Khoury *et al. Infrastructure Complexity* (2015) 2:1
DOI 10.1186/s40551-015-0004-9

Infrastructure Complexity
a SpringerOpen Journal

RESEARCH Open Access

Improving measures of topological robustness in networks of networks and suggestion of a novel way to counter both failure propagation and isolation

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

Abstract

The study of interdependent complex networks in the last decade has shown how cascading failure can result in the recursive and complete fragmentation of all connected systems from the destruction of a comparatively small number of nodes. Existing "network of networks" approaches are still in infancy and have shown limits when trying to model the robustness of real-world systems, due to simplifying assumptions regarding network interdependencies and post-attack viability. In order to increase the realism of such models, we challenge such assumptions by validating the following four hypotheses trough experimental results obtained from computer based simulations. Firstly, we suggest that, in the case of network topologies vulnerable to fragmentation, replacing the standard measure of robustness based on the size of the one largest remaining connected component by a new measure allowing secondary components to remain viable when measuring post-attack viability can make a significant improvement to the model. Secondly, we show that it is possible to influence the way failure propagation is balanced between coupled networks while keeping the same overall robustness score by allowing nodes in a given network to have multiple counter parts in another network. Thirdly, we challenge the generalised assumption that partitioning between networks is a good way to increase robustness and find that isolation is a force as equally destructive as the iterative propagation of cascading failure. This result significantly alters where the optimum robustness lies in the balance between isolation and inter-network coupling in such interconnected systems. Finally, we propose a solution to the consequent problem of seemingly ever increasing vulnerability of interdependent networks to both cascading failure and isolation: the use of permutable nodes that would give such systems rewiring capabilities. This last concept could have wide implications when trying to improve the topological resilience of natural or engineered interdependent networks.

Keywords: Resilience; Robustness; Interdependent networks; Symbiotic networks

Background

Avoiding a financial crisis, tackling global warming, or creating resilient infrastructures are problems that require researchers to look at the world from a "system of systems" perspective. Indeed, studying such physical or social systems in isolation does not grant sufficient information to capture the dynamics of an environment where global and local events result from the emergent complexity of interactions between different interdependent entities. Although network theory cannot in its present infant state model accurately real life interconnected complex networks such as infrastructures in all their complexity, it has nonetheless become a useful tool to discover certain basic topological rules that even these complex structures follow when confronted with cascading failure. Recent work modelling the robustness of "network of networks" (Buldyrev et al. 2010; Dunn et al. 2013; Gao et al. 2012, 2014; Leicht and D'Souza 2009; Parshani et al. 2010) has indeed demonstrated that taking into account the interdependencies between connected systems gives very different outcomes due to phenomena such as the amplification of the propagation of cascading failures. The

*Correspondence: mehdi.khoury@gmail.com
[1] University of Southampton, Highfield, SO17 1BJ Southampton, UK
Full list of author information is available at the end of the article

state of the art of network theory as a high-level modelling tool broadly stems from two different sources: mathematical models inspired from statistical physics and computer graph based simulations. As this field of research is still in infancy, such models are presently inevitably limited when trying to tackle complex real world networks from a practical point of view. We therefore limit the scope of this work to a study of network topology robustness to node removal in an abstract context, and avoid claims of modelling the functional robustness of real infrastructure networks, or any sort of risk analysis based on practical engineering concepts. This being said, we believe that some of the improvements we suggest to the network theory based model of robustness for coupled networks can be used to derive some potentially useful mechanisms to protect engineered networks from cascading failure and isolation from a topological perspective.

In this work, we consider the following four research questions and corresponding hypotheses. Firstly, can standard models of evaluation of multi-network vulnerability to cascading failure that rely on the existence of one largest connected component that remains in each network after losses lead to some substantial inaccuracies in some circumstances? We suggest that, in cases of network topologies vulnerable to fragmentation, modifying this model of robustness by allowing secondary components to remain viable when measuring post-attack viability can make a significant improvement. Secondly, if standard models of evaluation of multi-network vulnerability define the coupling relationship between nodes belonging to different networks to be one-to-one mappings, can allowing a node in given network to have multiple counter parts in another network change the system significantly? We suggest that it can have consequences on the way failure propagation is balanced between the coupled networks. Thirdly, is the generalised assumption that partitioning between network is a good way to decrease vulnerability to cascading failure in a network of networks misleading? We suggest that, introducing isolation as a force as equally destructive as failure propagation can alter drastically where the optimum robustness lies in such interconnected systems. Finally, we propose a solution to the consequent problem of seemingly ever increasing vulnerability of interdependent networks to both cascading failure and isolation: the use of permutable nodes that would give such systems rewiring capabilities.

I order to address these questions, the paper is structured as follows: after briefly expending on what the scope of this work does not cover (we do not claim to map interconnected abstract networks to real interdependent infrastructure networks), we then suggest changes to improve shortcomings of the topologically centred evaluation of multi-network vulnerability. An overview of the design of models and experiments is presented, as well as a description of the procedures, statistics, and metrics used to answer the research questions. Experimental results are then shown and interpreted. Finally the significance of the new adopted assumptions is discussed in term of changes to our understanding of the robustness of real interdependent networks, while some of the shortcomings of this work are identified leading to suggested potential improvements and novel avenues to explore.

The problem of mapping network theory to real-life interconnected infrastructure networks

Although a promising modelling paradigm, the topologically centred evaluation of multi-network vulnerability is still in infancy and has shown limits when trying to model real world problems such as, for example, infrastructures power grids blackouts (Hines et al. 2010) where the authors conclude that "evaluating vulnerability in power networks using purely topological metrics can be misleading". Another typical example of graph theory used to try to model the resilience of an electric power networks can be found in (Cerda Jacobo 2010). It presents the downside that it is mostly applied to DC (Direct Current) models of power flow (a simplified representation (Wood and Wollenberg 1996) of the Alternative Current or AC voltage). This limits the practical value of network theory as a high-level modelling tool in this area as most of the power transmission systems in use are based on AC. A long list of similar examples could be taken from the literature, and confirm that, despite ongoing efforts, network theory is still a world apart from practical engineering solutions.

But a closer look to the literature also provides examples of fundamental rules derived from network theory in an abstract context that are applicable to real life networks from a topological point of view. One example is the phenomenon of amplification of cascading failure in interconnected networks (Buldyrev et al. 2010; Dunn et al. 2013; Gao et al. 2012, 2014; Leicht and D'Souza 2009; Parshani et al. 2010), and another one the identification of the vulnerable portions of a network to different attacks by looking at distinct measures of centrality. These measures vary from degree (number of connections of a node), to betweeness-centrality and other complex and various types of centrality (Beyeler et al. 2007; Crucitti and Latora 2005; Crucitti et al. 2006; LaViolette et al. 2006; Newman 2003). From an attack/defense perspective these measures are vital to locate critical nodes in a network (Crucitti et al. 2004; Dorogovtsev et al. 2008; Motter 2004).

Therefore, we first want to emphasize that the work presented in this paper does not claim to analyse the functional robustness of real infrastructure networks, nor does it try to model these from a risk analysis perspective based on practical engineering concepts. We instead limit the scope of this work to study network topology

robustness to node removal. Nevertheless, we still believe that some of the findings presented in this paper might present some useful insight in a practical engineering context, in particular the fact that isolation can be as equally destructive as the propagation of cascading failure when determining the topological robustness of interdependent networks. One unexpectedly practical and perhaps potentially useful find derived from this observation is the suggestion of permutable nodes as an adaptive mechanism that could optimise interdependent networks topological robustness. Such a mechanism appears to protect coupled networks from the destructive consequences of isolation and cascading failure and at the same time preserves network resources by limiting the amount of redundancy needed to absorb a disturbance. In other words, while nodes that can provide simultaneous links to different networks tend to propagate cascading failure .i.e an electric line that would carry phone communications at the same time would in fact propagate topological failure through both phone and electricity networks in case of malfunction while, on the other hand, nodes that can provide alternated states of coupling to different networks limit the topological propagation of cascading failure while providing an alternate configuration to the system because of their rewiring capabilities .i.e. roads convertible to landing strips, the Stormwater Management and Road Tunnel (SMART) in Kuala Lumpur (a tunnel that can alternate between traffic and storm water management), energy storage devices on board electric vehicles that can be plugged to the power grid when not in use so as to store and produce energy whenever needed, or plants that generate electricity for production and that can shut down production and sell power instead.

Four suggested changes to improve models of the robustness of network of networks to cascading failure

Some of the shortcomings of the topologically centred evaluation of multi-network vulnerability as a modelling tool are rooted in the existence of assumptions that simplify the nature and extent of network interdependency and the rules that establish the post-attack viability of a connected component. In order to increase the realism of existing models of robustness of interdependent networks, we change these assumptions as follows: firstly, we propose to allow secondary components to remain viable when simulating cascading failure. Secondly, we introduce many-to-one interdependent mappings and analyse the consequences of allowing a node in given network to have multiple counter parts in another network. Thirdly, we present a measure of the symbiotic viability of network components when faced with isolation that results in novel strategies on how to achieve robustness in interdependent complex networks. Finally, we also propose a solution to the consequent problem of seemingly ever increasing vulnerability of interconnected networks introduced by these symbiotic dependencies: the introduction of permutable nodes that would give such systems rewiring capabilities.

Suggested change to the first assumption: changing the post-attack viability when secondary components remain viable

The first assumption found in many contemporary models of multi-network resilience relates to post-attack viability. Robustness has generally been evaluated using an iterative cascading failure process based on percolation theory where only the one largest connected component remains in each network after losses. Usually, no secondary component is considered alive (Albert et al. 2000a; Bak et al. 1988; Brummitt et al. 2012; Buldyrev et al. 2010; Callaway et al. 2000; Cohen and Havlin 2002; Latora and Marchiori 2005; Leicht and D'Souza 2009; Najjar and Gaudiot 1990; Parshani et al. 2010). The first modification suggested in this work is to allow secondary components to remain viable when estimating the robustness of a system. When evaluating the robustness of coupled networks, the standard approach (Albert et al. 2000a; Bak et al. 1988; Brummitt et al. 2012; Buldyrev et al. 2010; Callaway et al. 2000; Cohen and Havlin 2002; Latora and Marchiori 2005; Leicht and D'Souza 2009; Najjar and Gaudiot 1990; Parshani et al. 2010) has been to measure the size of the one largest connected component remaining in each interdependent network. This way of evaluating a pair of coupled networks ignores secondary components and their potential influence on the post-attack performance on such a system. However, in fragmented networks, the presence of secondary clusters could significantly increase system performance (as illustrated in the first row of Figure 1). Consequently, we propose to evaluate the post-attack viability of a network by summing up the relative sizes of all components above some critical minimum number of nodes.

Suggested change to the second assumption: changing dependency links from one-to-one to one-to-many mappings between networks

A second assumption widely in use in state of the art models representing inter-network dependencies (Buldyrev et al. 2010; Fu et al. 2014; Gao et al. 2012; Parshani et al. 2010) defines the coupling relationship between nodes belonging to different networks to be one-to-one mappings (e.g. a node from network A is coupled to a unique distinct node in a network B). Existing work tends to focus on varying the density, the correlation

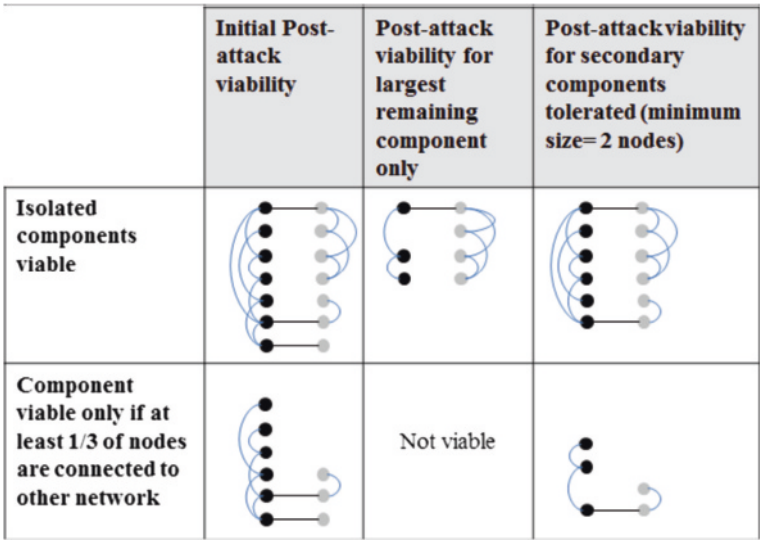

Figure 1 Single versus multiple components post attack viability. We visualise what is left of interdependent networks after attack depending on different post-attack viability rules: single versus multiple components tolerated, and isolated versus dependent clusters.

structure, and the directed versus undirected character of dependencies in order to analyse their effects on network dynamics. Hence, scenarios where several nodes from one network are likely to be coupled to one single node in the other network (no many-to-one relationship) have not yet been fully explored. We change the nature of network interdependency by allowing a node in given network to have multiple counter parts in another network (many-to-one mapping). Existing work (Buldyrev et al. 2010; Gao et al. 2012; Parshani et al. 2010; Schneider et al. 2013) generally links interdependent networks with one-to-one mappings (i.e. nodes in network A have a unique counterpart in network B). A reason for that situation is that present mathematical frameworks tend to use generating functions to predict the size of the largest remaining component after cascading failure and these are constructed with the assumption that "each node in network B depends exactly on one node from network A" (Buldyrev et al. 2010). Although this assumption was relaxed in further work such as (Schneider et al. 2013) by stating that a fraction of nodes in A could be coupled with nodes in B, it remains that if one wish to use the generating functions in their present form, nodes in one network cannot have several counterparts in another network. Another reason explaining the absence of multiple mappings is the very large size of the parameter space needed to build interdependent networks and the high computational cost of running simulations that so far have prevented the exploration of this particular feature. Assuming the prevalence of one to one mappings between coupled networks does not fit with the fact that many nodes in infrastructure networks can have multiple dependencies (i.e. an airport might require connections to multiple power nodes). Consequently, here we explore a scenario where many-to-one mapping are possible between interconnected networks (i.e. a node in network B has in average m supporting nodes from A where $m > 1$). In this work, a many-to-one mapping was chosen, but a one-to-many mapping (with $0 < m < 1$) is another alternative way of coupling networks that could potentially be explored in future work. Figure 2 shows how failure propagates between networks through undirected dependency in that type of scenario.

Suggested change to the third assumption: changing the post-attack viability by taking into account symbiotic interdependency

Symbiotic networks are networks that need to be mutually connected in order to be viable. In this scenario, a connected component (i.e., a network fragment) in one network is viable only if a minimum fraction of its nodes are connected to a surviving network component from the other network. Connected components in both infrastructure networks are subject to this survival constraint. A third assumption is that there is no gradient in the degree of isolation that could influence the viability of a symbiotic clusters: research focuses on the limited case where either clusters are never isolated from the other network (when all nodes in A are linked to nodes in B) or clusters can stay alive even if isolated from their counter-part network (Buldyrev et al. 2010; Gao et al. 2012; Parshani et al. 2010; Schneider et al. 2013). Consequently, the lesser the connections between networks, the smaller the

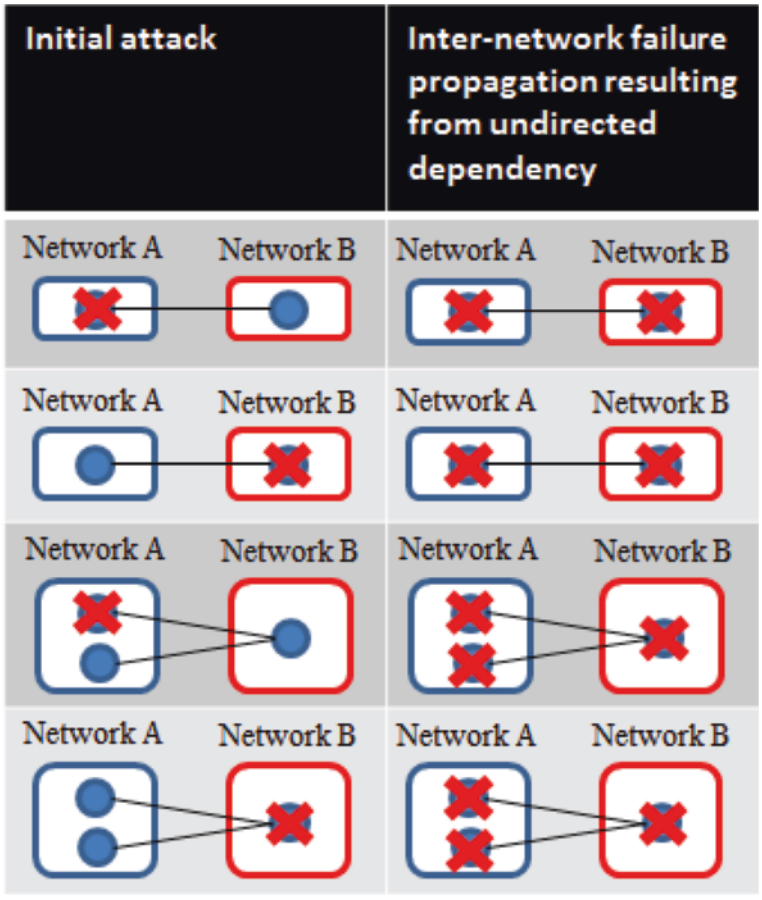

Figure 2 Failure propagation between networks through undirected dependency: one-to-one and many-to-one mapping situations.

probability of cascading failure due to node removal, and the greater the topological robustness of such systems (Battiston et al. 2009; Brummitt et al. 2012; Gao et al. 2011b; Panzieri and Setola 2008; Schneider et al. 2013). We present a novel measure of the symbiotic viability of network components when faced with isolation that results in novel strategies on how to achieve robustness. Previous studies have evaluated the post-attack performance of a pair of interdependent networks, A and B, by measuring the size of the remaining connected component(s) in each network after cascading failure. This calculation has ignored the extent to which either of these components is connected to surviving nodes in the other network and assumes implicitly either that clusters are never isolated (if all A nodes are linked to a B nodes) (Buldyrev et al. 2010; Gao et al. 2012), or that a cluster of surviving B nodes can exist as a viable network in the absence of any connection to the A network, and vice versa (Schneider et al. 2013). As a consequence, standard analysis shows that reducing the number of interdependencies between A and B is a good way of improving system resilience, since when one network is attacked the other is shielded from the consequences. However, this approach to measuring post-attack viability does not take into account a gradient in the possible degrees of isolation and their impact on the symbiotic nature of systems. For example, in modern infrastructures, a railway network cannot survive in complete isolation from a road transport network because it needs the road network to deliver a minimum amount of passengers, goods, and personnel in order to operate. Consequently, here we evaluate the symbiotic post-attack viability of a network by measuring the size of the largest component that meets a dependency threshold expressed in terms of the proportion of nodes within the component that are connected to at least one surviving node in the other network. Setting the threshold at 10%, for instance, demands that in order for a network B component to be viable, at least 10% of its nodes must be connected to a surviving A node, i.e., an A node that itself is within a component that meets the 10% interdependency threshold. This requirement for the viability of a connected component can be expressed as the

dependency threshold Γ, that is to say, the ratio of nodes in this component that are connected to other live clusters. The symbiotic viability condition for a given component can be defined in its simplest form as maintaining the coupling ratio of the component above an interdependency threshold Γ and can be expressed by the following equation:

$$\frac{\sum_{i=1}^{q} W_i}{\sum_{i=1}^{q} W_i + \sum_{j=1}^{\bar{q}} W_j} \geq \Gamma \tag{1}$$

Where q is the number of nodes in this component which are coupled to another component from a different complementary network, $\bar{q}$ is the number of uncoupled nodes, Γ is the interdependency threshold below which the component is not viable, and each coupled node i has a weight w_i while each uncoupled node j has a weight w_j (so as to quantify how important or vital some nodes are compared to each other). In this work, we study the robustness of complex interdependent networks by using a simplified version of the symbiotic viability condition detailed above: we consider the case where all nodes have an equal weight an can then rewrite the condition as:

$$\frac{q}{q + \bar{q}} \geq \Gamma \tag{2}$$

A suggested solution to decrease the vulnerability of interdependent networks to cascading failure: permutable nodes

Finally, we propose a solution to the consequent problem of seemingly ever increasing vulnerability of interconnected networks introduced by multiple symbiotic dependencies: the use of permutable nodes that would give such systems rewiring capabilities akin to those found in the human brain. We use the measure of symbiotic viability detailed in equation 2 to evaluate the post-attack viability of symbiotic networks. There are only two ways to increase the viability condition expressed by this coupling ratio: either add extra coupled nodes to a component to increase the weighted sum in the numerator, or remove uncoupled nodes to reduce the weighted sum in the denominator. One way to achieve this is to treat coupled and uncoupled nodes like valuable resources that can be exchanged between mutually connected components via the creation of permutable infrastructure nodes. An abstract example of such a mechanism could be the training of defending players that could alternate between the roles of midfielders and strikers inside a football team. Although they might be less efficient as defenders, their ability to occupy other positions would make their team more resilient if some strikers were taken out of the game. If a permutable node is active in one network, its counter-part in another network is inactive and vice versa. When permutation occurs, the active side changes allowing the allocation of a node from one non-essential role in one network to a potentially crucially needed position in another. There can be permutation between coupled nodes, between uncoupled nodes, or between uncoupled and coupled nodes. Permutation between coupled nodes is only useful when several remaining components can exist in each network. In this limited specific case, interdependent links can be "rewired" and exchanged as a valuable resource between components of different networks so as to preserve viability.

Permutation between uncoupled nodes shown in Figure 3 is only possible when one of the components can absorb the accumulated loss resulting from the deactivation of the uncoupled nodes. This renders this permutation more difficult to achieve, because in order to obtain the same increase in the coupling ratio, the minimum required number of uncoupled nodes to remove from the denominator is much higher than to the number of coupled nodes one has to add in the numerator. One advantage of swapping uncoupled nodes is that it minimises the vulnerability to cascading failure because we do not increase the number of interdependencies.

Design of models and experiments

We consider two coupled networks A and B of same size N. The coupled networks sizes considered was $N = 500$, so as to guarantee computational feasibility while keeping generalisable topologic features. Four different types of network topologies are explored: Erdos Reyni, Watts Strogattz, Barabasi Albert, and ring lattice. We deliberately chose these as they are well known and are affected in distinctive ways when confronted to random attacks (Hu and Verma 2011). Different versions of these paired networks are built, each one with an average degree k varying from 4 to 24 in order to show the effects of internal network redundancy over the robustness of the whole system.

The degree of coupling between the networks is defined by the fraction q of nodes in network A that are linked to nodes in network B, as in (Fu et al. 2014) that includes descriptions of a similar setting. The links between the networks are constructed with a coupling degree q varying (through a range of 19 evenly spaced values) from 0.05 to 1.0, in order to show the effects of network interdependency over the robustness score. Regarding the correlation of inter-network dependencies, nodes that are linked to another network are selected at random.

Failure propagates between networks through undirected dependency (i.e. if one node in A that is linked to another node in B is disabled, then the node in B will also be disabled). The robustness of interdependent networks is evaluated by attacking one network and then by looking at the post-attack viability of both networks

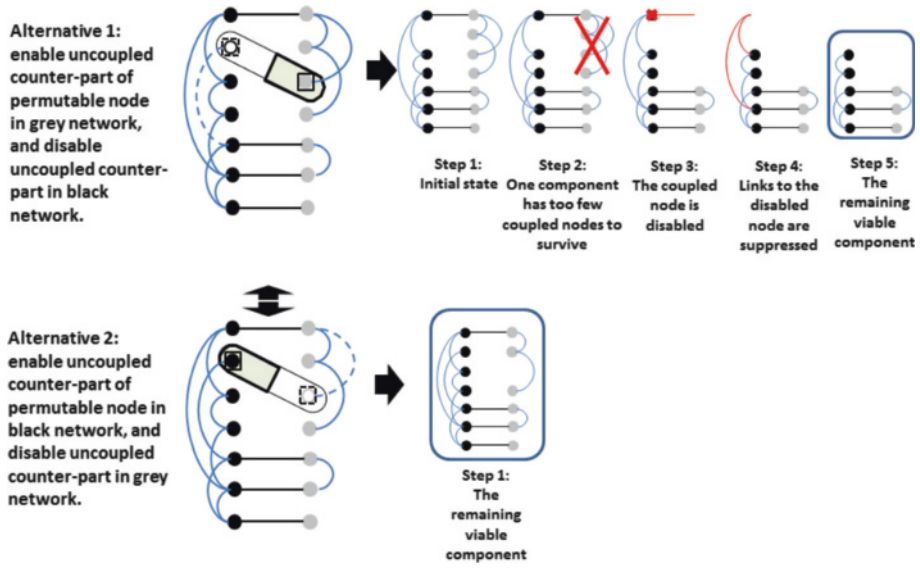

Figure 3 One example case of the influence of node permutability on post attack viability. We use a permutable node in components with the following symbiotic viability condition: a component is only alive if at least 1/3 of its nodes are connected to other network. The large network diagrams on the left represent the two different alternative networks made possible by swapping the states of the permutable node. In the first alternative scenario, this uncoupled node can be activated in the grey network, with an extra internal (blue) edge. In the second alternative situation, the grey network node is disabled and the node counter-part in the black network is activated. Disabled nodes and connections in each alternative scenario are shown with dashed lines. After applying the post-attack viability rule, alternative 2 seems to leave the coupled networks in a much better state than alternative 1.

after cascading failure. The initial attack is always done by selecting a fraction $(1 - p)$ of randomly chosen nodes in network A.

When secondary components remain viable, the algorithm that evaluate the number of active nodes left in both networks after attack differs from standard procedure in one aspect: it does not prune anymore all secondary components with the attached iterative failure propagation. Instead, any component that is above a certain minimum number of nodes is kept and considered live. In our experiments, any secondary component whose size is superior to three nodes is considered alive.

One-to-many mappings are created by choosing at random a certain number n of distinct nodes in network A, and then choosing a corresponding number of randomly selected coupled nodes in network B, with no obligation for them to be distinct from each other, and then creating coupling links between them. This produces many instances of nodes in network A that depend on multiple coupled nodes in network B. Failure propagation between networks follows the same rule for both one-to-one and many-to-one mappings: for each network node to operate, all of the nodes upon which it depends must be also be operational.

When taking into account the effects of isolation as a destructive force as well as the propagation of cascading failure, the post attack viability of connected components is evaluated as described in the Algorithm 1.

Algorithm 1 Evaluate symbiotic viability

Require: S, a set of components of networks A and B
  Attack S and update S equal cascading_failure(S)
  Set there_are_still_components_to_check to TRUE
  while there_are_still_components_to_check_flag is TRUE **do**
    Set there_are_still_components_to_check_flag to FALSE
    for each component, $c \in S$ **do**
      if proportion of coupled nodes, q_c/n_c, is inferior to Γ **then**
        Disable all nodes in the component
        Disable any dependent nodes in other components
        Propagate cascading failure and update S throughout cascading_failure(S)
        Set there_are_still_components_to_check_flag to TRUE
      end if
    end for
  end while
  return Viability(remaining components)

When we use permutable nodes to decrease the vulnerability of interdependent networks to cascading failure, we first evaluate the symbiotic post-attack viability of connected components, and if these connected components

are damaged, we then set to switch permutable nodes in a process as described by Algorithm 2.

Algorithm 2 Permute node roles

Require: S, a set of components of networks A and B
  Get list of permutable nodes in S
  for each component, $c \in S$ **do**
    while proportion of coupled nodes, q_c/n_c, is inferior to Γ **do**
      Permute a new random permutable node out of c (unless by doing so it would have no living neighbours)
    end while
  end for
  Set V = Evaluate_Symbiotic_Viability(S)

Permutation between uncoupled and coupled nodes as shown in Figure 4 generally offers a significant increase of the coupling ratio in both networks for the smallest number of permutations as shown in the result section. We evaluate the change in post-attack viability of symbiotic networks (expressed in Equation 2 and implemented as in algorithm 1) over a hundred trials triggered by the introduction of permutable nodes for different values of the dependency threshold (0.1 for a weak symbiotic interdependency, 0.3 for an intermediate value, and 0.5 for a strong symbiosis). Each coupled network has a size of 100 nodes, a coupling degree of 0.5, and a fraction of swappable nodes equal to 40%. Two types of permutation are considered: either between uncoupled nodes, or between uncoupled and coupled nodes. In each case, we show the percentages of coupled networks prevented from being destroyed after attack, the average number of nodes saved per trial, and the frequency of dead networks saved for each attack degree.

The resulting size of the parameter space is such that around 1675800 simulations of cascading failure have to be run every time we change the nature of network interdependency or the post-attack viability rules. The IRIDIS High Performance Computing Facility available at the University of Southampton, was used over a period of several weeks in order to complete this work using the Python programming language. Results are saved in multidimensional arrays for each combination of the following experimental parameters: network type, network

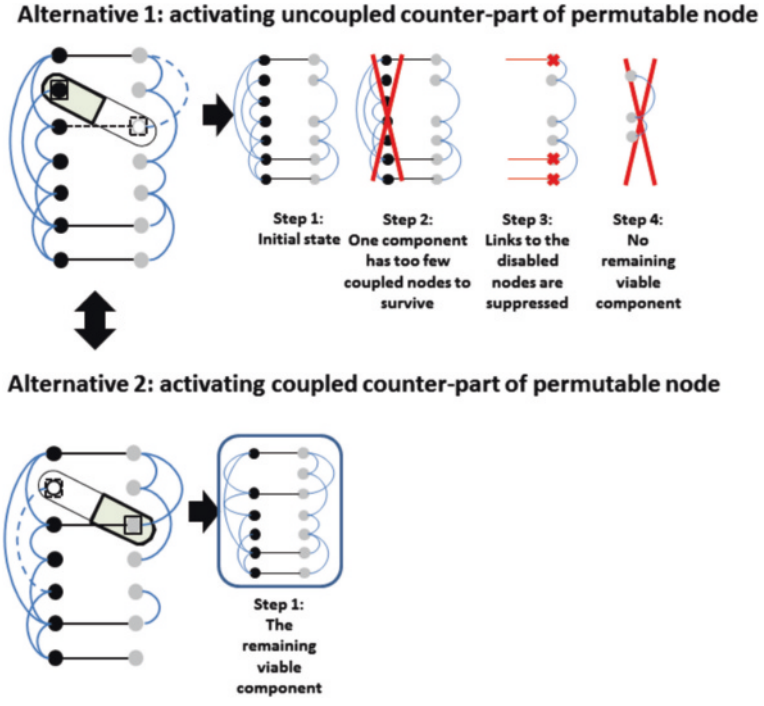

Figure 4 A different example case of the influence of node permutability on post attack viability. We use a permutable node that can switch from an uncoupled to a coupled counter-part in components with the following symbiotic viability condition: a component is only alive if at least 1/3 of its nodes are connected to other network. The large network diagrams on the left represent the two different alternative networks made possible by swapping the states of the permutable node. Either the uncoupled counter-part of the node is activated in the black network, or the counter-part in the grey network is activated with an associated interdependent (black) edge, and an extra internal (blue) edge. Disabled nodes and connections in each alternative scenario are shown with dashed lines. After applying the post-attack viability rule, alternative 2 seems to leave the coupled networks in a much better state than alternative 1.

degree, coupling degree, attack degree, and run number. The values saved are the number of active nodes left, the transitivity, the average shortest path length, and the degree histogram for each network, but also for each connected component inside each network. In the experiments described below, we only use the number of active nodes left in both networks as raw data. The complete data sets are quite extensive (in total around 20 Gigabytes) are available as well as the Python code leading to their production upon contacting the authors.

Procedures, statistics, and metrics used to answer the research questions

The robustness of the system is expressed as the area under the curve defined by the fraction of nodes still alive in each network for a degree of attack $(1 - p)$ varying (through a range of 21 evenly spaced values) from 0 to 1.0.

Let R_s be the standard measure of the robustness of a system of interdependent networks based on the size of the one largest remaining connected component in each interdependent network. Let $1 - p$ be the attack size, and $P(1 - p)$ be the relative size of the largest connected cluster in a network after failure. R_s is the area under the curve defined by the fraction of nodes still alive in each network for varying degrees of attack can be expressed as follows in Equation 3:

$$R_s = \int_{1-p=0}^{1.0} P(1-p) \tag{3}$$

Let R_m be the robustness of a system of interdependent network obtained by measuring the aggregate of the sums of the relative sizes of all components above some critical minimum number of nodes. Let $S(1-p, C_{min})$ be the sum of the relative sizes of connected clusters above or equal a minimum critical size C_{min} in a network after attack. R_m can be expressed as follows in Equation 4:

$$R_m = \int_{1-p=0}^{1.0} S(1-p, C_{min}) \tag{4}$$

R_s and R_m values are used to plot respectively the single and multiple cluster measurements of robustness throughout the whole parameter space over these 25 runs. Each robustness value is represented by a colored cell in a heatmap, where the position along the horizontal axis expresses the average internal degrees for each network, and the position along the vertical axis expresses the degree of coupling between the networks. (See figures in result section).

Let Δ_R be the difference of robustness between multiple and single cluster measurement. $\Delta_R = R_m - R_s$ can be defined as follows in Equation 5:

$$\Delta_R = \int_{1-p=0}^{1.0} \left[S\left(1-p, C_{min}\right) - P(1-p)\right] \tag{5}$$

Δ_R values are used in Figure 5 to show directly the difference of robustness between multiple and single cluster measurement for different topologies. Negative values are represented by a different color gradient (here white to black) than positive values (here red to yellow).

A similar approach is taken to show the difference of robustness between one-to-one and many-to-one interdependent mappings as shown in Figure 6.

The robustness is evaluated over 25 runs, where for each run, new networks are generated. Average value, standard deviation, and the p value obtained by t-test are then obtained to compare the robustness in systems with a different network interdependency or the post-attack viability rule and produce more standard graphs such as the bar charts seen in the results section.

Results presentation and interpretation

In the following, we will present our analysis of the difference in robustness that results from the changes outlined above over the standard assumptions simplifying the nature and extent of network interdependency and the rules that establish the post-attack viability of a connected component.

Change in robustness when secondary components are viable

In this section, we attempt to find if there is a significant difference of robustness when considering secondary components as viable instead of just the one single largest remaining connected component in each network. Existing work (Albert et al. 2000b) has observed that network fragmentation results in a distribution of various cluster sizes (e.g. when a gaint component exist, the second is significantly smaller than the largest one, etc...). Still, even if secondary components are small, if there are enough of them, they can have a potentially important supporting role regarding the robustness of a coupled system. Results from Figure 7 show that there does not seem to be a significant difference between single and multiple components evaluation for Erdős-Rényi and Barabàsi-Albert pairs of networks (a one-tail t-test shows an average p-value superior to 0.1). On the other hand, tolerating secondary components seems to increase significantly (for a t-test p value <0.005) the post attack performance of Watts-Strogatz, and ring lattice topologies.

There is nearly no null or negative difference in Watts-Strogatz, and ring lattice networks, showing that robustness using multiple components is systematically outperforming the single component robustness for these topologies. It is also worth noticing that for Erdős-Rényi and Barabàsi-Albert networks, the maximum difference of robustness is less than is 5%, while for network topologies more vulnerable to fragmentation such as Watts-Strogatz, and ring lattice, the maximum difference is more than

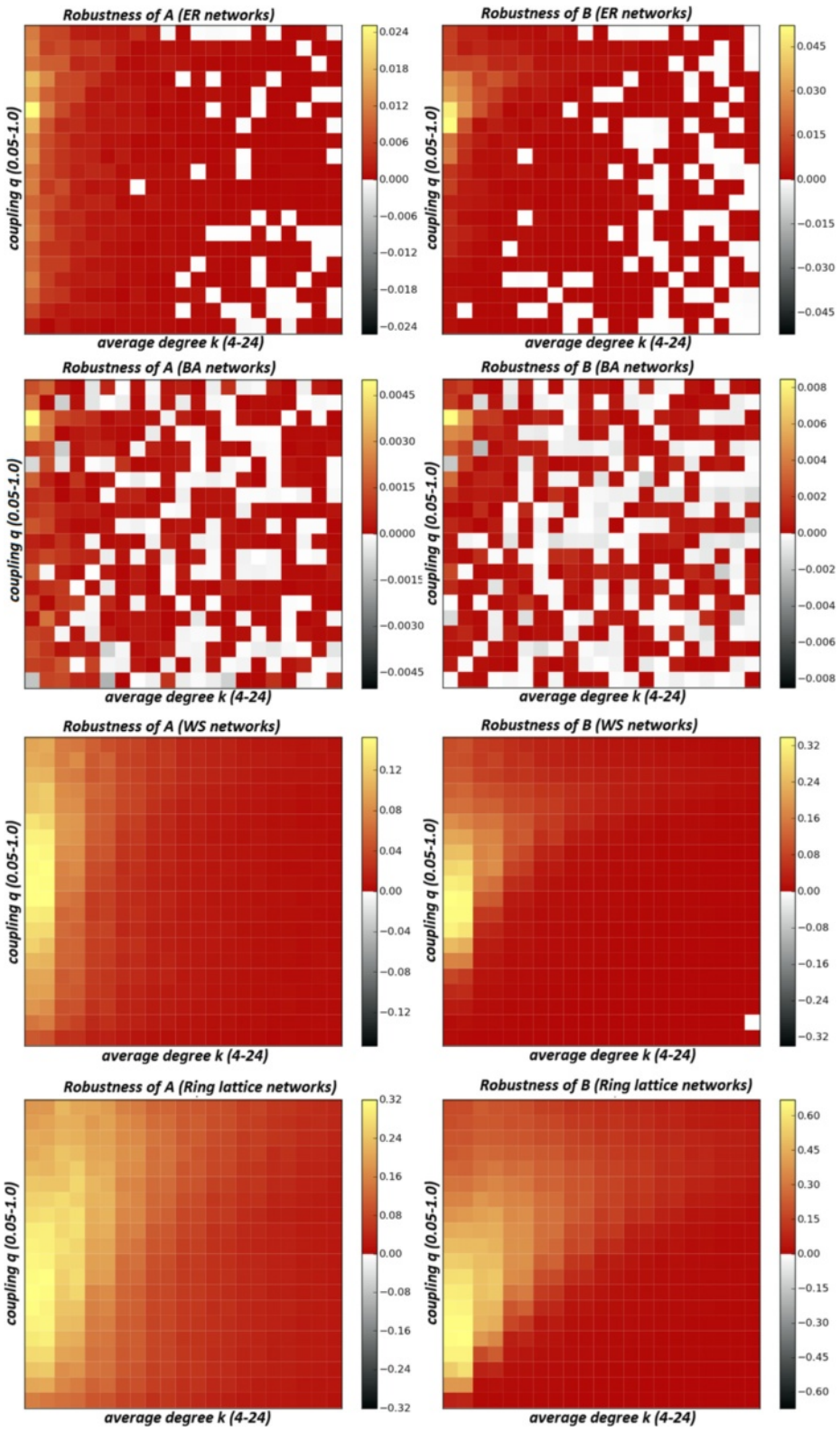

Figure 5 Difference between multiple and single cluster measurement of robustness for Erdős-Rényi, Barabàsi-Albert, Watts-Strogatz, and ring lattice topologies. Each coloured heat-map cell represents the average of the difference of robustness Δ_R between multiple and single cluster measurements for 25 pairs of random 500-node networks in function of the degree of coupling between A and B and the average degree of each network. The gray scale expresses negative differences while the coloured scale expresses positive differences.

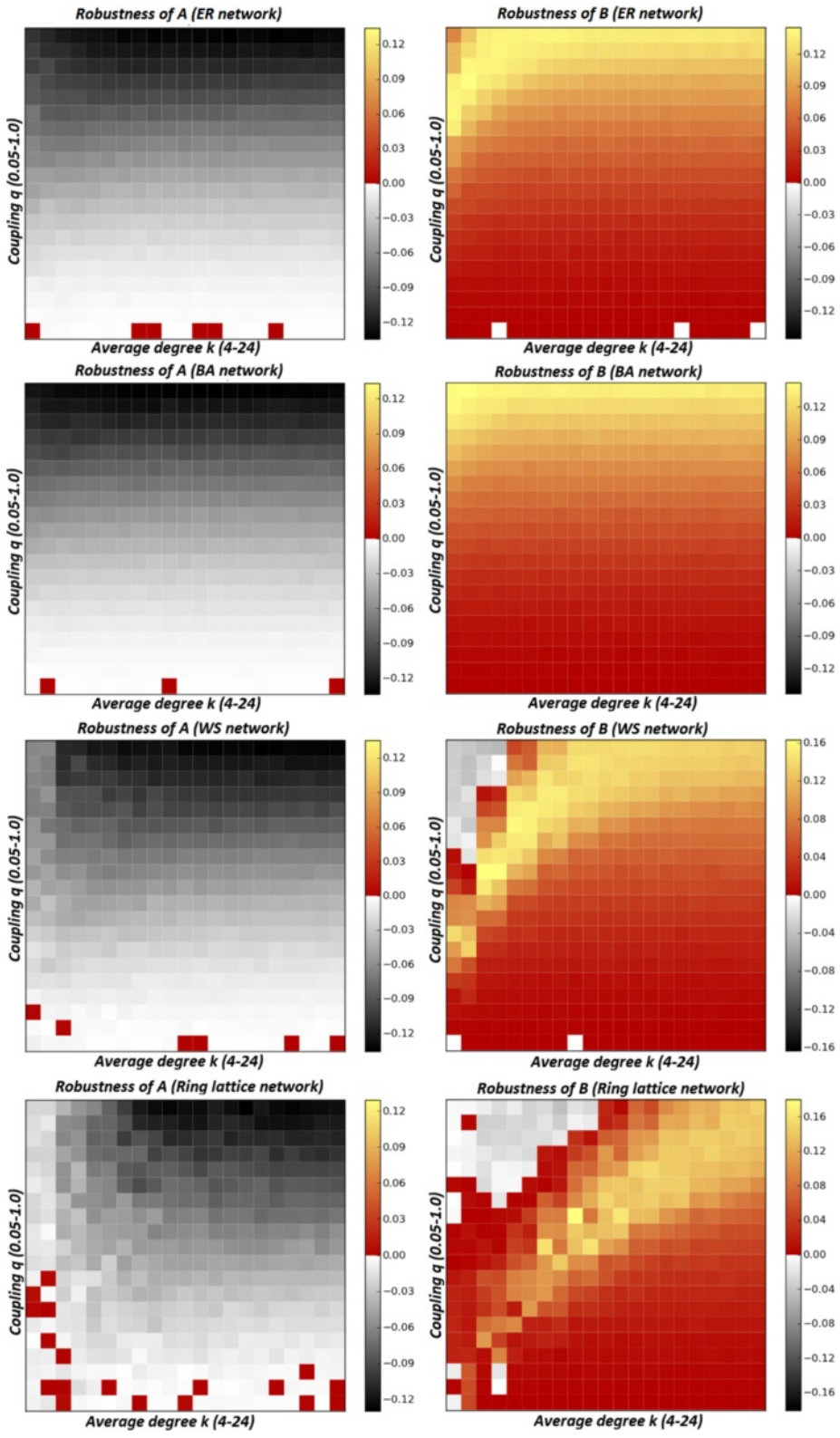

Figure 6 Difference of robustness between between many-to-one and one-to-one dependency mappings for Erdős-Rényi, Barabàsi-Albert, Watts-Strogatz, and ring lattice topologies. Each coloured heat-map cell represents the average of the difference of robustness between multiple and single dependency mappings for 25 pairs of random 500-node networks in function of the degree of coupling between A and B and the average degree of each network. The gray scale expresses negative differences while the coloured scale expresses positive differences.

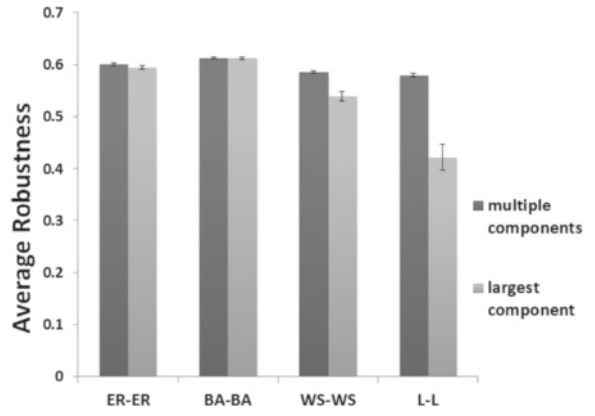

Figure 7 Robustness with secondary components versus robustness with single largest remaining connected component.

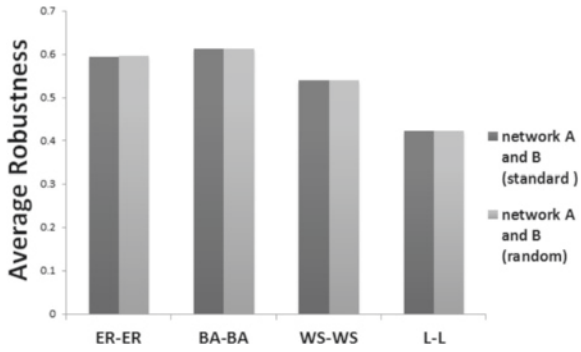

Figure 8 Difference between multiple and unique dependencies when considering the global average robustness of all networks.

30%. Networks with lower average degree tend to fragment more easily after attack, and results show that the lower the degree k, the higher the chance that multi-component robustness will significantly outperform the single component robustness. This can be explained by the fact that, when under attack, networks with lower internal connectivity tend to transform into a collection of disconnected components. In this situation, measuring the one largest remaining component and ignoring all secondary clusters leads to a significant difference in the evaluation of robustness. The easier to fragment a network is, the greater the influence exerted by these secondary components on the functional integrity of an infrastructure network.

Change in robustness when one node can have multiple counter parts in another network

Initial results from Figure 8 show that there does noes seem to be a significant difference of overall robustness between multiple (a node in network B has in average m supporting nodes from A where $m > 1$) and unique ($m = 1$) dependencies. Erdős-Rényi, Barabàsi-Albert, Watts-Strogatz, and ring lattice topologies show seemingly identical results.

On the other hand, when comparing the robustness of individual networks, a significant difference seems to emerge as shown in Figure 9. In the case of the many-to-one mapping explored by linking unique nodes in A to randomly chosen nodes in B, the percolation damages seem to be increased in network A and decreased in network B. A typical example of such phenomena can be observed in Figure 10 that shows the difference of robustness between many-to-one and one-to-one mappings for both Erdős-Rényi networks of average degree $k = 4$ and $q = 1.0$. Failure will spread to a greater portion of network A, while a smaller fraction of B will be damaged.

In the case of a many-to-one mapping, linking unique nodes in A to randomly chosen nodes in B seems to be transfer the effects of percolation back to A. Further results shown in Figure 6 support this hypothesis as the heat-maps representing the differences of robustness between multiple and single dependency mappings showing predominantly gray scales for network A (negative differences) and mostly red and orange areas for network B (positive differences). This can be explained by the fact that, when under attack, the network A has multiple nodes that depend on a failure from a single node in B. Therefore, it has less chance to preserve a remaining component as the propagation of cascading failure is amplified. On the other hand, there is a greater chance that a portion of network B will remain untouched because a smaller number of nodes in B are coupled to potential failures in A. This result seem to indicate that a many to one mapping can be used as an effective control mechanism to transfer damages due to cascading failure from one network to another.

A measure of symbiotic post-attack viability and resulting novel strategies to achieve robustness

In this scenario, a connected component is viable only if a minimum fraction of its nodes are connected to another surviving cluster in a different network. This other cluster is itself subject to the same survival condition. This requirement for the viability of a connected component can be expressed as the dependency threshold Γ, that is to say, the ratio of nodes in this component that are connected to other live clusters.

Figure 11 shows that than when components need to meet a dependency threshold $\Gamma = 0.1$, the robustness expressed by the area under the curve measuring the fraction of nodes still alive in network B for varying degrees of attack is significantly smaller than in the standard case where the post-attack viability of remaining components

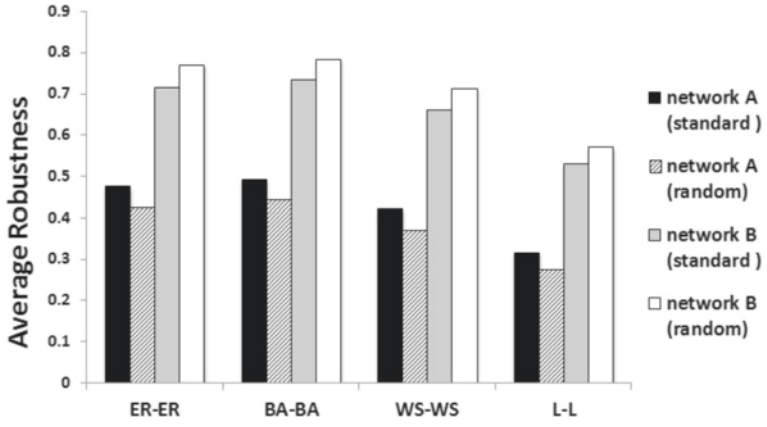

Figure 9 Difference between multiple and unique dependencies when considering the robustness of individual networks.

is not affected by their isolation (for $\Gamma = 0$). This indicates that there might be a very different optimum when looking at the landscape of robustness scores if a symbiotic post-attack viability rule is chosen.

Figure 12 confirms that using standard and symbiotic interdependency results in different robustness landscapes. Post-attack viability is plotted in function of the degree of coupling q and the average degree k in two interdependent Barabàsi-Albert networks. The standard measure of post-attack viability ($\Gamma = 0$) shows an optimum robustness score at the bottom of the heat map where the degree of coupling is at its lowest. On the other hand, when the viability of a cluster is linked to a dependency threshold $\Gamma = 0.1$ or $\Gamma = 0.2$, the heat map shows that the robustness score is optimal when q is between some intermediary values (in this particular case, 0.35 and 0.6). This optimum range of values changes depending of the value of Γ. The Dark blue area at the very bottom shows a region where the robustness score is null because the degree of coupling between networks being inferior to the dependency threshold, the networks end up isolated. Simulations results have shown that the size of this "null-viability" area grows linearly with Γ. Incidentally, similar results are observable for Erdős-Rényi, Barabàsi-Albert, Watts-Strogatz, and ring lattice, suggesting a new landscape of robustness that has features independent from the network topology considered.

Figure 13 emphasizes how the introduction of various level of symbiotic interdependency changes the relationship between robustness and coupling. The robustness of two interdependent networks A and B with respect to the degree of coupling q is shown for scenarios where the value of Γ ranges from 0 (standard post-attack viability) up to 0.5 (at least half of a cluster needs to be connected to another network to be alive). For $\Gamma = 0$, the optimum robustness is attained for the lowest possible coupling value $q = 0$. For cases where $\Gamma > 0$, the optimal robustness does not lie where $q = 0$, but soars as soon as the minimum amount of coupling is reached in order to prevent isolation, then quickly reaches a maximum value, and

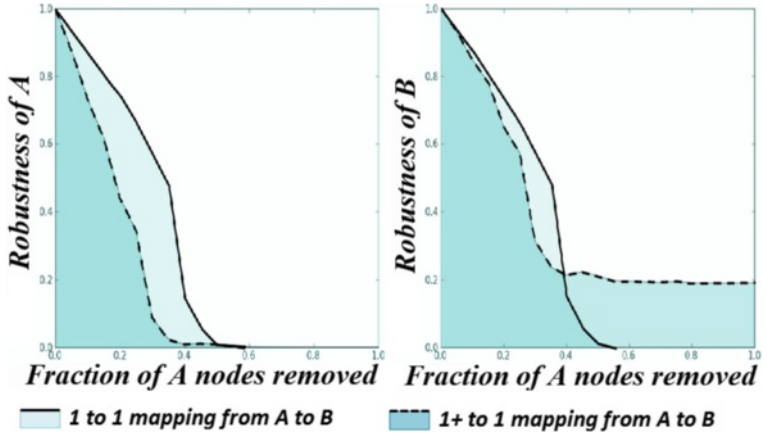

Figure 10 Robustness of each coupled Erdős-Rényi network ($k = 4$ and $q = 1.0$): multiple versus unique dependencies.

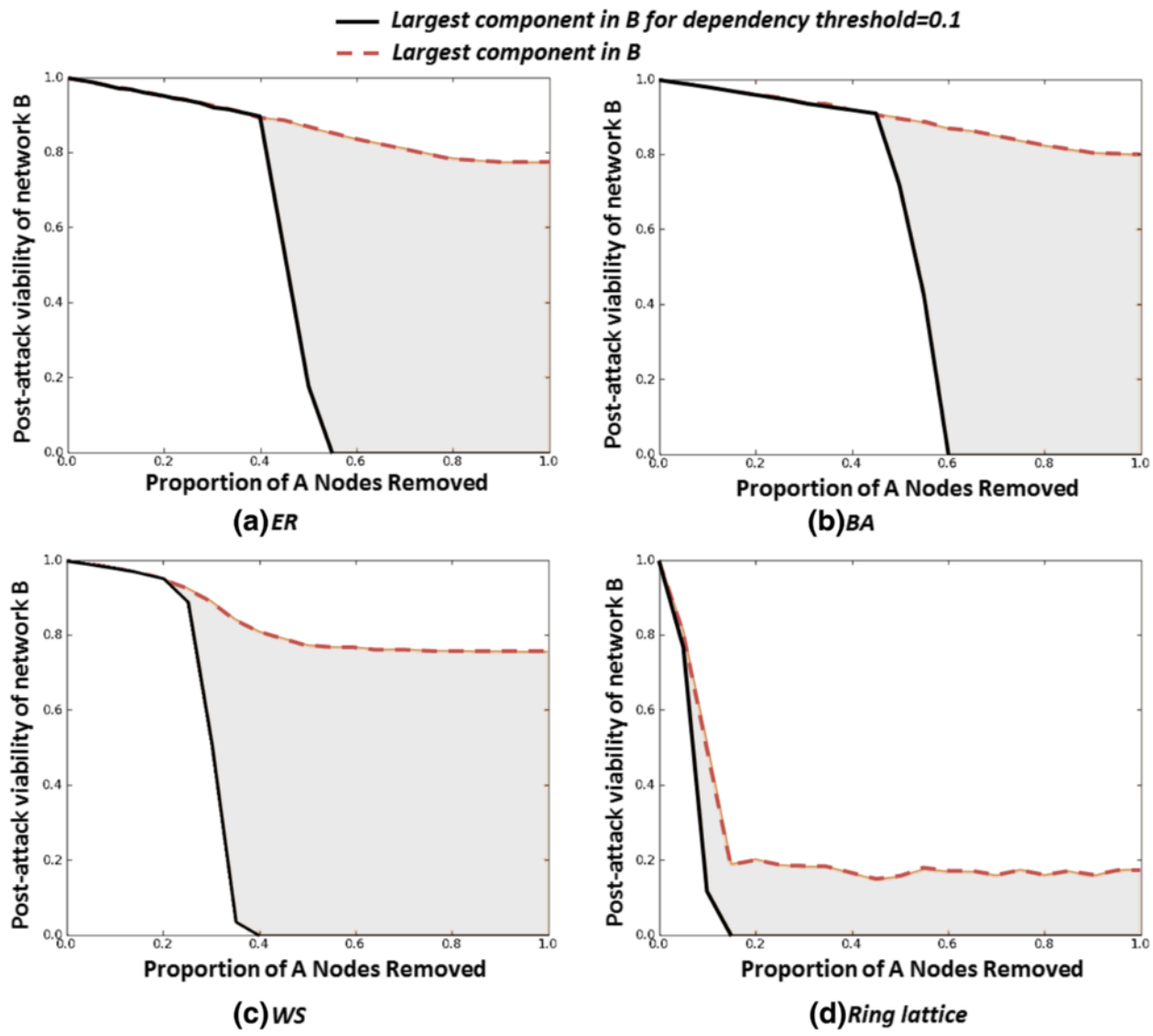

Figure 11 Robustness of coupled networks: impact of the dependency threshold requirement. We compare the robustness - here, the area under the curve defined by the fraction of nodes still alive in network B for varying degrees of attack on network A - of coupled Erdős-Rényi ***(a)***, Barabàsi-Albert ***(b)***, Watts-Strogatz ***(c)***, and ring lattice ***(d)*** networks for standard post-attack viability (for $\Gamma = 0$), and when components need to meet a dependency threshold $\Gamma = 0.1$.

finally gradually converges to lower average values corresponding to a situation where the increased coupling has amplified cascading failure and lead to a lower percolation threshold.

Figure 14 shows that even for very different network topologies, the average robustness of the system always decreases when the symbiotic viability condition expressed by the dependency threshold Γ increases because the conditions for post-attack viability are made more stringent. This result may have wide implications, because it demonstrates that the dynamic process of fragmentation decouples interdependent networks during a cascading failure is as important as the process of percolating failure within each network when it comes to quantifying and predicting the resilience of interdependent networks. This implies that systems built to rely on the combined availability of different resources such as transport, power, ICT, and water can only become increasingly vulnerable to catastrophic failure. Unfortunately, this propensity of modern infrastructure systems to require an increasing number of services to work together in order to function is not likely to reverse. In this context, one important question one might ask is: is there a practical and feasible way to reduce the vulnerability of such systems to both isolation and cascading failure? In the next section we propose one possible solution

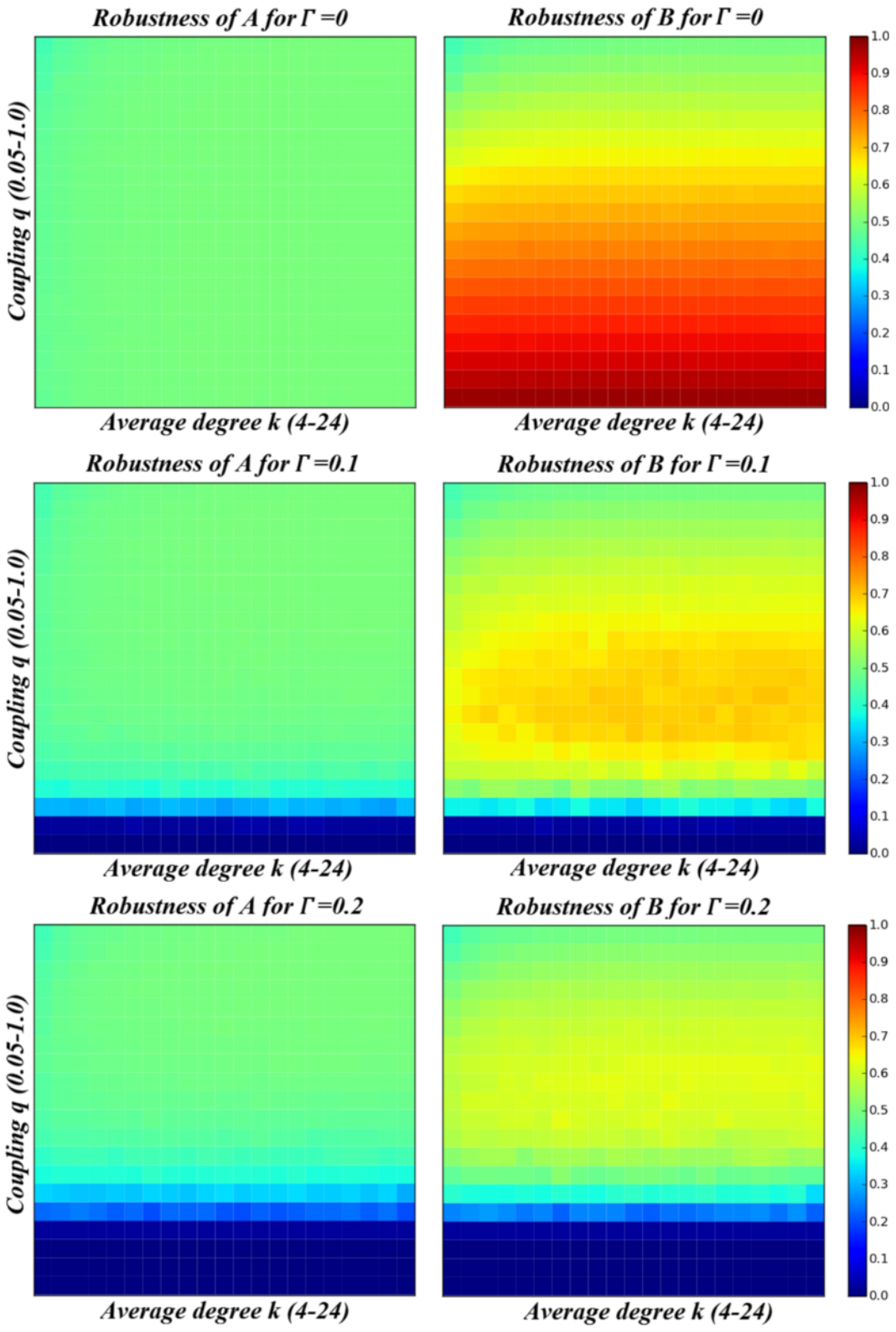

Figure 12 Measures of post-attack viability for two interdependent Barabàsi-Albert networks. The heat-maps represent respectively the post attack viability for networks A and B where clusters can survive isolated ($\Gamma = 0$) or where they can only be alive if they meet a dependency threshold $\Gamma = 0.1$, and 0.2. Each coloured heat-map cell represents the mean aggregate post-attack viability of 25 pairs of random 500-node Barabàsi-Albert networks in function of the degree of coupling between A and B and the average degree of each network.

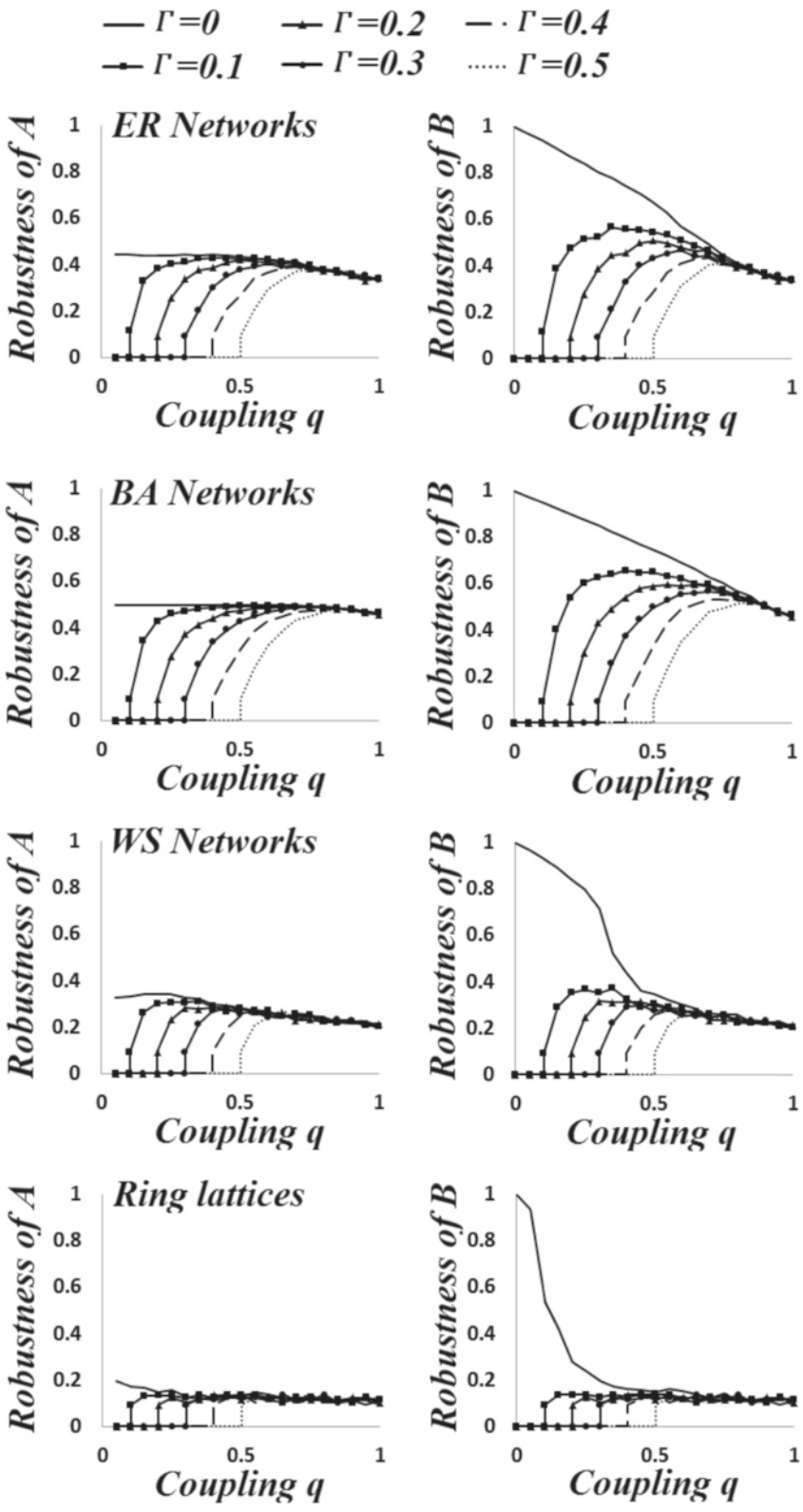

Figure 13 Plotting the robustness of coupled Erdős-Rényi, Barabàsi-Albert, Watts-Strogatz, and ring lattice networks in function of their degree of coupling q. For each network, the average degree $k = 4$. The different types of lines mean that different post-attack viability rules are used to compute the robustness where the dependency threshold Γ can vary from 0 (isolated components are tolerated) to 0.5 (at least half of a cluster needs to be connected to another network to be alive).

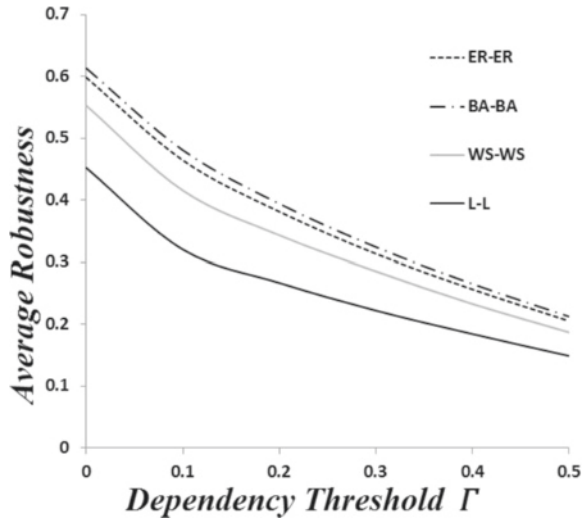

Figure 14 Plotting the robustness of two interdependent networks (Erdős-Rényi, Barabàsi-Albert, Watts-Strogatz, and ring lattice) in function of the dependency threshold Γ. Each robustness score corresponds to the average of all the robustness values obtained for each degree of coupling between 0.05 and 1.0.

to this problem: giving infrastructure networks rewiring capabilities akin to those found in the human brain by introducing nodes with permutable roles.

Change in symbiotic post-attack viability when infrastructure nodes have permutable roles

Figure 15 shows that the permutation between uncoupled nodes results in an increase in the chance to save the largest remaining component in each network (+1.8% for a low symbiotic interdependency, +9.8% for a medium value, and +3% for a high value of Γ), and that the permutation between uncoupled and coupled nodes results in a large gain in viability(+7% for a low symbiotic interdependency, +24.3% for a medium value, and +32.5% for a high value of Γ). Also, in the first type of permutation, maximum gain is obtained for a medium symbiotic interdependency, while in the latter, the best gain happens for a high symbiotic interdependency. This can be explained because in order to obtain an increase in the coupling ratio expressed by the symbiotic viability condition, the minimum required number of uncoupled nodes to remove from the denominator via the first type of permutation is much higher than the minimum required number of coupled nodes that can be added in the numerator via the second type of permutation. When using permutation between uncoupled nodes, components have to absorb the accumulated loss resulting from the deactivation of uncoupled nodes, generally only few of them can be sacrificed, and therefore this results in modest gains of viability unlikely to be sufficient for stringent conditions imposed by a high symbiotic viability. On the other hand, as the second type of permutation generally offers a significant increase of the coupling ratio in both networks for a smaller number of permutations, it offers a better gain of viability for Γ = 0.5.

Figure 16 shows that the average number of nodes saved per trial (reflecting the size of the largest remaining components) is relatively small for permutations between uncoupled nodes (18 for a low symbiotic interdependency, 129 for a medium value, and 57 for a high value of Γ) and quite large for permutations between uncoupled and coupled nodes (70 for a low symbiotic interdependency, 297 for a medium value, and 539 for a high value of Γ).

Figures 17 shows that the percentage of dead networks saved per attack degree follows different distributions depending on the type of permutation and the level of symbiotic interdependency. For permutations between uncoupled nodes, the percentages of saved networks are lower and distributed over narrower ranges of attack degrees, indicating that viability gains are more difficult to achieve. For permutations between uncoupled

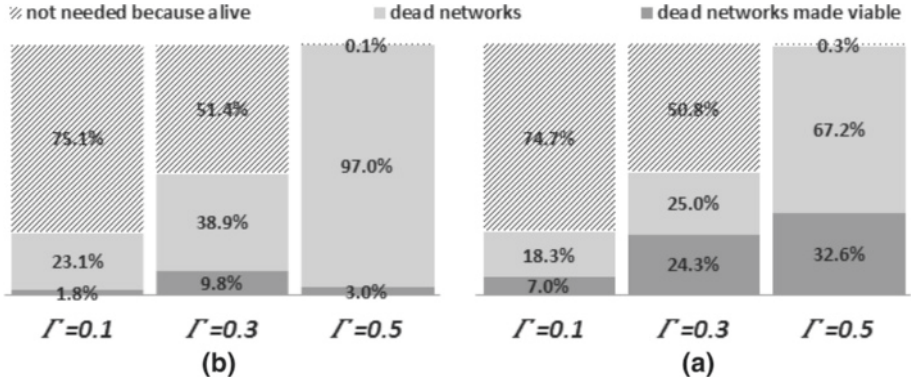

Figure 15 Percentages of coupled networks preserved when using permutation. Percentages of coupled networks prevented from being destroyed after attack when using permutation between uncoupled nodes **(a)** and permutation between uncoupled and coupled nodes **(b)** for low ($\Gamma = 0.1$), medium ($\Gamma = 0.3$), and high ($\Gamma = 0.5$) symbiotic interdependency values.

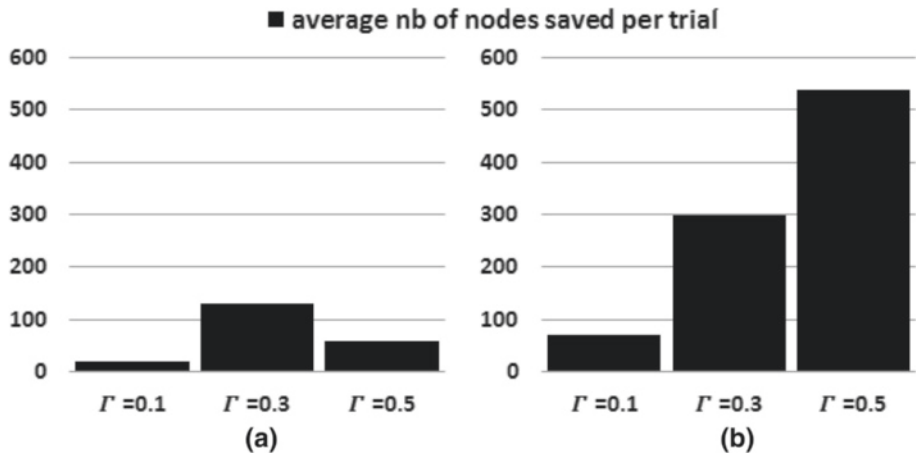

Figure 16 The average number of nodes saved per trial when using permutation. The average number of nodes saved per trial when using permutation between uncoupled nodes **(a)** and permutation between uncoupled and coupled nodes **(b)** for low ($\Gamma = 0.1$), medium ($\Gamma = 0.3$), and high ($\Gamma = 0.5$) symbiotic interdependency values.

nodes and coupled nodes, the percentages of saved networks are higher and distributed over larger ranges of attack degrees, indicating that viability gains are easier to achieve. Scenarios with an intermediate value of Γ and a medium attack degree exhibit the highest frequency of saved networked: up to around 65% of dead networks can be saved for an attack degree of 0.6 in the case of the permutation between uncoupled nodes, and up to 95% of dead networks can be saved for an attack degree of 0.65 for permutations between uncoupled and coupled nodes. When the attack degree is low, there is little room for viability gain because in most cases, the remaining connected components are alive, while when the attack degree is high, the remaining components are smaller and more isolated which results in a symbiotic viability condition more difficult to achieve with the rapidly shrinking number of permutable nodes left alive. Permutation will therefore grant a symbiotic interdependent system the greatest gain in viability for a combination of intermediate values of attack and a moderately stringent interdependency threshold condition Γ.

Discussion

We have presented changes to ways to define network interdependency and post-attack viability that significantly impact the topological robustness of coupled networks to random attacks from our simulation results. We have first shown that the topological robustness of more easily fragmented interconnected networks topologies (such as Watts-Strogattz and ring lattices topologies) can be significantly improved by allowing multiple largest remaining components to be viable. This points to the possibility that in easily fragmented networks, granting secondary, and by extension smaller connected components a greater viability could enhance significantly the robustness of the whole system. Furthermore, we have provided evidence that allowing a node in a given network to have multiple counter parts in another network

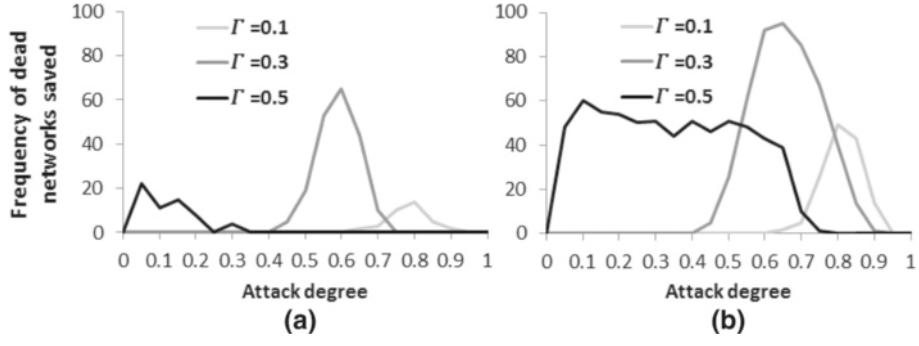

Figure 17 The frequency of dead networks saved for each attack degree when using permutation. The frequency of dead networks saved for each attack degree when using permutation between uncoupled nodes **(a)** and permutation between uncoupled and coupled nodes **(b)** for low ($\Gamma = 0.1$), medium ($\Gamma = 0.3$), and high ($\Gamma = 0.5$) symbiotic interdependency values.

(many-to-one mapping) can be an effective way to transfer damages due to cascading failure from one network to another without changing the robustness of the overall system. This observation could lead to speculate on the possibility of creating mechanisms of damage transfer, similar to the way water is transferred betweeen ballasts in a ship, but instead applied to shifting damages due to cascading failure in sub-networks. We have also observed that, in symbiotic networks, the highest robustness cannot be achieved just by increasing partitioning that would result in cutting off entire sub-networks, but rather by finding an optimal degree of coupling that simultaneously minimises the negative impact of isolation while limiting the probability of spreading cascading failure. If we were to speculate on how to translate this topological observation to the domain of functional robustness of infrastructure networks, we would observe that cascading failure being inherent to symbiotic interdependency, the more an infrastructure depends on connections between multiple different types of services in order to function properly, the more likely failure is to spread iteratively through different parts of a system during periods of stress or perturbation. The apparent propensity of modern infrastructure systems to require an increasing number of services to function together is likely to amplify that significant problem. One way to reduce the impact of the resulting symbiotic interdependency could be to design infrastructure nodes that can switch between different roles across distinct interdependent networks, such that they have the capacity to be functionally permutable. This mean that these nodes should not fulfil simultaneously multiple roles (e.g., dual infrastructures), but rather that they would have the ability to perform only one type of alternate service at any particular time. These rewiring capabilities akin to those found in the human brain could possibly give infrastructure networks the capacity to adapt while limiting the topological sensitivity to disruption associated with symbiotic interdependency.

While our simulation results can provide some insight into how isolation and other mechanisms can affect robustness in interdependent networks, there are substantial limitations to their applicability and generality. So far, we have limited our analysis to a pair of coupled networks, but real-world problems can display a dizzying number of interconnected systems. In such cases, the viability of a component will not just depend on being connected to only one other network, but to many more. With the increase of the dimensionality of dependency thresholds, the robustness of the whole system might become drastically lower. If the effects of high-dimensional dependency thresholds over the robustness of such systems are so far not explored, the implications of a one-dimensional dependency threshold as shown in this paper are already far reaching. Moreover, our models are biased in that choosing the nodes coupled between networks randomly does not necessarily reflect the attachment preferences encountered in real world cases. Other selection strategies such as correlation based on nodes with the highest degree, or the highest betweenness centrality, or even spatially embedded networks (Beyeler et al. 2007; Gao et al. 2014; LaViolette et al. 2006; Newman 2003) would result in different biases. Similarly, one could argue that random attacks are just one way to destroy the networks, and that other attack strategies based on different measures of centrality or system load as in (Su et al. 2014) might give a different view of the problem. The proposed introduction of permutable nodes that would give interconnected systems rewiring capabilities, and guarantee a higher symbiotic viability seems sound from a topological point of view, but would require some feasibility study from the point of view of functional robustness and cost implications to make it applicable to real-life networks such as the industrial complex when day to day operations depend on the simultaneous availability of multiple technologies, ecosystems where the mutually dependent species cannot exist in isolation, or mutually dependent transport networks.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
MK designed the study, programmed the simulation tools, conducted experiments and drafted the manuscript. SB provided supervisor guidance, participated in the study design and coordination and helped to draft the manuscript. RD and GH contributed to the study design and helped to draft the manuscript. All authors read and approved the final manuscript.

Authors' information
MK is a postdoctoral resarch fellow in computer science previously working in the University of Southampton on modelling the resilience of interdependent and symbiotic networks to cascading failure. He is presently working in the University of Surrey on developing tools to model metabolic network activity of the cells and their resilience to cascading failure from a toxicologic point of view. SB is Professor of Computer Science in the University of Southampton, and helped found the Agents, Interaction and Complexity (AIC) research group. Some of his research interests lie in modelling the behaviour of complex networks such as infrastructures from a "system of systems" perspective. GF is a Senior Researcher modelling Infrastructure Resillience in Newcastle University. RD is Professor of Earth Systems Engineering and EPSRC Research Fellow in the University in Newcastle University. One of his research interests lies in developing adaptative solutions to ensure our infrastructures and cities are resilient and sustainable in the face of intensifying global change.

Acknowledgements
The authors acknowledge the use of the IRIDIS High Performance Computing Facility, and associated support services at the University of Southampton, in the completion of this work. This research is supported by the UK Engineering and Physical Sciences Research Council (EPSRC) and Economic and Social Research Council (ESRC) Resilient Futures project (EP/I005943/1). We are grateful to other members of the Resilient Futures team for motivating and interesting discussions on network disruption and resilience. Richard Dawson is funded by an EPSRC fellowship (EP/H003630/1).

Author details
[1]University of Southampton, Highfield, SO17 1BJ Southampton, UK.
[2]Newcastle University, Cassie Building, NE1 7RU Newcastle upon Tyne, UK.

Received: 2 October 2014 Accepted: 2 April 2015
Published online: 30 April 2015

References

Albert R, Jeong H, Barabsi A (2000a) Error and attack tolerance of complex networks. Nature 406:378–382
Albert R, Jeong H, Barabasi AL (2000b) Error and attack tolerance of complex networks. Nature 406(6794):378–382
Bak P, Tang C, Wiesenfeld K (1988) Self-organized criticality. Phys Rev A 38(1):364–374
Battiston S, Gatti DD, Gallegati M, Greenwald BC, Stiglitz JE (2009) Liaisons dangereuses: Increasing connectivity, risk sharing, and systemic risk. Technical report, National Bureau of Economic Research
Beyeler WE, Glass RJ, Bech ML, Soramäki K (2007) Congestion and cascades in payment systems. Physica A: Stat Mech Appl 384(2):693–718
Brummitt CD, D'Souza RM, Leicht EA (2012) Suppressing cascades of load in interdependent networks. Proc Natl Acad Sci 109(12):E680–E689
Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S (2010) Catastrophic cascade of failures in interdependent networks. Nature 464(7291):1025–1028
Callaway DS, Newman MEJ, Strogatz SH, Watts DJ (2000) Network robustness and fragility: Percolation on random graphs. Phys Rev Lett 85(25):5468–5471
Cerda Jacobo J (2010) A decentralised graph-based framework for electrical power markets. PhD thesis, School of Electronics and Computer Science, University of Southampton
Cohen R, Havlin S (2002) Percolation critical exponents in scale-free networks. Phys Rev E 66(3):036113
Crucitti P, Latora V, Marchiori M (2004) Model for cascading failures in complex networks. Phys Rev E 69(4):045104-1 to 045104-4
Crucitti P, Latora V (2005) The importance of being central. In: Proc. 31st Workshop Erice. World Scientific Publishing, Singapore
Crucitti P, Latora V, Porta S (2006) Centrality measures in spatial networks of urban streets. Phys Rev E 73(3):036125
Dorogovtsev SN, Goltsev AV, Mendes JFF (2008) Critical phenomena in complex networks. Rev Modern Phys 80(4):1275–1335
Dunn S, Fu G, Wilkinson S, Dawson R (2013) Network theory for infrastructure systems modelling. Proc ICE - Eng Sustainability 166:281–29211
Fu G, Dawson R, Khoury M, Bullock S (2014) Interdependent networks: vulnerability analysis and strategies to limit cascading failure. Eur Phys J B 87(7):1–10
Gao J, Buldyrev SV, Havlin S, Stanley HE (2012) Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes. Phys Rev E 85(6):066134
Gao J, Buldyrev SV, Havlin S, Stanley HE (2011b) Robustness of a network of networks. Phys Rev Lett 107:195701
Gao J, Li D, Havlin S (2014) From a single network to a network of networks. Nat Sci Rev 1(3):346–356
Hines P, Cotilla-Sanchez E, Blumsack S (2010) Do topological models provide good information about electricity infrastructure vulnerability? Chaos 20(3):033122
Hu Z, Verma PK (2011) Topological resilience of complex networks against failure and attack. In: Advanced Networks and Telecommunication Systems (ANTS), 2011 IEEE 5th International Conference On. IEEE, USA. pp 1–6
Latora V, M (2005) Vulnerability and protection of infrastructure networks. Phys Rev E 71(1):015103
LaViolette RA, Beyeler W, Glass R, Stamber K, Link H (2006) Sensitivity of the resilience of congested random networks to rolloff and offset in truncated power-law degree distributions. Physica A: Stat Mech Appl 368(1):287–293
Leicht EA, D'Souza RM (2009) Percolation on interacting networks. ArXiv e-prints. http://adsabs.harvard.edu/abs/2009arXiv0907.0894L
Motter AE (2004) Cascade control and defense in complex networks. Phys Rev Lett 93(9):098701
Najjar W, Gaudiot JL (1990) Network resilience: A measure of network fault tolerance. Comput IEEE Trans 39(2):174–181
Newman ME (2003) The structure and function of complex networks. SIAM Rev 45(2):167–256
Panzieri S, Setola R (2008) Failures propagation in critical interdependent infrastructures. International Journal of Modelling, Identification and Control 3(1):69–78
Parshani R, Buldyrev SV, Havlin S (2010) Interdependent networks: Reducing the coupling strength leads to a change from a first to second order percolation transition. Phys Rev Lett 105(4):048701
Schneider CM, Yazdani N, Araujo NAM, Havlin S, Herrmann HJ (2013) Towards designing robust coupled networks. Scientific reports 3. Nature Publishing Group
Su Z, Li L, Peng H, Kurths J, Xiao J, Yang Y (2014) Robustness of interrelated traffic networks to cascading failures. Sci Rep 4:5413–5413
Wood A, Wollenberg B (1996) Power generation operation and control. In: Fuel and Energy Abstracts. Energy Institute, Great Britain Vol. 37. pp 195–195