Model for cascading failures with adaptive defense in complex networks*

Hu Ke(胡 柯), Hu Tao(胡 涛) and Tang Yi(唐 翌)†

Department of Physics and Institute of Modern Physics, Xiangtan University, Xiangtan 411105, *China*

(Received 8 December 2009; revised manuscript received 23 December 2009)

This paper investigates cascading failures in networks by considering interplay between the flow dynamic and the network topology, where the fluxes exchanged between a pair of nodes can be adaptively adjusted depending on the changes of the shortest path lengths between them. The simulations on both an artificially created scale-free network and the real network structure of the power grid reveal that the adaptive adjustment of the fluxes can drastically enhance the robustness of complex networks against cascading failures. Particularly, there exists an optimal region where the propagation of the cascade is significantly suppressed and the fluxes supported by the network are maximal. With this understanding, a costless strategy of defense for preventing cascade breakdown is proposed. It is shown to be more effective for suppressing the propagation of the cascade than the recent proposed strategy of defense based on the intentional removal of nodes.

Keywords: cascading failure, adaptive defense, complex network

PACC: 0250, 0590

1. Introduction

The study of cascading failure in complex networks is a topic of recent interest and practical importance.[1−4] In particular, this issue is crucial for a large number of technological networks, such as power grids, information communication networks, and transportation networks, on which modern human society very much relies. Evidence has shown that in such networks, a small initial attack or failure has the potential to trigger a global cascade, which either causes the network to fragment or severely limits the communication of the network. Typical examples are several blackouts of electrical power in some countries[5] and internet congestion.[6−8] Benefiting from the need of understanding and controlling these incidents, cascading behaviours have been investigated quite intensively in recent years,[9] where researchers have focused their attention on different aspects.[10−27] Among them, the following two issues are closely related to each other and of significant interests. One is to develop the theoretical model for describing cascade phenomena,[3,10−15] also including the analytical calculation of capacity parameter,[16,17] the modeling of the real-world data,[18,19] and congestion effects on the cascading failures.[20−23] The other is to design effective strategies of defense,[17,24−26] optimize capacity layout,[11,12,27,28] and optimize the weighting scheme[29] to minimize the risk of the cascading failures.

In a few previous models for description of the cascading failure,[3,12−14] for simplification, the flux of the relevant quantity exchanged between each pair of nodes, is assumed to be uniform and constant (usually is one unit). The load at a node is then the total flow passing through the node. The capacity of a node is the maximum load that the node can handle. In order to insure a node function properly, its load must be less than the capacity at all time; otherwise the node fails. Generally if the node with a large amount of load fails, the consequence could be serious because this amount of load needs to be redistributed into some other nodes and it is possible that for some nodes, the new load exceeds their capacities. These nodes will then fail, causing further redistribution of the load, and so on. As a consequence, a large fraction of the network can shutdown. In most of the previous studies of cascading failures, both the fluxes and the redistribution of load are treated in a time-independent or static way. Recently, considering the fact that the source fluxes at the nodes are neither

*Project supported by the National Natural Science Foundation of China (Grant No. 30570432) and the General Project of Hunan Provincial Educational Department of China (Grant No. 07C754).

†Corresponding author. E-mail: tangyii@yahoo.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

uniform nor static in many real networks, Heide *et al.*[11] have introduced the flux fluctuations into the model of cascading failures. They found that the flux fluctuations lead to the load fluctuations at the nodes, which may cause them to become overloaded and to induce a cascading failure. Moreover, an alternate robustness layout of the network is proposed against fluctuation-induced cascading failures.[11] In addition, Simonsen *et al.*[10] have proposed a dynamical flow model, where the transient dynamics of the redistribution of loads are taken into account. It is found that such transient dynamics results in the transient oscillations of load at the nodes and the network robustness is thus reduced in comparison with previous static overload failure models.[3,11] In this stage, the robustness of networks against cascading failures may be generally given by a complex interplay between the network topology and the flow dynamics.

Note that in many realistic circumstances when a heavily loaded node or link is lost for some reason, an adaptive adjustment of source fluxes on individual nodes can occur automatically,[30] in an attempt to prevent further overload failures for other nodes or links. From the perspective of communication, any removal of the network elements can reduce the efficiency of communication of a network,[31,32] leading to the adjustment of the source fluxes to adapt the perturbed network. Here we introduce a simple adaptive adjustment rule of the source fluxes and study a static overload model of cascading failure by considering the adaptive adjustment of the source fluxes in response to the perturbation of network. In general, the adaptive adjustment always tends to provide an underlying protection against cascading failures. Thus, we will refer to the adaptive adjustment as the adaptive defense.

2. The model with adaptive defense

For concreteness, we consider the model of overload failures introduced by Motter and Lai (ML),[3,11] which is defined as follows. For a given network $W(V,E)$ described by the sets of nodes V and links E, we assume that at every time step one flux $s_{ij}(t)$ is sent from node i to node j along the shortest-hop path $[i \to j]$, for every ordered pair of nodes (i,j) belonging to the same connected component of W. If there is more than one shortest path connecting two given nodes, the flux is divided evenly at each path. The load L_v on a node v is the total fluxes passing node per unit of time, which is written as

$$L_v(t) = \sum_{i,j \in V} r_{\rm sp}([i \to j]; v) s_{ij}(t). \tag{1}$$

The value of the path function $r_{\rm sp}([i \to j]; v)$ is either 1 or 0, depending on whether the node v is part of the shortest-hop path from node i to node j or not.[1)] The flux matrix s_{ij} is assumed to be uniform and constant in the ML model,[3] or temporal fluctuations in the recent proposed flux fluctuation model.[11,19] Each node v is then assigned to have a finite capacity C_v. The node operates in free-flux regime if $L_v(t) \le C_v$; otherwise the node is assumed to fail and is removed from the network. Initially, the network is assumed to be a connected one, and the load of each node is given by Eq. (1). The capacity C_v of node v is assumed to be proportional to the initial load $L_v(0)$:

$$C_v = \alpha L_v(0), \quad v = 1, 2, \ldots N, \tag{2}$$

where $\alpha \ge 1$ is the tolerance parameter and N is the number of nodes in the initial network.

The efficiency of the network, which provides a precise quantitative measure of how efficiently the networks exchange information,[31−34] is defined according to the length of the shortest path. Thus, we introduce the adaptive adjustment of the flux into the modeling (1) by varying the strengths s_{ij} according to the change of the shortest path lengths Δd_{ij}. Since the efficiency of network is a decreasing function of the length of the shortest path,[31,32] we expect that the fluxes should be a decreasing function of the length of the shortest path. For demonstration, we adopt an exponential relation with adjustable decreasing velocity

$$s_{ij}(t) = s_{ij}(0) \exp[-\beta \Delta d_{ij}(t)], \tag{3}$$

where $\Delta d_{ij}(t) = d_{ij}(t) - d_{ij}(0)$ and $d_{ij}(t)$ denotes the shortest path length between node i and node j at time t. The nonnegative coefficient β exponentially regulates the dependence of the fluxes on change of the distance between a pair of nodes. The exponential relation is motivated by the dependent relation of links formation on spatial distance. It is presented during the development of many real networks. In biological systems, for instance, gradients of chemical concentrations, or molecular interactions, decay exponentially with distance.[35] Particularly, when $\beta = 0.0$,

[1)] In the case of shortest-path degeneracy, the value of the path function is reduced by a factor depending on the degrees and depths of the respective branching points.

this model can be reduced to the ML model[3] if the initial flux matrix $s_{ij}(0)$ is assumed to be uniform and constant, or reduced to the traffic fluctuation model[11,19] if $s_{ij}(0)$ is assumed to be fluctuations and follows a certain distribution. In addition, it is worth while remarking that, while we focus on the exponential relation, we can consider different choices of s_{ij} with a linear or other nonlinear relation to Δd_{ij}, or depending on the length of the effective path[36,37] or the specific properties of each pair of nodes (degree, unoccupied capacity,[19] overload probability[19]).

3. The results

To be specific, we consider both the Barabási–Albert (BA) scale-free network model[38] and the real network structure of the western U. S. power transmission grid[39] to study the cascading failures. The BA network is a heterogeneous one with power-law degree distribution $P(k) \sim k^{-\gamma}$ with the degree exponent $\gamma = 3$,[38] and it has been shown that the load distribution also exhibits the power-law behaviour,[40] which indicates that there exist a few nodes with very large flow passing them. We focus on the cascades triggered by initial attacks on a small fraction p of most loaded nodes. Initially, the fluxes $s_{ij}(0) = 1$ for each pair of nodes. After an initial attack, a small fraction p of nodes with highest loads is removed from the network, and then both the shortest path lengths and the fluxes for each pairs of nodes are recomputed. Particularly, $s_{ij} = 0$ when node i and node j do not keep connectivity, i.e., $d_{ij}(t) = \infty$. Both the removal of nodes and the reduction of the fluxes lead to the next redistribution of load among the remaining nodes, and the subsequent overload, i.e., $L_v(t) > C_v$ for some nodes, the phenomenon that the failures are propagated may occur. The cascading process continues until the updated load satisfies $L_v(t) \leq C_v$ for all existing nodes, and the size of the largest connected component N' at the final state is measured. Usually, the damage caused by a cascade is quantified in terms of the relative size G of the largest connected component,[3]

$$G = \frac{N'}{N}, \tag{4}$$

which is viewed as a measure of the robustness of network. Figure 1 shows the relative size G of the largest component after a cascading, as a function of the tolerance parameter α, for different values of β. Without adaptive reduction of the fluxes, the initial attack on only 0.1% of the nodes triggers global cascades even for relatively large values of the tolerance parameter [Fig. 1(a), stars]. However, the relative size of the largest component G is shown to be larger when the fluxes among some pairs of nodes are reduced according to the adaptive defense mechanism mentioned above [Fig. 1(a), open symbols]. For example, for $\alpha = 1.5$, we have $G \approx 0.96$ with the adaptive defense with $\beta = 0.5$ and $G \approx 0.05$ without the adaptive defense.

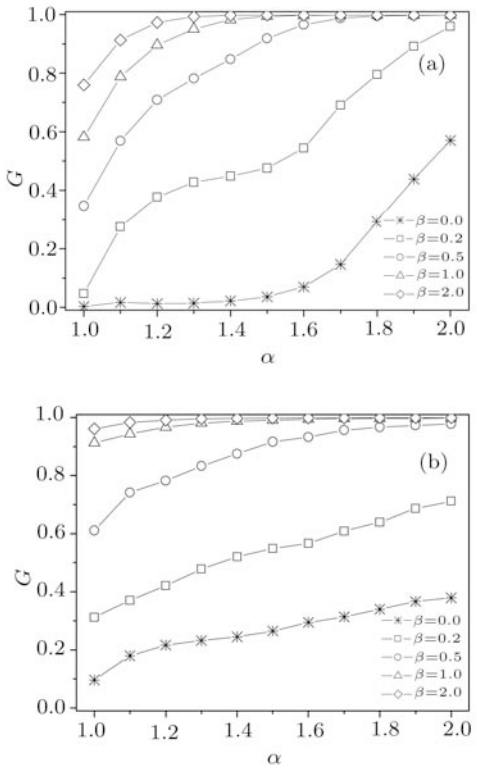


Fig. 1. Cascading failures with adaptive defense: (a) the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$, and (b) the western U. S. power transmission grid with $N = 4941$ and $\langle k \rangle \approx 2.67$, as triggered by the removal of a fraction $p = 0.001$ of nodes. Stars correspond to cascade failures without adaptive defense. Each curve corresponds to an average over 100 independent realizations for the BA network and 100 different triggers for the power grid.

The real network structure of the western U. S. power transmission grid considered here was compiled by Duncan Watts and Steven Strogatz and available at the web site http://cdg.columbia.edu/cdg/datasets, contains 4941 nodes and 6594 links,[39] corresponding to an average connectivity $\langle k \rangle \approx 2.67$. Although the power grid is a very homogeneous network in terms of the degree distribution, the load distribution, in a sharp contrast, shows a strong heterogeneity.[3,12] In other words, the degree distribution is more like an exponential one, while the

load distribution is similar to the power-law one.

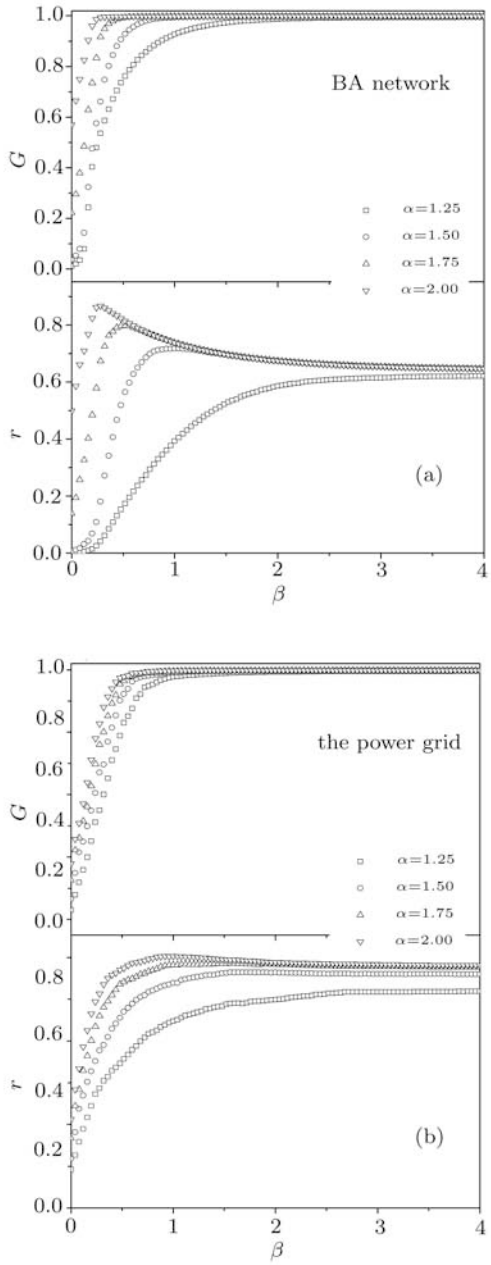


Fig. 2. The relative size G of the largest connected component and the relative remaining fluxes r as a function of the parameter β in both (a) the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$, and (b) the power grid for various values of the tolerance parameter α. Each curve corresponds to an average over 100 independent realizations for the BA network, while corresponds to an average over 100 different triggers for the power grid.

In such a network, our simulations present the results that do not have a fundamental deviation from those in the BA scale-free network [see Fig. 1(b)]. This indicates that the broad load distribution can be one of the reasons that the adaptive defense can effectively enhance the robustness of networks.

The final remaining fluxes that can be supported by the network may be a more intuitive measure for the ability of communication of network than the relative size G of the largest connected component. We define the relative remaining fluxes r as the ratio of the remaining fluxes to the initial fluxes:

$$r = \frac{f_{\text{remaining}}}{f_{\text{initial}}} = \frac{f_{\text{remaining}}}{N(N-1)}, \tag{5}$$

where $f_{\text{remaining}}$ is the final remaining fluxes supported by the network and f_{initial} represents the total fluxes in the initial network. In Fig. 2, we report both the relative remaining fluxes r and the relative size of the largest component G as a function of β. With the increase of β, the relative remaining fluxes firstly increase sharply and then encounter a slowly decrease, finally approach a nonzero plateau value. Especially, for the large tolerance parameter α, a sharp peak for the relative remaining fluxes can be easily observed, where the relative size of the largest component G is close to 1. From Fig. 2, one can find an interesting result that at a suitable value of β, a high robustness of network can be reached and at the same time less fluxes of the physical quantity are required to be removed. Obviously, it will be of practical importance for how to enhance the robustness of the network by reducing least fluxes. In general, an increase of β seems to make the final fluxes reduce even more. However, the reduction of fluxes can effectively prevent further overload failures of nodes and thus stop the further reduction of the fluxes.

4. The strategy of defense

Motivated by the above results, we also design an alternative strategy to prevent cascading failures based on an intentional removal (IR) of a fraction of fluxes. Usually, a cascade can be divided into two parts:[24] (I) the initial attack, where a fraction of nodes is removed; (II) the propagation of the cascade, where another fraction of nodes is removed due to the subsequent overload failures. In a real network, (I) and (II) are separated by time interval but this time interval is usually much shorter than the time scale in which the network evolves. Therefore, it is reasonable to consider that no edges or nodes can be rewired or added to the system after the initial attack because any of these operations would involve extra costs. In this perspective, we assume that, after the initial attack, the only operations allowed in order to reduce

the size of the cascade are the IR of fluxes, nodes or edges. Among them, the IR of nodes or edges has been investigated by Motter,[24] which has been shown that it can drastically reduce the size of the cascade, especially for the IR of nodes.[24] Now we argue that the size of the cascade can be more effectively reduced by the IR of the fluxes not necessarily connected to the IR of network elements (i.e., nodes and edges). In the initial network, if the communication or traffic flux is closed between node i and node j, the total load generated by the fluxes between node i and node j

$$L_{ij}^{g} = 2s_{ij}(d_{ij}+1) \tag{6}$$

is removed. The factor 2 comes from the fact that a physical quantity is sent from node i to node j and another is sent from node j to node i, i.e., the flux is symmetrical. In general, the flow through the shortest path with large length d_{ij} not only generates more loads to the network but also travels via more nodes with high load. Additionally, it has been proved that if the nodes with high loads are protected, the network would possess high robustness against cascading failures.[19] This observation is our starting point to argue that the size of the cascade can be drastically reduced with the IR of a certain fraction f of the fluxes according to the following strategy: fluxes with the largest L_{ij}^{g} are removed first.

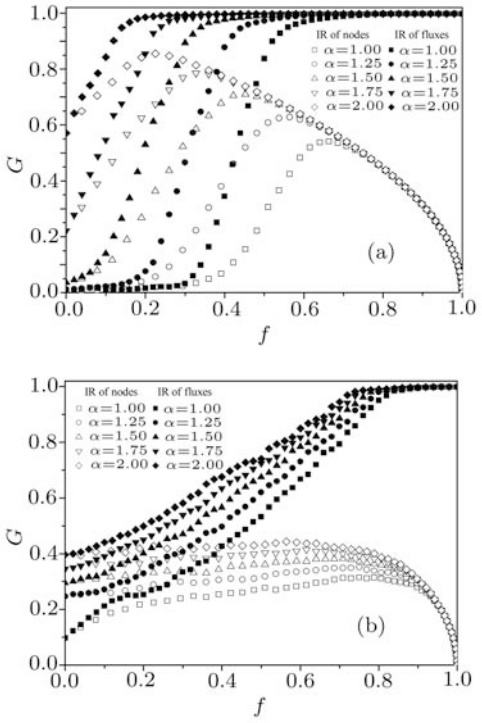


Fig. 3. The relative size G of the largest connected component as a function of the fraction f of the removed fluxes for both the IR of nodes and the IR of fluxes: (a) the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$, and (b) the power grid. Each curve corresponds to an average over 100 independent realizations for the BA network, while it corresponds to an average of over 100 different triggers for the power grid.

We consider the static overload failure model proposed by ML[3] to estimate the efficiency for the two defense strategies: the IR of fluxes and the IR of nodes. Figure 3 shows the relative size of the largest component G as a function of the fraction f of the removed fluxes by using the two kinds of strategies in the BA network, where great improvement of the robustness of network against the cascading failures becomes clear when comparing the result for the IR of fluxes with that obtained for the IR of nodes. The fluxes are reduced less while the relative size of the largest component is larger than those for the IR of nodes. In fact, the IR of nodes corresponds to the removal of all fluxes generated by the removed nodes. Let g denote the fraction of the removed nodes. The fraction of the removed fluxes $f \approx 2g - g^2$. However, for these fluxes, only a part of them plays an important role to trigger further overload failure. In this stage, the present strategy saves a large amount of fluxes since it is not necessary to remove the fluxes $s_i = 2\sum_j s_{ij}$ sent out and received by a node i. In addition, any removal of nodes in general reduces the final number of nodes in the largest connected component, and thus limits the maximum of G. When g is large, though the propagation of the cascade is strongly suppressed, the damage, nearly all of which is caused by the IR of nodes, is large. When g is small, most of the damage is caused by the cascade itself. The maximum of G is always smaller than $1 - g$, although it lies in a region of intermediate g where the propagation of the cascade is significantly suppressed and damage caused by the IR of nodes is relatively small.[24] In our strategy, since no damage is caused by the IR of fluxes, G can approximate to 1 when f is large enough.

Finally, we also apply both the IR of fluxes and the IR of nodes to the power grid of the western United States. In Fig. 4, we report the ratio G for both the IR of nodes and the IR of fluxes. One can note that the IR of the nodes cannot in fact constitute an efficient strategy of defense in the power grid, while the IR of fluxes can effectively suppress the propagation of the cascade.

Here it should be pointed out that the IR of nodes used above is based on the scheme that nodes with the

smallest load L_i are removed first. In fact, in the IR of nodes proposed by Motter, four different schemes can be applied to implement the strategy.[24] However,

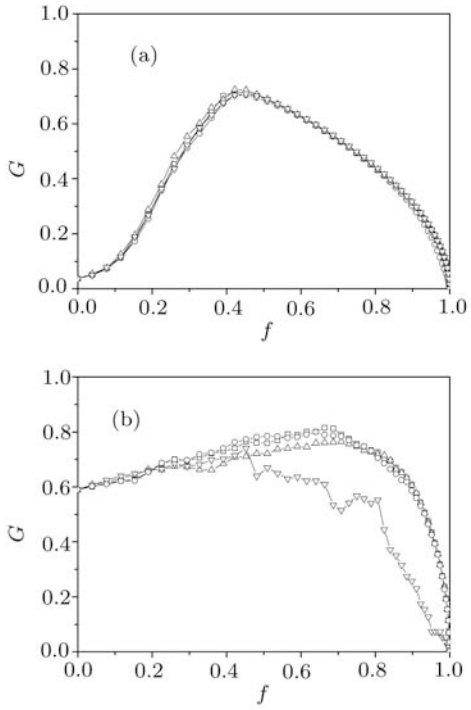


Fig. 4. The relative size G of the largest connected component as a function of the fraction f of the removal fluxes for both the IR of nodes: (a) the BA network with the system size $N = 5000$ and the average degree $\langle k \rangle = 4$; (b) the power grid, for $\alpha = 1.5$. The IR of nodes is based on the four following schemes: nodes with the smallest L_i are removed first (Δ); nodes with the smallest closeness centrality $\overline{D_i}^{-1}$ are removed first, where $\overline{D_i}$ is the average shortest path length from node i to all the others ($\circ$); nodes with the smallest $\Delta_i = L_i - L_i^g$ are removed first where $L_i^g = \sum_j (d_{ij} + 1)$ is the total load generated by node i ($\square$); nodes with the smallest degree k_i are removed first (∇). Each curve corresponds to an average over 100 independent realizations for the BA network, while corresponds to an average over 100 different triggers for the power grid.

the IR of nodes based on the four different schemes shows an almost same efficiency [see Fig. 4]. Thus in this paper, we consider the IR of nodes according to the only scheme that nodes with the smallest load L_i is removed first.

5. Conclusion and discussion

In summary, we have introduced an adaptive defense mechanism into the model of cascading failure. The results show that the network can be robust against cascading failures when adaptively adjusting the fluxes. Indeed, the adaptive adjustment mechanism of fluxes described here, which stems from alternative dynamical schemes of fluxes, should be considered as only the first step in exploring the underlying factors driving the fluxes into temporal fluctuations or dynamical evolution. Proper formation of complex adjustment mechanism requires taking many more detailed factors into account.

For the control and defense of the cascade, we have also proposed an alternative strategy to reduce the size of cascades of overload failures. By applying it to both the artificially created scale-free network and the real network structure of the power grid, we have shown that the size of the cascade can be drastically reduced by selectively removing a small fraction of fluxes exchanged between the nodes with large length of the shortest path. Recent evidence has shown that the fragility of networks to cascading failures is rooted in the broad load distribution. Especially, the existence of nodes with a high load can make the network vulnerable to cascading failures which have been observed in many transportation networks.[40−42] Thus a more effective strategy might be designed by considering the IR of the fluxes that flows through the nodes with high load. In addition, all these strategies based on the IR of nodes, edges or fluxes, require a complete knowledge about network structures, or at least fairly good knowledge of the degree of each node in the network. Such global information often proves hard to gather.[43] From this perspective, it will be of practical importance to develop effective strategy of defense by using only local information about the network.

References

[1] Holme P and Kim B J 2002 *Phys. Rev.* E **65** 066109

[2] Holme P 2002 *Phys. Rev.* E **66** 036119

[3] Motter A E and Lai Y C 2002 *Phys. Rev.* E **66** 065102(R)

[4] Moreno Y, Gmez J B and Pacheco A F 2002 *Europhys. Lett.* **58** 630

[5] Sachtjen M L, Carreras B A and Lynch V E 2000 *Phys. Rev.* E **61** 4877

[6] Jacobson V 1988 *Comput. Commun. Rev.* **18** 314

[7] Guimerà R, Arenas A, Diaz-Guilera A and Giralt F 2002 *Phys. Rev.* E **66** 026704
[8] More information can be found in the web site http://www.ofta.gov.hk/en/DATASTAT/ibccds.html
[9] Boccaletti S, Latora V, Moreno Y, Chavez M and Hwang D U 2006 *Phys. Rep.* **424** 175
[10] Simonsen I, Buzna L, Peters K, Bornholdt S and Helbing D 2008 *Phys. Rev. Lett.* **100** 218701
[11] Heide D, Schäfer M and Greiner M 2008 *Phys. Rev.* E **77** 056103
[12] Wang B and Kim B J 2007 *Europhys. Lett.* **78** 48001
[13] Crucitti P, Latora V and Marchiori M 2004 *Phys. Rev.* E **69** 045104(R)
[14] Moreno Y, Pastor-Satorras R, Vazquez A and Vespignani A 2003 *Europhys. Lett.* **62** 292
[15] Wang W X and Chen G 2008 *Phys. Rev.* E **77** 026101
[16] Zhao L, Park K and Lai Y C 2004 *Phys. Rev.* E **70** 035101(R)
[17] Zhao L, Park K, Lai Y C and Ye N 2005 *Phys. Rev.* E **72** 025104(R)
[18] Kinney R, Crucitti P, Albert R and Latora V 2005 *Eur. Phys. J.* B **46** 101
[19] Kim D H and Motter A E 2008 *New Journal of Physics* **10** 053022
[20] Zhao X M and Gao Z Y 2007 *Chin. Phys. Lett.* **24** 283
[21] Wu J J, Gao Z Y, Sun H J and Huang H J 2006 *Europhys. Lett.* **74** 560
[22] Zheng J F, Gao Z Y and Zhao X M 2007 *Europhys. Lett.* **79** 58002
[23] Zheng J F, Gao Z Y and Zhao X M 2007 *Physica* A **373** 873
[24] Motter A E 2004 *Phys. Rev. Lett.* **93** 098701
[25] Huang L, Lai Y C and Chen G 2008 *Phys. Rev.* E **78** 036116
[26] Gallos L K, Cohen R, Argyrakis P, Bunde A and Havlin S 2005 *Phys. Rev. Lett.* **94** 188701
[27] Schäfer M, Scholz J and Greiner M 2006 *Phys. Rev. Lett.* **96** 108701
[28] Li P, Wang B H, Sun H, Gao P and Zhou T 2008 *Eur. Phys. J.* B **62** 101
[29] Yang R, Wang W X, Lai Y C and Chen G 2009 *Phys. Rev.* E **79** 026112
[30] Newth D and Ash J 2005 *Complexity International* **11** 125
[31] Latora V and Marchiori M 2001 *Phys. Rev. Lett.* **87** 198701
[32] Latora V and Marchiori M 2007 *New Journal of Physics* **9** 188
[33] Nagurney A and Qiang Q 2007 *Europhys. Lett.* **79** 38005
[34] Vragović I, Louis E and Díaz-Guilera A 2005 *Phys. Rev.* E **71** 036122
[35] Murray J D 1990 *Mathematical Biology* (Heidelberg: Springer)
[36] Yan G, Zhou T, Hu B, Fu Z Q and Wang B H 2006 *Phys. Rev.* E **73** 046108
[37] Zhao H and Gao Z Y 2007 *Eur. Phys. J.* B **57** 95
[38] Barabási A L and Albert R 1999 *Science* **286** 509
[39] Watts D J and Strogatz S H 1998 *Nature* (London) **393** 440
[40] Goh K I, Kahng B and Kim D 2001 *Phys. Rev. Lett.* **87** 278701
[41] Ohira T and Sawatari R 1998 *Phys. Rev.* E **58** 193
[42] Holme P 2003 *Adv. Complex Syst.* **6** 163
[43] Cohen R, Havlin S and Ben-Avraham D 2003 *Phys. Rev. Lett.* **91** 247901