New Journal of Physics
The open–access journal for physics

Building catastrophes: networks designed to fail by avalanche-like breakdown

M Woolf[1], Z Huang and R J Mondragón
Department of Electronic Engineering, Queen Mary University of London,
Mile End Road, London, E1 4NS, UK
E-mail: m.woolf@elec.qmul.ac.uk

New Journal of Physics **9** (2007) 174
Received 31 January 2007
Published 28 June 2007
Online at http://www.njp.org/
doi:10.1088/1367-2630/9/6/174

Abstract. We present a simple method for constructing networks designed to fail catastrophically due to an avalanche-like breakdown. Our method simulates an avalanche in reverse, building a network designed to fail by avalanche-like breakdown. Some restrictions are imposed on the output flow rates of the nodes. An expression for the critical output flow rate of a node is derived. Nodes in the network are considered to have failed when their output flow rate exceeds this value. Two cases are considered: networks where total flow in the network increases with network size; and networks where the total flow is constant. We also consider networks in which nodes have weighted output flow rates. The topology of the generated networks is studied, and it is seen that networks that are almost homogeneous in node degree may still fail catastrophically. Finally we present some possible extensions to the method.

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

PII: S1367-2630(07)42950-0

Contents

1. Introduction

Man-made complex networks [1]–[3] such as the Internet, power transmission grids and telephone systems are susceptible to catastrophic failures in which the entire network ceases to function [4]–[6]. The most common cause of a catastrophic failure is an avalanche-like breakdown. This can result from the failure of a single node in a network in which nodes are sensitive to overloading. Redistribution of the load of this failed node over the network may cause other nodes to fail, triggering an avalanche-like event in which node failures propagate through the network. The entire network may in the end fragment into disconnected subnetworks. Networks with heterogenous node degree distribution, such as scale-free networks [7], are much more likely to suffer this type of event [8]. This is because a small subset of core nodes will be highly connected and handle much of the traffic in a scale-free network. If one of these heavily loaded core nodes ceases to function, either through malicious attack or random failure, it will have a large impact on other nodes in the network, making subsequent failures very likely. However, similar catastrophic failures are possible in networks with more homogeneous degree distributions. As we show in this paper, if the network degree distribution has just a small amount of heterogeneity then avalanche-like breakdowns are possible when all nodes are close to their failure load. Similar behaviour has been seen in social networks [6]. In the theoretical case of a completely homogeneous network in which all nodes are close to their maximum load, failure of a single node could cause the whole network to collapse in a single stage.

In this paper, we are concerned with transport networks in which particles of information (we shall call them packets in this paper) are transported through the network. Packet data networks such as the Internet are the most familiar examples of this, but the model can also be applied to road networks [9] and social acquaintance networks [10]. The most obvious approach to routing packets through a network, and the one used in the Internet, is to pass them through the shortest path. In Internet routing weights are placed on links according to different metrics. These weights are used to calculate shortest paths and generate routing tables [11, 12]. Much work has been done in finding better alternatives to shortest path routing [13]–[17]. All show considerable improvements in carrying capacity, that is the load that can be carried by the network before jamming occurs. However, as Sreenivasan *et al* [18] showed, there is a limit to how much improvement may be made in this way. All heavily loaded networks are in the end vulnerable to cascade failure.

In [6, 8], [19]–[21], cascading breakdown in static networks has been studied. In [6, 8, 20, 21], the method is to overload one or more nodes in a pre-existing network and study the resulting cascade. Holme and Kim [19] have a slightly different approach, evolving a scale-free network until cascade failure occurs due to the increasing load in the network. (Load here is defined by the topological property betweenness centrality, defined in section 2.1 below.) In [19, 20], breakdown is simulated by computer, whereas [6, 8, 21] use mathematical models. One difficulty of the former approach is that this type of simulation is very computationally demanding, which imposes a limit on the size of network that can be modelled. This makes it difficult to find out how well the mathematical models scale with network size. In this paper, we approach the study of cascading failure from another direction. We build networks in such a way as to ensure their breakdown. In essence we follow the cascading breakdown in reverse. By doing this we hope to better understand the dynamics of the process. This approach is also less computationally demanding and will therefore allow the simulation of larger networks. The model can be easily extended to real-world networks.

2. Preliminaries

2.1. Definitions and network measures

It is conventional to represent a complex network by an undirected graph, $\mathcal{G}(\mathcal{V},\mathcal{E})$. Here $\mathcal{V}$ is the set of vertices of the graph representing the nodes of the network; $\mathcal{E}$ is the set of edges representing the links of the network. In a packet data network, for example, the vertices would represent routers or hosts; the edges data links. Edges are unweighted and there are no self-edges or duplicate edges between vertices. We assume that flows between source and destination all follow the shortest possible path (the geodesic path). The average shortest path length,

$$\bar{\ell} = \frac{1}{N(N-1)} \sum_{s\in\mathcal{V}} \sum_{d\neq s\in\mathcal{V}} \ell_{s,d}, \tag{1}$$

where $\ell_{s,d}$ is the length of the shortest path between source, s, and destination, d. N is the number of nodes in the network.

As in [13, 14, 19, 21] and others, we chose $B(v)$, the vertex betweenness centrality [22, 25] (often abbreviated to 'betweenness') to give a measure of the load on a node based purely on the topology of the network. If one imagines that for a single time step one packet of information is passed between each node pair in the network, the route taken always being the shortest path, then the load on any given node would be equivalent to the number of shortest paths passing through that node.[2] This is the basis of betweenness. The proportion of shortest paths from s to d containing vertex v, $p_{s,d}(v) = \sigma_{sd}(v; s, d)/\sigma_{sd}(s, d)$ where $\sigma_{\mathrm{sd}}(s, d)$ is the number of shortest paths between s and d, and $\sigma_{sd}(v; s, d)$ is the number of shortest paths between s and d that pass

[2] If each node pair had only one shortest path between them this would be exactly the case. In fact, since there may be more than one path of the shortest length between a given node pair, the fraction of those shortest paths passing through v are summed for that pair when calculating $B(v)$.

through node v. The betweenness of node v is then

$$B(v) = \sum_{v \in \mathcal{V}} \sum_{d \neq s \in \mathcal{V}, d \neq v} p_{s,d}(v). \tag{2}$$

It should be noted that our definition of $B(v)$ is slightly different from others. In Freeman's original definition [22], node v is not counted as either source or destination when summing values of $p_{s,d}(v)$ in (2). Other authors do include v as source or destination [10, 23]. In our case we would like to include single hop routes (routes with no intervening nodes) and allow packets to leave the network immediately on reaching their destination. Hence when summing in (2), v can be the source, but not the destination.

A property of the betweenness centrality as defined here is that[3]

$$\sum_{v \in \mathcal{V}} B(v) = \sum_{s,d} \ell_{s,d} = N(N-1)\bar{\ell}. \tag{3}$$

2.2. *Load and congestion at a node*

The average information flow arriving at node v is [24, 26, 27]

$$\lambda_v = \frac{F(\Lambda, N)B(v)}{N(N-1)}, \tag{4}$$

where $F(\Lambda, N)$ is the flow generated per unit time by the whole network. The flow is a function of the rate of packet production at a node, Λ, and network size, N. If μ_v is the output flow, then the node will get congested if its input flow is greater than its output flow, $\lambda_v \geqslant \mu_v$. The onset of congestion therefore occurs at the critical value:

$$\lambda_v^* = \mu_v = \frac{F(\Lambda, N)B(v)}{N(N-1)}. \tag{5}$$

We consider two cases:

1. Each node v produces packets at a rate $\Lambda_v = \Lambda$, distributed evenly between the $N-1$ destinations. In this case total flow in the network increases with network size. The total flow in the network is $F(\Lambda, N) = N\Lambda$. If node v is the first to get congested in the network, it follows from (5) that this will occur when the packet production rate reaches the critical value [24]:

$$\Lambda^* = \frac{\mu_v(N-1)}{B(v)}. \tag{6}$$

In terms of betweenness, congestion will occur when (see [13, 14, 17, 18, 26])

$$B(v) = \frac{\mu_v(N-1)}{\Lambda^*}. \tag{7}$$

[3] This can be understood as performing the sum on the left-hand side of (3) in a different order: taking each node pair in the network and counting which betweennesses they contribute to.

2. Only K of the nodes produce packets (all at rate Λ) distributing flow evenly amongst the $N-1$ possible destination nodes. The total flow in the network is then $F(\Lambda, N) = K\Lambda$ where K is a constant. That is, total flow in the network is independent of network size. The average arrival rate of packets at node v is

$$\lambda_v = \frac{K\Lambda}{N(N-1)} B(v). \tag{8}$$

The corresponding critical load and betweenness for node v are:

$$\Lambda^* = \frac{\mu_v N(N-1)}{B(v)K}. \tag{9}$$

and

$$B(v) = \frac{\mu_v N(N-1)}{\Lambda^* K}. \tag{10}$$

2.3. Avalanches and betweenness

An avalanche in one of our networks would occur in the following way. When a node became congested all edges connected to that node would be removed. After removal of this node and its edges, loads would be recalculated. The load on other nodes might increase sufficiently for them to also get congested: these nodes also would be removed from the network and loads would again be recalculated. The process would continue until no nodes in the network were overloaded.

Considering the first case of section 2.2 in which the total flow in the network increases as the network grows: equation (7) holds, that is node v will get congested when $B(v) = (\mu_v(N-1))/\Lambda^*$. After node v and its links are removed, node w will become congested when $B'(w) = (\mu_w(N'-1))/\Lambda^*$, where $B'(w)$ is the betweenness of node w in the reduced network and N' is the size of the reduced network. Hence $B(v)$ and $B'(w)$ must satisfy

$$B'(w) = \frac{(N'-1)}{(N-1)} \frac{\mu_w}{\mu_v} B(v). \tag{11}$$

If we consider the case $\mu_v = 1$ for all v, then a lower bound for the betweenness of the network is obtained from (3). In this case the vertex with the highest critical load is the vertex with the largest betweenness, so if the average betweenness in the network is given by

$$\frac{1}{N} \sum_{v \in \mathcal{V}} B(v) = (N-1)\bar{\ell} \tag{12}$$

and the maximum betweenness, $B_{\max} = \max\{B(v), v \in \mathcal{V}\}$, then we have a lower bound to $B_{\max}$ [19]: $B_{\max} \geqslant (N-1)\bar{\ell}$.

From (7) we can obtain an upper bound to the maximum betweenness by noticing that the vertex with the largest betweenness will be congested if its load is greater than or equal to Λ^*, in this case $B_{\max} \leqslant (N-1)/\Lambda^*$.

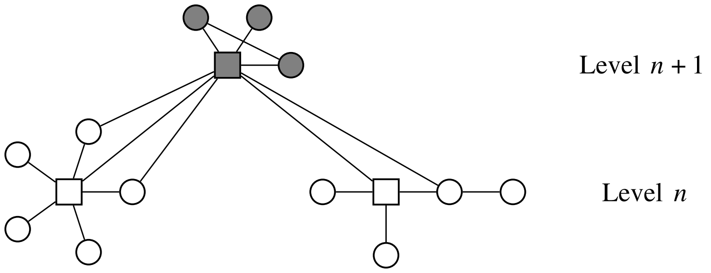

Figure 1. Building the network. The grey vertices are the new nodes introduced at step $n+1$. The square vertices are the nodes that will get congested and removed when the avalanche occurs. Note that all connections from the new nodes to the nodes of stage n are made via the grey square vertex.

A similar argument may be applied in the second case of section 2.2. Here the total flow is constant, independent of network size. The betweennesses in the original and reduced networks are related by

$$B'(w) = \frac{N'(N'-1)}{N(N-1)}\frac{\mu_w}{\mu_v}B(v). \tag{13}$$

As before, if we take $\mu_v = 1$ for nodes v, then $(N-1)\bar{\ell} \leqslant B_{\max} \leqslant N(N-1)/(K\Lambda^*)$.

3. Building catastrophes

To build a catastrophic network we follow the avalanche process in reverse. Starting with one or more small core networks we build the network a node at a time. The process is illustrated in figure 1. Square nodes are congestion nodes, required to fail in the avalanche. n of these congestion nodes have been added to the network at level n. At level $n+1$ the $(n+1)$th node is added—the grey square. To satisfy the conditions for an avalanche we require this node to fail. The condition for this is $\Lambda^*_{n+1} \geqslant \Lambda^*_n$, where Λ^*_n and Λ^*_{n+1} are the critical packet production rates for the network as it is at level n and at level $n+1$. For our purposes we want $\Lambda^*_{n+1} \approx \Lambda^*_n$. Apart from changing Λ_n, we can affect the load either by adding links between the new node (grey square) and the original network or by adding a new node that connects with the new congestion node and/or any of the other nodes (grey circles) introduced at level $n+1$. We carry on adding new nodes and links, following these rules, until the condition $\Lambda^*_{n+1} \geqslant \Lambda^*_n$ is satisfied. We then continue to level $n+2$ where the next square node is added.

3.1. Examples

A possible starting network is a star network. For a star the betweenness of the rays of the star (as defined in (2)) is given by $B_{\mathrm{r}} = N-1$; for the centre of the star the betweenness is $B_{\mathrm{c}} = (N-1)^2$. The centre of the star will become congested at the critical packet production rate $\Lambda^*{}_{\mathrm{c}} = (N-1)/B_{\mathrm{c}}$. In figure 2 the maximum betweenness (that is the betweenness of congestion node n) is plotted against network size. In this case output flow μ_v is assumed constant for all nodes. Squares show the maximum betweenness at each step of the growth; circles represent the

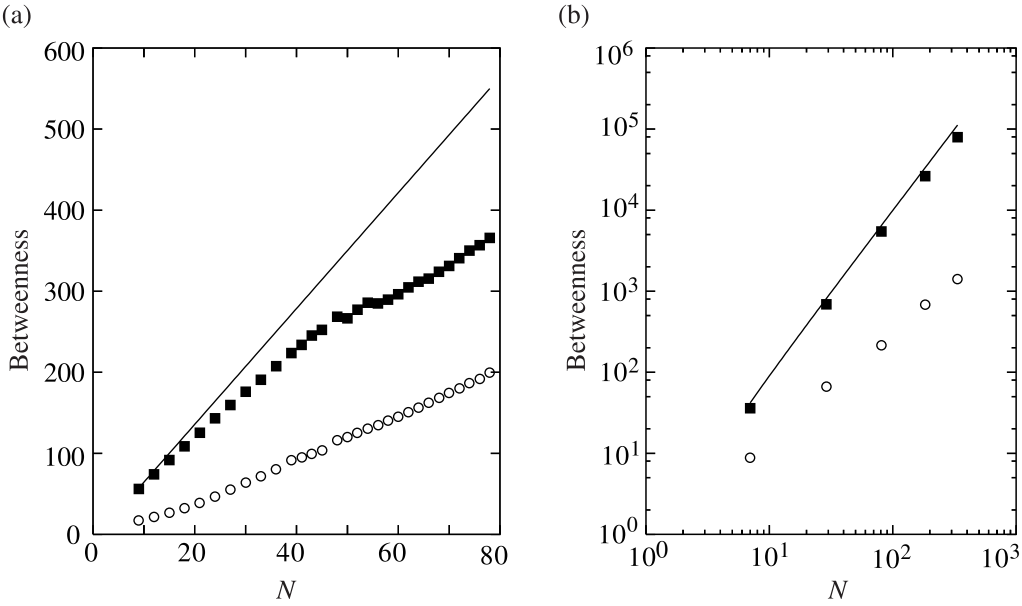

Figure 2. The maximum value of the betweenness centrality as a function of the number of nodes in (a) a network with total flow that increases with network size and (b) a network with a flow independent of network size. Solid squares show the maximum betweenness at each step of the network growth. Circles represent the lower bounds in $B_{\max}$, given by $B_{\max} \geqslant (N-1)\bar{\ell}$ of both (a) and (b). The solid lines represent the upper bounds: $B_{\max} \leqslant (N-1)/\Lambda^*$ for (a) and $B_{\max} \leqslant N(N-1)/(K\Lambda^*)$ for (b).

lower bound of maximum betweenness values, $B_{\max} \geqslant (N-1)\bar{\ell}$. The solid lines are the upper bounds of the betweenness. The two cases of section 2.2, where expressions for the upper and lower bounds are derived, are illustrated in figures 2(a) and (b). In figure 2(a) total flow increases with network size; in figure 2(b) total flow is independent of network size. The lower bound is the same in both cases: $B_{\max} \geqslant (N-1)\bar{\ell}$. The upper bound in figure 2(a) is $B_{\max} \leqslant (N-1)/\Lambda^*$; in figure 2(b) the upper bound is: $B_{\max} \leqslant N(N-1)/(K\Lambda^*)$. At each step in the building of the network the program searches for a network satisfying $\Lambda^*_{n+1} \approx \Lambda^*_n$ with the constraint that $\Lambda^*_{n+1} \geqslant \Lambda^*_n$ (or the avalanche will not occur). Finding a network satisfying these conditions was not always possible, especially in the case of figure 2(a). A network that becomes congested at the target Λ^* does not always exist and becomes harder to find as the network grows. This explains the divergence of $B_{\max}$ from the upper limit in figure 2(a). The upper bound is followed closely in figure 2(b), so the maximum betweenness is approximately proportional to the square of the network size in this case.

In figure 3 we show histograms of the degrees of the nodes in the network. As in figure 2, figure 3(a) shows data for a network in which total flow grows with network size; in figure 3(b) the total flow is independent of network size. In the first case there is not much variation in node degree. In the second case the degree distribution is skewed and has an exponential shape for low degree values, so this is a heterogeneous network in terms of node degree.

It is also possible to construct networks in which the output flow μ is not the same for all nodes. This makes it possible to build networks in which the majority of node failures triggered

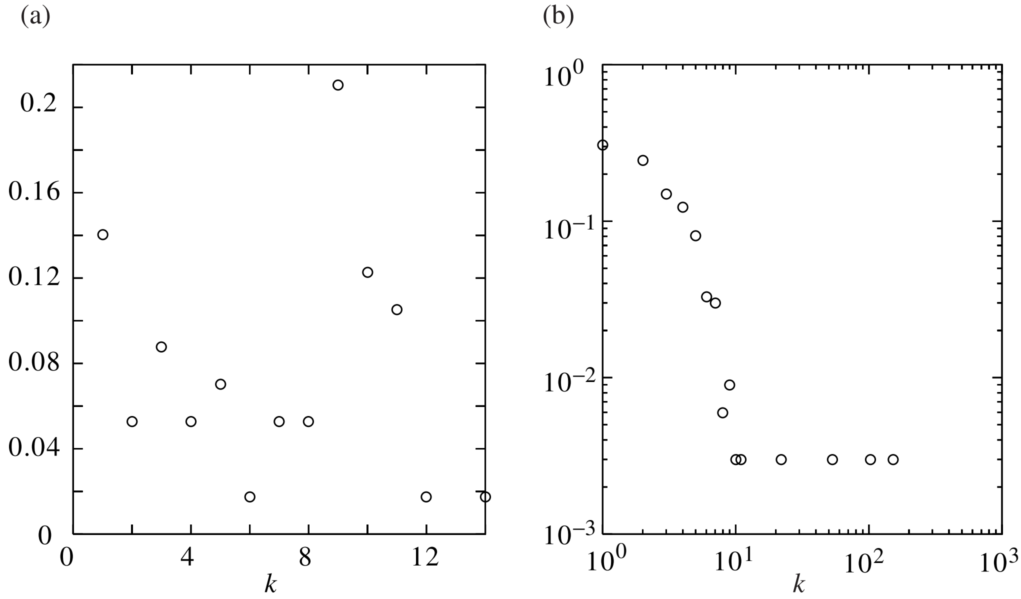

Figure 3. Histograms of the degree k for (a) a network with total flow that grows with the network size and (b) a network with total flow independent of the network size.

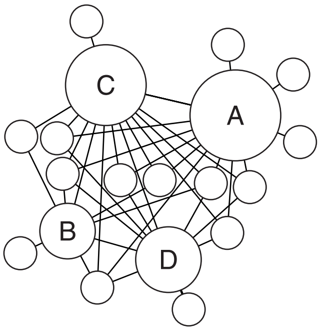

Figure 4. Catastrophic network with heterogeneous vertices.

by the avalanche happen at nodes having a large output flow; the remainder at nodes having a small output flow. This simulates man-made networks such as the Internet or power grids where a main server or an electrical substation has a large output flow and consequently more ‘importance’ in the network. Failure may begin with a node with high centrality (measured by betweenness), but the next node to fail in the avalanche may have a relatively small centrality, yet be fundamental to the propagation of the avalanche. In this case the node’s betweenness does not reflect its importance in the cascade sequence. This behaviour is illustrated in figure 4. Here nodes failed in the sequence A, B, C, D even though A, C and D can handle twice the flow B can. The radii of the nodes in the figure are proportional to the square root of their betweennesses. Clearly the order of failure is unrelated to the betweenness of a node.

4. Conclusions

We have presented a simple mechanism for building networks designed to fail catastrophically. The failure of nodes in the network is related to the node's output flow rate. The technique can be used to construct networks with nodes that have differing output flows, so we can produce a network with nodes that have low topological importance (or centrality), but are crucial in the avalanche-producing catastrophe.

In the case where total flow in the network increases linearly with network size, we find that the network formed has a small amount of heterogeneity in node degree distribution. This shows that catastrophic failure does not only occur in highly heterogeneous networks like the Internet. If all nodes have similar loads and are close to their failure threshold, then cascade failure is also possible in almost homogeneous networks.

The next stage in the work is to modify the technique so that the generated networks have more realistic topologies. In addition, our method applies to bufferless networks, we intend to extend it to account for queueing at nodes in the network as occurs in packet data networks. There is a need for more rigorous theoretical results to accompany this future work.

There are many other ways to extend our method. Other measures of centrality representing different flow mechanisms could be used, and routing mechanisms other than shortest path [13]–[17] might be considered. Another possibility is to allow the creation of edges between nodes that do not get congested.

Finally, we make the comment that usually, as the name implies, catastrophic failures are unwanted and efforts are made to prevent their occurrence. However, there are circumstances in which this property is desirable. In vehicle and shop windows, for example, tempered glass is used, partly because it is stronger, but also because it has the property of shattering into much safer small pieces when broken. In cases like this catastrophic failure might be seen as being 'engineered into' the material. Another example in which catastrophic failure would be desirable is that of criminal networks where one person's capture may result in the collapse of the whole network. These types of total catastrophic failure are similar to that seen in our current model.

Acknowledgment

This research was supported by the EPSRC, UK (EP/C520246/1).

References

[1] Barabási A-L and Albert R 2002 Statistical mechanics of complex networks *Rev. Mod. Phys.* **74** 47

[2] Strogatz S H 2001 Exploring complex networks *Nature* **410** 268

[3] Newman M E J 2003 The structure and function of complex networks *SIAM Rev.* **45** 167

[4] DeMarco C L 2001 Cascading network failure *IEEE Control Sys. Mag.* (December) 40

[5] Pereira L 2004 Cascade to black *IEEE Power Energy Mag.* **2** 54

[6] Watts D J 2002 A simple model of global cascades on random networks *Proc. Natl Acad. Sci. USA* **99** 5766

[7] Barabási A-L and Albert R 1999 Emergence of scaling in random networks *Science* **286** 509

[8] Motter A E and Lai Y-C 2002 Cascade-based attacks on complex networks *Phys. Rev.* E **66** 065102

[9] Nagel K and Schreckenberg M 1992 A cellular automaton model for freeway traffic *J. Phys. I (France)* **2** 2221

[10] Newman M E J 2003 A measure of betweenness centrality based on random walks *Preprint* cond-mat/0309045

[11] Ericsson M, Resende M G C and Pardalos P M 2002 A genetic algorithm for the weight setting problem in OSPF routing *J. Comb. Optim.* **6** 299

[12] Fortz B and Thorup M 2002 Optimizing OSPF/ISIS weights in a changing world *IEEE J. Sel. Areas Commun.* **20** 756

[13] Danila B, Yu Y, Marsh J A and Bassler K E 2006 Optimal transport on complex networks *Phys. Rev.* E **74** 046106

[14] Danila B, Yu Y, Marsh J A and Bassler K E 2007 Transport optimization on complex networks *Preprint* cond-mat/0701184

[15] Echenique P, Gómez-Gardeñes J and Moreno Y 2004 Improved routing strategies for Internet traffic delivery *Phys. Rev.* E **70** 056105

[16] Echenique P, Gómez-Gardeñes J and Moreno Y 2005 Dynamics of jamming transitions in complex networks *Europhys. Lett.* **71** 325

[17] Yan G, Zhou T, Hu B, Fu Z-Q and Wang B-H 2006 Efficient routing on complex networks *Phys. Rev.* E **73** 046108

[18] Sreenivasan S, Cohen R, López E, Toroczkai Z and Stanley H E 2006 Communication bottlenecks in scale-free networks *Preprint* cs.NI/0604023

[19] Holme P and Kim B J 2002 Vertex overload breakdown in evolving networks *Phys. Rev.* E **65** 066109

[20] Moreno Y, Gómez J B and Pacheco A F 2002 Instability of scale-free networks under node-breaking avalanches *Europhys. Lett.* **58** 630

[21] Zhao L, Park K and Lai Y-C 2004 Attack vulnerability of scale-free networks due to cascading breakdown *Phys. Rev.* E **70** 035101

[22] Freeman L C 1977 A set of measures of centrality based on betweenness *Sociometry* **40** 35

[23] Zhou T, Liu J-G and Wang B-H 2006 Notes on the algorithm for calculating betweenness *Chin. Phys. Lett.* **23** 2327

[24] Zhao L, Lai Y-C, Park K and Ye N 2005 Onset of traffic congestion in complex networks *Phys. Rev.* E **71** 026125

[25] Newman M E J 2001 Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality *Phys. Rev.* E **64** 016132

[26] Guimerà R, Díaz-Guilera A, Vega-Redondo F, Cabrales A and Arenas A 2002 Optimal network topologies for local search with congestion *Phys. Rev. Lett.* **89** 248701

[27] Guimerà R, Arenas A, Díaz-Guilera A and Giralt F 2002 Dynamical properties of model communication networks *Phys. Rev.* E **66** 026704