Eur. Phys. J. B (2014) 87: 148
DOI: 10.1140/epjb/e2014-40876-y

THE EUROPEAN PHYSICAL JOURNAL B

Regular Article

Interdependent networks: vulnerability analysis and strategies to limit cascading failure*

Gaihua Fu[1,a], Richard Dawson[1], Mehdi Khoury[2], and Seth Bullock[2]

[1] School of Civil Engineering and Geosciences, Newcastle University, NE1 7RU Newcastle upon Tyne, UK
[2] School of Electronics and Computer Science, University of Southampton, SO17 1BJ Southampton, UK

Received 26 September 2013 / Received in final form 31 March 2014
Published online 1 July 2014

Abstract. Network theory is increasingly employed to study the structure and behaviour of social, physical and technological systems – including civil infrastructure. Many of these systems are interconnected and the interdependencies between them allow disruptive events to propagate across networks, enabling damage to spread far beyond the immediate footprint of disturbance. In this research we experiment with a model to characterise the configuration of interdependencies in terms of direction, redundancy, and extent, and we analyse the performance of interdependent systems with a wide range of possible coupling modes. We demonstrate that networks with directed dependencies are less robust than those with undirected dependencies, and that the degree of redundancy in inter-network dependencies can have a differential effect on robustness depending on the directionality of the dependencies. As interdependencies between many real-world systems exhibit these characteristics, it is likely that many such systems operate near their critical thresholds. The vulnerability of an interdependent network is shown to be reducible in a cost effective way, either by optimising inter-network connections, or by hardening high degree nodes. The results improve understanding of the influence of interdependencies on system performance and provide insight into how to mitigate associated risks.

1 Introduction

Network theory is a powerful tool to help us understand the structure and behaviours of systems found in nature, technology and human society [1–3]. Previous research has tended to focus on studying single, isolated systems [4–10], thereby neglecting the complex coupling that can exist between these systems [3,11–15]. For instance, in the civil infrastructure domain, the successful operation of a power system requires water for cooling, transport to supply fuel, and ICT (information and communication technology) systems for control; and these systems in turn require power systems to supply electricity. This interdependence on the one hand may improve network functionality and efficiency, but on the other hand may introduce unforeseen vulnerabilities. As demonstrated in references [11,13,16–19], the failure of one network component may propagate across the system boundary, resulting in cascading failure across multiple sectors.

The importance of understanding the effects associated with network interdependencies has been widely recognised [12,20–29]. Important insights from previous modelling of interdependent systems show that (i) analysis of systems with one-to-one undirected dependencies show that failure initiated in one network can propagate across networks recursively and lead to a cascading failure of the wider networked system [12]; (ii) the vulnerability of an interdependent system is reduced when the extent of coupling between networks decreases [21]; and (iii) traditional network protection strategies, such as protecting high degree nodes, are less effective in an interdependent network than in a single network [30].

Previous research has used relatively simple and constrained representations of interdependencies that are not particularly representative of those observed in real-world systems. Here we present a model that describes coupled systems as a network of networks. We consider how the configuration of network interdependencies plays an important role in determining how failure propagates between networks, and the ability of the system to absorb disruptions. The model characterises interdependencies along multiple dimensions, enabling systems of different strength of coupling to be represented. We analyse the behaviour and performance of a range of interdependent system configurations, and explore strategies to reduce the risks of cascading failure. Our research reveals a number of non-intuitive insights into the behaviour of interdependent systems. The severity of cascading failure is shown to increase significantly when inter-network connections are directed, and the degree of redundancy in

* Supplementary material in the form of one pdf file available from the Journal web page at http://dx.doi.org/10.1140/epjb/e2014-40876-y

[a] e-mail: gaihua.fu@newcastle.ac.uk

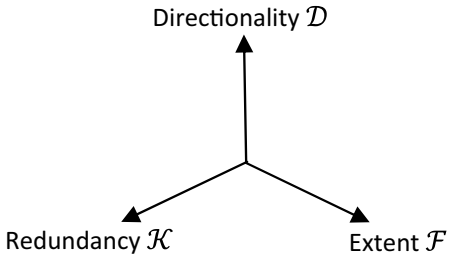

Fig. 1. Dimensions of interdependency measurement.

inter-network connections can have a differential effect on the robustness of systems depending on the directionality of inter-network connections. Network topology also influences system performance although this is heavily mediated by the mechanism of network disruption. We further demonstrate that the risks of cascading failure can be reduced in a number of ways, either by manipulating the directionality of inter-network connections, or by *hardening* high degree nodes.

By providing some quantitative insights into the impact of interdependencies, it is intended that results presented in the paper could be valuable to stakeholders of various social-technological systems by providing hitherto unavailable analysis of how to: (i) maximise the reliability of interdependent systems; (ii) adapt an existing system to meet the challenges imposed by natural and manmade hazards. The remaining parts of the paper are organised as follows. Section 2 describes the interdependent network model. Section 3 outlines the model of cascading failure. Sections 4 and 5 report results derived from the model. Section 6 discusses how structural vulnerability of interdependent systems can be reduced. Section 7 provides conclusions and identifies future research needs.

2 Interdependent network model

Interdependencies in real-world networks are more homogeneous than previous modelling studies have considered [31]. Here we present a model that characterises inter-network dependencies along three key dimensions (Fig. 1), that enables us to describe and simulate a wide range of network coupling modes.

We define a "network of networks" that couples $k \geqslant 2$ disjoint networks and is represented as a pair $\{\mathcal{V}, \mathcal{L}\}$, where $\mathcal{V} = \{\mathcal{V}_1, \ldots, \mathcal{V}_j, \ldots, \mathcal{V}_k\}$ and $\mathcal{L} = \{\mathcal{L}_{1,1}, \ldots, \mathcal{L}_{1,k}, \ldots, \mathcal{L}_{i,j}, \ldots, \mathcal{L}_{k,k}\}$. $\mathcal{V}_i$ is the set of nodes in network i, and $\mathcal{L}_{i,j}$ the set of links that connect nodes from network i to network j. Links in $\mathcal{L}_{i,i}$ connect nodes within the same network, and we call such links the "intra-links". When $i \neq j$, links in $\mathcal{L}_{i,j}$ connect nodes in two disjoint networks, and we call such links the "inter-links", i.e., interdependent links.

We acknowledge that not every node in a network depends on another network. For example, in a coupled road and ICT system, some but not all road junctions require traffic signals (controlled by an ICT system) for their operation. Furthermore dependencies between networks are *unbalanced*. For example, a significant portion of a transport network nodes require the support of an ICT network for control and management, but the number of dependent nodes of ICT on transport network is considerably small. Thus, the first dimension of our model considers the *extent* of dependency (denoted as $\mathcal{F}$), defined here as the fraction of network nodes that are dependent on another network[1]. For a system consisting of two networks i and j, $\mathcal{F}$ is partitioned into two components, $\mathcal{F}^{i,j}$ and $\mathcal{F}^{j,i}$. The former specifies the fraction of nodes in network i that depend on network j. The latter specifies the fraction of nodes in network j that depend on network i. Two networks i and j are *fully* inter-dependent when $F^{i,j} = F^{j,i} = 1.0$, otherwise they are *partially* inter-dependent.

Interdependency relations are not always restricted to one-to-one. For example, emergency services such as hospitals frequently have multiple power connections, so that failure of one power line or generator will enable continued operation. Our second dimension, redundancy of dependencies, $\mathcal{K}$ is partitioned into $\mathcal{K}^{i,j}$ and $\mathcal{K}^{j,i}$, where $\mathcal{K}^{i,j}$ represents the redundancy of the dependency of network i on network j, i.e., the average number of supporting nodes that a dependent node in network i has from network j. Similarly, $\mathcal{K}^{j,i}$ describes the redundancy of the dependency of network j on network i. As with any network link, an interdependency link has an associated cost, hence $\mathcal{K}$ in real world is usually very small when comparing to system size N, (i.e. $\mathcal{K} \ll N$), as discussed and evidenced in references [12,26,32,33].

Finally we observed that inter-network dependencies are not always *mutual* or *symmetric*. For example, whilst a power substation might supply electricity to an ICT hub, this same hub does not necessarily provide information control to the power plant. Hence interdependencies can be quantified in term of *directionality*. An undirected interdependent link $(u, v) \in \mathcal{L}_{i,j}$ $(i \neq j)$ exists where there also exists a $(v, u) \in \mathcal{L}_{j,i}$. Otherwise it is directed. We use parameter $\mathcal{D}$ to specify the directionality of an interdependent system. $\mathcal{D}$ is partitioned into two components, $\mathcal{D}^{i,j}$ and $\mathcal{D}^{j,i}$. The former specifies the fraction of directed dependencies that network i has on network j. The latter specifies the fraction of directed dependencies that network j has on network i. Systems of two extremes are identified. One extreme is an *undirected sy*stem, a system that is connected by undirected dependencies only, i.e., $\mathcal{D}^{i,j} = \mathcal{D}^{j,i} = 0$. Another extreme is a *directed* system, a system that is connected by directed dependencies only, i.e., $\mathcal{D}^{i,j} = \mathcal{D}^{j,i} = 1$. Real world systems usually have a mixture of directed and undirected links and hence sit in between these two extremes.

The proposed model captures some basic yet important features which have a significant role to play in characterising network interdependency. By configuring interdependent directionality, redundancy and extent, the model can represent, and simulate the performance of, interdependencies that are more representative of real world

[1] $\mathcal{F}$ could be generalised into a vector when number of networks $k > 2$. This also applies to parameters $\mathcal{K}$ and $\mathcal{D}$ as described below.

couplings. For example, a *one-way* interdependent system can be generated if we set $\mathcal{F}^{i,j} = 0$ and $\mathcal{F}^{j,i} > 0$, a typical relationship that exists between ICT and other infrastructure networks. An *unbalanced* interdependent system is modelled if we set $\mathcal{F}^{i,j}\mathcal{K}^{i,j} \neq \mathcal{F}^{j,i}\mathcal{K}^{j,i}$, a commonly observed relationship between a pair of interdependent networks.

3 Cascading failure model

In order for any network node to function, we assume that at least one of its supporting nodes from each of the networks on which it depends is available. Nodes fail via three mechanisms (i) through direct disruption; (ii) if it loses all of its supporting nodes from at least one of the networks that support it; (iii) finally, in line with percolation theory approaches [34], a node fails if it is disconnected from the largest component (the giant component) of the network to which it belongs.

We recognise that this is a simplified description of failure and that a number of other factors such as storage capacity, human intervention and component condition modulate failure processes. For example, if a road junction loses the control signal from its ICT network, it does not fail completely. Rather, its capacity for accommodating traffic flow is altered. By removing capacity, lag and latency, our analysis is more tractable and enables us to focus on generating insights into the implication of interdependency in a worst case scenario where these other factors are not able to modulate the failure processes.

For simplicity, we consider an interdependent system composed of two networks A and B, initially with size N_0^A and N_0^B. We assume that network disruption is initiated by disabling a fraction q of nodes from network A. When these nodes are removed, all their links fail (including both intra- and inter-links). The failure of these nodes and links may result in fragmentation of network A. Only the nodes belonging to the largest connected component are still functional, while nodes that are part of the remaining smaller network fragments become non-functional. The failure of these network A nodes removes or reduces the support that network B obtains from network A. A network B node fails if it loses all its supporting nodes from network A. The failure of network B nodes may cause fragmentation of network B. Again, only the nodes belonging to the largest component of B remain functional. We call this point the end of stage 1 of a cascading failure and record the numbers of nodes in the giant components of networks A and B at this stage as N_1^A and N_1^B.

During cascade stage 2, we remove nodes in A that have lost all their support from B, and then remove all A nodes that are disconnected from the largest component of A. We then apply the same to network B. We use N_t^A and N_t^B to specify the sizes of the largest components of the system at the end of stage t of the cascade of failure. At the end of the cascade process, both networks stop losing nodes, and the system stabilises at stage T when:

$$\begin{cases} N_{T+1}^A = N_T^A \\ N_{T+1}^B = N_T^B. \end{cases} \tag{1}$$

This is shown visually, for a system of size $N_0^A = N_0^B = 6$, in Figure 2 where the system stabilises at $t = 2$.

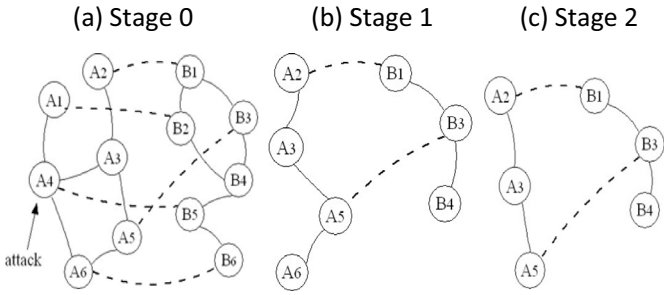

Fig. 2. Cascading failure process of an interdependent system. The initial system, shown in (a), has a set of nodes in network A and B, labelled $\{A_1, A_2, \ldots\}$ and $\{B_1, B_2, \ldots\}$, respectively. An intra-link is represented as a solid line, and an inter-link is represented as a dashed line. At Stage 0, node A_4 is disabled/attacked. When A_4 fails, all links connected to A_4 fail. This disconnects A_1 from the largest component of network A, and therefore A_1 fails. The failure of A_4 and A_1 triggers the failure of B_5 (supported by A_4) and B_2 (supported by A_1). The failure of B_5 disconnects B_6 from the largest component of network B, hence B_6 fails. This leads to the system configuration shown in (b). The failure of B_6 leads to the failure of A_6, before the system eventually stabilises in the configuration shown in (c).

We use the following measures to quantify the post-attack performance of an interdependent system.

(1) The connectedness of a system is measured by the relative size of the largest component, P, of the final stabilised system after the cascading failure, as follows:

$$\begin{cases} P = \frac{N_T^A + N_T^B}{N_0^A + N_0^B} \\ P^A = N_T^A / N_0^A \\ P^B = N_T^B / N_0^B. \end{cases} \tag{2}$$

The larger P is, the more nodes remain in the largest connected component, the better the system is considered to perform.

(2) The failure threshold q_c is the minimum size of disruption that causes a system to collapse to $P = 0$. The larger q_c is, the more robust the system.

(3) The aggregate performance, IP, characterises the behaviour of an interdependent system subjected to a full range of network disruption event sizes q_0, $q_1, \ldots, q_i, \ldots, q_n$ where $q_0 = 0$, $q_n = 1$ and $q_{i+1} > q_i$. IP is the integral of $P(q)$ which, for the n disruptions tested, is calculated as:

$$IP = \sum_{i=0}^{i=(n-1)} P_i \left(q_{i+1} - q_i\right). \tag{3}$$

A larger IP indicates a more robust system.

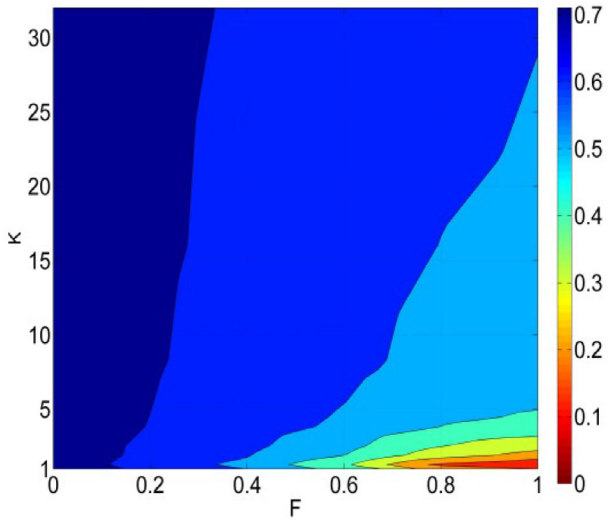

Fig. 3. Aggregated system performance IP of a directed interdependent system with $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = K$ and $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = F$.

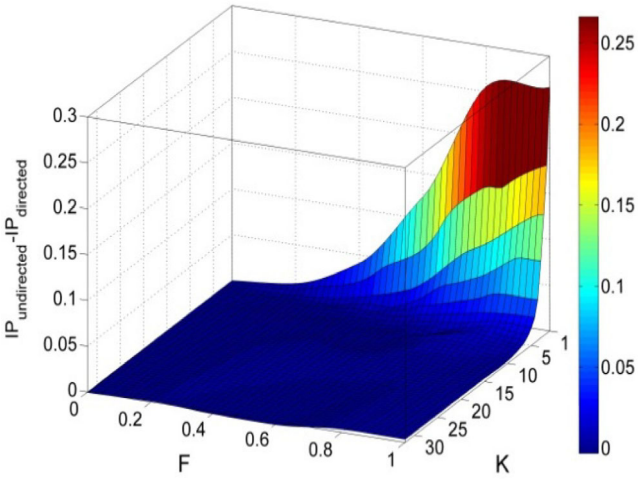

Fig. 4. Difference between the aggregate performance ($IP_{undirected} - IP_{directed}$) of *undirected* and *directed* systems when $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = K$ and $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = F$ are varied.

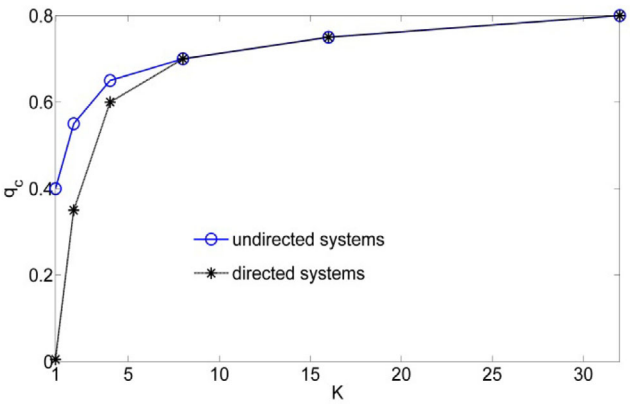

Fig. 5. Failure threshold, q_c, as a function of $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = \mathcal{K}$ when $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$.

4 Influence of interdependency

We measure the performance of interdependent systems over a wide range of extent, redundancy and directionality as defined in Section 2. This section analyses systems that consist of two Erdös-Rényi (ER) networks. We will explore the impact of network size, topology and disruption modes in Section 5.

Experiments were carried out over systems that couple two networks of $N_0^A = N_0^B = 10\,000$ nodes, with an average degree $K_0^A = K_0^B = 4$. We initiate disruption by removing a randomly selected fraction q of network A nodes. The choice of system size is based on our observation of real networks, in particular civil infrastructure systems. Most of these are characterised by large number of nodes (a few thousands or more), with a typically small degree distribution (often 3–4) [2,4,35], and with only a proportion of nodes dependent on another network. We therefore investigated a much wider variable space to consider not only how real-world systems perform, but how deviations from this might enhance or reduce performance.

4.1 Impact of interdependent directionality

The most vulnerable interdependent configuration is when two networks are inter-connected only with directional links, i.e. $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 1$. Figure 3 shows the aggregate performance of a directed interdependent system when $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = K$ and $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = F$ are varied, respectively. The worst performance (IP is nearly 0) occurs when $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1$ and $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 1$. In this situation, even a small portion of network disruption can cause catastrophic cascade and lead to the collapse of a whole system.

This compares to $IP \approx 0.3$ when the networks are connected via undirected links only, i.e. $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 0$, which is dramatic improvement over a directed system of otherwise the same configuration. Figure 4 shows the difference in performance between undirected and directed systems. For any given K and F a directed system never has greater IP, hence is more vulnerable than an undirected system. The greatest difference in performance occurs when $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} > 0.5$ and $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} < 5$. Our research shows that when $\mathcal{K}$ is sufficiently large or $\mathcal{F}$ is very small, the IP of a directed system approaches that of an undirected system.

The robustness of an undirected system is further manifested by the facts that it has a larger failure threshold q_c than a directed system. As shown in Figure 5, the smaller $\mathcal{K}^{B,A}$ and $\mathcal{K}^{A,B}$ (or the larger $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$, see Fig. S5 of the supplementary information*), the bigger the impacts they make, and the larger performance differences observed between two extremes of systems.

The main reason for the poorer performance of a directed system is that it presents more possibilities for the existence of longer *dependency chains* than an undirected system. A dependency chain exists where a network A node, u, supports a network B node, v, and v in turn

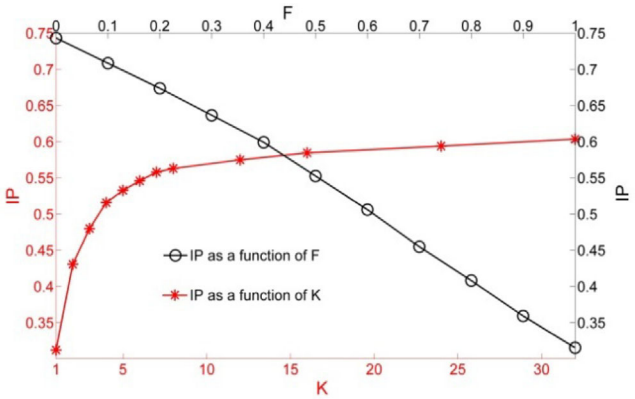

Fig. 6. Aggregate performance IP as a function of K ($\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = K$, $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1$ and $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 0$), and IP as a function of F ($\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = F$, $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 1$ and $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 0$).

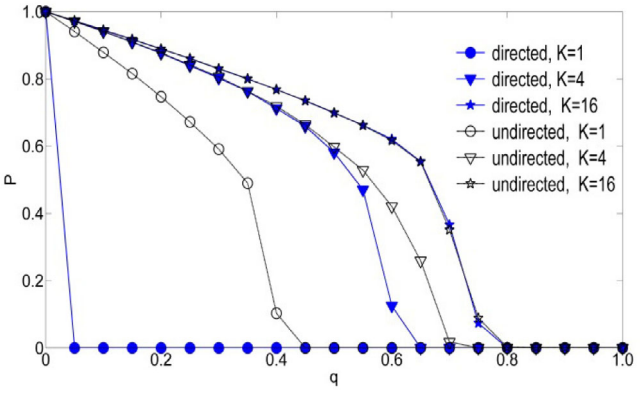

Fig. 7. Relative size of giant component P as a function of q (the size of the attack on network A), where $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$, and $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = K$ are varied.

supports a further network A node w (where $w \neq u$), and so on. These dependency chains run back and forth between the two inter-connected networks. A failure of u compromises the robustness of all *downstream* nodes in the dependency chain, potentially triggering their failure and a possible cascade.

In an undirected system, as inter-network dependency is mutual, when u supports v, v also supports u. As well as u, v supports $\mathcal{K}^{B,A} - 1$ other A nodes, i.e., v introduces $\mathcal{K}^{B,A} - 1$ nodes into the dependency chain. However, in a directed setting, as inter-network dependencies are not symmetric, v does not necessarily support u, instead introducing $\mathcal{K}^{B,A}$ additional A nodes into the dependency chain. Hence in a directed system dependency chains tend to be longer than in an undirected system, causing a more effective propagation of failure across networks and an increased system vulnerability. The smaller $\mathcal{K}^{B,A}$, the greater the difference made by switching from undirected to directed dependencies (Fig. 5), which is consistent with other analysis [36].

4.2 Impact of interdependent extent $\mathcal{F}$ and redundancy $\mathcal{K}$

The vulnerability of an interdependent system can be reduced by either increasing $\mathcal{K}^{B,A}$ and $\mathcal{K}^{A,B}$ or decreasing $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$, as illustrated in Figure 6. Our experiments reveal that system performance (in terms of P) increases linearly as $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$ decrease. An interdependent system improves its performance at a slow rate when we increase $\mathcal{K}^{B,A} = \mathcal{K}^{A,B} = \mathcal{K}$, and a good fit[2] to the simulated results was observed for $P = a + b\sqrt{\log(K)}$. Increasing $\mathcal{K}^{B,A}$ and $\mathcal{K}^{A,B}$ is more effective when $\mathcal{K}^{B,A}$ and $\mathcal{K}^{A,B}$ are small and this strategy becomes less responsive when $\mathcal{K}^{B,A}$ and $\mathcal{K}^{A,B}$ are large (exceeding 8 in this setting). On the other hand, decreasing $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$ can achieve a more consistent performance gain throughout the range of $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$. However, it is important to note that two strategies for reducing vulnerability do not represent the same cost. Whilst the performance gain achieved by increasing $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 1$ to $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$ can be accomplished by decreasing $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1$ to $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} \approx 0.75$, however, if all nodes in network B are fully dependent on a connection to network A (e.g. all components in one network may require connection to an electricity grid) then options for altering $\mathcal{F}$ will be limited, or require development of new decentralised energy systems which must be balanced against the costs of doubling the number of inter-network connections associated with doubling $\mathcal{K}$.

Low interdependent redundancy not only leads to reduced system performance, but also abrupt system failure, as shown in Figure 7. Under the setting of $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$, when $\mathcal{K}^{A,B}$ and $\mathcal{K}^{B,A}$ are small, a large functioning component exists when $q < q_c$, and it suddenly collapses when q reaches q_c. Increasing $\mathcal{K}^{A,B}$ and $\mathcal{K}^{B,A}$ can ease off the abruptness of network failure and results in a relatively continuous phase transition at q_c[3]. This is because the larger $\mathcal{K}^{A,B}$ and $\mathcal{K}^{B,A}$, the more support a node receives from another network. In this instance, both network A and B behave as independent networks. Our experiment indicates that as there is little cascading effect, P^A will tend to approach the size of a giant component for a single network of the same scale[4]; for network B, when $q < q_c$, removing nodes from network A does not impact on the integrity of network B and P^B approaches 1.0. Network B collapses only when network A collapses, i.e., P^B approaches zero when $q > q_c$.

The abrupt failure was only observed on systems when $F^{A,B}$ and $F^{B,A}$ are sufficient large, e.g. greater than 0.5 under the setting of $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$, as shown in

[2] The values of a and b depend on the setting of $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$, and $a = 0.325$ and $b = 0.152$ were identified for the setting and results presented in Figure 6.

[3] Phase transition here means the change of network size from non-zero to zero.

[4] See Section 1 of the supplementary information* for the performance comparison between interdependent and single, isolated systems.

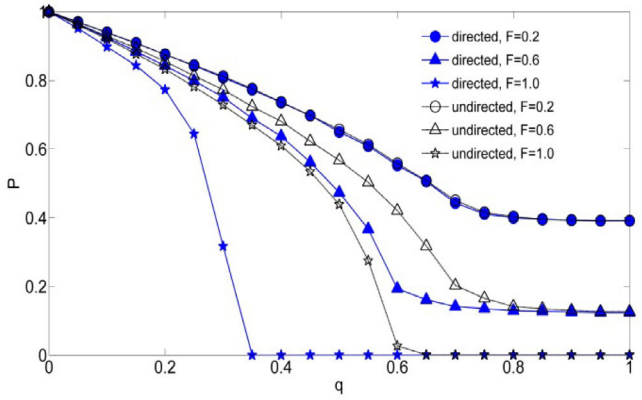

Fig. 8. Relative size of giant component P as a function of q (the size of the attack on network A), where $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$, and $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = F$ are varied.

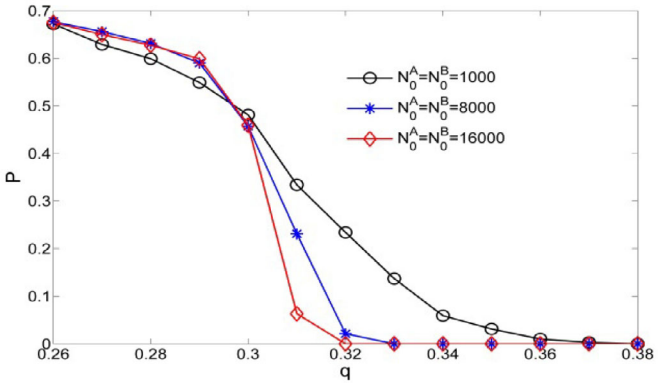

Fig. 9. Impact of network size. P is plotted as a function of q. Results are obtained on systems with $K_0^A = K_0^B = 4$, $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$, $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$ and $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 1$.

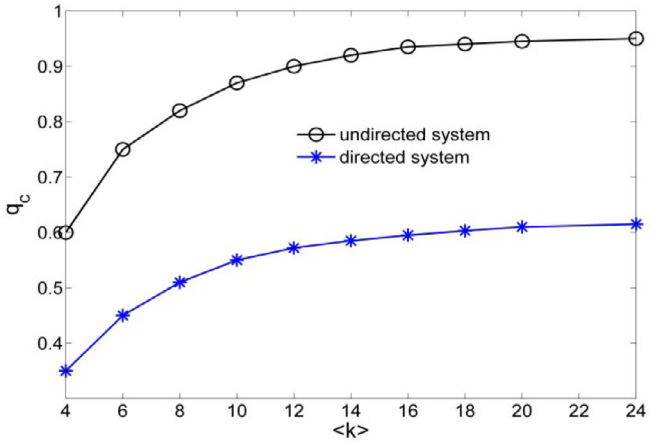

Fig. 10. Impact of network node degree. Failure threshold q_c is plotted as a function of $K_0^A = K_0^b = \langle k \rangle$ for systems under the interdependency setting of $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$ and $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$.

Figure 8. This is because the larger $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$, the more tightly network A and B depend on each other. This naturally results in increased propagation of failure across networks, and the reduced system performance. When $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$ are small, the performance of systems approach that of single networks, exhibiting a relatively continuous phase transition, but with A and B behaving differently. P^A is zero but P^B is non-zero at the end of a cascade. Total fragmentation of network B happens in a cascade only when $\mathcal{F}^{B,A}$ (the fraction of dependent nodes in network B) exceeds the failure threshold of a single network of the same properties as network B. When $\mathcal{F}^{B,A}$ is smaller than the failure threshold of such a single network, collapse of network A does not cause the collapse of network B, and P^B approaches the size of the giant component of a single network when it has $\mathcal{F}^{B,A}$ fraction of nodes removed. This results in the non-zero P as shown in Figure 8. Examples of such a phenomenon are often observed in a coupled gas and electricity system. When only a small portion of an electricity network relies on a gas network for fuel supply, the collapse of the gas network will only disrupt a portion of the electricity network.

In summary, varying interdependency can modify system behaviour and the limits within which it can operate safely. Systematically testing a range of interdependency configurations has provided a more complete picture of the role interactions between networks play in mediating system performance[5]. Subsequent sections consider the influence of other network properties, and potential countermeasures to mitigate vulnerabilities associated with interdependency.

5 Influence of network sizes, topologies and disruption modes

The performance of an interdependent system can be influenced by factors such as network size, topologies and disruption modes.

[5] Readers are referred to the supplementary information* for additional supporting analysis.

5.1 Network size

We applied our model to interdependent systems comprising different numbers of network nodes, N_0^A and N_0^B, and average node degree, K_0^A and K_0^B. These results exhibit similar trends and patterns to those reported in Section 4. Aggregate system performance IP and failure threshold q_c varies very little for a range of network sizes. However, Figure 9 indicates that P (size of giant component) collapses more abruptly for larger networks. Thus, and perhaps non-intuitively, larger interdependent systems can be more fragile. This agrees with results reported in reference [12].

Furthermore, the performance of interdependent networks is shown to improve when we increase node degrees K_0^A and K_0^b. Figure 10 shows that q_c increases with $K_0^A = K_0^b = \langle k \rangle$. This observation is consistent with the analytical solution obtained for a single network [34] for ER networks.

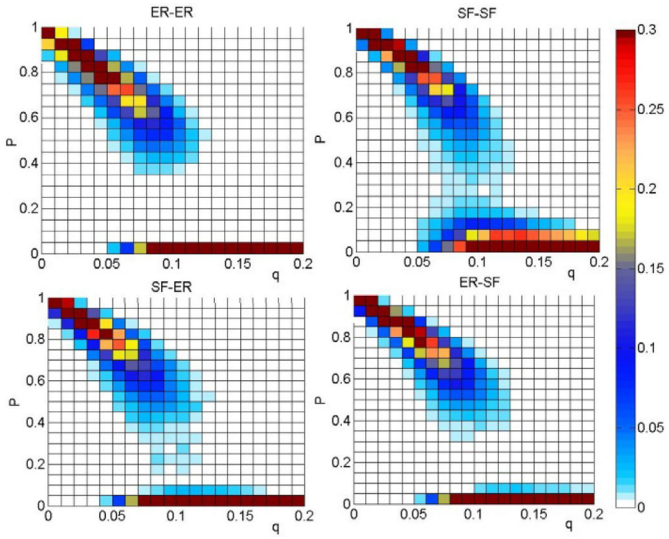

Fig. 11. Impact of network topologies. Frequency of relative size of giant component P is plotted as a function of q and P Dependencies are set with $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 1$, $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 0.8$ and $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 1$.

5.2 Network topology

We also studied systems that couple networks of different topologies[6]. These results show similar trends and patterns in overall performance to those reported for the ER-ER networks in Section 4 (see Fig. S6 of the supplementary information⋆). However, the aggregate measure of performance, IP, obfuscates variability in system behaviour. Figure 11 shows the variability of giant component size, P, for a given initial network disruption q, and the frequency that a system stabilises at P, for q.

Variability is greatest in a system that couples two scale free networks (SF-SF system) and smallest in an ER-ER system. The parameter region where variability is greater is for small P (when $P < 0.5$ in this setting). This suggests that a SF-SF system is more volatile or unpredictable, when compared with similar systems that contain one or more ER networks. The lower variability of P for ER-ER systems stems from the more uniform node degree distribution of ER networks, so that the initial failure is over nodes of similar connectivity. The greater variability of node degree distribution of a SF network makes performance more sensitive to the connectivity of nodes that are disabled. This results in different forms of network fragmentation and thus a wider range of P.

5.3 Network disruption strategy

Network disruption strategies can influence system performance. We explore two types of deliberate attack: high degree node biased attack (highBias attack) and low degree node biased attack (lowBias attack) on both SF-SF and ER-ER systems (Fig. 12) (see Fig. S7 of the supplementary information⋆ for the results on ER-SF and SF-ER systems). For the highBias attack, we set the probability that a node is disrupted as being proportional to its degree. In lowBias attack, the probability is inversely proportional to its degree. The SF-SF are most heavily impacted by highBias attacks, but perform better when subjected to lowBias attacks. The degree distribution of SF networks leads to more highly connected hub nodes compared to ER networks. Consequently highBias attacks lead to more fragmentation in a system with SF networks than in a system with ER networks. On the other hand, due to the existence of a large portion of low degree nodes in SF networks, when lowBias attack is employed, nodes of lower connectivity are preferentially targeted so the SF-SF systems outperform the other configurations as a result of a lowBias attack.

[6] We focus on ER and SF networks as they are consistent with the structure of many social and engineered systems, enabling us to interpret results in the context of real systems.

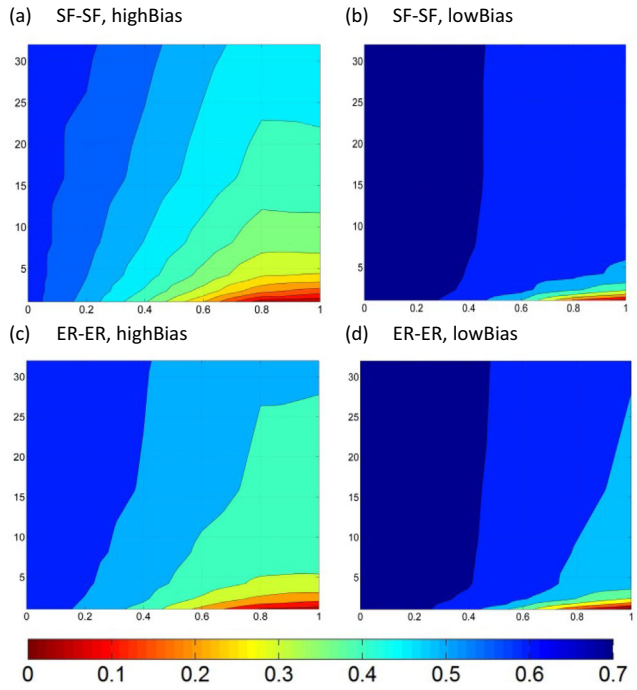

Fig. 12. Results for systems under lowBias and highBias attacks. Aggregate performance IP is plotted as a function of $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = K$ (vertical axis) and $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = F$ (horizontal axis), under dependency setting of $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 1$.

6 Reducing vulnerability: outlook and discussion

Results presented in previous sections indicate that vulnerability can be introduced into systems when network structures and interdependency are sub-optimal. The performance of interdependent systems can be improved if the extent of dependency decreases or the redundancy of dependency increases, as we discussed earlier. In this section we present two alternative countermeasures to reduce the vulnerability of interdependent systems.

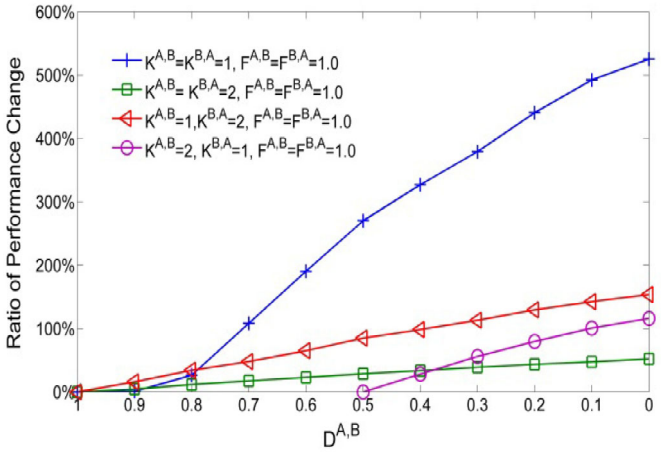

Fig. 13. Reducing vulnerability: ratio of performance change in term of aggregate performance IP, when the proportion, $\mathcal{D}^{A,B}$, of directed dependencies decreases in an interdependent system.

6.1 Optimising interdependent directionality

Results in Section 4 indicate that a directed system is more vulnerable than an undirected system. In this section we study how a directed system might improve its performance through turning directed dependencies into undirected dependencies. To do this, we start with a system that has maximum possible directed links, e.g. $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 1$. We gradually decrease $\mathcal{D}^{A,B}$ and $\mathcal{D}^{B,A}$ until it reaches the lowest limit or becomes an undirected system[7]. We record how the system changes its performance against that of the original system. Figure 13 presents our results for a few different settings of $\mathcal{K}^{A,B}$, $\mathcal{K}^{B,A}$, $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$.

A dramatic improvement was observed for relatively vulnerable systems, e.g., systems where $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 1$ and $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$. For such systems, by turning 30% of the directed links to undirected links, over 100% performance improvement can be achieved. The improvement reaches 270% when 50% of the directed links were turned into undirected links. However, the effectiveness of this strategy reduces for systems with large $\mathcal{K}^{A,B}$ and $\mathcal{K}^{B,A}$ or small $\mathcal{F}^{A,B}$ and $\mathcal{F}^{B,A}$. For example, the 270% improvement achieved in the last case drops to only about 30% when $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$. Hence we can conclude that changing directed links into undirected links is a cost effective way to reduce vulnerability. Without introducing additional dependency links (and therefore cost), this strategy is extremely effective for systems that are particularly vulnerable to cascading failure, i.e, those with a significant extent of dependency, but a low degree of redundancy in these dependencies.

[7] Since undirected dependencies are symmetric, $\mathcal{D}^{A,B}$ and $\mathcal{D}^{B,A}$ relate to each other via equation $\left(1-\mathcal{D}^{A,B}\right)\mathcal{F}^{A,B}\mathcal{K}^{A,B} = \left(1-\mathcal{D}^{B,A}\right)\mathcal{F}^{B,A}\mathcal{K}^{B,A}$. This can restrict what values $\mathcal{D}^{A,B}$ and $\mathcal{D}^{A,B}$ can take. The effect of this is shown in Figure 13, where in certain scenarios the range of $\mathcal{D}^{A,B}$ is [0.5,1.0] instead of [0.0,1.0].

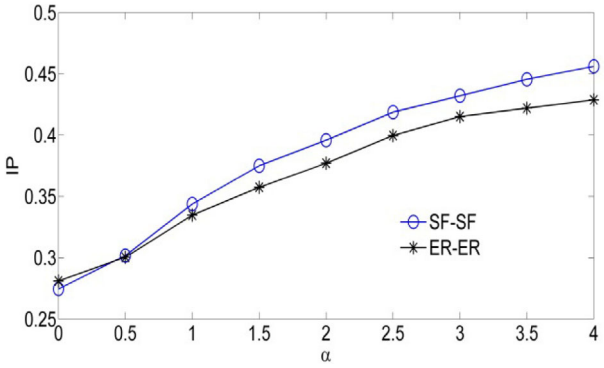

Fig. 14. Performance improvement when high degree nodes are hardened. Aggregate performance, IP, is plotted as function of α as specified in equation (4). Both SF-SF and ER-ER systems have dependency setting $\mathcal{D}^{A,B} = \mathcal{D}^{B,A} = 1$, $\mathcal{F}^{A,B} = \mathcal{F}^{B,A} = 1.0$ and $\mathcal{K}^{A,B} = \mathcal{K}^{B,A} = 2$.

6.2 Hardening high degree nodes

Since the failure of high degree nodes is more likely to lead to large scale network fragmentation, we investigated the effect of *hardening* or *protecting* high degree nodes as a means to reducing vulnerability. We explore the strategy that improves the *hardness* of a high degree node and make it less likely to fail when facing an attack. In our experiments, we assign the level of hardening that a node receives as proportional to its degree such that the failure probability of a node is inversely proportional to its degree:

$$P(k) \sim \frac{1}{k^{\alpha}} \tag{4}$$

where $\alpha \geqslant 0$. When $\alpha = 0$, $P(k)$ has the same value for all k, i.e. the model simulates a scenario that all nodes receive same level of protection. For $\alpha > 0$, higher values indicate increased hardening of high degree nodes. By tuning α, we can configure the significance of protecting high degree nodes. Figure 14 plots how the performance of SF-SF and ER-ER systems improves when we increase α. Aggregate performance IP is shown to increase with α for all the networks considered in our research. SF-SF networks exhibit the greatest performance gains because protection of their high degree hub nodes reduces the probability of large scale fragmentation. The more investment we put on protecting high degree nodes, the more performance gain we obtain. However care must be taken when practising this method due to the cost involved.

In summary, the vulnerability of an interdependent network is shown to be reducible either by optimising inter-network connections, or by hardening high degree nodes. Our additional research on reducing the vulnerability of interdependent systems is in the supplementary document*.

7 Conclusions

This paper presents an approach to studying the vulnerability of interdependent systems. The proposed network

model characterises interdependencies along multiple dimensions, and provides the capacity to capture many of the interdependencies encountered in natural, engineered or social systems. Unlike previous research where the description of interdependency was more limited, thereby enabling analytical solutions to be found, we have sought to understand interdependencies through numerical simulations. Our research reveals that varying the nature of cross-network dependency can modify the behaviour of an interdependent system and hence change the conditions for its safe operation. The most salient findings are:

- The *directionality, extent and redundancy* that we use to characterise inter-network dependency are pertinent properties that mediate the performance of an interdependent system.
- The disruption to a system can be disproportionate to attack size when inter-network dependent configurations are sub-optimal.
- Networks with directed dependencies are less robust than those with undirected dependencies.
- The degree of redundancy in inter-network dependencies can have a differential effect on robustness depending on their direction.

The above observations are applicable to a range of classical network topologies, which include structures observed in many social and engineered systems. However, the performance of interdependent networks is heavily influenced by attack mechanisms. A large scale system is more likely to experience abrupt collapse during a cascade than a small scale system does. Networks with hubs, or broad degree distributions were more sensitive to degree biased attacks, and they exhibited much wider variability in their system response when the surviving components of these systems are small.

The most vulnerable interdependent configuration is for networks to have each node connected to another network by a directed link, but with few redundant connections. As most real-world systems have a very small number of redundant inter-connections and such interdependencies are rarely wired mutually or symmetrically between networks, we expect they often operate near their critical points and significant cascading failure could be triggered by a relatively small scale initial disruption. This is consistent with real examples of failure across inter-connected infrastructure systems, such as the 2003 Italy power blackout [37] and the 2009 UK Cumbrian floods [38]. Typically, infrastructure systems are managed independently of each other so understanding the best strategies to protect the network for which an operator is responsible must account for dependencies with other networks. We have demonstrated several strategies for improving the performance of interdependent systems and shown that the magnitude of cascading failure can be significantly decreased when the directionality of inter-network dependencies is optimised. *Hardening* high degree nodes is another effective way to improve system performance.

The model describes important features of network interdependencies that have been observed in real systems. The results represent an improved understanding of complex interdependencies and risks associated with them. We recognise that they do not capture all the processes associated with failure of real systems but provide conservative insights into the implications of different interdependent structures on network performance. We are extending this analysis to consider issues around capacity and flow in network connections and the spatial properties of systems.

This research is supported by the UK EPSRC Resilient Futures project (EP/I005943/1). Richard Dawson is funded by an EPSRC fellowship (EP/H003630/1). We are grateful to other members of the Resilient Futures team for motivating and interesting discussions on network disruption and resilience. We thank the anonymous reviewers for the careful reading of our manuscript and the valuable comments, which significantly contributed to improving the quality of the paper.

References

1. *The Structure and Dynamics of Networks*, edited by M. Newman, A. Barabasi, D. Watts, 1st edn. (Princeton University Press, USA, 2006)
2. R. Albert, A. Barabasi, Rev. Mod. Phys. **74**, 47 (2002)
3. J.F. Donges, H.C.H. Schultz, N. Marwan, Y. Zou, J. Kurths, Eur. Phys. J. B **84**, 635 (2011)
4. R. Albert, I. Albert, G.L. Nakarado, Phys. Rev. E **69**, 025103 (2004)
5. R. Cohen, K. Erez, D. Ben-Avraham, S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001)
6. P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, Physica A **340**, 388 (2004)
7. Y.K. Rui, Y.F. Ban, J.W. Wang, J. Haas, Eur. Phys. J. B **86**, 74 (2013)
8. C. Ten, C. Liu, G. Manimaran, IEEE T. Power Syst. **23**, 1836 (2008)
9. M. Rosas-Casals, S. Valverde, R.V. Sole, Int. J. Bifurcation Chaos Appl. Sci. Eng. **17,** 2465 (2007)
10. T. Hasegawa, K. Konno, K. Nemoto, Eur. Phys. J. B **85**, 262 (2012)
11. J. Gao, S. Buldyrev, S. Havlin, H. Stanley, Phys. Rev. Lett. **107**, 195701 (2011)
12. S. Buldyrev, R. Parshani, G. Paul, H. Stanley, S. Havlin, Nature **464**, 1025 (2010)
13. C.D. Brummitt, R.M. D'Souza, E.A. Leicht, Proc. Natl. Acad. Sci. USA **109**, E680 (2012)
14. O. Min, H. Liu, Z. Mao, M. Yu, F. Qi, Simul. Model. Pract. Theor. **17**, 817 (2009)
15. E. Zio, G. Sansavini, IEEE Trans. Reliab. **60**, 94 (2011)
16. S. Rinaldi, J. Peerenboom, T. Kelly, IEEE Contr. Syst. Mag. **21**, 11 (2001)
17. C.M. Schneider, N. Yazdani, N. Araujo, S. Havlin, H.J. Herrmann, Sci. Rep. **3**, 1969 (2013)
18. S. Dunn, G. Fu, S. Wilkinson, D. Dawson, Proc. Inst. Civ. Eng., Eng. Sustain. **166**, 281 (2013)
19. R. Little, J. Urban Technol. **9**, 109 (2002)
20. *Networks of Networks: the Last Frontier of Complexity*, edited by G. D'Agostino, A. Scala, 1st edn. (Springer, Cham, Heidelberg, 2014)

21. R. Parshani, S. Buldyrev, S. Havlin, Phys. Rev. Lett. **105**, 048701 (2010)
22. L. Dueñas-Osorio, S. Vemuru, Struct. Saf. **31**, 157 (2009)
23. S. Buldyrev, N. Shere, G. Cwilich, Phys. Rev. E **83**, 016112 (2011)
24. M. Kurant, P. Thiran, P. Hagmann, Phys. Rev. E **76**, 026103 (2007)
25. K. Lee, J. Kim, W. Cho, K. Goh, I. Kim, New J. Phys. **14**, 033027 (2012)
26. J. Gao, S. Buldyrev, S. Havlin, H. Stanley, Phys. Rev. E **85**, 066134 (2012)
27. A. Bashan, Y. Berezin, S. Buldyrev, S. Havlin, Nat. Phys. **9**, 667 (2013)
28. S.W. Son, G. Bizhani, C. Christensen, P. Grassberger, M. Paczuski, Europhys. Lett. **97**, 16006 (2012)
29. M.A.B. Promentilla, J.F.D. Tapia, C.A. Arcilla, N.P. Dugos, P.D. Gaspillo, S.A. Roces, R.R. Tan, Environ. Modell. Softw. **50**, 21 (2013)
30. X. Huang, J.X. Gao, S. Buldyrev, S. Havlin, H. Stanley, Phys. Rev. E **83**, 065101 (2011)
31. W. Kröger, C. Nan, in *Networks of Networks: the Last Frontier of Complexity Understanding Complex Systems*, edited by G. D'Agostino, A. Scala, 1st edn. (Springer, Cham, Heidelberg, 2014), p. 279
32. M. Beccuti, G. Franceschinis, M. Kaaniche, K. Kanoun, Critical Information Infrastructures Security **5508**, 48 (2009)
33. J.C. Laprie, K. Kanoun, M. Kaaniche, in *Proceedings of the 26th international conference on Computer Safety, Reliability, and Security, Germany, 2007*, edited by F. Saglietti, N. Oster (Springer-Verlag, Berlin, 2007), p. 54
34. D.S. Callaway, M.E.J. Newman, S.H. Strogatz, D.J. Watts, Phys. Rev. Lett. **85**, 5468 (2000)
35. M. Kurant, P. Thiran, Phys. Rev. E **74**, 036114 (2006)
36. W. Li, A. Bashan, S. Buldyrev, H. Stanley, S. Havlin, Phys. Rev. Lett. **10**, 228702 (2012)
37. V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. De Porcellinis, R. Setola, Int. J. Crit. Infrastruct. **4**, 63 (2008)
38. *Resilience of UK Infrastructure* (Parliamentary Office of Science & Technology, UK, 2010)