An Entropy-based Metric to Quantify the Robustness of Power Grids against Cascading Failures

Yakup Koç[1,*] Martijn Warnier[1] Robert E. Kooij[2,3] Frances M.T. Brazier[1]
[1]Systems Engineering Section
Faculty of Technology, Policy and Management
Delft University of Technology
[2]Network Architecture en Services Section
Faculty of Electrical Engineering, Mathematics and Computer Science
Delft University of Technology
[3]TNO (Netherlands Organisation for Applied Scientific Research)
Information and Communication Technology

Abstract

The cascading failure phenomenon in a power grid is related to both the structural aspects (number and types of buses, density of transmission lines and interconnection of components), and the operative state (flow distribution and demand level). Existing studies most often focus on structural aspects, and not on operative states. This paper proposes a new metric to assess power network robustness with respect to cascading failures, in particular for cascading effects due to line overloads under targeted attacks. The metric takes both the effect of structural aspects and the effect of the operative state on network robustness into account, using an entropy-based approach. IEEE test systems and real world UCTE networks are used to demonstrate the applicability of this robustness metric.

Keywords: Cascading Failures, Robustness, Complex Networks, Power Grid, Entropy, Metric

1 Introduction

The electric power grid is indispensable in today's society. The large dependency in developed countries on the electric power necessitates a great reliability and availability of the electric power grid. Although careful control and management of the power grid greatly limits the risk

[*] Corresponding Author, Email: Y.Koc@tudelft.nl, Address: Jaffalaan 5, 2628BX Delft, The Netherlands, Phone: +31 (0)15 27 88380

of failures, analysis of 15 years of blackout data by the North American Electrical Reliability Council (NERC) reveals that blackouts exhibit a power law distribution suggesting that large blackouts are much more likely than expected [12]. Accordingly, Chen et al. [8] show that the US power transmission grid suffered more than 400 major blackouts between 1984 and 1999, causing economic cost in the order of tens of billion dollars per year. For example, in 2003, the North-Eastern and Mid-Western United States and, South-Eastern Canada suffered a catastrophic blackout leaving 50 million people without power for up to several days [24]. A more recent example is the large blackout in Brazil in 2009 that left 40% of the country without power for up to five hours [9].

Post-mortem investigations of blackouts reveal that major blackouts are mainly due to successive malfunctioning of a large set of dependent components that are often triggered by an initial disturbance (e.g. lightning, natural disasters, contact between vegetation and conductors and human error) [3, 25]. In a scenario of cascading failures due to line overloads, failure of any single transmission line changes the balance of power flow and leads to a global redistribution of flows across the grid. Global redistribution of flows, in turn, lead to overloaded transmission lines. Circuit breakers trip these overloaded lines when they reach their maximum flow limits (due to thermal, stability or voltage drop constraints) and new overload failures follow. This cascading process may stop after a few steps but it can also propagate and leave a considerable part of a network without power.

To counter this effect, the problem of cascading failures has to be analysed from the point of view of the system level and from the perspective of the global network [1, 22]. Recent advances in the field of complex networks theory [31, 4] have shown the promising potential of the complex networks approach to model and analyse power networks at the system level.

This paper proposes a metric that quantifies robustness of a power transmission grid with respect to cascading failures by targeted attacks. A power grid is considered to be a complex network, and the electric power the physical quantity flowing through it. Steady-state operation and cascades due to line overloads are considered. The rest of this paper is organized as follows. Section 2 provides an overview of literature on modelling and quantifying cascading failures and robustness in power networks. Section 3 explains how cascading effects in a power grid are modelled by using a complex networks approach. Section 4 introduces the robustness metric based on the model proposed in Section 3. Section 5 applies the proposed robustness metric on different use cases and analyses their robustness. The paper ends with a discussion, conclusions and suggestions for future work.

2 Cascading Failures in Power Grids

Power grid robustness, including the cascading failures phenomenon, is an active field of research. Most contributions from the literature are based on modelling and analysing cascading effects in power networks using complex systems approaches [12, 8, 11, 30]. In addition [19, 10, 17], authors also deploy complex network theory where the power grid is considered as a complex network in which electricity is exchanged between nodes through the shortest or most efficient path. The cascading failure mechanism is simulated in the resulting models of power grids. In these approaches, the load of a particular component is modeled by betweenness centrality [27], that equals the number of shortest paths from all nodes to all others that pass through that component. The capacities of individual transmission lines are assumed to be proportional to their initial loads with a modelling parameter, namely, the network tolerance parameter α (See Eq. (6) in Sec. 3.3 for details). In [19] and [17] the damage of cascading failures is quantified in terms of the relative size of the giant component [27] while in [10] it is measured in terms of the decrease in network efficiency [18]. In contrast to these more theoretical studies, Kinney et al. [15] have deployed the model proposed in [10] to simulate cascading failures in the North American power grid. They assess network robustness with respect to cascading failures for different tolerance parameter values in targeted- and random failure scenarios, while Wang et al. [30] investigate the robustness of the Western United States power grid under different attack strategies.

In addition to these cascading failure modelling studies, other studies address the problem of locating the most important components in the network so that these components can be backed up in emergency cases to avoid overloading of these components [18, 19, 20]. Although there is substantial literature on understanding/analysing cascading failures in power networks, and increasing network survivability, little attention has been paid to quantifying network robustness with respect to cascading failures. To the best of our knowledge, Youssef et al. [33] and Bao et al. [3] are the only studies that propose metrics to measure network robustness with respect to cascading failures induced by *random failures*, and there is no metric yet to quantify network robustness against cascading failures under *targeted attacks*. The robustness metric in [33] depends on the probability of link survivals as well as the depth of the cascading failure, while Bao et al. [3] deploy the entropy of global load distribution as an indicator of the size of cascading failures. However, the computation of these metrics for a power grid necessitates substantial computational time because it requires simulating a cascading failure in a power grid. This makes it very challenging to deploy these metrics as real-time measures based on which the grid can be dynamically optimized.

Two aspects are of importance in determining the cascading failure robustness of a power network: (i) the structure and (ii) the operative state of a network. The structure of a network defines the interconnection of the components (i.e. topology) together with their specific attributes (e.g. electrical characteristics and maximum flow limits of transmission lines). The operative state of a network relates to how homogeneously load flow is distributed across a network and how heavily a network is loaded. The structure of a network is mainly static while the operative state is continuously changing depending on the loading profile in the network. This dynamic character of the operative state makes cascading failure robustness of power networks also dynamic. This means that a power grid can be assessed to be very robust at time t, while a new operative state (e.g. due to a new loading profile) at time $t + k$ can make the same grid to be critically vulnerable.

Although the importance of the operative state on cascading effects is emphasized by numerous researchers [19, 10, 17, 6], existing studies [5, 6] attempt to assess the power grid robustness for cascading failures relying solely on the structural properties of a network. This paper proposes a robustness metric, that, in contrast to the existing studies, takes both relevant aspects into account: the structural properties and the operative states when determining network robustness.

This paper extends the previous work [16], that presents the initial concepts of R_{CF}. In [16], Koç et al. focus on validation of the robustness metric. This paper elaborates on the modelling of cascading effects in power grids and application of the robustness metric on different use cases including the IEEE test systems and real world transmission grids.

3 Modelling Cascading Failures in Power Grids

This section models cascading effects due to line overloads in power networks using a complex networks approach. This requires modelling a power grid as a graph, estimating line flows across the grid by using direct current (DC) load flow analysis [13, 26], modelling cascading effects in the grid and finally quantifying the damage caused by cascading failures.

3.1 Modelling power grid as a graph

This paper models a power grid as a graph to analyse the cascading effects due to line overloads. A power grid is a complex interconnected network, composed of three functional parts: generation, transmission, and distribution. Power is provided from generation buses to distribution stations through transmission buses that are inter-connected to each other via transmission lines. In a graph representation of a power grid, generation, transmission, distribution buses, substations and transformers are represented by nodes. Transmission lines are modelled as links. Fig. 1 and Fig. 2 illustrate the single-line diagram and the graph representation of IEEE 30 bus system [14] consisting of 30 bus bars and 41 transmission lines.

3.2 Estimating line power flows: DC load flow equations

The power flow in a grid is controlled by its physical properties: impedances, voltage levels at each individual power station, voltage phase differences between power stations and loads at terminal stations. Power flow equations estimate the flow values for each component in the network. Alternative current (AC) power flow equations are non-linear equations that model the flows of both active and reactive powers, while DC load flow equations are a simplification and linearisation of AC power flow equations that consider only the flow of active power [13, 26]. Throughout this paper, DC load flow analysis is performed to estimate the flow values across the network because AC load flow analysis may not converge when the lines and generators trip and it introduces significant complexity in the model [3]. In the AC model, the active power flow f_{ij} through a transmission line l_{ij} connecting node *i* and node *j* is related to complex voltage at both nodes *i* and *j* and impedance value of the line l_{ij} as follow [26]:

$$f_{ij} = \frac{|V_i||V_j|}{z_{ij}} \sin(\theta_{ij}) \tag{1}$$

where $|V_i|$ is the voltage amplitude at node *i*, θ_{ij} is the voltage phase difference between node *i* and node *j*, and z_{ij} is the impedance of transmission line l_{ij}. The above non-linear equation is linearised by the following assumptions:

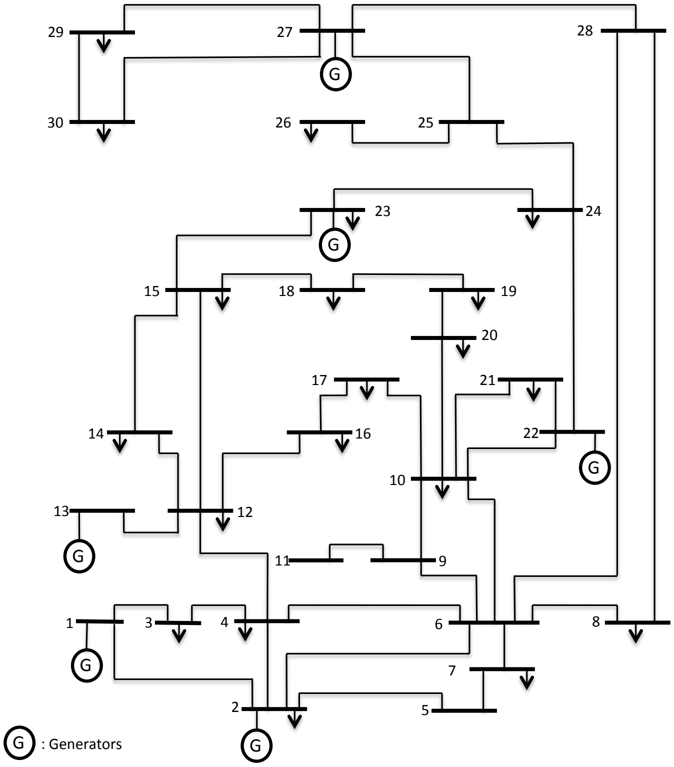

Figure 1: Single-line diagram of IEEE 30 buses test case

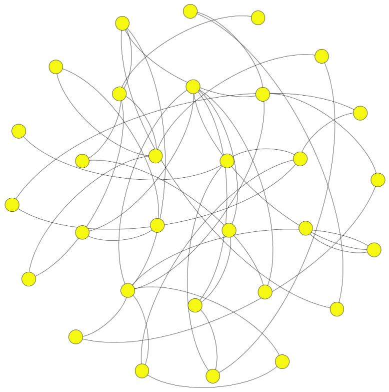

Figure 2: Graph representation of IEEE 30 buses test case topology

- reactive power balance equations are neglected;
- all voltage magnitudes are considered to be 1 p.u.;
- line resistance is ignored so that line impedance equals line reactance $z_{ij} \approx x_{ij}$;
- voltage phase differences are very small so that $\sin(\theta_{ij}) \approx \theta_{ij}$.

These assumptions make DC load flow analysis seven to ten times faster compared to AC load flow analysis. On the other hand, DC assumptions introduce 5% error in the systems and constrain the model to be used only in high voltage transmission grids [21]. By incorporating the above assumptions in Eq. (1), the DC power flow equation is obtained:

$$f_{ij} = \frac{\theta_{ij}}{x_{ij}} = b_{ij}\theta_{ij} \tag{2}$$

where b_{ij} is the susceptance of line l_{ij}. The entire system can be modelled solely by using the following linear equation:

$$P_i = \sum_{j=1}^{d} f_{ij} = \sum_{j=1}^{d} b_{ij}\theta_{ij} \tag{3}$$

where P_i is the real power flow at node *i* and *d* is the degree of node *i*. In terms of matrices, Eq. (3) can be rewritten as:

$$\mathbf{P} = \mathbf{B}\boldsymbol{\theta} \tag{4}$$

where **P** is the vector of real power injections, $\boldsymbol{\theta}$ contains the voltage angles at each node, and **B** is the bus susceptance matrix in which $B_{ij} = -\frac{1}{x_{ij}}$ and $B_{ii} = \sum_{j=1}^{d} -B_{ij}$. Since the losses in the system are neglected, all active power injections are known in advance. Hence, given the bus susceptance matrix **B**, the voltage angles at each node can be calculated directly by using:

$$\boldsymbol{\theta} = \mathbf{B}^{\textbf{-1}}\mathbf{P} \tag{5}$$

After obtaining the voltage angle values at each node, power flow values through each line can be computed using Eq. (2).

3.3 Modelling cascading effects due to line overloads

A cascading effect in a power grid can be induced in different ways including instability of voltage and frequency, malfunctioning of protection system, and overloads. This paper focusses on cascading effects due to line overloads. The capacity of a line is defined as the maximum power flow that can be carried by the line. This paper assumes that the maximum capacity of line i, C_i, is proportional to its initial load $L_i(0)$. A tolerance parameter of line i, α_i, relates C_i to $L_i(0)$ as:

$$C_i = \alpha_i L_i(0) \tag{6}$$

To simulate a cascading failure, the line-to-be-attacked is removed from the topology. Once a line is pruned, its flow is distributed over its neighbours. This simulation assumes that the excess power is distributed over all available adjacent lines based on their initial load [29]. Distribution of the excess power may cause overloading of other neighbours resulting in disconnection of these lines by circuit breakers. This paper focuses on line failures due to cascading effects and not on node failure as a result of overload. Power carried by the newly failed lines is also redistributed. This procedure continues until no more lines are overloaded. For the sake of simplicity, this paper assumes a deterministic model for line tripping. A circuit breaker for line l trips at the moment the load of the line l exceeds its maximum capacity. Furthermore, no mitigation strategies are deployed to alleviate the cascade process.

3.4 Quantifying the damage by cascading effect

After a cascading failure occurs, the survivability of a network against cascading failures is quantified empirically by the metrics Demand Survivability (DS), Link Survivability (LS) and Capacity Survivability (CS). DS is the fraction of the satisfied power demand after a cascading failure occurs in a network. LS is defined as the fraction of lines that are still in operation after a cascading failure, whereas CS is formulated as the fraction of the capacity of these operational lines. A line is considered to be operational if it is not tripped by its protection mechanism and if it is not disconnected and isolated from generators so that it still delivers power after the cascading failure. LS and CS are given in Equation (7) and Equation (8). L and C stand for the total number of links and the sum of the capacity of these links in the original network before the cascading failure while $L^{'}$ and $C^{'}$ are the new values after the cascading failure.

$$LS = \frac{L^{'}}{L} \tag{7}$$

$$CS = \frac{\sum_{i=1}^{L^{'}} C_i}{\sum_{j=1}^{L} C_j} \tag{8}$$

DS, LS and CS are simulation-based metrics quantifying power network robustness empirically. They are computed off-line and require substantial computational power and time for large networks, unlike the proposed robustness metric R_{CF} (See Sec. 4). DS, LS and CS are used to validate R_{CF} in Sec. 5.2 and in Sec. 5.3.

4 Robustness Metric

The proposed robustness metric R_{CF} relies on two main concepts: electrical nodal robustness and electrical node significance. This section elaborates on these new concepts and explains the computational algorithm with which to calculate the robustness metric value.

4.1 Electrical nodal robustness

The robustness metric this paper introduces is an aggregate of local robustness values that indicate *electrical nodal robustness*. Electrical nodal robustness quantifies the ability of a node to resist cascades of link overload failures based on the model introduced in Sec. 3. Quantifying electrical nodal robustness requires both flow dynamics and network topology to be taken into account. Three factors are of importance: (i) the homogeneity of load distribution on out-going links; (ii) the loading level of the out-going links; and (iii) the out-degree of the node.

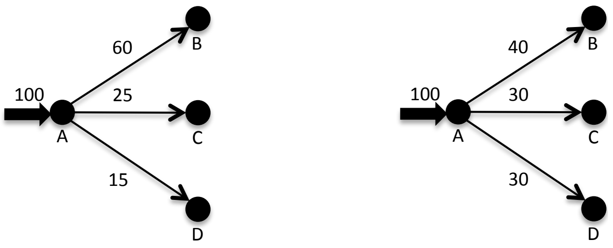

Figure 3: Different load distribution homogeneities, same node out-degree

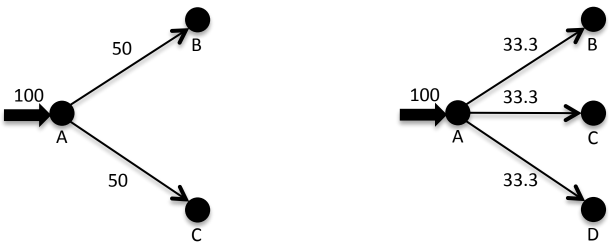

Figure 4: Same load distribution homogeneities, different node out-degree

In Figure 3, the effect of load distribution homogeneity on cascades of link overload failures is considered in a very simple case to provide a basic intuition about cascading failure robustness. Node A distributes 100 unit of power to nodes B, C, and D. Assuming a network tolerance parameter α of 2, for a load distribution of 60, 25 and 15 unit power (i.e. capacity of lines A-B, A-C and A-D are 60 $\times$ α = 120, 25 $\times$ α = 50 and 15 $\times$ α = 30, respectively), a failure in line A-B results in a load increase of line A-C to 62.5 and A-D to 37.5. New flow values exceed the maximum capacities of the line A-C (i.e. 50) and A-D (i.e. 30), causing an overload failure in both lines A-C and A-D. However, if the load is distributed relatively more homogeneously over lines (e.g. 40, 30 and 30: capacity values for links are 80, 60 and 60, respectively), when one of the links fails, none of the neighbouring links overloads (none of the line capacities is exceeded). Consequently, a more homogeneous load distribution across lines increases robustness with respect to cascades of link overload failures while a relatively heterogeneous load distribution increases the chance of link overload failure spread. Note that for an increased loading level of 60%, link overload failure occurs in both of the cases in Figure 3, whereas for a loading level of 30%, in neither of the cases failure spreads. This shows that there is an inverse relationship between the electrical nodal robustness and loading level of the network. Finally, the effect of node out-degree on the electrical nodal robustness is illustrated in Figure 4. In both of the cases, flow is distributed uniformly over the available paths. However, again for the loading level of 50%, Case 2 is more tolerant to cascade of link overload failures than Case 1. This reflects the effect of out-degree on the electrical nodal robustness: the larger out-degree a node possess the higher electrical nodal robustness it has.

Quantifying the electrical nodal robustness entails incorporating the three factors illustrated in Figure 3 and Figure 4. To capture the first and the last behaviours a well-known concept from information theory is used: entropy. Furthermore, the network tolerance parameter α, proposed in [19], is used to incorporate the loading level of the network. Deployment of entropy for the electrical nodal robustness computation makes it possible to capture important cascading failure dynamics. Entropy of a load distribution of a node increases as flows over lines are distributed more homogeneously and the node out-degree increases. The entropy of a given distribution is computed by Equation (9):

$$H = \sum_{i=1}^{L} p_i \log p_i \tag{9}$$

where p_i stands for values in the distribution under consideration, while L refers to the number of the samples in the distribution. Tailoring Equation (9) to the electrical nodal robustness concept, L refers to the out-degree of the corresponding node, whereas p_i corresponds to normalized flow values on the out-going links, given as:

$$p_i = \frac{f_i}{\sum_{j=1}^{L} f_j} \tag{10}$$

In Equation (10) f_i refers to the flow value in line i. When applying Equation (9) to the cases in Figure 3, the absolute values of entropy are 0.4072 and 0.4729, respectively. Assuming the same network loading level for each case, these values imply that the second case is more robust than the first case with respect to cascades of overload failures coinciding with the aforementioned observations. When computing entropy values for the cases in Figure 4, 0.3010 and 0.4772 are obtained for Case 1 and Case 2 respectively. Note that in case of a higher out-degree and a more homogeneously load distribution, the resulting entropy value becomes larger. This illustrates how the entropy concept captures topology-and load distribution homogeneity effects on cascading failure robustness.

The effect of the loading level of the network on robustness is incorporated using the network tolerance parameter α. The loading level of an arbitrary line *i* (LL_i) is the ratio between the load and the maximum capacity of the corresponding line. Hence, there is an inverse relationship between the loading level and the tolerance parameter of a line:

$$\alpha_i = \frac{1}{LL_i} \tag{11}$$

Combining Equations (9), (10) and (11), the electrical nodal robustness of a node i (i.e. $R_{n,i}$), which takes both the flow dynamics and topology effects on network robustness into account, is then defined as:

$$R_{n,i} = -\sum_{i=1}^{L} \alpha_i p_i \log p_i \tag{12}$$

In Equation (12), the minus sign (-) is used to compensate the negative electrical nodal robustness value that occurs due to logarithm of normalized flow values (i.e. p_i).

4.2 Electrical node significance

Due to the scale-free nature of power grids, some of the buses act as hubs i.e. deal with a relatively larger amount of power, while other nodes distribute a relatively small amount of power. When a failure occurs at a link that originates from one of the hub buses, a significant amount of power is exposed to the remainder of the network. Redistributing this excess power over adjacent components eventually causes further link overload failures, which potentially results in a large-scale power outage. Nevertheless, if a failure occurs at a link that is connected to a less important node, its power is immediately re-routed to adjacent components and the disturbance can, usually, be suspended. This suggests that nodes have different impacts on the context of cascading failure robustness and this impact depends on the amount of power, distributed by the corresponding node. In this paper, impact of a particular node is reflected by electrical node significance (i.e. δ). Electrical node significance of an arbitrary node i is computed as:

$$\delta_i = \frac{P_i}{\sum_{j=1}^{N} P_j} \tag{13}$$

where P_i stands for total power distributed by node i while N refers to number of nodes in the network.

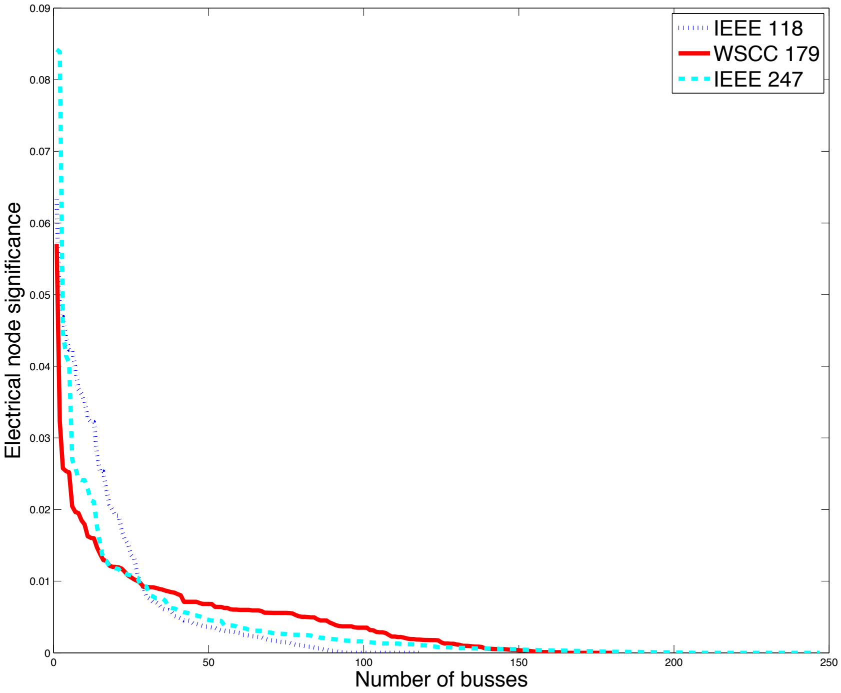

Figure 5: Electrical node significance distributions (in a sorted fashion) for IEEE 118, WSCC 179 and IEEE 247 bus test systems

Electrical node significance is a centrality measure which can be used to rank the relative importance (i.e. criticality) of nodes in a power grid in the context of cascading failures. An attack on the node with the highest δ results, most likely, in the largest cascading effect in the network. An assessment of different centrality measures (i.e. betweenness centrality, node degree, and closeness centrality) together with δ shows that an attack strategy based on δ values results in the largest cascading failures in a grid [28] conforming the effectiveness of δ to anticipate the criticality of nodes in a power grid. Electrical node significance distribution can be related to load distribution across the nodes and shows the electrical topology of a network along with how the importance is distributed over the nodes.

The electrical node significance distributions for IEEE 118, IEEE 247 [14] and WSCC 179 [7] bus test systems, plotted in Figure 5, exhibit a power-law like character for their electrical node significance distributions, with a scaling exponent [32] of 1.7, 2.8 and 2, respectively. Figure 5 indicates the existence of a few nodes with a relatively heavier load to distribute, leading to the high heterogeneity among node. This is widely accepted as the substantial incentive for large-scale cascading failures induced by overload failures [19, 34, 2]. However, note that δ distribution can not be used by itself to determine the robustness level of a grid, as it does not include the effects of structural properties on network robustness. For example, in a grid configuration, a node can be very critical because of the amount of power that it distributes. However if the corresponding node has a large out-degree, then the imbalance of node criticality distribution in the grid configuration does not necessarily comprise a vulnerability for the network. R_{CF} incorporates the effect of structural aspects on network robustness by the electrical nodal robustness measure.

4.3 Network Robustness Metric

After computing the electrical nodal robustness and node significance values, two different values are obtained for each node in the network. The product of these two values indicates the individual contribution of each node to the network robustness. The network robustness metric calculation is finalized by summing up these individual contributions of each node in the network. The resulting metric R_{CF}, given in Equation (14), quantifies network robustness with respect to cascading failures in power networks.

$$R_{CF} = \sum_{i=1}^{N} R_{n,i}\delta_i \tag{14}$$

The normalized nature of electrical node significance assures that the robustness of power networks with different size can be compared.

5 Cascading failures robustness analysis of electric power grid: Case studies

This section applies the robustness metric R_{CF} to different networks to analyse and assess their robustness with respect to cascading failures. First a radial network is considered and new lines

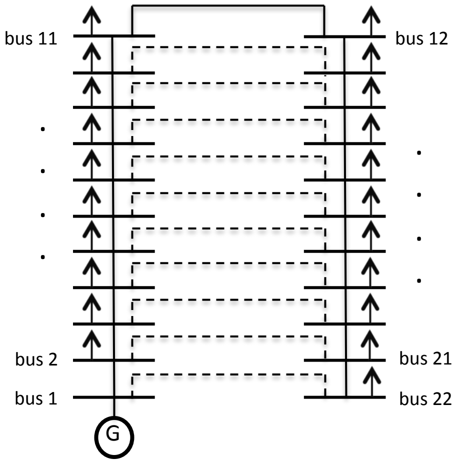

Figure 6: Radial network

are added to the original topology to analyse the effect of line adding on network robustness. Then, robustness of different IEEE test configurations are assessed. Finally R_{CF} is applied on a real-world network- Union for the Coordination of Transport of Electricity (UCTE) network [23] - to see how the network robustness evolves by changing operative states.

5.1 Effect of line adding

Adding a line to a grid topology changes the flow distribution across the network and the loading level of the components in the network. The impact of line adding on network robustness is explained conceptually by considering a radial network (See Figure 6) consisting of 1 generator and 21 load buses [6]. The generator bus (i.e. Bus 1) feeds load buses through a line topology containing 21 transmission lines. All of the load buses and transmission lines have the same properties (i.e. demand and impedance values-line capacities). The radial network is the base network configuration, and new lines are added progressively one at a time. Accordingly, first, a line is added between nodes 1-22 and its impact on average electrical nodal robustness and the network robustness R_{CF} is assessed. Then another line is added between nodes 2-21 and again the assessment on robustness metric is done. This is repeated until the last line is added between nodes 10-13. Dashed lines in Figure 6 show the added lines.

Initially, in the base case, the electrical nodal robustness at each node is zero because there is no redundancy at any node, and any failure at any node causes disintegration of the network leaving the remainder of the network without power. Consequently, robustness of the network is also zero (See Eq. 14). Effect of progressive line adding on the electrical nodal robustness average and overall network robustness is shown in Fig. 7.

Adding a line to the base case results in an increase in node out-degree and a decrease in loading level of transmission lines causing a improved electrical nodal robustness in the network.

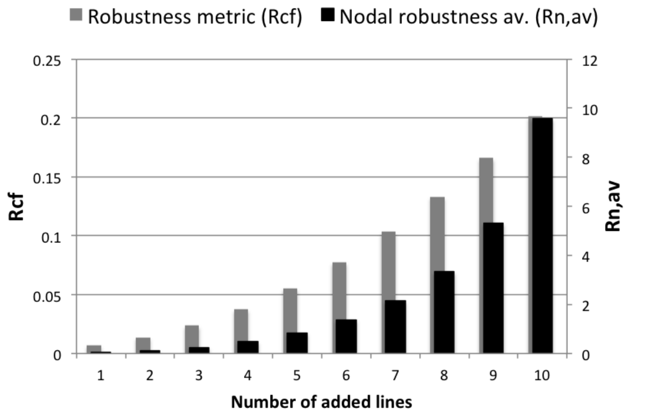

Figure 7: Effect of line adding on network robustness for a radial network

As a consequence, the overall network robustness R_{CF} also increases. Fig. 7 shows that there is an approximate quadratic relationship between the number of lines added and overall network robustness metric R_{CF}. On the other hand, the electrical nodal robustness average increases more steeply when more lines are added progressively. The difference in the electrical nodal robustness and R_{CF} behaviours is due to the electrical node significance behaviour. Fig. 7 suggests that the more lines are added to the original radial network, the higher network robustness gain is achieved.

5.2 Robustness assessment of different IEEE test systems under targeted attacks

This subsection applies the robustness metric (R_{CF}) on different test systems with a different topology and different operative states. The data required for the robustness metric analysis includes the admittance matrix of the network, the number of buses, their types and finally their generation capacity and load values. The IEEE test systems include all of these data. In this paper the IEEE 57, 118, and 247 [14] buses test systems are considered for robustness assessment. Following the computational algorithm given in Sec. 4 the robustness levels of these test systems are computed using R_{CF}. Subsequently, a cascading failure is simulated in these test systems and their robustness levels are quantified empirically (following Sec. 3.3 and Sec.3.4, respectively) to assess whether R_{CF} can anticipate the network robustness. A cascading failure in a network is induced by attacking *the most important outgoing link (i.e. most heavily loaded outgoing link) from the most critical node (i.e. the node with the largest δ) in the network.* Removal of this link results in a cascading failure for the power network, which relates directly to the robustness of the power network with respect to targeted attacks. The lines-to-be-attacked in the IEEE 57, IEEE 118 and IEEE 247 buses test systems are determined as l_{1-15}, l_{89-92}, and l_{1-43}, respectively. After simulating a cascading failure in the test systems, following the computational algorithm in Sec. 3.4, Link Survivability (*LS*) and Capacity Survivability (*CS*) are computed for the test systems.

Table 1: Robustness metric (R_{CF}), LS and CS values for IEEE 57, IEEE 118 and IEEE 247 bus test systems.

Network	R_{CF}	LS	CS
IEEE 57	0.6351	0.5256	0.7508
IEEE 118	0.6806	0.8659	0.8990
IEEE 247	0.4875	0.0430	0.0517

Table 1 shows the computed R_{CF} and empirically-determined LS-CS values. R_{CF} suggests that IEEE 118 buses test system is the most robust system with respect to cascading failures amongst other configurations, while IEEE 247 buses test system is the least robust one. Robustness assessment by simulation-based LS and CS values has the same results verifying the ability of R_{CF} to anticipate the network robustness.

The result of robustness assessment can be justified by taking a closer look to the topology of IEEE 247 test system. In IEEE 247 buses test systems, as also can be seen in Figure 5, criticality is distributed very heterogeneously across the network. This is because one node (i.e. Node 1) dominates generation in the configuration resulting in a relatively more heterogeneous load distribution over the network. Another pitfall of the configuration is that Node 1 is connected to the rest of the network very weakly (out-degree of Node is 1). Consequently, any attack on this single line isolates the most important node from the rest of the network reducing the generation in the network drastically. This context-based and topological weaknesses are captured by the robustness metric R_{CF} and IEEE 247 buses configuration is assessed as the least robust network.

Note that this assessment of test topologies holds for the given loading profile of the network. For a different loading profile, the order of robustness of the networks can change. This is because the operative state (i.e. homogeneity of load distribution across the networks and the loading level of the networks) will change. The effect of operative state on the grid robustness is investigated thoroughly in Sec. 5.3.

5.3 Evolution of network robustness by new operative states

This subsection applies the robustness metric R_{CF} on a real world network -the interconnected European UCTE network- with different loading profiles to assess the evolution of network robustness depending on different operative states. The topology of the network is static while the operative state is changing because of new loading profiles. The UCTE network consists of 1254 nodes and 1944 links. Three different loading profiles are adopted for the network. The loading profiles are registered in the year of 2002 and they correspond to a summer (a total demand of 2.49 TW), a winter peak (a total demand of 3.15 TW) and a winter off-peak (a total demand of 2.32 TW) loading profile [23]. Figure 8 illustrates loading profiles for UCTE network plotting the bus ID's versus the demand level at the corresponding bus. In Figure 8, the biggest loads are observed in clusters of buses with the ID of 542-546 (a cluster of buses in Belgium), 621-629 (a cluster of buses in the Netherlands) and 800-802 (buses in Germany).

A DC load flow analysis is performed to estimate flow values in the network based on the

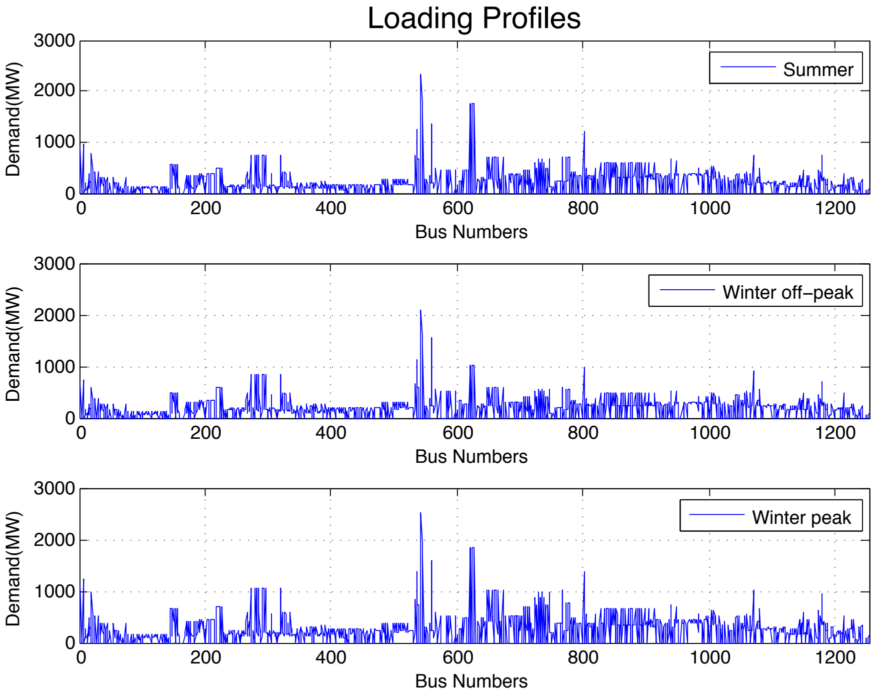

Figure 8: Loading profiles for UCTE network

model introduced in Sec. 3.2. Then following the computational algorithm given in Sec. 4, the robustness metric R_{CF} for different configurations are computed. Maximum capacity values of transmission lines are determined based on UCTE summer configuration and these capacity values are used also in other configurations. In this way, the effect of the loading level on the grid robustness is included in the robustness level calculation. Table 2 shows the result.

Table 2: Robustness metric (R_{CF}) values for UCTE network with different loading profiles.

Configuration	R_{CF}
UCTE summer	0.5429
UCTE winter off-peak	0.5703
UCTE winter peak	0.4414

Table 2 suggests that the UCTE winter off-peak configuration has the highest level of robustness while the UCTE winter peak configuration is the most vulnerable configuration. The result is not surprising especially when considering the demand level of each configurations. When the grid is loaded most heavily (i.e. winter peak configuration), the aptitude of the grid to afford failures degrades resulting in a vulnerable grid. On the other hand, when the grid has a relatively lower demand level (i.e. winter off-peak configuration), it becomes more resilient against failures. This effect of loading level on grid robustness is captured by R_{CF}. To investigate the effect of load flow distribution homogeneity on the grid robustness, the robustness levels of UCTE configurations are re-calculated. This time all of the configurations are assumed to have the same network tolerance parameter α. Accordingly all the grid configurations are assumed to have the same loading level so that the effect of loading level on the network robustness is ignored. After computing R_{CF} values, a cascading failures is simulated in each configuration and its robustness level is quantified empirically so that the theoretical R_{CF} values can be verified. The fraction of satisfied power (DS) after cascading failures happened is deployed as an empirical metric. Table 3 shows the result.

Table 3: Robustness metric (R_{CF}) values and fraction of satisfied demand (DS) after cascading failures for UCTE network with different loading profiles (effect of loading level ignored).

Configuration	R_{CF}	DS
UCTE summer	0.4072	0.4434
UCTE winter off-peak	0.4187	0.5040
UCTE winter peak	0.4174	0.4791

R_{CF} values in Table 3 suggests that the UCTE winter off-peak configuration is the most robust configuration while the UCTE summer configuration is the least robust one. This theoretical result is confirmed also by the simulation-based DS values. Figure 9 illustrates how the fraction of satisfied power demand decreases at each stage of the cascading failure. It shows that the winter off-peak configuration preserves the highest level of power (i.e. most robust), while, on the contrary, the summer configuration has the highest power loss (i.e. least robust).

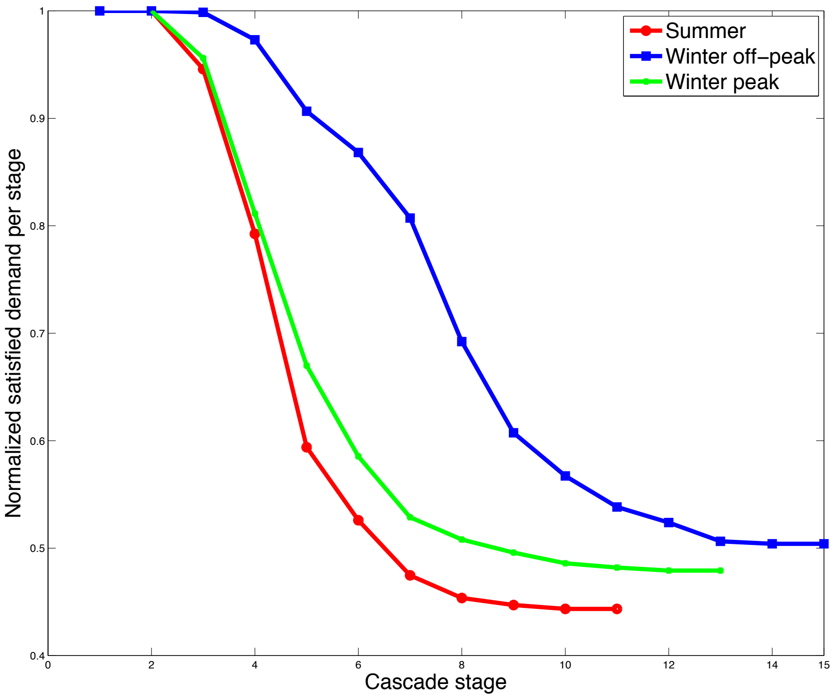

Figure 9: Normalized satisfied power demand per stage of the cascade in each UCTE configuration

To further the robustness analysis, Fig. 10 illustrates the electrical node significance distributions for all three configurations in a sorted fashion while Table 4 shows the most critical 10 nodes with corresponding δ values for each configuration. In the UCTE summer configuration, criticality is distributed the most heterogeneously amongst others while the winter off-peak configuration distributes the node criticality most homogeneously. This means that in summer configuration, very critical node(s) are appearing (e.g Node 627) and an attack on these nodes can have severe effects making the UCTE summer configuration more vulnerable. On the other hand, in the winter configurations, the criticality is distributed more homogeneously making the network more robust against attacks.

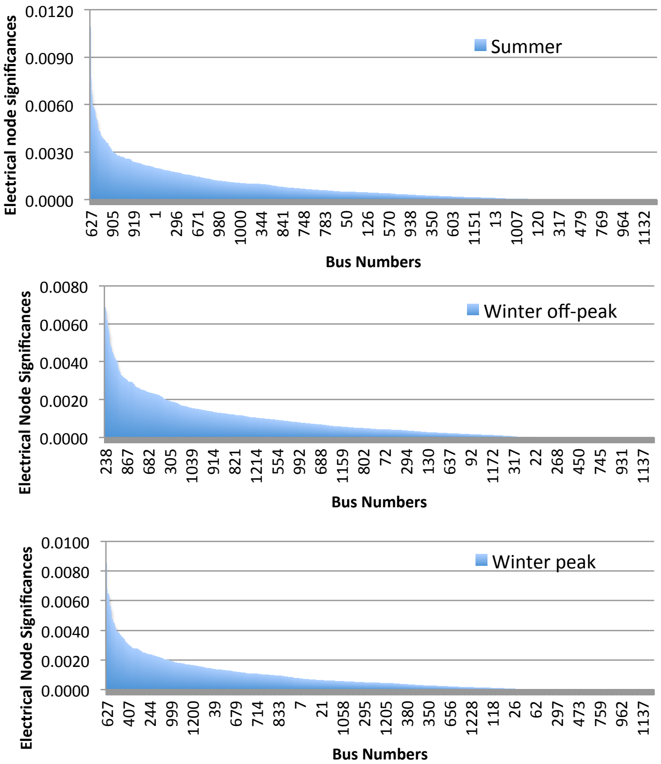

Figure 10: Electical Node Significances Distribution of different UCTE configurations in a descending order

Both Fig. 10 and Tables 3- 4 show that, in a power grid, the cascading failure robustness and the criticality of nodes in the context of cascading failures change depending on the loading profile. This suggests that the power grid robustness against cascading failures is dynamic and increasing this robustness requires reconfiguration/optimization of the grid dynamically.

Table 4: Top 10 critical nodes in UCTE network for different loading profiles

	Summer		Winter off-peak		Winter Peak	
Rank	δ	Node ID	δ	Node ID	δ	Node ID
1	0.0109	627	0.0068	238	0.0085	627
2	0.0076	624	0.0068	535	0.0068	624
3	0.0071	535	0.0068	255	0.0065	829
4	0.0069	829	0.0067	218	0.0065	535
5	0.0066	932	0.0062	624	0.0065	255
6	0.0060	255	0.0062	829	0.0064	238
7	0.0059	623	0.0060	627	0.0063	218
8	0.0058	218	0.0057	486	0.0057	844
9	0.0057	238	0.0057	1122	0.0056	932
10	0.0057	844	0.0055	844	0.0056	486

6 Conclusion and discussion

This paper proposes a metric (R_{CF}) to assess the robustness of a given power grid with respect to cascading failures by targeted attacks. A dynamic model of cascading failures in a power grid is created relying on complex networks theory. A power grid is modelled as a directed graph and DC load flow equations are used to estimate flow values in the model. The proposed robustness metric accounts for the effects of structural properties as well as for the effect of the operative state on network robustness. This is accomplished by two new measures of which R_{CF} is composed: electrical nodal robustness and electrical node significance. The electrical nodal robustness deploys an entropy-based approach to model (i) homogeneity of load distribution; (ii) loading level of the network; and (iii) out-degree of each particular node, while electrical node significance is a nodal centrality measure quantifying the importance of each node in the context of cascading failures robustness. The proposed robustness metric is applied on a conceptual radial network, IEEE test systems, and real-world UCTE network to demonstrate the applicability of the R_{CF} in different use cases. The effectiveness of R_{CF} in anticipating a power grid cascading failures robustness is verified by experimental results from the developed model.

In addition to capturing the effect of the operative states on the power grid robustness, another significant property of the proposed robustness metric is that the computation of the robustness metric R_{CF} does not require executing computational expensive tasks such as simulation of cascading failures (in contrast to [3, 33]). Moreover the metric can be computed in parallel. This makes it possible to compute the robustness metric R_{CF} during run-time and to monitor the robustness level of a grid dynamically. These collective properties of R_{CF} enables it to serve as a real-time measure based on which the network (flow) can be optimized dynamically by deploying flow controlling devices (e.g. phase shifting transform devices, thyristor controlled series capacitor) so that a higher level of robustness can be achieved [20].

Future work will focus on (i) determining the upper and lower bounds of the R_{CF} for a given grid, and (ii) optimizing the grid in a self-organized and distributed manner. After determining the upper and lower bounds of R_{CF}, a robustness threshold value can be determined for a given power grid. When the robustness of a grid is lower than the threshold value then the grid can be intervened. Optimization of the grid implies adapting power flow in the grid dynamically. Within the context of SmartGrids, dynamically optimizing power flow in the grid based on the proposed robustness metric R_{CF} has the potential to ensure a higher level of cascading failure robustness in the network.

Acknowledgements

This work is funded by the NWO project *RobuSmart: Increasing the Robustness of Smart Grids through distributed energy generation: a complex network approach*, grant number 647.000.001. The authors also thank Evangelos Pournaras for fruitful discussions, Prof. Ian Dobson for providing WSCC 179 bus test system data.

References

[1] S. Y. Auyang. *Foundations of complex-system theories: In economics, evolutionary biology, and statistical physics*. Cambridge University Press, Cambridge, UK, 1998.

[2] W.-J. Bai, T. Zhou, Z.-Q. Fu, Y.-H. Chen, X. Wu, and B.-H. Wang. Electric power grids and blackouts in perspective of complex networks. In *Proceedings of International Conference on Communications, Circuits and Systems*, volume 4, pages 2687–2691, june 2006.

[3] Z. J. Bao, Y. J. Cao, G. Z. Wang, and L. J. Ding. Analysis of cascading failure in electric grid based on power flow entropy. *Physics Letters A*, 373:3032–3040, 2009.

[4] A. L. Barabasi and R. Albert. Emergence of scaling in random networks. *Science*, 286:509–512, 1999.

[5] E. Bompard, R. Napoli, and F. Xue. Analysis of structural vulnerabilities in power transmission grids. *International Journal of Critical Infrastructure Protection*, 2(1-2):5–12, May 2009.

[6] E. Bompard, R. Napoli, and F. Xue. Extended topological approach for the assessment of structural vulnerability in transmission networks. *IET Generation, Transmission and Distribution*, 4:716–724, 2010.

[7] B. Carreras, I. Dobson, and J. Thorp. First year progress report: Complex systems approach to cascading failures. Avaliable at: `http://www.see.ed.ac.uk/~jbialek/Europeloadflow/`.

[8] J. Chen, J. S. Thorp, and I. Dobson. Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. *International Journal of Electrical Power Energy Systems*, 27(4):318 – 326, 2005.

[9] J. Conti. The day the samba stopped. *Engineering Technology*, 5(4):46 –47, March 2010.

[10] P. Crucitti, V. Latora, and M. Marchiori. Model for cascading failures in complex networks. *Phys. Rev. E*, 69:045104, 2004.

[11] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman. An Initial Model for Complex Dynamics in Electric Power System Blackouts. In *Hawaii International Conference on System Sciences (HICSS)*, 2001.

[12] I. Dobson, J. Chen, J. S. Thorp, B. A. Carreras, and D. E. Newman. Examining criticality of blackouts in power system models with cascading events. In *Hawaii International Conference on System Sciences (HICSS)*, page 63, 2002.

[13] J. J. Grainger, J. Stevenson, and D. William. *Power System Analysis*. McGraw-Hill, 1994.

[14] IEEE test systems data. Avaliable at: `http://www.ee.washington.edu/research/pstca/`.

[15] R. Kinney, P. Crucitti, R. Albert, and V. Latora. Modeling cascading failures in the north american power grid. *The European Physical Journal B*, 46, 2005.

[16] Y. Koç, M. Warnier, R. E. Kooij, and F. Brazier. A robustness metric for cascading failures by targeted attacks in power networks. In *Proceedings of the IEEE International Conference on Networking Sensing and Control*, 2013.

[17] Y.-C. Lai, A. Motter, and T. Nishikawa. Attacks and cascades in complex networks. pages 299–310. 2004.

[18] V. Latora and M. Marchiori. Efficient behavior of small-world networks. *Phys. Rev. Letters*, 87(19):198701, 2001.

[19] A. E. Motter and Y.-C. Lai. Cascade-based attacks on complex networks. *Phys Rev E*, Dec. 2002.

[20] E. Pournaras, M. Yao, R. Ambrosio, and M. Warnier. Organizational control reconfigurations for a robust smart power grid. In N. Bessis, F. Xhafa, D. Varvarigou, R. Hill, and M. Li, editors, *Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence*, Studies in Computational Intelligence. Springer, 2013.

[21] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans. Usefulness of dc power flow for active power flow analysis. In *Power Engineering Society General Meeting, 2005. IEEE*, pages 454–459 Vol. 1, 2005.

[22] K. Sun and Z.-X. Han. Analysis and comparison on several kinds of models of cascading failure in power system. In *Transmission and Distribution Conference and Exhibition: Asia and Pacific, 2005 IEEE/PES*, 2005.

[23] UCTE data. Avaliable at: `http://www.see.ed.ac.uk/~jbialek/Europeloadflow/`.

[24] U.S.- Canada Power System Outage Task Force, Final Report on the August 14th Blackout in the United States and Canada: Causes and Recommendations, April 2004.

[25] M. Vaiman, K. Bell, Y. Chen, B. Chowdhury, I. Dobson, P. Hines, M. Papic, S. Miller, and P. Zhang. Risk assessment of cascading outages: Part i; overview of methodologies. In *Power and Energy Society General Meeting, 2011 IEEE*, pages 1 –10, july 2011.

[26] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. Kling. Usefulness of dc power flow for active power flow analysis with flow controlling devices. In *The 8th IEEE International Conference on AC and DC Power Transmission*, march 2006.

[27] P. Van Mieghem. *Performance analysis of communications networks and systems*. Cambridge University Press, 2006.

[28] T. Verma. Vulnerability of power grids to cascading failures, 2012.

[29] J. W. Wang and L. L. Rong. Cascade-based attack vulnerability on the us power grid. *Safety Science*, 47:1332–1336, 2009.

[30] J.-W. Wang and L.-L. Rong. Robustness of the western united states power grid under edge attack strategies due to cascading failures. *Safety Science*, 49(6):807 – 812, 2011.

[31] D. J. Watts and S. H. Strogatz. Collective dynamics of small-world networks. *Nature*, 393(6684):440–442, June 1998.

[32] G. P. Williams and J. H. P. book. *Chaos Theory Tamed.* Joseph Henry Press, 1 edition, Oct. 1997.

[33] M. Youssef, C. Scoglio, and S. Pahwa. Robustness measure for power grids with respect to cascading failures. In *Proceedings of the Cnet 2011*, pages 45–49. ITCP, 2011.

[34] T. Zhou and B. H. Wang. Catastrophes in scale-free networks. *Chinese Physics Letters*, 22:1072–1075, 2005.

.