SIXTH FRAMEWORK PROGRAMME

Project contract no. 043363

MANMADE
Diagnosing vulnerability, emergent phenomena and volatility in man-made networks

SPECIFIC TARGETED PROJECT

NEST PATHFINDER
Sub-Priority Tackling Complexity in Science

M36: Deliverable 3.4 - Emergence simulator in generic graphs to mimic long-range coupling in networks

Revision [2]

Submission date: December, 2009

Start date of project: 1st of January 2007 Duration: 36 months

Lead author for this Report: W. Just (QMUL).

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

SUMMARY

The idea was to consider the development of networks that responded to the requirement of increased connectivity between vertices that experience correlated activity in some sense – this is the so-called Hebbian response . The paradigm for type of behaviour is found in neural networks where correlated behaviour usually results in improved connectivity between the neural centres for associated activity.
Our investigations have followed this principle in constructing network algorithms which emphasize connectivity response which produces graphs which are acutely prone to cascade breakdown. The networks are designed to breakdown catastrophically by cascade breakdowns. These networks can be characterized in terms of node degree distribution. The deliverable was basically a theoretical investigation. But the ability to characterize these graphs gives the potential for finding a measure of how much real networks differ from these extreme contructs . This would be a further tool in characterising or measuring the vulnerability of real networks to cascade breakdown.
It is quite well established that overloading transmission lines in transport or energy networks can trigger a cascade of failures resulting in a critical breakdown. It is one of the main questions of this deliverable to investigate which features of the connectivity and of the dynamics are the cause for such a behaviour, and ultimately to propose countermeasures which can be employed to prevent such catastrophes.
In particular, we focus on generating and identifying structures which support and sustain cascading breakdown of complex infrastructure networks.
The main idea for this purpose is to follow a cascading breakdown in reverse, thus generating a critical infrastructure network, and finally to identify its topological and dynamical characteristics.

A standard approach to simulate cascading breakdowns consists in identifying critical connections which suffer from overload and closing down such critical links. Redistribution of the loads may result in additional critical transmission lines causing further overload and resulting in a cascading breakdown. Although one can envisage other more dynamical approaches, e.g., by employing power flow models or master equations on evolving graphs we stay here with the aforementioned simpler topological set up. As a collaborative effort between mathematics and electronic engineering at QMUL we have implemented such an idea and developed a growth algorithm which generates networks showing critical failure by running cascading breakdowns in reverse.

Dissemination:

The contribution to D3.4 have evolved over the last few years and have finally resulted in two manuscripts which have been already published in international peer reviewed journals (annex 1,2) and another preprint which summarises the concept (annex 3).

Impact:

The identification of mechanisms resulting in cascading breakdowns and the development of countermeasures have an obvious technological and economic relevance. The first preliminary

steps were motivated by studies in telecommunication and electricity networks and are now going to be applied in the context of other infrastructure networks such as gas and transport. We expect considerable benefit from a combination of the results of D3.3 and D3.4 to inform policy makers about strategies to improve resilience of infrastructure networks.

Annex 1

M. Woolf, Z. Huang, and R. Mondragon, Building catastrophes: networks designed to fail by avalanche-like breakdown, New J. Phys. 9 (2007) 174

The paper was prepared by the department of electronic engineering, QMUL

Annex 2

R. Mondragon, Topological modelling of large networks, Phil. Trans. Roy. Soc. A (2008) 366, 1931-1940.

The paper was prepared by the department of electronic engineering, QMUL

Annex 3

Z. Huang and R. Mondragon, Fragile networks

The manuscript "Fragile networks" was prepared by the department of electronic engineering, QMUL.

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 **2**
2. Preliminaries **3**
2.1. Definitions and network measures 3
2.2. Load and congestion at a node 4
2.3. Avalanches and betweenness 5
3. Building catastrophes **6**
3.1. Examples 6
4. Conclusions **9**
Acknowledgment **9**
References **9**

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 $B_{\max} \leqslant (N-1)/\Lambda^*$.

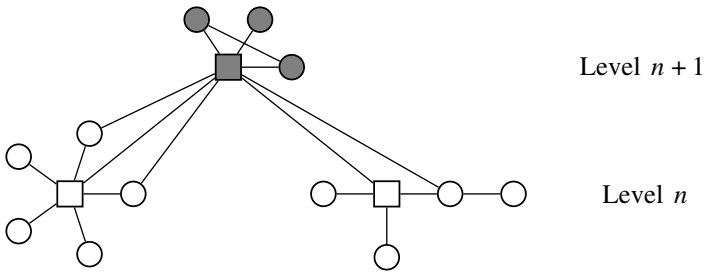

Figure 1. Building the network. The grey vertices are the new nodes introduced at step $n + 1$. The square vertices are the nodes that will get congested and removed when the avalanche occurs. Note that all connections from the new nodes to the nodes of stage n are made via the grey square vertex.

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 $B_r = N - 1$; for the centre of the star the betweenness is $B_c = (N-1)^2$. The centre of the star will become congested at the critical packet production rate $\Lambda^*{}_c = (N-1)/B_c$. 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

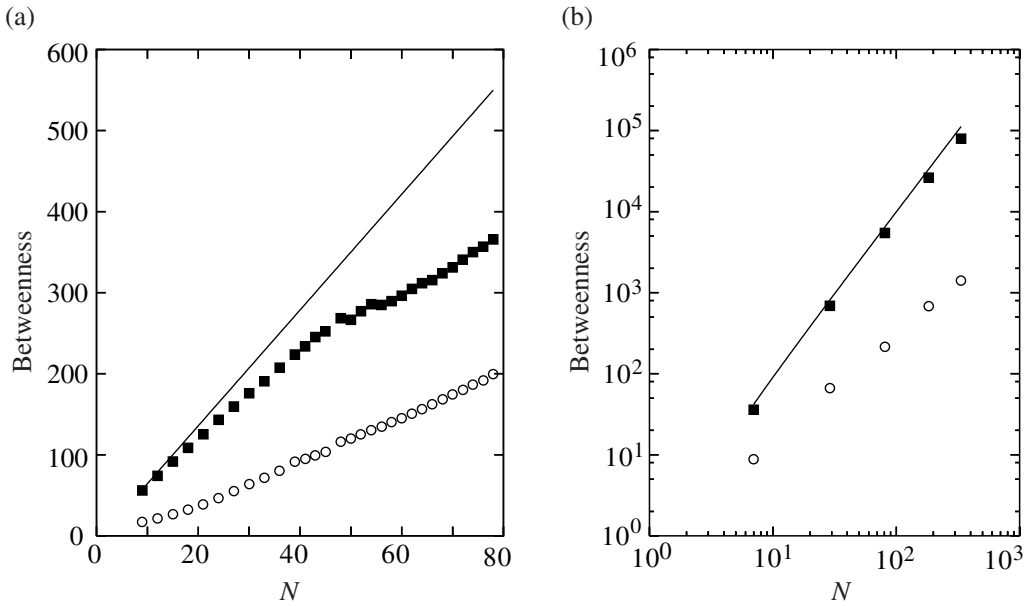

Figure 2. The maximum value of the betweenness centrality as a function of the number of nodes in (a) a network with total flow that increases with network size and (b) a network with a flow independent of network size. Solid squares show the maximum betweenness at each step of the network growth. Circles 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

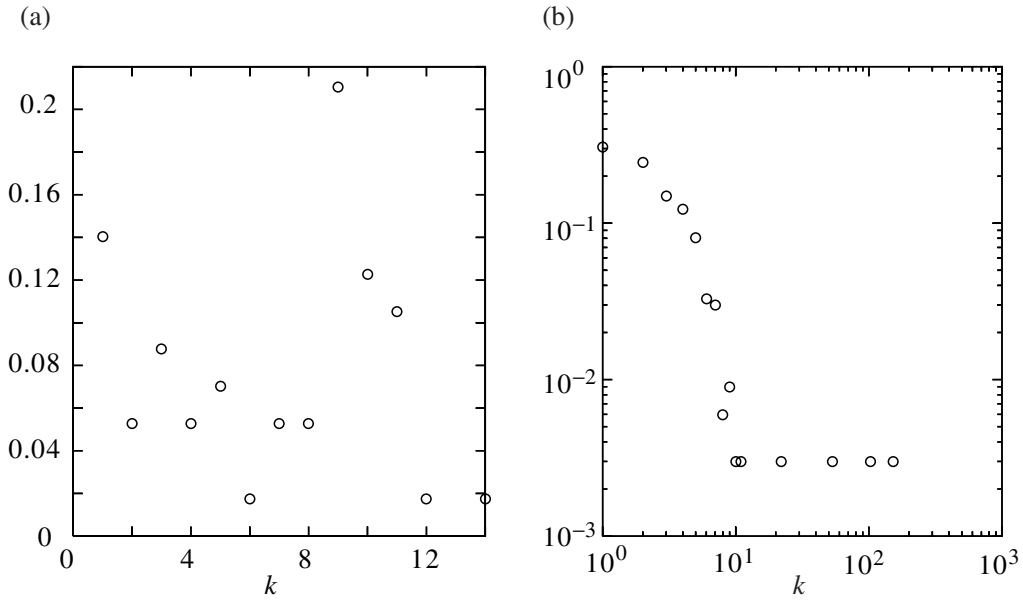

Figure 3. Histograms of the degree k for (a) a network with total flow that grows with the network size and (b) a network with total flow independent of the network size.

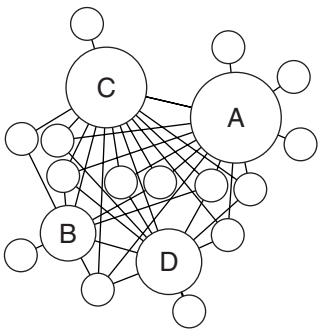

Figure 4. Catastrophic network with heterogeneous vertices.

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

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A

Phil. Trans. R. Soc. A (2008) **366**, 1931–1940
doi:10.1098/rsta.2008.0008
Published online 6 March 2008

Topological modelling of large networks

By Raúl J. Mondragón*

Department of Electronic Engineering, Queen Mary University of London, Mile End Road, London E1 4NS, UK

In a complex network, there is a strong interaction between the network's topology and its functionality. A good topological network model is a practical tool as it can be used to test 'what-if' scenarios and it can provide predictions of the network's evolution. Modelling the topology structure of a large network is a challenging task, since there is no agreement in the research community on which properties of the network a model should be based, or how to test its accuracy. Here we present recent results on how to model a large network, the autonomous system (AS)-Internet, using a growth model. Based on a nonlinear preferential growth model and the reproduction of the network's rich club, the model reproduces many of the topological characteristics of the AS-Internet. We also identify a recent method to visualize the network's topology. This visualization technique is simple and fast and can be used to understand the properties of a large complex network or as a first step to validate a network model.

Keywords: Internet; network models; visualization

1. Introduction

A network can be described as a set of nodes and links. An accurate description of how the nodes are connected via the links is important because *form* and *functionality* are closely related. Modelling large complex networks has practical applications. Models can provide realistic network scenarios for simulations and can be used to predict network evolution. As specific networks have different characteristics, we tend to avoid general topological models and select properties to model based on the problem at hand. Here we consider the Internet at the autonomous system (AS) level.

The Internet can be described at the router or AS level. At the router level, the nodes and links of the network represent physical entities. The nodes describe the routers and switches managing the passage of traffic through the network. The links represent the different physical connections between the nodes, for example, optical fibres, copper, wires, etc., and have specific directions between the endpoint nodes. At the router level, a basic topological model of the Internet should include the geographical position of the nodes and links, the capacity of the links and the direction that the Internet traffic follows. For management purposes, the Internet is divided into sub-networks. Each sub-network adheres to common routing conventions, usually the interior gateway

*r.j.mondragon@elec.qmul.ac.uk

One contribution of 16 to a Discussion Meeting Issue 'Networks: modelling and control'.

protocol. The management of a sub-network and its routers falls under one administrative entity called an AS that should exhibit to other ASs a coherent interior routing plan and the destinations reachable through the AS. At the AS level, the Internet can be considered in an abstract space where the relevant property is the connectivity between ASs. At this level, we tend to disregard many physical properties of the network like the geographical location of the ASs, which could be in different continents, or the direction of the links and their capacities.

For the Internet, there is considerable data describing it at the router and AS levels (Cooperative Association for Internet Data Analysis (CAIDA) 2007, http://www.caida.org). In §2, we introduce some of the topological properties obtained from the measurements that are used in the development of network models.

There are two general approaches to model a network (Bu & Towsley 2002; Dorogovtsev & Mendes 2003; Costa *et al.* 2007; Krioukov *et al.* 2007): static models (Doar 1996; Zegura *et al.* 1996; Calvert *et al.* 1997; Winick & Jamin 2002) based on random networks and dynamical models based on network growth models. The latter are considered to be the more promising as, if correct, they can describe the evolution of the network (Willinger *et al.* 2002; Krioukov *et al.* 2007). There are two kinds of dynamical models: *descriptive* models based on matching various topological properties of a network are used to study which topological properties give a good description of a network; and *explanatory* models that attempt to simulate the core principles and factors responsible for the network's structure and evolution, in particular the router network (Willinger *et al.* 2002). A proper validation of all the network models is lacking due to the limited quality of the available measures (Krioukov *et al.* 2007). In §3, we describe a dynamical descriptive network model that reproduces many properties of the AS-Internet.

Section 4 describes a recent visualization technique that can be used to understand the topological properties of a network or as a first step to validate a network model and conclusions are given in §5.

2. Topological description of a network

The AS-Internet is described as an undirected graph $\mathcal{G}=(\mathcal{N}, \mathcal{L})$, where $\mathcal{N}=\{n_i\}$ is a finite set of N nodes and $\mathcal{L}=\{l_i\}$ is a finite set of L links. Two nodes are neighbours if there is a link joining them. The connectivity of the nodes is described by the adjacency matrix whose a_{ij} entry is 1 if node n_i is adjacent to node n_j and 0 otherwise. For undirected graphs, $a_{ij}=a_{ji}$. The degree k of a node is the number of neighbours that a node has, $k_i=\sum_j a_{ij}$. The degree is the principal parameter to characterize a network. Two of the simplest properties of a network are its maximum degree $k_{\max}=\max\{k_i\}$, $i=1, \ldots, N$ and its average degree $\langle k\rangle=\sum_{j=1}^{N} k_j/N$.

A first step to describe and discriminate between different networks is to measure the degree distribution $P(k)$; the fraction of nodes in the network with degree k. For the AS-Internet, Faloutsos *et al.* (1999) found that its degree distribution decays as the power law $P(k)\sim k^{-\gamma}$, $\gamma=2.1$. This means that the majority of the nodes have few neighbours and there is a small set of nodes that

have a very large number of neighbours. Networks with a power-law decay in their degree distribution are known as *scale free* (Barabási & Albert 1999). This kind of decay is also present in other technological, biological and sociological networks (Dorogovtsev & Mendes 2003).

The degree distribution gives only partial information about the network structure. A better description can be obtained from the correlations between the degrees of different nodes (Pastor-Satorras *et al.* 2001; Newman 2002). In a finite network, this correlation is defined by the degree–degree distribution

$$P(k,k') = \frac{1}{N^2}\left\langle \sum_{i,j=1}^{N} \delta_{k_i,k} a_{ij} \delta_{k_j,k'} \right\rangle; \tag{2.1}$$

the probability that an arbitrary link connects a node of degree k with a node of degree k'. In the equation, δ_{ij} is the Kronecker delta. The degree–degree correlation can also be described using the conditional probability that a node with degree k has a neighbour with degree k'

$$P(k'|k) = \frac{\langle k \rangle P(k,k')}{kP(k)}, \tag{2.2}$$

where $\sum_{k'} P(k'|k) = 1$. In scale-free networks due to the small number of nodes with high degree and the finite size of the network, it is not possible from the network's measurements to evaluate accurately the degree–degree distribution. Hence, the structure of the network is characterized using different projections of the degree–degree correlation.

One way to characterize a network is by comparing it with a random network. To obtain a meaningful comparison, the random network is restricted such that its degree distribution $P(k)$ is the same as the network under study (Maslov & Sneppen 2002). The random network is obtained by randomly reshuffling link pairs of the original network with the restriction that the reshuffling process should not change the degree distribution. By comparing a network with its randomized version, scale-free networks can be classified into assortative, disassortative and neutral networks (Newman 2002). Social networks tend to be assortative, in which high-degree nodes prefer to attach to other high-degree nodes and low-degree nodes to low-degree nodes. Information networks (e.g. the World Wide Web and the AS-Internet) and biological networks have been classified as disassortative networks, in which high-degree nodes tend to connect with low-degree ones.

A projection of the degree–degree correlation used to describe the structure of the network is the average degree of the nearest neighbours. If k is the degree of a node, then

$$k_{\mathrm{nn}}(k) = \sum_{k'=1}^{k_{\max}} k' P(k'|k) \tag{2.3}$$

is its average degree of nearest neighbours (Pastor-Satorras *et al.* 2001). If $k_{\mathrm{nn}}(k)$ is an increasing function of k the network is assortative; if $k_{\mathrm{nn}}(k)$ is a decreasing function of k the network is disassortative.

While the AS-Internet is disassortative (Pastor-Satorras *et al.* 2001; Vázquez *et al.* 2002), this property does not describe the explicit connectivity between the high-degree nodes. The high-degree nodes are also referred to as 'rich nodes'. If the rich nodes share many connections the set containing these nodes is known

as the 'rich club' (Zhou & Mondragón 2004*b*). The AS-Internet has a densely interconnected rich club that plays a dominant role in the functionality of the network. Realistic models of the Internet should reproduce this hub structure.

If the rich nodes are the r best-connected nodes in the network then their connection density is measured by the rich-club coefficient (Zhou & Mondragón 2004*b*) $\Phi(r) = 2E_r/(r(r-1))$, where E_r is the number of links among the top r richest nodes and $r(r-1)/2$ is the maximum number of links that these nodes can share. If $\Phi(r)=0$ there is no club at all; if $\Phi(r)=1$ the members of the club form a clique. As a function of the node's degree, the rich-club coefficient is $\phi(k) = 2E_k/(N_k(N_k-1))$ (Colizza *et al.* 2006), where N_k is the number of nodes with degree equal to or higher than k and E_k is the number of links among these N_k nodes. The rich-club coefficient is another projection of the degree–degree distribution as its satisfies (Colizza *et al.* 2006)

$$\phi(k) = \frac{2N\langle k\rangle \sum_{i=k}^{k_{\max}} \sum_{j=k}^{k_{\max}} P(i,j)}{\left(N \sum_{i=k}^{k_{\max}} P(i)\right)\left(N \sum_{i=k}^{k_{\max}} P(i) - 1\right)}. \tag{2.4}$$

Alternatively, from the definition of the rich-club coefficient,

$$\Delta L_k = \frac{1}{2}(\phi(k+1)N_{k+1}(N_{k+1}-1) - \phi(k)N_k(N_k-1)) \tag{2.5}$$

is the number of links that have at one end a node with degree k and at the other end a node with degree k', with $k' \geq k$. In terms of the conditional probability

$$\Delta L_k = \left(N \sum_{i=k}^{k+1} P(i)\right)\left(\sum_{k'=k}^{k_{\max}} P(k'|k) - \frac{1}{2}P(k+1|k)\right). \tag{2.6}$$

3. Models

The main property that any model tends to reproduce is the degree distribution $P(k)$. $P(k)$ apart, there is no agreement on which other statistical properties an Internet model should be based (Tangmunarunkit *et al.* 2002; Alvarez-Hamelin *et al.* 2005; Rodrigues *et al.* 2007). In a dynamical network model, starting from a small seed network, new links and nodes are added to the network until it evolves to the specified size. The difficulty when developing a dynamical model is that these should evolve networks to match specific topological characteristics. A starting point in generating networks with power-law decay in their degree distribution is to use the Barabási–Albert (BA) model (1999). The model grows a network using a preferential growth mechanism: starting with a small random network, the system grows by attaching a new node with m links to m different nodes that are already present in the system ($m=3$ to obtain Internet-like networks); the attachment is preferential because the probability that a new node will connect to node i with degree k_i is

$$\Pi(i) = \frac{k_i}{\sum_j k_j}. \tag{3.1}$$

As a model of the AS-Internet, the BA model has several limitations. The model generates a power-law degree distribution with exponent $\gamma=3$ compared with $\gamma=2.1$ obtained from the measurements. The BA model also creates networks where the value of the maximum degree $k_{\max}$ is too small compared with the value measured in the Internet. Nevertheless, the BA model can be extended to obtain degree distributions with other power-law exponents (Krapivsky *et al.* 2001; Albert & Barabási 2002; Dorogovtsev & Mendes 2003). However, a network model based solely on the reproduction of the power-law exponent of the degree distribution has its limitations as it will not describe the Internet hierarchical structure (Newman 2002; Pastor-Satorras & Vespignani 2004) neither will it reproduce the rich-club connectivity of the AS-Internet (Zhou & Mondragón 2004*a*).

Equations (2.5) and (2.6) show that a model that recreates the rich-club connectivity $\phi(k)$ of the network under study will also generate a good approximation of the network's degree–degree distribution $P(k, k')$ (Krioukov & Krapivsky 2006; Zhou & Mondragón 2007). It is possible to modify the BA model to generate networks with a rich club by adding internal links as the network evolves (Dorogovtsev & Mendes 2000; Bu & Towsley 2002; Bar *et al.* 2004; Caldarelli *et al.* 2004; Zhou & Mondragón 2004*a*). This addition of internal links in the model is supported by observations of the Internet evolution (Pastor-Satorras *et al.* 2001; Vázquez *et al.* 2002). Simon (1955) introduced a model based on the addition of new nodes and the addition of new links between nodes that belonged to the same class, where a class is the set of nodes with the same degree. Simon's model generates networks with a power-law scaling in the node degree. This growth mechanism allows different growth rates for different classes of nodes and hence it can create a well-connected rich club (Bornholdt & Ebel 2001).

The new growth mechanism has two components, a new node attaches with m old nodes or m new links appear between old nodes. In both cases, the attachment is done using the BA growth model or a modification of the BA model. For example, Bu & Towsley (2002) used a generalized linear preference model with $\Pi(i)=(k_i-\beta)/(\sum_j k_j-\beta)$, where m and β are parameters that are adjusted to produce the correct power-law decay. The Bu & Towsley model can create a well-connected rich club but generates networks with a maximum degree $k_{\max}$ smaller than the one measured in the Internet. It is possible to increase the maximum degree $k_{\max}$ produced by a model using the nonlinear preferential attachment (Dorogovtsev & Mendes 2000; Krapivsky *et al.* 2001)

$$\Pi(i)=\frac{k_i^{\alpha}}{\sum_j k_j^{\alpha}}, \quad \alpha>1. \tag{3.2}$$

In this case, the rich nodes get all the connections and the degree distribution $P(k)$ does not decay as a power law.

From the Internet history data, it is known that the probability that a new node links with a low-degree node follows the linear preferential attachment given by equation (3.1) (Pastor-Satorras *et al.* 2001; Vázquez *et al.* 2002), whereas high-degree nodes have a stronger ability of acquiring new links than predicted by equation (3.1) (Chen *et al.* 2002). Taking into account these

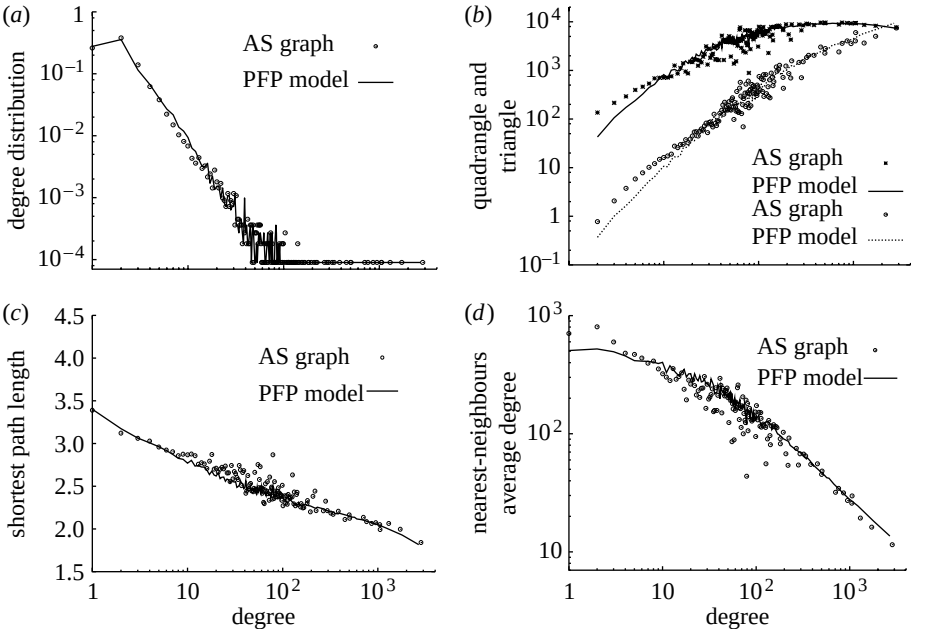

Figure 1. Comparison of topological properties of the AS-Internet and the PFP model (Zhou & Mondragón 2004*a*): (*a*) the degree distribution, (*b*) distribution of triangles and quadrangles, (*c*) distribution of shortest paths and (*d*) nearest-neighbour average degree k_{nn}.

observations the nonlinear preferential attachment

$$\Pi(i) = \frac{k_i^{1+\delta \ln k_i}}{\sum_j k_j^{1+\delta \ln k_j}} \tag{3.3}$$

has been used to model the AS-Internet (Zhou & Mondragón 2004*a*; Zhou 2006; Zhou *et al.* 2007). The function $f(x) = 1 + \delta \ln x$ was used because it describes the strength of the preferential attachment with only one parameter. The parameter δ is set such that maximum degree $k_{\max}$ generated by the model matches the one observed in the Internet. This model, referred to as the positive-feedback preference (PFP) model, reproduces many of the properties measured in the Internet (figure 1). In the model, the rich club is generated by the addition of new links between old nodes. The degree distribution $P(k)$ obtained from computer simulations has a pre-asymptotic power-law decay. The exponent of the power law depends on the addition of new links between old nodes and the preferential attachment (Zhou 2006). The PFP model is one of the most successful models describing the Internet (Mahadevan *et al.* 2005). However, we do not know if the model can predict the future shape of the Internet. Krioukov & Krapivsky (2006) noted that the PFP model does not produce degree distributions with asymptotic power-law decay. The power law observed in the model is pre-asymptotic and it is the modelling of the rich club that is responsible for this pre-asymptotic power-law decay.

We finish this section with a cautionary note. In the Internet, the network's connectivity can be obtained by direct probing of the network or by the routing tables. Direct probing is done by recording the nodes that are visited by a packet

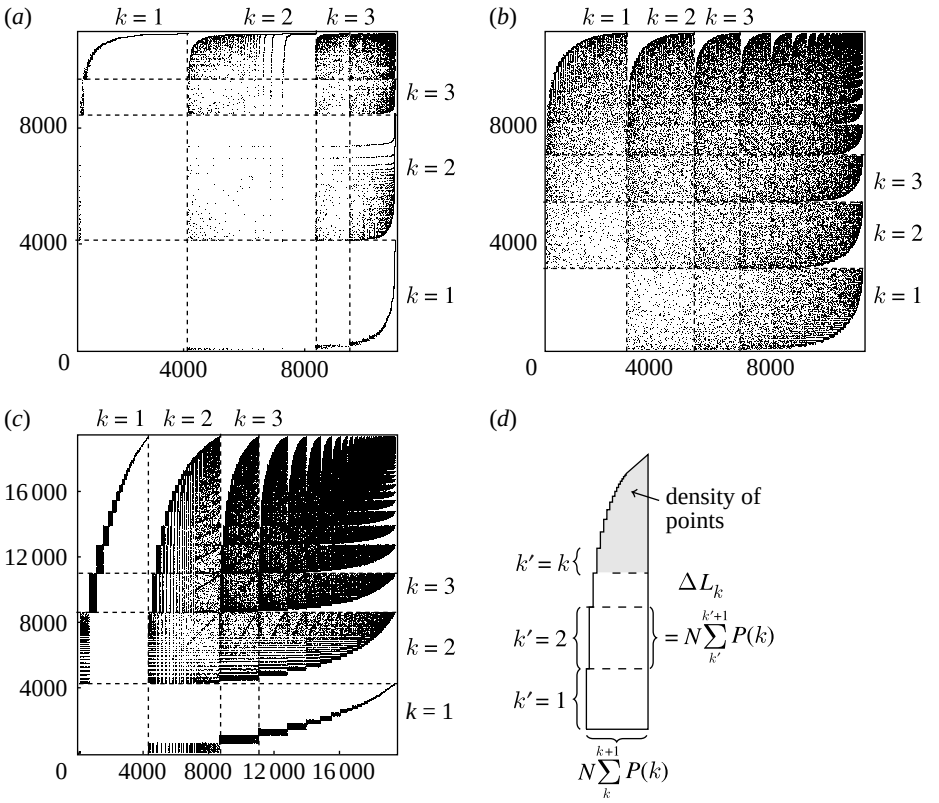

Figure 2. (*a*) The AS-Internet bitmap. (*b*) A BA network bitmap; the network has the same number of nodes as the AS-Internet. (*c*) The router Internet network; the network has 192 244 nodes. (*d*) The characteristic component of the router graph.

travelling the network. The routing tables describe which nodes a packet should visit when crossing the network. Both measurement methods have several limitations as they can create a skewed description of the network (Petermann & de los Rios 2004). It is also the case that so far, all the measurements of the Internet are incomplete (Krioukov *et al.* 2007) so any model based on these measurements will not represent the actual structure of the whole Internet.

4. Visualization

A method to visualize if a network generated by a model *looks* similar to the original network would be a useful tool to validate a model. As networks are very large, drawing them as a set of discs joined by lines is not helpful; the density of connections obscures the network features. Recently, a visualization of the adjacency matrix has been used to distinguish different networks (Chakrabarti *et al.* 2007; Guo *et al.* 2007). As the labelling of the nodes is arbitrary, the idea is that the label of a node should be related to its degree. Then a linear order relationship, based on the connectivity, is used to arrange the node labels (Nagle 1966). Using this labelling, the adjacency matrix is plotted as a binary diagram: white if there is no link between node i and j; black otherwise. The binary

diagram gives an overall impression of the network connectivity. The *degree tuple* of a node is defined as $\{k_{i,0}, k_{i,1}, \ldots, k_{i,j}\}$, where $k_{i,0}$ is the degree of node i; $k_{i,j}$, $j=1, \ldots, n$ is the degree of its neighbours; and $j<m$ if $k_{i,j}>k_{i,m}$. The nodes are labelled in increasing order of their degree, the node with lowest degree is labelled 1. If two nodes have the same degree the node with the highest degree neighbour will rank higher. If the highest degree of the neighbours is the same, the second highest degree neighbour is used for the ranking and so on until all the neighbours are considered.

Figure 2*a–d* shows the plot for the AS-Internet, a model of the AS-Internet using the BA model, the router Internet and a sketch of a characteristic component of the router Internet. The bitmaps of the networks look like a fractal structure constructed by the repetition and scaling of a characteristic component. The dimensions of the component in figure 2*d* are related to properties of the network in the following way. The length of its base is the number of nodes with degree k given by $N\sum_{i=k}^{k+1} P(i)$. The height of the steps is equal to the number of nodes with degree k', again given by $N\sum_{i=k'}^{k'+1} P(i)$. The tread of the k'th step is given by the number of links that have degree k at one end and degree less than k' at the other end. The density of points inside the main component is related to the conditional probability $P(k'|k)$. The density of points in the tip of the component is related to the rich-club coefficient via $\Delta L(k)$ (see equation (2.5)).

For networks like the Internet, it is known that the degree–degree distribution $P(k', k)$ gives a very good description of the network structure (Mahadevan *et al.* 2006). What the bitmap diagrams show are features of the whole network that are related to the degree–degree distribution; our cognitive response is to integrate this information as patterns. Different patterns correspond to different networks with different degree–degree distribution. In figure 2, the BA network was produced to model the AS-Internet. From the scaling of the characteristic component, it is clear that the BA model does not reproduce the scaling behaviour of the AS-Internet. The density of points in the BA network is more evenly distributed than in the AS-Internet, reflecting that the BA model generates neutral networks compared with the AS-Internet which is disassortative. The router Internet shows a feature not present in the AS-Internet and BA network, a dense number of points aligned in diagonal lines. This feature is present because the network is assortative (Echenique *et al.* 2005), high-degree nodes tend to connect with high-degree nodes and low-degree nodes with low-degree nodes.

5. Conclusions

The starting point for a model is to describe the network's degree distribution. This has been the approach used by many researchers to create a model of the AS-Internet. However, the extension of these models to reproduce other characteristics of the network has been erratic. In part, this is because we do not know which basic topological characteristics a model should reproduce. From our experience trying to model the AS-Internet, a starting point to obtain a good model of a scale-free network is to recreate the rich-club connectivity of the network under study. The rich-club connectivity is simple to measure and a model that recreates this connectivity will also give a good approximation to the degree–degree distribution.

The validation of a model usually means the comparison of several topological characteristics which can be time consuming. The visualization of the adjacency matrix based on a linear order relationship between the node connectivity is a good initial step in assessing the validity of a model. It is computationally fast and cheap.

The author would like to thank the EPSRC EP/C520246/1 for support.

References

Albert, R. & Barabási, A.-L. 2002 Statistical mechanics of complex networks. *Rev. Mod. Phys.* **74**, 47–97. (doi:10.1103/RevModPhys.74.47)

Alvarez-Hamelin, J.-I., Dall'Asta, L., Barrat, A. & Vespignani, A. 2005 k-core decomposition: a tool for the visualization of large scale networks. In *Advances in neural information processing systems 18*. Cambridge, MA: MIT Press. (http://arxiv.org/abs/cs/0504107)

Bar, S., Gonen, M. & Wool, A. 2004 An incremental superlinear preferential Internet topology model. In *Passive and Active Network Measurement: 5th International Workshop, PAM'04*, vol. 3015 (eds C. Barakat & I. Pratt), pp. 53–62. Springer Lecture Notes in Computer Science. Berlin, Germany: Springer.

Barabási, A. & Albert, R. 1999 Emergence of scaling in random networks. *Science* **286**, 509–512. (doi:10.1126/science.286.5439.509)

Bornholdt, S. & Ebel, H. 2001 World-wide web scaling exponent from Simon's 1955 model. *Phys. Rev. E* **64**, 035104. (doi:10.1103/PhysRevE.64.035104)

Bu, T. & Towsley, D. 2002 On distinguishing between Internet power law topology generators. In *Proc. INFOCOM 2002. 21st Ann. Joint Conference of the IEEE Computer and Communications Societies*. IEEE, vol. 2, pp. 638–647. (doi:10.1109/INFCOM.2002.1019309)

Caldarelli, G., de los Rios, P. & Pietronero, L. 2004 Generalized network growth: from microscopic strategies to the real Internet properties. (http://arXiv:cond-mat/0307610v1)

Calvert, K. L., Doar, M. B. & Zegura, E. W. 1997 Modeling Internet topology. *IEEE Commun. Mag.* **35**, 160–163. (doi:10.1109/35.587723)

Chakrabarti, D., Faloutsos, C. & Zhanet, Y. 2007 Visualization of large networks with min-cut plots, A-plots and R-MAT. *Int. J. Hum. Comput. Stud.* **65**, 434–445. (doi:10.1016/j.ijhcs.2006.11.002)

Chen, Q., Chang, H., Govindan, R., Jamin, S., Shenker, S. J. & Willinger, W. 2002 The origin of power laws in Internet topologies (revisited). In *Proc. INFOCOM 2002. 21st Ann. Joint Conference of the IEEE Computer and Communications Societies*. IEEE, vol. 2, pp. 608–617. (doi:10.1109/INFCOM.2002.1019306)

Colizza, V., Flammini, A., Serrano, M. A. & Vespignani, A. 2006 Detecting rich-club ordering in complex networks. *Nat. Phys.* **2**, 110–115. (doi:10.1038/nphys209)

Costa, L. da F., Rodrigues, F. A., Travieso, G. & Villas Boas, P. R. 2007 Characterization of complex networks: a survey of measurements. *Adv. Phys.* **56**, 167–242. (doi:10.1080/00018730601170527)

Doar, M. 1996 A better model for generating test networks. In *Proc. Global Telecommunications Conference, GLOBECOM '96. Communications: The Key to Global Prosperity*, pp. 86–93. (doi:10.1109/GLOCOM.1996.586131)

Dorogovtsev, S. N. & Mendes, J. F. 2000 Scaling behaviour of developing and decaying networks. *Europhys. Lett.* **52**, 33–39. (doi:10.1209/epl/i2000-00400-0)

Dorogovtsev, S. N. & Mendes, J. F. 2003 *Evolution of networks: from biological nets to the Internet and WWW*. Oxford, UK: Oxford University Press.

Echenique, P., Gómez-Gardeñes, J., Moreno, Y. & Vázquez, A. 2005 Distance-d covering problems in scale-free networks with degree correlations. *Phys. Rev. E* **71**, 035102. (doi:10.1103/PhysRevE.71.035102)

Faloutsos, M., Faloutsos, P. & Faloutsos, C. 1999 On power-law relationships of the Internet topology. *Comput. Commun. Rev.* **29**, 251–262. (doi:10.1145/316188.316229)

Guo, Y., Chen, C. & Zhou, S. 2007 Topology visualisation tool for large-scale communications networks. *Electron. Lett.* **43**, 597–598. (doi:10.1049/el:20070514)

Krapivsky, P. L., Rodgers, G. J. & Redner, S. 2001 Degree distributions of growing networks. *Phys. Rev. Lett.* **86**, 5401–5404. (doi:10.1103/PhysRevLett.86.5401)

Krioukov, D. & Krapivsky, P. 2006 Power laws as a pre-asymptotic regime of the PFP model. See http://www.caida.org/publications/presentations/2006/isma0605.dima.

Krioukov, D., Chung, F., Claffy, K. C., Fomenkov, M., Vespignani, A. & Willinger, W. 2007 The workshop on Internet topology (WIT) report. *ACM SIGCOMM Comput. Commun. Rev.* (*CCR*) **37**, 69–73. (http://www.caida.org/publications/papers/2006/wit/wit.pdf)

Mahadevan, P., Krioukov, D., Fomenkov, M., Huffaker, B., Dimitropoulos, X., Claffy, K. C. & Vahdat, A. 2005 Lessons from three views of the Internet topology: technical report, CAIDA. See http://www.caida.org/outreach/papers/2005/tr-2005-02/.

Mahadevan, P., Krioukov, D., Fomenkov, M., Dimitropoulos, X., Claffy, K. C. & Vahdat, A. 2006 The Internet AS-level topology: three data sources and one definitive metric. *SIGCOMM Comput. Commun. Rev.* **36**, 17–26. (doi:10.1145/1111322.1111328)

Maslov, S. & Sneppen, S. 2002 Specificity and stability in topology of protein networks. *Science* **296**, 910–913. (doi:10.1126/science.1065103)

Nagle, J. F. 1966 On ordering and identifying linear graphs. *J. Math. Phys.* **7**, 1588–1592. (doi:10.1063/1.1705069)

Newman, M. E. J. 2002 Assortative mixing in networks. *Phys. Rev. Lett.* **89**, 208701. (doi:10.1103/PhysRevLett.89.208701)

Pastor-Satorras, R. & Vespignani, A. 2004 *Evolution and structure of the Internet—a statistical physics approach*. Cambridge, UK: Cambridge University Press.

Pastor-Satorras, R., Vázquez, A. & Vespignani, A. 2001 Dynamical and correlation properties of the Internet. *Phys. Rev. Lett.* **87**, 258701. (doi:10.1103/PhysRevLett.87.258701)

Petermann, T. & de los Rios, P. 2004 Exploration of scale-free networks: do we measure the real exponents? *Eur. Phys. J. B* **38**, 201–204. (doi:10.1140/epjb/e2004-00021-5)

Rodrigues, F. A., Villas Boas, P. R., Travieso, G. & Costa, L. da F. 2007 Seeking the best Internet model. (http://arXiv:0706.3225v1)

Simon, H. A. 1955 On a class of skew distribution functions. *Biometrika* **42**, 425–440.

Tangmunarunkit, H., Govindan, R., Jamin, S., Shenker, S. & Willinger, W. 2002 Network topology generators: degree-based vs. structural. In *Proc. 2002 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 147–159. New York, NY: ACM Press. (doi:10.1145/633025.633040)

Vázquez, A., Pastor-Satorras, R. & Vespignani, A. 2002 Large-scale topological and dynamical properties of the Internet. *Phys. Rev. E* **65**, 066130. (doi:10.1103/PhysRevE.65.066130)

Willinger, W., Govindan, R., Jamin, S., Paxson, V. & Shenker, S. 2002 Scaling phenomena in the Internet: critically examining criticality. *Proc. Natl Acad. Sci. USA* **99**, 2573–2580. (doi:10.1073/pnas.012583099)

Winick, J. & Jamin, S. 2002 Inet-2.0 Internet topology generator. Technical report UM-CSE-TR-456-02, University of Michigan, Ann Arbour.

Zegura, E., Calvert, K. & Bhattacharjee, S. 1996 How to model an Internet network. In *Proc. IEEE INFOCOM The Conference on Computer Communications*. IEEE, vol. 2, pp. 594–602.

Zhou, S. 2006 Understanding the Internet topology evolution dynamics. *Phys. Rev. E* **74**, 016124. (doi:10.1103/PhysRevE.74.016124)

Zhou, S. & Mondragón, R. J. 2004*a* Accurately modeling the Internet topology. *Phys. Rev. E* **70**, 066108. (doi:10.1103/PhysRevE.70.066108)

Zhou, S. & Mondragón, R. J. 2004*b* The rich-club phenomenon in the Internet topology. *IEEE Commun. Lett.* **8**, 180–182. (doi:10.1109/LCOMM.2004.823426)

Zhou, S. & Mondragón, R. J. 2007 Structural constraints in complex networks. *New J. Phys.* **9**, 1–11. (doi:10.1088/1367-2630/9/6/173)

Zhou, S., Zhang, G. & Zhang, G. 2007 Chinese Internet AS-level topology. *Commun. IET* **1**, 209–214. (doi:10.1049/iet-com:20060518)

Building Fragile Networks

Zhijia Huang, *Graduate Student Member, IEEE,* and Raúl J. Mondragón

***Abstract*—A simple and successful method to construct catastrophic networks is presented. We describe a methods for generating networks that are designed to fail catastropically by avalanche-like (or cascade) breakdowns. Starting from a small seed network and then growing the network, an avalanche is simulated in reverse. In this way catastrophic failure is 'built into' the final network. The resulting networks are shown to have marked invariant properties, making it possible to predict the degree distribution for a given size of network.**

***Index Terms*—Congestion, Catastrophe**

I. Introduction

INFRASTRUCTURES like telecommunication systems, power transmission grids or the Internet are complex networks that are vulnerable to catastrophic failure. A common mechanism behind this kind of failure is an avalanche–like breakdown of the network's components. If a component fails due to overload, its load will be redistributed, causing other components to overload and fail. These failures can propagate throughout the entire network. From studies of catastrophic failures in different technological networks [1, 2, 3], the consensus is that the occurrence of a catastrophe is due to the interaction between the connectivity and the dynamical behaviour of the network elements.

Here we are interested in packet–oriented communication networks. In these networks the traffic (dynamics) and the topology (connectivity) are coupled by the routing mechanisms. The interactions between the network's connectivity and its traffic are complex as they depend on many different parameters, e.g. QoS congestion management (queueing), link bandwidth, type of traffic, link delay, packet lost, etc. So it is not straightforward to predict whether a network will fail catastrophically or not. Furthermore, even if we consider a very simplified version of a packet network, there are still fundamental questions about catastrophic behaviour that we do not have an answer. Questions like: will a network become unstable and fail catastrophically as its size increases; do catastrophic networks have specific connectivity properties? As a first approach to study these questions we consider a simple model of a packet network, where the basic element to create a catastrophe is the interaction between the traffic and topology due to a shortest–path routing mechanism. We disregard any other detail of the network.

A common technique to obtain a catastrophic network is to overload different elements of a pre–existing network and check if a cascading–failure is produced [3, 4, 5, 6]. If there is no cascade, another network topology is considered and checked. These approach can be very computationally demanding as many different networks need to be tested. Our approach is to grow a network in such a way as to ensure their breakdown [7], essentially we follow the cascading breakdown in reverse.

Z. Huang and R. J. Mondragón are with the School of Electronic Engineering and Computer Science, Queen Mary University of London, Mile End Rd., London E1 4NS, UK

II. Methodology

A. Topology and Traffic

To build a catastrophic network we correlate the topology of the network with the traffic that it carries via a routing mechanism. The simplest routing mechanism is to deliver the packets through the shortest paths connecting a source and destination node. The load on a particular node w can be approximated by counting the fraction of shortest paths that pass through the node w. This approximation is given by the betweenness centrality [7]

$$C(w) = \sum_{s\in\mathcal{V}} \sum_{d\neq s\in\mathcal{V}, d\neq w} \frac{g(w;s,d)}{g(s,d)}, \tag{1}$$

where $g(w;s,d)$ is the number of shortest paths from source node s to destination node d which visit node w, $g(s,d)$ is the number of different shortest paths from s to d and $\mathcal{V}$ is the set containing all the network's nodes. If the traffic in the network is distributed evenly throughout all shortest paths, then the normalized betweenness centrality $\hat{C}(w) = C(w)/\sum_{v\in\mathcal{V}} C(v)$ gives the relative usage of node w against the rest of the network's nodes.

For simplicity we consider that each node w produces packets at a rate $\Lambda_w = \Lambda$ for all w, distributed evenly between the $N-1$ destinations. The total flow in the network, $F(\Lambda, N)$, increases linearly with network size $F(\Lambda, N) = N\Lambda$. Node w will become overloaded when its packet arrival rate, λ_w, is equal to or larger than its packet service rate, μ_w. The average number of packets that arrive to node w is [8]

$$\lambda_w = \Lambda N \bar{\ell} \hat{C}(w) = \frac{\Lambda C(w)}{N-1}, \tag{2}$$

where N is the number of nodes, ΛN is the number of packets generated by unit of time by the whole network, $\bar{\ell}$ is the average shortest path of the network to account for the average number of packets that were produced in the past and they are still in transit and, $\hat{C}(w)$ is the proportion of all the packets in transit that pass through the node w. Equation (2) is obtained by using the property that $\sum_{w\in\mathcal{V}} C(w) = N(N-1)\bar{\ell}$ and relates the topology of the networks, via C, with the traffic that it carries via Λ.

B. Node Failure

Node w will become overloaded when the traffic arrival rate λ_w is equal to or larger than the node's service rate, μ_w. Previous work shows that this congestion model can be used to

study the robustness of mission critical networks [9]. As all the nodes produce the same amount of traffic, from equation (2), the condition of congestion is

$$\Lambda^* \geq \frac{\mu_w(N-1)}{C(w)}. \tag{3}$$

C. Cascading failure

We consider overload as the cause of node failure. When a node overloads, the node, its links, and the traffic produced by the node are removed from the network. Then routing mechanism redistributes the remaining traffic throughout the network. The load on other nodes might increase sufficiently for them to get overloaded. These newly overloaded nodes and their links are also removed from the network and the traffic load is redistributed again. This process continues until no further nodes are overloaded. In a large cascade, the network will break down into many disconnected sub–networks.

The cascading condition can be expressed in terms of the network's connectivity via the betweenness centrality. If n_f^i and n_f^{i+1} are two nodes that fail one after the other and at the same traffic load Λ^* then from equation (3) we have that

$$C(n_f^{i+1}) = C(n_f^i)\left[\frac{\mu_{n_f^{i+1}}(N^{i+1}-1)}{\mu_{n_f^i}(N^i-1)}\right], \tag{4}$$

where N^i is the size of the sub–network where n_f^i belongs to after removing node n_f^i and its links.

III. Growing Catastrophic Networks

To grow a catastrophic network, we follow the avalanche process in reverse [7]. Starting from a "seed" network, we build step by step the catastrophic network. At each step, we first add a new 'failing' node n_f^i (see Fig. 1). This node is connected to the existing network A that contains N_A nodes. We also introduce the sub–network B with N_B nodes and connect n_f^i to this sub–network. There are no direct connections between the network A and sub–network B, that is n_f^i is a bridge between A and B. The main problem is to finding out the set of connections between n_f^i and A and n_f^i and B such that, if the load Λ^* is given, then n_f^i is overloaded.

Suppose that at the ith–step of the reverse–avalanche process the node n_f^i fails when $C(n_f^i) = \mu_{n_f^i}(N_A-1)/\Lambda^*$. In this case n_f^i overloads if the average packet–production load is $\Lambda_{n_f^i} = \Lambda^*$. It is feasible that at the next step of the reverse–avalanche process it is not possible to find a network that has a failing node n_f^{i+1} for the given Λ^*. Though it is possible that the node n_f^{i+1} will fail for $\Lambda_{n_f^{i+1}} \geq \Lambda_{n_f^i}$. If we now consider that the average packet load for all the nodes is $\Lambda_{n_f^{i+1}}$ then we will guarantee that at the step ith and (i+1)th the nodes n_f^i and n_f^{i+1} will overload. In other words to construct the avalanche in reverse requires an increase on the average packet load. This observation implies that

$$C(n_f^{i+1}) - \frac{\mu_{n_f^{i+1}}(N_A+N_B)}{\mu_{n_f^i}(N_A-1)}C(n_f^i) \leq \epsilon. \tag{5}$$

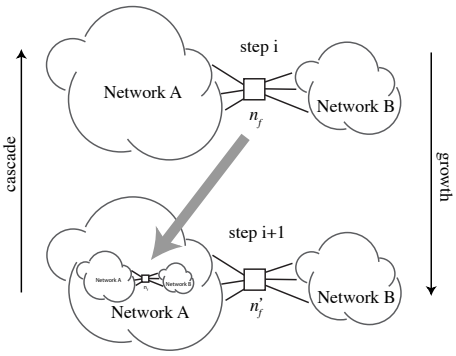

Fig. 1. Schematic representation of the method to build the cascade in reverse.

where we have used equation (3), $\epsilon \geq 0$ and that the size of the network nth+1 step is $N_A + N_B + 1$. At each step of the inverse–cascade process the aim is to find the solution that minimizes ϵ.

The betweenness centrality of node n_f^{i+1} can be written as

$$C(n_f^{i+1}) = C_A + C_B + N_A + N_B + 2N_AN_B, \tag{6}$$

where the term N_A is the number of shortest paths that start from n_f^{i+1} and end in A (similarly the term N_B), the term $2N_AN_B$ is the number of paths that start in A and end in B (and vice versa) which correspond to N_A sources going to N_B destinations. The term C_A are the number of paths that start and end in A and they go through node n_f^{i+1}, and similarly for C_B. To obtain the desired $C(n_f^{i+1})$, which satisfies equation (5) and minimizes ϵ, one could either change the linkage between A and n_f^{i+1} or change the topology of B and its linkage to n_f^{i+1}. There are three variables in equation (6) associated with these changes: C_A, C_B, and N_B.

It is possible to find a bound for N_B, the number of nodes in sub–network B. The maximum size of B occurs when $C_A = 0$. This happens if there is only one link between A and n_f^{i+1} and B forms a star network with n_f^{i+1} at its center. In this situation $C_B = N_B(N_B-1)$. Using equations (5) and (6)

$$N_B^2\alpha + N_B(2N_A\alpha - C(n_f)\mu_{n_f^{i+1}}) + N_A(\alpha - C(n_f)\mu_{n_f^{i+1}}) \leq \epsilon. \tag{7}$$

where $\alpha = (N_A-1)\mu_{n_f^{i+1}}$ For the networks that we considered $\max(N_B) \leq 4$. In this case we evaluated C_B for all possible networks of size less equal to N_B and created a lookout table. This is an efficient way to evaluate the contribution of C_B to $C(n_f^{i+1})$.

A. The Branch and Bound Search Algorithm

To obtain the minimal value of ϵ, we need evaluate how different connection configurations between the network A and node n_f^{i+1} contribute to $C(n_f^{i+1})$. If the nodes in A are labelled as n_i then the links of these nodes with n_f^{i+1} can be expressed as the binary sequence $L = \{l_1, \ldots, l_{N_A}\} = \{0, 1, \ldots,\}$ where $l_i = 1$ if node n_i in A is connected with n_f^{i+1}, otherwise $l_i = 0$. The number of different binary sequences grows

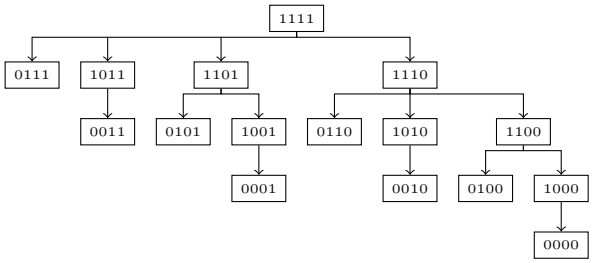

Fig. 2. Solution space represented as a tree for the case when the network A has four nodes

exponentially fast, as 2^{N_A}. To search which of the binary sequence minimizes ϵ we use a branch and bound algorithm based on the following observation: If all the nodes in A where directly connected to n_f^{i+1} then, for any pair of nodes in A which are not directly connected, there will be at least one shortest path between these two nodes that passes through n_f^{i+1}. The length of this path is 2 hops. This connectivity between A and n_f^{i+1} gives the maximum possible value of C_A, removing any link between A and n_f^{i+1} will reduce C_A. To use this property in the search for the minimal ϵ, we use the binary sequence L to organise the space of solutions as a rooted tree. The root corresponds to the solution where all nodes of A are linked to n_f^{i+1}. The branches of the tree are explored by removing connections between A and n_f^{i+1}. Figure (2) shows an example of the solution space tree for $N_A = 4$. The branch and bound algorithm to solve one step of the inverse cascade is given below.

Algorithm Inverse–Cascade

1: Start with the case that all the nodes in A are connected to n_f^{i+1} (i.e. C_A is maximum and $\{l_i, \ldots, l_{N_A}\} = \{1, \ldots, 1\}$.
2: Evaluate C_A, initialize $i = 1$, $j = 1$
3: Disconnect n_i from n_f^{i+1}, i.e. $l_i = 0$
4: **for all** sub–networks B of size $\leq \max(N_B)$ **do**
5: evaluate $\min(\epsilon)$ using eqs.(6)-(7)
6: **end for**
7: **if** $\min(\epsilon) \geq 0$ **then**
8: **if** $\min(\epsilon) \approx 0$ **then**
9: stop, solution found
10: **end if**
11: **Search Branches:** remove link l_j where $j < i$
12: $j \leftarrow j + 1$
13: goto step 3 unless there are no more branches to select
14: **else**
15: **Cut Branches:** Deleting links between network A and n_f^{i+1} will only decrease $C(n_f^{i+1})$. So sub-branches under this branch will not produce high enough values of $C(n_f^{i+1})$, which is not necessary to investigate.
16: Connect n_i back to node n_f^{i+1}.
17: $i \leftarrow i+1$ return to step 2 unless there are no more links to select i.e. $i = N_A$ then stop
18: **end if**

The output of the algorithm is the sequence L and the connectivity of the sub–network B.

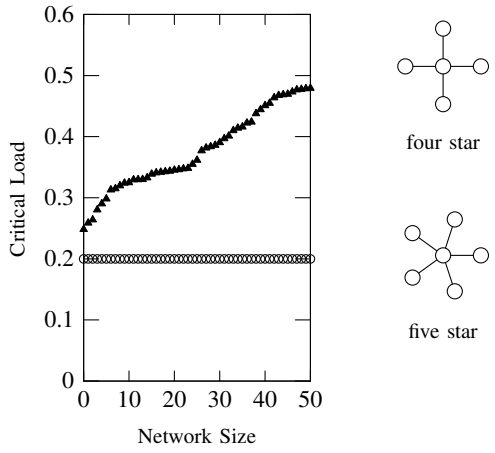

Fig. 3. The critical load as the network size increases for two different seed networks.

IV. Results

From equation (3),the connectivity of the seed networks defines the traffic production rate Λ_0^* when congestion happens. When building the catastrophes, our target is to construct a network that at each step of the avalanche the congestion load is Λ_0^*. However this is not always possible. When building the catastrophic networks, it is possible that the congestion only occurs at a larger loads than Λ_0^*. This opens the question if we can build a catastrophe network at any given Λ^*. Fig. 3 shows the value of Λ^* as the catastrophic network is build for a four and five star-shape seed network. For the four–star network the initial congestion load is $\Lambda^* = 0.25$ and the figure shows that to sustain the avalanche as the network grows, the congestion load has to increase. However for the five–star network with $\Lambda^* = 0.2$ it is possible to construct a catastrophic network that at each step fails this load. In general we noticed that if the congestion load of the seed network is "high", $\lambda^* \geq 0.25$, then to build a catastrophic network the congestion load has to increase.

For the case of networks that fail at each step at the same load Λ^*, we observed that there is a special family of catastrophic networks that their connectivity follows a pattern. Fig. 4 shows (a) the betweenness centrality and (b) the degree distribution of a network at two different steps of its growth. By construction the nodes are split into two groups, the nodes that will congest and trigger the avalanche and the rest of the nodes. We noticed that this distinction between the nodes is also reflected in the betweenness centrality and the degree distribution of the nodes. In the figure, the nodes with highest value of degree or centrality correspond to the failure nodes. We also noticed that the centrality of these nodes tends to increase with the network size as $C(w) \approx \exp(w/A(N)) + C_{min}$, where $A(N)$ is an increasing function of N and $C_{min} = N - 1$ which is the minimum betweenness that a node can have (see Fig. 4(c)). From the catastrophic networks that we constructed we were not able to determine if $A(N)$ tends to a constant or grows linearly as the size N of the network increases. From Eq. (2) and if the betweenness

grows exponentially then

$$\lambda_w = \Lambda \frac{\exp(w/A(N)) + N - 1}{N - 1} \geq \mu_w. \quad (8)$$

If $A(N)$ tends to a constant for large N then the arrival rate at a node $\lambda_w \to \infty$ implying that after a certain size the networks will fail catastrophically. If $A(N) \approx a + bN$ grows linearly with N then $\lambda_w \to \Lambda \geq \mu_w$ as $N \to \infty$. If $\mu_w = 1$, then the catastrophe will occur if $\Lambda = 1$ and if the network is fully connected. If $\mu_w \geq 1$ it is still an open question if catastrophic networks occur for large N.

For the node's degree Fig. 4(b) shows that the degree for failure and non-failure nodes change linearly with network size: the former increases with network size and the latter decreases. These two trends follow the lines $node\ degree = \alpha \pm node\ number/2$. Using different seed networks and checking this linear behaviour at different stages of the avalanche we obtained that $\alpha \approx \gamma N$ and $\beta \approx 0.5$ where γ is a constant and N is the number of nodes in the network. In Fig. 4(d) one of the data sets is rescaled to show how the degree of the nodes follow an invariant as the network grows.

This observation hints that it is possible to construct very large catastrophic network by only specifying the degree and betweenness centrality. Notice that this results covers only one family of potential catastrophic networks. It is possible to create a catastrophic network that it is not evident how the failure/non-failure nodes are related to each other.

V. Conclusion

This is a new approach to study the problem of cascade failure in networks. Instead of taking a given network and test if and how it will fail catastrophically we construct the catastrophic networks. With our method we have control on the critical load that produces the cascade and the number of steps that the cascade has.

These networks can be very large and have a predetermined degree distribution. We believe that extending this approach will provide further important insights into how topology and traffic flow are linked to catastrophic failure. We have concentrated on packet data networks, but our results also apply to other infrastructure networks.

Various extensions to the work are being considered. Currently our catastrophic networks cascade down to the original seed network, typically a small star. This is unlike cascade failure in real networks, where the tendency is for the network to break down into disconnected subnetworks. To account for this we intend to use a number of cores simultaneously in generating networks in the future.

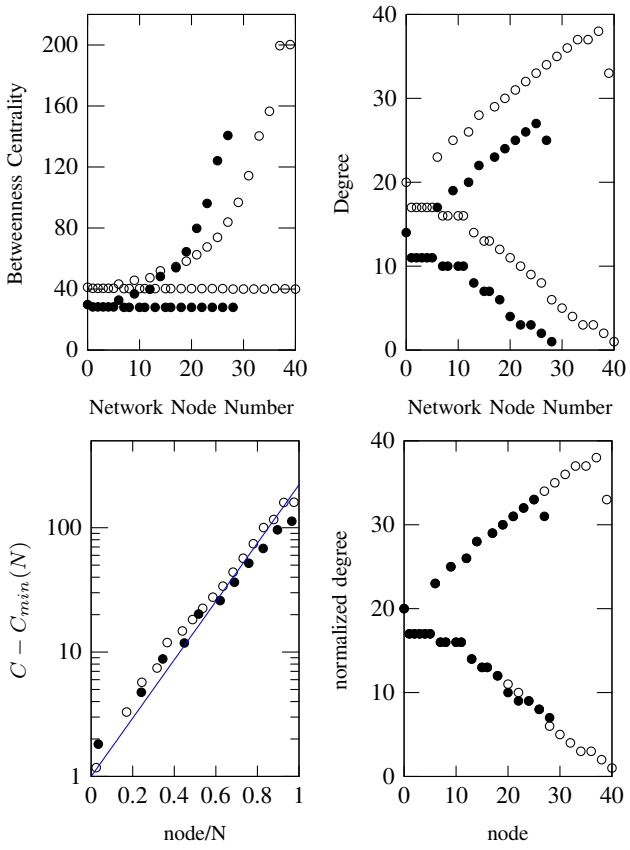

Fig. 4. The betweenness centrality and the degree of the nodes of the catastrophic network as the size of the network increases (top) and their normalisation independent of the network size (bottom).

Acknowledgment

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

References

[1] C.L.DeMarco, "A phase transition model for cascading network failure," *IEEE Control System Magazine*, vol. Dec, pp. 40–51, 2001.

[2] L. Pereira, "Cascade to black," *IEEE Power Energy Magazine*, vol. 2, p. 54, 2004.

[3] D. J. Watts, "A simple model of global cascades on random networks," *Proceeding of the National Academy of Sciences USA*, vol. 99, p. 5766, 2006.

[4] A.E.Motter and Y.C.Lai, "Cascade-based attacks on complex networks," *Physical Review E*, vol. 66, p. 065102, 2002.

[5] J. Y.Moreno and A.F.Pacheco, "Instability of scale-free networks under node-breaking avalanches," *Europhys. Lett.*, vol. 58, p. 630, 2002.

[6] L.Zhao, K.Park, and Y.C.Lai, "Attack vulnerability of scalefree networks due to cascading breakdown," *Physical Review E*, vol. 70, p. 035101, 2004.

[7] M. Woolf, Z. Huang, and R. Mondragon, "Building catastrophes: networks designed to fail by avalanche-like breakdown," *New Journal of Physics*, vol. 9, p. 174, 2007.

[8] L.Zhao, YC.Lai, K.Park, and N.Ye, "Onset of traffic congestion in complex networks," *Physical Review E*, vol. Volume 71, p. 026125, 2005.

[9] A.Tizghadam and A.Leon-Garcia, "On congestion in mission critical networks," in *Computer Communications Workshops, 2008. INFOCOM*, 2008.