Physica A 395 (2014) 405–415

Contents lists available at ScienceDirect

Physica A

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

An improved framework for power grid vulnerability analysis considering critical system features

YuanYu Dai [a,b], Guo Chen [c,d,*], ZhaoYang Dong [c,d], YuSheng Xue [b,a], David J. Hill [c,e], Yuan Zhao [d]

[a] School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China

[b] State Grid Electric Power Research Institute (SGEPRI), Nanjing 210003, China

[c] School of Electrical and Information Engineering, The University of Sydney, Sydney 2006, Australia

[d] State Key Laboratory of Equipment and System Safety of Power Transmission and Distribution & New Technology, College of Electrical Engineering, Chongqing University, Chongqing 400044, China

[e] Department of Electrical and Electronic Engineering, the University of Hong Kong, Hong Kong

HIGHLIGHTS

- We propose an improved framework for vulnerability analysis of power grids.
- The framework considers some important characteristics of power transmission networks.
- Theoretically, this improvement gives a more realistic approximation of a power grid.
- Simulation results also verify the effectiveness and efficiency of the proposed framework.

ARTICLE INFO

Article history:
Received 23 January 2013
Received in revised form 23 August 2013
Available online 26 October 2013

Keywords:
Power grids
Reactance matrix
Efficiency
Power angle
Cascading failure

ABSTRACT

In recent years the rapid development of complex network theory has provided a new angle on the vulnerability analysis of a power grid. However, current analysis models are usually general ones that may ignore some specific features of power systems. In order to address the issue, this paper proposes an improved framework for the vulnerability analysis of power grids. Firstly, the traditional topology based graph model is improved by depicting a power grid as a weighted graph based on the reactance matrix. Secondly, the concept of load is redefined by using power angle information. Thirdly, the power flow constraints are adopted instead of the shortest path based flow scheme. Based on the proposed framework, an improved dynamic analysis model is developed. In addition, numerical simulations for both a general traditional model and the proposed model are investigated based on the *IEEE* 118-bus system respectively. The comparison demonstrates that the improved model is more effective and efficient for the vulnerability analysis of a power grid.

1. Introduction

A power grid is regarded as one of the most critical infrastructures for a country since modern society is dramatically dependent on the availability of high-quality power supply. Undoubtedly, vulnerability analysis plays an important role in the electrical power industry. However, large scale blackouts all over the world still occur from time to time, in spite of huge investments in power system reliability and security. For example, a historic blackout was triggered in the power grid of

* Corresponding author at: School of Electrical and Information Engineering, The University of Sydney, Sydney 2006, Australia. Tel.: +61 2 9351 4283.
E-mail address: guo.chen@sydney.edu.au (G. Chen).

0378-4371/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.physa.2013.10.029

India in July 2012. The outage resulted in billion-dollar losses and cut the power supply to 620 million people [1]. In August 2003, more than 50 million people in seven states of the USA and two provinces of Canada were out of power service [2]. Several other large blackouts in the world also happened over the past decade, such as the London blackout, the Moscow blackout, the Sweden–Denmark blackout etc.

The series of blackouts have exposed the potential problems of current mathematical models and analysis methodologies in power systems motivating both academic and industrial societies to seek alternative solutions [3]. In recent years, successful applications of complex networks theory in many natural and artificial networks vulnerability analysis [4,5] have attracted increasing attention. Initially, this emerging theory and its vulnerability analysis methodology were put forward by physicists and they mainly studied some complicated abstract networks. For example, the Erdös–Rényi (ER) random networks and the Barabási–Albert (BA) scale-free networks have been thoroughly investigated [6–14]. Moreover, some physicists attempted to find the relationship between the structural vulnerability of those abstract networks and power networks which in fact are complex networks and can be described as a graph of nodes connected by edges [15–20]. Casals et al. [15] discussed the structural vulnerability of the European power grid and demonstrated that this grid was robust against random failures of nodes but vulnerable to critical node attacks. Motter et al. [16] studied the impact of cascade-based attacks on real complex networks and indicated that power grids also have the robust-yet-fragile property. Similar results have been revealed in Crucitti et al.' s work [17,18]. They analyzed the Italian electric power grid and the North American power grid respectively. Undoubtedly, these studies provide a promising way to analyse the vulnerability of power systems. However, these works neglect some specific features of power grids. Consequently, the obtained results might mislead engineers when making a decision.

Generally, a power network is quite different from those abstract networks. Its special characteristics result in a unique pattern of interaction between nodes. Recently, there have been some initial attempts to further investigate the complex problems by considering power system features and complex networks theory together [21]. Chen et al. [22] introduced a bus admittance matrix into a traditional topological model. Bompard et al. [23] extended the purely topological approach of complex networks theory by considering the distance in terms of network impedances. Arianos et al. [24] presented a new parameter called net-ability to evaluate the performance of power grids. Following the previous work, an improved framework is proposed in this paper where several critical power system features are considered together. The main contribution of this paper is in the following three aspects: (1) The electrical feature is considered by depicting a power grid as a weighted graph based on the reactance matrix. This feature reflects the Kirchhoff's Laws. (2) The operational feature is considered by redefining the load using power angle information. (3) The power flow feature is adopted instead of the shortest path based flow scheme. In general, compared with the traditional model, the proposed one is a closer approximation to a real power grid. It will be shown in later sections that this innovation can form better approximation models for the vulnerability analysis of a power network.

The remaining parts of the paper are organized as follows. Section 2 introduces traditional topological models. Section 3 presents some specific features of power grids. Section 4 proposes the improved framework for power grid vulnerability analysis. Numerical simulations are displayed in Section 5 and conclusions follow in Section 6.

2. Traditional topological structure based analysis models

Traditional analysis models, which were developed to vulnerability analysis via the error and attack resilience of complex networks, are a class of general models and have been applied in both artificially abstract networks (e.g. the ER and the BA) and real world networks (e.g. the Internet and power networks). Basically, a network can be described as a graph G with N nodes and K edges. Furthermore, G can be expressed by a $N \times N$ adjacency matrix $\{a_{ij}\}$ which represents the physical topological connections of the network based on the rule: if there is an edge between nodes i and j, a_{ij} is set to 1, otherwise 0. The geodesic path d_{ij} between two nodes i and j is defined as the shortest path between them. The efficiency e_{ij} between nodes i and j is denoted as the reciprocal of the geodesic path. This means that the larger the d_{ij} is, the less efficiently information can spread between the two nodes. If there is no path between them, $e_{ij} = 0$. Once the efficiency is defined, the global efficiency (average efficiency) of a network can then be given by

$$E(G) = \frac{1}{N(N-1)} \sum_{i \neq j \in G} e_{ij}. \tag{1}$$

The index is usually used to assess the vulnerability of a network by measuring the efficiency of the graph G before and after disturbances [9,17,20]. It should be noted that in most complex networks, the failure of a single or a very small size of nodes can cause a cascading failure that would lead a whole system to break down due to the dynamic redistribution of flow on a network. Thus a dynamic model was widely applied [9,17,20]. The model introduces the concept of load or betweenness in order to mimic the dynamic redistribution. The load at a node i is defined as the total number of the geodesic paths passing through this node. An important feature of the model is to allocate a given capacity to each node, namely the maximum load that a node can bear. The capacity C_i of a node i is assumed as directly proportional to the initial load carried by i, i.e.

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

where $\alpha \geq 1$ is a tolerance parameter and $L_i(0)$ is the initial load handled by node i at iteration step $t = 0$ [9,17,20]. Using these definitions of load and capacity, the dynamic redistribution of flow can be simulated. The removal of a node changes