Universität Zürich[UZH]

Network Science

Catastrophic cascade of failures in interdependent networks

Luc Seiler (13-937-941), Lorin Sidler (13-913-686) & Wenxi Feng (18-745-257)

Network Science for Business, Economics, Informatics and Social Sciences

Faculty of Business, Economics and Informatics

8th December 2019

ABSTRACT

Networks today become increasingly interdependent, which makes them more susceptible to random node failure. A random removal of a small number of nodes from one network can lead to a cascade of failures in several connected networks, potentially even result in a complete fragmentation of the system. Therefore, the characteristics of interacting networks differs substantially from single, non-interacting networks. As we follow closely the approach of Buldyrev et al. (2010) in the analysis of node failures in interdependent networks, we include both a real-world example of a network, as well as differently specified random networks to simulate the iterative process of a cascade of failures. The aim of this project is to be able to understand the robustness of interacting networks. As a result, we find that both our real-world and random Erdös-Réyni interdependent networks are in fact very fragile. Furthermore, we find some evidence that interdependent scale-free networks are susceptible to fragmentation when attacked with the cascading failure process.

1 INTRODUCTION

In complex modern networks, the systems are often coupled together and, therefore, dependent on each other. Hence, a failure of nodes in one network may lead to failure of corresponding nodes in interdependent networks, ultimately resulting in the cascade of failures. One real-world example is the electric blackout in Italy in 2003, described in the paper by Buldyrev et al. (2010) where the shutdown of a few power stations lead to the failure of nodes in the internet communication network, which lead to the recursive failure of more power stations, resulting in a catastrophic cascade of failure in both interdependent networks.

For the scope of our project, we aim to replicate the approach and the corresponding results presented in Buldyrev et al. (2010). To model the interdependent reaction between two real-world networks, we investigate the consequence of a node failure, initially occurring in an electrical grid, on an educational telecommunication

network. As a real-world example, we focus on the analysis of the dependence between the German transmission grid for renewable energy sources (RES) and the German research network (X-WiN) of the DFN. Section 2 describes the real-world data that we have acquired. Section 3 discusses the methods we used to construct our interdependent networks and the iterative process of cascade of failure. In Section 4, we subject both our real-world interdependent network and random interdependent network the the iterative cascade of failures. Lastly, in section 5, we conclude the findings of our project.

2 DATA DESCRIPTION

For the scope of our project, we wanted to analyse a real-world network. Thus, we looked for data we could use to construct an interdependent network comprised of a power grid and an internet network. We were not able to find the exact same data on Italy that has been used in Buldyrev et al. (2010). However, we were able to find the respective data for Germany, that allowed us to construct a real-world interdependent network.

2.1 Power Grid of Germany

Official data on power grids are rarely published due to data handling issues and security concerns. The data we are using have been developed by Mureddu (2016) and are inferred from a number of sources. Recently, the German energy grid experienced a rapid surge in sustainable renewable energy sources (RES). The power grid network thus incorporates both RES and conventional generators, in an attempt to accurately portray the current German energy grid. With this energy revolution, the power systems are now faced with a big number of small and medium sized generators distributed over all voltage levels, which induced a complete redesign of the network structure. The network provides information on the full DC Power Flow operative states in the presence of various amounts of RES share. The network topology is based on Hutcheon and Bialek (2013), enriched with the RES generation available in Germany in 2014 from the Goverment of Germany (2016).

The dataset contains 231 KV buses (network nodes, $N = 231$) which correspond to a transmission substation, lines (network edges) and connected generators in Germany. Most importantly for our study, the geographical position of the nodes was determined by georeferencing. The resulting position is given in latitude (y) and longitude (x) values. Each node code and ID is available and corresponds to the original dataset. For each of the 302 existing lines ($E = 302$) between the network nodes, the following information is given: the starting and ending nodes given in terms of nodes ids and codes as well as their estimated length, obtained by calculating the geodetic distance between the edge terminal nodes. The 89 connected generators included in the dataset are described by their ids and codes, as well as the id and code of the node at which the generator is attached to the network.

2.2 Research Network of Germany

The research network X-WiN we are using in our project was developed by the DFN. It is a national research and education network for data communication between over 400 universities and research institutes in Germany.

The network is managed by the "Association to Promote German Education and Research Network" and it is essentially built up by routers (network nodes, $N = 58$) connected to each other (network edges, $E = 87$). Each node contains metadata on its geographic location in the from of longitude and latitude. The fiber optic connections enable highest transmission rates and almost unlimited transmission capacities. Furthermore, due to the high number of nodes in the network core, DFN is very flexible and can meet the increasing requirements of the science applications. These properties make it one of the most powerful communications networks in the world (Adler et al. 2014).

3 METHODS

We follow closely the approach of Buldyrev et al. (2010) to analyze the cascade of failures in interdependent networks. Therefore, our analysis subjects both a real-world network and differently specified random networks to the iterative process of a cascade of failures.

3.1 Real-world interdependent network

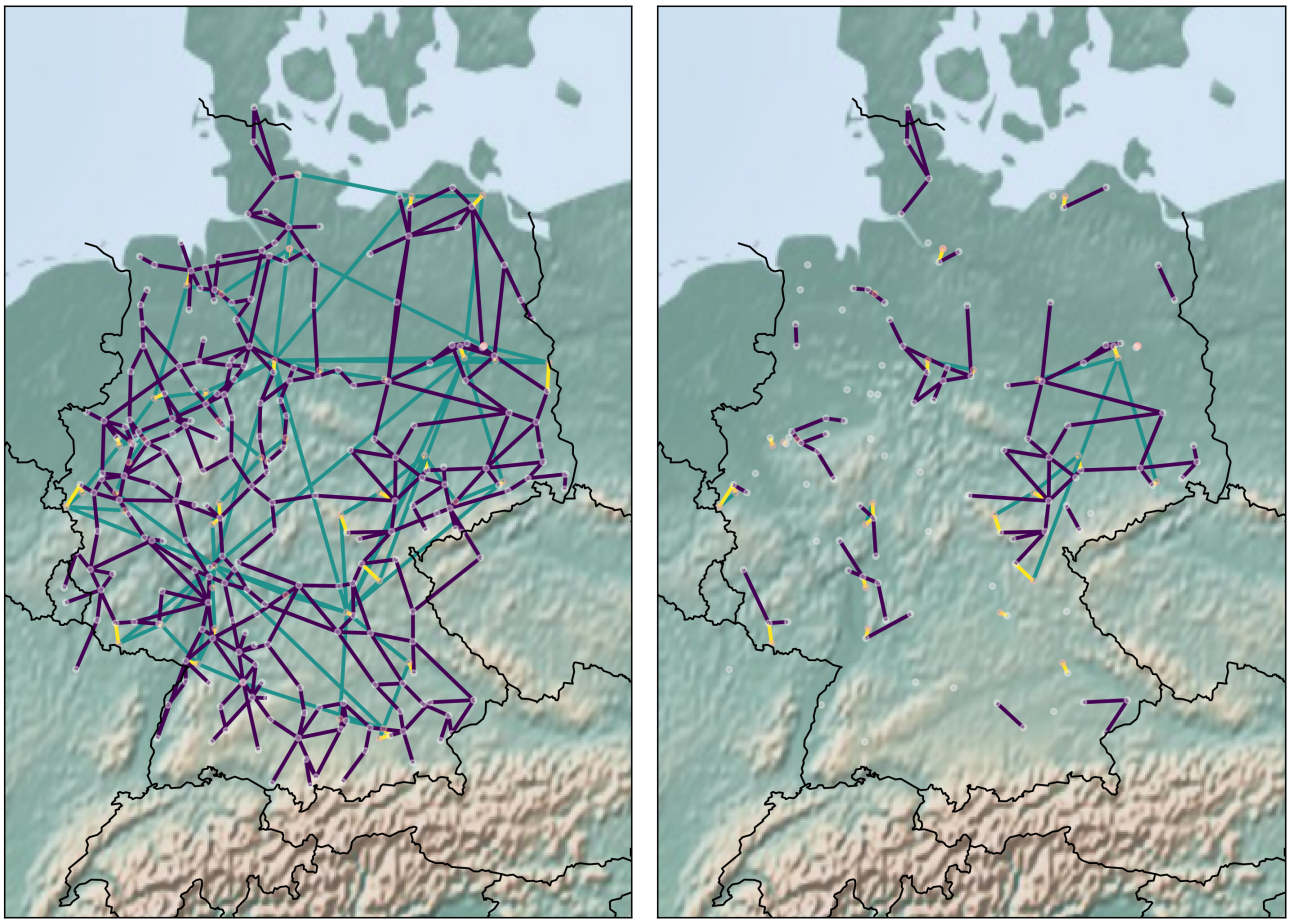
The real-world interconnected network has been constructed based on the approach of Rosato et al. (2008), who are referenced for the Italian real-world network in Buldyrev et al. (2010). In order to connect the two independent networks, we first identified node-pairs between the networks which are geographically close. Distance was computed with the Euclidean distance $\sqrt{(x_a - x_b)^2 + (y_a - y_b)^2}$ from latitude (y) and longitude (x) of each node a in Network A and each node b in Network B. Under the assumption that geographically close nodes are functionally related, we then connected each DFN internet node to the spatially closest power grid station. Moreover, we assumed that each DFN internet node is connected to only one power station, but that a power station could be connected to several DFN internet nodes. To visualize this interdependent network, we projected it onto a basemap of Germany with respect to their true location (Fig 1a).

Whereas Buldyrev et al. (2010) used a real-world graph of Italy to illustrate the iterative process of a cascade of failures based on a historic event of a power outage, we have no record of such an event for Germany. Hence, we subjected our real-world network to random attacks on the power grid, via the process that is described in section 3.3. Fig 1b visualizes such an instance of a random attack via this process, where 50% of power graph stations are removed.

3.2 Random interdependent networks

Random networks provide us with the possibility to generate networks with different topologies, by varying their size and connectedness. This allows us to distinguish whether the robustness of networks is an inherent feature of the the network's topology or occurring at random.

For the first part our analysis, we generate two random Erdös-Réyni networks A, B with average degree $\langle k_A \rangle$ and $\langle k_B \rangle$ and network size N. We assume that the operation of Node A_i $(i = 1, 2, ..., N)$ depends on the the



(a) Full interdependent network

(b) Network after one instance of a random attack where 50% of the power grid stations have been attacked

Fig. 1: Interdependent Network comprised of German Power Grid and Internet (DFN). *Purple edges* represent Power Grid lines, *green edges* represent Internet links and *yellow edges* are the power source for each internet node, that have been established based on geographical proximity.

provision of viable resources from node B_i, and *vice versa*. Hence, to generate an interdependent network, we interlink each node A_i to node B_i (i.e. create edges (A_1, B_1), (A_2, B_2),...).

For the second part, we extend our analysis to scale-free networks. Whereas Erdös-Réyni only allows us to control the network's density by varying the mean degree, scale-free networks require that we fix the degree distribution. In order to create such random graphs with a specific degree distribution, we applied the configuration model. For each of the two networks A and B, we sample a degree distribution of size N from a power-law distribution $P_A(k) = P_B(k) \propto k^{-\lambda}, (k = 2, 3, ...)$. With this specification, we avoid the creation of isolated nodes ($k = 0$) or nodes with only one link ($k = 1$), otherwise our networks would not be connected, or only connected weakly, and break down immediately. The degree distribution is required to be even in total, and therefore sampled until it meets that requirement. The configuration model then creates N nodes with "stubs"

corresponding to the degree distribution. These stubs then become randomly connected until no further pair of stubs can be connected. Even though multiple edges and self-loops are prohibited, we cannot enforce this requirement in this case. Dependent on the random assignment of pair of stubs, we could end up with stubs that can only be assigned to the same node or to an edge that already exists. This is a necessary relaxation of our network model, otherwise the network generating process would not be able to finish. The two resulting networks A and B then are paired up with the same process as described above.

3.3 Modelling an iterative process of a cascade of failures

A fundamental property of interdependent networks is that a failure of nodes in one network may lead to failure of dependent nodes in another network. Compared to a single network, a failure of one sub-network's node can have far more severe consequences on the sub-network itself, but also the interdependent network as a whole. The reason is that the process spreads to the other network and can iteratively compartmentalise the network into clusters, and hence lead to a cascade of failures.

We implemented the process that is described in Buldyrev et al. (2010) and evolves as follows: Lets assume an interdependent network with the same number of nodes where each node in network A depends on exactly one node in network B, and *vice versa*. There can be random connections between nodes of one network itself (network-links), that are determined by the mean degree or the degree distribution. As we attack nodes from network A with probability $1 - p$, the connected nodes in network B are also eliminated. With the nodes in both networks being removed, there is a chance for both networks to break down into clusters. B-links which connect B-nodes to different A-clusters are eliminated. Iteratively, the same process is applied to A-links and the network starts to break down (see Fig. 2).

The implementation of this process into working code proved to be quite a challenge for us. We divided the steps of the process (attack node A, delete neighbor B, remove B-links link between A-clusters) into different functions, while keeping both sub-networks as reference to identify the clusters. The links between those clusters are identified and deleted using a recursive approach.

4 RESULTS

The following section presents the results we obtained by subjecting both the real-world network and random networks of different specifications to the process of iterative cascade of failures. After each attack on the nodes of on of the two sub-networks with probability $1 - p$, we computed the size of the largest mutually connected component relative to the initial network size. We denote this statistic as P_∞, a common definition in network science. The largest mutually connected component is of fundamental interest in our study because it is largest fully functioning part of our interdependent network, where both sub-networks still receive the vital resource that is required to operate.

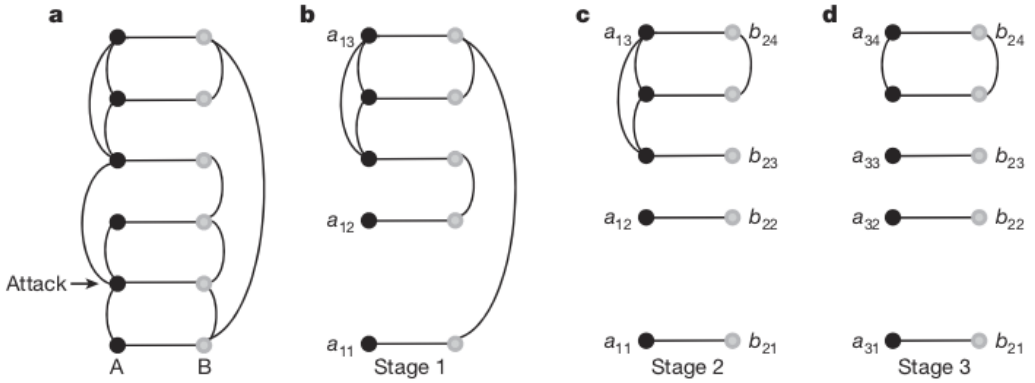


Fig. 2: The iterative process of cascade of failures as proposed in Buldyrev et al. 2010. **(a)** A node in Network A is attacked. **(b)** Any connected nodes in Network B are removed as well. This results in a fragmentation of the network as it breaks into clusters a_i, b_i. **(c - d)** Iteratively, any connecting edges of network B (A) between clusters of network A (B) are removed, until there can be no further link removed. The cluster of a_{34} and b_{24} constitutes the largest mutually connected component.

4.1 Real-World Network

For our real-world network, the two sub-networks are comprised of a power grid and an internet network. The largest mutually connected component in this specific case are the cluster of nodes from the internet that still receive power and nodes from the power grid that still have a connection to the internet (e.g., to manage the power load). We made the assumption that not every power grid station needs to be connected to the internet, so not all power grid station are reliant on the internet.

For our analysis, we staged random attacks on the power grid by removing each node with probability $1 - p$. We averaged our results over multiple attacks to get a more conclusive result that is not dependent on individual node selection. As we would expect from theory and the results presented by Buldyrev et al. (2010), the interdependent network is very fragile. The size of the mutually connected component starts to decrease quickly and early on in the attack (see Fig. 3). In comparison to a single network, the theoretical threshold at which an ER network would dissolve is $p^c = 1/\langle k \rangle$. Both networks have a $\langle k \rangle \approx 3$. Hence, we would expect the network to dissolve at a much later stage in the attack ($p \approx 0.33$). We see this result an initial confirmation of the results presented in Buldyrev et al. (2010).

4.2 Random Networks

For this part we attempted to replicated the results of Buldyrev et al. (2010) presented in Figure 3. Due to time constraints and computational complexity with increasing network size, we could not run an exact replica. Instead, we restricted our analysis to network sizes below 8000 nodes. Even for 8000 nodes, the computation ran for more than 24 hours. Generously, we were able to outsource the computations the university computer, where we could run them in parallel. Otherwise, our result could not have been obtained.

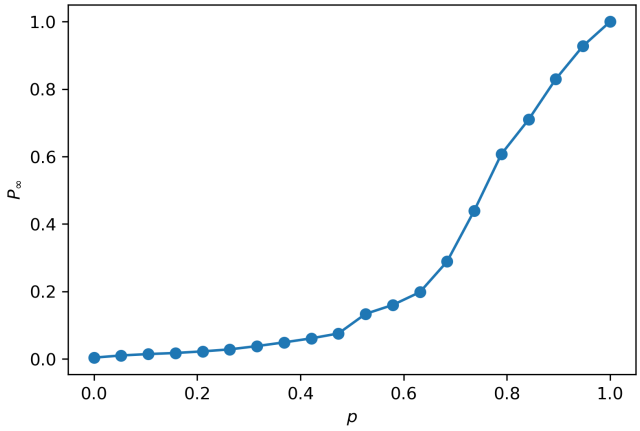


Fig. 3: Results for the real-world interdependent network from Germany

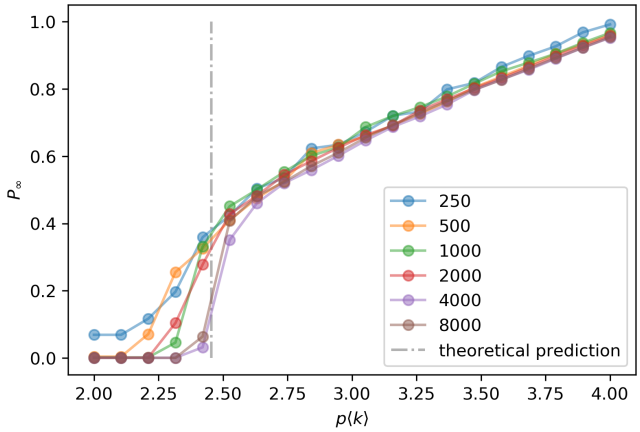


Fig. 4: Results for the ER random networks with $\langle k \rangle = 4$

The first part of our time-intensive results are presented in Fig. 4. What becomes immediately apparent is how our P_∞ decrease steadily, whereas in Buldyrev et al. (2010) it remains at around one even when 20% of the network's nodes are removed. With our understanding of P_∞, this could under no circumstances occur. Since the authors never specifically mention their understanding of this statistic, we cannot fathom the reason for this discrepancy. However, our results do support their theoretical prediction, since the networks start to dissolve at $p^c = 2.4554$. In theory, as $N \to \infty$, the function of the cascade failure process should approach a step function at that critical point. Due to our limited resources, we cannot definitively support this theory. Nevertheless, a pattern does emerge in our data, where with increasing network size, the function decreases more drastically at the critical threshold. A slight deviation from the pattern are the result for $N = 8000$ and $N = 2000$ that decrease a bit less after the threshold than their smaller counterparts. Due to time constraints, we could only repeat the random attack ten times, so this might be a result of a biased attack on a particularly robust part of the network.

The second part of our replication analysis of random networks concerned interdependent scale-free networks. In theory, scale-free networks (with $\lambda \leq 3$) are very robust to random attacks, but fragile when it comes to

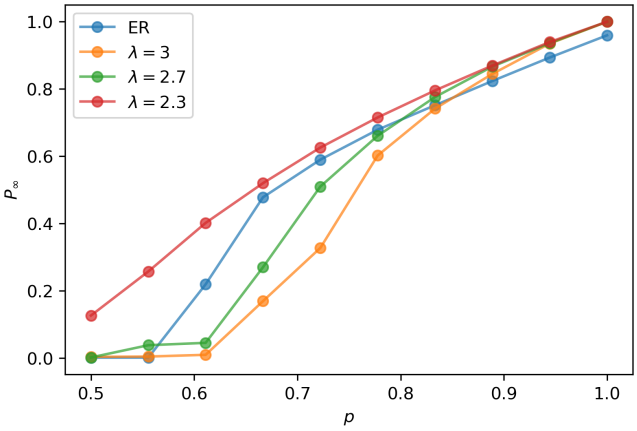


Fig. 5: Results for the ER ($\langle k \rangle = 4$) and scale-free random networks, all with network size $N = 2000$

targeted attacks. This is due to the fact that they contain few high-degree nodes that act as hubs (fragile part), that are attached to many low-degree nodes (robust part). For a simple scale-free network with $\lambda \leq 3$, this means that giant component exists for all $p > 0$. However, when we turn to interdependent scale-free network, the low-degree nodes make the network susceptible to fragmentation when attacked with the cascading failure process. Rather ironically, the broad degree distribution that makes a single network robust against random attack, becomes a disadvantage for interdependent networks.

As a result, we can observe that interdependent scale-free networks do dissolve when subjected to random attacks and have generally a lower threshold than ER networks (see Fig. 5). However, in contrast to Buldyrev et al. (2010), with decreasing λ, the scale-free networks seem to become more robust. The scale-free network with $\lambda = 2.3$ is even more robust than the ER random network. Even though this specification should contain the most low-degree nodes, this network remains the most robust, even in its interdependent form. Again, this might be due to some sample bias, where a particularly robust part of the network was attacked. However, in this case we repeated the attack 30 times, which makes this conjecture less likely. We cannot further reason the discrepancy between our results.

5 CONCLUSION

This project aimed to understand the robustness of interdependent networks on the basis of a real-world example, as well as simulations of random networks. We come to the conclusion that our real-world interdependent networks are in fact very fragile and prone to a cascade of failures. Furthermore, we find evidence that both interdependent ER random networks and scale-free networks are susceptible to fragmentation when attacked with the cascading failure process. Therefore, it is necessary to distinguish between interdependent and single, non-interacting networks. Even if there are minor differences in our results, compared to the findings of the paper by Buldyrev et al. (2010) which is due to the fact that we were constrained in time and resources, we can still conclude that the models presented do capture the phenomenon of cascade failure in connected networks.

REFERENCES

Adler, H.-M., P. Eitner, K. Ullmann, H. Waibel, and M. Wilhelm (2014) "Die Netzinfrastruktur X-WiN des DFN" in: *DFN-Verein*.

Buldyrev, Sergey V., Roni Parshani, Gerald Paul, H. Eugene Stanley, and Shlomo Havlin (Apr. 2010) "Catastrophic cascade of failures in interdependent networks". In: *Nature* 464.7291, pp. 1025–1028. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/nature08932.

Goverment of Germany (2016) *Energy Map project*. http://www.energymap.info/. Last accessed: 28/11/2019.

Hutcheon, Neil and Janusz W. Bialek (2013) "Updated and validated power flow model of the main continental European transmission network". In: *IEEE Grenoble Conference PowerTech*, pp. 1–5.

Mureddu, Mario (2016) "Representation of the German transmission grid for Renewable Energy Sources impact analysis". In: *figshare*. DOI: http://doi.org/10.6084/m9.figshare.4233782.v2.

Rosato, V., L. Issacharoff, F. Tiriticco, S. Meloni, S. De Porcellinis, and R. Setola (2008) "Modelling interdependent infrastructures using interacting dynamical models". In: *International Journal of Critical Infrastructures* 4.1, p. 63. ISSN: 1475-3219, 1741-8038. DOI: 10.1504/IJCIS.2008.016092.