Geodesic Vulnerability Index for Contingency Analysis in Electric Infrastructures

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

***Abstract*— This technical contribution contains formulation of topological indexes for structural vulnerability assessment in high voltage power grids, based upon the combination of power flow models and scale free graphs measures. Hence, it is possible to analyze risk scenarios according to those events that may result in cascade failures within an electric power system. Technical development of the proposal is carried out upon the study of those random risks and those possible threats of deliberate attacks into the high voltage transmission system. The authors validate the usefulness of graph theory to assess vulnerability into the power grid. This includes the study of those events that trigger cascade failures and consumers disconnections. Moreover, the methodology is applied in order to evaluate the structural vulnerability in high voltage power systems in countries like Colombia and Spain.**

As a result, new tools are provided and incorporated for risk analysis into electric infrastructures, particularly within high voltage power networks.

***Index Terms* —critical infrastructure, vulnerability analysis, cascade failures**

***Resumen*— En esta ponencia se formulan indicadores de vulnerabilidad estructural en redes de transporte de alta tensión, a partir de la combinación de modelos de flujos de carga y medidas de grafos de libre-escala. De esta manera, es posible estudiar los escenarios de riesgos en función de los eventos que pueden desencadenar fallos en cascada dentro de un sistema eléctrico de potencia. La propuesta se desarrolla a partir del estudio de riesgos de tipo aleatorio y las posibles amenazas de ataques deliberados al sistema de transporte de alta tensión. Se demuestra la utilidad de las técnicas de teoría de grafos para analizar las respuestas de los sistemas eléctricos de potencia y evaluar la vulnerabilidad de las redes de transporte. Lo anterior involucra el estudio de los eventos que desencadenan fallos en cascada y desconexión de consumidores. Adicionalmente, se ha realizado una aplicación de la propuesta metodológica para evaluación de vulnerabilidad en los sistemas eléctricos de alta tensión en Colombia y España.**

Como resultado, se aportan nuevos instrumentos para la gestión de riesgos en infraestructuras eléctricas, en particular en redes de transporte en alta tensión.

***Palabras Clave* — infraestructura crítica, análisis de vulnerabilidad, fallos en cascada**

I. INTRODUCTION

This technical contribution proposes a methodology for structural vulnerability assessment in electric power networks in high and medium voltage grids. Studies for vulnerability in power systems are required within the evaluation stage of risk management frameworks for organizations that own or operate electric infrastructures. Such assessments should also include the study of events that may lead to cascade failure events as well as consumer disconnections.

Authors apply a useful methodology as a mechanism for explaining power outages events or blackouts, based upon the use of graph theory. These techniques have arisen as a recent knowledge area in the study of interdependencies within critical infrastructure systems by studying their topology. This leads to evaluation of impacts in networks due to the removal of specific components as well as their consequences for congestion power flow, among others.

Based upon such innovative contribution, in this paper the authors apply a modeling graph theory methodology in order to assess vulnerability in a study case within two countries: Colombia and Spain. Tolerance against random errors and deliberate attacks is evaluated through cascading failure events.

Moreover, an analysis of the effectiveness of expansion investments is performed according to the information established in each country's network planning, especially those aimed at improving the robustness of the system and the grid expansion. The evolution of networks is analysed by focusing only on their topological aspects, caused by node removal. This leads to conclude how vulnerable the networks are when nodes with higher connectivity are targeted, in order to assess their vulnerability under certain risk scenarios.

The purpose of the paper is not to identify weak points of a grid but to compare the relative vulnerability between networks, which may guide decision-making concerning the effectiveness and impact of expansion plans, e.g., providing greater robustness to the electric network (improvement of the mesh and higher degree of connectivity of buses) and their responses in both random risk scenarios and intentional attack threats; this aims to evaluate an existing system, and to be able to follow up changes of the system.

II. GRAPH THEORY APPLIED TO ELECTRIC POWER SYSTEMS

The fields of application of **graph theory**, also known as

[1] [1] Faculty of Engineering, Fundación Universitaria Luis Amigó, Medellín, Colombia (e-mail: Gabriel.correa@amigo.edu.co).

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

complex network theory [1], are characterized by the ease that it provides when performing an abstract representation of a system as a network topology with statistical measures. This leads to evaluate the effects of the changes in topology on the robustness of the system when subjected to different types of attacks and failures.

A. Topology Representation in Power Networks

Electric power networks resemble scale-free graphs [2] which allows to represent most assets that conform the power grid. Some researchers simplify such representation as a complex network where substations are specified as *nodes* and electric lines are sketched as *links* [3-8]. In those cases such approach allows the calculation of cluster measures (triangles) in order to determine the grid's vulnerability.

Fig. 1 shows the proposed topological representation of a 14-bus electric network, compared to the traditional representation (which only considers buses and links). Note that both transformers and electric towers are also taken into account as assets susceptible to be removed due to attacks or errors in the power grid. Thus, the resulting network is constituted by a graph of 50 nodes and 56 links. The topological representation herein proposed looks for a more realistic 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 [9].

In the scale-free graph, when a node is randomly removed, it is very likely to be one of low connectivity degree. In statistical terms, those nodes with less connectivity are the most likely to disrupt.

B. Graph's Geodesic Vulnerability Index

This section presents some statistical measures that describe scale-free graphs in order to analyze the disintegration of networks, their evolution to successive node removal. These indicators constitute the basis to a new *geodesic vulnerability index* which has revealed an equivalence to power load shedding in any electric power grid [8, 9]. The formulation of these indices was established from the definition of the *geodesic distance* $\boldsymbol{d_{ij}}$ concept which describes the shortest distance between two nodes directly, by counting the minimum number of traversing nodes required to join them [10].

Proposing this indicator allows better measurements in networks performance when subjected to contingency events, with regard to its steady condition (base case, previous to incidents). This index also standardizes geodesic efficiency as formulated by [11-13] and permits effective comparisons of successive iterations of cascading failures events [9].

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

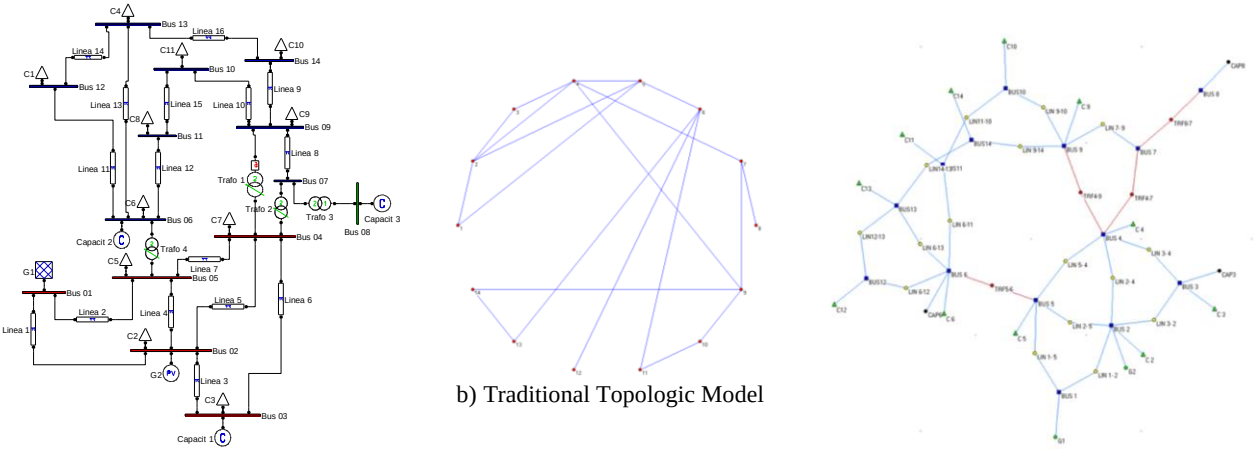
d_{ij}^{LC}: shortest path between a pair of nodes of the scale-free graph, after a node removal in each iteration.

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

Index $\bar{v}$ in (1) 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 and therefore, electric power must flow through more paths. This is consistent with the network's fragmentation and isolation of power loads into the system.

Consequently, it is possible to substitute time-consuming computational tools (as classic power flow routines) with more efficient techniques (as graph theory parameters) in order to evaluate structural vulnerability of any electric network, depending on the events that trigger cascade failures [8].

It has been validated the utility of combining power flow models and scale-free graphs measures both numerically and graphically This fact has been demonstrated in [8, 9] through calculation of the responses in different IEEE networks, by contrasting the results of traditional electrical engineering parameters, referred as portion of disconnected loads or power load shedding [14-17], with geodesic vulnerability $\bar{v}$, and thus allowing comparisons between different power systems to determine which is most vulnerable. This validation implies an important advantage when combining classic methodologies of electric power flows and graph theory measurements in order to study cascade failures [8].



a) Traditional Electric Model

b) Traditional Topologic Model

c) Proposed Topologic Model

Fig. 1. Proposed representation of electric network as a scale-free graph (14-bus network).

III. STUDY CASE IN HIGH VOLTAGE TRANSMISSION NETWORKS

Vulnerability analysis aims to assess power systems conditions and track their evolution when subjected to changes that may generate cascading failures.

A. Definitions on Tolerance to Random Errors and Deliberate Attacks

Concepts on disintegration of scale-free networks were first introduced by [18], whose studies show the performance of complex networks in case of events of systematic node removals at either random events (errors tolerance) or deliberately actions (attacks tolerance). Analyzing contingencies that lead to cascade failures on scale-free networks involves the use of parameters that measure the evolution on the connectivity and functionality of the network. This is performed through successive iterations that represent node removal from the network. Each node removal is associated to a contingency and considered as an iteration step in the network disintegration. A node removal also implies the elimination of all links connected to it, and therefore, the corresponding geodesic paths also disappear.

Removal strategy due to random errors: Tolerance to random errors relates to those damages in infrastructure systems triggered by random contingencies, for example, natural disasters, equipment failures or human error procedures. It has been shown that this kind of cascading failures may cause the collapse of the network service (blackout) when isolated up to 20% of the system nodes [8]

Removal strategy due to deliberate attacks: Tolerance to deliberate attacks relates to targets in the network that are chosen deterministically by the attacker. An extreme scenario, but possible, is one in which the targets of the network are defined as most important, either by their nodal degree [19], or by their betweenness degree [4, 20]. It has been shown that deliberate attacks may cause blackout of the grid when isolated 2% to 5% of the nodes in the system [8].

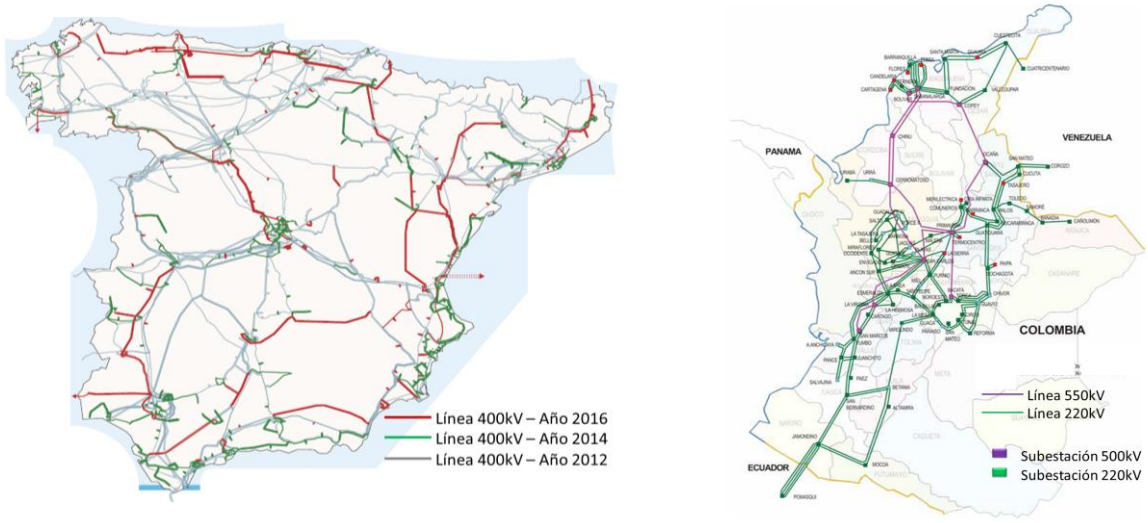
On this section, interconnected power grids are modeled as complex networks (both in Colombia and Spain) whose topology is defined according to their current state. Each network's tolerance is analyzed taking into account the robustness provided by their expansion plans. This study case involves the representation of assets as nodes (substations, electrical towers, transformers, connection bars, etc.) and links (airlines, underground, etc.), regardless of physical distances or the electrical parameters (line impedances, voltage regulation, power loss, etc.) in the network.

Structural vulnerability studies presented in subsequent sections include analysis of network tolerance against random errors, corresponding to the average of 35 samples to describe the cascading failure indices. For these cases, 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 [21].

The algorithm to evaluate tolerance to random errors and deliberate attacks has been implemented in ***Matlab***®. The script incorporates features of the *MatlabBGL* toolbox for graph theory [22]. Geodesic distances are calculated through shortest-paths Bellman-Ford algorithm [10], and therefore calculations of geodesic vulnerability $\bar{v}$ in (1) can be easily determined.

B. Description of Power Networks in Spain 400kV and Colombia 220kV/500kV

In order to accomplish a topological representation of any power system, it would be natural to study the amount of assets that assemble one or another network. However, since information from power systems of any region or country is classified and its access is very limited, it is necessary to validate the methodologies proposed through public data.



a) Equivalent Spanish network 400kV

b) Equivalent Colombian network 220kV/500kV

Fig. 2. High Voltage Interconnected Power Networks in Spain and Colombia [27, 29]

TABLE 1
EVALUATION ON NETWORK PLANNING: BASE CASE (CASE 1), ROBUSTNESS (CASE 2), EXPANSION (CASE 3)

Country	Transmission network	Study Case	Circuit Lenght (Km)	Buses	Nodes	Links
Spain	400 kV	1	19.622	48	190	212
		2		48	198	228
		3		76	278	332
Colombia	220 kV - 500 kV	1	14.300	94	340	380
		2		94	348	403
		3		117	405	471

The Spanish interconnected power system is composed by more than 40.000 kilometers of power lines, over 4,000 positions in substations and about 75.000 MVA transformation capacity [23]. Its assets are managed by *Red Eléctrica de España*, responsible for the operation and maintenance of the high voltage transmission network, both within the Iberian Peninsula, the Balearic Islands and the Canary archipelago. The company has been definitively consolidated as the single system operator in Spain [29].

The effective power capacity installed in the Colombian grid at the end of the year 2011 was 14.420 MW, of which 9.200MW (64%) came from hydropower [24]. Most of the hydroelectric generation centers are located in the Andean region. Thermal generation (gas and coal) are mostly located in the Caribbean region and in the highlands Cundinamarca-Boyacá, where there is also availability of fuel gas and coal for the operation of these generators. Assets in the Colombian interconnected power grid are managed by the company *ISA (Interconexión Eléctrica S.A)*, which is also responsible for their operation and maintenance [27].

Fig. 2 contains a network sketch of high voltage power grids in Spain and Colombia [27, 29]. In order to illustrate the application of the methodology we focus on the 400 kV networks that are represented in the graph showed in **Fig. 2** containing those 48 substations (buses) determined as most important for the power system [25]. Moreover, in the Colombian case some previous works [26] and reports delivered by Colombian government [27] constitute the basis to construct an equivalent scale-free graph of the network topology in 220kV and 500kV, which reports 94 substations (buses).

Structural vulnerability of the transmission system is then evaluated taking into account the current system conditions, possible execution of the government's plans for grid expansion in Spain and Colombia. Basically, we consider the following three case studies: the base case (Case 1), robustness improvement plans by meshing the grid (Case 2), network expansion plans (Case 3), as explained in Table 1

C. Results on Tolerance to Random Errors

We recall that the random errors are associated to those risk scenarios of random nature: natural phenomena, inadvertent human error, random technical failure in equipment and hardware, etc. The resulting curve of geodesic vulnerability index $\bar{v}$ in (1) shows the impact throughout the interconnected network as a function of the isolated nodes in the network (f).

A comparison among the resulting curves of network vulnerability of Spanish and Colombian networks shows that the latter is relatively more vulnerable. In all cases, for the same fraction of interdicted nodes (f) there is greater impact on the vulnerability index of the Colombian network, as shown in

Fig. 3.

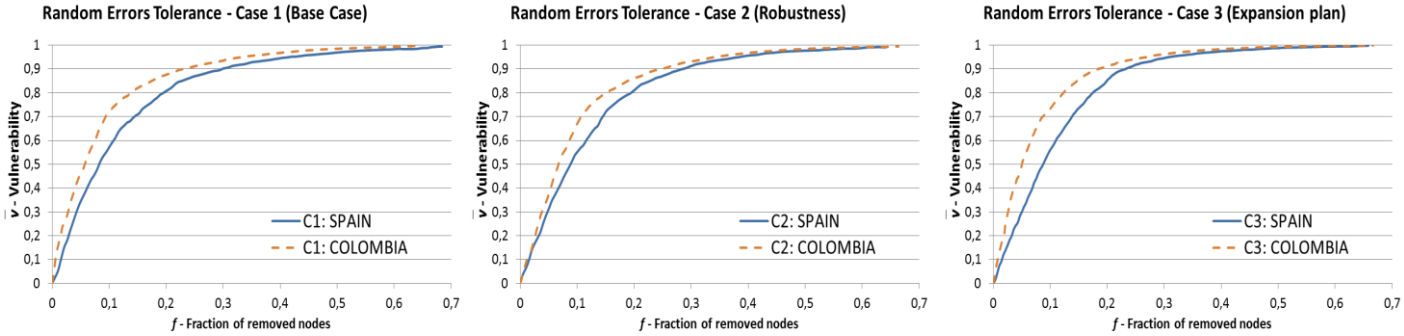


Fig. 3: Geodesic Vulnerability to Random Errors for three study cases in Spain and Colombia

A comparison between the case 1 (base case) and case 2 (robustness strategy) reveals a slight improvement of the network vulnerability in both countries. However, comparisons between case 1 and case 3 (government plans for expansion) show that expanded network is the most vulnerable. One explanation for this has to do with the fact that construction of a less compact network increases the geodesic distance between nodes.

The policies involved into government's plans to build new transmission lines have clear objectives: in Spain they try to attend growing demand, and also to increase the capacity of the electric system in order to transport energy from new renewable generation facilities. Whereas in Colombia those plans seek to provide greater reliability in order to attend growing demand and avoid the isolation of interconnected areas in the event that some disruption event shuts down any region connected to the power grid [28].

An interesting outcome on this response refers to the effectiveness of those plans to make a more robust network. This can be corroborated when comparing case 1 and case 2, in both countries. Reducing vulnerability $\bar{v}$ in the network is evident when increasing the average value of the degree of connection $\bar{k}$, meaning that building a more meshed network with new transmission lines without increasing the number of substations, then a less vulnerable network is expected. Results from Fig. 3 show the remarkable effect of decreased vulnerability $\bar{v}$ in the Colombian network for $f \approx 5\%$ and $f \approx 10\%$, whereas the effect on the Spanish network shows a slight improvement.

D. Results on Tolerance to Deliberate Attacks

The vulnerability calculations for deliberate attacks are performed according to a degree based node removal strategy, starting with those that have the most connections. This way, it is possible to represent risk scenarios that relate to attacks caused by malicious individuals, for instance acts of terrorism, cyber-attacks, acts of vandalism, etc. Fig. 4 shows the results of structural vulnerability calculation in tolerance against deliberate attacks. As exposed in both cases, the disruption of a small number of nodes (f <5%) has very high impact on the entire system ($\bar{v}$ > 85%). This means that an attack addressed against substations with high connectivity would represent a shut-down on almost the whole electric infrastructure and therefore a blackout would be expected through a wide geographical region.

The results of vulnerability in Fig. 4 show a similar behavior in both networks against deliberate attacks, even though their values are slightly higher in the Colombian network than in the Spanish (for the same fraction of removed nodes).

When comparing case 1 (base case) and case 2 (robustness strategy) for both countries, vulnerability curves practically overlap one over other. This means that the strategy of creating a more robust network does not imply greater protection against deliberate attacks in infrastructures.

On the other hand, comparisons between case 1 and case 3 (government plans for expansion), show that the expanded network is more vulnerable to deliberate attacks. When building an expanded network, it becomes less compact, and therefore electric power must flow through more paths under node disruption events. This is explained since removal of nodes with higher connectivity has the effect of dramatically increase the geodesic distance between network nodes.

A comparison between results for both countries in case 1 (base case) and case 2 (robustness) shows no evidence of significant improvements in tolerance against deliberate attacks. Since most of vulnerability values overlap, then the strategy to build a more meshed infrastructure may not be effective enough in deliberate attacks risks.

Particularly in both countries, the expanded network in case 3 is even more vulnerable to deliberate attacks than case 1. This is explained since expansion planning takes into account new connections to substations with high nodal degrees, eg substation Madrid (Spain) substation and Esmeralda (Colombia), both with $k = 10$. Additionally, some other buses with $k > 7$ have wide effect on almost the whole power grid when they are disrupted [29].

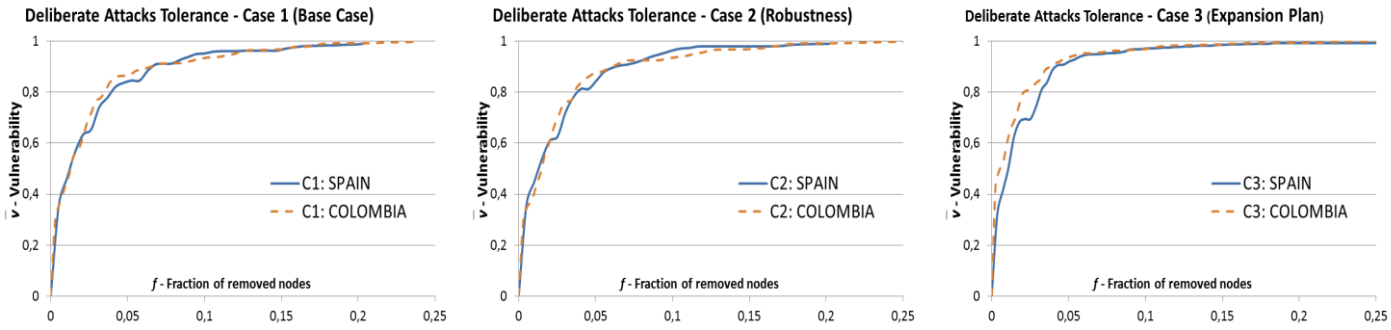


Fig. 4: Geodesic Vulnerability to Deliberate Attacks for three study cases in Spain and Colombia

IV. CONCLUSION

The practical utility of graph theory techniques in power grid systems, relates to the ability of assessing the vulnerability of networks without the need to use electrical parameters. The proposed vulnerability $\bar{v}$ may be a very useful index, whose results may lead to conclusions by associating its tendency to the comparison among different networks and determine which network is the most vulnerable under certain risk scenarios.

The graph model implemented here has some obvious drawbacks. The model has some limitations to incorporate the electric parameters needed to perform a dynamic stability analysis of the power grid. However, although system protection has not been considered, results obtained under the developed research confirm the validation of the use of graph theory to assess relative vulnerability among different networks. By calculating the topological properties of two power grids, we are able to conclude which system is the most vulnerable.

Through the illustrated application in networks of Colombia and Spain, it has been possible to compare the relative vulnerability between two infrastructures, and the impact of their expansion plans as set out by governments. The strategy to provide greater robustness to the networks (improvement of the mesh and higher degree of connectivity of buses), provides slight improvements in the vulnerability of the network against random errors (technical failures, natural disasters, human errors, etc.) however, no improvements are evident in the case of deliberate attacks to the infrastructures.

The numerical simulations 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). But the same heterogeneity makes scale-free networks 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 what we show in the paper when implementing this strategy.

V.REFERENCES

[1] M. E. Newman, "The Structure and Function of Complex Networks" *SIAM Review*, vol. 45, pp. 167-256, 2003.

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

[3] 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.

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

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

[6] 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.

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

[8] G. J. Correa, 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.

[9] 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

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

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

[12] 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.

[13] V. Latora, M. Marchiori, "Efficient Behavior of Small-World Networks" *Physical Review Letters*, vol. 87, 2001.

[14] 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.

[15] V. Donde, V. Lopez, B. Lesieutre, A. Pinar, Y. Chao, J. Meza, "Severe Multiple Contingency Screening in Electric Power Systems," *IEEE Transactions on Power Systems*, vol. 23, pp. 406-417, 2008.

[16] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, W. Magua, K. R. Wierzbicki, "Methodology for identifying near-optimal interdiction strategies for a power transmission system" *Reliability Engineering and System Safety*, vol. 92, pp. 1155-1161, 2007.

[17] 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.

[18] R. Albert, L. Barabási, "Statistical mechanics of complex networks," *Review Modern Physics*, vol. 74, pp. 47-97, 2002.
[19] A. J. Holmgren, E. Jenelius, J. Westin, "Evaluating Strategies for Defending Electric Power Networks Against Antagonistic Attacks," *IEEE Transactions on Power Systems*, vol. 22, pp. 76-84, 2007.
[20] G. Chen, D. Zhao, D. J. Hill, X. Sheng, "Exploring Reliable Strategies for Defending Power Systems Against Targeted Attacks," *IEEE Transactions on Power Systems*, vol. 26, pp. 1000-1009, 2011.
[21] D. R. Anderson, D. J. Sweeney, T. A. Williams, *Essentials of Statistics for Business and Economics* vol. 6. London, UK: Cengage Learning, 2010.
[22] D. Gleich, "MATLAB_BGL: Graph Theory Toolbox," S. University, Ed. Palo Alto, CA (USA), 2008. [Online] Available: http://www.mathworks.com/matlabcentral/fileexchange/10922
[23] REE, El sistema de transporte eléctrico español, Madrid (Spain), *Red Eléctrica de España S.A*, 28p, 2011
[24] XM, Descripción del Sistema Eléctrico Colombiano, Medellín (Colombia), *Expertos en Mercados S.A*, 2012.
[25] REE, Mapas de la red eléctrica de transporte, Madrid (Spain), *Red Eléctrica de España S.A*, 2012
[26] O. Buitrago, D. Tauta, "Análisis del sistema de transmisión nacional de energía colombiano desde el punto de vista de redes complejas", *Bachelor Thesis in Electrical Engineering*, Universidad Nacional de Colombia, Bogotá (Colombia), 85p, 2008.
[27] UPME, Plan de Expansión de referencia Generación - Transmisión 2012-2024, Bogotá (Colombia), *Ministerio de Minas y Energía de Colombia*, 2012.
[28] J. M. Yusta, G. J. Correa, R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy*, vol. 39, pp. 6100-6119, 2011.
[29] MINETUR, "Planificación de los sectores de Electricidad y Gas: Desarrollo de las redes de transporte 2008-2016 en España", Madrid (Spain), *Ministerio de Industria, Turismo y Comercio de España*, 2008.

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.