Protecting infrastructure networks from cost-based attacks

2009 New J. Phys. 11 033006

(http://iopscience.iop.org/1367-2630/11/3/033006)

New Journal of Physics
The open-access journal for physics

Protecting infrastructure networks from cost-based attacks

Xingang Wang[1,2,3,5], **Shuguang Guan**[2,3] **and Choy Heng Lai**[3,4]
[1] Institute for Fusion Theory and Simulation, Zhejiang University, Hangzhou, 310027, People's Republic of China
[2] Temasek Laboratories, National University of Singapore, 117508 Singapore, Singapore
[3] Beijing–Hong Kong–Singapore Joint Centre for Nonlinear and Complex Systems (Singapore), National University of Singapore, Kent Ridge 119260, Singapore
[4] Department of Physics, National University of Singapore, Singapore 117542, Singapore
E-mail: wangxg@zju.edu.cn

New Journal of Physics **11** (2009) 033006 (9pp)
Received 6 January 2009
Published 3 March 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/3/033006

Abstract. It is well known that heterogeneous networks are vulnerable to the intentional removal of a small fraction of highly connected or loaded nodes, implying that to protect the network effectively, the important nodes should be allocated more defense resource than the others. However, if too much resource is allocated to the few important nodes, the numerous less-important nodes will be less protected, which if attacked together can still lead to devastating damage. A natural question is therefore how to efficiently distribute the limited defense resource among the network nodes such that the network damage is minimized against any attack strategy. In this paper, taking into account the factor of attack cost, the problem of network security is reconsidered in terms of efficient network defense against cost-based attacks. The results show that, for a general complex network, there exists an optimal distribution of the defense resource with which the network is best protected from cost-based attacks. Furthermore, it is found that the configuration of the optimal defense is dependent on the network parameters. Specifically, networks of larger size, sparser connection and more heterogeneous structure will more likely benefit from the defense optimization.

[5] Author to whom any correspondence should be addressed.

Contents

1. Introduction

Modern human societies depend very much on the efficient functioning and stable operation of complex infrastructure networks [1]. Typical examples are electrical power grids, telecommunication networks, the Internet and transportation systems such as road, railway and airline networks. A significant and common feature of these networks is that they all possess a heterogeneous degree distribution. In particular, several of these networks are scale-free networks (SFNs) [2]. Although the adoption of SFN structure could improve the network performance significantly, e.g. a shorter average network diameter, it also causes problems for the network security. For instance, it has been shown that the connectivity of an SFN could be largely damaged if a small fraction of the large-degree nodes were intentionally removed. In contrast, if the removal is of the small-degree nodes, the network damage will be very limited [3]. The robust-yet-fragile property of SFNs is more evident when the intrinsic dynamics of the network flow is taken into account [4]. This has been shown by a model of a cascade network in [5], where it is found that, due to the existence of flow dynamics, the removal of even a single node could trigger such a large-scale avalanche that only a small portion of the nodes survive cascading failures. Since practical networks typically carry flows, their being secure from cascading failures is thus of great importance and has drawn much attention in the past few years. The areas involved include: model design [6], damage estimation [7], dynamics characterization [8], capacity allocation [9], topology dependence [10], cascade control and defense strategies [11], etc.

2. Problem formulation

While the fragility of SFNs to intentional node removal has been well addressed, the studies performed so far have concentrated only on 'technical' failures, instead of intentional external attacks. More specifically, the previous studies were mainly interested in comparing the extent of the network damage caused by different attack implementations, ignoring the cost incurred in doing so. In a real attack, the attacker and the defender are two sides of a game. Their aims are in a sense the same, i.e. to maximize their gains with limited resources. The defender, knowing the importance of the large-degree nodes, will allocate more defense resources to them. On the other hand, the attacker who would like to attack the large-degree nodes has to worry about the higher cost involved in doing so. Thus, in a realistic situation, the attacker will strike a balance between the network damage and the attack cost, and search for the most effective attack to perform. For

example, in view of the higher cost of attacking an important and well-protected node, the attacker may choose to attack a number of unimportant and less-protected nodes together, since the latter alternative may generate greater damage. Thus, the attacker would analyze the network security before choosing the target(s).

To analyze the network security, the attacker usually compares various alternatives (or virtual attacks), based on the available network information, e.g. the network structure and the defense configuration, and evaluates the possible damages caused by the attacks. The attacker will then choose and implement the most damaging action. Usually the virtual attacks are based on two strategies: (i) concentrating all the efforts on attacking a few important and well-protected nodes and (ii) distributing the efforts to attack a number of less-important and less-protected nodes. We call the former the concentrated attack (CA) strategy and the latter the distributed attack (DA) strategy. It is clear that, if the nodes are equally protected, the network will be vulnerable to CA. In contrast, if too much defense resources are allocated to the important nodes, the network will be vulnerable to DA. Accordingly, the challenge faced by the defender is the following: *how to optimize the network defense so that the network damage will be minimized whatever attack strategy the attacker takes?*

The problem of cost-based attacks can be formulated as follows. Let $P = \{p_i,\ i = 1, \ldots, N\}$ be the existing defense of an infrastructure network consisting of N nodes. The defense resources allocated to node i is p_i. So the total amount of the network defense is $R = \sum_{i=1}^{N} p_i$. In the current study, we assume that the attacker has a full knowledge of the network, including the network topology, the flow dynamics and the defense distribution (the general case will be discussed later). Based on these pieces of information, the attacker will scheme a series of virtual attacks, $A_n = \{a_{n,j},\ j = 1, \ldots, N'\}$, based on either the CA or DA strategy. In the attack A_n, N' out of N nodes in the network will be selected as targets, and the cost of removing target j is denoted by $a_{n,j}$. The total attack cost of A_n is therefore $E_n = \sum_{j=1}^{N'} a_{n,j} = E$, which is identical for all the attacks aimed at the defense P. In general, we have $E \ll R$. The network damage caused by A_n is denoted by $D_n = \{b_{n,l},\ l = 1, \ldots, M\}$, where $\{l\}$ is the set of the failed nodes due to the attack A_n, and $b_{n,l}$ is the amount of network damage due to the failure of l. Then the total network damage caused by A_n can be quantified by $B_n = \sum_{l=1}^{M} b_{n,l}$. Evaluating the damage of each of the virtual attacks, the attacker will then identify the most devastating attack.

The optimal defense is defined as follows. If the defense resources are distributed in such a way that all the virtual attacks generate the same amount of network damage, then this distribution of defense resources is called the optimal defense, and the network is considered secure from cost-based attacks. Otherwise, if there are different amounts of network damage, the distribution is considered nonoptimal and the network is considered vulnerable to cost-based attacks. That is, if by changing the attack strategy the attacker can increase the network damage, the network is considered insecure.

3. The model

We implement the above idea of network security by using a model of a cascade network [5] (the generalization to other models is straightforward [3]). Let $L_i(0)$ be the transmission load (betweenness centrality) of node i, which accounts for the total number of shortest paths passing through i in the original network [12]. Define the node capacity as $C_i = (1+\alpha)L_i(0)$, which stipulates the maximum load that node i can handle. $\alpha > 0$ is the tolerance parameter. Once a

node is attacked, it will be removed from the network, together with the links that are associated with it. Because of node removal, the shortest paths of the network will be redistributed and, consequently, the load of the remaining nodes will be updated. In this process, any node that is overloaded, i.e. $L_i(t) > C_i$, will be removed from the network. The new removal will cause a new distribution of the shortest paths, thus generating another wave of node failures, and so on and so forth, until no node is overloaded in the remaining network. To fit this model to our problem of cost-based attacks, it is necessary to make a few assumptions. Firstly, it is assumed that the defense resources have the following power-law distribution:

$$p_i = R \times (C_i^{\beta} / C(\beta)), \tag{1}$$

where R is the total defense of the network and $C(\beta) = \sum_i C_i^{\beta}$ is a normalizing factor that is dependent on the parameter β. Without loss of generality, here we set $R = C(\beta = 1)$, i.e. the network defense equals the network capacity. Secondly, it is assumed that the cost of removing a node is equivalent to the node defense, i.e. $a_i = p_i$. Finally, it is assumed that the network damage relies only on the removed nodes. In the current study, the network damage is measured by two quantities: (i) the size of the largest component in the remaining network, G, and (ii) the total capacity of the removed nodes, $B = \sum_{l=1}^{M} b_l$. We emphasize that these assumptions are only made for the purpose of illustration. In real applications, they should be redefined according to the relevant situation. The key parameter in this model is therefore β, which gives the distribution of the defense resources. When $\beta \ll 0$, sufficient resources will not be allocated to the important (high-load) nodes, making the network vulnerable to CA. In contrast, if $\beta \gg 0$, the important nodes will be overprotected, making the network vulnerable to DA. So, to protect the network from cost-based attacks efficiently, the value of β should be set properly.

We next describe the method used in our analysis of network security. As the virtual attacks can be divided into two classes, CA and DA, one can see that network security can be evaluated by considering two representative attacks. For CA, we choose to attack the single node with the largest capacity (and thus also the highest protection). For DA, *with the same amount of attack cost*, we choose to attack a group of nodes with the smallest capacity (and thus also the lowest protection). Specifically, if the nodes are ranked by ascending order of the node capacity, i.e. $C_1 < C_2 < \cdots < C_N$, then in CA only node N will be attacked, whereas in DA the nodes 1 to N' will be attacked simultaneously. Here N' is a number to be determined by the relation $\sum_{i=1}^{N'} a_i \ \square \ a_N$. Note that in a realistic situation it is possible that the most devastating attack is neither of the above representative attacks. However, such a devastating attack, if it exists, will be very much dependent on the network details, and should be treated case by case [13].

4. Numerical results

To simulate the cost-based attacks, first we generate an SFN based on the model proposed in [2]. The network consists of $N = 3000$ nodes and has an average degree of $\langle k \rangle = 4$. The degree distribution follows a power-law $P(k) \sim k^{\gamma}$, where $\gamma = -3$. Secondly, we calculate the transmission load of each node and calculate the node capacity according to the value of α. As an example, we set $\alpha = 0.3$. We can then obtain the total defense of the network R, which in our model is set to be the total network capacity, i.e. $R = \sum_i C_i$. Thirdly, we choose a value for β and distribute the defense resources among the nodes according to equation (1). Fourthly, we analyze the network security against the two representative attacks and evaluate their damages $G_{1,2}$ and $B_{1,2}$, with subscripts 1 and 2 standing for CA and DA, respectively. Finally, by scanning

Figure 1. For SFNs of size $N = 3000$, average degree $\langle k \rangle = 4$, and tolerance parameter $\alpha = 0.3$, the dependence of the network damage on parameter β for CA and DA is shown. (a) $G_{1,2}$ versus β. The optimal defense is found at about $\beta_g \approx 1.25$. Inset: ρ_g versus β. (b) $B_{1,2}$ versus β. The optimal defense is found at about $\beta_b \approx 1.28$. Note the semi-logarithmic plot of $B_{1,2}$. Inset: ρ_b versus β. Each data point has been averaged over 50 network realizations.

β, we can determine the location of the optimal defense, i.e. the value of β when the two attacks generate the same network damage.

The variations of G and B as a function of β are plotted in figure 1. For the measurement G, the optimal defense is found at about $\beta_g \approx 1.25$ (figure 1(a)), and for the measurement B, the optimal defense is found at about $\beta_b \approx 1.28$ (figure 1(b)). Note that the optimal defense is only meaningful to the defender, as it tells him how to configure the defense resources against cost-based attacks. For the attacker, by knowing the specific network defense (the value of β), the only task is to figure out which attack is more damaging, DA or CA. For instance, if the attacker is interested in greater damage of network capacity and has learned that the network defense parameter is $\beta = 0.5$, after a comparison of the virtual attacks, the attacker will find that using CA will cause more damage than using DA (figure 1(b)).

It is important to note that in our numerical simulations, CA is always implemented by removing the single node with the largest capacity. That is why the network damage caused by CA is constant in figure 1. However, as β increases, the cost of removing the largest-capacity node is monotonically increased, i.e. $E = a_N \sim C_N^{\beta}$. This leads to the problem of attack efficiency, which is defined as the amount of network damage per unit attack cost. For measurement G, it is defined as $\rho_g = (N - G_M)/E$, with $G_M = \min(G_1, G_2)$. For measurement B, it is defined as $\rho_b = B_M/E$, with $B_M = \max(B_1, B_2)$. Interestingly, it is found that, at the optimal defense, the attack efficiency is also minimized (the insets of figure 1). Thus, we can see that with the optimal defense the network is protected not only from the attack strategy, but also from the attack efficiency.

Physically, optimal defense as defined here can be understood as follows. When β is small, say for example $\beta \approx 0$, the network nodes are equally protected regardless of their importance level. To generate a large amount of damage, the attacker will certainly choose to attack the important nodes, i.e. by adopting CA. As β increases, more defense resources will be shifted to the important nodes and, correspondingly, the defense of the non-important nodes will be

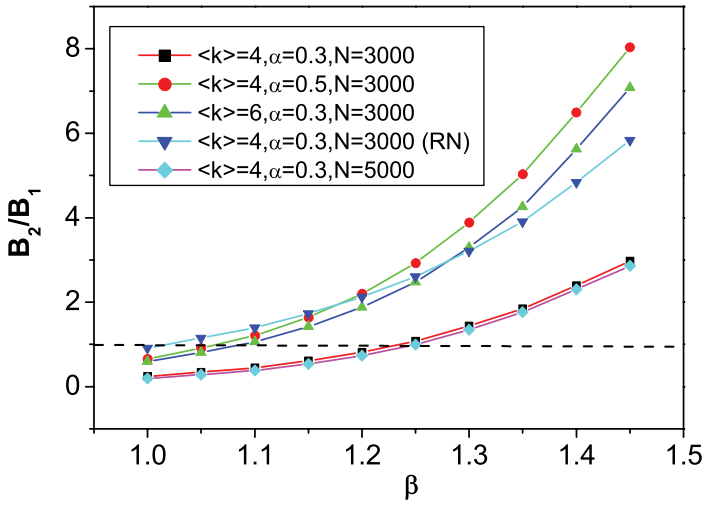

Figure 2. The dependence of β_b (characterized by the point where $B_2(\beta) = B_1(\beta)$) on the network parameters. It is found that β_b increases with N, but decreases with α, γ and $\langle k \rangle$. Each data point has been averaged over 50 network realizations.

weakened. However, as long as $\beta < \beta_{g,b}$, the damage caused by CA will still be larger than that of DA. So, in this range, CA will always be the choice for the attacker. Nevertheless, as β increases, the damage difference between CA and DA will be gradually narrowed. Then, at the optimal defense $\beta_{g,b}$, both attacks will generate the same amount of network damage. Since at this point the attacker cannot benefit from changing the attack strategy, the cost-based attacks are considered to have failed. After that, as β increases from $\beta_{g,b}$, the few important nodes will be overprotected, and the numerous non-important nodes will be less protected. Noticing this, the attacker will *switch* the attack from CA to DA, so as to achieve more damage. In the extreme situation of $\beta \to \infty$, all the defense resources will be allocated to the single node with the largest capacity, while the other nodes of the network can be easily attacked together.

As realistic networks have various structures, it is necessary to check the dependence of the optimal defense on the network parameters. In particular, we shall check the dependence of β_b on the following network parameters: the tolerance parameter α, the average degree $\langle k \rangle$, the degree exponent γ and the system size N. (A similar dependence is also valid for β_g.) The numerical results are plotted in figure 2. The general finding is that the value of β_b increases with N, but decreases with α, $\langle k \rangle$ and γ. (For RN, we have $\gamma \to \infty$.) In other words, it is the larger, sparser and more heterogeneous networks that will suffer more from the cost-based attacks and will therefore more likely benefit from the optimal defense. Since infrastructure networks normally have a larger size and a heterogeneous structure, the studies of optimal defense are thus of practical concern.

How about the defense of realistic networks? To address this question, we have analyzed the security of two typical infrastructure networks in our society: (i) the electrical power grid of the western United States [14] and (ii) the Internet at the autonomous level [15]. The power-grid network consists of $N = 4941$ nodes and has an average degree of $\langle k \rangle \approx 2.67$, and has been widely used in the literature as an example of cascade networks [5]. The variations of $G_{1,2}$ as a function of β is plotted in figure 3(a), where the optimal defense is found at about

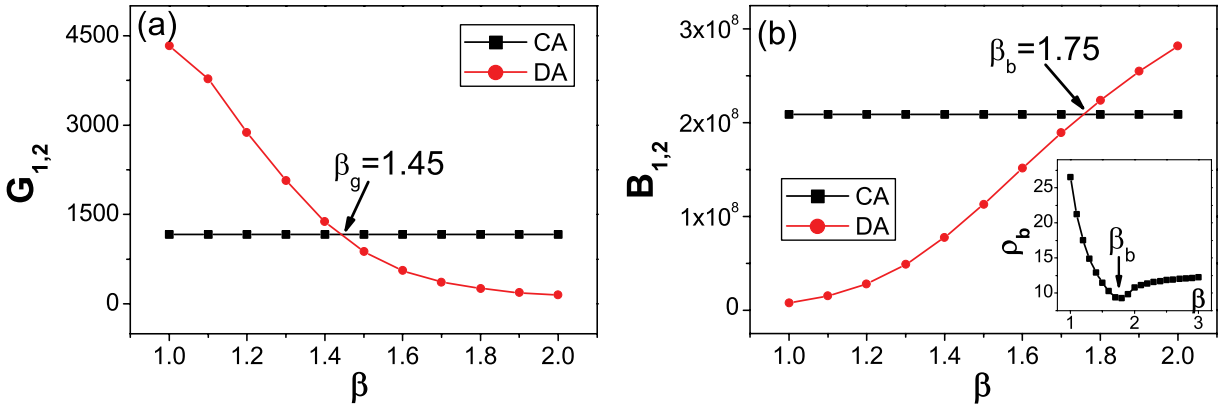

Figure 3. Security analysis for the western US power grid. (a) The dependence of $G_{1,2}$ on β, the optimal defense, is found at about $\beta_g \approx 1.45$. (b) The dependence of $B_{1,2}$ on β, the optimal defense, is found at about $\beta_b \approx 1.75$. Inset: ρ_b versus β, where ρ_b is minimized at β_b. Each data point is averaged over ten attack realizations. For CA, the top ten nodes of the highest load are attacked, while for DA, the nodes are attacked in ascending order of their capacities.

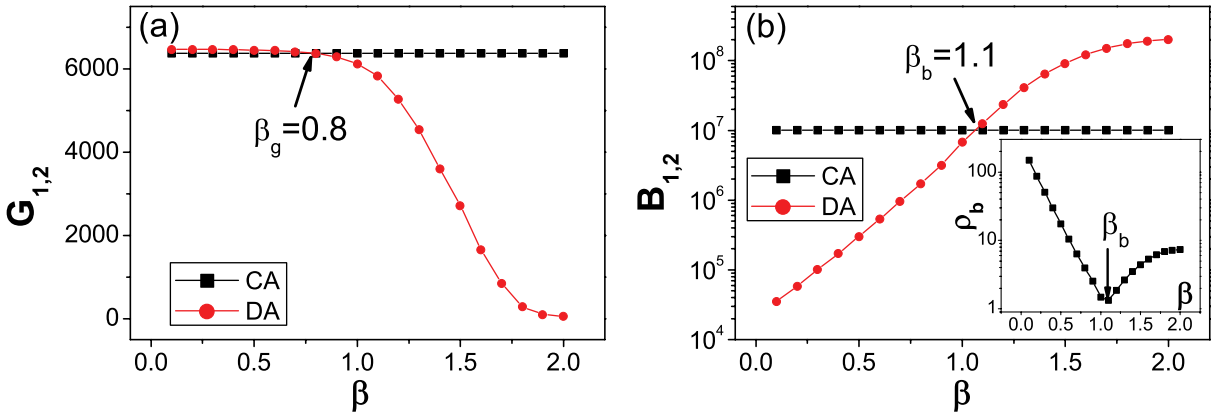

Figure 4. Security analysis for the Internet at the autonomous level. (a) The dependence of $G_{1,2}$ on β, $\beta_g \approx 0.8$. (b) The dependence of $B_{1,2}$ on β, $\beta_b \approx 1.1$. Please note the semi-logarithmic plot of $B_{1,2}$. Inset: ρ_b versus β, where ρ_b is minimized at β_b. Each data point is averaged over ten attack realizations, just as we have done in figure 3.

$\beta_g \approx 1.45$. In figure 3(b) we plot the dependence of $B_{1,2}$ on β, where the optimal defense is found at about $\beta_b \approx 1.75$. As we have done in figure 1, we have also calculated the dependence of the attack efficiency, ρ_b, on the defense parameter β, where ρ_b is found to be minimized at β_b. For the Internet we have employed $N = 6474$ nodes having an average degree of $\langle k \rangle \approx 3.88$. The variation of $G_{1,2}$ and $B_{1,2}$ as a function of β is plotted in figures 4(a) and (b), respectively. For the measurement G, the optimal defense is found at about $\beta_g \approx 0.8$, whereas for measurement B, the optimal defense is found at about $\beta_b \approx 1.1$. Still, ρ_b is minimized at β_b. It is interesting to see that, compared to the standard SFN model (figure 1) and the power-grid network (figure 3), the Internet is less vulnerable to CA when $\beta < \beta_g$ in terms of the measurement G (figure 4(a)). We attribute this strange behavior to the unique topology of the Internet, e.g. the modular

structure, the degree correlation and the hierarchical property. This also confirms our previous finding of the dependence of optimal defense on network parameters (figure 2).

5. Discussion and conclusion

The main purpose of the present study is to highlight the *variability and flexibility* of the network attacks possibly encountered in real situations (which is shown here by incorporating the new factor of attack cost), so as to bring out a point of caution in the defense of complex networks. Our main finding is that, if the defense resources of a network are not well distributed, the attacker could benefit from choosing between the attack strategies. In showing this, we employed the simple model of a cascade network and made a few assumptions on the network defense and attack, which when applied to real situations should be carefully modified and redefined. For instance, it has been shown recently that, as a balance between network robustness and frangibility, the relationship between node capacity and load could be nonlinear [16]. This indicates that, to analyze the security of such a network, the constant tolerance parameter used in the current model should be modified accordingly. This kind of modification, however, will not change the general picture of optimal defense. In fact, as long as the cost factor of network attack is considered, an optimal defense will exist and this is an important issue in network security.

It should be noted that the present model requires full knowledge of the network, including detailed information about the network structure and flow dynamics. These pieces of information, while available for some public systems such as the power grid [17] and the Internet, are difficult to obtain for others, such as terror and Mafia networks. In a secret network, the important nodes, which possess the larger degree and have higher ranks in the hierarchy, are usually well hidden and difficult to identify. This gives rise to the problem of attacking probability, a question recently investigated by Gallos *et al* [18]. In that study, the probability of removing a node was determined by three factors: the node degree k, the intrinsic network vulnerability α' and the node knowledge α''. There, a key finding was that, as the information on the important nodes is gradually exposed (increasing the value of α''), the fraction of nodes needed to break the network will be quickly reduced. Thus, if we regard hiding the network information as an approach to network defense, the paper by Gallos *et al* [18] and the present work have essentially the same basis. In particular, if we replace the parameter β in equation (1) by a new parameter $(\alpha' + \alpha'')/\kappa$ (where $\kappa \approx 1.6$ is the exponent that characterizes the relationship between the node capacity and degree [19]), then the node defense defined in equation (1) is just the reciprocal of the node vulnerability defined in [18]. For this reason, we can say that the paper [18] is a special case of the cost-based attacks considered here. Despite this similarity, the two studies actually deal with very different problems. Gallos *et al* [18] focus on the scale of network damage, in which the attack cost (information discovery) is variable and the attack strategy is always CA. In contrast, the current study deals with variable attack strategy and fixed attack cost, i.e. it is a question of network optimization [20].

In summary, we have proposed the idea of cost-based attacks on complex networks and investigated the problem of optimal network defense. Different from previous studies, we emphasize here the initiative and flexibility of the attacker in implementing the attacks, which is a step forward in the modeling of real situations. Hopefully, this study will stimulate new thinking on the security of complex networks and will be helpful in the design and defense of infrastructure networks.

Acknowledgment

XGW is supported by the National Natural Science Foundation of China under grant numbers 10805038 and 10805003. This work is supported under Project Agreement POD0613356 with the Defence Science and Technology Agency of Singapore.

References

[1] Albert R and Barabási A-L 2002 *Rev. Mod. Phys.* **74** 47
Newman M E J 2003 *SIAM Rev.* **45** 167
[2] Barabási A-L and Albert R 1999 *Science* **286** 509
[3] Albert R, Jeong H and Barabási A-L 2000 *Nature* **406** 378
Cohen R, Erez K, ben-Avraham D and Havlin S 2000 *Phys. Rev. Lett.* **85** 4626
Cohen R, Erez K, ben-Avraham D and Havlin S 2001 *Phys. Rev. Lett.* **86** 3682
Callaway D S, Newman M E J, Strogatz S H and Watts D J 2000 *Phys. Rev. Lett.* **85** 5468
[4] Watts D J 2002 *Proc. Natl Acad. Sci.* **99** 5766
Holme P and Kim B J 2002 *Phys. Rev.* E **65** 066109
Mereno Y, Gómez J B and Pacheco A F 2002 *Europhys. Lett.* **58** 630
Holme P 2002 *Phys. Rev.* E **66** 036119
[5] Motter A E and Lai Y-C 2002 *Phys. Rev.* E **66** 065102
[6] Wang B and Kim B J 2007 *Europhys. Lett.* **78** 48001
Wang W-X and Chen G 2008 *Phys. Rev.* E **77** 026101
[7] Crucitti P, Latora V and Marchiori M 2004 *Phys. Rev.* E **69** 045104
[8] Wang X G, Lai Y-C and Lai C-H 2006 *Phys. Rev.* E **74** 066104
Simonsen I, Buzna L, Peters K, Bornholdt S and Helbing D 2008 *Phys. Rev. Lett.* **100** 218701
[9] Heide D, Schäfer M and Greiner M 2008 *Phys. Rev.* E **77** 056103
Li P, Wang B-H, Sun H, Gao P and Zhou T 2008 *Eur. Phys. J.* B **62** 101
Gong X, Li K and Lai C-H 2008 *Europhys. Lett.* **83** 28001
[10] Wu J-J, Gao Z-Y and Sun H-J 2008 *Phys. Rev.* E **74** 066111
Gleeson J P 2008 *Phys. Rev.* E **77** 046117
[11] Motter A E 2004 *Phys. Rev. Lett.* **93** 098701
Buzna L, Peters K, Ammoser H, Kühnert C and Helbing D 2007 *Phys. Rev.* E **75** 056107
[12] Newman M E J 2001 *Phys. Rev.* E **64** 016132
Newman M E J 2001 *Proc. Natl Acad. Sci. USA* **98** 404
[13] Zhao L, Park K and Lai Y-C 2004 *Phys. Rev.* E **70** 035101
Latora V and Marchiori M 2005 *Phys. Rev.* E **71** 015103
[14] ftp://ftp.santafe.edu/pub/duncan/power_unweighted
[15] http://moat.nlanr.net/AS/Data/ASconnlist.20000102.946809601
[16] Kim D-H and Motter A E 2008 *New J. Phys.* **10** 053022
Kim D-H and Motter A E 2008 *J. Phys. A: Math. Theor.* **41** 224019
[17] Sachtjen M L, Carreras B A and Lynch V E 2000 *Phys. Rev.* E **61** 4877
Dobson I, Carreras B A, Lynch V E and Newman D E 2007 *Chaos* **17** 026103
Solé R V, Rosas-Casals M, Corominas-Murtra B and Valverde S 2008 *Phys. Rev.* E **77** 026102
[18] Gallos L K, Cohen R, Argyrakis P, Bunde A and Havlin S 2005 *Phys. Rev. Lett.* **94** 188701
[19] Kim J-H, Goh K-I, Kahng B and Kim D 2003 *Phys. Rev. Lett.* **91** 058701
Park K, Lai Y-C and Ye N 2004 *Phys. Rev.* E **70** 026109
[20] Motter A E and Toroczkai Z 2007 *Chaos* **17** 026101