Energy Conversion and Management 77 (2014) 408–418

Contents lists available at ScienceDirect

Energy Conversion and Management

journal homepage: www.elsevier.com/locate/enconman

Structural vulnerability in transmission systems: Cases of Colombia and Spain

Gabriel J. Correa [a], José M. Yusta [b,*]

[a] Faculty of Engineering, Fundación Universitaria Luis Amigó, Medellín, Colombia
[b] Department of Electrical Engineering, Universidad de Zaragoza, Zaragoza, Spain

ARTICLE INFO

Article history:
Received 17 June 2013
Accepted 1 October 2013

Keywords:
Critical infrastructure
Vulnerability analysis
Network topology
Risk managing

ABSTRACT

In this paper the authors apply methodological strategies for the structural vulnerability assessment in high voltage power networks based upon the combination of power flow models and scale-free graph statistic indexes. Thus, it is possible to study risk scenarios based on events that may trigger cascading failures within a power system. The usefulness of graph theory techniques has been validated on previous works of the authors, and may be applied in analysis of the vulnerability of different power electric networks. A case study for vulnerability analysis is carried out through methodologies that allow comparison on random error and deliberate attack tolerance evaluation in transmission electric systems from countries like Colombia and Spain. Such vulnerability assessment methodology takes into account the current conditions of the power networks (base case), as well as the impact of expansion plans into infrastructures as defined by their governments. Consequently, the authors show the advantage on the use of graph theory based techniques for vulnerability analysis of electrical power systems.

1. Introduction

State governments nowadays consider security of supply as one of the principal objectives within their energy policies, involving institutional efforts on the protection of homeland security, economic activities, public health, etc. This fact evidences the close relationship between global security of electric infrastructures with other critical infrastructure sectors of the economy [1,2]. This concern has been addressed by both European Commission and US Homeland Security Department regarding the security of countries' infrastructures, as a response against new international threats. In 2008 the European Council adopted Directive 2008/114/CE [3], which gave rise to the "European Programme for Critical Infrastructure Protection (EPCIP)". In 2009, the National Infrastructure Protection Plan (NIPP) [4] was launched in the United States, following the release of several frameworks established by the US Department of Homeland Security [5,6]. In order to achieve the goal of energy infrastructure protection, policies suggest implementation of risk management programmes involving vulnerability analysis, threat assessments and risk control measures [7]. The risk management framework involves dealing 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.

Several episodes of sudden disruptions in the electrical service covering large geographic areas have deeply impacted both economic and social sectors in affected countries. Some resembled blackout incidents refer to events on Canada and the U.S. (August 2003), Germany, Belgium, Italy, France, Spain and the Netherlands (November 2006), Brazil (November 2009), as well as short-term acts of terrorism on certain assets of electric infrastructures, such as those experienced in Colombia (1998–2003). As a result, the need to incorporate studies to assess vulnerability of systems has become a requirement in the management of those risks that impact the operations of the electric infrastructures.

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 are among the most used criteria in power industry [8,9].

Graph theory constitutes a relatively new knowledge area in which it is possible to study interdependencies among critical infrastructure systems, specifically the power electric network. In

* Corresponding author. Address: Universidad de Zaragoza, Departamento Ingeniería Eléctrica. C/Maria de Luna 3, Zaragoza 50018, Spain. Tel.: +34 976761922; fax: +34 976762226.

E-mail addresses: gabriel.correa@amigo.edu.co (G.J. Correa), jmyusta@unizar.es (J.M. Yusta).

0196-8904/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.enconman.2013.10.011

this paper, the authors apply a method based on graph theory modelling (theory of complex networks), which allows a simpler representation of electric infrastructures, by analysing their robustness when disrupted. This implies the study of vulnerability due to effects of certain risks and threats that affect normal operation of the power grid [10].

Modelling of power systems as complex networks has focused important research in the last few years, following the first definition of scale-free networks proposed by Barabási and Albert in [11]. Such definition was followed by the release of concepts on statistical measures, vulnerability analysis, robustness and resilience estimation in scale-free networks, with applications to power grids, computer networks and many other engineering areas [10,12,13]. Motter and Lai in [14] formulated the problem of cascading failures into scale-free networks by modelling a degree-based node removal strategy, which constituted the basis to perform vulnerability assessment into electric power networks [15]. As discussed by Holmgren in [16,17] graph theory statistical measures (clustering, connection degree, geodesic distance, nodal distribution) are suitable to perform vulnerability assessment of a power system and for estimation of events that may trigger cascading failures.

Other measures obtained from complex networks models are also suitable to perform vulnerability assessment of electric power networks, as formulated by Chen et al. in [18], who have suggested the use of geodesic efficiency indicators to diagnose cascade event failures. Other approach to assess the power grid's condition on robustness and resilience is formulated by Johansson in [19] and by Wang et al. in [20] who propose measuring the betweenness among nodes of the graph model.

Among many graph models of the electric power grid in certain countries, it is worthy to bring up some studies performed upon the system of the Nordic countries [16,19,21], the continental European power system [22,23] and some South American countries [24], in which are shown advantages of calculating topological measures (node clustering, geodesic distance, geodesic efficiency) to analyse the grid's vulnerability.

So far, modelling with complex networks has become a well-accepted methodology to perform studies for protection of electric networks against certain threats, as revealed by Holmgren et al. in [25] and by Chen et al. in [18,26,27]. Furthermore, a recent research formulated in Correa et al. [28,29] has provided a validation of the equivalence between power load flow techniques and scale-free graph modelling in order to perform vulnerability studies in transmission networks. This fact allows assessing the vulnerability of electric infrastructures based on graph theory models, which are a least time consuming technique, instead of classic power flow indexes.

Based upon such innovative contribution, in this paper the authors apply a modelling graph theory methodology in order to perform a comparative vulnerability assessment on the electric power systems of two countries (Colombia and Spain). This includes an analysis of the network's tolerance against random errors and against deliberate attacks. Moreover, an analysis of the effectiveness of expansion investments is performed according to the information established in each country's power grid expansion planning.

The paper is organized as follows: Section 2 introduces the scale-free topology equivalence for power networks and describes appropriate indexes to measure power grid disruption events. Section 3 shows a case study according to an algorithm for random errors and deliberate attack vulnerability assessment applied to some illustrative examples that are based upon the topologic representation of power networks in Colombia and Spain. This corresponds to a practical application of the methodology previously validated in [29]. Discussion and conclusions on usefulness of scale-free graph modelling and vulnerability assessment is also provided at the end of the paper.

2. Modelling electric power systems with complex networks

It is necessary to transcend risk qualitative assessment in order to generate an effective evaluation framework of vulnerability in transmission, which must involve the study of relations with other systems, their interdependence and their response to both threats and changes under different operating conditions. This involves the study of the events that trigger cascade failures and disconnection of consumers. The methodology explained in this section could be particularly useful as a mechanism for explaining events like power outages or blackouts.

2.1. Proposal for representing network topology

Electric networks can be resembled to scale-free graphs [11], which allows the representation of 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* [16,19,21,26,30]. In those cases such approach allows the calculation of cluster measures (triangles) in order to determine the grid's vulnerability.

Such representation is quite simple, but incomplete, since many important assets in the power grid cannot be properly taken into account in structural vulnerability assessment, as they are, transmission towers, transformers, generation centres, load consumers, capacitors and other assets.

Fig. 1 shows the proposed topological representation of a 5-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 16 nodes and 17 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.

In scale-free graphs 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) [11,12].

2.2. Graph theory and power flow indexes

This section shows some statistical measures that describe scale-free graphs in order to analyse the disintegration of networks (evolution to successive node removal). The formulation of these measures are based upon 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 [31].

2.2.1. Geodesic efficiency

This indicator was originally proposed by Latora and Marchiori in [32], for estimation of the efficiency in which information is exchanged within a network. It is assumed that the flow between two nodes must pass through the shorter geodesic distance [18,26]. Therefore, the *efficiency* between a pair of nodes e_{ij} is defined as the inverse of their geodesic distance. If there were no connection