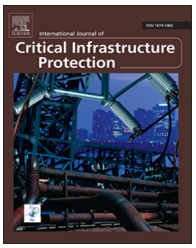
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 16 (2017) 3–12

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Using interdependency matrices to mitigate targeted attacks on interdependent networks: A case study involving a power grid and backbone telecommunications networks

Diego F. Rueda, Eusebi Calle*

Institute of Informatics and Applications, Universitat de Girona, P-IV Building, Campus Montilivi, Girona 17071, Spain

ARTICLE INFO

Article history:
Received 25 November 2015
Received in revised form
29 June 2016
Accepted 16 November 2016
Available online 9 December 2016

Keywords:
Interdependent Critical Infrastructures
Interdependent Networks
Failure Propagation
Attack Mitigation
Robustness
Interdependency Matrices
Power Grid
Backbone Telecommunications Networks

ABSTRACT

Analysis of the interdependencies between interconnected critical infrastructures can help enhance the robustness of the individual infrastructures as well as the overall interconnected infrastructures. One of the most studied interdependent critical infrastructure network scenarios is a power grid connected to a backbone telecommunications network. In this interdependent infrastructure scenario, the robustness of the entire system is usually analyzed in the context of cascading failure models in the power grid. However, this paper focuses on targeted attacks, where an attack on a telecommunications network node directly affects a connected power grid node, and vice versa. Cascading failures are outside the scope of this paper because the objective is to enhance the robustness of the interconnections between the infrastructures. In order to mitigate the impacts of targeted attacks on the interdependent infrastructures, three interdependency matrices for connecting the infrastructures are specified and analyzed. The analysis identifies the interdependency matrix that best reduces the impacts of targeted attacks and the propagation of failures between the infrastructures. Additionally, the impacts of interconnecting a power grid to different telecommunications networks, each with different susceptibilities to targeted attacks, is evaluated.

1. Introduction

Large-scale critical infrastructure failures rarely occur, but when they do, the consequences are catastrophic and expensive. In 2014, a human error in configuring Time–Warner's Internet routers in the United States resulted in a failure that prevented 11.4 million clients from accessing broadband services for three hours [21]. Network robustness, defined as the ability of a network to continue to operate when subjected to failures [2], can be evaluated by measuring the impacts of large-scale failures. However, most critical infrastructures, such as water supply systems, transportation systems, power grids, oil and gas pipelines, and telecommunications systems, need to interact with other networks to provide goods and services.

Interdependencies between critical infrastructures mean that the behavior and reliability of one network depend on the other networks [1]. A fundamental property of

*Corresponding author.
E-mail address: u1930599@campus.udg.edu (D.F. Rueda).

http://dx.doi.org/10.1016/j.ijcip.2016.11.004

interdependent networks is that a node failure in one network can spread to nodes in other networks, leading to cascading failures and dramatic consequences [1]. A good example of interdependent networks is a power grid and a telecommunications network, where the power grid relies on the telecommunications network for control and the telecommunications network relies on the power grid for electricity supply [14]. An example of a large-scale failure in interdependent networks is the Italian blackout of 2003, where a single failure in the power grid resulted in failures that propagated over a telecommunications network, ultimately affecting more than 55 million people [1,14]. The robustness of this interdependent critical infrastructure to cascading failures has been studied, but the impacts and mitigation of targeted attacks have yet to be analyzed.

This paper focuses on identifying critical nodes that are targeted by attacks. Whether or not a failure spreads and generates a cascading failure is beyond the scope of this paper. Instead, the focus is on protecting telecommunications and power grid networks from propagating failures. By identifying the appropriate models for interconnecting the two types of networks, it is possible to enhance their robustness.

In targeted attacks, the most important nodes, usually determined according to a centrality metric, are first removed. In such a scenario, it is possible to discern the nodes that could have serious impacts on the interdependent networks. Therefore, it is important to study network robustness under targeted attacks when a backbone telecommunications network and power grid are interconnected. Through this analysis, the best interdependency matrix for mitigating the impacts of targeted attacks on the interdependent critical infrastructures can be identified. The interdependent critical infrastructures also support analyses of the effects of the interdependency matrices on the propagation of targeted attacks between the two networks, which may have different topological properties.

Drawing on the results of Sydney et al. [20] and Iyer et al. [7], it is possible to determine which attacks would produce the greatest damage based on the topology of a single network. A backbone telecommunications network can be modeled as an Erdos–Renyi (ER) graph [3] while a power grid may be modeled as a Watts–Strogatz small-world (SW) graph [28]. An Erdos–Renyi graph shows vulnerability to targeted attacks based on node betweenness centrality b_c [20]. Moreover, the less robust Erdos–Renyi networks under targeted attacks have low values of average nodal degree $\langle k \rangle$ and high values of average shortest path length $\langle l \rangle$ and diameter D. Based on [7], it can be concluded that, for disassortative networks (with disassortative values $r<0$), simultaneous targeted attacks based on node degree centrality d_c are most effective at degrading the networks. In contrast, assortative networks (with assortative values $r>0$) are more vulnerable to sequential targeted attacks based on node betweenness centrality [7]. Interested readers are referred to [8] for a detailed coverage of graph theory and its relevance to this research.

The primary goal of this paper is to use interdependency matrices to evaluate and mitigate the impacts of the most dangerous attacks on a backbone telecommunications network interconnected with a power grid. Specifically, the backbone telecommunications network is targeted by sequential attacks that leverage betweenness centrality while the power grid is targeted simultaneously by attacks based on degree centrality; this enables the robustness of the interconnected networks to be measured. In order to simplify the interdependency model, it is assumed that investments have been made in the power grid to prevent the failure of one node from inducing cascading failures and to redistribute excessive loads to other network elements. In other words, a targeted attack on one node in the telecommunications network only damages the power grid node to which it is directly connected and the failure does not spread to other power grid nodes, and vice versa.

2. Previous work

Previous research has focused on analyzing the robustness of interdependent networks to cascading failures resulting from random and targeted initial failures. Buldyrev et al. [1] have examined the robustness of interdependent networks to cascading failures using the notion of percolation ρ. They show the existence of a critical percolation threshold ρ_c above which a considerable fraction of the nodes in the two networks remain functional at steady state. However, if $\rho<\rho_c$, then both networks fragment completely and the entire system collapses.

Parandehgheibi and Modiano [14] have shown that the robustness of the interdependent Italian telecommunications and power grid networks can be evaluated using the notion of minimum total failure removal (MTFR). In this situation, the larger the minimum total failure removal, the more robust are the networks. Other researchers have used algebraic connectivity λ_2 to analyze the robustness of interdependent networks. Martin-Hernandez et al. [10] analyze the critical number of interlinks beyond which any further inclusion does not enhance the algebraic connectivity; this phase transition depends on the topology of the graph model and they discovered that the transition point also increases with assortativity. Tauch et al. [22] evaluate algebraic connectivity as a robustness metric and use it to rewire interlinks. They also employ the effective graph resistance (EGR) as a robustness metric for interdependent networks by considering the Laplacian matrix of the entire system [23].

Several researchers have analyzed the robustness of interdependent networks to cascading failures generated by initial targeted attacks on high-degree nodes in two scale-free (SF) networks. Huang et al. [6] introduce a general technique that maps the targeted attack problem in interdependent networks to a random attack problem; they discovered that, when the highly-connected nodes are protected and have lower probabilities of failure compared with single networks, then the coupled networks are more vulnerable with ρ_c values significantly greater than zero. Zhang et al. [29] extend the interdependent network model by considering network flows and study the robustness under different attack strategies; in their model, nodes fail due to overloading or loss of interdependency. Pinnaka et al. [16] analyze the robustness of the U.S. critical infrastructure network to cascading failures; they

select the nodes to be removed based on four centrality metrics and compare the robustness in these scenarios.

Researchers have also studied the effects of various interdependency matrices on the robustness of interdependent networks. Wang et al. [26] have shown that link patterns can dramatically improve the robustness of interdependent networks by preventing cascade propagation. Specifically, the best of the three link patterns for avoiding cascading failure propagation in an Erdos–Renyi/small-world interdependent network is when the nodes with the highest nodal degrees are interconnected. Similarly, Golshan and Zhang [4] have shown that "high-to-high" degree coupling is better at mitigating cascading failures in real and synthetic interdependent networks. With respect to targeted attacks, the best interdependency matrix for reducing the impacts of sequential targeted attacks based on betweenness centrality in two Erdos–Renyi telecommunications networks is when the highest betweenness centrality nodes in one of the networks are connected to the lowest betweenness centrality nodes in the other network [18]. The opposite is true for an interdependency matrix in which the nodes with the highest betweenness centrality are interconnected [18].

Several approaches have been proposed for modeling and analyzing interdependent critical infrastructures, including network-based methods, empirical methods, agent-based methods, system-dynamics-based methods, economic-theory-based methods, hierarchical holographic modeling, high-level-architecture-based methods, Petri nets, dynamic control system theory and Bayesian networks [13]. These approaches all have utility in capturing interdependencies between critical infrastructures. However, this work models interdependent critical infrastructures using a network-based approach. Specifically, each infrastructure is modeled as a network and the interdependencies between the networks are expressed by interlinks. This representation captures the topological properties and flow patterns of the interdependent critical infrastructures [13]. Interested readers are referred to [13] for detailed descriptions and comparisons of the various modeling approaches.

In summary, the main objectives of this work are to evaluate and mitigate the impacts of the most dangerous targeted attacks on the robustness of interdependent critical infrastructures comprising a power grid and a backbone telecommunications network. Three distinct link patterns for the interdependency matrix are used to analyze the robustness of the power grid when a targeted attack occurs on the backbone telecommunications network, and vice versa. This analysis identifies the best interdependency matrix that mitigates the impacts of targeted attacks on the robustness of the interdependent critical infrastructures. The interdependent critical infrastructures also support the investigation of the effects of the interdependency matrices on the propagation of targeted attacks between the two networks, which have different topological properties. Moreover, the consequences of interconnecting the power grid to different telecommunications networks, each with different susceptibilities to targeted attacks, are evaluated.

3. Interdependency matrices and failure model

In targeted attacks, the most important nodes based on certain centrality metrics are the first to be removed from a network. Several metrics have been proposed to identify the critical nodes in networks and to discern the probability that a node will be attacked initially and become inactive. These metrics are based on graph theory (e.g., degree, betweenness, closeness and eigenvector centrality metrics), network failure analysis or "real-world" features (e.g., number of affected users and sociopolitical or socioeconomic considerations). In order to enhance the robustness of interdependent critical infrastructures, it is necessary to determine the appropriate models that should be used to interconnect networks.

In the network-based approach considered in this research, the propagation of an attack between a telecommunications network and power grid is modeled using the link patterns of various interdependency matrices. Moreover, centrality metrics based on graph theory are used to rank the nodes that are affected by targeted attacks. This section defines three interdependency matrices based on [4,18] and describes the failure model involving targeted attacks.

3.1. Interdependency matrices

Definition 1. Consider two undirected networks $G_1(S,U)$ and $G_2(T,V)$, each with sets of nodes (S,T) and links (U,V), respectively. Let $|N_1|$ and $|N_2|$ be the numbers of nodes in G_1 and G_2, respectively, and $|L_1|$ and $|L_2|$ be the numbers of links in G_1 and G_2, respectively. When G_1 and G_2 interact, a set of bidirectional interlinks L_{12} joining the two networks is introduced. Consequently, an interdependent network is defined as $G(N,L)=(S \cup T, U \cup V \cup L_{12})$.

Definition 2. Let B be an $|N| \times |N|$ interconnection matrix representing the interlinks $S_i \leftrightarrow T_j$ between G_1 and G_2, and vice versa. In order to interconnect the nodes between these networks, the nodes in G_1 are ordered according to a centrality metric and labeled S_i ($i=1,2,\ldots,N_1$), i.e., $c_{S_1} \geq c_{S_2} \geq \ldots \geq c_{S_{i-1}} \geq c_{S_i} \geq c_{S_{i+1}} \geq \ldots \geq c_{S_{N_1-1}} \geq c_{S_{N_1}}$, where c_{S_i} denotes the centrality value of node S_i. Similarly, the nodes in G_2 are ordered according to a centrality metric and labeled T_j ($j=1,2,\ldots,N_2$), i.e., $c_{T_1} \geq c_{T_2} \geq \ldots \geq c_{T_{j-1}} \geq c_{T_j} \geq c_{T_{j+1}} \geq \ldots \geq c_{T_{N_2-1}} \geq c_{T_{N_2}}$, where c_{T_j} denotes the centrality value of node T_j. In both cases, if some nodes have the same centrality measure, then they are labeled randomly. Then, three interdependency matrices can be generated to interconnect the networks:

- *High Centrality Interdependecy Matrix (B_{HC})* denoted as a dependency by an interlink $S_i \leftrightarrow T_i$ and which defines a one-to-one correspondence between nodes in G_1 and G_2, i.e., high-centrality (low-centrality) nodes in G_1 are connected to high-centrality (low-centrality) nodes in G_2.
- *Low Centrality Interdependecy Matrix (B_{LC})* denoted as a dependency by an interlink $S_i \leftrightarrow T_{N-i+1}$ and which defines a one-to-one correspondence between nodes in G_1 and G_2, i.e., high-centrality nodes in G_1 are connected to low-centrality nodes in G_2, and vice versa.

- *Random Interdependency Matrix (B_{RA})* denoted as a dependency by an interlink $S_i \leftrightarrow T_j$ and which defines a random one-to-one correspondence between nodes in G_1 and G_2, i.e., nodes in G_1 and G_2 are connected randomly without their centrality measures being considered, thus generating a random pattern.

The one-to-one nodal interconnections between two networks can be conditioned by a coupling weight $p>0$. In this model, the consequences of a failure in one network on the other network depend on a diffusion process provided by the strengths of the interconnections between the nodes. Thus, depending on the coupling weight p, different diffusion processes can be expressed in interdependent networks. When $p=0$, there are no interactions between the networks [10]. However, if $p<p^*$, then the two networks are structurally distinguishable; on the other hand, if $p>p^*$, the two networks behave as a whole [17]. The p^* value represents a structural transition point. For large p values, a superdiffusion process is observed, i.e., diffusion in the interconnected networks takes place faster than in either of the networks separately [5]. Superdiffusion is a synergistic phenomenon in an interconnected network that can occur for values of $p<p^*$, where the network components function distinctly [19].

Although the impact of a telecommunications network failure on the power grid could be weighted by the coupling coefficient p, this paper focuses on a scenario where a failure in one node of a network leads to a failure in the dependent node in the other network. Thus, the p value does not condition the failure propagation between the nodes in the two networks and does not limit the evaluation of the three interdependency matrices to mitigate the impacts of targeted attacks. The analysis of the effects of p on failure propagation is a topic for future research.

3.2. *Failure model*

In order to maximize the impact of an attack on a network, the network elements (nodes or links) are removed according to their importance. In the case of a single network, two distinct schemes can be used to select the elements to be removed. In a simultaneous targeted attack on a single network, the centrality metric is calculated for all the nodes in the network. Then, a specified fraction of the nodes are removed in order of their centrality measures (highest to lowest) [7]. In sequential targeted attacks on a single network, the node with the highest centrality value is the first to be removed. Next, the node with the highest centrality value in the resulting network is removed. This procedure of recalculating the centrality measures and removing the highest ranked node is repeated until the desired fraction of nodes have been removed [7].

Definition 3. When two networks are interconnected by bidirectional interlinks, each node S_i $(i=1,2,\ldots,N_1)$ in G_1 depends on one and only one node T_j $(j=1,2,\ldots,N_2)$ in G_2 to continue functioning, and vice versa. Thus, when a targeted attack occurs on a node S_i in G_1, the dependent node T_j in G_2 is removed without allowing the attack to propagate to other nodes in G_2, and vice versa.

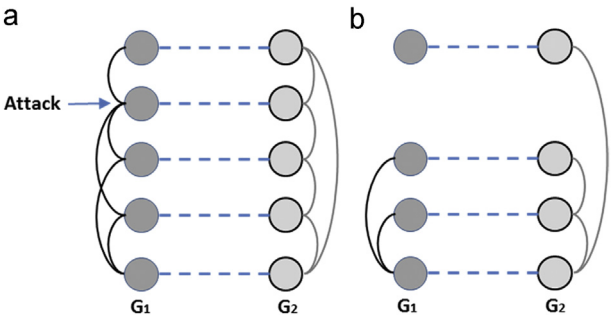


Fig. 1 – Targeted attacks on interdependent networks.

Fig. 1 shows targeted attacks on two interdependent networks. Each node in G_1 depends on one, and only one, node in G_2, and vice versa. Bidirectional interlinks between G_1 and G_2 are shown as dashed horizontal lines while U and V intralinks are shown as non-directed solid arcs. In Fig. 1(a), one node in G_1 is attacked based on its centrality measure. In Fig. 1(b), only the dependent node in G_2 is removed.

A simple functional model is used to express the failure dependencies between a power grid and backbone telecommunications network. The power grid incorporates generators and substations that are connected to power lines. Similarly, the backbone telecommunications network incorporates routers connected by communications links. Each router receives power from a substation and every substation sends data and receives control signals to/from one router [14]. In this model, a substation continues to operate if it is connected to a router and a router continues to operate if it is connected to a substation. Thus, an attack on a power grid node causes a failure of a dependent node in the telecommunications network, and vice versa. Additionally, it is assumed that investments are made in the power grid to expand the capacity of its network elements and, consequently, when a power grid node fails, the load is redistributed to other nodes without leading to cascading failures. Although this model is not completely realistic, it captures the essential properties of interdependent critical infrastructures.

4. Network topologies

In the network-based approach, interdependent critical infrastructures are modeled as graphs that express the main topological properties of the interconnected networks. The backbone telecommunications networks and the power grid model considered in the case study are described in this section. The random connection property of a backbone telecommunications network is modeled using an Erdos–Renyi (ER) random graph with a Poisson nodal degree distribution. This indicates that most nodes have approximately the same number of links close to the average nodal degree [3].

Figs. 2 and 3 show the topologies of the backbone telecommunications networks ER_1 and ER_2, respectively. The two telecommunications networks are Erdos–Renyi random graphs such that, the larger the nodes, the higher their

Fig. 2 – Backbone telecommunications network ER_1.

Fig. 3 – Backbone telecommunications network ER_2.

betweenness centrality values. Note that ER_2 has more nodes with similar betweenness centrality values than does ER_1. Hence, for targeted attacks based on betweenness centrality, ER_2 is able to maintain network connections for larger numbers of removed nodes than ER_1.

The power grid is modeled as a small-world (SW) graph. A small-world graph is a regular graph with increased randomness; thus, it exhibits the high clustering property of a regular graph and the short characteristic path length of a random graph [28]. However, in order to capture the topological properties of a power grid, the IEEE_300 real network [24] used by several researchers (see, e.g., [27]) was selected. Fig. 4 shows the topology of the IEEE_300 power grid, where the larger nodes have higher degree centrality values.

For simplicity, the ER_1 and ER_2 backbone telecommunications networks and the IEEE_300 power grid have the same number of nodes $|N_i| = 300$, but different numbers of links, $|L_1| = 437$, $|L_2| = 549$ and $|L_3| = 411$, respectively. As shown in Table 1, the ER_1 and ER_2 networks have assortative values close to zero, $r_1 = 0.0134$ and $r_2 = 0.0093$, respectively; and the

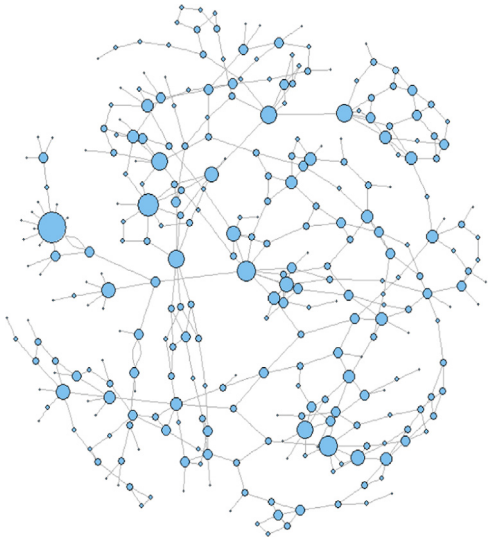


Fig. 4 – IEEE_300 power grid.

Table 1 – Topological properties of the interdependent networks.

Network	N	L	$\langle k \rangle$	k_{max}	$\langle l \rangle$	D	r
ER_1	300	437	2.91	9	5.57	12	0.0134
ER_2	300	549	3.66	8	4.57	10	0.0093
IEEE_300	300	411	2.74	12	9.94	24	−0.2137

IEEE_300 has a disassortative value $r = -0.2137$. The three networks have low values of average nodal degree $\langle k \rangle$ (2.91 for ER_1, 3.66 for ER_2 and 2.74 for IEEE_300) and high values of average shortest path length $\langle l \rangle$ (5.57 for ER_1, 4.57 for ER_2 and 9.94 for IEEE_300) and diameter D (12 for ER_1, 10 for ER_2 and 24 for IEEE_300).

Because telecommunications networks and power grids are more vulnerable to different types of attacks, the nodes in each network should be weighted using different centrality metrics. Therefore, the high centrality (B_{HC}) and low centrality (B_{LC}) interdependency matrices interconnect the two types of networks with a one-to-one correspondence between the nodes of the networks according to the centrality metric used to rank the nodes in each targeted attack.

The next section presents a number of application contexts for the three interdependency matrices. The B_{HC} matrix may be used when the most important telecommunications and power grid nodes serve each other. For example, in a large city where the nodes in a telecommunications network and power grid depend on population density. The B_{LC} matrix may be used when the most vulnerable power nodes serve the least critical telecommunications nodes, and vice versa. For example, a telecommunications operator can identify zones where blackouts occur frequently; thus, any of the most critical telecommunications nodes can be located at these points. In contrast, the B_{RA} matrix connects nodes randomly without considering the centrality values of nodes; this is the case of telecommunications networks and power grids in non-urban or rural areas.

5. Numerical results and discussion

This section analyzes the robustness of the power grid when an attack targets a backbone telecommunications network (and vice versa) for the three interdependency matrices, B_{HC}, B_{LC} and B_{RA}.

Although several metrics have been proposed for assessing network robustness (see, e.g., [25]), this work uses the average two-terminal reliability (ATTR) [11] as the network robustness metric. The metric has been used widely in previous work [9,11,12,15] to measure network robustness because it provides a good approximation and sensitivity for quantifying network connectivity under failure scenarios. Furthermore, ATTR can be used to compare network robustness under various failure scenarios, so it supports analyses of the effects of the three interdependency matrices with regard to the propagation of targeted attacks in the interdependent critical infrastructures.

ATTR measures the probability that a randomly-chosen pair of nodes is connected [11]. The two-terminal reliability between two nodes is equal to one if a path exists between them; otherwise, it is equal to zero [12]. Thus, when the network is fully connected, exactly one component exists and ATTR=1. In another case [12], the ATTR metric is calculated as the sum over the number of node pairs in each connected component and divided by the total number of node pairs in the network. However, in this work, the following equation is used to compute the ATTR metric [11]:

$$ATTR = \frac{\sum_{i=1}^{c} K_i(K_i-1)}{N(N-1)} \quad (1)$$

where c is the number of components, K_i is the number of nodes in component i and N is the number of nodes in the network. In failure scenarios, the successive removal of nodes or links brings ATTR closer to zero [11]. If a targeted attack affects two network topologies with the same percentages of nodes or links, then the network with the highest ATTR value is considered to be more robust and, therefore, is more resistant to the attack [11].

In the failure scenarios considered in this paper, the percentage of nodes removed P ranged from 1% to 70%. Ten runs were conducted and, based on whether the targeted attacks were simultaneous or sequential, different subsets of nodes were selected for removal.

The next section analyzes the robustness of the two telecommunications networks and the power grid as a single network scenario. Following this, the three interdependency matrices are analyzed in terms of their abilities to mitigate targeted attacks in two interdependent networks, resulting from the interconnection of the power grid to each of the two telecommunications networks. Finally, the results are discussed along with the lessons learned.

5.1. *Robustness comparison of single networks*

Fig. 5 shows the ATTR measures in a single network scenario for the ER_1 and ER_2 telecommunications networks and the IEEE_300 power grid under targeted attacks.

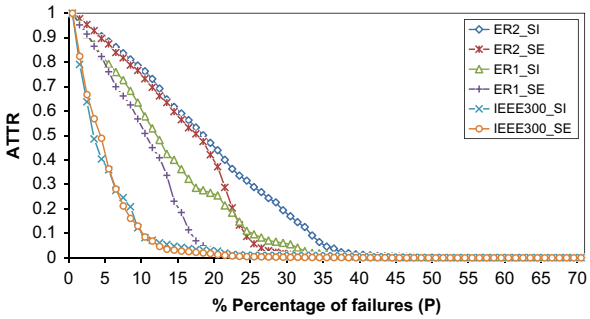


Fig. 5 – Robustness of the backbone telecommunications networks and the IEEE_300 power grid.

The graphs show that ER_1 is more vulnerable to a targeted attack than ER_2; this is because ER_1 has lower $\langle k \rangle$ and higher $\langle l \rangle$ and D values than ER_2. Moreover, both telecommunications networks are more vulnerable to sequential targeted attacks based on betweenness centrality (curves ER1_SE and ER2_SE in Fig. 5) than to simultaneous targeted attacks based on betweenness centrality (curves ER1_SI and ER2_SI in Fig. 5); this is because the assortative values are close to zero. The high vulnerability of Erdos–Renyi random networks to sequential targeted attacks based on betweenness centrality is reported in [7,18].

The IEEE_300 power grid is more vulnerable to targeted attacks than the ER_1 and ER_2 networks, which is expected because of the small-world characteristics of the IEEE_300 network. Fig. 5 shows that the IEEE_300 network is more vulnerable to simultaneous targeted attacks based on degree centrality (curve IEEE300_SI) than to sequential targeted attacks based on degree centrality (curve IEEE300_SE).

In analyzing the robustness of the ER_1 and ER_2 telecommunications networks, the two attacks produce similar damage for specific percentage ranges P of nodes removed. For ER_1, this range is between 1% and 5%, where the network connections are reduced to 76%; in the case of ER_2, the range is between 1% and 18%, where the network connections are reduced to 47%. For the remaining P values, the robustness behaviors of ER_1 and ER_2 differ for the two attacks. Thus, under a sequential targeted attack based on betweenness centrality, the network connections of ER_1 (curve ER1_SE in Fig. 5) and ER_2 (curve ER2_SE in Fig. 5) are close to 0% when the P values are approximately equal to 20% and 25%, respectively. In contrast, under a simultaneous targeted attack based on betweenness centrality, the network connections of ER_1 (curve ER1_SI in Fig. 5) and ER_2 (curve ER2_SI in Fig. 5) are close to 0% when the P reaches 30% and 37%, respectively. Additionally, as seen in Fig. 5, the robustness of the IEEE_300 power grid is similar for simultaneous and sequential targeted attacks based on degree centrality (curves IEEE300_SI and IEEE300_SE). Specifically, for P ranging from 1% to 5%, the network connections in the IEEE_300 network dramatically decrease to 36% and the network is completely disconnected when P reaches 10%.

The robustness analysis reveals that the ER_1 and ER_2 telecommunications networks are more vulnerable to a sequential targeted attack based on betweenness centrality while the IEEE_300 power grid is more vulnerable to a simultaneous targeted attack based on degree centrality. This

is a significant result because, in the case of the B_{HC} and B_{LC} matrices, the telecommunications network and power grid nodes are interconnected according to the centrality metrics used in the most dangerous targeted attack (i.e., nodes in the telecommunications networks are ranked by betweenness centrality while nodes in the power grid are ranked by degree centrality). However, in the case of the random interdependency matrix B_{RA}, the nodes in the two networks are interconnected randomly without considering any centrality metric.

5.2. *Mitigation of targeted attacks in interdependent networks*

In the interdependent critical infrastructures considered in this work, dependent nodes in the ER_1 and ER_2 telecommunications networks are only removed as a result of nodal failures in the IEEE_300 network, and vice versa. In this scenario, telecommunications network nodes that are removed are weighted by their betweenness centrality values because Erdos–Renyi networks are highly vulnerable to sequential targeted attacks based on betweenness centrality [20]. In a real scenario, the betweenness metric could represent the number of shortest paths passing through a router.

In the case of a power grid, the nodes to be removed are ranked by their degree centrality values. This is because power grid functionality depends on nodes with high degree centrality (i.e., generators and substations). Therefore, a simultaneous targeted attack on the power grid based on degree centrality is considered to eliminate the nodes. Additionally, it is assumed that the electrical properties of real power grid elements are extended. Therefore, when a node in the IEEE_300 grid is attacked, the load is distributed to other nodes without leading to cascading failures. This section analyzes the robustness of two interdependent networks (ER_1-IEEE_300 and ER_2-IEEE_300) under targeted attacks.

5.2.1. *ER_1 telecommunications network and IEEE_300 power grid*

Fig. 6 shows the robustness of the ER_1 backbone telecommunications network when a simultaneous targeted attack based on degree centrality is launched against the IEEE_300 power grid. When the ER_1 and IEEE_300 networks are interconnected by a high centrality interdependency matrix B_{HC}, a simultaneous targeted attack based on degree centrality of the IEEE_300 network causes exactly the same damage to the ER_1 network as a simultaneous targeted attack based on betweenness centrality does to ER_1 in the single network scenario. This is because, in the case of the B_{HC} matrix, nodes in ER_1 with the highest betweenness centrality values are removed first when an attack is launched against the IEEE_300 power grid. This interesting result can be seen by comparing curves ER1_SI in Fig. 5 and ER1_HC in Fig. 6. Additionally, the greatest impact on ER_1 network robustness occurs when the networks are interconnected by a link model based on the B_{HC} interdependency matrix (curve ER1_HC in Fig. 6).

For the low centrality (B_{LC}) and random (B_{RA}) interdependency matrices, the ER_1 network is more robust to a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid. As expected, in the case of the B_{LC} matrix, nodes in ER_1 with the lowest betweenness centrality values are the first to be removed when the IEEE_300 is attacked; this generates the least impact on the robustness of ER_1 (curve ER1_LC in Fig. 6). In the case of the B_{RA} matrix, a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid produces a random failure in the ER_1 network (curve ER1_RA in Fig. 6) and generates an intermediate impact on its robustness. In the case of the B_{LC} and B_{RA} matrices, when the percentages of nodes removed P are between 1% and 10%, network connections are reduced by 20% and 30%, respectively. In the case of the B_{RA} matrix, network connections in ER_1 reach 0% when P is approximately 57%; whereas for the B_{LC} matrix, P may be greater than 70% to reach 0% network connections.

Fig. 7 shows the robustness of the IEEE_300 power grid when a sequential targeted attack based on betweenness centrality is launched against the ER_1 backbone telecommunications network. When P is between 1% and 7%, the robustness in the case of the B_{HC} matrix (curve IEEE300_HC in Fig. 7) is approximated by the degradation level produced by a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid (curve IEEE300_SI in Fig. 5). For this range of p values, there is a 65% reduction of network connections in the IEEE_300 power grid. When P is increased, the B_{HC} matrix (curve IEEE300_HC in Fig. 7) produces the worst IEEE_300 network robustness compared with the B_{LC} matrix (curve IEEE300_LC in Fig. 7) and B_{RA} matrix (curve IEEE300_RA in Fig. 7).

In the case of the B_{HC} matrix, the IEEE_300 network connections dramatically decrease, until they reach 0% when P is about 30% (curve IEEE300_HC in Fig. 7). In the case of the B_{RA} and B_{LC} matrices, the network connections reach 0% when the P values are about 55% and 65%, respectively

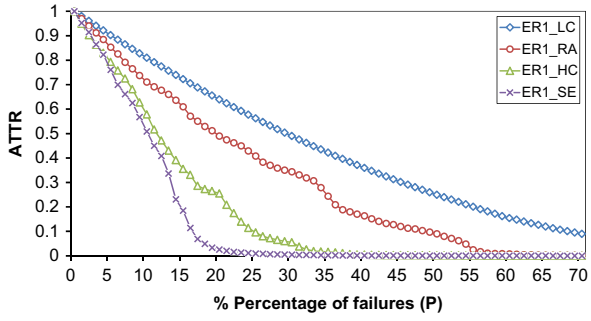


Fig. 6 – Robustness of the ER_1 telecommunications network.

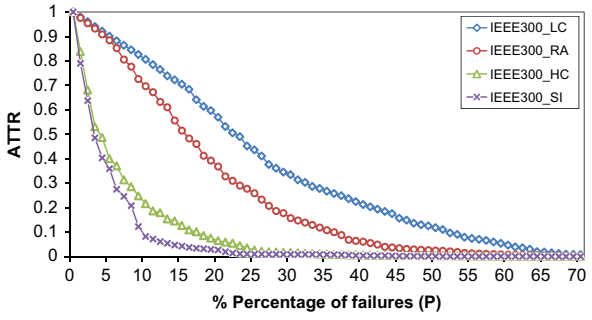


Fig. 7 – Robustness of the IEEE_300 power grid.

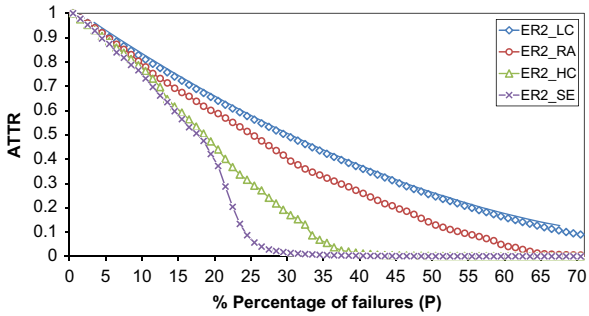


Fig. 8 – Robustness of the ER_2 telecommunications network.

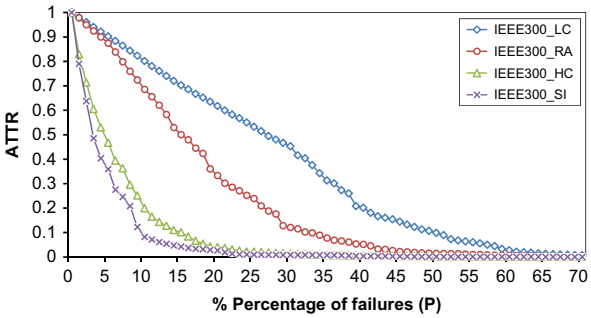


Fig. 9 – Robustness of the IEEE_300 power grid.

(curves IEEE300_RA and IEEE300_RA in Fig. 7, respectively). In the case of the B_{RA} matrix, a sequential targeted attack based on betweenness centrality on the ER_1 network causes a random failure in the IEEE_300 power grid and generates an intermediate impact on its robustness (curve IEEE300_RA in Fig. 7) compared with the B_{HC} and B_{LC} interdependency matrices. Consequently, in order to mitigate the impacts of the targeted attacks considered in this work, it is recommended that an Erdos–Renyi backbone telecommunications network and a power grid should be connected using an interdependency matrix based on the B_{LC} link pattern model.

5.2.2. *ER_2 telecommunications network and IEEE_300 power grid*

Fig. 8 shows the robustness of the ER_2 backbone telecommunications network when a simultaneous targeted attack based on degree centrality is launched against the IEEE_300 power grid. In fact, the results are similar to those obtained for the ER_1 network. The greatest impact on ER_2 network robustness is seen with the B_{HC} interdependency matrix (curve ER2_HC), intermediate impact is seen with the B_{RA} interdependency matrix (curve ER2_RA) and the least impact is seen with the B_{LC} interdependency matrix (curve ER2_LC).

However, in this interdependency scenario and for the failure model considered in this work, the ER_2 network is more robust than ER_1 for increasing values of P. In the range 1% to 7%, the robustness behavior produced by the three matrices is similar for ER_2, with a reduction to 20% network connections. ER_2 network connections reach 0% when P is 40% for B_{HC} and 67% for B_{RA} (curves ER2_HC and ER2_RA in Fig. 8, respectively), whereas for B_{LC}, P may be greater than 70% (curve ER2_LC in Fig. 8). Again, when the ER_2 and IEEE_300 networks are interconnected by a B_{HC} matrix, a simultaneous targeted attack based on degree centrality on the IEEE_300 power grid causes exactly the same damage to the ER_2 network as a simultaneous targeted attack based on betweenness centrality on ER_2 in the single network scenario (curves ER2_SI in Fig. 5 and ER2_HC in Fig. 8).

Fig. 9 shows the robustness of the IEEE_300 power grid when a sequential targeted attack based on betweenness centrality is launched against the ER_2 backbone telecommunications network (which is more robust than the ER_1 network). Comparison of Figs. 7 and 9 shows a slight improvement in IEEE_300 network robustness when it is interconnected with ER_2 by the B_{HC} and B_{LC} interdependency matrices. For example, when P is in the range 1% to 5% for the IEEE_300 power grid connected to ER_2 by the B_{HC} matrix (curve IEEE300_HC in Fig. 9), the IEEE_300 network connections decrease to 47%; on the other hand, when the IEEE_300 power grid is connected to ER_1, its network connections dramatically decrease to 35% (curve IEEE300_HC in Fig. 7). For P equal to 15%, when the IEEE_300 power grid is connected to ER_2 by the B_{LC} matrix, the network connections are 71% (curve IEEE300_LC in Fig. 7), whereas when it is connected to ER_1, the network connections are 70% (curve IEEE300_LC in Fig. 9).

5.3. *Discussion and lessons learned*

Table 2 summarizes the effects of the three interdependency matrices in mitigating targeted attacks on the interdependent critical infrastructures. The table shows that each matrix produces a different impact in terms of propagating targeted attacks in the interconnected networks. This is because the three interdependency matrices considered in this work provide different link patterns for interconnecting interdependent critical infrastructures based on the centrality metrics used to rank nodes in the networks (b_c: betweenness centrality; d_c: degree centrality; and random). However, it is important to remember that different metrics can be used to rank the most vulnerable nodes in a network.

The numerical results presented in Section 5.2 can be used to identify the interdependency matrices that best mitigate targeted attacks on networks with different topological properties. Specifically, the low centrality interdependency matrix B_{LC} reduces the impact on the telecommunications network when a targeted attack is launched against the power grid, and vice versa. This is because, when a targeted attack occurs in one network, the nodes that are less important are the first to be removed in the other network and the lowest impact on network robustness is achieved.

However, the high centrality interdependency matrix B_{HC} produces the greatest impact on the robustness of each network. This is because the most important nodes are the first to be removed in both networks.

For the random interdependency matrix B_{RA}, a targeted attack on a network produces a random failure in the other network with an intermediate impact on network robustness. Analogous results for the robustness of two interconnected networks with similar topological properties that are highly vulnerable to sequential targeted attacks based on betweenness centrality are presented in [18].

Table 2 – Effects of the B_{HC}, B_{LC} and B_{RA} interdependency matrices.

Type of Interdependent Network	Type of Attack on First Network	Interdependency Matrix (Centrality Metrics)	Resulting Attack on Second Network	Impact on Network Robustness
	Sequential by b_c	B_{HC} (b_c,b_c)	Approximately to simultaneous by b_c	Highest
ER–ER [18]	Sequential by b_c	B_{LC} (b_c,b_c)	–	Lowest
	Sequential by b_c	B_{RA} (random)	Random failure	Intermediate
	Sequential by b_c	B_{HC} (b_c,d_c)	Approximately to simultaneous by d_c	Highest
ER-Power Grid	Sequential by b_c	B_{LC} (b_c,d_c)	–	Lowest
	Sequential by b_c	B_{RA} (random)	Random failure	Intermediate
	Simultaneous by d_c	B_{HC} (d_c,b_c)	Exactly equal to simultaneous by b_c	Highest
Power Grid-ER	Simultaneous by d_c	B_{LC} (d_c,b_c)	–	Lowest
	Simultaneous by d_c	B_{RA} (random)	Random failure	Intermediate

With regard to the propagation of targeted attacks between the two networks, an interesting result is that, in the case of a link model based on the high centrality interdependency matrix B_{HC}, a simultaneous targeted attack based on degree centrality on the power grid causes exactly the same damage to the Erdos–Renyi telecommunications networks as a simultaneous targeted attack based on betweenness centrality in a single network scenario. This is because, for the B_{HC} matrix, the nodes with the highest betweenness centrality in an Erdos–Renyi telecommunications network are the first to be removed when a simultaneous attack based on degree centrality occurs on the power grid. In contrast, in the case study described in [18], when two networks with similar topological characteristics are connected by a B_{HC} matrix, the impact of a sequential targeted attack based on betweenness centrality in one of the networks generates an impact that approximates that of a simultaneous targeted attack based on betweenness centrality on the other network.

This research also assesses the effects of interconnecting the power grid with different telecommunications networks, each with different susceptibilities to targeted attacks. The numerical results reveal that connecting a power grid via B_{HC} and B_{LC} interdependency matrices to a telecommunications network that is less vulnerable to targeted attacks yields a slight improvement in the robustness of the power grid. This is because, in the interdependency scenario considered in this work (one-to-one nodal interconnections), a sequential targeted attack based on betweenness centrality on any of the telecommunications networks propagates to the same nodes in the power grid. Thus, approximately the same impact on network robustness is observed.

6. Conclusions

This paper has analyzed the efficacy of interdependency matrices in mitigating the propagation of targeted attacks in interdependent critical infrastructures; specifically, a power grid connected to a telecommunications network. In addition, the consequences of interconnecting the power grid to different telecommunications networks with different susceptibilities to targeted attacks have been evaluated.

To achieve the least impact on the power grid when the most dangerous targeted attack is launched on the telecommunications network, and vice versa, it is recommended to interconnect the two networks using the low centrality interdependency matrix B_{LC}. In contrast, the high centrality interdependency matrix B_{HC} has the greatest impact on network robustness whereas the random interdependency matrix B_{RA} has an intermediate impact on network robustness. These results are due to the fact that the interconnections embodied by the interdependency matrices take into account the vulnerabilities of the networks to specific types of attacks.

The case study of the power grid connected to a backbone telecommunications network yields interesting insights with regard to the propagation of targeted attacks in the interdependent critical infrastructures. When the two infrastructures are interconnected by a link model based on the B_{HC} matrix, a simultaneous targeted attack based on degree centrality on the power grid causes exactly the same damage to the telecommunications network as a simultaneous targeted attack based on betweenness centrality in a single network scenario. However, when the two infrastructures are interconnected via the B_{RA} matrix, a targeted attack on one of the networks propagates randomly in the other network.

The B_{HC} and B_{LC} interdependency matrices slightly improve the robustness of the power grid when it is interconnected to a telecommunications network that is more robust to a sequential targeted attack based on betweenness centrality. This is because, in the one-to-one nodal correspondence of the interdependency matrices, a targeted attack on each of the two telecommunications networks propagates to the same nodes in the power grid.

Future research will focus on identifying the most important nodes in the power grid. The nodes will be ranked based on their electrical properties that lead to large-scale failures and network robustness will be evaluated based on this new metric. Research will also study other strategies for mitigating the impacts of targeted attacks on the robustness of interdependent networks. Additionally, future research will

use the proposed methodology to evaluate the robustness of other interdependent critical infrastructures under various attack and failure scenarios.

Acknowledgement

This research was supported in part by the Spanish Ministry of Economy and Competitiveness and the DURSI Consolidated Research Group (CSI Reference SGR-1469) through the GIROS Project (TEC2015-66412-R).

REFERENCES

[1] S. Buldyrev, R. Parshani, G. Paul, H. Stanley and S. Havlin, Catastrophic cascade of failures in interdependent networks, *Nature*, vol. 464(7291), pp. 1025–1028, 2010.

[2] W. Ellens, Effective Resistance and Other Graph Measures for Network Robustness, Master's Thesis, Mathematical Institute, Leiden Universty, Leiden, The Netherlands, 2011.

[3] P. Erdos and A. Renyi, On the evolution of random graphs, *Publication of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[4] G. Golshan and Z. Zhang, The effect of different couplings on mitigating failure cascades in interdependent networks, *Proceedings of the IEEE Conference on Computer Communications Workshops*, pp. 677–682, 2015.

[5] S. Gomez, A. Diaz-Guilera, J. Gomez-Gardenes, C. Perez-Vicente, Y. Moreno and A. Arenas, Diffusion dynamics in multiplex networks, *Physical Review Letters*, vol. 110, pp. 028701-1–028701-5, 2013.

[6] X. Huang, J. Gao, S. Buldyrev, S. Havlin and H. Stanley, Robustness of interdependent networks under targeted attack, *Physical Review E: Statistical, Nonlinear and Soft Matter Physics*, vol. 83(6), pp. 065101-1–065101-4, 2011.

[7] S. Iyer, T. Killingback, B. Sundaram and Z. Wang, Attack robustness and centrality of complex networks, *PLoS ONE*, vol. 8(4), article no. e59613, 2013.

[8] T. Lewis, *Network Science: Theory and Applications*, John Wiley and Sons, Hoboken, New Jersey, 2009.

[9] M. Manzano, K. Bilal, E. Calle and S. Khan, On the connectivity of data center networks, *IEEE Communications Letters*, vol. 17(11), pp. 2172–2175, 2013.

[10] J. Martin-Hernandez, H.Wang, P. van Mieghem and G. D'Agostino, Algebraic connectivity of interdependent networks, *Physica A: Statistical Mechanics and its Applications*, vol. 404, pp. 92–105, 2014.

[11] S. Neumayer and E. Modiano, Network reliability with geographically correlated failures, *Proceedings of the IEEE International Conference on Computer Communications*, 2010.

[12] S. Neumayer and E. Modiano, Network reliability under geographically correlated line and disk failure models, *Computer Networks*, vol. 94, pp. 14–28, 2016.

[13] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety*, vol. 121, pp. 43–60, 2014.

[14] M. Parandehgheibi and E. Modiano, Robustness of interdependent networks: The case of communications networks and the power grid, *Proceedings of the IEEE Global Communications Conference*, pp. 2164–2169, 2013.

[15] W. Peng, Z. Li, Y. Liu and J. Su, Assessing the vulnerability of network topologies under large-scale regional failures, *Journal of Communications and Networks*, vol. 14(4), pp. 451–460, 2012.

[16] S. Pinnaka, R. Yarlagadda and E. Cetinkaya, Modeling robustness of critical infrastructure networks, *Proceedings of the Eleventh International Conference on the Design of Reliable Communications Networks*, pp. 95–98, 2015.

[17] F. Radicchi and A. Arenas, Abrupt transition in the structural formation of interconnected networks, *Nature Physics*, vol. 9 (11), pp. 717–720, 2013.

[18] D. Rueda, E. Calle, F. Maldonado-Lopez and Y. Donoso, Reducing the impact of targeted attacks in interdependent telecommunications networks, *Proceedings of the Twenty-Third International Conference on Telecommunications*, pp. 348–352, 2016.

[19] F. Sahneh, C. Scoglio and P. van Mieghem, Exact coupling threshold for structural transition reveals diversified behaviors in interconnected networks, *Physical Review E: Statistical, Nonlinear and Soft Matter Physics*, vol. 92(4), pp. 040801-1–040801-5, 2015.

[20] A. Sydney, C. Scoglio, M. Youssef and P. Schumm, Characterizing the robustness of complex networks, *International Journal of Internet Technology and Secured Transactions*, vol. 2(3/4), pp. 291–330, 2010.

[21] D. Talbot, Massive Internet outage points to flaws in policy and technology, *MIT Technology Review*, August 28, 2014.

[22] S. Tauch, W. Liu and R. Pears, Evaluating the cascade effect in interdependent networks via algebraic connectivity, *International Journal of Information, Communication Technology and Applications*, vol. 1(1), pp. 55–68, 2015.

[23] S. Tauch, W. Liu and R. Pears, Measuring cascade effects in interdependent networks by using effective graph resistance, *Proceedings of the IEEE Conference on Computer Communications Workshops*, pp. 683–688, 2015.

[24] University of Washington – Department of Electrical Engineering, Power Systems Test Case Archive, Seattle, Washington. ⟨www2.ee.washington.edu/research/pstca⟩, 2016.

[25] P. van Mieghem, C. Doerr, H. Wang, J. Martin-Hernandez, D. Hutchison, M. Karaliopoulos and R. Kooij, A Framework for Computing Topological Network Robustness, Technical Report 20101218, Network Architectures and Services, Delft University of Technology, Delft, The Netherlands, 2010.

[26] J. Wang, C. Jiang and J. Qian, Robustness of interdependent networks with different link patterns against cascading failures, *Physica A: Statistical Mechanics and its Applications*, vol. 393, pp. 535–541, 2014.

[27] Z. Wang and R. Thomas, On bus type assignments in random topology power grid models, *Proceedings of the Forty-Eighth Hawaii International Conference on System Sciences*, pp. 2671–2679, 2015.

[28] D. Watts and S. Strogatz, Collective dynamics of "small-world" networks, *Nature*, vol. 393(6684), pp. 440–442, 1998.

[29] P. Zhang, B. Cheng, Z. Zhao, D. Li, G. Lu, Y. Wang and J. Xiao, The robustness of interdependent transportation networks under targeted attack, *Europhysics Letters*, vol. 103(6), article no. 68005, 2013.