Indian Academy of Sciences Conference Series (2019) 2:1
DOI: 10.29195/iascs.02.01.0009

Interplay of intra- and inter-dependence affects the robustness of network of networks

ARADHANA SINGH[1,*] and SITABHRA SINHA[1,2]

[1]The Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai 600 113, India
[2]Homi Bhabha National Institute, Anushaktinagar, Mumbai 400 094, India
[*]Corresponding author. E-mail: aradhana22singh@gmail.com

Abstract. The existence of inter-dependence between multiple networks imparts an additional scale of complexity to such systems often referred to as 'network of networks' (NONs). We have investigated the robustness of NONs to random breakdown of their components, as well as targeted attacks, as a function of the relative proportion of intra- and inter-dependence among the constituent networks. We focus on bi-layer networks with two layers comprising different numbers of nodes in general and where the ratio of intra-layer to inter-layer connections, r, can be varied, keeping the total number of nodes and overall connection density invariant. We observe that while the responses of different networks to random breakdown of nodes are similar, dominantly intra-dependent networks ($r \ll 1$) are robust with respect to attacks that target nodes having the highest degree but when nodes are removed on the basis of the highest betweenness centrality (CB), they exhibit a sharp decrease in the size of the largest connected component (LCC) (resembling a first-order phase transition) followed by a more gradual decrease as more nodes are removed (akin to a second-order transition). As r is increased resulting in the network becoming strongly inter-dependent ($r \gg 1$), we observe that this hybrid nature of the transition in the size of the LCC in response to targeted node removal (based on the highest CB) changes to a purely continuous or second-order transition. We also explore the role of layer size heterogeneity on robustness, finding that for a given r having layers comprising very different numbers of nodes results in a bimodal degree distribution. For dominantly inter-dependent networks, this results in the nodes of the smaller layer becoming structurally central. Selective removal of these nodes, which constitute a relatively small fraction of the network, leads to breakdown of the entire system – making the inter-dependent networks even more fragile to targeted attacks than scale-free networks having power-law degree distribution.

Keywords. Networks; inter-dependence; robustness; percolation transition.

PACS Nos 89.75.Hc; 05.70.Fh; 89.65.Gh; 64.60.ah

1. Introduction

Robustness, a property often attributed to complex systems occurring in nature, refers to their ability to maintain most of their vital functions even when subjected to noise or perturbations, both extrinsic and intrinsic, that may result in loss or damage of a significant fraction of their components [1]. The investigation of robust systems, especially those that occur in biology and ecology, with the aim of identifying the features that contribute to their ability to withstand component failures or attacks on parts thereof, has obvious implications in terms of applications. These include designing robust man-made systems, as well as, arriving at fail-safe strategies to reduce vulnerabilities of existing systems such as the electrical power grid, where an initially small local perturbation (such as shorting caused by a branch falling on a transmission line) can occasionally trigger a massive system-wide breakdown resulting in power blackouts over entire regions [2]. As many complex systems can be represented as networks, with the components represented as nodes while the interactions between them are represented as links, robustness can also be measured in terms of the ability of a system to maintain its integrity even after a specified fraction of its nodes and/or links has been removed [3–5]. An oft-cited example is the internet, comprising servers (nodes) connected by data cables (links), whose functioning should not be affected significantly by temporary loss of components through failures occurring randomly, as well as, malicious denial-of-service attacks that may target specific nodes [6]. Following the 2007–9 financial crisis, the robustness of the network of financial institutions has also been the subject of intense investigation by scientists who seek to understand factors contributing to systemic risk that can cause credit default by a few firms to eventually result in an overall economic catastrophe [7].

Complicating the already difficult question of what factors lead to robustness of complex networks is the fact that in reality, most networks do not operate completely in isolation but often are seen to interact with other equally complex networks. Moreover, inter-dependence between multiple networks could be a crucial feature underlying the proper functioning of each of them. An example is the coupled system of the electrical power grid and the communication network of computers [8]. While the network of computers controls the functioning of the power grid, the computers are dependent on the grid for their power. Failure in nodes of one of the networks (e.g. shutting down of a power generation unit) would affect nodes in the other network (e.g. disrupting the communication between computers), which in turn will lead to further breakdowns of both the networks in a recursive fashion [9–11]. In general, inter-dependent networks can be seen as comprising different layers in a composite network of networks (NONs).

A strikingly novel aspect of inter-dependent networks is that they typically respond very differently to structural perturbations such as removal of a fraction of their nodes when compared to the behavior of the component networks in isolation. In particular, inter-dependent networks exhibit a first-order phase transition in the size of the largest connected component (LCC) when nodes are gradually removed, which changes to a continuous transition when the fraction of inter-dependent nodes is reduced [12]. Assuming that only nodes belonging to the LCC remain functional, this would suggest that inter-dependent networks are more vulnerable to node failure and targeted attacks than the individual systems that they comprise [8, 13]. While a few earlier studies have considered the role of intra- and inter-network dependences in determining the robustness of NONs [14–16], it is important to maintain the average degree of the nodes invariant when comparing systems with different ratios of intra- to inter-network connections (as otherwise we cannot disambiguate the contribution of the overall number of connections from that specifically of the inter-dependent links). In addition, different networks have often been chosen to be of the same size. However, in reality, NONs can comprise component networks comprising widely differing number of nodes. In this paper we report the results of a systematic investigation of the robustness of NONs to different types of node removal strategies, incorporating the different aspects mentioned above.

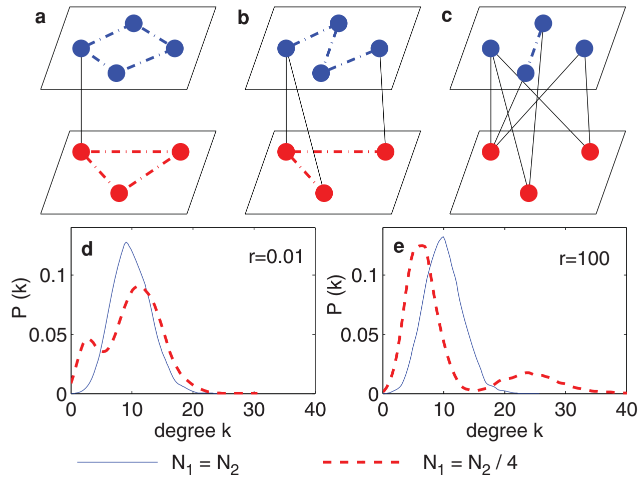

Figure 1. NONs consisting of two layers of nodes that have connections both within a layer (broken lines) and between layers (solid lines) representing intra- and inter-dependence, respectively, exhibit very different degree distributions depending on relative sizes of the layers. (**a**)–(**c**) Schematic diagram of bi-layer networks corresponding to situations where the networks are dominantly intra-dependent (**a**), homogeneous (**b**) and dominantly inter-dependent (**c**). (**d**)–(**e**) Degree distributions for bi-layer networks having different ratios of intra-layer to inter-layer connections, r (viz., $r = 0.01$ in (**d**) and $r = 100$ in (**e**)), where the layers could be either of equal size, i.e. $N_1 = N_2$ (solid curves) or of unequal sizes, viz., $N_1 = N_2/4$ (broken curves). While the former case does not show much variation between dominantly intra-dependent (i.e. $r \ll 1$) and dominantly inter-dependent (i.e. $r \gg 1$) systems, NONs with heterogeneous layer sizes show bimodal degree distributions whose profiles differ for dominantly intra-dependent and dominantly inter-dependent systems. Each distribution is averaged over 10 realization with total network size $N = N_1 + N_2 = 500$ and average degree $\langle k \rangle = 10$.

2. Model

The model system we consider for our investigation is a NON of two networks comprising N_1 and N_2 nodes, respectively. In order to analyze the relative contributions of intra- and inter-dependence in this system, we alter the probabilities of a connection between nodes belonging to the same layer (p_{intra}) and those belonging to different layers (p_{inter}). This is performed by assigning different values to the ratio $r = p_{\text{inter}}/p_{\text{intra}}$ while keeping the total size of the NON ($N = N_1 + N_2$) and the average degree of the network $\langle k \rangle$ invariant [17, 18]. For $r \ll 1$, the NON is dominantly intra-dependent (figure 1a), while it is dominantly inter-dependent if $r \gg 1$ (figure 1c). The special case of $r = 1$ corresponds to a homogeneous Erdös–Renyi network (figure 1b). Thus, as r is increased from 0, the NON changes gradually from being completely intra-dependent (consisting of two isolated modules) in one limit to completely inter-dependent (corresponding to a bipartite network, which can be viewed as a hierarchical network consisting of two levels) in the other limit.

Randomly connected bi-layer networks where the two layers are of the same size ($N_1 = N_2$) have Poisson degree distributions regardless of r (figures 1d and e, solid curves). However, if N_1 and N_2 are very different, this results in the two layers having very different average degrees (even though average degree of the NON, $\langle k \rangle$, remains unchanged) with the overall degree distribution exhibiting a bimodal form (broken curves in figures 1d and e). The exact profile of the bimodal distribution depends on the value of r, with the lower peak corresponding to the smaller (larger) layer for dominantly intra-dependent (inter-dependent) networks.

We have considered the robustness of the model bi-layer networks described above using a standard percolation-theoretic approach [3]. Specifically, we remove nodes one at a time using different strategies, e.g. at random or choosing nodes having the highest degree or betweenness centrality (CB). After removing a fraction f of the N nodes in the NON, we measure the probability that a randomly chosen node is still part of the LCC of the NON after these removals ($P_{\text{LCC}}(f)$), by expressing it in terms of the probability that the node was part of the LCC of the NON before any nodes were removed ($P_{\text{LCC}}(0)$). Note that, for a homogeneous Erdös–Renyi random network (for $r = 1$), it is well-known that even after the removal of a fraction f of the nodes (such that the effective size of the network is now $N_{\text{eff}} = (1 - f)N$), the Poisson character of the degree distribution is preserved with only the effective average degree reducing to $k_{\text{eff}} = (1 - f)k$. As the condition for a Erdös–Renyi network to possess a giant component is $\langle k^2 \rangle / \langle k \rangle \gtrsim 2$ [19], the critical value of fraction of nodes removed beyond which the network exhibits a transition to isolated fragments is given by $f_c = 1 - (1/\langle k \rangle)$. This provides a natural benchmark against which to compare the robustness of the random bi-layer networks in response to the removal of a fraction of their nodes. We have also compared the results with that of the Price–Barabasi–Albert scale-free network that has been shown to be more robust with respect to random removal of nodes compared to Erdös–Renyi networks, but extremely vulnerable to attacks targeted at nodes with the highest degree or CB [5].

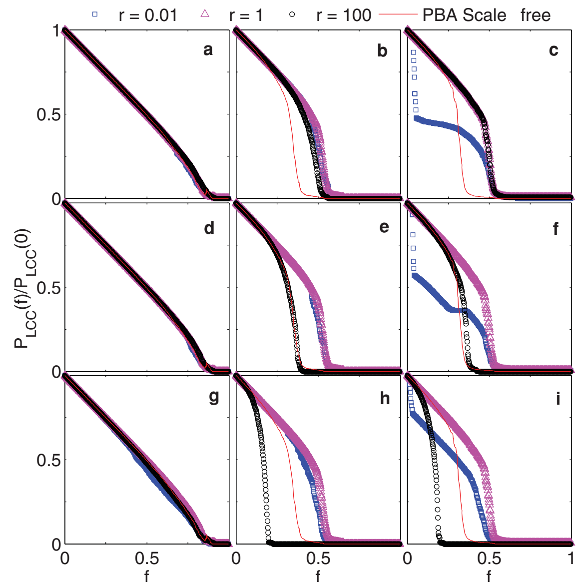

Figure 2. Robustness of random networks comprising two layers (with N_1 and N_2 nodes, respectively) that have different proportions of intra- and inter-layer dependence shown for different types of node failures and layer size heterogeneity. On removing a fraction f of the nodes in the network, the probability $P_{\text{LCC}}(f)$ that a node will be part of the largest LCC is expressed relative to the probability $P_{\text{LCC}}(0)$ that it was part of the LCC in the original network. The first row (panels (**a**)–(**c**)) shows the situation where the two layers possess an identical number of nodes (i.e. $N_1 = N_2$), while the second row (panels (**d**)–(**f**)) and third row (panels (**g**)–(**i**)) considers layers of unequal size, viz., $N_1 = 2N_2/3$ and $N_1 = N_2/4$, respectively. In all cases the total size of the network $N = N_1 + N_2 = 500$ and average degree $\langle k \rangle = 10$. In each row, different panels show the robustness of a network against different types of node failure protocols, corresponding to the removal of nodes at random (left), according to the highest degree (center) and according to the highest CB (right). Each panel shows the response to successive removal of nodes for networks that are (i) dominantly intra-dependent ($r = 0.01$, blue squares), (ii) homogeneous ($r = 1$, maroon triangles) and (iii) dominantly inter-dependent ($r = 100$, black circles). For comparison, we also show the response of Price–Barabasi–Albert scale-free networks (red curve). Each data point is obtained by averaging over 10 network realizations. We note that while for random breakdown of nodes, the response of the different networks has similar profiles, with respect to attacks that target nodes having the highest degree or CB, the dominantly inter-dependent networks are relatively more vulnerable than the other types of networks when the layers have very different sizes. In addition, the dominantly intra-dependent networks show a sharp decrease in the fraction remaining in LCC for low f when the attacks target nodes having the highest CB.

3. Results

We first consider the response of bi-layer networks to the removal of nodes chosen at random for NONs characterized by different ratios of intra- and inter-dependence and where the layers are of the same size (figure 2a). We observe that regardless of r, the networks exhibit a similar response profile to the removal of nodes. A second-order transition is seen to occur at a critical value $f_c \sim 0.9$ of the fraction of nodes removed, where the system reduces to several disconnected fragments. Introducing layer size heterogeneity does not appreciably alter the results as can be seen from panels (d) and (g) of figure 2 that correspond to $N_1 = 2N_2/3$ and $N_1 = N_2/4$, respectively.

We next consider robustness of the NON against targeted attacks aimed at structurally important nodes. These could either be the hubs, i.e. nodes having the highest degree, or may be connecting a large number of nodes to each other through the shortest paths that pass through them, i.e. nodes with the highest CB [4]. We observe that dominantly intra-dependent networks are almost as robust as Erdös–Renyi networks against attacks targeted at the highest degree nodes, while the dominantly inter-dependent networks are only marginally less robust (figure 2b). We observe that at around $f_c \sim 0.5$, the networks exhibit a smooth transition to fragmentation. Note that, the Price–Barabasi–Albert scale-free network is much less robust against degree-based attacks and collapses at $f_c \sim 0.4$. With increasing layer size heterogeneity, however, the dominantly inter-dependent networks become increasingly fragile with the transition to fragmented state occurring at critical values of f that may be even lower than that for scale-free networks (see panels (e) and (h) of figure 2). By contrast, intra-dependent networks do not show any variation with respect to changing sizes of the layers.

Dominantly inter-dependent networks show a similar behavior when instead of targeting the highest degree nodes, the highest BC nodes are removed preferentially (panels (c), (f) and (i) of figure 2). However, the dominantly intra-dependent networks exhibit a strikingly different response, with the size of the LCC showing a very sharp decrease (resembling a first-order phase transition) from N to N_1 upon removing only about 3% of the nodes. This suggests that at this value of f (~0.03), the layers of the NON become isolated from each other. Following this, the effect of removing additional nodes according to the highest CB is similar to that for Erdös–Renyi networks and consequently, we observe a continuous transition to the fragmented state, explaining the hybrid phase transition seen for the case of dominantly intra-dependent networks. Increasing layer size heterogeneity only changes this picture by decreasing the critical value of f at which the initial sharp decrease in the LCC size occurs, as well as, the amount by which the LCC size decreases.

The response of the dominantly inter-dependent networks with respect to targeted attacks on nodes (based either on the highest degree or highest CB) as layer size heterogeneity increases can be understood in terms of the changing connectivity profile as revealed by the degree distribution (figure 1e). When the two layers are similar in terms of size, almost all nodes are equivalent in terms of their degree. Thus, the response of the network to attacks will be almost identical to that seen for Erdös–Renyi networks. However, when the sizes of the two layers are very different, the nodes of the smaller layer typically would have much higher degree than the average degree of the NON (as revealed by the bimodal degree distribution shown in panel (e) of figure 1). Thus, these will function as hubs of the network. Targeting these relatively fewer number of nodes will severely damage the network in terms of connectivity. However, identifying such nodes in dominantly inter-dependent NONs and providing them additional protection will be an efficient procedure for increasing the robustness of the entire system.

We would like to point out that the framework outlined here for investigating the robustness of NONs, particularly in situations where the connections between two layers have a partially bipartite character, can be useful for understanding how initially localized perturbations can eventually result in global failure in complex systems that occur in reality. In particular, it could be relevant for estimating systemic risk, specifically, risk spillover in the financial system triggered by the collapse of a financial institution or company. The NON comprising banks in one layer and firms in the other resemble an almost bipartite graph as typically banks are linked to firms (and vice versa) through credit relations [20]. The connections between banks through inter-bank financial liabilities, and that between firms through trade credit, have relatively lower densities. The nodes in such a system could be fairly heterogeneous in terms of their degree as a few large banks may account for the bulk of the lending to firms. In addition, the larger firms may be borrowing from a large number of banks, possibly with degree homophily between the bank nodes and firm nodes [21]. Thus, analysis of robustness of NONs with a heterogeneous degree distribution [22] may provide us with insights into how economy-wide catastrophic failures [23], such as that witnessed during the 2008 global financial crisis, can come about.

4. Conclusion

In this paper we have reported the results of our investigation on the role played by intra- and inter-dependence in imparting robustness to NONs by considering an ensemble of model random bi-layer networks. By systematically varying the relative density of intra- and inter-layer connections we show that increasing inter-dependence can make such NONs vulnerable to targeted attacks on nodes, especially when different layers are populated by very different numbers of nodes. This can be related to the very different connectivity profiles of the nodes in the two layers, manifested in a bimodal degree distribution for the NON. We also observe that when faced with attacks targeted at nodes having the highest CB, increased dominant intra-dependence results in a hybrid transition. This corresponds to an initially sharp decrease in the size of the LCC (resembling a first-order phase transition) followed by a continuous or second-order transition with increasing fraction of nodes removed. As in NONs that occur in nature, the sizes of the different component networks can be quite different, our results may provide insights into their robustness and help in suggesting guidelines for constructing more robust artificial NONs.

Acknowledgements

The authors would like to thank Shakti N Menon for helpful discussions. This work was supported in part by the IMSc Complex Systems (XII Plan) Project funded by the Department of Atomic Energy, Government of India. The authors thank the IMSc High Performance Computing Facility for access to the Nandadevi cluster in which the simulations required for this work were done.

References

[1] See, e.g. *Robust Design: A Repertoire of Biological, Ecological, and Engineering Case Studies*, ed. E Jen (Oxford University Press, New York, 2005)

[2] National Academies of Sciences, Engineering and Medicine, *Enhancing the Resilience of the Nation's Electricity System* (National Academies Press, Washington DC, 2017), https://doi.org/10.17226/24836

[3] D S Callaway, M E J Newman, S H Strogatz and D J Watts, *Phys. Rev. Lett.* **85**, 25 (2000)

[4] R Albert, H Jeong and A-L Barabasi, *Nature* **406**, 378 (2000)

[5] A-L Barabasi, *Network Science* (Cambridge University Press, Cambridge, 2016)

[6] J C Doyle, D L Alderson, L Li, S Low, M Roughan, S Shalunov, R Tanaka and W Willinger, *Proc. Natl. Acad. Sci. USA* **102**, 14497 (2005)

[7] R M May, S A Levin and G Sugihara, *Nature* **451**, 893 (2008)

[8] S V Buldyrev, R Parshani, G Paul, H E Stanley and S Havlin, *Nature* **464**, 08932 (2010)

[9] M M Danziger, A Bashan, Y Berezin, L M Shekhtman and S Havlin, *Nonlinear Dynamics of Electronic Systems*, eds V M Mladenov and P Ch Ivanov (Springer, Cham, 2014), 189

[10] J Gao, S V Buldyrev, H E Stanley and S Havlin, *Nat. Phys.* **8**, 40 (2012)

[11] S Perera, M G H Bell and M C J Bliemer, *Appl. Netw. Sci.* **2**, 33 (2017)

[12] R Parshani, S V Buldyrev and S Havlin, *Phys. Rev. Lett.* **105**, 048701 (2010)

[13] X Huang, J Gao, S V Buldyrev, S Havlin and H E Stanley, *Phys. Rev. E* **83**, 065101 (2011)

[14] Y Hu, B Ksherim, R Cohen and S Havlin, *Phys. Rev. E* **84**, 066116 (2011).

[15] E A Leicht and R M D'Souza, arXiv:0907.0894 (2009), https://arxiv.org/abs/0907.0894

[16] R K Singh and S Sinha, *Phys. Rev. E* **96**, 020301 (2017)

[17] R K Pan and S Sinha, *Europhys. Lett.* **85**, 68006 (2009)

[18] A Singh, M I Ashraf and S Sinha, arXiv:1902.02668 (2019), https://arxiv.org/abs/1902.02668

[19] M Molloy and B Reed, *Random Struct. Algor.* **6**, 161 (1995)

[20] L Marotta, S Micciche, Y Fujiwara, H Iyetomi, H Aoyama, M Gallegati and R N Mantegna, *Plos One* **10**, e0123079 (2015)

[21] G De Masi and M Gallegati, *Empir. Econ.* **43**, 851 (2012)

[22] A Hintze and C Adami, *Biology Direct* **5**, 32 (2010)

[23] C Reinhart and K Rogoff, *This Time is Different* (Princeton University Press, Princeton, 2009)