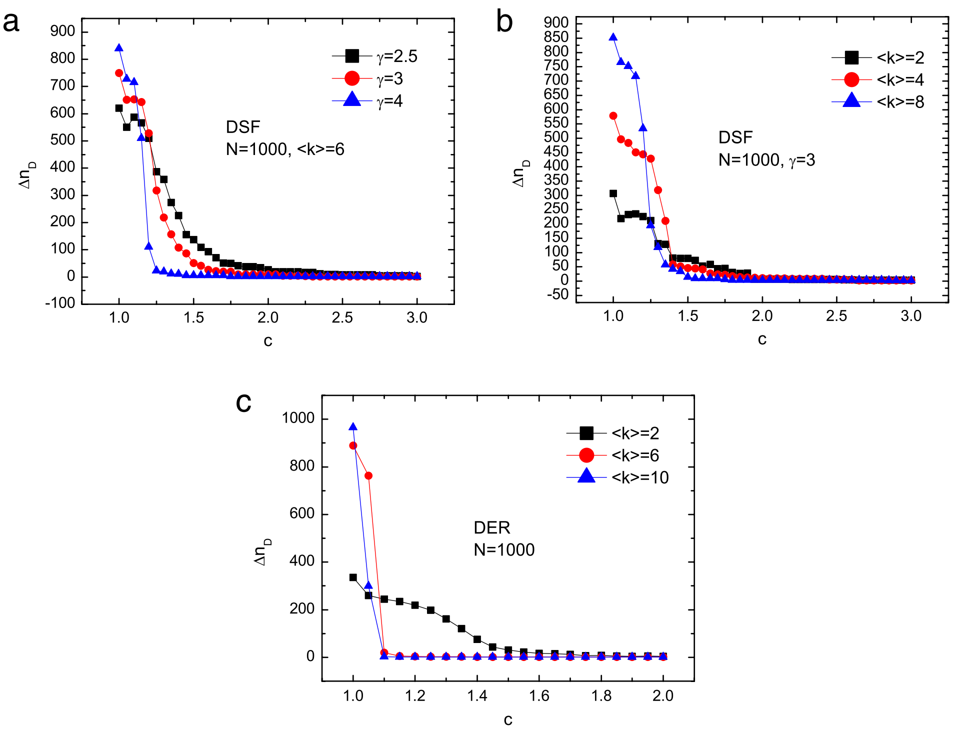

Fig. 4. Addition of driver nodes Δn_D vs. network parameter c, (a) different γ for DSF networks, (b) different average node degree $\langle k \rangle$ for DSF networks, and (c) different average node degree $\langle k \rangle$ for DER networks. Each data point is the average of 10 independent runs.

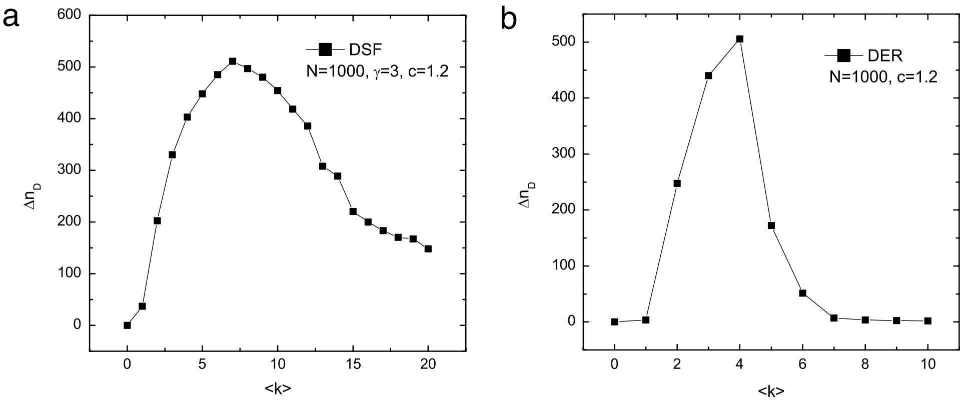

Fig. 5. Addition of driver nodes Δn_D vs. average degree $\langle k \rangle$ on (a) DSF networks and (b) DER networks. Every data points is averaged over 10 independent runs.

Therefore, the damage of the cascading failure attack to the network controllability is not very significant. However, between these two situations, there is a peak where the damage of the cascading failure attacks are significant. We also simulate the cascading failure attacks on network controllability of the power grid [15], as shown in Fig. 6. We see the damage of the network controllability decreases with an increase of the network parameter c. There is some fluctuation in the curve due to the specific topology structure of the power grid.

4. Conclusion

In summary we study the behavior of network controllability under vulnerability for networks of different topologies. We find that degree-based attack is more efficient than random attack on network controllability for both the DER and DSF networks. The damage to network controllability by cascading failure attacks strongly depends on the network's tolerance parameter. Generally, more links as well as network homogeneity is beneficial for the robustness of network controllability

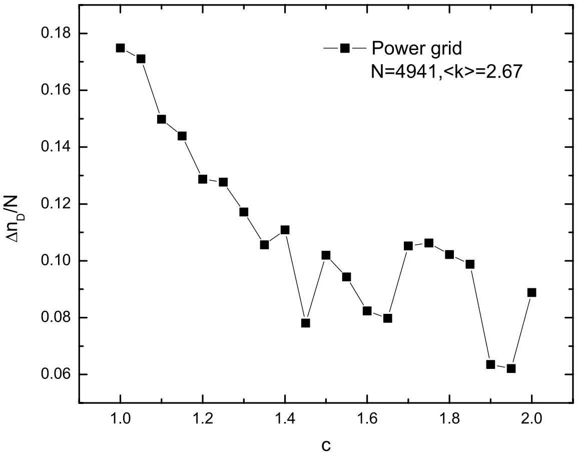

Fig. 6. Damage of the controllability $\frac{\Delta n_D}{N}$ vs. network parameter c. The underlying network is the Northwestern US power grid with network size $N = 4941$, and average node degree $\langle k \rangle = 2.67$.

against cascading failure attacks. We also test the robustness of controllability of the power grids. In the future, we will further study network controllability, and develop novel methods to improve the robustness of network controllability.

Acknowledgments

The authors thank Prof. Albert-Lázló Barabási, Dr. Chao-Ming Song, Dr. Yang Liu and all the reviewers for their valuable comments and suggestions. This work was supported by the Natural Science Foundation of China under Grant No. 60672095, No. 60972165, the National High-Technology Project of China under Grant No. 2007AA11Z210, the Doctoral Fund of Ministry of Education of China under Grant No. 20070286004, the Foundation of High-Technology Project in Jiangsu Province, the Natural Science Foundation of Jiangsu Province under Grant No. BK2008281, the Special Scientific Foundation for the Eleventh-Five-Year Plan of China, the National torch plan, and the Excellent Young Teachers Program of Southeast University.

References

[1] A.L. Barabási, Science 325 (2009) 412.
[2] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.U. Hwang, Phys. Rep. 424 (2006) 175.
[3] R. Albert, A.L. Barabsi, Rev. Modern Phys. 74 (2002) 47.
[4] M. Newman, Phys. Today (2008) 33.
[5] S.N. Dorogovtsev, A.V. Goltsev, J.F.F. Mendes, Rev. Modern Phys. 80 (2008) 1275.
[6] C.M. Song, S. Havlin, H.A. Makse, Nature 433 (2005) 392.
[7] Z.X. Wu, X.J. Xu, Z.G. Huang, S.J. Wang, Y.H. Wang, Phys. Rev. E 74 (2006) 0241107.
[8] W.X. Wang, G.R. Chen, Phys. Rev. E 77 (2008) 026101.
[9] W.X. Wang, B.H. Wang, B. Hu, G. Yan, Q. Ou, Phys. Rev. Lett. 94 (2005) 188702.
[10] W.X. Wang, R. Yang, Y.C. Lai, Phys. Rev. E 81 (2010) 035102(R).
[11] T. Zhou, M. Zhao, B.H. Wang, Phys. Rev. E 73 (2006) 037101.
[12] G. Yan, Z.Q. Fu, J. Ren, W.X. Wang, Phys. Rev. E 75 (2007) 016108.
[13] M. Zhao, T. Zhou, B.H. Wang, W.X. Wang, Phys. Rev. E 72 (2005) 057102.
[14] A.E. Motter, C.S. Zhou, J. Kurths, Phys. Rev. E 71 (2005) 016116.
[15] R. Yang, W.X. Wang, Y.C. Lai, G.R. Chen, Phys. Rev. E 79 (2009) 026112.
[16] Y.Y. Liu, J.J. Slotine, A.L. Barabási, Nature 473 (2011) 167.
[17] J. Sun, S.P. Cornelius, W.L. Kath, A.E. Motter, posted on 31 Aug 2011. arXiv:1108.5739.
[18] R. Yang, T. Zhou, Y.B. Xie, et al., Phys. Rev. E 78 (2008) 066109.
[19] G.Q. Zhang, D. Wang, G.J. Li, Phys. Rev. E 76 (2007) 017101.
[20] X.F. Wang, G.R. Chen, Physica A 310 (2002) 521.
[21] X. Li, X.F. Wang, G.R. Chen, IEEE Trans. Circuits Syst. 51 (2004) 2074.
[22] A.E. Motter, Phys. Rev. Lett. 93 (2004) 098701.
[23] A.E. Motter, N. Gulbahce, E. Almaas, A.L. Barabási, Mol. Syst. Biol. 4 (2008) 168.
[24] S. Sahasrabudhe, A.E. Motter, Nature Comm. 2 (2011) 170.
[25] S.P. Cornelius, W.L. Kath, A.E. Motter, posted on 18 May 2011. arXiv:1105.3726v1.
[26] C.T. Lin, IEEE Trans. Autom. Control 3 (1974) 201.
[27] A.E. Motter, Y.C. Lai, Phys. Rev. E 66 (2002) 065102(R).
[28] A. Lombardi, M. Hrnquist, Phys. Rev. E 75 (2007) 056110.
[29] R.E. Kalman, Y.C. Ho, K.S. Narendra, Contrib. Differ. Equ. 1 (1962) 189.
[30] R.E. Kalman, J. SIAM Control 1 (1963) 152.
[31] R. Albert, H. Jeong, A.-L. Barabsi, Nature 406 (2000) 378.
[32] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. Stata, A. Tomkins, J. Wiener, Comput. Netw. 33 (2000) 309.
[33] P. Erdös, A. Rényi, Publ. Math. Inst. Hung. Acad. Sci. 5 (1960) 17.
[34] F. Chung, L. Lu, Ann. Comb. 6 (2002) 125.
[35] M.E.J. Newman, Social Networks 27 (2005) 39.
[36] K.I. Goh, B. Kahng, D. Kim, Phys. Rev. Lett. 87 (2001) 278701.