Electrical Power and Energy Systems 98 (2018) 219–232

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

Assessment of power grid vulnerabilities accounting for stochastic loads and model imprecision

Roberto Rocchetta, Edoardo Patelli*

Institute for Risk and Uncertainty, Liverpool University, United Kingdom

ARTICLE INFO

Keywords:
Vulnerability assessment
Contingency ranking
Power grid
Uncertainty
Overload cascading failures
Spectral graph metrics

ABSTRACT

Vulnerability and robustness are major concerns for future power grids. Malicious attacks and extreme weather conditions have the potential to trigger multiple components outages, cascading failures and large blackouts. Robust contingency identification procedures are necessary to improve power grids resilience and identify critical scenarios. This paper proposes a framework for advanced uncertainty quantification and vulnerability assessment of power grids. The framework allows critical failure scenarios to be identified and overcomes the limitations of current approaches by explicitly considering aleatory and epistemic sources of uncertainty modelled using probability boxes. The different effects of stochastic fluctuation of the power demand, imprecision in power grid parameters and uncertainty in the selection of the vulnerability model have been quantified. Spectral graph metrics for vulnerability are computed using different weights and are compared to power-flow-based cascading indices in ranking $N-1$ line failures and random $N-k$ lines attacks. A rank correlation test is proposed for further comparison of the vulnerability metrics. The IEEE 24 nodes reliability test power network is selected as a representative case study and a detailed discussion of the results and findings is presented.

1. Introduction

The Power Grid is the world's largest, man-made interconnected structure and plays a critical role in the well-being of society. The working productivity, comfort and safety of local citizens relies on power grids integrity and even modest power outages can seriously compromise their welfare. Severe blackouts may have a huge social and economic impact and is therefore necessary to develop resilient future power grids, capable of withstanding their occurrences. This requires vulnerability assessments of the electric power supply, the identification of critical scenarios, contingency plans and a high degree of confidence in the results. It is also necessary to better understand the relationship between power grids operational risks and those associated with a vulnerable topological structure. This will help mitigate the effects of unexpected and hazardous failures, and enhance the overall network robustness and resilience.

The structure and operations of power grids are changing radically [1,2]: The growing share of intermittent and uncertain renewable power sources is making grid behaviour less predictable; climate change is predicted to increase the intensity and frequency of extreme weather events with the potential to deeply compromise grid integrity [3]; and as highly meshed (non-radial) distribution grid topology is expected to become more common in the future [4], it is likely to see an increasing structural complexity and interconnection between the power grid components. Due to this scenario of increasing complexity and uncertainty, it is important to assess both the inherent variability in the system and imprecision affecting the network parameters. Topological and operational weaknesses have to be better understood in order to provide superior network designs capable of promptly react to unexpected hazardous situations. One potential method of achieving higher grid resilience is by enhancing existing frameworks for power grid vulnerability assessment and by adopting sophisticated uncertainty quantification techniques.

The robustness of power networks is defined as the degree to which the grid is able to withstand unexpected events without degradation in performance [5]. A closely related concept is the vulnerability, which is generally regarded as the lack of robustness. Vulnerability metrics can be obtained in several ways and, in the literature, overload cascading indices based on power-flow evaluations have been proposed to assess the effect of cascading failure events [6,7]. This approach has proven adequate in cases where the cascades are mainly driven by overload line trippings [7]. Alternative approaches have focused on the grid topology by using graph theory to analyse its structure [5,8–14]. The so-called pure topological analysis use unweighted adjacency matrices to calculate vulnerability whilst extended topological approaches enrich the analysis by incorporating electrical engineering information in

* Corresponding author.
E-mail addresses: roberto.rocchetta@liverpool.ac.uk (R. Rocchetta), edoardo.patelli@liverpool.ac.uk (E. Patelli).

https://doi.org/10.1016/j.ijepes.2017.11.047
Received 30 May 2017; Received in revised form 17 October 2017; Accepted 30 November 2017

the weights of the graph. The extended metrics have been introduced based on the idea that pure topological approach may fail in exhaustive captivation of the electric network complexity. Whether or not pure topological approaches and their extended version are capable of fully capture vulnerabilities of power grids is still an open debate [15].

Imprecision is a common problem for power grid models and their parameters, appearing in the calculations due to a number of factors such as, tolerance errors, scarcity of data, inconsistent information, and experts' judgement. This type of uncertainty is generally referred as epistemic or subjective. For example, earlier works dealt with this type of uncertainty using fuzzy power flow analysis [16] or stochastic frameworks for reliability analysis [17]. To the authors' knowledge, topological approaches are generally applied by assuming an exact knowledge of the network parameters and do not account for uncertainty in the calculations. Authors of Ref. [9] analysed the correlation between vulnerability metrics and power flow models. Bompard et al. [10] compared two enhanced metrics (i.e. the extended betweenness and net-ability) by ranking components with respect to the system vulnerability. Recently, Lucas Cuadra et al. [15] reviewed power grid robustness metrics which were computed by adopting complex network theory approaches. Correa et al. [9,18] investigated power network structural vulnerability to single and multiple failures and compared graph-theory approaches against power flow approaches. Cvijić and M. Ilić [11] discussed the applicability of graph-theory methods (generally applicable in transportation networks) to power grids. It was showed that some of the physical laws applied to power systems are limiting factors but, when graph-theory methods are applied, the computational cost of analysis is greatly reduced. Hines et al. [12] discussed the use of topological measures for power grid vulnerability analysis. Through the analysis of random failures it was argued that topological measures can be useful as general trend indicators of vulnerability, although physical-based models (e.g. power flow models) are believed to be more realistic. LaRocca et al. [13] investigated different measures for power grids vulnerability and risk assessment by randomly removing grid components. Similarly, Rocchetta and Patelli [14] compared graph-theoretic spectral vulnerability metrics to power flow based vulnerability metrics in ranking power grid most critical lines. They showed that load demand uncertainty and tolerance imprecision affect the results of the contingency ranking.

To the authors knowledge, none of the reviewed works analysed the effects of both aleatory and epistemic uncertainty on the computation of graph-theoretic spectral vulnerability metrics. However, it is known that sources of uncertainty will inevitably affect power grids robustness. There are several representative examples which consider these effects in the power grid reliability assessment literature. Few notable approaches include reliability assessments of power grids allocating renewable energy sources [19], increasing interdependency between different networks (e.g. telecommunication network transportation network, etc.) and the inherent variability of the (changing) external environmental conditions [3]. Accounting for relevant sources of uncertainty affecting power grid robustness and vulnerability may help to improve the overall confidence in the results and better identify critical scenarios. Being able to distinguish between the (inherently variable) aleatory component of the uncertainty and the (in principle) reducible epistemic uncertainty can be beneficial for the analysis and for improve confidence in the results. Furthermore, many vulnerability metrics have been proposed in the literature and the results will be inevitably affected by a specific metric selection. It is therefore necessary to assess the level of uncertainty associated to power grid robustness when different metrics are employed for vulnerability analysis.

In this work, drops in performance due to single and multiple line failures are analysed by employing algorithms developed by the authors. A novel weighting factor based on the line percentage of rating is also introduced and compared to weights applied in the literature. Load demand is inherently variable and the increasing allocation of non programmable renewable energy sources are making its behaviour even more uncertain. Thus, the aleatory and the epistemic uncertainty affecting load demands and network parameters are accounted for and propagated to the vulnerability metrics and respective contributions highlighted. The proposed framework is flexible and can account for renewable energy sources uncertainty. This can be done by proposing a different characterisation of the uncertainty in the load. One of the main contributions of this work is a systematic comparison of the vulnerability based on operational flow-based models and topological approaches (pure and extended). Furthermore, none of the reviewed works compared spectral vulnerability metrics for contingency ranking purposes embedding the methods within advanced uncertainty quantification framework. Thus, similarities and differences of the different metrics are discussed for increasing damage size and accounting for uncertainties due to stochastic loads and line parameters imprecision.

The paper is structured as follows: A concise review on power grid modelling and spectral graph analysis is proposed in Section 2. In Section 3, vulnerability metrics are defined. The uncertainty modelling and contingency analysis are described in Section 4. The developed algorithms and framework are summarised within Section 5. In Section 6 presents the analysis of the IEEE reliability test system. The limitation faced are discussed in Section 7 and in Section 8 conclusions are drawn.

2. Background and power grid modelling

A power network structure can be modelled using weighted or unweighted undirected graphs $\mathscr{G} = \{\mathscr{N},\mathscr{L},\mathbf{w}\}$, where $\mathscr{N}$ is the set of network buses (or nodes set), $\mathscr{L}$ is the set of lines connecting the nodes (i.e. links set) and $\mathbf{w}$ is the set of weights associated to the lines [10,20–22]. Generally when graph-theory approaches are used, a conservative (pessimistic) hypothesis is made on the network structure, to ease the calculations. Self-loops such as parallel lines are removed from the graph $\mathscr{G}$ and replaced by the equivalent single line model. Different weights define different graph models of the power network, for instance, if $\mathbf{w} = 1$ the model and following analysis will be named purely topological [15], since no electrical quantities are employed. Alternatively, weights can be used to represent specific electrical engineering information. Quantities such as the line susceptance (B_{ij}) or power flow (f_{ij}) have been previously adopted as line weights, see e.g. [8,23], where i and j represent the generic nodes. The number of buses and the number of branches in the power network is represented by the cardinality of the node set $N_b = |\mathscr{N}|$ and the cardinality of the line set $N_L = |\mathscr{L}|$, respectively. To simplify the notations the line subscript $(ij) \in \mathscr{L}$ can be replaced with the subscript l representing the line index.

2.1. Overflow cascading vulnerability

A 'cascade' is a sequential succession of dependent events [6]. In power systems cascading analysis a failure sequence (lines tripping) can be defined as load-driven when the thermal expansion results in the line dropping beneath its safety clearance, or load-independent such as in case of a mechanical failure. The metric adopted in this paper focuses on load-driven failures and is used to assess the network vulnerability to overload cascading events. The cascading index (CEI) is obtained computing the 'immediate' post-contingency power-flow operative state and it is defined as follows [6]:

$$CEI\,(C_{N-k}) = \sum_{l\in\mathscr{L}} \mathscr{P}(C_l|C_{N-k})\cdot S_l(C_{N-k}) \tag{1}$$

where $\mathscr{P}(C_l|C_{N-k})$ is the probability of a secondary (post-contingency) trip of the line (l) after the contingency denoted as C_{N-k} occurred. The severity $S_l(C_{N-k})$ is a overload severity function for the line l due to the