Resilience of Interdependent Communication and Power Distribution Networks against Cascading Failures

Wei Koong Chai, Vaios Kyritsis, Konstantinos V. Katsaros, George Pavlou
Department of Electronic and Electrical Engineering
University College London
London, WC1E 6BT, United Kingdom
Email: {w.chai, vaios.kyritsis.13, k.katsaros, g.pavlou}@ucl.ac.uk

***Abstract*—The operations of many modern cyber-physical systems, such as *smart grids*, are based on increasingly interdependent networks. The impact of cascading failures on such networks has recently received significant attention due to the corresponding effect of these failures on the society. In this paper, we conduct an empirical study on the robustness of interdependent systems formed by the coupling of power grids and communication networks by putting real distribution power grids to the test. We focus on the assessment of the robustness of a large set of medium-voltage (MV) distribution grids, currently operating live in the Netherlands, against cascading failures initiated by different types of faults / attacks. We consider both unintentional random failures and malicious targeted attacks which gradually degrade the capability of the entire system and we evaluate their respective consequences. Our study shows that current MV grids are highly vulnerable to such cascades of failures. Furthermore, we discover that a small-world communication network structure lends itself to the robustness of the interdependent system. Also interestingly enough, we discover that the formation of hub hierarchies, which is known to enhance independent network robustness, actually has detrimental effects against cascading failures. Based on real MV grid topologies, our study yields realistic insights which can be employed as a set of practical guidelines for distribution system operators (DSOs) to design effective grid protection schemes.**

I. Introduction

Our modern society is increasingly reliant on networks for various aspects of life, ranging from basic needs (*e.g.*, energy supplies) to those contributing to better standard of living (*e.g.*, transportation, information systems). The integration of these increasingly intelligent and critical infrastructure networks, in turn, has also made the various originally separate networks dependent on each other (*e.g.*, a cyber-network overlaying a physical-network). While the strong coupling of networks enhances their functionalities, it also significantly increases the vulnerability of the system as a whole [1], [2]. This is because failures in one network may cascade to the other and vice versa, resulting in an iterative failure process. Hence, robustness of such interdependent network systems (sometimes known as network of networks (NoN)) has recently received much attention (see for example [3]).

In this paper, we focus our study on the resilience of interdependent networks consisting of an electric power grid and a communication network against such cascading failures since the energy and telecommunication sectors are found to be the main sectors initiating such cascade of failures [4], [5]. The symbiotic relationship between the two networks is a result of the grid requiring the service from the communication network for monitoring, control and management operations, while the communication network depends on the grid for electricity supply. A real-world example demonstrating such interdependency and the corresponding vulnerability is the national blackout in Italy in September 2003 [1]. This interdependency is expected to increase with the advent of smart grids introducing bi-directional communication patterns among multiple entities.

Our work focuses on the medium-voltage (MV) distribution grid domain, which is recently undergoing transformative changes due to the advent of smart grid applications, but have yet to receive the same level of attention as its high-voltage (HV) counterpart (*e.g.*, as highlighted in [6], [7]). The introduction of multiple dynamic active components, *e.g.*, distributed (renewable) energy resources (DERs) such as solar/wind farms and electric vehicles (EVs), at the distribution level poses new significant challenges to the system stability especially on protection and reliability of the grid. The traditional assumptions of distribution networks being mostly passive and static no longer apply as they evolve towards the so-called Active Distribution Networks (ADNs)[1] where increased fine-grained observability of the grid power conditions, faster response and enhanced protection are needed to manage the increased volatility of the system in a timely fashion. The operation and, more importantly, the protection of distribution grids are thus increasingly reliant on a robust and efficient communication infrastructure that must provide seamless and timely communication service, such that full observability of power conditions is maintained at all times [8]. In fact, to cater for the challenges of next generation smart grids, there are already work in the literature to apply the latest information-centric networking paradigm for smart grid applications (*e.g.*, [9], [10], [11]).

However, the communication network landscape in the MV domain is far from clear [12]. The distribution grid (i.e., the MV domain) covers smaller geographical areas compared to HV grids, as well as areas of different nature *i.e.*, rural

[1]ADNs are distribution networks that have systems in place to control a combination of DERs (*e.g.*, generators, loads and storage). DSOs have the possibility of managing electricity flows via a flexible network topology. DERs take some responsibility for system support, depending on a suitable regulatory environment and connection agreement.

but also denser (sub-)urban areas. As a result, the adoption of technologies employed in the HV domain to our case is not straightforward, mainly due to the associated deployment costs [12]. Furthermore, distribution system operators (DSOs) have multiple options for the communication network, such as engaging the service of public Internet service provider(s) (ISPs), deploying their own private communication infrastructure (*e.g.*, investing in fibre optic and/or exploiting existing powerline communication (PLC) technologies, such as that proposed in [12]) or adopting a hybrid solution, using both the private and public options above. In view of this still evolving communication environment, we employ widely used network topology models with different characteristics, as the communication network component of the interdependent system, to gain insights on the robustness of the overall NoN.

Our work aims to close the gap in the study on the vulnerability of interdependent systems against cascading failures, which hitherto mainly focused on purely theoretical analysis (cf. Section II for model descriptions). For instance, focusing on a special case where the system consists of two totally identical networks dependent on each other, the authors in [13] studied the system using algebraic connectivity of an interdependent system as the robustness indicator. In [1], the robustness of the interdependent network system is studied assuming totally uncorrelated networks using percolation theory. Since it is known that such uncorrelated networks do not exist in the real world and almost always the interdependent networks do not share common topologies, we put real distribution grids to the test *i.e.*, we use a large set of real MV grid networks currently operating live in the Netherlands by a major Dutch DSO, engaging thus in an extensive empirical study (cf. Section III) to quantitatively gain insights into the system behaviour. Furthermore, we focus our study on the MV domain which is increasingly becoming more dynamic and thus, more prone to such cascading failures. While the communication network landscape in the MV domain is still shaping, our findings provide practical guidelines on the desirable topological characteristics that can enhance system robustness when designing / deploying the communication infrastructure over the distribution grid. Moreover, our study broadens the set of failure types encountered in the considered NoN. Namely, Hines *et al.* reported that the majority of cascading failures in power grids are results of natural disasters, but also highlighted the recent increase of cyber-attacks initiating blackouts via hacking of the communication network [14]. Our study covers a spectrum of different failure types, ranging from unintentional faults to malicious attacks, each characterized by specific node removal pattern (cf. Sections III-C1 and III-C2). Additionally, instead of considering one single failure that initiates a cascade of failures, we consider a more general context where multiple cascading failures occur. We discuss our observations and insights, providing a better understanding of the system behavior under failures and thus, facilitating the design of effective protection schemes against different types of cascading failures (cf. Section IV). We summarize and conclude our findings in Section V.

II. Cascading Failures in Interdependent Systems

We consider an interdependent system with two undirected graphs, $G^{sg} = (V^{sg}, E^{sg})$ and $G^{com} = (V^{com}, E^{com})$, representing the (smart) power grid and communication network respectively. Let N^{net} be the network size where $net \in \{sg, com\}$. Then, $V^{net} = v_1^{net}, \ldots, v_{N^{net}}^{net}$ and $E^{net} = e_1^{net}, \ldots, e_{M^{net}}^{net}$, where M^{net} is the number of edges / links in the corresponding network. Further, let A^{net} denote the $N^{net} \times N^{net}$ adjacency matrix with the elements, $A_{i,j}^{net} = 1$ if there exists a link between nodes i and j and 0 otherwise. The interdependency of the two graphs is represented by an $N^{sg} \times N^{com}$ matrix A^{dep} with $A_{v_i^{sg}, v_j^{com}}^{dep} = 1$ if there exists a link between v_i^{sg} and v_j^{com} and 0 otherwise.

A. Interdependent System Model

For this work, without loss of generality, we establish the baseline interdependent system as follows:

- Both networks are equal in size, $N^{sg} = N^{com} = N$, but they do not necessarily possess the same topologies (as opposed to [13] where $A^{sg} = A^{com}$ is assumed).
- There is 1-to-1 dependency between nodes in G^{sg} and G^{com} (*i.e.*, there are N interdependency links in the system). This can correspond to cases where each S-SS is equipped with a communication network node for the support of monitoring and control applications, *e.g.*, [8].
- The dependency is bi-directional (*i.e.*, mutually dependent). A node failure in G^{sg} will result in the failure of the corresponding dependent node in G^{com} and vice versa.
- Drawing on the observations of real-world interdependent systems reported in [15], we follow the *positive* degree correlation method and create dependency between nodes with similar level of degrees (*i.e.*, nodes with high degree (nodes having many immediate neighbors) in one network are coupled with nodes having high degrees in the other network and vice versa [16])[2].

Real-world interdependent systems may not always have such "balanced" interdependencies. Nevertheless, it is straightforward to accommodate unbalanced cases such as n-to-m node inter-network connections and non-symmetric dependencies (*e.g.*, in [17]) in our methodology (cf. Section III). In this case, we note system robustness may be enhanced with higher number of interdependency links (*i.e.*, a node may only fail when all of its counterpart nodes in the other network fails). However, as studied in [18], the cost to achieve the added robustness must be carefully considered.

B. Cascading Failure Model

In this work, we follow the cascading failure model described in [1] which has since been widely used in the literature as the basis of several studies (*e.g.*, [2], [19], [20], [21]). In this model, a cascading failure begins with the failure (*i.e.*,

[2]We have also experimented with *random* and *negative* degree correlations for creating interdependency between the two networks but insignificant divergences are observed.

[3]We leave out specific practical details of power grid in the example such as the switching of P-SS for power source or possibility of islanding operations.

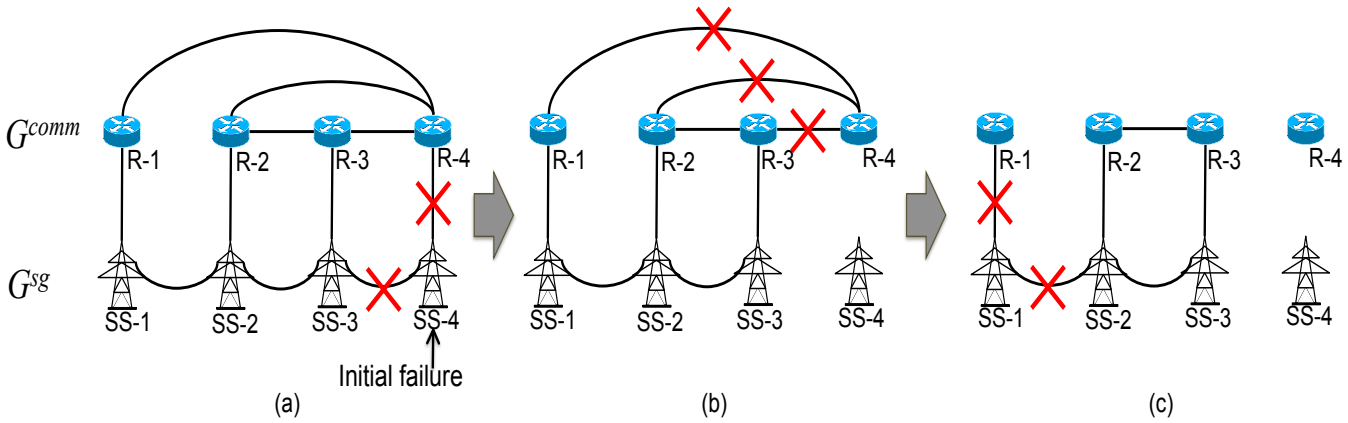

Fig. 1: (Color Online) An illustration of a cascading failure suffered by an interdependent system of size $N^{sg} = N^{com} = N = 4$ triggered by a failure at node SS-4[3].

removal) of a fraction, $1 - p$ of nodes from network **A**. All the links connecting to these failed nodes in network **A** will thus be down. Further, the nodes in network **B** depending on these nodes will also fail. Any link connected to these failed nodes in network **B** will also be removed. This process may fragment both networks and form different network components since the two networks are differently connected. The nodes belonging to the largest mutually connected component (*i.e.*, the giant component) retain their functionality while the smaller components fail.

Figure 1 illustrates a simple example of a cascading failure triggered by the failure of one node (*i.e.*, $N(1-p) = 1$) in an interdependent system consisting of $N = 4$ nodes in each network. The initial failure occurs at node SS-4 in G^{sg} causing its removal along with the link to node SS-3 and the interdependent link to node R-4 in G^{com}. The loss of the interdependent link causes the failure of node R-4 and of all the links connected to it. This causes G^{com} to fragment whereby only the giant component retains its functionality i.e., nodes R-2, R-3 and the link connecting them. The fragmented smaller clusters fail. This cascades back to G^{sg} causing the failure of node SS-1 and of all links connected to it.

III. Methodology

A. Network Models

In practice, the complete knowledge of how the separate networks are dependent on each other may not always be possible since multiple stakeholders are often involved. In our case, when DSOs rely on communication infrastructure providers, the exact communication network information (*e.g.*, the network topology) is confidential[4]. In our study, we create the interdependent systems using real data for G^{sg}. However, as the communication network environment in the MV domain still evolves, we resort to widely accepted theoretical graph models for G^{com}. Within this context, our objective is to investigate the key structural properties that improve the resilience of the considered interdependent networks, deriving practical guidelines for the design of communication networks for the MV domain.

Smart grid network, $\mathbf{G^{sg}}$ – we use real data extracted from 16 MV distribution grids, covering an area of approximately $350km^2$ in central eastern Netherlands. They include a total of 16 primary sub-stations (P-SSes) and 1,857 secondary sub-stations (S-SSes). The grid topologies resemble that of tree structures rooted at P-SS(es), which perform(s) the high-to-medium voltage transformation. Each tree branch emanating from the P-SS corresponds to a distinct feeder. Table I shows the basic topological characteristics of these grids[5] and Fig. 2 shows the aggregated degree distribution of all the sub-stations (SSes) across the entire set of MV grids. Almost 90% of SSes have low number of neighbors (*i.e.*, degree of one or two) while approximately 20% of SSes are leaf nodes (*i.e.*, nodes connected to only one other node).

Communication network, $\mathbf{G^{com}}$ – we use three main theoretical graph models widely used in the literature to study network robustness (*e.g.*, [22]) to gain insights into the graph properties that would deter/promote cascading failures.

- Erdős-Rényi (ER) model – Given N, a link randomly connects a pair of nodes with probability p_r independent of all other links. In our experiments, we use $p_r = \frac{lnN}{N}$ which is the sharp threshold of connectedness to ensure connected graphs while at the same time sufficiently small to avoid a highly meshed topology [23]. ER graphs are characterized by a short average path length and low clustering coefficient, since a consequence of pure random edge allocation is that the degree distribution converges to a Poisson distribution. The simplicity of the model has lent itself to many theoretical studies on network resilience (*e.g.*, [1]). In our case, the ER model can be considered as an "unplanned" network layer that is resulted from gradual ad hoc deployment of network nodes to incrementally support the new requirements from the grid over time.
- Small world (SW) model – We construct SW graphs following the Watts and Strogatz model [24], with

[4]This non-disclosure is mutual as DSOs also do not offer information regarding their own power grid.

[5]We "anonymize" the grids by removing location/power related information.

rewiring probability, $\gamma = 0.1$ and mean degree, $\bar{k} = 0.05 \times N$. A low γ value is used to avoid creating SW graphs that closely resemble ER graphs since when $\gamma = 1$, the resultant graph's average path length converges to that of a random graph (*i.e.*, $ln(N)/ln(\bar{k})$). In addition, when $\gamma << 1$, SW graphs also form local clusters (*i.e.*, having high clustering coefficient) as opposed to graphs such as lattices which exhibit the opposite characteristic ("big world" graphs). Moreover, since our work focuses on MV grids which usually do not span over large spatial proximity, there is high probability that the corresponding G^{com} will exhibit SW properties.

- Scale-free (SF) model – In our study, SF graphs are constructed based on the Barabási-Albert (BA) model [25], using a 3-node seed graph. In this model, each new node is connected to an existing node with a probability proportional to the existing nodes' degree (*i.e.*, the more neighbors a node has, the more likely it attracts a new node to attach to it). Owing to this preferential attachment process, SF graphs result in power law degree distribution. This property has been observed in many real-world networks (*e.g.*, [26]) which results in the forming of hubs within the graph. Since there is no prevailing communication network design for the support of smart grid applications in the MV domain, we also investigate the effect of the interdependent system when coupled with SF graph topologies.

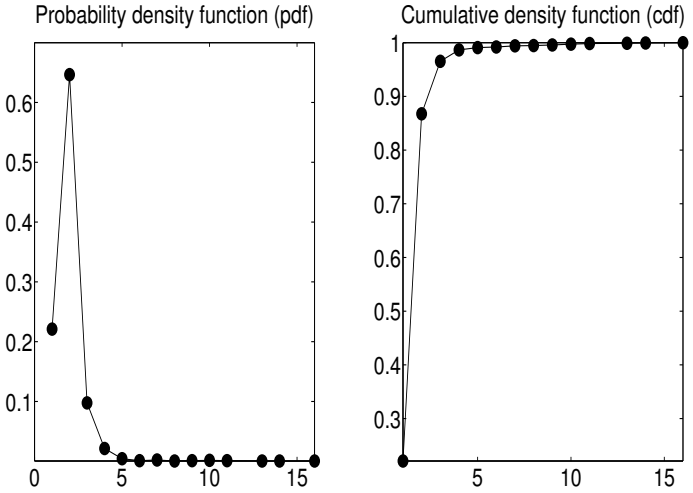

Fig. 2: Aggregated degree distribution of sub-stations in the dataset showing majority of sub-stations have low connectivity.

B. Metrics

To evaluate the impact of cascading failures, we follow the literature to use the size of the giant component which measures the level of connectivity of a network as an evaluation metric (*e.g.*, [1], [2], [16]). In practice, the functional component also depends on the actual power source (*i.e.*, P-SS), the re-configurability of the grid (*e.g.*, locations of breakers)

[6]Link density = $\frac{M^{net}}{N^{net}(N^{net}-1)/2}$.

TABLE I: Properties of real MV grid topologies of a large European DNO.[6]

Grid	N^{sg}	M^{sg}	Mean degree	Clustering coefficient	Link density	Mean path length
Area 1	126	126	2.000	0.0039	0.0160	8.3194
Area 2	83	82	1.9759	0.0000	0.0241	6.5601
Area 3	191	192	2.0105	0.0035	0.0106	9.6177
Area 4	23	22	1.9130	0.0000	0.0870	5.5652
Area 5	178	177	1.9888	0.0000	0.0112	10.0176
Area 6	29	28	1.9310	0.0000	0.0690	8.0296
Area 7	51	51	2.0000	0.0000	0.0400	7.1529
Area 8	102	101	1.9804	0.0000	0.0196	9.3345
Area 9	99	98	1.9798	0.0000	0.0202	8.4684
Area 10	209	210	2.0096	0.0000	0.0097	11.6043
Area 11	47	47	2.0000	0.0156	0.0435	8.1082
Area 12	294	298	2.0272	0.0024	0.0069	11.8471
Area 13	85	84	1.9765	0.0000	0.0235	8.1815
Area 14	42	41	1.9524	0.0000	0.0476	4.7433
Area 15	146	147	2.0137	0.0000	0.0139	9.7879
Area 16	168	169	2.0119	0.0000	0.0120	10.5974

as well as the ability to perform islanding operations. In this sense, the nodes in the system are not homogeneous and have different resiliency in reality. For instance, nodes located near breakers may be more easily switched to another power source and thus, in certain cases, becoming less vulnerable. Due to the fact that these specific cases are dependent on the distinct operations of the network, we take a topological approach to draw more general insights that should be applicable to different interdependent systems.

In addition, to understand how the communication functionality degrades, we measure the communication efficiency of the G^{com}, η following [27]:

$$\eta = \frac{\sum_{1 \le i < j \le N} 1/\sigma_{i,j}}{\binom{N}{2}} \quad (1)$$

where $\sigma_{i,j}$ is the shortest path length (in hopcount) between node i and j. It measures how fast information spreads in a network. A fully mesh network has $\eta = 1$ since all nodes are reachable in one hop (*i.e.*, all node pairs have 1-hop distance). This metric is especially relevant to time-critical smart grid applications such as synchrophasor-based monitoring where the measurements taken at geographically distributed locations are synchronized and must reach the phasor data concentrators (PDCs) within very stringent time window [8], [12].

C. Failure Models

Our investigation of the considered NoN's resilience properties is based on a sequential process where we remove one node after another, with each removal triggering a cascading failure each time. This results in a series of cascading failures. Throughout this process, we track the gradual degradation of the system functionalities in terms of both the above-mentioned metrics. The order in which nodes are removed from the system depends on the failure type. In the following, we describe the different types of failures considered in this work.

1) Unintentional Random Failures: Unintentional failures include those caused by equipment failures, natural disasters (*e.g.*, earthquake, tsunami, *etc.*) or simply accidental human errors (*e.g.*, misconfigurations). For such failures, the sites where they take place are usually non-determinable or forecasted. Such failures are modeled via random node removals. We use random point (RP) node removals for failures caused by equipment failures or human errors and random area (RA) node removals for failures caused by natural disasters that usually spread in a specific geographical area. Namely,

- Random Point (RP) failure – Given $1-p$, $N(1-p)$ nodes are randomly selected for removal.
- Random Area (RA) failure – Given $1-p$, start by removing a random node in the graph and then proceed to remove a random neighbor of the removed node that has survived the resulting cascading failure due to the removal of the initial node. Repeat the process of removing random neighbors of removed nodes until $N(1-p)$ nodes have been removed.

2) Malicious Targeted Attacks: Malicious attacks aim to maximize damage to the interdependent system by targetting parts of the system believed to be vulnerable. Such attacks may come in physical form, via equipment tampering or electronically via intentional misconfigurations or spreading of computer viruses. To conduct such an attack, the perpetrator must possess some prior intelligence regarding the targeted system such as knowledge on the topologies and their interdependencies. Logically, with the intention to cause maximum damage, the attacker will attack nodes deemed to be most important to the system operation. We assume that the attacker ranks the nodes based on their importance in descending order and attacks the system in that order.

To compute this ranking, we consider four centrality measures, widely used when studying network robustness [28], [29]:

- Node degree (DC) – relates node importance with the number of immediate neighbors *i.e.*, local connectivity.
- Betweenness (BC) – measures the involvement of a node in the set of shortest paths of all node pairs in the network
- Closeness (CC) – measures the distance of a node to all other nodes in a connected network
- Eigenvector (EC) – relates node importance to the importance of its neighbors

Each centrality measure above deduce importance of nodes based on different factor: DC – connectivity, BC – path, CC – distance and EC – spectral structure of the topology. In [29], an in-depth comparative assessment of these centrality measures in the context of communication networks is conducted.

We extend the centrality concepts to account for the added importance of each node with regards to its counterpart in the other network. Specifically, for each node, v, we compute the mean value of the normalized node centrality within its own network and those node(s) in the other network that have a connection to it. Table II shows the original centrality definitions and Eq. 2 gives the extended definitions.

TABLE II: Centrality indices used for targeted attacks.

Centrality Index	Definition
Degree (DC)	$c^{DC}(v) = \frac{deg(v)}{N^\alpha - 1}$
Betweenness (BC)	$c^{BC}(v) = \frac{2}{(N^\alpha-1)(N^\alpha-2)} \sum_{i\neq v\neq j \in V^\alpha} \frac{\sigma_{i,j}(v)}{\sigma_{i,j}}$
Closeness (CC)	$c^{CC}(v) = \frac{N^\alpha - 1}{\sum_{j\in V^\alpha, i\neq j} \sigma_{i,j}}$
Eigenvector (EC)	$c^{EC}(v) = \frac{1}{\lambda} \sum_{j\in V^\alpha} A^\alpha_{v,j} \times c^{EC}(j)$
N: graph size, α, β: indicates which network (either *sg* or *com*), $deg(v)$: number of neighbors of node v within its own network, λ: eigenvalue, $\sigma_{i,j}$: shortest path length from i to j, $\sigma_{i,j}(v)$: shortest path length via v	

For each centrality index, $x \in \{DC, BC, CC, EC\}$, we extend them to the coupled network system as follows:

$$c^x_{ext}(v) = \frac{c^x(v) + \sum_{j\in V^\beta} A^{dep}_{v,j} \times c^x(j)}{1 + \sum_{j\in V^\beta} A^{dep}_{v,j}}. \quad (2)$$

The above equation assumes the importance of a node is proportionally increased based on the (total) importance of the node(s) depending on it (*i.e.*, additive effect). Note that Eq. 2 is universally applicable to unbalanced interdependent systems (cf. as discussed in Section II-A).

IV. Vulnerability Analysis

We conducted an extensive simulation study across 16 real MV grids coupled with three types of communication network models (*i.e.*, $\{ER, SW, SF\}$) against six types of failure trigger patterns (*i.e.*, $\{RA, RP, DC, BC, CC, EC\}$) (cf. Section III). For each simulation setup, we obtained 95% confidence intervals for all metrics. For each repeat simulation run, we regenerated a new G^{com} since reusing the same one results in exact same node ranking for targeted attacks. Due to the large number of possible scenarios, we present selected but representative results and discuss our observations and findings.

A. Impact of Random Cascading Failures

We first show in Fig. 3 representative results of MV grid coupling with different G^{com} models. From all sets of results, we observe that MV grids coupled with SF networks are the least robust against both types of random cascading failures ($SF \prec ER \prec SW$[7]) with the size of the giant component rapidly decreasing. This corroborates with [1] where interdependent SF graphs with different power-law degree distributions are found to be more vulnerable to interdependent ER graphs. For the RA case, the degradation of the system is close for MV grids dependent on ER and SW networks. The distinction becomes less clear for small distribution grids (see insets in Fig. 3). The observed order of robustness, $SF \prec ER \prec SW$, is also observed in [22]

[7]To simplify discussion, we use $X \prec Y$ ($X \succ Y$) to indicate that X is less (more) robust against cascading failures than Y within the considered setup.

which considers failures in single layer network models with no interdependency.

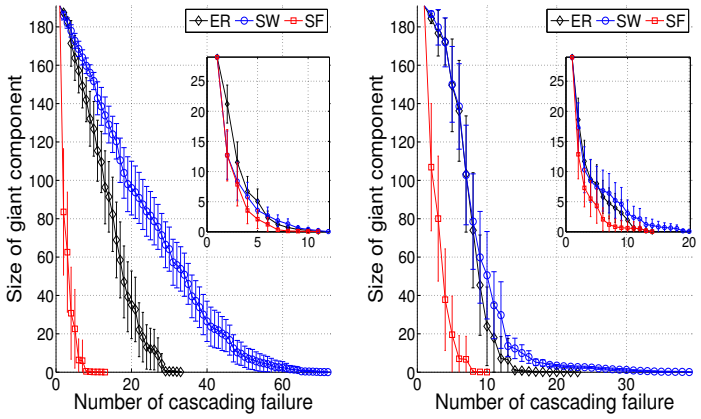

Fig. 3: (Color Online) The impact of cascading failures with RP (left) and RA (right) failures for an MV grid with $N > 30$. (Insets: Results for an MV grid with $N < 30$.)

We next show in Fig. 4 how the network degrades in terms of the communication efficiency at G^{com} and the size of the giant component at G^{sg}. Both metrics suffer similar deterioration for all cases. RP causes relatively less severe functionality degradation (RA $\succ$ RP). However, when $1-p$ increases, we observe consistently that at one point the reverse trend (RA $\prec$ RP) becomes true. This behavior is also observed in small MV grids with $N < 30$ (see insets of Fig. 4). This indicates that when the spreading effect of cascading failures is limited (*i.e.*, when the network system is small), randomized failure points cause more detrimental impact than the gradual failure of immediate neighbors of failed nodes.

B. Impact of Targeted Cascading Failures

To get a better understanding of the different types of targeted cascading failures, as expressed by our extended centrality (Eq. 2), we first investigate the extend to which different centrality measures result in attacks on different nodes. To this end, we use Spearman coefficients, as a full rank correlation proxy, and the percentage of top-10% node overlap, as a high rank-correlation proxy. Tables III and IV give a sample Spearman coefficient and top-10% overlap respectively. The Spearman coefficients across all the MV grids show that the centrality pairs have *low* correlations. In fact, extended EC often *negatively* correlates with others. The observation is consistent for high rank nodes (top-10% overlap) where the overlap tends to be low. As such, the actual targeted nodes (both the set of nodes and the order) are different when based on the different extended centrality rankings.

Interestingly, despite this, our results show that their impact to the system is rather similar. Figure 5 shows the impact of the different attacks on different network interdependencies where we observe overlapping curves. This behavior is consistent across all the MV grids, suggesting that the MV grid topology structures are especially vulnerable to cascading failures in general, regardless of the points of attack. This indicates that simple protection schemes protecting nodes with high centrality are not sufficient to defend MV grids against cascading failures. This observation agrees with the theoretical findings in [2]. Our observations here generalize [2]'s conclusion to include different types of attacks (*i.e.*, not only for degree-based attacks).

TABLE III: Sample Spearman coefficient for MV grid coupled with different G^{com} models.

	DC	BC	CC	EC	G^{com}
DC	1 1 1				ER SW SF
BC	0.5120 0.4636 0.8485	1 1 1			-//-
CC	0.7100 0.5258 0.3308	0.5155 0.5234 0.3851	1 1 1		-//-
EC	-0.7854 0.1728 -0.0622	-0.4488 -0.3482 -0.1734	-0.9162 -0.4642 0.2818	1 1 1	-//-

TABLE IV: Sample top-10% overlap (%) for MV grid coupled with different G^{com} models.

	DC	BC	CC	EC	G^{com}
DC	1 1 1				ER SW SF
BC	0.3158 0.4737 0.4211	1 1 1			-//-
CC	0.5263 0.5790 0.2105	0.5790 0.6316 0.4211	1 1 1		-//-
EC	0 0.3158 0.4211	0 0 0.1579	0 0.0526 0.2105	1 1 1	-//-

For all the three coupling cases, {ER, SW, SF}, we found that the different targeted attacks are very effective (*i.e.*, the size of the giant component and communication efficiency decrease rapidly after only approximately 10% of nodes removed). This is attributed to two factors: (1) the MV grids have (near-)zero clustering coefficient (see Table I) and (2) high number of nodes with degree $= 2$ ($\approx 65\%$ of total nodes, see Fig. 2). The co-existence of these properties results in high probability of network fragmentation as there is very good chance that a failure involves a "bridge" node that singularly connects the grid network. As only the giant component survives, such fragmentation rapidly disintegrates the system. Moreover, we note that the MV grids also have low path diversity and exhibit relatively long mean path lengths which further increase the importance of the "bridge" nodes in maintaining connectivity.

For all types of targeted attacks, we observe the robustness follows $SF \prec ER \prec SW$ order which is consistent with that observed for random failure cases. Therefore, for the case of MV grids, they are most resilient against cascading failures when dependent on a communication network exhibiting small-world properties such as low average path lengths and

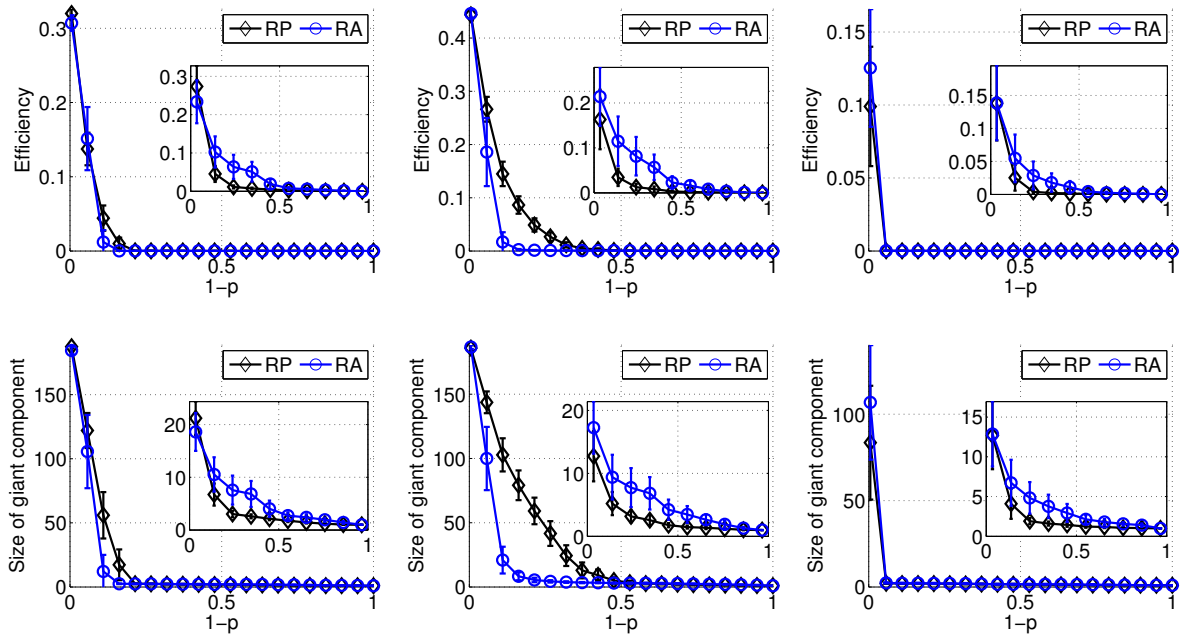

Fig. 4: (Color Online) The impact of random cascading failures on the communication efficiency (top row) and the size of giant component for an MV grid (bottom row) when $1-p$ fraction of nodes are removed based on RP and RA strategies for an MV grid with $N > 30$ (Inset: grid with $N < 30$) coupled with ER (left column), SW (center column) and SF (right column) graph.

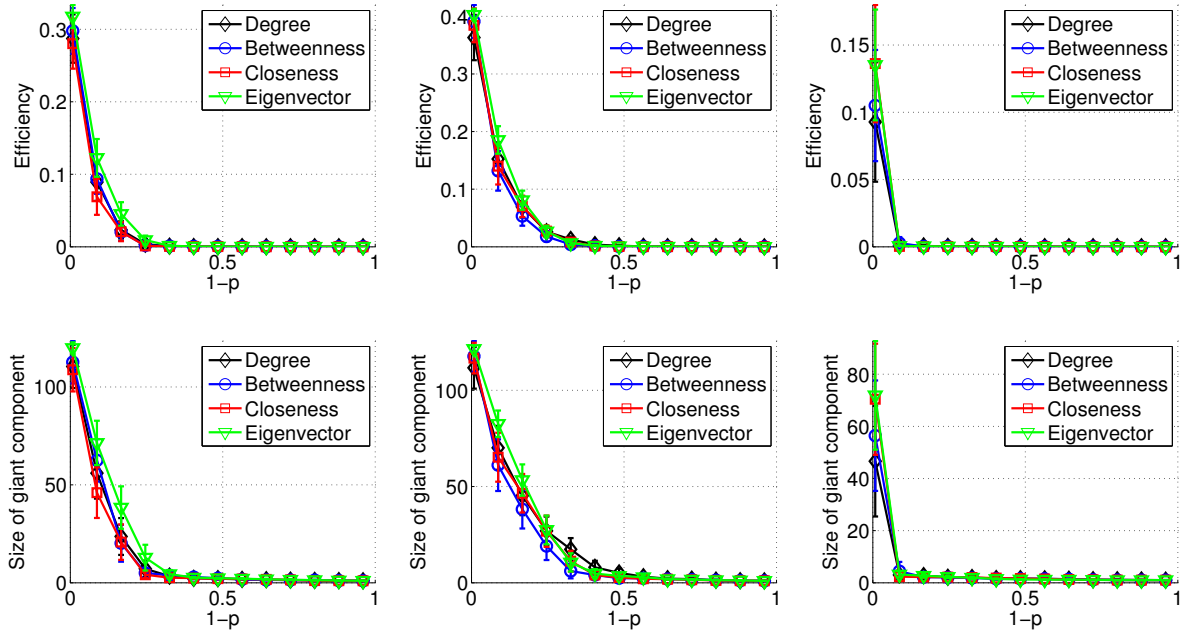

Fig. 5: (Color Online) The impact of cascading failures on the communication efficiency, η (top row) and the size of giant component (bottom row) when $1-p$ fraction of nodes are removed based on different targeted attacks for an MV grid coupled with $N > 30$ interdependent on ER (left column), SW (center column) and SF (right column) graph.

high clustering coefficient. Conversely, MV grids coupled with SF networks are always the least robust against cascading failures. On one hand, this corroborates with past analysis for targeted attacks (*e.g.*, [30]) since simultaneous removal of top well connected hubs rapidly fragments the network. On the other hand, this finding is also counter-intuitive as SF networks are known to be robust to random removals [25] due to the fact that (1) most nodes have small degree (non-hub) and (2) major hubs are usually connected to other smaller hubs; forming a hierarchy of hubs that resists network fragmentation. Tracking the system following our sequential cascading failure simulations, we found that such vulnerability

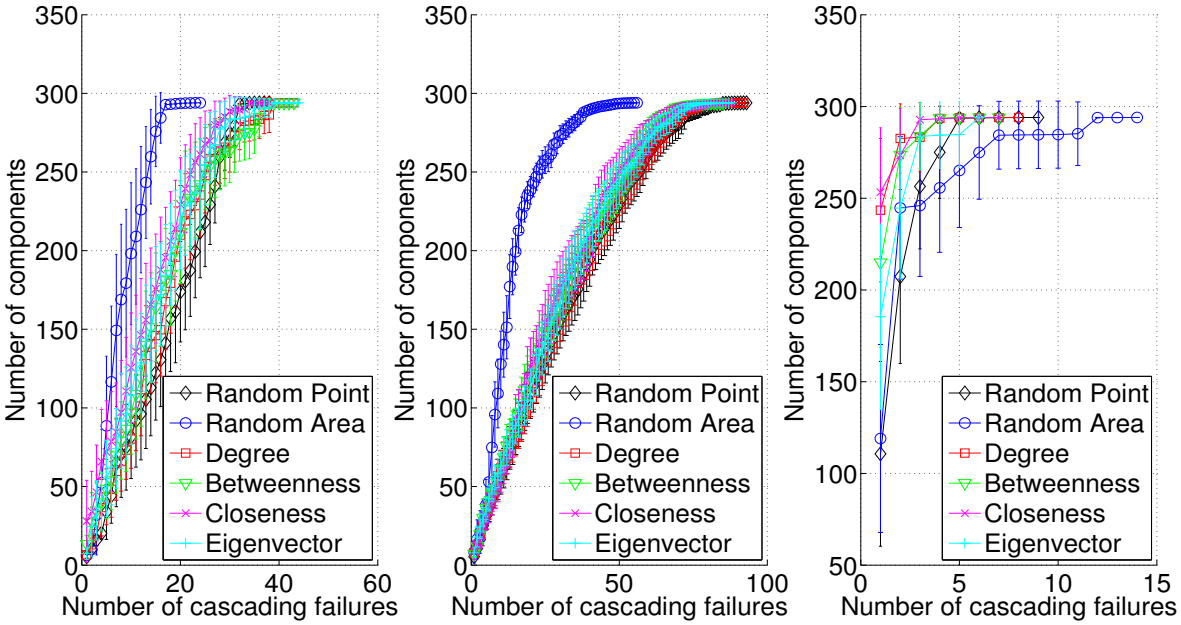

Fig. 6: (Color Online) Effect of cascading failures on the number of resulting components for MV grid coupled with ER (left), SW (center) and SF (right) networks.

is due to the fact that cascading failures have a spreading effect which in most cases, involves the removal of multiple hubs in a single cascade. Hence, the existence of multiple hubs surrounding a hub that "protects" the network from losing its connectedness turns out to be the very reason why coupling with SF networks is especially vulnerable, as cascading failures have high probability of removing multiple hubs in the near vicinity simultaneously.

For each type of theoretical graph model, we further experimented with varying clustering coefficient and link density. We found no direct relationship between clustering coefficient and the impact of cascading failures (*i.e.*, the size of giant component / communication efficiency) – high clustering coefficient does not necessarily provide better resilience. However, we find that, for relatively sparse networks (*i.e.*, at low link density region), link density can be a good relative robustness indicator with better system robustness found in systems with higher link density. Nevertheless, this is not to be used singularly as a determinant of system robustness as the robustness still depends on the exact degree distribution of the networks. For instance, an MV grid coupled with an SW graph with lower link density may still be more robust than a system coupled with an SF graph with high link density.

Next, we investigate the extreme case where we fail the system gradually until all nodes fail. For this, we relax the assumption that only the giant component retains functionality but allow any component of size > 1 to be functional. This allows us to gain insights into the change (if any) in the disruptive power of individual cascading failures when the networks are gradually disconnected. We show sample results with $N = 191$ in Fig. 6. Systems coupled with SF networks remain to be the most vulnerable ones. The system is completely disintegrated after only approximately $10 \sim 15$ cascading failures for SF networks while interdependent systems that couple with ER and SW networks require approximately 40 and 90 cascading failures respectively. While most failure types cause similar level of damage, RA failures seem to be most effective when MV grids are dependent on ER and SW networks. When MV grids couple with SF networks, RA failure is the least effective (on average) but the confidence interval indicates that the results differ significantly compared against others.

Finally, we show in Fig. 7 the average number of cascading failures required to complete the disintegration of the system (*i.e.*, all nodes disconnected) for the entire set of real MV grids from our dataset. We observe that MV grids coupled with SF networks are so vulnerable that an increase in N does not result in increasing number of cascading failures required. On the other hand, we see the gradual increase of the number of cascading failures required for MV grids coupled with SW networks when N increases, suggesting that small-world properties are beneficial to protect an interdependent system against cascading failures.

V. Summary and Conclusions

In this paper, we study the impact of cascading failures on an interdependent system consisting of a communication network and an MV distribution power grid, using real grid networks that are currently operating in the Netherlands. We evaluate the effect of such iterative failures on the MV grids coupled with different types of communication networks (including random, small world and scale-free network models) and types of failures (both unintentional and intentional failures). Our study shows that MV grids are extremely vulnerable to cascading failures, a finding of particular importance when considering the advent of the smart grid with the increasing interdependency of the grid and supporting communication network. The tree-like structure of MV grids, featuring very

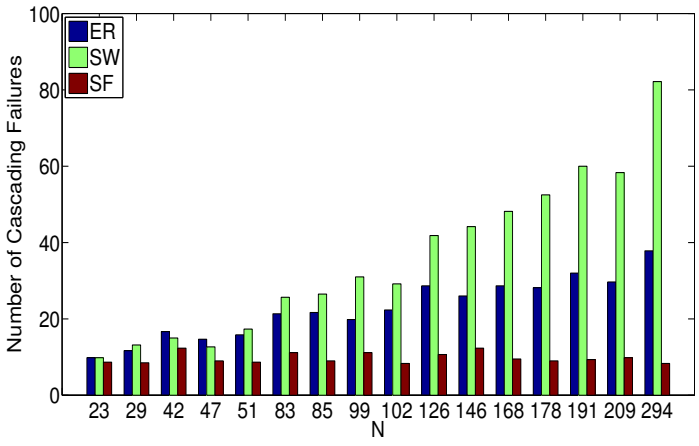

Fig. 7: (Color Online) Number of cascading failures to fully disintegrate the interdependent system.

low clustering coefficient, high mean path lengths and mean node degree close to two, is the main contributing factor to this, since a high number of "bridge" nodes increases the probability of fragmentation of the MV grids. The interdependent system as a whole is almost equally susceptible to catastrophic damage regardless of the nature of failures. Simple protection schemes focusing on protecting specific "important" nodes (*e.g.*, high centrality nodes) will not be effective against cascading failures. Furthermore, broad degree distribution of the communication network topologies, known to strengthen the resilience of network against single non-cascading failures, is found to have the reverse effect on interdependent systems. Specifically, the existence of multiple hubs (as in SF graphs) is detrimental to the system against cascading failures. Coupling with SW networks result in the most robust system, implying small-world properties are beneficial for the robustness of interdependent systems. Finally, we found that higher link density in sparse networks (*i.e.*, at low density region) provides better robustness for the same type of network model.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Commission's Seventh Framework Programme FP7-ICT-2011-8 under grant agreement no 318708 (C-DAX) and the CHIST-ERA / EPSRC UK project CONCERT (grant no. EP/L018535/1). The authors alone are responsible for the content of this paper.

REFERENCES

[1] S. V. Buldyrev, *et. al.*, "Catastrophic cascade of failures in interdependent networks," Nature, vol. 464, no. 7291, pp. 1025-1028, 2010.

[2] X. Huang, *et. al.*, "Robustness of interdependent networks under targeted attack," Physical Review E83, 065101 (R) 2011.

[3] G. D'Agostino and A. Scala, Eds., "Networks of Networks: The Last Frontier of Complexity," New York, NY, USA: Springer, 2014, (DOI) 10.1007/978-3-319-03518-5.

[4] E. Luiijf, *et. al.*, "Empirical findings on critical infrastructure dependencies in Europe," in Critical Information Infrastructure Security, Lecture Notes in Computer Science, Berlin, Germany, Springer, 2009.

[5] E. Zio and G. Sansavini, "Modeling interdependent network systems for identifying cascade-safe operating margins," IEEE Trans. Reliability, vol. 60, no. 1, March 2011.

[6] G. A. Pagani and M. Aiello, "Towards decentralization: A topological investigation of the medium and low voltage grids," IEEE Trans. Smart Grid, vol. 2, no. 3, pp. 538-547, Sept. 2011.

[7] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," Physica A 392 (2013) 2688-2700.

[8] W. K. Chai, *et. al.*, "An Information-centric Communication Infrastructure for Real-time State Estimation of Active Distribution Networks," IEEE Trans. Smart Grid, vol. 6, no. 4, pp. 2134-2146, July 2015.

[9] W. K. Chai, *et. al.*, "Enabling Smart Grid Applications with Information-centric Networking," Proc. 2nd ACM Conference on Information-Centric Networking (ICN 2015), San Francisco, USA, Sep. 30 - Oct. 2, 2015.

[10] K. V. Katsaros, *et. al.*, "Supporting Smart Electric Vehicle Charging with Information-Centric Networking," Int'l Workshop on Quality, Reliability, and Security in Information-Centric Networking, Greece, 2014

[11] K. V. Katsaros, *et. al.*, "Information-centric Networking for Machine-to-Machine Data Delivery - A Case Study in Smart Grid Applications," IEEE Networks Magazine, vol. 28, no. 3, pp. 58-64, May-June 2014.

[12] K. V. Katsaros, B. Yang, W. K. Chai and G. Pavlou, "Low Latency Communication Infrastructure for Synchrophasor Applications in Distribution Networks," Proc. SmartGridComm 2014, Venice, Italy, Nov 2014.

[13] J. Martín-Hernández, H. Wang, P. Van Mieghem and G. D'Agostino, "Algebraic Connectivity of Interdependent Networks", Physica A, Statistical Mechanics and its Applications, no. C, vol. 404, pp 92-105, 2014.

[14] P. Hines, K. Balasubramaniam and E. C. Sanchez, "Cascading failures in power grids," IEEE Potentials, vol. 28, no. 5, pp. 24-30, 2009.

[15] V. Rosato, *et. al.*, "Modelling interdependent infrastructures using interacting dynamical models," International Journal of Critical Infrastructures, 4(1/2):63-79, 2008

[16] T. N. Dinh, *et. al.*, "On new approaches of assessing network vulnerability: hardness and approximation," *IEEE/ACM* Trans. Netw., vol. 20, no. 2, pp. 609-619, April 2012

[17] G. Fu, *et. al.*, "Interdependent networks: vulnerability analysis and strategies to limit cascading failure," European Physical Journal B, 87:148, July 2014.

[18] Z. Huang, C. Wang, M. Stojmenovic and A. Nayak, "Balancing system survivability and cost of smart grid via modeling cascading failures," IEEE Transactions on Emerging Topics in Computing, June 2013.

[19] J. Guo, *et. al.*, "Networks formed from interdependent networks," Nature Physics, vol. 8, Jan. 2012, pp. 40-48.

[20] D. T. Nguyen, *et. al.*, "Detecting critical nodes in interdependent power networks for vulnerability assessment," IEEE Trans. Smart Grid, vol. 4, no. 1, pp. 151-159, March 2013.

[21] M. Parandehgheibi, E. Modiano and D. Hay "Mitigating Cascading Failures in Interdependent Power Grids and Communication Networks," in Proc. SmartGridComm 2014, Venice, Italy, Nov 2014.

[22] S. Trajanovski, J. Martín-Hernández, W. Winterbach and P. Van Mieghem, "Robustness envelopes of network," Journal of Complex Networks (2013) 1, pp. 44-62.

[23] P. Erdős, A. Rényi, "On the evolution of random graphs", Mathematical Institute of the Hungarian Academy of Sciences, pp. 17-61, 1960.

[24] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks", Nature 393 (6684); pp. 440-442, 1998.

[25] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," Science, vol. 286, no. 5439, pp. 509-512, Oct. 1999.

[26] G. Siganos, *et. al.*, "Power laws and the AS-level internet topology," *IEEE/ACM* Trans. Netw. vol. 11, no. 4, pp. 514-524, Aug. 2003.

[27] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," Phys. Rev. Lett., vol. 87, no. 19, 5 Nov 2001.

[28] S. Wasserman and K. Faust, "Social network analysis: Methods and Applications," Cambridge: Cambridge University Press, 1994.

[29] G. Nomikos, P. Pantazopoulos, M. Karaliopoulos and I. Stavrakakis, "Comparative assessment of centrality indices and implications on the vulnerability of ISP networks," 26th International Teletraffic Congress (ITC), 2014.

[30] R. Cohen, K. Erez, D. ben-Avraham and S. Havlin, "Breakdown of the Internet under intentional attack," Phys. Rev. Lett. 86: 36825, 2001.