The Impact of the Topology on Cascading Failures in a Power Grid Model

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

Abstract

Cascading failures are one of the main reasons for large scale blackouts in power transmission grids. Secure electrical power supply requires, together with careful operation, a robust design of the electrical power grid topology. Currently, the impact of the topology on grid robustness is mainly assessed by purely topological approaches, that fail to capture the essence of electric power flow. This paper proposes a metric, the effective graph resistance, to relate the topology of a power grid to its robustness against cascading failures by deliberate attacks, while also taking the fundamental characteristics of the electric power grid into account such as power flow allocation according to Kirchoff Laws. Experimental verification on synthetic power systems shows that the proposed metric reflects the grid robustness accurately. The proposed metric is used to optimize a grid topology for a higher level of robustness. To demonstrate its applicability, the metric is applied on the IEEE 118 bus power system to improve its robustness against cascading failures.

1. Introduction

Electric power is indispensable to modern societies. Security and availability of power supply is crucial. Disruption of power delivery systems has severe effects on the public order and substantial economic cost for society [1]. The safe operation of the power grid greatly reduces the risk of large-scale blackouts. Many countries, however, suffer from catastrophic blackouts paralysing daily life [2, 3]. Analysis of

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

international blackout data reveals that the probability distribution of the blackout sizes decreases with the size of the blackout in an approximate power law regime [4] with an exponent between -1 and -2, i.e. doubling the blackout size approximately halves its probability suggesting large scale blackouts are more likely than expected.

Cascading failures are the consequence of the collective dynamics of the complex power grid. Large scale cascades are typically due to propagation of a local failure into the global network. Consequently, analysing and mitigating cascading failures requires a system level approach. Recent advances in the field of network science [5, 6, 7, 8, 9] reveal the promising potential of complex networks theory to investigate power grids vulnerability at a system level.

This paper considers the *vulnerability* of a system as a sensitivity to threats (i.e. malicious attacks) and disturbances (e.g. random failures) that possibly limit the ability of the system to accomplish its tasks, and provide the intended services. As the polar opposite of vulnerability, *robustness* refers to the ability of a system to avoid malfunctioning when a fraction of its elements fail [10].

The operative state (e.g. loading level and power flow distribution), and structural aspects of a power grid (e.g. type of buses and their interconnection), together with the design choices of engineering systems (e.g. the protection systems, automatic controls, and towers and insulators) determine the robustness against cascading failures in a power grid. Enhancing the robustness of a power grid requires a careful assessment of engineering system design choices and optimization of the operative state and the topology of the grid. The operative state of a power grid continuously changes while the topology remains mainly unchanged. Optimization of the operative state of a power grid is a short-term optimization problem and requires a dynamic optimization approach [11, 12, 13]. On the other hand, optimization of the topology is a long-term optimization problem and requires investigating the impact of the grid topology on cascading failures. This paper focuses on the optimization of the topology, and investigates the relationship between a power grid topology and its robustness against cascading failures.

One way to analyse the impact of a power grid topology on the cascading effect is investigating the relationship between the robustness level against cascading failures and the general network properties in models of power grids. The electric power grid has small-world characteristics [6, 14]. A small average shortest path length (together with high clustering coefficient [15]) is one of the key characteristics of the small-world phenomenon. In small-world networks, the average shortest path length might dominate the network dynamics including, for example disease spreading [14]. These studies/results motivate power system researchers to investigate the impact of average shortest path length on the cascading failures robustness in power grids [14, 16]. They deploy a purely topological approach; assume that electric power behaves as a discrete data packet and follows the shortest or the most efficient path between two nodes. Relying on this assumption, the average shortest path length is determined, and its impact on the network robustness is investigated. However, this purely topological approach does not comply with the fundamental characteristics of power grids. Electric power obeys the laws of Kirchoff and flows through all available paths rather than following a distinct path (e.g. shortest path). Therefore, the notion of distance in power grids needs to be tailored based on power systems fundamentals. This paper

proposes the *effective resistance* as a measure of electrical path length between two nodes, and the *effective graph resistance* as a metric for electrical average path length of a power grid. The effective graph resistance [15] relates to the impact of the topology on cascading failure robustness while accounting for the fundamental properties of power grids such as power flow distribution through the grid according to Kirchoff Laws.

2. Dynamic Model of Cascading Failures in Power Grids

A power grid is a three-layered complex interconnected network consisting of generation, transmission, and distribution parts. Electric power is shipped from the generation buses to distribution substations through the transmission buses, all interconnected by transmission lines. Electric power flows in a grid according to Kirchoff's laws. Accordingly, impedances, voltage levels at each individual power station, voltage phase differences between power stations and loads at terminal stations control the power flow in the grid. AC power flow equations are non-linear equations that approximate the flows of both active and reactive powers. DC load flow equations are a linearised version of the AC power flow equations considering only flow of active power [17]. DC power flow analysis introduces an average line flow error up to 5% while it is 7 to 10 times faster than AC load flow model [17]. Following Ref. [18, 19, 20, 21], this paper deploys DC load flow analysis to estimate the flow values across the network.

The maximum capacity (i.e. flow limit) of a line is defined as the maximum power flow that can be afforded by the line. The flow limit of a transmission line is imposed by thermal, stability or voltage drop constraints [22]. In line with other recent studies [23, 24, 25, 26, 27, 28], this paper assumes that the maximum capacity of a line relates to its base (i.e. initial) load as follows:

$$C_i = \alpha_i L_i(0) \tag{1}$$

where C_i is the maximum capacity, $L_i(0)$ is the base load, and α_i [23] is the tolerance parameter of line i. In a power grid, each line has a relay protecting it from permanent damage due to e.g. excessive flows. For instance, in case of overloading, an over-current relay [29] notifies a circuit breaker to trip a line, when the current of the line remains exceeding its rated limit (i.e. maximum capacity) for a period of time, to avoid permanent damage of the line. For the sake of simplicity, this paper assumes a deterministic model for the line tripping mechanism, i.e. a circuit breaker for a line trips at the moment the flow of the line exceeds its rated limit. [2]

An initial outage of a component changes the balance of the power flow distribution over the grid and causes a redistribution of the power flow over the network. This dynamic response of the system to this triggering event might overload other parts in the network. The protection mechanism trips these newly overloaded components, and the power flow is again redistributed potentially resulting in new overloads. In case

[2] While the over-current relays are not the only relays that are used in the power transmission grid, for the sake of simplicity, this paper models the other type of relaying mechanisms (e.g. distance and differential protection) as over-current relays.

of islanding, cascading failures continue in each island in which generators or loads are shed respectively to attain a power balance. The cascade of failures continues until no more components are overloaded. After the cascade subsides, the robustness of the grid against cascading failures is quantified in terms of the fraction of the served power demand (DS) after the cascading failures.

3. Effective Graph Resistance in Electric Power Grids

This section explains the relevant basic concepts from complex networks theory, presents the effective graph resistance, and elaborates on how it is computed in electric power grids.

3.1. Complex networks preliminaries

A network *G($\mathcal{N}$,$\mathcal{L}$)* consisting of a set $\mathcal{N}$ of *N* nodes and a set of $\mathcal{L}$ of *L* links, can fully be represented by its adjacency matrix A. The *adjacency matrix* of a simple, unweighted graph *G($\mathcal{N}$,$\mathcal{L}$)* is an $N \times N$ symmetric matrix reflecting the interconnection of the nodes in the graph: $a_{ij} = 0$ indicates that there is no edge, otherwise $a_{ij} = 1$. In case of a weighted graph, the network is represented by a weighted adjacency matrix W where w_{ij} corresponds to the weight of the link between nodes i and j; a weight can be a distance, cost, or delay.

The *Laplacian matrix* [15] Q is another way to fully characterize a graph, and is defined as:

$$Q = \Delta - A \tag{2}$$

where Δ is the diagonal matrix of the strengths of G: δ_i=$\sum_j^N w_{ij}$. Hence, the Laplacian can be constructed as follows:

$$Q_{ij} = \begin{cases} \delta_i, & \text{if } i = j. \\ -w_{ij}, & \text{if } i \neq j \text{ and } (i,j) \in L \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

A *path* P_{ij} between pair of nodes *i* and *j* refers to the set of links connecting these nodes. The *path length* $l(P_{ij})$ is the sum of the weights of constituent edges in the path P_{ij}. The shortest path length $l(P_{ij}^*)$ is the minimizer of $l(P_{ij})$ over all P_{ij}. The *average shortest path length* l_G of a network G is defined as:

$$l_G = \frac{1}{N(N-1)} \sum_{i \neq j \in G} l(P_{ij}^*) \tag{4}$$

3.2. Effective graph resistance and its computation in electric power grids

The effective resistance [15] R_{ij} between a pair of nodes i and j is the potential difference between these nodes when a unit current is injected at node i and withdrawn at node j. And the effective graph resistance R_G is the sum of the individual effective resistance between each pair of nodes in the network. Computation of the effective graph resistance for a power grid necessitates information about the topology of the grid (i.e. interconnection of nodes), and reactance (or susceptance [30]) values of the

transmission lines in the grid. The effective graph resistance can be computed in two different ways: (a) by aggregating the effective resistances between each pair of nodes, and (b) by the eigenvalues of the Laplacian matrix of the grid.

The required steps to compute the effective graph resistance based on pairwise effective resistances are (i) constructing the Laplacian matrix of the grid, (ii) determining the generalised inverse of the Laplacian matrix, (iii) computing effective resistances between each pair of nodes, and (iv) summing up the effective resistances.

The Laplacian matrix of a power grid Q reflects the interconnection of buses with transmission lines. The weight w_{ij} corresponds to the susceptance (i.e. inverse of reactance) value between nodes *i* and *j*. The Laplacian matrix constructed by the susceptance values is equivalent to the admittance matrix in the electrical power systems theory.

The *effective resistance* R_{ij} between any pair of nodes i and j is computed as:

$$R_{ij} = Q^{+}_{ii} - 2Q^{+}_{ij} + Q^{+}_{jj} \tag{5}$$

where Q^{+} is the Moore-Penrose pseudo-inverse of the Q.

The *effective graph resistance* R_G of a power network is then computed by summing up all the effective resistances between all pairs in a network.

$$R_G = \sum_{i=1}^{N} \sum_{j=i+1}^{N} R_{ij} \tag{6}$$

Another way to compute the effective graph resistance of a power grid requires computation of the eigenvalues of the Laplacian matrix of the grid. This approach requires summing the inverse of the eigenvalues:

$$R_G = N \sum_{i=1}^{N-1} \frac{1}{\mu_i} \tag{7}$$

where μ_i is the i^{th} eigenvalue of the Laplacian matrix, and $\mu_1 \geq \mu_2 \geq ... \geq \mu_{N-1} \geq \mu_N$. This methodology is computationally more efficient, but it does not give any insight into the individual electrical path lengths between pair of buses.

4. Effective Graph Resistance as a Robustness Metric

Modelling power grid dynamics requires taking the power flow into account. In a dynamic power grid model, electric power flows through multiple paths. This precludes the existence of a distinct path (and subsequently the existence of the shortest path) between two nodes in a physical power grid. Yet, the concept of *equivalent impedance* makes it possible to determine a distinct *electrical path* between two nodes by conceptually replacing the multiple paths between two nodes with a single equivalent path. Fig. 1 illustrates the concept.

The concept of electrical path length makes it possible to construct the *electrical topology* of a power grid. An electrical topology of a power grid shows the electrical

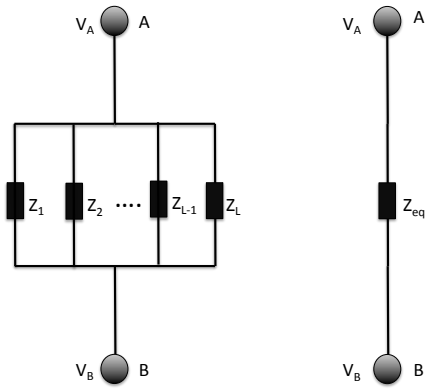

Figure 1: The equivalent impedance transforms the multiple L paths between nodes A and B with impedances $Z_1, Z_2, .., Z_L$ (on the left hand side) to a one single conceptual path with an impedance value $Z_{eq,AB}$ (on the right hand side).

connections/path lengths (i.e. equivalent impedances) between buses, rather than the physical connections as a physical topology does. In a power grid, the actual "distance" between two nodes is the electrical path length, and not the physical distance (or number of lines). Accordingly, the electrical topology of a power grid governs the network dynamics rather than the physical topology. Fig. 2 shows the physical and the electrical topology of the Institute of Electrical and Electronics Engineers (IEEE) 30 buses power system [31].

The initial concepts of "electrical distance" are discussed by power system researchers [32, 33, 34], and also by mathematicians as *effective resistance* [35, 36]. In a power grid, the effective resistance R_{ij} between buses i and j equals the equivalent impedance between these buses. Hence, in the electrical topology in Fig. 2, the connections are the effective conductances $(1/R_{ij})$ between each pair of nodes. The *effective graph resistance* R_G of a power grid G is an aggregate value of all effective resistances between any pair of nodes in a grid (see Eq. 6).

The existence of parallel paths between two nodes in a physical power grid topology, and a homogeneous distribution of their impedance values result in a smaller effective resistance between these two nodes (i.e. a stronger connection between these nodes in the electrical topology). The number of parallel paths in the physical topology refers to the number of redundant (backup) paths. In case of a failure in one of the paths between two nodes, the power flow carried by the rendered path is distributed over the backup paths. Therefore, a higher number of backup paths implies a more robust network against cascading failures due to line overloads. On the other hand, a relatively more homogeneous distribution of the impedance values results in a relatively more homogeneous distribution of power flow over these parallel paths increasing the robustness of the power grid against cascading failures [11, 12]. Therefore, a power grid with a relatively smaller effective graph resistance implies a relatively more robust power grid with respect to cascading failures.

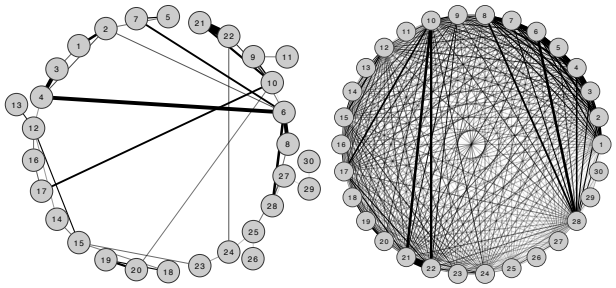

Figure 2: The physical (left) and the electrical (right) topology of IEEE 30 power system. In the physical topology the conductances, and in the electrical topology the equivalent conductances (i.e. $1/Z_{eq}$), are used as weights for a better illustration. A relatively thicker and more visible line corresponds to a stronger connection/a shorter electric path length (i.e. a smaller effective resistance), while a relatively thinner and less visible line corresponds to a relatively weaker connection/ a larger electric path length (i.e. larger effective resistance).

5. Effective Graph Resistance and Power Grid Robustness: Experimental Verification

This section verifies the potential of effective graph resistance to anticipate the cascading failures robustness of power networks. Experimental verification of the proposed robustness metric requires (i) creating synthetic test systems, (ii) determining the effective graph resistance of these synthetic test systems (i.e. theoretical results) and their robustness levels by simulations (i.e. experimental results that are considered as the ground truth), and (iii) quantifying the correlation between the theoretical results and experimental results to assess whether the effective graph resistance anticipates the power grid robustness with respect to cascading failures.

5.1. Test systems

The data required for the metric verification analysis includes the topology of a power grid (i.e. interconnection of buses with lines), reactance values of transmission lines, the types buses and their generation capacity and load values. Since the IEEE power systems provide all these data, they are considered as the reference systems and additional synthetic test systems are created based on them.

These synthetic test systems are generated with exactly the same properties as the reference IEEE test system (e.g. type and number of buses/lines, demand/generation capacity values, and the topology) except for the impedance values of certain randomly chosen lines. In each test system, all of the parameters that have an impact on the robustness (e.g. topology, generation/loading profile, and loading level) are fixed, except for the effective graph resistance and the power flow distribution over the grid that relates to the robustness. This assures that the differences in the robustness levels of these test systems is due to the change in the effective graph resistance of these grids, thus making it possible to assess the impact of the effective graph resistance on the grid robustness.

To vary effective graph resistance, an arbitrary number of the links of the reference IEEE test systems are randomly chosen and the reactance values of these transmission lines are increased. For example, when creating a synthetic test system based on the IEEE 118 power system [31], e.g. 4 transmission lines are randomly chosen: l_1, l_2, l_3, l_4. The reactance values of these lines (i.e. x_1, x_2, x_3, x_4) are doubled and a new synthetic test system is created with the new reactance values: $2x_1$, $2x_2$, $2x_3$, $2x_4$ for lines l_1, l_2, l_3, l_4 respectively.

The new synthetic test system has an increased R_G as the effective graph resistance is a monotonic increasing function of the individual reactance values in a network [36]. It also has a different robustness level against cascading failures because the manipulated impedances affect the power flow distribution in the networks [11, 12].

A second synthetic test system is created from the reference IEEE 118 power system by increasing the reactance values of the same lines l_1, l_2, l_3, l_4 by a factor of three resulting in the impedance values of $3x_1$, $3x_2$, $3x_3$, $3x_4$, respectively. The additional synthetic test systems are created following the same procedure.

5.2. Robustness levels by effective graph resistance and by simulations

The effective graph resistance is proposed in this paper to quantify the *theoretical* robustness levels of the test systems against cascading failures. The R_G of the test systems is compared to the simulation-based robustness levels to verify that R_G anticipates the grid robustness. The computation of R_G requires data about the admittance matrix of the systems (i.e. reactance values of the transmission lines and the topology of the grid). The effective graph resistance of each test system is calculated by Eq. 5 and Eq. 6 in Sec. 3. The *experimental* robustness levels of created synthetic power grids are determined using simulations. MATCASC [37] (a MATLAB-based tool implementing cascading failure simulations in power grids) is used to simulate cascading failures and to quantify the grid robustness. Cascading failures by targeted attacks are simulated for different values of tolerance parameter α (i.e. for different loading levels). DS metric is used to quantify the robustness of the test systems after the cascades subsides.

This paper uses an attack strategy based on the electrical node significance metric [11, 12]. The electrical node significance is a contextual node centrality measure, specifically designed for power grids. The electrical node significance δ of a node *i* is defined as the amount of power distributed by node *i*, normalized by the total amount of the power that is distributed in the entire grid:

$$\delta_i = \frac{P_i}{\sum_{j=1}^{N} P_j} \tag{8}$$

where P_i stands for total power distributed by node i while N refers to number of nodes in the network. This paper attacks a power grid by targeting *the most heavily loaded outgoing link from the node with the highest electrical node significance* in the network. Removal of this link most likely results in the largest cascading failure in the power network [38].

Assessing the robustness of a power grid against cascading failures by targeted attacks for an interval of tolerance parameters [α_{min}, α_{max}] results in the *robustness*

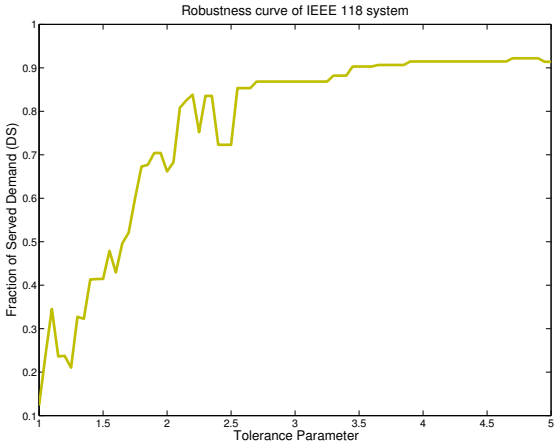

Figure 3: The robustness curve for the IEEE 118 test system

curve of the grid. For example, Fig. 3 shows the robustness curve for the IEEE 118 power system [31] obtained for [α_{min}=1, α_{max}=5] subdivided with Δ_α=0.05. The robustness curve in Fig. 3 suggests that, when the network is loaded by 20% (i.e. α=5), an attack results in the loss of almost 10% of the total demand. However, an attack when α=1.3 (i.e. *loading level* $\simeq$ 77%) results in collapse of the network and only 20% of the total demand can be satisfied.

Traditionally, power grid researchers focus on the robustness of a grid for a specific tolerance level of the grid. However, this paper considers the robustness of a power grid over the whole spectrum of tolerance levels (i.e. loading levels), and defines mathematically the normalized area r below the robustness curve as an empirical metric that quantifies the power grid robustness against cascading failures. The normalized area below a robustness curve is computed by a Riemann sum [39]:

$$r = \frac{1}{(\alpha_{max} - \alpha_{min})} \sum_{i \in d} DS(\alpha_i)\Delta_\alpha \tag{9}$$

where $DS(\alpha_i)$ is the DS after a cascading failure is triggered by an attack when the tolerance of the network is α_i, and d is the size of the set of tolerance parameters at which the robustness levels are determined. Because the maximum value of DS is 1, $(\alpha_{max} - \alpha_{min})$ refers to the maximum possible area below the robustness curve. Consequently, the factor $1/(\alpha_{max} - \alpha_{min})$ in Eq. 9 normalizes the area below the robustness curve ensuring that r has a value between 0 and 1. Evaluation of Eq. 9 for the robustness curve of a grid results in the experimental robustness level of the grid with respect to cascading failures. On the other hand, the vulnerability of the grid is the complementary of the robustness of the grid and defined as:

$$v = 1 - r \tag{10}$$

where v is the measure of vulnerability of the system, also having a value between 0 and 1.

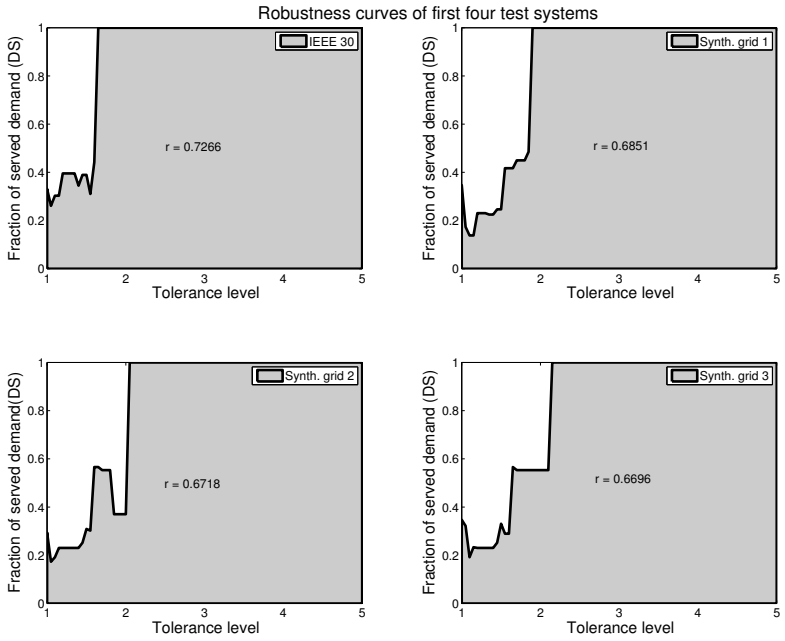

Figure 4: The robustness curves for the IEEE 30 and first 3 synthetic test systems, and the corresponding robustness (i.e. r) values. The test systems have their effective graph resistances in an ascending order, while their robustness levels are step by step decreasing.

5.3. Assessing the effectiveness of the effective graph resistance in anticipating power grid robustness

To gain more insight into the impact of R_G on the grid robustness, first a qualitative analysis is performed for a relatively small set of test systems. The IEEE 30 power system (see Fig. 2) is considered as a reference system. 4 lines are chosen randomly: l_2 (connecting nodes 1 and 3), l_{14} (connecting nodes 9 and 10), l_{38} (connecting nodes 27 and 30), l_{41} (connecting nodes 6 and 28), and based on the methodology explained in Sec. 5.1, three additional test systems are created. The robustness of these systems are determined by R_G and by r. Table 1 provides the R_G and r values while Fig. 4 shows the robustness curves of these test systems.

The effective graph resistance is a monotonic increasing function of the individual

Table 1: Effective graph resistance (R_G) and simulation-based robustness levels (r) of IEEE 30 and 3 synthetic test systems

	R_G	$r(\%)$
IEEE 30	151.86	72.66
Synthetic grid 1	162.71	68.51
Synthetic grid 2	169.43	67.18
Synthetic grid 3	174.07	66.96

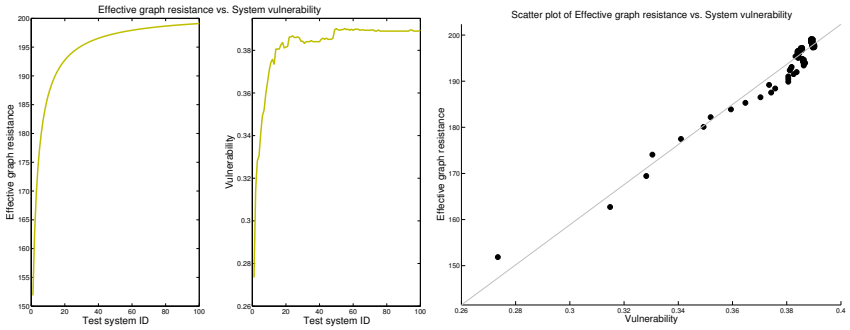

Figure 5: Experimental verification of the effective graph resistance for IEEE 30 test system. For 100 synthetic test systems, on the left hand side the effective graph resistance and the vulnerability values are plotted. On the right hand side a scatter plot visualizes the correlation between effective graph resistance and system vulnerability. Results show that the effective graph resistance captures the system vulnerability accurately.

impedance (consisting of resistance and reactance) values in the grid [36]. Accordingly, in Table 1, R_G increases as a result of the increase of individual reactance values. This indicates that the typical average electrical path length between the buses in the synthetic grids is increasing incrementally making these grids relatively loosely coupled. On the other hand, as a result of the increase of reactance values in these synthetic grids, r becomes step by step smaller: synthetic grid I is more robust compared to synthetic grid II, synthetic grid II is more robust compared to synthetic grid III, and so forth. Hence, the theoretical results (i.e. R_G) are evidently in line with the simulation results, and suggest that increasing the effective graph resistance of the IEEE 30 power system makes it less robust (i.e. more vulnerable) against cascading failures by targeted attacks. Fig. 4 visualizes the impact of R_G on grid robustness: an increase in R_G makes the power grid robustness smaller.

A statistically robust quantitative assessment of the impact of the effective graph resistance on the power grid robustness requires the robustness analysis for a larger set of networks. Accordingly, the small set of 4 test systems (see Table 1) is expanded to a set of 100 test systems. The effective graph resistances and the empirical robustness levels (i.e. r) of these networks are determined. The correlation level between these theoretical and experimental robustness levels is quantified: the linear correlation coefficient between R_G and r is over -90%. This nearly perfect anti-correlation level suggests that, in the deployed model, the effective graph resistance anticipates the power grid robustness with respect to cascading failures accurately. Fig. 5 plots R_G, v, and scatter diagram of R_G and v. Results in Fig. 5 visualizes how the effective graph resistance captures the power grid robustness. The vulnerability is plotted rather than the experimental robustness r for better illustration of coherence between the theoretical and experimental results.

Alternating the reactance values in a grid causes a different power flow distribution in the grid and, in turn, results in a different level of robustness against cascading failures [11, 12]. Fig. 5 shows that the vulnerability v reflects the variations in R_G of

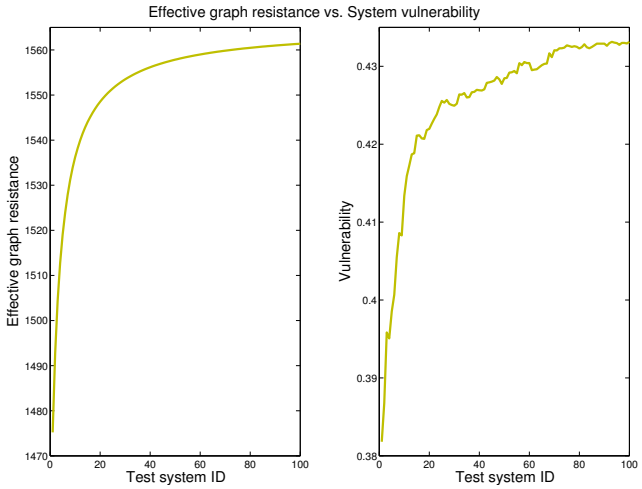

Figure 6: Experimental verification of the effective graph resistance for IEEE 118 test system. For 100 synthetic test systems, the effective graph resistance (on the left hand side), and the vulnerability values (on the right hand side) are plotted.

the power grids accurately: a steep increase in the grid effective graph resistance results in a steep increase in the grid vulnerability (i.e. steep drop in grid robustness), while a slight increase in the grid effective graph resistance causes a slight increase in the grid vulnerability (i.e. a slight drop in the grid robustness).

To investigate the validity of the impact of R_G on power grid robustness, the robustness analysis is performed for the larger IEEE 118 power systems. Again four lines are randomly chosen: l_{31} (connecting buses 23 to 25), l_{35} (connecting buses 28 to 29), l_{93} (connecting buses 59 to 63), and l_{175} (connecting buses 109 to 110). Furthermore, 99 additional test systems are created. For these test systems, R_G is computed and the experimental robustness levels are obtained by r (and grid vulnerability by v). Fig. 6 shows the R_G and v values for the 100 test systems. The correlation level between R_G and r resides again over -90%.

The experimental results (see Fig. 5 and Fig. 6) show that the effective graph resistance captures the robustness of the IEEE power systems accurately and suggests that an increased effective graph resistance results in a less robust power grid against cascading failures, as proposed in Sec. 4.

6. Use Case: Application for Power Grids

The aptitude of effective graph resistance to relate a power grid topology to its robustness can be exploited in different ways, including designing robust networks from scratch and identifying critical components in a power grid. Furthermore R_G also acts as a measure based on which a grid topology is optimized to maximize the grid robustness. The next section focusses on optimization of the IEEE 118 power system topology for a higher level of robustness against cascading failures.

6.1. Upgrading IEEE 118 power system to improve grid robustness

As a response to blackouts, additional transmission lines are placed to increase the power grid robustness. Determining the right pair of buses to connect in order to maximize the grid robustness is the challenge[3]. A solution to this problem requires (i) determining all possible additional transmission lines (i.e. candidate transmission lines), and (ii) assessing the impact of each candidate transmission line on the effective graph resistance.

For a grid consisting of N buses and L transmission lines, an additional line can be placed between any unconnected pair of nodes. Therefore, there are in total $\frac{N(N-1)}{2} - L$ number of lines that can be added to an existing power grid.

To assess the impact of an additional line on the effective graph resistance (i.e. on the grid robustness), this section deploys an analogous approach to the one given in [40, 41]: the optimum location for an additional line is determined by assessing its relative change on the effective graph resistance value of the original power grid. Because the effective graph resistance is a monotonic decreasing function of the number of lines [36] in a grid, adding a transmission line to an existing grid decreases the effective graph resistance of the grid. Therefore, the optimum location of an additional line is determined based on the relative decrease in R_G that is caused by adding the line l:

$$\Delta R_G^l = \frac{R_G - R_{G+l}}{R_G} \tag{11}$$

where G, $R_G(G+l)$ is the effective graph resistance of the improved grid, and ΔR_G^l is the relative decrease in the effective graph resistance of G as a result of adding line l.

The IEEE 118 power system is considered as a test case and the optimum location for an additional line to upgrade the power system is investigated. The IEEE 118 test system has 118 buses and 186 transmission lines. Hence, there are 6724 possible lines to be added. The reactance value of a candidate transmission line is assumed to be the average of all transmission lines in the IEEE 118 test system. For each of these candidate lines, Eq. 11 is evaluated and its impact on the effective graph resistance is determined. From these 6724 lines, Table 2 shows the top 10 most influential transmission lines to be added to IEEE 118 power system, while Fig. 7 plots the lines that have an impact higher than 0.7%.

The results in Table 2 and Fig. 7 can be used as starting point for an economic analysis. Since the impact of adding a line is not very different for the top ten candidates (see Table 2 and Fig. 7) a cost function can be used to determine which of these lines provides a significant increase in grid robustness at an acceptable or minimal cost.

Table 2 shows that the largest decrease in the effective graph resistance is achieved by adding a transmission line between nodes 111 and 117 (line ID 73 in Fig. 7). Placing a line between these nodes results in a decrease of nearly 0.79% in the effective graph resistance of the original power system.

[3]This section focuses on maximizing the grid robustness rather than minimizing the economic cost of placing a transmission line.

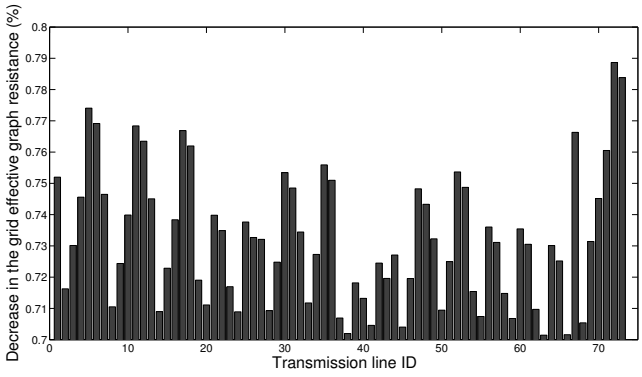

Figure 7: Relative decrease in the effective graph resistance as a result of adding a line for IEEE 118 test case. From 6724 total lines, 74 lines whose addition to IEEE 118 buses power system results in a R_G decrease of 0.7% or higher.

Table 2: The top 10 most influential lines to add in IEEE 118 system

Line ID	$\Delta R_G^l(\%)$
$l_{111-117}$	0.788
$l_{112-117}$	0.783
l_{1-111}	0.774
l_{1-112}	0.769
l_{2-111}	0.768
l_{3-111}	0.767
l_{87-117}	0.765
l_{2-112}	0.763
l_{3-112}	0.761
$l_{110-117}$	0.760

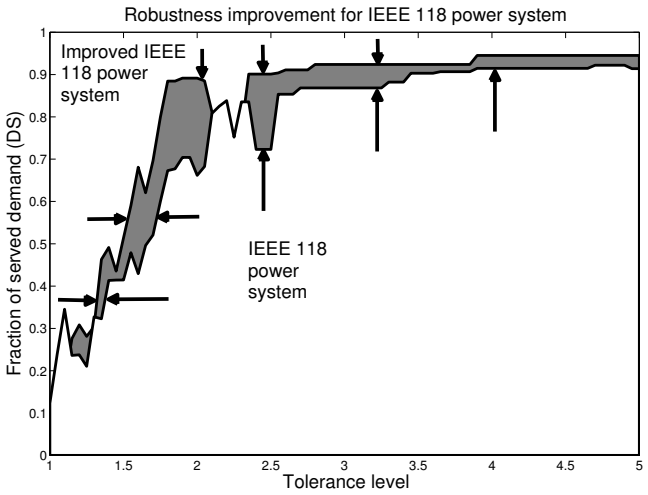

Figure 8: Robustness curves of IEEE 118 and improved IEEE 118 power systems. The difference (i.e. robustness improvement) is highlighted.

To assess the impact of placement of the additional line $l_{111-117}$ on the grid robustness, the robustness curve of the improved topology, and its robustness r are determined. The improved grid has a robustness r=0.6570 which is an increase by 6.7% compared to the original grid robustness (i.e. 0.6182). Fig. 8 plots the robustness curves of both topologies, and highlights the improvement in the grid robustness (shaded area in grey in Fig. 8).

7. Discussion and Conclusion

This paper proposes the *effective graph resistance* R_G as a metric to assess the impact of the power grid topology G on the robustness against cascading failures due to line overloads by targeted attacks. The effective graph resistance takes the number of backup paths and their ability to accommodate power flows into account to quantify power grid robustness. The experimental verification on IEEE and synthetic power systems demonstrates the ability of R_G to estimate the grid robustness against cascading line failures. Experimental results from simulations show that increasing the effective graph resistance of synthetic power systems results in decreased grid robustness against cascading failures by targeted attacks. The proposed metric is used to optimize the topology of the IEEE 118 power system to improve its robustness. Results show that adding a single line to IEEE 118 power system based on the effective graph resistance analysis improves the grid robustness by 6.7%.

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.

[1] P. Hines, K. Balasubramaniam, and E. Sanchez, "Cascading failures in power grids," *IEEE Potentials*, vol. 28, pp. 24–30, 2009.

[2] J. Conti, "The day the samba stopped," *Engineering Technology*, vol. 5, no. 4, pp. 46 –47, March 2010.

[3] "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.

[4] I. Dobson, A. B. Carreras, V. L. Lynch, and D. E. Newman, "Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization," *Chaos*, vol. 17, no. 1, p. 026103, 2007.

[5] A. L. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, 1999.

[6] D. J. Watts and S. H. Strogatz, "Collective dynamics of small-world networks," *Nature*, vol. 393, no. 6684, pp. 440–442, June 1998.

[7] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[8] X. Huang, S. Shao, H. Wang, S. V. Buldyrev, S. Havlin, and H. E. Stanley, "The robustness of interdependent clustered networks," *EPL*, vol. 101, p. 18002, 2013.

[9] S. Trajanovski, J. MartÃ■n-HernÃąndez, W. Winterbach, and P. Van Mieghem, "Robustness envelopes of networks," *Journal of Complex Networks*, vol. 1, pp. 44–62, 2013.

[10] M. Rosas-casals, S. Valverde, and R. V. Sole, "Topological vulnerability of the european power grid under errors and attacks," *Int. J. Bifur. Chaos*, vol. 17, pp. 2465–2475, 2007.

[11] Y. Koç, M. Warnier, R. E. Kooij, and F. Brazier, "A robustness metric for cascading failures by targeted attacks in power networks," in *Proc. of the IEEE Int. Conf. on Networking Sensing and Control*, 2013, pp. 48–53.

[12] Y. Koç, M. Warnier, R. E. Kooij, and F. M. Brazier, "An entropy-based metric to quantify the robustness of power grids against cascading failures," *Safety Science*, vol. 59, pp. 126 – 134, 2013.

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

[14] C. J. Kim and O. B. Obah, "Vulnerability assessment of power grid using graph topological indices," *Int. J. of Emerging Electric Power Systems*, vol. 8, pp. 1–15, 2007.

[15] P. Van Mieghem, *Graph Spectra for Complex Networks*. Cambridge, UK: Cambridge University Press, 2011.

[16] X. Chen, Q. Jiang, and Y. Cao, "Impact of characteristic path length on cascading failure of power grid," in *Proc. of the Int. Conf. on Power System Technology*, 2006, pp. 1–5.

[17] 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 *Proc. of the 8th IEEE Int. Conf. on AC and DC Power Transmission*, 2006, pp. 58–62.

[18] I. Dobson, "Where is the edge for cascading failure?: challenges and opportunities for quantifying blackout risk," in *Power Engineering Society, IEEE General Meeting*, 2007, pp. 1–8.

[19] 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," *Phys. Lett. A*, vol. 373, pp. 3032–3040, 2009.

[20] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the north american power grid," *Eur. Phys. J. B*, vol. 46, pp. 101–107, 2005.

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

[22] J. D. D. Glover and M. S. Sarma, *Power System Analysis and Design*, 3rd ed. Brooks/Cole Publishing Co., 2001.

[23] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys Rev E*, p. 065102, 2002.

[24] A. E. Motter, "Cascade control and defense in complex networks," *Phys Rev. Lett.*, p. 098701, 2004.

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

[26] T.-L. Ma, J.-X. Yao, C. Qi, H.-L. Zhu, and Y.-S. Sun, "Non-monotonic increase of robustness with capacity tolerance in power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 21, pp. 5516 – 5524, 2013.

[27] G. Chen, Z. Y. Dong, D. J. Hill, and G. H. Zhang, "An improved model for structural vulnerability analysis of power networks," *Physica A: Statistical Mechanics and its Applications*, vol. 388, no. 19, pp. 4259 – 4266, 2009.

[28] G. Chen, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," *Physica A: Statistical Mechanics and its Applications*, vol. 389, no. 3, pp. 595 – 603, 2010.

[29] Y. Zhang, M. Prica, M. Ilic, and O. Tonguz, "Toward smarter current relays for power grids," in *Power Engineering Society General Meeting, 2006. IEEE*, 2006, p. 8.

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

[31] "IEEE test systems data," avaliable at: `http://www.ee.washington.edu/research/pstca/`.

[32] P. Hines and S. Blumsack, "A centrality measure for electrical networks," in *Proc. of the Hawaii Int. Conf. on System Sciences*, 2008, pp. 185–185.

[33] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos*, vol. 19, no. 1, p. 13119, 2009.

[34] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," *IJCIP*, vol. 2, no. 1-2, pp. 5–12, May 2009.

[35] D. J. Klein and M. Randic, "Resistance distance," *Mathematical Chemistry*, vol. 12, no. 1, pp. 81–95, 1993.

[36] W. Ellens, F. M. Spieksma, P. Van Mieghem, A. Jamakovic, and R. E. Kooij, "Effective graph resistance," *Linear Algebra and Its Applications*, vol. 435, pp. 2491–2506, 2011.

[37] Y. Koç, T. Verma, N. Araujo, and M. Warnier, "Matcasc: A tool to analyse cascading line outages in power grids," in *arXiv e-Print archive: 1308.0174*, 2013. [Online]. Available: http://arxiv.org/abs/1308.0174

[38] T. Verma, W. Ellens, and R. E. Kooij, "Context-Independent Centrality Measures Underestimate the Vulnerability of Power Grids," in *arXiv e-Print archive: 1304.5402*, 2012. [Online]. Available: http://arxiv.org/abs/1304.5402

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

[40] V. Latora and M. Marchiori, "Vulnerability and protection of infrastructure networks," *Phys. Rev. E*, vol. 71, no. 1, Jan. 2005.

[41] P. Van Mieghem, D. Stevanovic, F. Kuipers, C. Li, R. van de Bovenkamp, D. Liu, and H. Wang, "Decreasing the spectral radius of a graph by link removals," *Phys. Rev. E*, vol. 84, p. 016101, 2011.