Newcastle University ePrints

Dunn S, Fu G, Wilkinson S, Dawson R.

[Network Theory for Infrastructure Systems Modelling.](#)

Proceedings of the ICE - Engineering Sustainability 2013, 166(5), 281-292.

Copyright:

Published by ICE Publishing, 2013.

For more information see publisher website:

<http://www.icevirtuallibrary.com/content/serial/ensu>

DOI link to published article:

<http://dx.doi.org/10.1680/ensu.12.00039>

Date deposited: 25th June 2014 [made available 1st October 2014]

This work is licensed under a [Creative Commons Attribution 3.0 Unported License](#)

ePrints – Newcastle University ePrints

<http://eprint.ncl.ac.uk>

Network theory for infrastructure systems modelling

Sarah Dunn MEng, GradICE

Researcher, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Gaihua Fu BSc, PhD

Research Associate, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Sean Wilkinson MEng, PhD

Senior Lecturer, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Richard Dawson MEng, PhD

Chair of Earth Systems Engineering, School of Civil Engineering & Geosciences, Newcastle University, Newcastle upon Tyne, UK

Currently, there is a great deal of interest in assessing the resilience of infrastructure systems. Much of this interest stems from the realisation that these systems are not only critical to civil defence but also, given the correct set of circumstances, can fail catastrophically. Three case studies are presented that show how network theory, which has been successfully applied to other fields, can also be used to help understand potential vulnerabilities in infrastructure systems. Through these case studies it is shown that traditional network theory can be extended to analyse infrastructures that are large, spatially distributed systems, or that carry flows of resources or are interconnected with other infrastructure systems. These methods demonstrate how this approach can help infrastructure designers, owners and operators to make rapid assessments of vulnerabilities in their systems and to identify components that are more important to the functioning of the these networks. Furthermore, this approach provides a basis for identifying and prioritising appropriate measures to improve the reliability of infrastructure at the systems scale.

1. Introduction

Infrastructure systems, such as water, transport, communication and energy networks, are crucial to the functioning of a modern society (Murray and Grubestic, 2007). The reliability and integrity of these physical assets and the services they provide is vital for ensuring national security, public health and productivity (HM Treasury and Infrastructure UK, 2011). As society becomes more developed, they not only place greater reliance on these systems but also become increasingly complex, so they have the potential to create larger impacts on both the environment that they are coupled to and the socioeconomic changes that they (in part) enable. This increased complexity and reliance is making these networked infrastructure systems harder to manage (Royal Academy of Engineering, 2011) as disruptive events can be propagated between networks and thus spread their impact far beyond the immediate footprint of a disturbance. For instance, the 2007 UK floods led to the inundation of energy and water facilities in the flood plain. This subsequently led to a regional loss of these services as well as the loss of electricity-dependent information communication technology (ICT) networks and reduced emergency response capacity as a result of transport network disruption (Pitt, 2008). On 28 September 2003 in Italy, a blackout that affected much of the country (Rosato *et al.*, 2008) was magnified by bi-directional interactions between ICT and energy systems because the ICT systems required an

electricity supply, while power stations were dependent on the communication systems for their operation (Buldyrev *et al.*, 2010).

Such events, that have manifested themselves over large spatial areas and across infrastructure sectors, have highlighted the importance of developing earth system engineering approaches to improve the management and analysis of physical infrastructure systems. Traditional approaches to engineering design do not capture the necessary system scale behaviour, requiring the development of new broad scale analyses that can capture interactions between physical infrastructures and the natural and social systems to which they are intrinsically coupled. Network theory provides a rigorous mathematical basis for the analysis of connected elements and enables aspects of the aggregate performance of networked systems to be rapidly calculated. It therefore has great potential as an earth systems engineering tool.

Network models are increasingly being employed to help us understand social (Amaral *et al.*, 2000; Arenas *et al.* 2003; Newman *et al.*, 2002), neural (Sporns, 2002; Stam and Reijneveld, 2007), biological (Rual *et al.*, 2005) and computer science networks (Valverde and Solé, 2003). More recent work has applied network theory to analyse infrastructure systems (Holmgren, 2006; Lhomme *et al.*, 2013; Wilkinson *et al.*, 2012)

and demonstrated their potential to support broad scale infrastructure network design and management.

After a brief introduction to network theory, this paper presents the results of three applications of network analysis to demonstrate using the flexibility and scalability of the method to understand a wide range of infrastructure problems. The first case study subjects a spatial network to different hazards, aiming to assess the resilience of the network to each hazard. The second case study shows the role of supply and pipe (network edge) resistances in mediating infrastructure performance. Finally, the authors demonstrate how these approaches can be extended to consider the implications of interdependencies between networks before discussing the potential of network modelling for earth systems engineering and for supporting the design and management of infrastructure systems.

2. Network analysis and graph theory systems for infrastructure

Network theory is an area of applied mathematics and part of graph theory that concerns itself with the representation of relations between discrete objects. Before describing how to build a network model, it is useful to define some basic terminology relevant to all the case studies. A network is a set of items, referred to as nodes, which are connected by links. There may be several types of node or link in a network with differing properties. The degree of a node is the number of connections it has with other nodes and the degree distribution of a network is the probability distribution of these degrees over the whole network (see Figures 1–3).

2.1 Infrastructure as a network

There has been a great deal of recent work using network theory to analyse naturally occurring networks, including infrastructure systems. Most of this research has focused on defining the degree distribution of the network by studying its nodal connectivity and using this information to identify its network class. In network theory there are four main classes of network, each of which describes a different pattern of nodal connectivity

Figure 1. (a) A sample random network and (b) the shape of its degree distribution

Figure 2. (a) A sample scale-free network and (b) its degree distribution (plotted on a log-log axes)

and has distinctive degree distributions, which are introduced below. That many infrastructure networks fit into only a small number of network classes may be surprising, as an airline network appears to be significantly different from an electrical power grid, but in fact they share similar characteristics.

The first documented network class was the random graph model (Erdos and Renyi, 1960) (Figure 1). Although this type of network has been shown to be a poor representation of real-world network architectures (Newman, 2003), random networks are widely studied and, in part because nodes have a similar degree that follows a Poisson distribution (Figure 1(b)), are often used for comparison with more structured networks (Batagelj and Brandes, 2005; Lewis, 2009) (Figure 1).

To model real-world systems more accurately, Watts and Strogatz (1998) modified the random graph model using the concept of six degrees of freedom (Milgram, 1967) to form

Figure 3. Degree distribution for the North American power grid: a real-world example of an exponential network plotted on a log-log axis (using data from Deng *et al.* 2007)

small-world networks. The main characteristic of small-world networks is that most nodal pairs are not directly connected, but can be reached by way of traversing very few links. The degree distribution is very similar to that of a random network (Figure 1(b)) (Barthelemy, 2011). Small-world networks have been shown to replicate a range of real-world networks, including subway systems (Latora and Marchiori, 2002).

Many real-world networks (including the world wide web (Barabasi and Albert, 1999; Barabasi *et al.*, 2000)) tend to form a power law degree distribution, more commonly known as a scale-free network. These are characterised by a small number of highly connected nodes (nodes with a high degree) and a large number of poorly connected nodes (nodes with a small degree), as shown in Figure 2.

Other real-world networks such as power grids have been found to have an exponential degree distribution and are termed exponential networks (Albert *et al.*, 2004; Amaral *et al.* 2000; Bompard *et al.*, 2011; Liu and Tang, 2005). The degree distribution for an exponential network is shown in Figure 3.

Some real-world networks do not neatly fit one network class in particular, as they include elements from several classes. The most well documented of these are air traffic networks (Figure 4(a)), which include elements of both scale-free and exponential network architectures. Their network architecture has been classed as a truncated scale-free distribution (or a scale-free distribution with an exponential tail) (Wilkinson *et al.*, 2012).

The degree distribution of a network can also provide insight into network resilience. For example, the architecture of scale-free

networks is such that they are quite resilient to random hazards but vulnerable to targeted attack. This is because a random hazard has a small chance of removing one of these few highly connected nodes in the network, while a targeted attack will often remove these nodes in seeking to cause maximum disruption to the network (Albert *et al.*, 2000).

2.2 Network model development

Transforming a real-world infrastructure network into a network model and assessing its hazard tolerance can be broken down into four steps.

Step 1 is to define basic network structure. This involves abstracting the key features of the real-world infrastructure system as a network model. According to the issue under investigation or the availability of data, two approaches are available. In case study 1 it is possible to apply (a), but for case studies 2 and 3, where more general insights are sought, only option (b) is applicable.

- (a) When the analysis of the existing network is the only objective, this is conceptually relatively straightforward: components of an infrastructure system responsible for consuming, generating or regulating a resource or service are represented as nodes. Network links connect these nodes if there is a mechanism for them to exchange their resource or service. This might be a logical supply (e.g. a communication signal) or a flow of resource (e.g. power, water or vehicles).
- (b) Frequently, it is of interest to analyse systems that are representative of real-world networks in order to test the resilience of alternative network structures and adapta-

Figure 4. Graphs showing (a) the degree distribution and (b) the spatial degree distribution for the North American air traffic network

tions. If required, network generation algorithms (described in detail by Barabasi and Albert, 1999; Erdos and Renyi, 1960; Liu and Tang 2005; and Watts and Strogatz, 1998) can be used to produce synthetic but realistic networks according to rules that define properties such as spatial distribution and connectivity.

Step 2 is to define component behaviour. Different infrastructure systems, and indeed their individual components, exhibit a range of engineering behaviour and subsequently mediate the performance of the network. For example, pipes and wires typically have varying capacities. Likewise, individual structures have different supply capabilities, demands and likelihoods of failure under extreme conditions. Network models are flexible and can be parameterised to represent only limited physical processes (e.g. a component is on or off), and are therefore computationally very efficient, but they can also incorporate detailed engineering behaviour. For example, in case study 2 flow is introduced into a network model. This step is crucial for the design of the network analysis as it is important to provide enough detail to capture important system behaviour for the issue under investigation, while avoiding unnecessary complexity.

Step 3 is to subject the model to a series of disruptions. To understand system performance it is crucial to analyse a series of attack strategies that represent different possible hazards or events. These could include random failures (e.g. corresponding to a lack of maintenance), a contagion (e.g. representing a computer virus in ICT systems), a targeted attack at an important location (e.g. representing a terrorist attack) or a spatial hazard (e.g. a flood or wind storm).

Step 4 is to analyse subsequent performance. This final stage is to quantify the impact of each disruption on the infrastructure network. A prerequisite to this is the selection of appropriate metrics to quantify the change in performance of the network. These might measure subsequent system size (e.g. the number of remaining components), output (e.g. a drop in total power supplied) or impact (e.g. the number of people without service).

In this paper the three case studies are used to demonstrate how this four-step process can be applied to analyse a range of infrastructure performance issues. For clarity, one issue is isolated in each case study. The first case study considers the effects of the spatial properties of the infrastructure network, the second incorporates resource flows through a network and the third considers interdependency between two infrastructure networks. In reality many infrastructures might include all of these, and other, factors. However, by presenting three different studies it is possible to explore the significance of infrastructure performance to each factor separately and also

demonstrate the flexibility of network modelling for the large-scale analysis of infrastructure systems.

3. Case study 1: using network topology to identify vulnerability in binary networks

In case study 1 the authors demonstrate how a network model of the North American air traffic network is created and consider how the spatial structure of the network affects its hazard tolerance. This network is subjected to three different types of hazard and the change in performance/connectivity of the network is quantified using graph theory metrics.

The North American air traffic network consists of 781 airports and 3751 air routes (the data were obtained from Openflights (2010)). To transform this air traffic network into a network model the airports are modelled using nodes and the connecting air routes are modelled using links. Using the network model, the degree of each node can be easily calculated, as it is equal to the number of links (air routes) attached to it and from this the degree distribution can be obtained (Figure 4(a)). From Figure 4 it can be seen that the network forms a truncated scale-free distribution, similar to other air traffic networks and, as discussed previously, should be resilient to random hazard but vulnerable to targeted attack.

The spatial degree distribution of these nodes (airports) has also been plotted (Figure 4(b)). This distribution was obtained by first calculating the geographical centre of the airports (weighted by their degree) and then plotting the cumulative degree of airports within a given radius. For the North American air traffic network the geographical centre of the network is located in Missouri, USA (approximately 190 km west of St Louis). The spatial distribution of airports in the North American air traffic network can be seen visually in Figure 5. This figure also indicates the degree of the node (the larger the circle the higher the degree) and the geographical centre of the network. From Figure 5 it can be seen that the high degree airports (or hub airports) are fairly well dispersed throughout the North American states but are less evident in northern Canada.

The resilience of this network is assessed by exposing it to three different types of hazard to assess its hazard tolerance under a range of conditions, as listed below.

- *Random node failure* – nodes are removed randomly from the network.
- *Degree attack* – nodes are removed from the network in the order of the highest to lowest degree. Previous studies have used this attack strategy to simulate a targeted attack, that is, the worst-case scenario.
- *Spatial hazard* – this hazard is based entirely upon the spatial layout of the network (unlike the other two attack strategies,

Figure 5. The location of real-world North American airports, where the size of the node indicates its degree (i.e. the number of air routes attached to it) (the larger the node the higher the degree)

which are based upon topological measures). For both networks the hazard starts in the geographical centre of the North American air traffic network (Figure 4(b) and Figure 5) and then grows outwards, removing nodes in order of distance from the geographical centre.

Following failure, nodes are removed from the network, which in turn will remove their connecting links (as it is not possible to operate an air route to a closed airport). To assess the hazard tolerance of the North American air traffic network to these three hazard types the percentage of links removed have been plotted against the percentage of nodes removed (Figure 6(a)). For the spatial hazard the percentage of links removed have also been plotted against the radius of the hazard, expressed as the percentage of distance from the geographical centre of the North American air traffic network to the edge of the network (Figure 6(b)). Two network theory measures have also been applied to the degraded networks to observe how the connectivity changes when different hazards are applied. The number of clusters is used to quantify how many unconnected parts (or clusters) that the network has broken into and the maximum cluster size (MCS) is used to indicate the size of the largest cluster in the network (Figures 6(c) and 6(d)).

From these results, it is clear that the degree attack strategy has the most devastating effect to the North American air traffic network, both in terms of the higher percentage of

links removed for the same percentage of nodes removed (Figure 6(a)) and a significantly lower MCS (Figure 6(c)). This seems intuitive, given the degree distribution of the network and considering the presence of a few highly connected nodes in the network.

The results for the random node failure and the spatial hazard to the network are broadly similar. This is due to the spatial dispersion of high degree nodes in the North American air traffic network, which can be seen in Figure 5. Therefore, to remove one high degree node a large proportion of low degree nodes must also be removed, which produces similar cluster sizes to a random attack. This spatial dispersion arises from the existence of a number of separate, densely populated areas across the USA (for example, the two large population areas on the east and west coasts). Given the spread of high degree airports, a hazard that is seeded from the sparsely populated centre of the USA is unlikely to be a worst-case location. Shifting the spatial hazard over a location with more high degree airports (e.g. along the east coast) the network's performance would be quite different, as has been shown for the analysis of the European air traffic network by Wilkinson *et al.* (2012).

4. Case study 2: using network topology to identify vulnerability in a flow-based network

The first case study does not consider passenger, freight or aircraft movements. Instead, the effective proportion of the network following a disruption was considered. Given the availability of people, freight and aircraft movements, this analysis could be extended to incorporate these issues using the approach described in case study 2. Here, using a synthetic network of $n = 15$ nodes and 23 links for illustrative purposes, flow is incorporated into the network analysis. In the previous study degree was a suitable proxy for identifying important nodes but when flow is also considered this ranking changes.

Flow around this network model is simulated using the reduced complexity flow model of Dunn and Wilkinson (2012). This model has been shown to represent the flows in infrastructure networks in general, rather than focusing on the flows in a specific type of infrastructure system. Therefore, the present sample network could represent such networks as a power grid or a water distribution system. To generate flow around the network, one node is designated as the supply node (in the case of a water distribution system this would be the reservoir) and the remaining nodes as demand nodes (areas of housing requiring a supply of water, for example). The value of demand is assigned to the demand nodes in proportion to their degree. Given suitable water infrastructure data this demand would be the actual amount of service required by the node. It is assumed that the supply node has enough capacity to meet

Figure 6. The response of the North American air traffic network to three disruptive events

the demand of the other nodes in the network (e.g. for a water distribution network, it is assumed that the reservoir contains enough water to supply the required demands).

In their study Dunn and Wilkinson (2012) were not considering weighted networks, and therefore set the weight of each link to be equal (also equalling the resistances of each link in the reduced complexity flow model). The weight of a link can be used to represent different pipe lengths and/or resistances in a water distribution network, for example. Here the present authors consider the impact of flow on the ranking of vulnerable components in the network and therefore alter the weight of each link using two methods. The first method assigns weight to the links based on their proximity to the supply node (Figure 7(a)). A link that is connected to the supply node will have a resistance of 1, links that are connected to these links have a resistance of 2 and so on. In the second

method, values of weight/resistance are assigned to the links randomly (Figure 7(b)).

The authors also use the concept of a roving supply node used by Dunn and Wilkinson (2012). In the absence of a real-world network this method is used to negate the effect that the proximity of the supply node has to the demand nodes (i.e. demand nodes directly connected to the supply node will not only have their demand flowing through them but will also transfer flow to those not directly connected to the supply node). The vulnerability of each node is determined by analysing the $n - 1$ possible demand node failures for each of the n ($n = 15$ here) possible supply node locations (210 simulations in total). The location of the supply node, v_{si} , is fixed (e.g. at node $i = 1$, as shown in Figure 7) and the flows across the network as a function of this supply node location, $Q(v_{si})$, are evaluated. A single demand node, v_d , is removed and

Figure 7. The synthetic network, with the links weighted (a) with distance and (b) randomly

the flows as a function of this diminished network, $Q(v_s, v_d)$, recalculated. Flows are subsequently calculated for each of the n possible supply node locations and $n - 1$ single demand node failures to understand the influence that the supply node can have. The change in flow over the entire network, ΔQ , for the i th supply node is calculated as the square root of the sum of the squares of the change in flow across the remaining demand nodes in the network.

$$1. \quad \Delta Q(v_{si}) = \sqrt{\sum_{j=1, j \neq i}^n (Q_j(v_{si}) - Q_j(v_{si}, v_d))^2}$$

To test the predictive skill of the model, $\Delta Q(v_{si})$ is correlated against the original flow, Q_j (the flow through the demand node prior to its removal), node degree (k_j), weighted betweenness centrality, $C(v_j)$, and a combined measure as alternative metrics of network performance. The R^2 from these correlations is plotted in Figure 8. The betweenness centrality of a node is equal to the number of shortest paths between all other nodes that pass through the node (Freeman, 1979; Lewis, 2009). As flow preferentially chooses the shortest path between areas of supply and demand it could be argued that the measure that accounts for the shortest distance between pairs of other nodes indicates the important nodes in the network. The $C(v_j)$ is calculated as follows (Brandes, 2001)

$$2. \quad C(v_j) = \sum_{v_j \neq v_a \neq v_b} \frac{c(v_a, v_b, v_j)}{c(v_a, v_b)}$$

where $c(v_a, v_b)$ is the number of shortest paths between a pair of nodes v_a and v_b and $c(v_a, v_b, v_j)$ is the number of shortest paths from v_a to v_b that pass v_j . The final measure used is a combined measure, CM_j , developed by Dunn and Wilkinson

(2012), and again this measure is modified to account for the weight/resistance of each link.

$$3. \quad CM_j = \frac{Q_j \times C(v_j)}{v_j}$$

When the network is unweighted, Dunn and Wilkinson (2012) showed that this combination of Q_j (a physically based measure) and betweenness centrality (a measure derived from graph theory) improved the predictive skill at identifying vulnerable nodes (Figure 8).

First, the skill of each method compared to the others is shown for each position of the supply node (but the results are ranked in descending order for the CM_j to enable an easier comparison) (Figures 8(a) and 8(c)). Each measure is also ranked individually to identify the performance of each measure for ranking the most vulnerable nodes (Figures 8(b) and 8(d)).

For the networks where the link weights/resistances were added with distance from the supply node, the CM_j appears to most consistently identify the vulnerable nodes (Figure 8(a)). The measures of Q_j and $C(v_j)$ achieve better correlations for a few positions of the supply node, but also noticeably weaker in most other correlations. Ranking all the measures (Figure 8(b)) shows that the degree of a node is not a good indication of the vulnerability of that node, defined as the change in flow across the network after its removal.

The combined measure appears to most effective, although not consistent, at identifying the most important nodes for overall network performance in both situations. Ranking these results, for all measures, shows that $C(v_j)$ is not a good indicator of node vulnerability, which therefore reduces the performance of the combined measure.

Figure 8. The skill of four approaches to predicting network performance where link resistances are (a, b) weighted with distance or (c, d) assigned randomly. Results are ranked in

descending order according to R^2 , for (a, c) all measures are ranked according to CM_j , while for (b, d) each measure is ranked independently

5. Case study 3: using network topology to understand the impact of interdependency on the performance of binary networks

The previous two case studies assumed the networked infrastructure was isolated from other infrastructure systems. In many instances this is an appropriate simplifying assumption to make. However, more recently approaches to networks of networks analysis (i.e. modelling the dependence of one system on another) have started to emerge (Gao *et al.*, 2011; Pederson *et al.*, 2006). For example, the successful operation on an electrical distribution system relies on a supply of water for cooling and ICT systems for control and management. The final case study seeks to understand the impact that interdependency can have on the performance of interconnected networks. As with the other two studies, the focus is on

a single issue of interest, interdependency, and so space or flows are not considered.

Data on infrastructure interdependencies are not typically available but, as described by Hall *et al.* (2013), this situation is improving. With this in mind the present authors have developed a simplified network model to explore cascading failure in interdependent networks (Figure 9). First a number of isolated networks are established, each representing an infrastructure system. In this example two networks with random topology have been produced using the approach outlined in step 1(b). Interdependencies between networks are represented by a number of links, each connecting a node in one network with a node in another. Figure 9(a) shows an interdependent system that couples two networks, A and B. The set of nodes in network A are labelled ($u_1, u_2, \dots$), while the set of nodes in network B are

Figure 9. An interdependent system: (a) in its initial state, subject to failure of node u_4 ; (b) after the first iteration of cascading failure; (c) the stabilised system

labelled ($v_1, v_2, \dots$). An intra-network link is represented as a solid line. An inter-network dependency is represented as a dashed line.

This model allows inter-network dependencies to be configured along a few dimensions so as to provide the capacity to model various network coupling modes. First, inter-network dependencies can be generated according to different criteria, including random connections, or co-related connections according to spatial proximity or node degree. Second, the dependencies between two networks can be customised with three parameters, $\langle F, K, D \rangle$. F specifies the extent of inter-network dependencies, that is, the portion of nodes that a network has and depends on another network. K specifies the redundancy of dependencies, that is, the number of supporting nodes that a node has from another network. D specifies the directionality of dependencies. An interdependent link is bi-directional if its inter-network dependencies are symmetric, for example, when a node u in network A supports a node v in network B, v also supports u . A link is uni-directional when these dependencies are not mutual. That is, when a network A node, u_1 , supports a network B node, v_1 , and v_1 in turn may support a different network A, node, u_2 . For example, the system in Figure 9(a) is a bi-directional system, and a link between node u_1 and v_2 means that they mutually depend on each other.

To function properly, it is assumed that a dependent node requires the availability of at least one of its supporting nodes from each of its supporting networks. Failures happen in a system in the following three cases. First, a node fails if it is attacked directly. Second, a node fails if it is a dependent node and it loses all of its supporting nodes from at least one of the networks that it is supported by. Finally, in line with percolation theory approaches (Albert and Barabasi, 2002), a node fails if it is disconnected from the largest component of the network to which it belongs (Figure 9).

An attack on network A is modelled that disables some proportion of the network nodes directly and indirectly brings about a cascade of additional node failures in network B as a consequence of compromised interdependencies. Such additional node failures happen recursively and may result in system failure extending far beyond the original attack footprint. For the system in Figure 9(a), suppose that the node u_4 is attacked. When u_4 fails, all links connected to u_4 also fail. The failure of u_4 also disconnects u_1 from the giant component of A, and therefore u_1 fails. The failure of u_4 and u_1 triggers the failure of v_5 (supported by u_4) and v_2 (supported by u_1). The failure of v_5 disconnects v_6 from the largest component of network B, hence v_6 fails. The resulting system at this stage is shown in Figure 9(b). The failure of v_6 causes the failure of u_6 . As no further failure occurs, the system reaches a stabilised state and the remaining functioning component of the system is shown in Figure 9(c).

To measure the performance of such an interdependent system, the connectedness of a system is calculated in terms of the relative size of the largest component, P , of the final stabilised system after the cascading failure.

$$4. \quad P = \frac{\sum_i N_T^i}{\sum_i N_0^i}$$

where N_0^i is the numbers of nodes from network i before cascading failure, and N_T^i are the number of nodes in the largest components of network i after cascading failure. The largest component can be an important quantity in, for example, a communication network where it represents the largest fraction of the network within which communication is possible and hence is a measure of the effectiveness of the network to provide its communication service. The aggregate performance, IP , characterises the behaviour of an interdependent

system when network disruptions of different magnitude are considered, and is calculated as the integral of P with respect to attack size, q .

$$5. \quad IP = \int_0^1 P(q)$$

The larger P and IP , the more nodes remain in the largest connected component of a system, the better the system performs and the easier the system is to recover or repair.

The study was carried out over systems that couple two random networks, A and B, each comprising 10 000 nodes, and with an average degree of 4. Network disruption was initiated by removing a randomly selected fraction q of network A nodes. Figure 10 plots relative size, P , of giant components as function of, q , the size of initial disruption to network A, when $F = 1.0$ and $K = 2$ for a bi-directional system. The results are compared against that of a system in which networks A and B are isolated from each other. It shows that an interdependent system has smaller P and therefore is more vulnerable than an isolated system. While an isolated network undergoes continuous transition at the failure threshold q_c (the point when a system collapses or P becomes zero), an abrupt transition is observed at q_c for an interdependent system. That is, P at q_c is non-zero, and abruptly drops to zero when $q > q_c$ (Figure 10).

These results demonstrate that the interdependent system is most vulnerable when $K = 1$ and $F = 1.0$, that is, when both networks are fully connected to each other and each node has only one supporting node from the other network. The performance of the interdependent system improves when the number of supporting

nodes that a node has is increased (i.e. increasing K) or the extent a network depends on another network is decreased (i.e. decreasing F). When either K is sufficiently large or F is sufficiently small, the performance of an interdependent system approaches that of a system in which each of its sub-networks is isolated from or independent of the others (Figure 11).

Figure 11 shows the performance difference, $IP_{bi} - IP_{uni}$, of uni-directional and bi-directional systems, where IP_{bi} and IP_{uni} are aggregate performance of a bi-directional and a uni-directional system, respectively. It can be seen that a uni-directional system is more vulnerable than a bi-directional system, and the bigger F or/and smaller K are, the more remarkable is the difference of performance between a bi-directional and a uni-directional system. The main reason for the worse performance of a uni-directional system is that it presents more possibilities for the existence of longer dependency chains than a bi-directional system. These dependency chains run back and forth between the interconnected networks. A failure of one node compromises the robustness of all downstream nodes in the dependency chain, potentially triggering their failure and a possible cascade (described by Fu *et al.*, 2012).

6. Conclusions

Modern infrastructure systems are complex, interconnected networks. In this paper the authors have demonstrated the applicability of network theory on three different case studies. These examples have shown that the resilience of an infrastructure system is sensitive to a number of factors, including the

- spatial distribution of infrastructure nodes (such as airports and power stations)

Figure 10. Comparison of the performance of interdependent systems against isolated systems

Figure 11. Comparison of the performance of bi-directional and uni-directional systems for a range of interdependent configurations

- type and magnitude of disruptive event to which the infrastructure is exposed (whether it is random, targeted or a spatially coherent hazard)
- degree of connectivity in an infrastructure network
- number of connections between infrastructure networks and their directionality
- capacity, and other properties, of the links that connect nodes.

In the first case study network graph theory was used to assess the vulnerability of the North American air traffic network to spatial and topological hazards and it was demonstrated that the degree attack strategy had the most devastating effect. For spatial hazards this network was found to have a similar spatial vulnerability to a random hazard. This is because the high degree hubs in the network are geographically distributed relatively evenly and therefore a spatial hazard must become relatively large before it has a significant impact on the network. In the second case study various network graph theory measures, flow based metrics and combinations of these were tested to better identify vulnerable nodes in a weighted network. In this example it was demonstrated that at times flow-based measures were superior and at other times graph theory measures were superior, but in general a combination of the two had the best predictive capabilities. Finally, a system of interdependent networks was analysed and it was demonstrated that an interdependent system is most vulnerable when both networks are fully connected to each other in a uni-directional manner and each node has only one supporting node from the other network. This case study highlighted the need to identify and characterise interdependencies and, where appropriate, add in redundancy or other mitigation measures.

While the authors recognise that the characterisation of the reliability of individual components in a system is important to understanding its behaviour, an earth systems engineering

approach that considers system-level interactions is essential for understanding impacts on the wider environment. A priority for future work should be to identify, for different infrastructure design problems, the right balance between the computational efficiency of network (or other broad scale) analyses and the full representation of the physical processes. The case studies presented here show the potential for network theory to address a wide range of challenges such as broad scale risk assessment, national infrastructure planning and the development of adaptation plans, as well as understanding the potential impact of cascading impacts from random failure, spatial hazards such as floods, malicious attack or fragilities due to interdependencies. The authors therefore conclude that systems-scale analysis of infrastructure networks must be an important stage in infrastructure design, planning and management in the context of resilience and sustainability.

Acknowledgements

This work has benefited from funding support from Resilient Futures project that was funded by the Engineering and Physical Sciences Research Council and Economic and Social Research Council (EP/I035781/1). Richard Dawson is funded by an Engineering and Physical Sciences Research Council Fellowship (EP/H003630/1) and Sarah Dunn is partially funded by an Engineering and Physical Sciences Research Council studentship.

REFERENCES

- Albert R and Barabasi AL (2002) Statistical mechanics of complex networks. *Reviews of Modern Physics* **74**(1): 47–97.
- Albert R, Jeong H and Barabasi AL (2000) Error and attack tolerance of complex networks. *Nature* **406**(6794): 378–382.
- Albert R, Albert I and Nakarado GL (2004) Structural vulnerability of the North American power grid. *Physical Review E* **69**(2), <http://dx.doi.org/10.1103/PhysRevE.69.025103>.
- Amaral L, Scala ANA, Barthelemy M and Stanley HE (2000) Classes of small-world networks. *Proceedings of the National Academy of Sciences of the United States of America* **97**(21): 11 149–11 152.
- Arenas AL, Danon A, Diaz-Guilera P, Gleiser M and Guimera R (2003) Community analysis in social networks. *European Physical Journal B* **38**(2): 373–380.
- Barabasi AL and Albert R (1999) Emergence of scaling in random networks. *Science* **286**(5439): 509–512.
- Barabasi AL, Albert R and Jeong H (2000) Scale-free characteristics of random networks: the topology of the world-wide web. *Physica A* **281**(1–4): 69–77.
- Barthelemy M (2011) Spatial networks. *Physics Reports – Review Section of Physics Letters* **499**(1–3): 1–101.
- Batagelj V and Brandes U (2005) Efficient generation of large random networks. *Physical Review E* **71**(3), <http://dx.doi.org/10.1103/PhysRevE.71.036113>.
- Bompard E, Wu D and Xue F (2011) Structural vulnerability of power systems: a topological approach. *Electric Power Systems Research* **81**(7): 1334–1340.

- Brandes U (2001) A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology* **25**(2): 163–177, <http://dx.doi.org/10.1080/0022250X.2001.9990249>.
- Buldyrev SV, Parshani R, Paul G, Stanley HE and Havlin S (2010) Catastrophic cascade of failures in interdependent networks. *Nature* **464**(7291): 1025–1028.
- Deng K, Zhao HP and Li DJ (2007) Effect of node deleting on network structure. *Physica A – Statistical Mechanics and Its Applications* **379**(2): 714–726.
- Dunn S and Wilkinson S (2012) Identifying critical components in infrastructure networks using network topology. *Journal of Infrastructure Systems* **19**(2): 157–165, [http://dx.doi.org/10.1061/\(ASCE\)IS.1943-555X.0000120](http://dx.doi.org/10.1061/(ASCE)IS.1943-555X.0000120).
- Erdos P and Renyi A (1960) On the evolution of random graphs. *Publication of the Mathematical Institute of the Hungarian Academy of Sciences* **5**: 17–61.
- Freeman LC (1979) Centrality in social networks conceptual clarification. *Social Networks* **1**(3): 215–239, [http://dx.doi.org/10.1016/0378-8733\(78\)90021-7](http://dx.doi.org/10.1016/0378-8733(78)90021-7).
- Fu G, Khoury M, Dawson R and Bullock S (2012) Vulnerability analysis of interdependent infrastructure systems. *Proceedings of ECCS2012 European Conference on Complex Systems, Brussels, Belgium*, p. 18.
- Gao J, Buldyrev SV, Havlin S and Stanley HE (2011) Robustness of a network of networks. *Physical Review Letters* **107**(19), <http://dx.doi.org/10.1103/PhysRevLett.107.195701>.
- Hall JW, Henriques JJ, Hickford AJ and Nicholls RJ (2013) Systems-of-systems analysis of national infrastructure. *Proceedings of the Institution of Civil Engineers – Engineering Sustainability* **166**(5): 281–292, <http://dx.doi.org/10.1680/ensu.12.00028>.
- HM Treasury and Infrastructure UK (2011) *National Infrastructure Plan*. Stationery Office, London, UK.
- Holmgren AJ (2006) Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis* **26**(4): 955–969.
- Latora V and Marchiori M (2002) Is the Boston subway a small-world network? *Physica A – Statistical Mechanics and Its Applications* **314**(1–4): 109–113.
- Lewis TG (2009) *Network Science: Theory and Practice*. John Wiley, Oxford, UK.
- Lhomme S, Serre D, Diab Y and Laganier R (2013) Analyzing resilience of urban networks: a preliminary step towards more flood resilient cities. *Natural Hazards and Earth Systems Sciences* **13**(2): 221–230, <http://dx.doi.org/10.5194/nhess-13-221-2013>.
- Liu JZ and Tang YF (2005) An exponential distribution network. *Chinese Physics* **14**(4): 643–645, <http://dx.doi.org/10.1088/1009-1963/14/4/001>.
- Milgram S (1967) The small-world problem. *Psychology Today* **1**(1): 61–67.
- Murray A and Grubecic T (2007) *Critical Infrastructure: Reliability and Vulnerability*. Springer, Berlin, Germany.
- Newman MEJ (2003) The structure and function of complex networks. *Siam Review* **45**: 167–256.
- Newman MEJ, Watts DJ and Strogatz SH (2002) Random graph models of social networks. *Proceedings of the National Academy of Sciences of the United States of America* **99**: 2566–2572.
- Openflights (2010) OpenFlights.org. See <http://openflights.org/> (accessed 13/08/2010).
- Pederson P, Dudenhoeffer D, Hartley S and Permann M (2006) *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho National Laboratory, Idaho, USA.
- Pitt M (2008) *The Pitt Review: Learning Lessons from the 2007 Floods*. Cabinet Office, London, UK.
- Rosato V, Issacharoff L, Tiriticco F *et al.* (2008) Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures* **4**: 63–79.
- Royal Academy of Engineering (RAE) (2011) *Infrastructure, Engineering and Climate Change Adaptation – Ensuring Services in an Uncertain Future*. RAE, London, UK, see http://www.raeng.org.uk/news/publications/list/reports/Engineering_the_future_2011.pdf.
- Rual JF, Venkatesan K, Hao T *et al.* (2005) Towards a proteome-scale map of the human protein-protein interaction network. *Nature* **437**(7062): 1173–1178.
- Sporns O (2002) Network analysis, complexity, and brain function. *Complexity* **8**(1): 56–60.
- Stam CJ and Reijneveld JC (2007) Graph theoretical analysis of complex networks in the brain. *Nonlinear Biomedical Physics* **1**(3): 1–19.
- Valverde S and Solé RV (2003) Hierarchical small worlds in software architecture. *Arxiv*: preprint cond-mat/0307278.
- Watts DJ and Strogatz SH (1998) Collective dynamics of ‘small-world’ networks. *Nature* **393**(6684): 440–442.
- Wilkinson S, Dunn S and Ma S (2012) The vulnerability of the European air traffic network to spatial hazards. *Natural Hazards* **60**(3): 1027–1036.

WHAT DO YOU THINK?

To discuss this paper, please email up to 500 words to the editor at journals@ice.org.uk. Your contribution will be forwarded to the author(s) for a reply and, if considered appropriate by the editorial panel, will be published as discussion in a future issue of the journal.

Proceedings journals rely entirely on contributions sent in by civil engineering professionals, academics and students. Papers should be 2000–5000 words long (briefing papers should be 1000–2000 words long), with adequate illustrations and references. You can submit your paper online via www.icevirtuallibrary.com/content/journals, where you will also find detailed author guidelines.