Design of Robust Dependent Networks against Flow-based Cascading Failures

T.M. Ouboter, D.T.H. Worm, R.E. Kooij
TNO
Delft, the Netherlands
{tanneke.ouboter,daniel.worm,robert.kooij}@tno.nl

Huijuan Wang
Delft University of Technology
Delft, the Netherlands
h.wang@tudelft.nl

***Abstract*—In this paper we propose strategies to increase the robustness of a communication network which depends on the proper functioning of an electricity network. The strategies involve selecting nodes of the communication network and removing their dependency on the electricity network. Compared to existing literature on this topic, such as Schneider et al. [1], we use a more realistic model of the electricity network by taking the essential characteristics of the power flow into account, instead of considering purely the topological structure. The effect of the flow-based cascading failures originating from the electrical grid, on the communication network is studied, where the coupling between those networks plays an important role. We have computed the performance of our proposed selection strategies by averaging over many configurations of communication networks, which are modelled both as scale-free networks and as Erdös-Rényi random graphs, applied to an electricity network formed by the IEEE 118 bus test system. We show that a hybrid strategy, based on the degree of the communication nodes and the failure probabilities of the electricity nodes, give a significant improvement over a random selection strategy, as well as over other strategies we proposed. Our method is also tested on a real-world interdependent network: the high voltage electricity grid in Italy coupled with a communication network, inspired by the Italy blackout in 2003.**

Keywords—Network robustness; dependent network; cascading failure; network design

I. Introduction

Government, industry and citizens are becoming more and more convinced of the need to increase the robustness of critical infrastructures, such as energy systems, water infrastructures and communication networks. Nowadays, these infrastructures are increasingly more interconnected, and recent research has shown that these coupled networks are also more vulnerable against failures than uncoupled networks, see [2], [3], [4]. In practice we see that disruptions in communication systems can cause immediate disruption in the physical world, e.g. in transportation systems, automated teller systems and the control of power and water systems, see [5]. On the other hand, outages in power systems are known to cause failures often in other critical infrastructures as well, see [6].

In this paper we will consider an one-directional coupling between a communication network and a (high voltage) electricity network, meaning that nodes in the communication network are dependent on nodes in the electricity network but not vice versa. It has been shown in [6] that considering a one-directional dependency between energy and telecommunication infrastructure is more realistic than considering a bi-directional coupling between these two sectors. Based on European empirical data they have analyzed that critical infrastructure dependency on energy is substantially higher, as 60% of all cascades originate from the energy sector, and 22% of them had an effect on the telecommunication sector. While 28% percent of all cascades were originated from the telecommunication network, only 2% of them affected the energy sector. The reason is that most energy networks have their own local communication infrastructure (called SCADA) which is not connected to the main telecommunication infrastructure.

The research question we want to address is how to make such dependent systems more robust against the cascading failures in the electricity network originated from a random link failure, by reducing the degree of coupling i.e. by making some communication nodes autonomous from the electricity network. Note that random link failures in the electricity network can be caused e.g. by (unexpected consequences of) maintenance actions, bad weather and disruptions due to aging of the power grid [7]. The design of dependency links has also been addressed in [1] where the cascading failures are topology or connectivity based, i.e. introduced by two assumptions: a. when a node fails, its dependent node also fails; b. Within each component network, e.g. the power grid or the communication network, only nodes within the largest connected cluster of functional nodes can function. However, the dynamics of real electricity network are flow-based and cascading failures may occur even within a power grid due to the overflow of links. In this paper, we consider the more realistic *flow dynamics* on the electricity network, which is modeled by DC power flow equations and by involving parameters such as generators, demand values, link impedances and capacities.

Making nodes autonomous in this context means placing a local back-up energy power supply at the specific communication nodes. Of course, making too many nodes autonomous will involve a high amount of costs. Therefore the question is, given a small number of communication nodes that can be made autonomous, what is a good strategy for selecting this set of nodes to make the system more robust?

978-1-4799-7040-7

Using simulations, with a realistic electrical flow model based on DC power flow, which quantifies the voltage angles and flows in a electricity network, we want to determine the set of nodes which will increase the robustness of the system significantly. This involves protecting the communication network the best from the effect of various disturbances on a given electricity network. To quantify the effect on the electricity network, we consider, for each electricity node, the quantity of electricity demand which cannot be met as a result of the disruption such as a random link failure. If the total amount of energy supplied at a node in the electrical power grid is less than a certain fraction of the total demand at this node, all communication nodes depending on it are switched off. Within the communication network, failures of certain communication nodes may cause further failures due to nodes no longer being connected to the largest connected component (LCC).

Network modification strategies to optimize network robustness regarding to either network topology or network function have been widely studied aiming to determine where e.g. to add, remove or rewire links based on topological centrality metrics that describe properties of nodes [8], [9], [10], [11]. Degree[1] and betweenness[2] turned out to be good measures to determine the most vulnerable nodes whose removal has the most destructive effect in disconnecting a network [12], [13]. In this paper, we propose a set of network strategies based on not only topological properties but also functional features of nodes. Specifically, we consider centrality metrics, including both topological and functional features of nodes, that also take the coupling and the fundamental properties of the electrical flow into account. In [14] it is shown that the metric 'effective graph resistance' gives a good approximation of the actual robustness of the electricity network. However in this paper we try to find the centrality metric that best reflects the optimal selection of communication nodes to protect, i.e. the selection of nodes such that the total disruption effect on the communication is as small as possible when these nodes are made autonomous.

The rest of this paper is organized as follows: In Section II, the problem studied in this paper is described in more detail. In Section III the coupled network model used for the simulations is described. In Section IV various strategies for selection of the autonomous nodes are proposed and the results of these strategies are shown. In Section V the best selection strategies are applied to a real-word example, a coupled electricity-communication network in Italy. Finally, in Section VI conclusions are made, with suggestions for further research.

II. Problem Description

Our goal is to improve the robustness of the communication network, which depends on the electricity network, by removing a small number of dependency links. In particular, we want to ensure that the cascading failures originated from initial random link failure in the electricity network have the minimal effect on the communication network. Note that re-designing the coupled networks may lead to a high robustness, but often this is not feasible for existing infrastructures, especially on a short term. Instead, we aim to obtain a good strategy (in terms of robustness) for selecting autonomous nodes, i.e. nodes in the communication network that are made *independent* from the electricity network, for instance by installing a local back-up power supply at these nodes. Such a strategy should be a significant improvement over a random selection of autonomous nodes. Since making communication agents autonomous can be an expensive operation, we consider that only a small number of nodes can be made autonomous, i.e. the number of dependency links that can be removed is small. Compared to [1], a paper dealing with a similar research question, the cascading models we use also take flow dynamics into account, instead of only considering topological characteristics of the networks. Another difference with [1] is that we only consider one-directional dependency relations: the communication network is dependent on the electricity network, but not vice versa. This creates an interesting imbalance in the problem: we want to remove those interdependency links that connect communication nodes that are most essential for the connectivity in the communication network and the nodes in the electricity network that are most likely to fail in the flow-based cascading failures. A good balance between these two is needed to ensure a good selection strategy for the autonomous nodes.

III. Modelling the Coupled System

A. Electricity network

We have analyzed the data from the electrical test case IEEE 118 [15], consisting of 118 nodes and 186 links, see Fig. 1. The nodes are responsible for either generation, transmission or distribution of power. Electric power is shipped from the generation buses to distribution substations through the transmission buses, all interconnected by transmission lines. Electric power flows in a grid according to Kirchoff's laws. Accordingly, impedances, voltage levels at each individual power station, voltage phase differences between power stations and loads at terminal stations control the power flow in the grid. AC power flow equations are non-linear equations that approximate the flows of both active and reactive powers. DC load flow equations are a linearized version of the AC power flow equations considering only flow of active power [16]. Our focus is on (high voltage) transmission grids, for which DC power flow is a sufficient approximation to reality [16]. For the simulations we use a realistic model environment (MATCASC) [17] for modelling cascades of failures where impedances on each link , voltage levels at each individual power station, loads at terminal stations, together with capacity of the links, are taken as inputs.

In power grids, relays are applied to protect links from permanent damage due to extreme power flows. It is assumed in this paper that when a link is overloaded, i.e. the load on this link exceeds its capacity, the link will be temporarily

[1] The degree of a node is the number of connections or direct neighbors a node has in a network.

[2] The betweenness of a node is the total number of shortest paths between all possible nodes pairs that pass through this node.

closed down to avoid permanent damage. This can be caused by e. g. an overcurrent relay, notifying a circuit breaker to trip a link under excess current.

When a link (or group of links) fails, power is redistributed over the grid according to DC power flow. If this causes the power in a link to surpass its capacity, this link will also shut down, possibly causing more failures somewhere else in the network. This cascading effect is simulated in MATCASC, returning as output all the failed links, and for each node, the amount of electricity demand that has been satisfied. We assume node 1 in the IEEE 118 network to be the slack node; this node is used to balance the active and reactive power by emitting or absorbing power to and from the system. Apart from this specific node, there are other generators in the network (given by the IEEE 118 case file), however, these have a maximum amount of power they can generate. Due to the cascade of link failures, parts of the grid may get disconnected from the slack node. This need not mean they malfunction; however, the demand nodes on such separate islands can get no more than the generators contained within this island can deliver. If that is less than the total demand, the supplied electricity to each demand node in this island is assumed to be lowered proportionally.

In line with other recent studies [14], [18], [19], this paper assumes that the maximum capacity of a link (i.e., the flow limit) is given by a factor α, the tolerance parameter, times the initial load of the link. The results in this paper are presented for a fixed α=1.5, i.e. a loading level of 67%. We will see later in this paper that this value of α, combined with random link failures in the electricity grid, would lead to an average failure of 30% of the communication nodes, if none of the communication nodes were made autonomous from the electricity grid.

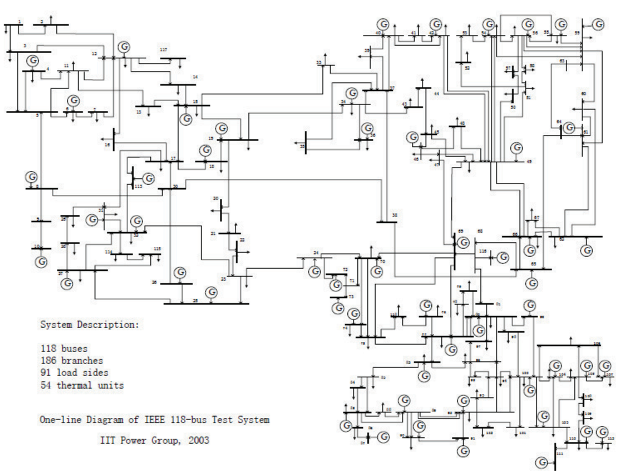

Fig. 1. IEEE 118 bus test system

B. Communication network

The communication networks are generated from network models, including both scale-free and Erdös-Rényi random networks, with the additional condition that the networks should be connected [20]. An Erdös-Rényi random graph of **n** nodes is generated by starting with **n** nodes and sequentially adding a link between two randomly selected but not yet connected nodes until the average degree reaches <**k**>. Erdös-Rényi networks follow a binomial degree distribution whereas scale-free networks possess a scale-free degree distribution $P(k) \sim k^{-\lambda}$. Real-life communication networks are often scale-free [21], but we also consider the Erdös-Rényi random graphs for comparison. For scale-free networks, there are also two parameters: **n**, the number of nodes, and **λ**, the power exponent. To generate a scale-free network, a degree sequence (describing the degree of each node) that follows the given scale-free distribution is firstly generated and afterwards, nodes are randomly linked according to their degrees.

We choose the size of the communication network, **n**, to be equal to the number of nodes in the electricity network with a positive energy demand, which is 99 in the case of the IEEE 118 network. We have generated 100 connected random networks of 99 nodes for the communication network, for different parameters of λ, namely λ=2.3, λ=2,5, λ=2,7, λ=3,0. For the Erdös-Rényi graphs we have chosen the average degree to be equal to the average degree over all λ's of the scale-free networks, which is equal to <**k**>=2.24.

A communication node fails if it is no longer connected to the LLC of functional nodes in the communication network, or when it does not get sufficient electricity (see Section II.C) from the corresponding electricity node.

C. Dependencies

In this paper we will consider a one-directional coupling between the communication network and the electricity network, which means that communication nodes are dependent on electricity nodes but not vice versa. For the coupling, we use similar assumptions as in [22]: Each communication node is dependent on one electricity node (only those with positive energy demand), no two communication nodes are dependent on the same electricity node, and a communication node fails whenever the fraction of demand served in the corresponding electricity node is less than a certain threshold. We set the threshold at 75%, as assumed in [22]. The initial one-to-one dependency links are assumed to be set up randomly.

D. Failures

As start of a cascade, we consider a random link failure in the electricity network. This represents for instance disruptions due to maintenance. This link failure may cause a cascade within the electricity network due to redistribution of power flow, which may cause other links to fail because of overflow. For all the electricity nodes that do not get more than 75% of their energy demand, the communication nodes depending on these nodes are switched off.

IV. RESULTS

In the following, we focus on a selection of 10 communication nodes (out of the 99 in total) that are to be made autonomous, which is similar as [1], where they have chosen to make 10% of the nodes autonomous.

A. Strategies to optimize the robustness

The main question is how to select the autonomous nodes in order to increase the robustness as much as possible, given the topological and flow dynamical properties of the network. Here the robustness is assessed as the average fraction of nodes in the LCC of functional nodes in the communication network after a random link failure in the electricity network. Actually, we have computed the effect for each of the 186 possible link failures and have averaged over those. The robustness is determined for 8 different strategies for the selection of autonomous nodes and for 5 types of communication networks.

Except for strategy 1, which is the reference scenario where there are no autonomous nodes, each of the strategies describes a method for selecting the autonomous nodes. Strategies are based on nodal properties of the communication network alone, of the electricity network alone or of both networks. In the electricity network we only consider the nodes with positive demand, since only those nodes are connected with communication nodes. Selection of a node means that the dependency link connecting that node will be removed, and hence the corresponding communication node will be made autonomous. All strategies are listed below:

1. The reference scenario, where no nodes are autonomous. All 99 communication nodes are connected with electricity nodes.
2. Nodes from the communication network or electricity network are chosen uniformly random.
3. Nodes with the highest degree in the communication network are chosen.
4. Nodes with the highest degree in the electricity network are chosen.
5. Nodes with the lowest degree in the electricity network are chosen.
6. Nodes with the highest probability to fail in the electricity network are chosen. The probability of a node to fail is based on simulations.
7. Dependency links with the highest measure H_{ij}, as defined in (1) below, are chosen. The metric H_{ij} is a linear combination of the degree of the communication node on one side and the probability that an electricity node fails on the other side. This strategy is a linear hybrid of strategy 3 and 6.
8. Dependency links with the highest measure B_{ij}, as defined in (2) below, are chosen. The metric B_{ij} is a non-linear combination of the degree of the communication node on one side and the probability that an electricity node fails on the other side. This strategy is a non-linear hybrid of strategy 3 and 6.

Some of the strategies only relate to the communication network (strategy 3), some only to the electricity network (strategy 4 - 6) and some are hybrid strategies which use information from both networks (strategy 7,8).

For strategy 6, we choose electricity nodes that are most likely to fail, i.e., those demand nodes with the highest probability that less than 75% of their energy demands are satisfied after an initial random link failure (and the following cascades). As mentioned in Section II, we suspect it is important to involve these nodes in the final decision. We compute these probabilities via simulations: we run MATCASC for the IEEE 118 electricity network (here not coupled to a communication network), and for each possible initial link failure we keep track of the nodes that had insufficient energy. We compute a probability of each node to fail over all the realizations of the initial link failure and the corresponding cascades. The complement of these probabilities, i.e. the probabilities to survive after an initial link failure and the corresponding cascades, is depicted in Fig. 2.

For strategy 7 the dependency links to be removed are chosen based on the following linear combination:

$$H_{ij} = (1 - \gamma) * P_j + \gamma * d_i/d_{max} , \qquad (1)$$

where γ is a parameter we can tune between 0 and 1, P_j is the fraction of times that node *j* fails in the electricity network, d_i is the degree of node *i* in the communication network, d_{max} is maximum degree in the communication network. We choose γ within [0,1] and the normalization by d_{max} so that the metric H_{ij} of a dependency link (i,j) ranges within $0 \leq H_{ij} \leq 1$. For our simulations, we vary γ between 0 and 1 (with steps of 0.1), and select the γ that gives the best robustness (per communication topology type).

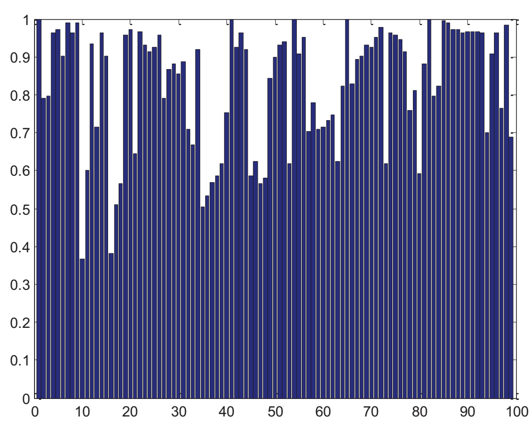

Fig. 2. Probability of each demand node NOT to fail

For strategy 8 we use the following non-linear combination of P_j and d_i to select the dependency links:

$$B_{ij} = (d_i/d_{max})^{\beta} * P_j , \qquad (2)$$

where $\beta > 0$. Again we vary in our simulations β from 0 with step size of 0.1, and choose for each communication topology type the β that leads to the best robustness.

In Table 1 we illustrate the outcome of these strategies on the robustness, which is the average over all 186 possible initial single link failures in the electricity network, and over the 100 randomly generated communication networks (for each topology type). Apart from the sample means, we also computed the two-sided 95% confidence intervals, all having lengths between 0.002 and 0.004, rounded to three decimals.

TABLE I. ROBUSTNESS FOR DIFFERENT STRATEGIES AND TOPOLOGIES

Strategy	Robustness per topology type				
	Scale free, λ=2.3	*Scale free, λ=2.5*	*Scale free, λ=2.7*	*Scale free, λ=3.0*	*Erdös-Rényi, k=2.24*
1.	0.709	0.696	0.705	0.693	0.736
2.	0.732	0.722	0.725	0.714	0.765
3.	0.816	0.823	0.828	0.836	0.794
4.	0.716	0.703	0.712	0.700	0.744
5.	0.744	0.731	0.738	0.733	0.774
6.	0.773	0.767	0.776	0.764	0.817
7.	0.836	0.840	0.846	0.857	0.834
8.	0.842	0.847	0.850	0.860	0.835

B. *Comparison of strategies*

Based on Table 1, we can make some interesting observations:

- All strategies improve the average robustness compared to the reference scenario: choosing nodes uniformly at random only improved robustness with 2% while strategy 8 is able to improve the robustness by more than 24%, for some type of communication networks.
- Choosing the highest degree nodes within the communication network (strategy 3) or the nodes with the highest probability to fail within the electricity network (strategy 6), improves the robustness significantly better than choosing nodes uniformly at random (strategy 2).
- Interestingly, choosing nodes with the highest degree in the electricity network (strategy 4) actually performs *worse* compared to choosing nodes randomly (strategy 2). The reason is that, as shown in Fig. 3, nodes with a high degree in the electricity network have a low chance to fail or a high probability to survive. Choosing nodes with the lowest degree in the electricity network (strategy 5) indeed performs better than choosing nodes randomly, but still, not as good as choosing the nodes with the highest probability to fail (strategy 6). The most relevant feature in the electricity network turns out to be the probability to fail.
- Strategy 3 (choosing the communication nodes with the highest degree) and 6 (choosing the electricity nodes with the highest probability to fail) perform differently depending on the topology of the communication network. For scale-free networks, strategy 3 performs better than 6, while for the Erdös-Rényi topologies, strategy 6 performs better. This can be explained by the fact that when the communication network is scale-free, the high degree nodes, so called hubs, are essential for the connectivity of the network, for the robustness. In this case, protecting high degree communication nodes is effective. When the communication network is an Erdös-Rényi random graph, the contribution of each communication node to the connectivity does not differ much. In this case, selecting the electricity nodes with the highest probability to fail is efficient, since it reduces effectively the number of communication nodes that are likely endangered by the dependent electricity nodes.
- We have found that hybrid strategies (7 and 8), i.e. using a combination of node properties from both the electricity network and the communication network, outperform any strategy (2-6) that considers node features from only one of the two networks. Our advice is to use strategy 8 in this case.

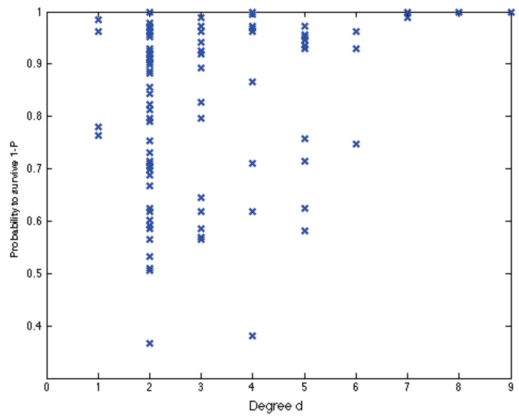

Fig. 3. Scatter plot of the probability to survive versus the degree of a node in the electricity network

V. Real world example

A real-world example of cascading failures between different critical infrastructure networks is the electrical blackout in Italy on September 28, 2003, that affected most of Italy [23], and also had a cascading effect on the communication network. To demonstrate the effectiveness of our hybrid strategy 8, we will apply it to this real coupled network data in Italy [22]. This data consists of topology and electrical properties of the Italian high-voltage (380 kV) electrical transmission grid, consisting of 310 nodes and 361 links, and the Italian high-bandwidth backbone of the internet network dedicated to linking universities and research institutes (GARR), consisting of 39 nodes and 58 links.

Similar to [22] we have chosen to connect each node of the Internet network to the closest demand node in the electricity network. This causes an Internet node to be coupled to only one electricity node, while an electricity node may be connected to more than one Internet node.

Again we simulate the cascading effects of random link failures in the electricity network on the functioning of the communication network, using the same approach as for the IEEE test case. It turns out that here a choice of $\alpha = 1.5$ (load level is 67%) in the setting of random link failures leads to very few failures in the electricity network, so we choose here for a lower α (1.3). This corresponds to a load level of 77%, which is closer to the loads that caused the cascade in the 2003 blackout [23].

Applying our MATCASC simulations on this real-world example, we see that on average 57% of the 39 communication nodes survive a random link failure in the electricity network. Now, again we want to protect 10% (=4) of these nodes by making them autonomous from the electricity network. Applying our best hybrid strategy 8 ensures that on average 71% of the 39 nodes survive, which is higher than the random selection strategy that leads to a survival of on average 61% of the nodes.

VI. Conclusions and Future work

In this work, we address the challenging question: how to design dependent networks, when the real flow dynamics of the electricity network are taken into account? The flow-based cascading failures in a power grid are fundamentally different from those, as in previous interdependent network studies, based on network connectivity. Simply, but possibly even more realistically, we consider one-directional dependency, where the communication network depends on the electricity network but not the other way round. We investigate, specifically, given the dependent network structure, which dependency links should be removed, or equivalently which communication nodes should be made autonomous, in order to optimize the robustness of the communication network. Using synthetic dependency networks, where the communication network is generated from classic network models and is dependent on the IEEE 118 bus test system, we test the 7 strategies that we proposed. We find that the degree of the communication nodes and the failure probability of the electricity nodes, play an important role in determining the dependency links which are to be removed. Hybrid strategies, combining both features, lead to even better robustness. One of the hybrid strategies has also been tested in the real interdependent communication and electricity network in Italy.

Our findings inspire more interesting questions. The two proposed hybrid strategies, one linear, the other non-linear, are both controled by a weighting factor. How is the optimal weighting factor related to the interdependent network structure? What is the difference in performance between the previously proposed strategy based on topology and our strategies based on flow dynamics? The failure probability of a node in the electricity network turns out to be crucial, but these probabilities are determined through simulation. Is it possible to estimate the failure probability of a node by topological properties of this node in the electricity network? The issues mentioned above all require tests on a large number of large dependent networks so that the results are statistically conclusive. Most importantly, our work on one directional dependent networks lays a solid foundation for the further understanding of interdependent flow-based networks beyond communication and electricity networks.

Acknowledgments

We wish to thank Vittorio Rosato and Gregorio D'Agostino for providing us the interdependent network dataset of Italy and the European Commission within the framework of the CONGAS project FP7-ICT-2011-8-317672.

References

[1] N. Yazdani, C. M. Schneider, N. A. Araújo, S. Havlin and H. J. Herrmann, "Towards designing robust coupled networks," Sci. Rep., vol. 3, no. 1969, pp. 1-7, 2013.

[2] S. V. Buldyrev, R. Parshani, H. E. Stanley and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, pp. 1025-1028, 2010.

[3] J. Gao, S. V. Buldyrev, H. E. Stanley and S. Havlin, "Networks formed

from interdependent networks," Nature physics, vol. 8, no. 1, pp. 40-48, 2012.

[4] C. D. Brummit., R. M. D'Souze and E. A. Leicht, "Surpressing cascades of load in interdependent networks," Proc. Nat. Acad. of Sciences, vol. 109, no. 12, pp. E680-E689, 2012.

[5] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," Reliability engineering & System safety , vol. 121, pp. 43-60, 2014.

[6] E. Luijff, A. Nieuwenhuijs, M. Klaver, M. van Eeten and E. Cruz, "Empirical findings on critical infrastructure dependencies in Europe," in Critical Information Infrastructure Security, Berlin, Springer Berlin Heidelberg, 2009, pp. 302-310.

[7] P. Hines, K. Balasubramaniam and E. Sanchez, "Cascading failures in power grids," IEEE Potentials, vol. 28, pp. 24-30, 2009.

[8] G. Paul, S. Sreenivasan, S. Havlin and H. Stanley, "Optimization of network robustness to random breakdowns," Physica A, vol. 85, p. 370, 2006.

[9] H. Wang and P. V. Mieghem, "Algebraic connectivity optimization via link addition," BIONETICS, no. November 25-28, Hyogo, Japan, 2008.

[10] P. V. Mieghem, D. Stevanovic, F. A. Kuipers, C. Li, R. v. d. Bovenkamp, D. Liu and H. Wang, "Decreasing the spectral radius of a graph by link removals," Physical Review E, vol. 84, no. 1, p. 016101, 2011.

[11] H. Wang, Q. Li, G. D'Agostino, S. Havlin, H. Stanley and P. V. Mieghem, "Effect of the interconnected network structure on the epidemic threshold," Physical Review E, vol. 88, no. 2, p. 022801, 2013.

[12] S. Trajanovski, J. Martin-Hernandez, W. Winterbach and P. V. Mieghem, "Robustness envelopes of networks," Journal of Complex Networks, vol. 1, pp. 44-62, 2013.

[13] H. Wang, J. M. Hernandez and P. V. Mieghem, "Betweenness centrality in a weighted network," Physical Review E, vol. 77, no. 4, p. 046105, 2008.

[14] Y. Koç, M. Warnier, P. van Mieghem, R. E. Kooij and F. M. Brazier, "The impact of the topology on cascading failures in a power grid model," Physica A: Statistical mechanics and its applications, vol. 402, pp. 169-179, 2014.

[15] " http://www.ee.washington.edu/research/pstca/," [Online].

[16] D. V. Hertem, J. Verboomen, K. Purchala, R. Belmans and W. Kling, "Usefulness of DC power flow for active power flow analysis with flow controlling devices," Proc. of the 8th IEEE Int. Conf. on AC and DC Power Transmission, pp. 58-62, 2006.

[17] Y. Koç, T. Verma, N. A. Araujo and M. Warnier, "MATCASC: A tool to analyse cascading line outages in power grids.," in Intelligent Energy Systems (IWIES), 2013 IEEE International Workshop on, 2013.

[18] P. Crucitti, V. Latora and M. Marchiori, "Model for cascading failures in complex networks," Physical Review E, vol. 69, p. 045104, 2004.

[19] G. Chen, Z. Y. Dong, D. J. Hill and G. H. Zhang, "An improved model for structural vulnerability analysis of power networks," Physica A: Statistical Mechanics, vol. 388, no. 19, pp. 4259-4266, 2009.

[20] P. V. Mieghem, "Performance analysis of complex networks and systems," Cambridge University Press, ISBN: 9781107058606, 2014.

[21] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," Science, vol. 286, pp. 509-512, 1999.

[22] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis and R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," International Journal of Critical Infrastructures, vol. 4, no. 1, pp. 63-79, 2008.

[23] UCTE, "Final report of the investigation committee on the 28 September blackout in Italy," 2004.