Topologic Representation of Electric Power Systems and Application to Risk Analysis

Gabriel J. Correa [1]; José M. Yusta [2]

***ABSTRACT* — Usually vulnerability assessment of high voltage power grids (both locally and nationally) has been linked to interests of organizations that are either owner or operators of critic infrastructure systems. Most vulnerability studies are normally developed after the occurrence of high impact events (e.g. blackouts with vast geographic coverage) in order to determine the root causes of cascade failures within certain power systems. Such studies may be conducted through structural vulnerability analysis into the power grids, and they require well-defined methodologies that may guide decision-making for implementation of actions to prevent and to recover normal operation in the power system (e.g. N-1 and N-t contingency studies are considered as the most accepted criterion into electric industries). As an alternative to classic tools for contingency analysis, in this technical contribution the authors provide some techniques based upon graph theory and complex networks, which in the last few years have been proposed as useful methodologies for analysis of physical behavior of power electric grids. This can be applied in system vulnerability evaluation, as well as its performance into risks scenarios: random risks and deliberate attacks threats. This way, it is possible to infer the consequences of those threats determined as critical or important, among others, acts of terrorism and vandalism, adverse natural phenomena, adverse weather conditions, failures in hardware and installations (which sometimes are related to human errors). Results shown in this paper lead to conclusions on the use of complex networks for contingency analysis. This also involves the study of those events that result in cascade failures and consumer disconnections.**

***Index Terms* —critical infrastructure protection, vulnerability analysis, cascade failures, homeland security**

I. INTRODUCTION

Critical infrastructure is described by many governments as the whole set of assets that are essential for the functioning of a society and its economy. In recent years, the European Commission (EC), the United States (US) Department of Homeland Security, and others have been concerned about the security of their country infrastructure. In 2008, the Council of the European Union adopted Directive 114/08/EC [1], which gave rise to the European Programme for Critical Infrastructure Protection (EPCIP). In 2009 was launched the US National Infrastructure Protection Plan [2]. The frameworks established by those protection plans can be summarized as a risk management plan involving six steps: establishing safety goals, identification of resources and risks, risk assessment, prioritization of actions, implementing protection programs, and measuring their effectiveness [3].

It should be noted the emphasis on incorporating threat quantification on the risk assessment stage, so it may be possible to deal with sets of risks that are most likely to impact critical infrastructures operations, ranging from severe weather conditions and technical failures in assets, to sabotages and terrorist attacks.

Power systems are always regarded as one of the most important critical infrastructures to social, economic and military issues in a country. In order to analyze the electric system *vulnerability* to threats, some new concepts have arisen in an attempt to describe the grid performance. The *resilience* concept suggests that a system can adapt to reach a new stable position, after suffering a disturbance or contingency in one or more of its elements. Additionally, *robustness* implies that the system will operate its undamaged infrastructure, despite being exposed to perturbations [4]. Therefore, a robust and resilient network is equivalent to a *low vulnerability network*.

Power grid vulnerability, either locally or nationally, is usually tight to the interest of the system operating companies. Most of vulnerability studies are carried out after the occurrence of high-impact events (for example, a widespread blackout) determining the causes of cascade failure events within a specific power grid. Such studies are achieved through *structural vulnerability analysis* in power transmission networks, requiring well-established methodologies that may guide decision-makers on prevention and recovery from disruptions on the power grid. For example, *N*-1 and *N-t* contingency studies [5-7] are among the most used criteria in power industry.

On the other hand, the first definition of scale-free networks resembled the infrastructure systems to complex networks [8, 9]. Ever since then, graph theory has provided a new perspective on the study of power systems. Furthermore, concepts of resilience and robustness in scale-free networks have been applied to both power grids and computer networks [10]. They have proved to be a good approach in order to understand the grid's dynamic behaviors that generally lead to cascade effect failures. As a result, when applied to power systems, structural vulnerability analysis focuses on the performance of the complex network in events of their systematic disruptions, either randomly (*tolerance against errors or faults*) or deliberately (*tolerance against attacks*).

The way the nodes are removed from a scale-free network depends upon graph statistical measures. Some studies suggest

[1] Faculty of Engineering, Fundación Universitaria Luis Amigó, Medellín, Colombia (e-mail: gcorreah@une.net.co).

[2] Department of Electrical Engineering, Universidad de Zaragoza, 50018, Zaragoza, Spain (e-mail:jmyusta@unizar.es).

node removal according to their *degree of connection* [4, 10-12]. Other studies suggest node removal based on their *betweenness* [13-16]. Besides considering random node removals or degree-based node attacks, some authors also propose recalculation of degree distribution at each iteration, after every node disruption [4, 12].

In this paper, the authors investigate the effectiveness of scale-free graph statistic measures as an accurate methodology to assess vulnerability of power transmission grids. This is done through comparison of operational indexes in classic AC power flow techniques versus scale-free graph statistics, by assessing vulnerability to both random error and deliberate attack network tolerance. This shows the validation of a faster method than AC power flow, as it is graph theory modeling, which also may provide acceptable results for understanding the complex nature of electric critical infrastructure and their response against risks and threats that may disrupt the normal operation of the power grid.

The paper is organized as follows: Section II introduces the scale-free topology equivalence for power networks, and describes appropriate indexes to measure power grid disruption events. Section III proposes an algorithm for risks scenarios of random error and deliberate attack vulnerability assessment applied to some illustrative examples based upon IEEE test power networks, using N-1 contingency analysis and N-t dynamic simulation model for cascade failure events. Section IV shows the results of the proposed model on selected IEEE testing networks (30, 118, 300 bus). Discussion and conclusions on practical applicability of scale-free graph modeling under risk scenarios is also provided at the end of the paper.

II. DEFINITIONS ON INDEXES FOR TOPOLOGICAL REPRESENTATION OF THE POWER NETWORK

An intuitive topological representation of a power network would consist in a set of assets like generators, substations, loads, transformers, and electric towers, representing graph nodes, whereas transmission lines and cables represent graph edges. Mathematically, a graph corresponds to an adjacency matrix composed by pair of sets $G = (N, E)$, where $N(G)$ is the set of nodes and $E(G)$ is the set of edges. An edge correspond to a connection between pairs of nodes with the form (i, j) such that $i, j \in E$. For simplicity, the link (i, j) is denoted as ij. An edge connecting two nodes denotes $G_{ij}= 1$, corresponding to the location of a pair of nodes, and $G_{ij} = 0$ otherwise. Studying the properties of a graph is equivalent to studying the properties of the adjacency matrix.

The *nodal degree* **(k_i)** is the set of converging edges ($\boldsymbol{E}_i$) to a particular node ($\boldsymbol{N}_i$):

$$k_i = |N_i| \qquad (1)$$

where:

$$N_i = \{j \in \boldsymbol{N} \mid \{i; j\} \in \boldsymbol{E}\} \qquad (2)$$

This property describes some graph's statistical measures, for example, its robustness and its connectivity.

In a scale-free graph a few nodes are highly connected, meaning that they have a large number of edges to other nodes, although the degree of connection throughout the graph is quite low. Such graphs are closer to reality, since the network will grow preferentially on the basis of the nodes of greater connectivity (preferential attachment) [8, 10].

Table 1 shows the proposed topological representation of different IEEE testing networks, including their traditional equivalence (which only considers buses and edges) contrasted with the proposed representation.

Plant generators and loads are connected through a single link to the system. This means that their nodal degree is $k = 1$. Even though representation of power systems as scale-free networks has been well documented [17-20], the topological representation herein proposed looks for a representation of the power system as a scale-free graph, where the set of towers that hold power lines are also considered as a node in the graph. Similar consideration is made for the set of transformers. Capacitors, generators and loads also constitute nodes in the network with very low connection degree, whereas buses have the largest number of connections in the scale-free graph. It is reasonable to affirm that the proposed topology in Table 1 for the IEEE testing networks can be modeled as a scale-free graph considering the transformers and transmission towers to be the nodes of the system. A more detailed explanation on this approach can be consulted in [9, 21].

A. Graph Theory Performing Indexes

Graph geodesic distances describe how compact a network is. The shortest geodesic distance between two nodes d_{ij} is calculated by counting the minimum number of nodes in the path between a pair of nodes i and j. The graph average distance $\bar{d}$ is calculated as a function of all geodesic distances d_{ij} and the total number of nodes N [15], as shown in Eq. (3):

$$\bar{d} = \frac{1}{N \cdot (N-1)} \sum_{i \neq j} d_{ij} \qquad (3)$$

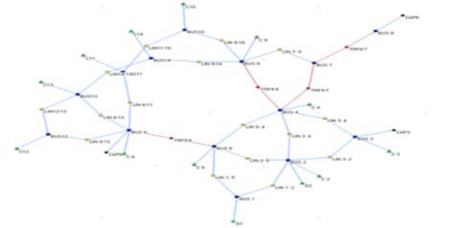
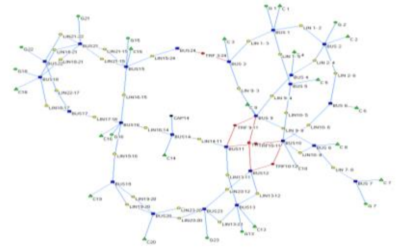
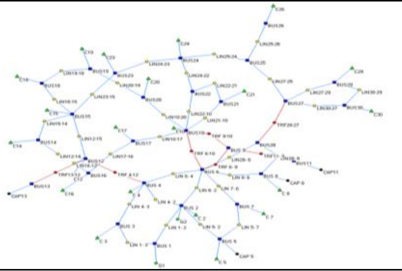
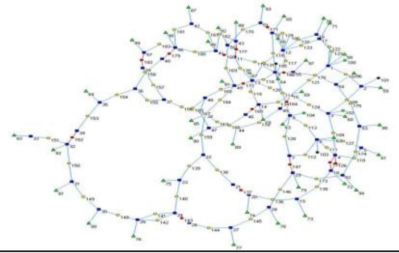
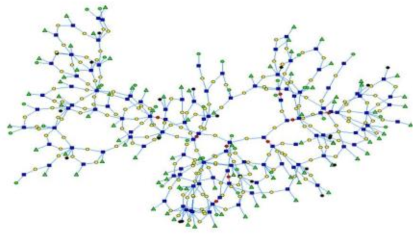
The most common procedures in the calculation of the geodesic distances are Dijkstra, Bellman-Ford, Floyd-Warshall and Johnson algorithms [22].

An equivalent index may be intended to quantify how efficiently flows can be exchanged within a network. Therefore, the *efficiency* between a pair of nodes e_{ij} is defined as the inverse of their geodesic distance. If there were no connection between two nodes, $d_{ij} \approx \infty$, $e_{ij} = 0$ [11, 13, 23]. From Eq. (3) the *Average Efficiency* ($\bar{e}$) is formulated as:

$$\bar{e} = \frac{1}{N \cdot (N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \qquad (4)$$

From Eq. (4) we define the *geodesic vulnerability* $\bar{v}$ as a parameter that measures the functionality of a network when subjected to a contingency as shown in Eq. (5), with regard to its steady condition (base case).

TABLE 1
TOPOLOGIC REPRESENTATION OF IEEE TESTING NETWORKS AS SCALE-FREE GRAPHS.

IEEE Test Network	Scale-free graph equivalence	Scale-free graph representation
14 buses: 16 lines, 4 transformers, 11 loads, 1 generator, 1 slack, 3 capacitors.	50 nodes, 56 links	
24 buses: 33 lines, 5 transformers, 17 loads, 9 generators, 1 slack, 1 capacitor.	90 nodes, 104 links	
30 buses: 34 lines, 7 transformers, 21 loads, 1 generator, 1 slack, 4 capacitors.	98 nodes, 109 links	
57 buses: 65 lines, 15 transformers, 42 loads, 3 generators, 1 slack, 3 capacitors.	186 nodes, 209 links	
118 buses: 177 lines, 9 transformers, 91 loads, 33 generators, 1 slack, 20 capacitors.	449 nodes, 517 links	

$$\bar{v} = 1 - \frac{\sum_{i\neq j}\left(\frac{1}{d_{ij}^{LC}}\right)}{\sum_{i\neq j}\left(\frac{1}{d_{ij}^{BC}}\right)} \qquad (5)$$

d_{ij} ^{LC}: shortest path between a pair of nodes of the scale-free graph, after a node removal in each iteration.

d_{ij} ^{BC}: shortest path between a pair of nodes of the scale-free graph at base case.

N: total number of nodes in the initial scale-free graph

Index $\bar{v}$ in Eq. (5) varies between zero and one. The higher *vulnerability* index value $\bar{v}$, the greater impact on the network due to congestion problems and cascading failures, as some geodesic paths get disrupted.

The *impact on the connectivity of the network S* can be easily calculated at each iteration by determining the number of nodes that are connected to the scale-free graph:

$$S = 1 - \frac{N^{LC}}{N} \qquad (6)$$

N^{LC}: amount of nodes connected on the remaining scale-free graph, after a node removal in each iteration.

N: total number of nodes in the scale-free graph (base case)

The functionality and performing of the network are then quantified by *impact on the connectivity* (6) and *geodesic vulnerability* (5) measured as function of the *fraction of* *removed nodes* (*f*).

B. Power Flow Performing Index

Although structural vulnerability analysis can be performed through evolution of indexes in Eq. (5) and (6) that describe graph's error and attack tolerance, it is not clear that this evaluation method may be reliable, since electrical values are not involved into these calculations. Therefore, classic power flow indexes need to be considered in order to compare the effectiveness of graph theory measurements. The calculation of steady state power and voltages in each bus of the grid may be performed through Standard Power Flow (SPF) routine [5], corresponding to nonlinear equations are solved iteratively using Newton's Method [24].

Power flow indexes that appear in literature are mainly used to determine the impact of N–1 contingencies in the power grid: Maximum Load Conditions [6], Comprehensive Information System [25], Power System Loss [26], and Index of Severity [5].

A good measure of functionality for the power grid network would be the consumer loads that remain connected to the electrical service after a disruption event. An intuitive power flow index to understand evolution of cascade failure events corresponds to *Power Load Shedding (PLS)* [27, 28].

$$PLS = 1 - \frac{\sum_{i} \sqrt{\left(\left(P_{Di}^{LC}\right)^{2} + \left(Q_{Di}^{LC}\right)^{2}\right)}}{\sum_{i} \sqrt{\left(\left(P_{Di}^{BC}\right)^{2} + \left(Q_{Di}^{BC}\right)^{2}\right)}} \qquad (7)$$

${P_{Di}}^{LC}$: active power load that remains electrically connected, after a node removal in each iteration.

${Q_{Di}}^{LC}$: reactive power load that remains electrically connected, after a node removal in each iteration.

${P_{Di}}^{BC}$: active power load at base case.

${Q_{Di}}^{BC}$: reactive power load at base case.

PLS in Eq. (7) is calculated as a percentage of the load that is shed at each node removal iteration, in order to avoid cascade outage. Its range varies between zero and one. The higher PLS index value, the greater impact on energy not supplied.

III. ALGORITHM DESIGN FOR VULNERABILITY ASSESSMENT ON THE POWER GRID UNDER RISK SCENARIOS

This section explains the procedure for computational analysis of structural vulnerability in power networks, considering a first approach through N-1 contingency analysis and extending it to random errors and deliberate attacks tolerance with an N-t dynamic cascade failure simulation model. At this point, graph theory techniques become a useful tool since they show higher correlation to power flow indicators.

A. N-1 Contingency Analysis Model and N-t Dynamic Failure Model Simulation

Cascade failure events may be estimated from a power grid that operates under steady-state conditions (base case). Network cascade failure events are determined by the disruption of the nodes according to the removal strategy. A node disruption implies the elimination of all edges connected to it and therefore, its corresponding connected links also disappear.

A first approach to determine the most critical assets on the power grid, consists on N-1 contingency analysis, which results may provide information about the nodes that require the most attention for their protection, due to the effects on throughout the network when they are disrupted from the system [6].

The described technique can be extended to a dynamic simulation model, which is equivalent to successive contingency N-1 and N-*t* iterations over a constantly changing topology structure. Since power flows can only be performed based upon the existence of the reference (slack) bus generator, removal of nodes are handled around the reference slack generator bus (this means that slack generator must always be present in the network and cannot be removed). The algorithm has been designed to measure parameters only with components that remain connected to the network as it disintegrates. Generators outages are considered in random failures routines, since generators are treated as nodes in the scale-free graph that may be subject to disruptions.

The proposed N-t cascade failure dynamic model takes into account two different scenarios in which multiple samplings are performed for random error phenomena, unlike deliberate attacks that run only one sample [9]. Since error distribution is highly asymmetric in N-t analysis, we propose taking the statement of the *Central Limit Theorem*, which suggests that a sufficiently large number of independent random values will be approximately normally distributed, but if the sample size is relatively large. Thus, it is possible to conclude that the approximation is good enough when more than 30 samples have been collected [29].

The described algorithm has been implemented in *Matlab*®. Its programming takes into account power flow algorithms provided by the tool *PSAT* (Power System Analysis Toolbox) [30, 31]. Furthermore, the script incorporates features of the *MatlabBGL* toolbox for graph theory [32]. Geodesic distances are calculated through shortest-paths Bellman-Ford algorithm [22].

B. Algorithm Implementation and Computing Time

Realistic scenarios have been applied in order to prove the usefulness of graph theory models, especially for N-t contingency analysis. They correspond to IEEE Power Flow Test Cases of 14, 24, 30, 57, 118 and 300 buses, whose iterative processes are shown in Table 2. The data can be accessed through flat text files [33].

In N-t contingency analysis, the constant reconfiguration of the network, after each successive node removal, may turn out in divergences on the power flow results when executing a *Standard Power Flow* (SPF) routine.

TABLE 2
SUMMARY OF ITERATIVE PROCESSES FOR N-*T* DYNAMIC SIMULATION MODEL ON IEEE TEST NETWORKS.

Disruption strategy	IEEE Network	N° samples	Iterations per sample	Execution time (min)
Random	14 buses	35	33	35’
Random	24 buses	35	62	80’
Random	30 buses	35	67	90’
Random	57 buses	35	120	570’
Random	118 buses	35	293	1140’
Random	300 buses	35	635	3150’
Deliberate	14 buses	1	10	1’
Deliberate	24 buses	1	18	2’
Deliberate	30 buses	1	26	2’
Deliberate	57 buses	1	42	4’
Deliberate	118 buses	1	107	12’
Deliberate	300 buses	1	213	21’

In cases the SPF routine does not converge, a convenient PSAT feature provides a *Continuation Power Flow* (CPF) routine [24], an efficient method for solving ill-conditioned cases. Thus, it is possible to calculate the vulnerability of the network by evaluating the evolution of the indexes from Eq. (5), (6) and (7) on each iteration.

Other PSAT feature allows identification over which buses are electrically isolated (not connected to the slack generator). Each iteration step takes into account the existence of these isolated buses in order to calculate the impact on the connectivity of the network by index *S* in Eq. (6).

Table 2 shows the iterations required to perform de proposed dynamic cascade failure model, for N-t contingency analysis. The *Matlab*® program completes its execution until it may not be possible to remove more nodes from the network, either because all nodes are isolated or because there are no more electric circuits to perform power flows routines.

The implementation of the algorithm presented in this section was performed on a personal computer with Matlab® version 7.2, and hardware corresponding to an Intel Core Duo 2.33 GHz processor, and 2GB of RAM memory.

Table 2 shows some statistics relevant to the simulation of deliberate attacks and random errors on IEEE networks. Note that the number of iterations per sample is greater in random disruptions than node degree based attacks.

IV. SIMULATION RESULTS ON IEEE TEST NETWORKS

The results of the simulation can be seen in Fig. 1 for N-1 contingency analysis, whereas Fig. 2 show the results for the N-t dynamic model simulation for random error node removal strategy, and Fig. 3 for deliberate attack node removal strategy. In order to keep the illustrations clear in both figures, the results of only three bus networks have been plotted, corresponding to IEEE testing networks of 30, 114 and 300 buses (considered a good representation of the methodology).

The plotted results correspond to the grid response in N-1 contingency analysis, as well as the index evolution during cascade failures due to node disruptions in the N-t dynamic model. A comparison can be accomplished between the electrical *PLS* parameter of Eq. (7), contrasted with those indexes applied on complex networks, *S*, $\overline{v}$, in Eq. (5) and (6). The scales for all indexes are indicated in per-unit values, measured as function of the *fraction of removed nodes f*.

A. N-1 Contingency Analysis

The study of N-1 contingency analysis refers to those events that occur when a network element is removed or taken out of service due to unforeseen circumstances. For every grid’s disruption, power flows are redistributed throughout the network and voltage bars change. As a result, there may be overloaded lines and transformers [5].

Fig. 1 shows the results for power load shedding index (Eq. 7), compared to geodesic vulnerability and connectivity index (Eq. 5 and Eq. 6) for N-1 contingency analysis in IEEE test networks of 30, 118 and 300 buses. The analysis is performed through successive execution of Standard Power Flow Newton-Raphson algorithm [5, 24, 30]. In Fig. 1 the x-axis refers to the node name failed on an N-1 contingency (unfortunately it is not possible to display all of those names).

As explained in Eq. (7) the contingency results are compared to the base case, i.e., the network operating under normal conditions. Hence, N-1 contingency analysis allows the identification of the most vulnerable nodes in the power network, which is the first step for decision-making in critical infrastructure protection.

Graph theory indexes $\overline{v}$ in Eq. (5) and *S* in Eq. (6) show that in all cases the greatest impact on the network occurs through the removal or isolation of nodes with a higher degree of connectivity, especially buses, while with less nodes (such as generators, capacitors and loads) have a minimal impact on both connectivity and geodesic vulnerability indexes. Therefore, the most critical nodes may be identified as those whose removal leads to the biggest impact on either connectivity or vulnerability.

However, N-1 contingency analysis provides a more realistic scenario when calculating *PLS* index of Eq. (7), since it relates to the power grid operating parameters. In the particular case of the IEEE 30 bus network, composed by 98 nodes, the isolation of its generators in either node 5 or node 43 implies the decoupling of system loads, configuring a blackout event that affects near 30% of the power grid.

In IEEE 118 bus test network, even though there are no nodes that lead to a total breakdown, in few cases (nodes 60 and 170) the *PLS* index may rise up to 7.5% on the system load in the power grid.

Similarly, in the IEEE 300 bus test network, composed by 978 nodes, there are 18 nodes that may impact the whole system. In this particular case, N-1 contingency analysis allows the identification of 7 buses as most critical nodes, as well as 4 transformers nodes, 3distribution lines, and 4 active power generators. Removing such nodes may lead to a total collapse of the system (*PLS* ≈ 100%).

B. Dynamic N-t model for random error tolerance

Complex networks may boast remarkable tolerance against faults and attacks, usually attributed to redundant paths of their infrastructures.

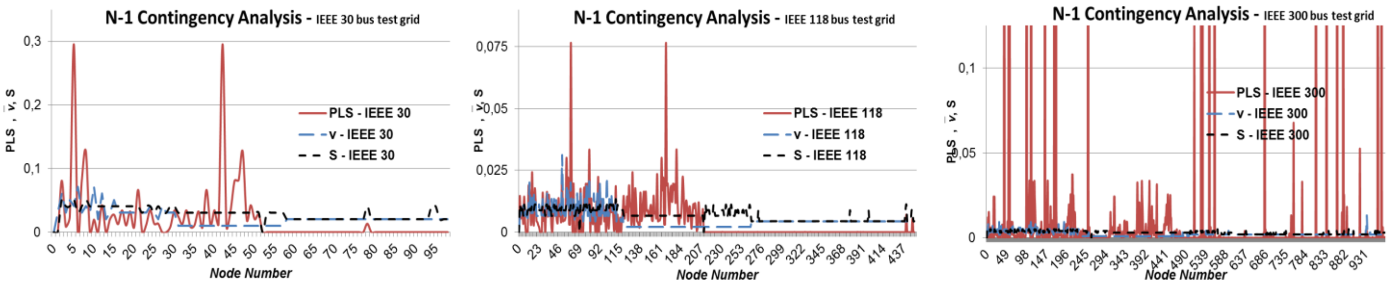


Fig. 1: N-1 Contingency Analysis in IEEE Test Networks

A network may become a target in different risks scenarios either by deliberate attacks or random errors. This fact can be studied assuming that from a connected scale-free graph of *N* nodes, there might be a fraction *f* of nodes that may be removed.

This section compares vulnerability results using both graph theory indexes and classic power flow indicators, in several realistic scenarios. In this section, nodes removal strategy is related to random perturbations causing the failure of some nodes (natural disasters, equipment faults, procedure failures), thus the first mechanism to be studied is the removal of nodes randomly selected.

The numerical simulations in Fig. 2 indicate that scale-free networks display a topological robustness against random node failures (since low degree nodes are far more abundant than nodes with high degree).

From Fig. 2, random errors risk scenarios cause total collapse of the network service (blackout) after the removal of 20% of the nodes. The *PLS* index evolution shows that the 118 bus test network is the most vulnerable (collapses completely by the removal of 20% of the nodes). On the other hand, disconnection of 90% of loads is achieved on 35% node removal at 30 and 300 bus test-networks.

The comparison between results of graph connectivity index *S* and *PLS* in Fig. 2 shows that nodal connectivity is not proportionally related to the grid's electrical condition. This means that *PLS* electrical index evolves at different bias rate than impact on connectivity graph index *S*.

Unlike the geodesic path distance $\bar{d}$ (4), the geodesic vulnerability $\bar{v}$ (6) has proved to be a well-defined index. The use of the average geodesic vulnerability $\bar{v}$, showed in Fig. 2, does really facilitate comparison of results between classic electrical and topological indicators, since the results of the vulnerability parameter $\bar{v}$ completely agree with the forecasts obtained through electric index *PLS* from Eq. (7).

This can be contrasted by comparing *PLS* and $\bar{v}$ for events of random error disruptions (Fig. 2) which shows that the 118 bus test-network is the most vulnerable, followed by 30 and 300 bus test-networks.

C. Dynamic N-t model for deliberate attack tolerance

Other realistic risks scenario representation refers to deliberate attacks, consisting on those risks caused by antagonist attackers on the power grid, i.e. emulating an intentional attack on the network.

This second removal strategy, in which the most highly connected nodes are removed at each iteration, relates to the most damaging scenario to the integrity of the system [34]. In the case of an intentional attack, when the nodes with the highest number of edges are targeted, the network breaks down faster than in the case of random node removal.

The *PLS* index evolution in Fig. 3 shows that, under deliberate attacks, the removal of only 2% of the nodes in the plotted bus-test networks causes a total blackout (100% of loads have no power supply). This demonstrates the reason why scale-free networks may be fragile to intentional attacks, since the removal of the nodes with higher connectivity has a dramatic disruptive effect on the network, and this fact is can be observed in Fig. 3.

Moreover, in Fig. 3 is noteworthy a slight recovery of the *PLS* index when removed about 15% of the nodes in the IEEE 30 bus test network. This is explained because there is an electrically connected circuit around the slack generator, which allows the circulation of power flows. Nonetheless, the iteration that follows these cascading failures causes a new collapse in the network.

Taking into account the results showed in Fig. 2 and Fig. 3, the networks are completely isolated when removing respectively 25% and 70% of nodes at deliberate attack and random error removal strategies.

Results for deliberate attack disruptions (Fig. 3) shows the existence of a better correlation between geodesic vulnerability index $\bar{v}$ (5) and *PLS* parameter (7), than connectivity index *S* (6).

When the geodesic vulnerability $\bar{v}$ has a value close to one implies a greater fragmentation of the network, and hence flows between generators and loads pass through more paths, which means less resilience and less robustness to cascading failures. This is consistent with isolation of consumer loads out of the system in disruption events.

V. DISCUSSION

Although the use of graph theory is insufficient to determine the power transfer capacity between generators and loads, the methodology allows an understanding of general mechanisms governing complex networks.

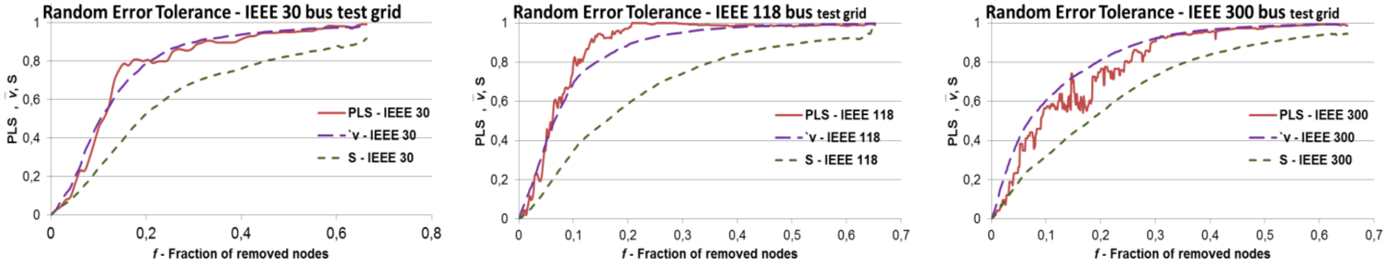


Fig. 2: Results for graph theory indexes and power flow parameters for random errors in IEEE test networks, after averaging 35 samples in N-t dynamic model. Nodes are removed randomly

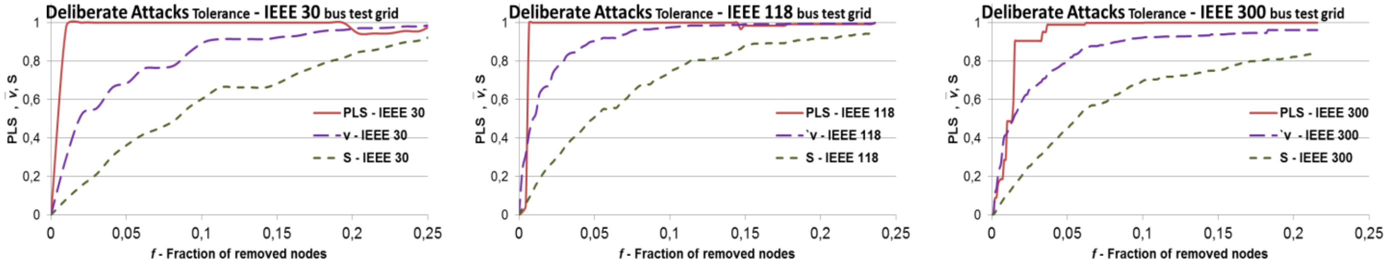


Fig. 3: Results for graph theory indexes and power flow parameters for deliberate attacks in IEEE test networks in N-t dynamic model. Nodes are removed in decreasing degree order

A practical measure to determine dependence between electric *PLS* index and graph theory (S, $\bar{v}$) is the *Pearson correlation coefficient* ρ, which is obtained via division of the covariance of two variables by the product of their standard deviations σ [29]:

$$\rho_1 = \frac{\mathrm{cov}(PLS,S)}{\sigma_{PLS}\sigma_S}\ ;\ \rho_2 = \frac{\mathrm{cov}(PLS,v)}{\sigma_{PLS}\sigma_v} \qquad (8)$$

ρ_1: Correlation between index *PLS* and connectivity index *S*

ρ_2: Correlation between index *PLS* and geodesic vulnerability index $\bar{v}$.

Table 3 reveals the results for correlations between indexes, calculated from (8).

In random error node removal strategy, the Pearson correlation ρ_2 is closer to +1, which implies a positive linear relationship between *PLS* index and geodesic vulnerability $\bar{v}$. According to this comparison, $\bar{v}$ parameter would also be useful to determine the disconnected electric load P_{Di} out of the power grid during cascade failures events.

The comparison for connectivity index *S* shows low correlation ρ_1 with electrical index *PLS*. This means that it should not be considered as a precise indicator to assess the vulnerability of electric networks. Therefore, this correlation confirms the comparisons of the bias trend between index $\bar{v}$ (5) and *PLS* (7) showed in Fig. 2 and Fig. 3

In deliberate attacks, correlation ρ_2 for parameter $\bar{v}$ is weaker than ρ_1 for index *S*. Thus, average geodesic vulnerability $\bar{v}$ is still of great interest to make comparisons between different power systems and determine which one is the most vulnerable.

TABLE 3
PEARSON CORRELATION BETWEEN ELECTRIC PARAMETER *PLS* AND GRAPH THEORY INDEXES *S* AND $\bar{v}$

Disruption strategy	IEEE Network	ρ_1	ρ_2
Random	14 buses	0.9485	0.9903
Random	24 buses	0.9532	0.9826
Random	30 buses	0.9503	0.9920
Random	57 buses	0.8047	0.9099
Random	118 buses	0.8584	0.9828
Random	300 buses	0.9743	0.9868
Deliberate	14 buses	0.8566	0.9491
Deliberate	24 buses	0.8268	0.8780
Deliberate	30 buses	0.3941	0.6586
Deliberate	57 buses	0.6266	0.7897
Deliberate	118 buses	0.4264	0.7321
Deliberate	300 buses	0.7130	0.9012

VI. CONCLUSION

A new methodology has been proposed to compare numerical indexes of graph theory (S, $\bar{v}$) and power flow techniques (*PLS*) in order to assess vulnerability for any power grid. It has been demonstrated the usefulness of combining power flow models and scale-free graphs measurements, making it possible to substitute time-consuming computational tools (as classic power flow routines) with more efficient techniques (as graph theory parameters) to evaluate structural vulnerability of any electric network, depending on the events that trigger cascade failures.

It has been showed the convenience of N-1 contingency analysis to identify the most vulnerable nodes in the power system, which is the first step for decision-making in the protection of these assets.

It has been proved that scale-free graphs indexes can be used to qualify the vulnerability of a power grid topology compared to another one, especially for N-t dynamic cascade failure events.

Hence, this feature is a great advantage since it is not necessary to run power flow routines to compare the vulnerability among different power systems. This result also demonstrates the computational efficiency of proposed method.

VII. REFERENCES

[1] CEU, "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection," in *Council Directive December/2008*, Directive 114, Council of the European Communities. Brussels (Belgium): *Official Journal of the European Communities*, 2008, 75p

[2] NIPP, "National Infrastructure Protection Plan", Washington DC (USA): *U.S. Department of Home Security*, 2009, 175 p.

[3] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy*, vol. 39, pp. pp. 6100-6119, 2011.

[4] Å. J. Holmgren, "Using Graph Models to Analyze the Vulnerability of Electric Power Networks," *Risk Analysis*, vol. 26, pp. 955-969, 2006.

[5] A. Gómez-Expósito, "Análisis y operación de sistemas de energía eléctrica". Madrid (Spain) *McGraw-Hill*, 2002.

[6] F. Milano, "Pricing System Security in Electricity Market Models with Inclusion of Voltage Stability Constraints," *Doctoral Thesis in Electrical Engineering*, University of Genova (Italy), 218p, 2003 .

[7] C. Qiming and J. D. McCalley, "Identifying high risk N-k contingencies for online security assessment," *Power Systems, IEEE Transactions on*, vol. 20, pp. 823-834, 2005.

[8] A.-L. Barabási and R. Albert, "Emergence of Scaling in Random Networks," *Science*, vol. 286, pp. 509-512, 1999.

[9] G. J. Correa and J. M. Yusta, "Grid vulnerability analysis based on scale-free graphs versus power flow models," Electric Power Systems Research, vol. 101, pp. 71-79, 2013.

[10] R. Albert and L. Barabási, "Statistical mechanics of complex networks," *Review Modern Physics*, vol. 74, pp. 47-97, 2002.

[11] A. Motter and Y. Lai, "Cascade-based attacks on complex networks" *Physical Review E*, vol. 66, pp. 065-102, 2002.

[12] E. Jelenius, "Graph Models of Infrastructures and the Robustness of Power Grids," *Master Thesis. Master of Science in Physics Engineering*, Royal Institute of Technology (KTH). Stockholm (Sweden) 89p, 2004 .

[13] G. Chen, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 389, pp. 595-603, 2010.

[14] G. Chen, Z. Y. Dong, D. J. Hill, and G. H. Zhang, "An improved model for structural vulnerability analysis of power networks," *Physica A: Statistical Mechanics and its Applications*, vol. 388, pp. 4259-4266, 2009.

[15] J. Johansson, "Risk and Vulnerability Analysis of Interdependent Technical Infrastructures" *Doctoral Thesis in Industrial Electrical Engineering*, University of Lund (Sweden), 189p, 2010.

[16] K. Wang, B.,H. Zhang, Z. Zhang, X.,G. Yin, and B. Wang, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A: Statistical Mechanics and its Applications*, vol. 390, pp. 4692-4701, 2011.

[17] R. Solé, M. Casals, B. Murtra, and S. Valverde, "Robustness of the European power grids under intentional attack," *Physical Review E*, vol. 77, p. 026102, 2008.

[18] A. Murray, T. Matisziw, and T. Grubesic, "Critical network infrastructure analysis: interdiction and system flow," *Journal of Geographical Systems*, vol. 9, pp. 103-117, 2007.

[19] D. E. Newman, B. Nkei, B. A. Carreras, I. Dobson, V. E. Lynch, and P. Gradney, "CASCADE: Risk Assessment in Complex Interacting Infrastructure Systems," in *IEEE 38th Conference on System Sciences*, Big Island Hawaii, (EEUU), 2005.

[20] A. Holmgren, "Quantitative Vulnerability Analysis of Electric Power Networks," in *Doctoral Thesis in Safety Analysis* Royal Institute of Technology (KTH). Stockholm (Sweden), 47p, 2007.

[21] G. Correa, "Identificación y Evaluación de Amenazas a la Seguridad de Infraestructuras de Transporte y Distribución de Electricidad," *Doctoral Thesis in Renewable Energy and Energetic Efficiency*, Universidad de Zaragoza, Zaragoza (Spain), 238p, 2012

[22] J. L. Gross and J. Yellen, *Handbook of graph theory*: CRC Press, 2004.

[23] P. Crucitti, V. Latora, M. Marchiori, A. Rapisarda, "Error and attack tolerance of complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 340, pp. 388-394, 2004.

[24] F. Milano, "Continuous Newton's Method for Power Flow Analysis," *Power Systems, IEEE Transactions on*, vol. 24, pp. 50-57, 2009.

[25] A. M. A. Haidar, A. Mohamed, and A. Hussain, "Vulnerability Assessment of a Large Sized Power System Using Radial Basis Function Neural Network," in *5th Student Conference on Research and Development, 2007. (SCOReD 2007).* pp. 1-6, 2007.

[26] A. M. A. Haidar, A. Mohamed, A. Hussain, and M. Al-Dabbagh, "Vulnerability assessment and control of large scale interconnected power systems using neural networks and neuro-fuzzy techniques," in *Power Engineering Conference, 2008. AUPEC '08. Australasian Universities*, pp. 1-6, 2008.

[27] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *Power Systems, IEEE Transactions on*, vol. 19, pp. 905-912, 2004.

[28] A. M. A. Haidar, A. Mohamed, A. Hussain, "Vulnerability Assessment of a Large Sized Power System Using a New Index Based on Power System Loss," *European Journal of Scientific Research*, vol. 17, pp. 61-72, 2007.

[29] D. R. Anderson, D. J. Sweeney, T. A. Williams, *Essentials of Statistics for Business and Economics* vol. 6. London, UK: Cengage Learning, 2010.

[30] F. Milano, "An Open Source Power System Analysis Toolbox," *Power Systems, IEEE Transactions*, vol. 20, pp. 1199-1206, 2005.

[31] F. Milano, "PSAT: Power System Analysis Toolbox," Universidad Castilla la Mancha, Ciudad Real (Spain), 2012. [Online] Available: http://www.uclm.es/area/gsee/web/Federico/psat.htm

[32] D. Gleich, "MATLAB_BGL: Graph Theory Toolbox," S. University, Ed. Palo Alto, CA (USA), 2008. [Online] Available: http://www.mathworks.com/matlabcentral/fileexchange/10922

[33] IEEE-Group, "Common Format For Exchange of Solved Load Flow Data," in *Power Apparatus and Systems, IEEE Transactions on*. PAS-92, I. W. Group, Ed. Rosemead, CA (USA): Southern California Edison Company, 1973, pp. 1916-1925. [Online] Available: http://www.ee.washington.edu/research/pstca/

[34] A. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks," *Power Systems, IEEE Transactions on*, vol. 22, pp. 76-84, 2007.

Gabriel J. Correa received the Electrical Engineer degree in 2001, the M.Sc. degree in Computer Science in 2004, from Universidad Nacional de Colombia, Medellín, Colombia, and the Master degree in business administration in 2007 from Universidad San Pablo, Madrid, Spain. He also received the PhD degree in Renewable Energy and Energetic Efficiency from Universidad de Zaragoza, Spain in 2012. He is currently a lecturer and researcher at Faculty of Engineering in Fundación Universitaria Luis Amigó, in Medellín, Colombia, with research interests on distributed generation, power system security analysis and decision-making methodologies.

José M. Yusta received a degree in Industrial Engineering (1994) and a PhD. in Electrical Engineering (2000) from Universidad de Zaragoza, Spain. He is currently a Senior Lecturer at the Department of Electrical Engineering of Universidad de Zaragoza. From 2004 to 2007 he was Vicedean of the Faculty of Engineering at Universidad de Zaragoza. His research interests include technical and economic issues in electric distribution systems, power systems security analysis, and demand side of electricity markets.