

Resilience and Reliability of Infrastructures

Resilience of Hierarchical Critical Infrastructure Networks

Craig Robson, Stuart Barr, Philip James and Alistair Ford

School of Civil Engineering and Geosciences, Newcastle University, UK

ABSTRACT

Concern over the resilience of critical infrastructure networks has increased dramatically over the last decade due to a number of well documented failures and the significant disruption associated with these. This has led to a large body of research that has adopted graph-theoretic based analysis in order to try and improve our understanding of infrastructure network resilience. Many studies have asserted that infrastructure networks possess a scale-free topology which is robust to random failures but sensitive to targeted attacks at highly connected hubs. However, many studies have ignored that many networks in addition to their topological connectivity may be organised either logically or spatially in a hierarchical system which may significantly change their response to perturbations. In this paper we explore if hierarchical network models exhibit significantly different higher-order topological characteristics compared to other network structures and how this impacts on their resilience to a number of different failure types. This is achieved by investigating a suite of synthetic networks as well as a suite of 'real world' spatial infrastructure networks.

Keywords: Critical Infrastructures, Hierarchical Networks, Infrastructure Resilience

INTRODUCTION

The well documented failures of infrastructure systems, such as large scale electricity blackouts across Europe and the US in 2003, along with more recent extreme weather and cyber-attack disruption, has driven significant interest in gaining a better understanding of how different types of infrastructure network responded to a range of perturbations. To this end a wealth of research has investigated the resilience of infrastructure networks using graph-theory, where graph metrics (e.g., node degree, average path length, betweenness etc.) have been used to quantify the resilience of infrastructure networks with respect to theoretical graph-models (e.g., random, small-world and scale-free)¹. In many cases, results have suggested that infrastructure networks exhibit a scale-free structure which is robust to random failures but much more vulnerable to targeted attacks.

However, such studies have often just investigated an individual type of infrastructure system and often only a single network instance within this. This has the potential limitation that the spectrum of infrastructure network topologies may be insufficiently analysed and understood. In particular, it is now recognised that a number of infrastructure networks may be organised logically and/or spatially over multiple levels forming a potential family of hierarchical networks that may exhibit a different behaviour/response to perturbations². In this work we present the results of

1 Albert, R. and Barabasi, A.-L. (2002) 'Statistical mechanics of complex networks', *Reviews of Modern Physics*, 74, pp. 47-97.

2 Svendsen, N.K. and Wolthusen, S.D. (2007) 'Analysis and Statistical Properties of Critical Infrastructure Interdependency Multiflow Models', *IEEE Workshop on Information Assurance*. pp. 247-254.

a comprehensive analysis of the resilience of infrastructure networks to different forms of failure. On the basis of a detailed analysis of a synthetically generated suite of network models along with a subsequent analysis of real world infrastructure network systems, we show that a number of infrastructure systems exhibit a clear hierarchical organisation which results in a notably different response to failures compared to the established scale-free model.

INFRASTRUCTURE NETWORK MODEL SUITES

In order to provide a theoretical baseline and comparison for this study a suite of synthetic networks was created. This comprised of a number of common graph models to create a full spectrum of networks; from those with a random topology through to those with a hierarchical organisation. Network models were generated for random (Erdos-Renyi and GNM)³, scale-free⁴, small-world⁵ and hierarchical community^{6,7} models. These were augmented with a tree model and two modified hierarchical models (hierarchical-random and hierarchical-random+) developed during this study. For six of the graph families, where there is a parameterised exponent to the model, 1,000 realisations with a maximum of 2,000 nodes were created for each. In the case of the tree and hierarchical community models only 45 and 9 realisations were generated respectively due to the rigid structure of these.

Spatial networks for different critical infrastructure sectors (energy, transport, water, telecommunications etc.) were compiled from a variety of sources including the UK ITRC (Infrastructure Transitions Research Consortium) database⁸, Ordnance Survey UK products and Open Street Map data. In total 31 different networks were constructed (6 air route networks, 2 energy networks, 13 rail networks, 5 road networks, 4 river networks and 1 communication network) ranging in scale from national through to local spatial infrastructure systems. In order to create valid topological and spatial network models, the data-sets describing node and edge assets were processed and networks built using a suite of open source network processing software built around the Networkx package⁹.

METRIC ANALYSIS AND FAILURE MODELLING

In order to compare the synthetic network models and also the real infrastructure network models a graph-metric analysis was undertaken. In our work we have employed two key metrics to characterise the structure of the topology of a network under investigation; maximum betweenness centrality and the assortativity coefficient. Maximum betweenness centrality characterises the propensity of a network to be able to efficiently carry a load or flow via its topological structure, while the assortativity coefficient is essentially a measure of how correlated overall the degree of nodes are with respect to their topological neighbours. Both measures were selected due to their ability to characterise high-order topological characteristics of a network compared to traditional measures such as degree distribution and average path length^{10,11}. In order to statistically evaluate the resulting metrics in terms of whether they are different for different types of synthetic and real world networks a transformed divergence analysis was undertaken.

In addition to the graph-metric analysis, both the synthetic and real infrastructure networks were subjected to failure modelling. The implemented failure models remove a chosen node at each epoch, along with their corresponding edges. This process continues iteratively until all nodes are removed from the network (at any epoch nodes that become isolated due the removal of another node are also removed). Three approaches were used for the node

3 Erdos, P. and Renyi, A. (1959) 'On random graphs I.', *Publ. Math. Debrecen*, 6, pp. 290-297.

4 Barabasi, A.-L. and Albert, R. (1999) 'Emergence of Scaling in Random Networks', *Science*, 286, pp. 509-512.

5 Watts, D.J. and Strogatz, S.H. (1998) 'Collective dynamics of 'small-world' networks.', *Nature*, 393, pp. 440-2.

6 Ravasz, E., Somera, A.L., Mongru, D.A., Oltvai, Z.N. and Barabasi, A.-L. (2002) 'Hierarchical organization of modularity in metabolic networks.', *Science (New York, N.Y.)*, 297, pp. 1551-5.

7 Ravasz, E. and Barabasi, A.-L. (2003) 'Hierarchical organization in complex networks', *Physical Review E*, 67.

8 Barr, S.L., Alderson, D., Robson, C., Otto, A., Hall, J., Thacker, S. and Pant, R. (2013) 'A National Scale Infrastructure Database and Modelling Environment for the UK', *International Symposium for Next Generation Infrastructure*. Wollongong, New South Wales, Australia.

9 Ibid.

10 Albert, R. and Barabasi, A.-L. (2002) 'Statistical mechanics of complex networks', *Reviews of Modern Physics*, 74, pp. 47-97.

11 Newman, M.E.J. (2003) 'The Structure and function of complex networks', *Physics*, p. 58.

selection; (i) random, (ii) targeted by maximum node degree and (iii) targeted by maximum node betweenness^{12,13}. At each epoch graph metrics on the number and average size of components, size of the largest component, and the average path length were calculated to capture the behaviour of the network during failure modelling. This allows comparisons to be made in how a network fragments and the performance changes as the number of nodes removed increases. For the synthetic network models 100 from each 1,000 realisations (where possible) were randomly analysed.

RESULTS

Figure 1 shows the calculated metric values of maximum betweenness centrality and assortativity coefficient for all the realisations of the eight different types of synthetic network model investigated, along with their corresponding standard deviational ellipses. Noticeable overlap occurs between the traditional network models employed in infrastructure analysis (random, small-world and scale-free) while the family of hierarchical models seem to exhibit a distinctly different structure in terms of these metrics. The average transformed divergence from the hierarchical communities and tree model compared to the 4 non-hierarchical models (two random, scale-free and small-world) was 99.28, contrasting with intra hierarchical and intra non-hierarchical values of 83.2 and 84.9 respectively. In the case of the actual infrastructure networks investigated, a number of these were found to exhibit similar characteristics to the synthetic hierarchical models, as illustrated in Figure 2. The plot shows that two air networks (routes for the USA and British Airways), the four UK river networks (Tyne, Eden, Dee and Severn) and three rail networks (Tyne and Wear metro, rail for Greater London and the Paris RER) returned metric values with a strong association to the hierarchical synthetic networks. These all lie in closer proximity to the ellipse and the mean centres of hierarchical models than non-hierarchical models, suggesting a hierarchical organisation similar to the model in question.

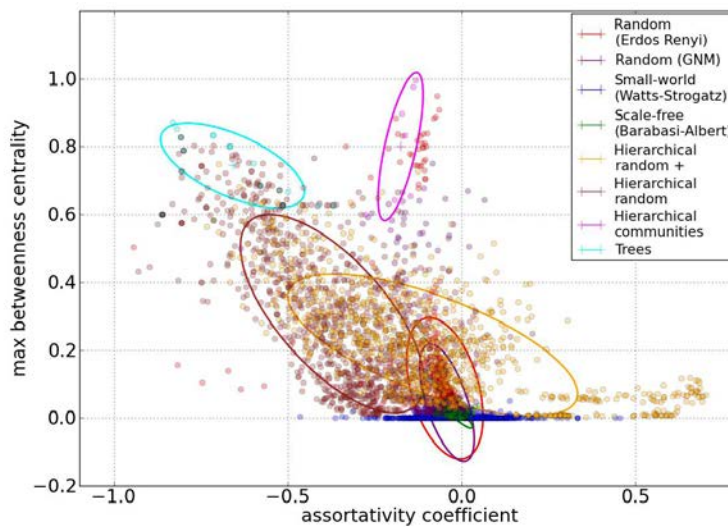


Figure 1: Metric values for the synthetic networks along with mean and single standard deviation ellipse of each model.

¹² Ibid.

¹³ Dueñas-Osorio, L.A., Craig, J.I., Goodno, B.J. and Bostrom, A. (2007) 'Interdependent Responce of Networked Systems', *Journal of Infrastructure Systems*, 13, pp. 185-194.

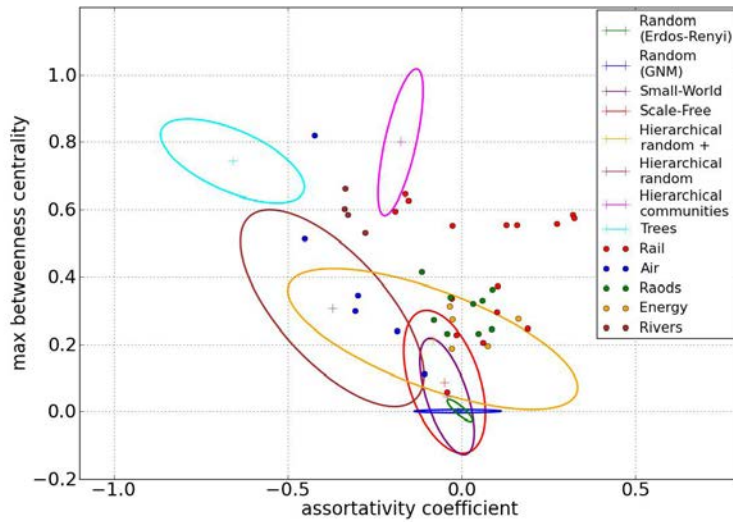


Figure 2: Metric values for the infrastructure networks along with the synthetic standard deviation ellipses.

Failure analysis focused on comparing the failure characteristics of the synthetic non-hierarchical networks with that of the synthetic hierarchal networks, and then an analysis of the failure characteristics of the real infrastructure networks that may be hierarchal. Figure 3 shows the model results for two synthetic network models; a scale-free model and a hierarchical model (a hierarchical random+ network). It is clear that the hierarchical model shows a more dramatic response to the three failure types both in terms of when the network becomes disconnected and also in terms of the number of separate components and their respective size. It is also evident that overall the hierarchical network fails quicker, with less than 60% of the total number of potential epochs required compared to nearly 80% for the scale-free network. This indicates that the hierarchal network is less resilient to all types of perturbation.

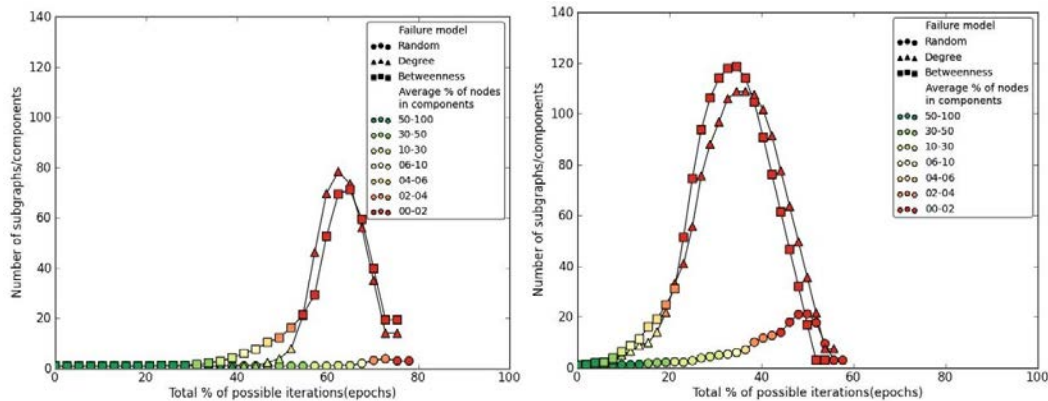


Figure 3: Response of a scale-free network (left) and a hierarchical network (right) to all three failure models.

Results similar to Figure 3 were consistently found across the range of synthetic network models investigated (Figure 4), with three of the hierarchical models being consistently less resilient to the three failure models with, for the two targeted failure models, complete failure occurring at around 40% of the total number of possible epochs for the tree model, and 50% for the HR and HR+ models. In the case of the random failure model the hierarchical response is around 15-20% better compared to the targeted models.

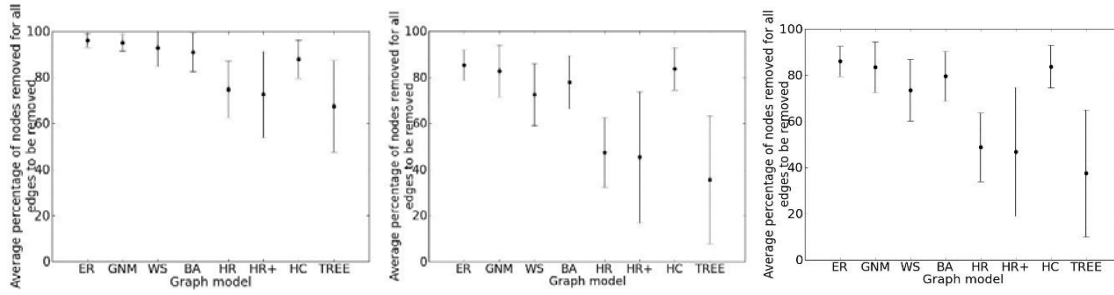


Figure 4: The average and standard deviation of the percentage of nodes that needed to be removed for the total failure of each synthetic network model for the three failure models; random(left), degree(center) and betweenness(right).

Figure 5 shows the response of applying the failure models to the road network for the Tyne and Wear region of the UK (around Newcastle-upon-Tyne) which was indicative of a scale-free network and the rail network for Greater London which exhibited a hierarchical structure in terms of the metrics. The hierarchical rail network is noticeably less resilient to all forms of failure compared to the scale-free road network. While both show a relatively high-sensitivity to the targeted attacks (degree and maximum betweenness), the rail network also shows a noticeable sensitivity to random attack. Indeed, for even a relatively small number of epochs the hierarchical rail network shows a dramatic level of fragmentation with the number of components at 10 epochs ranging between 20-55 compared to 5-8 for the scale-free road network. Similar results were found for the other infrastructure networks that exhibited a hierarchical structure, with the average response to the failure models around 10% worse in terms of the number of nodes required to generate a null graph in terms of the network edges removed (Table 1).

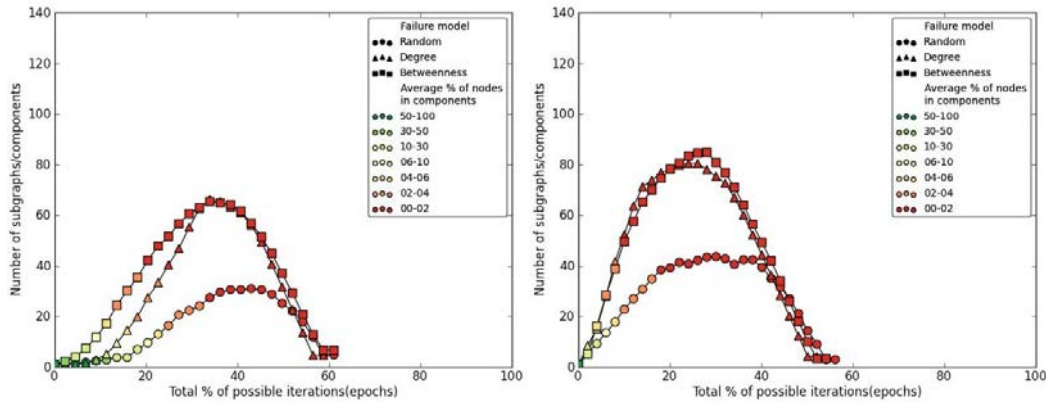


Figure 5: Response to the failure models of (left) road network for the Tyne and Wear region and (right) rail for Greater London.

Table 1: Failure comparison of the hierarchical infrastructure networks and the non-hierarchical.

	Average percentage of nodes removed for network to fail and the standard deviation (σ)		
Network	Random	Degree	Betweenness
Hierarchical infrastructures (as found through the metrics)	58.5 (10.7)	41.6 (13.2)	42.7 (13.3)
Non-hierarchical infrastructures	66.2 (6.7)	51.4 (7.5)	52.0 (7.2)

CONCLUSION

Through the use of a suite of synthetic networks and critical spatial infrastructures this research has shown that networks with a hierarchical organisation exhibit a greater vulnerability to failures when compared to non-hierarchical models (including the scale-free model), with a number of infrastructure networks shown to share this organisation and the associated failure characteristics. Networks with a hierarchical organisation show a much greater rate of fragmentation with subgraphs forming at a quicker rate as well as becoming empty graphs much sooner during failure analysis. The greater vulnerability of those infrastructures which are hierarchically organised as shown in this work highlights that by understanding the underlying structure of networks we can begin to improve how we model their characteristics and behaviour. This can help to develop infrastructure networks with improved levels of resilience to perturbations through policies and management strategies which are founded on a greater level of understanding of network structure and behaviour.