Physica A 389 (2010) 595–603

Contents lists available at ScienceDirect

Physica A

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

Attack structural vulnerability of power grids: A hybrid approach based on complex networks

Guo Chen [a,*], Zhao Yang Dong [b], David J. Hill [c], Guo Hua Zhang [c], Ke Qian Hua [a]

[a] School of Information Technology and Electrical Engineering, The University of Queensland, QLD 4072, Australia

[b] Department of Electrical Engineering, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong

[c] Research School of Information Sciences and Engineering, The Australian National University, ACT 0200, Australia

ARTICLE INFO

Article history:
Received 19 May 2009
Received in revised form 5 September 2009
Available online 1 October 2009

Keywords:
Power grids
Complex networks
Vulnerability
Power flow equations

ABSTRACT

Power grids have been studied as a typical example of real-world complex networks. Different from previous methods, this paper proposes a hybrid approach for structural vulnerability analysis of power transmission networks, in which a DC power flow model with hidden failures is embedded into the traditional error and attack tolerance methodology to form a new scheme for power grids vulnerability assessment and modeling. The new approach embodies some important characteristics of power transmission networks. Furthermore, the simulation on the standard IEEE 118 bus system demonstrates that a critical region might exist and when the power grid operates in the region, it is vulnerable to both random and intentional attacks. Finally, a brief theoretical analysis is presented to explain the new phenomena.

1. Introduction

Power transmission networks, often called power grids, have been regarded as one of the most important infrastructures critical to national security across the world. However, in recent years, several large blackouts occurred in USA and Europe, which has resulted in direct loss up to billions of dollars. For instance, in July and August 1996, two blackout events took place successively in the power grid of west American, which led to more than 4 million people in 11 states out of power service [1]. In August 2003, a historic blackout was triggered in the power grid of the United States and Canada, which cut power to over 50 million people [2]. Furthermore, also in 2003, several large blackouts happened in the world, such as UK blackout, Sweden–Denmark blackout and Italy blackout [3].

The frequent occurrence of blackouts exposes potential problems of current mathematical models and analysis methodology in power systems. Moreover, with the rapid development of modern society, power grid is also continually evolving and now it has been considered as one of the largest and complex man-made systems in the technological age. Therefore, it is extremely necessary to develop new models and methodologies for avoiding large blackouts in future. Recently, advances in information science, statistical and nonlinear physics, applied mathematics and social science have given birth to a new interdisciplinary field [4], i.e. complex networks, which brings novel concepts and approaches to the study of network vulnerability. The new theory proposed an error and attack tolerance methodology which has drawn the link between the topological structure and the vulnerability of networks. Many literatures have been published. Albert et al. [5] pointed out that scale-free networks are robust against random failures of nodes but fragile to intentional attacks. Latora et al. [6] proposed the concept of network efficiency to characterize small-world networks, which is a quantity of how

* Corresponding author.
E-mail address: guochen@itee.uq.edu.au (G. Chen).

0378-4371/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.physa.2009.09.039

efficiently it exchanges information. Crucitti et al. [7] discussed network efficiency on scale-free networks and modeled the cascading failures of complex networks [8]. Motter et al. [9] studied small-world phenomenon in scale-free networks and found that they are more sensitive to attacks on short-range than on long-range links. Sun et al. [10] analyzed statistical properties of the evolving networks and the responses of these networks under random errors and intentional attacks. Costa et al. [11] discussed the relationship between structure and random walk dynamics in directed complex networks. Ash et al. [12] presented an effective algorithm to evolve complex networks that can be resilient to cascading failure.

Furthermore, mathematically, power networks can be described as a network with hundreds or even thousands of nodes connected by edges [13]. The feature has attracted the interest of the scientific community to apply complex network theory to power network vulnerability analysis [14–20]. Motter et al. [14] discussed cascade-based attacks on power networks and specially studied the capacity–load relation in Texas power grid [15]. Casals et al. [16] analyzed topological vulnerability of European power grid. Crucitti et al. and Kinney et al. made structural vulnerability analysis for Italian electric power grid [17] and North American power grid [18] respectively. Arianos et al. [19] proposed a new parameter, i.e. net-ability, to evaluate the performance of a power grid. Chassin et al. [20] used Barabasi–Albert network model to estimate the reliability of North American eastern and western electric grids.

Those initial attempts [14–20] provide a new direction for power network vulnerability research. However, it is well known that electrical power network is a special network which is governed by Kirchoff's Laws and power flow constraints. This might result in a unique pattern of interaction between nodes. Consequently, given the particular characteristics of electrical power systems and complex network theory together should be an interesting work. In this paper, we will further study the structural vulnerability of power networks by introducing a hybrid approach to investigate the error and attack tolerance. The new scheme takes into account power flow equations and hidden failures of power systems. Moreover, we compare the results obtained from traditional model and the proposed one. Some new phenomena can be observed. The rest of this paper is organized as follows: Section 2 introduces traditional error and attack tolerance methodology. In Section 3, the hybrid approach is fully described. The numerical simulation has been displayed in Section 4 and the theoretical analysis is shown in Section 5. Finally, the conclusions are followed in Section 6.

2. Error and attack tolerance methodology

The aim of the methodology is to investigate structural vulnerability by removing a single or a group of nodes randomly or intentionally and then evaluate how much the performance of the network is affected. Usually, a generic network can be described as an undirected graph G with N nodes and K edges. G is denoted by a $N \times N$ adjacency matrix $\{w_{ij}\}$. If there is not an edge between nodes i and j, then w_{ij} is set to 0, otherwise w_{ij} equals to 1. Based on the topological graph structure, initially, the error and attack tolerance methodology adopted a static model: to investigate structural vulnerability by removing a group of nodes. Refs. [5,9,16] illustrated that with the increase of removed nodes randomly or intentionally, different networks have different performance. Thus, the static model can be used for vulnerability analysis. However, in most real-world complex networks, the breakdown of a single node or a very small size of nodes can be sufficient to cause the entire systems collapsing due to the dynamics of redistribution of flows on the networks. Therefore, a dynamical model [6,7,17,18] is proposed and adopted widely at present.

The dynamical model introduces a concept, i.e. flow, which represents the information or energy that is transmitted on networks. Moreover, the model assumes that the flow between two nodes i and j takes the shortest path connecting them. In order to characterize the flow distribution in networks, the betweenness is used [6,7,17,18]. The betweenness at a node i is defined as the total number of shortest paths passing through this node. The capacity of a node is the maximum betweenness that the node can handle. For a real-world network, the capacity is severely limited by cost. Thus it is natural to assume that the capacity C_i of a node i is proportional to its initial betweenness carried by i

$$C_i = \alpha L_i(0) \quad i = 1, 2, \ldots, N, \tag{1}$$

where $\alpha >= 1$ is a tolerance parameter of the network and $L_i(0)$ is the initial betweenness handled by node i. In addition, the dynamical model introduced the efficiency or efficiency loss of networks [6,7,17,18] to evaluate how well a system works before and after the breakdown. With such a definition, the network is in a stationary state in which it operates with an initial efficiency. The removal of a node triggers the dynamics of redistribution of flow on the network. In fact the removal of a node changes shortest paths between nodes and consequently the distribution of betweenness, which would create overloads on some nodes. For mimicking the dynamics of network after removing a single node randomly or intentionally, at each iteration step t, the following iterative rule is adopted

$$w_{ij}(t+1) = \begin{cases} w_{ij}(0)\dfrac{L_i(t)}{C_i} & \text{if } L_i(t) > C_i \\ w_{ij}(0) & \text{if } L_i(t) \le C_i \end{cases} \tag{2}$$

where w_{ij} is the adjacency matrix of the network and j extends to all the first neighbors of i. In this way if at each iterative step, a node i is overloaded, the length of all the edges passing through it will be increased, which can change the shortest paths between nodes, leading to a new redistribution of the betweenness and then some nodes may be overloaded. The process