A network approach for power grid robustness against cascading failures

Xiangrong Wang[1], Yakup Koç[2], Robert E. Kooij[1,3], Piet Van Mieghem[1]
[1]Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, The Netherlands
[2]Systems Engineering Section, Faculty of Technology, Policy and Management, Delft University of Technology, The Netherlands
[3]TNO (Netherlands Organization for Applied Science Research), Information and Communication Technology, The Netherlands

***Abstract*—Cascading failures are one of the main reasons for blackouts in electrical power grids. Stable power supply requires a robust design of the power grid topology. Currently, the impact of the grid structure on the grid robustness is mainly assessed by purely topological metrics, that fail to capture the fundamental properties of the electrical power grids such as power flow allocation according to Kirchhoff's laws. This paper deploys the effective graph resistance as a metric to relate the topology of a grid to its robustness against cascading failures. Specifically, the effective graph resistance is deployed as a metric for network expansions (by means of transmission line additions) of an existing power grid. Four strategies based on network properties are investigated to optimize the effective graph resistance, accordingly to improve the robustness, of a given power grid at a low computational complexity. Experimental results suggest the existence of Braess's paradox in power grids: bringing an additional line into the system occasionally results in decrease of the grid robustness. This paper further investigates the impact of the topology on the Braess's paradox, and identifies specific sub-structures whose existence results in Braess's paradox in power grids. Careful assessment of the design and expansion choices of grid topologies incorporating the insights provided by this paper optimizes the robustness of a power grid, while avoiding the Braess's paradox in the system.**

I. Introduction

The electrical power grid is crucial for economic prosperities of modern societies. Disruptions to electrical power grids paralyze the daily life and cause huge economical and social costs for these societies [5], [16], [32]. The strong dependency of other crucial infrastructures such as telecommunication, transportation and water supply on electrical power grids amplifies the severity of large scale blackouts [13]. The key importance of the power grid encourages further research into sustaining power system reliability and developing new approaches to evaluate and mitigate the risk of cascading blackouts.

Cascading failures are one of the main reasons for large scale blackouts [7]. Cascading failures are the consequence of the collective dynamics of a complex power grid. Large scale cascades are typically due to the propagation of a local failure into the global network [36]. Consequently, analyzing and mitigating cascading failures requires a system level approach. Recent advances in the field of network science [8], [14] provide the promising potential of complex network theory to investigate the robustness of power grids at a system level. The robustness of power grids in this paper refers to their maintenance of function after cascading failures triggered by targeted attacks.

Analyzing and improving the network robustness includes two parts. The first goal is the proposal of a proper metric that characterizes the robustness of a specific class of networks [24], [29]. A second goal is to propose efficient strategies on graph modification in order to increase the value of the proposed robustness metric. Consequently, an effective robustness metric that incorporates the essence of the power grids and effective strategies for graph modification are required to improve the robustness of power grids.

The effective graph resistance is a graph metric which characterizes the essence of electrical power grids such as power flow allocation according to Kirchhoff's laws. Researchers in [17] shows that the effective graph resistance effectively captures the impact of cascading failures in a power grid. The lower the effective graph resistance is, the more robust a power grid is against cascading failures. Moreover, adding a link decreases the effective graph resistance [9]. This paper focuses on enhancing the grid robustness against cascading failures by applying the effective graph resistance as a metric for network expansion.

Determining the right pair of nodes to connect in order to maximize the robustness is a challenge. Exhaustive search, i.e. checking all the possibilities, is computationally expensive. Compared to exhaustive search, this paper proposes four strategies that provide a trade-off between a higher decrease of the effective graph resistance and a lower computational complexity.

Exhaustively evaluating the impact of each link addition on robustness reveals the occurrence of Braess's paradox in power grids. Braess's paradox, originally found in traffic networks [2], shows that adding a link can decrease the robustness of the network. Specific sub-structures that might result in Braess's paradox by adding an extra link are investigated. Simulation results indicate that the effective graph resistance effectively identifies a link whose addition increases the robustness while avoids the Braess's paradox. Moreover, most of the strategies highly increase the robustness at a low computational complexity.

This paper is organized as follows: Section II introduces the model of cascading failures in power grids. Section III presents the computation of the effective graph resistance in power grids. Strategies to add a transmission line are illustrated in Section IV. The experimental methodology is illustrated in Section V and the improvement of the grid robustness is evaluated in Section VI. Section VII concludes the paper.

II. Model of Cascading Failures in Power Grids

A power grid is a three-layered network consisting of generation, transmission and distribution parts. A graph can represent a power grid where nodes are generation, transmission, distribution buses and substations, and links are transmission lines. Additionally, links are weighted by the admittance (or impedance) values of the corresponding transmission lines.

Electrical power in a grid is distributed 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. This paper approximates the flow values in a grid by using a linear DC flow equation [25] that approximates the nonlinear AC power flow equation [12].

The maximum capacity C_l of a line l is defined as the maximum power flow that can be afforded by the line. As in [17], we assume that the maximum capacity of a transmission line is proportional to its initial load $L_l(0)$ as follows:

$$C_l = \alpha_l L_l(0) \tag{1}$$

where α_l is called the tolerance parameter of the line l.

In a power grid, transmission lines are protected by relays and circuit breakers. A relay of a transmission line measures the load of that line and compares the load with the maximum capacity C_l computed by equation (1). When the maximum capacity is violated, and this violation lasts long enough, the relay notifies a circuit breaker to trip the transmission line in order to prevent the line from permanent damage due to overloading. We assume a deterministic model for the line tripping mechanism. A circuit breaker trips at the moment the load of a transmission line exceeds its maximum capacity.

The failure of a transmission line 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 transmission lines in the network. The protection mechanism trips these newly overloaded transmission lines and the power flow is again redistributed potentially resulting in new overloads. This cascading failure continues until no more transmission lines are overloaded.

III. Effective Graph Resistance in Power Grids

This section explains the complex network preliminaries, presents the effective graph resistance, and elaborates on how it is computed in electric power grids.

A. Complex Network Preliminaries

The topology of complex networks can be represented by a graph $G(N, L)$ consisting of N nodes connected by L links. Graphs with N nodes are completely described by an $N \times N$ adjacency matrix A, in which the element $a_{ij} = 1$ if there is a link between nodes i and j, otherwise $a_{ij} = 0$. In case of a weighted graph, the network is represented by the weighted adjacency matrix W where the element w_{ij} is a real number that characterizes a certain property of the link $i \sim j$. The weight can be distances in transportation networks, the delay in the Internet, the strength of the interaction in the brain networks, and so on.

The weighted Laplacian matrix $Q = \Delta - W$ of G is an $N \times N$ matrix, where $\Delta = \text{diag}(d_i)$ is the $N \times N$ diagonal degree matrix with the element $d_i = \sum_{j=1}^{N} w_{ij}$. The eigenvalues of Q are non-negative and at least one is zero [26]. Thus, the smallest eigenvalue of Q is zero. The eigenvalues of Q are ordered as $0 = \mu_N \leq \mu_{N-1} \leq \ldots \leq \mu_1$.

Graph metrics measure the structural and spectral properties of networks. The degree d_i of a node i specifies the number of connected neighbors to that node. The largest eigenvalue λ_1 (also called the spectral radius) of the adjacency matrix highly influences the dynamic processes on networks such as virus spreading and synchronization processes [23]. The eigenvector corresponding to the spectral radius is called principle eigenvector x_1 that characterizes the influence of link/node removal on spectral radius [19], [30]. The second smallest eigenvalue μ_{N-1} of the Laplacian matrix Q is coined by Fiedler [10] as the algebraic connectivity α_G. The corresponding eigenvector is called the Fiedler vector. The entries of the Fiedler vector provide a powerful heuristic for community detection [21] and graph partitioning [20]. The strategies illustrated in Section IV are based on these structural and spectral graph metrics.

B. Effective graph resistance in power grids

Effective resistance R_{ij} is the electrical resistance between nodes i and j computed by series and parallel manipulations when a graph is seen as an electrical circuit where each link in the graph has a unit resistance. According to the Ohm's law, the effective resistance R_{ij} is the potential difference between nodes i and j when a unit current is injected at node i and withdrawn at node j. The effective graph resistance R_G is the sum of the effective resistance R_{ij} over all pairs of nodes in the network $R_G = \sum_{i=1}^{N} \sum_{j=i+1}^{N} R_{ij}$. Effective graph resistance takes into account all the possible paths between two nodes and the total weight on each path.

Computation of the effective graph resistance for a power grid necessitates the topology of the grid (i.e. interconnection of nodes) and reactance (or susceptance) values of the transmission lines in the grid. The weighted Laplacian matrix Q of a power grid reflects the interconnection of nodes by transmission lines. The weight w_{ij} corresponds to the susceptance (the inverse of reactance) value of the line $l = i \sim j$. The effective resistance R_{ij} between a pair of nodes is computed as [26]:

$$R_{ij} = \left(\hat{Q}^{-1}\right)_{ii} + \left(\hat{Q}^{-1}\right)_{jj} - 2\left(\hat{Q}^{-1}\right)_{ij} \tag{2}$$

where $\hat{Q}^{-1}$ is the Moore-Penrose pseudo-inverse of the Q.

In terms of eigenvalues of the weighted Laplacian matrix Q, the effective graph resistance can be written as [26]

$$R_G = N \sum_{i=1}^{N-1} \frac{1}{\mu_i} \tag{3}$$

where μ_i is the ith eigenvalue of Q and N is the number of nodes in a power grid. In this paper, we use equation (3), which is computationally efficient, to compute the effective graph resistance.

IV. Strategies for Adding a Transmission Line

As a response to blackouts, additional transmission lines are placed aiming to increase the robustness of power grids. Determining the right pair of nodes to connect in order to maximize the robustness is the challenge. An exhaustive search, identifying the best pair of nodes to connect by checking all $L_c = \binom{N}{2} - L$ possibilities, is computationally expensive especially when the number of nodes increases. Therefore, strategies that determine the transmission line to be added based on topological and spectral properties of a network, provide a trade-off between a scalable computation and a high increase of the grid robustness.

Topological and spectral metrics, such as degree, algebraic connectivity and spectral radius, characterize the connectivity of a network and highly influence the dynamic processes executed on a network [10], [27]. The effective graph resistance is shown to be able to anticipate the robustness of power grids with respect to cascading failures [17]. This section investigates four strategies, studied in [33], for selecting a link whose addition potentially minimizes the effective graph resistance and accordingly maximizes the robustness. A strategy defines a link $l = i \sim j$, where l is not existed before. The selection criteria of nodes i and j for each strategy are illustrated in the rest of this section.

A. Degree product

The nodes i and j have the minimum product of degrees $\min(d_i d_j)$, where $d_i = \sum_{j=1}^{N} w_{ij}$. If there are multiple node pairs with the same minimum product of degrees, one of these pairs is randomly chosen.

The complexity for the strategy is $O(N^2 - N + 2L_c)$ computed as follows: (i) $O(N(N-1))$ is for counting the degrees of all the nodes. (ii) $O(L_c)$ is for computing $d_i d_j$ for L_c unconnected node pairs. (iii) $O(L_c)$ is for finding the minimum product $\min(d_i d_j)$.

B. Principle eigenvector

The nodes i and j correspond to the i^{th} and j^{th} components of the principal eigenvector x_1 that have the maximum product $\max((x_1)_i(x_1)_j)$ of the principle eigenvector components. The principal eigenvector x_1 belongs to the largest eigenvalue of the weighted adjacency matrix W.

The complexity of the strategy is $O(N^3 + 2L_c)$ computed as follows: (i) $O(N^3)$ is for computing the principle eigenvector x_1 assuming the adoption of the QR algorithm [11] for computation. (ii) $O(L_c)$ is for computing $(x_1)_i(x_1)_j$ for L_c unconnected node pairs. (iii) $O(L_c)$ is for finding the maximum product $\max((x_1)_i(x_1)_j)$.

C. Fiedler vector

The nodes i and j correspond to the i^{th} and j^{th} components of the Fiedler vector y that satisfy $\Delta y = \max(|y_i - y_j|)$, where $|y_i - y_j|$ is the absolute difference between the i^{th} and j^{th} components of the Fiedler vector [31].

For this strategy, the complexity is $O(N^3 + 2L_c)$ computed as follows: (i) $O(N^3)$ is for computing the Fiedler vector y_i assuming the adoption of the QR algorithm [11] for computation. (ii) $O(L_c)$ is for computing $|y_i - y_j|$ for L_c unconnected node pairs. (iii) $O(L_c)$ is for finding the maximum of the difference $|y_i - y_j|$.

TABLE I: A summary of the strategies and the order of their computational complexity.

	Node i Node j	Complexity Order
DegProd	$\arg\min_{i,j}(d_i d_j)$	$O(N^2)$
PrinEigen	$\arg\max_{i,j}((x_1)_i(x_1)_j)$	$O(N^3)$
FiedlerVector	$\arg\max_{i,j}(\lvert y_i - y_j \rvert)$	$O(N^3)$
EffecResis	$\arg\max_{i,j}(R_{ij})$	$O(N^3)$
Exhaustive Search	$\arg\min_{i,j}(R_G)$	$O(N^5)$

D. Effective resistance

The nodes i and j have the highest effective resistance $\max(R_{ij})$. The pairwise effective resistance R_{ij} is computed by equation (2). Similarly, if multiple node pairs have the maximum effective resistance, one of these pairs is randomly chosen.

The complexity for the strategy is $O(N^3 + 4L_c)$ computed as follows: (i) $O(N^3)$ is for computing $\widehat{Q}^{-1}$. (ii) $O(3L_c)$ is for computing R_{ij} for L_c unconnected node pairs. (iii) $O(L_c)$ is for finding the maximum R_{ij}.

Table I summarizes all the strategies that identify a link $l = i \sim j$ and the order of their corresponding computational complexity. Table I also presents the complexity order of the exhaustive search in order to compare with the complexity of the four strategies. The complexity order $O(N^5)$ of the exhaustive search is computed by $O(N^2)$ for checking all the possibilities multiplied by $O(N^3)$ for computing the effective graph resistance after a link addition.

V. Experimental Methodology

The experimental method presented in this section evaluates the robustness of the improved power system against cascading failures triggered by deliberate attacks. This approach can be used to assess the performance of the effective graph resistance as a metric for link addition on improving the robustness of power grids. This section elaborates on attack strategies and the quantification of the grid robustness after cascading failures.

A. Attack Strategies

This paper designs attack strategies based on electrical node significance centrality and link betweenness centrality. The electrical node significance [16] is a flow-based measure for node centrality, specifically designed for power grids. The electrical node significance δ_i of a node i is defined as the total power P_i distributed by node i normalized by the total amount of power that is distributed in the entire grid:

$$\delta_i = \frac{P_i}{\sum_{j=1}^{N} P_j} \tag{4}$$

An attack based on δ_i refers to target the link incident to the node i that has the highest electrical node significance. Since

node i has the number d_i of incident links, the link with the highest load is chosen.

The link betweenness centrality is a topological graph metric quantifying the centrality of a link in complex networks [28]. The betweenness centrality of a link is defined as the total number of the shortest paths that traverse the link l.

$$B_l = \sum_{i=1}^{N} \sum_{j=1}^{N} 1_{l \in \mathcal{P}(i,j)} \tag{5}$$

where $1_{\{x\}}$ is the indicator function: $1_{\{x\}} = 1$ if the condition $\{x\}$ is true, else $1_{\{x\}} = 0$, and $\mathcal{P}(i,j)$ is the shortest path between nodes i and j. An attack based on betweenness centrality targets the link with the highest betweenness centrality.

Placing an additional line according to different strategies (presented in Section IV) results in different improved power systems. In order to compare cascading damages of these improved systems, we always attack the same link identified by the node significance centrality or link betweenness centrality of the original power grid.

B. Robustness Evaluation

The robustness of power grids is evaluated by the criticality of the additional line and the damages after cascading failures triggered by targeted attacks. To assess the criticality of the newly added transmission line based on the effective graph resistance, we deploy an analogous approach as in [18]: the criticality of an added line l in a graph G is determined by the relative decrease of the effective graph resistance ΔR_G^l that is caused by the addition of a link l:

$$\Delta R_G^l = \frac{R_G - R_{G+l}}{R_G} \tag{6}$$

where R_{G+l} is the effective graph resistance of the grid after adding a link l into G. Evaluation of equation (6) results in the theoretical robustness level of a power grid.

Initially, a transmission line identified by the four strategies and exhaustive search is added into the power grid. Then, the newly obtained grids are attacked and the cascading damages are quantified.

The damage caused by the cascade is quantified in terms of normalized served power demand DS: served power demand divided by the total power demand in the network. Computing the normalized served demand for an interval of tolerance parameters $[\alpha_{min}, \alpha_{max}]$ results in a robustness curve of a grid. The normalized area below the robustness curve is computed by a Riemann sum [28]:

$$r = \frac{\sum_{i=1}^{m+1} DS(\alpha_i)\Delta_\alpha}{\alpha_{max} - \alpha_{min}} \tag{7}$$

where the closed interval $[\alpha_{min}, \alpha_{max}]$ is equally partitioned by m points and the length of the resulting interval is $\Delta_\alpha = \frac{\alpha_{max} - \alpha_{min}}{m+1}$. $DS(\alpha_i)$ is the normalized served demand when the tolerance parameter of the network is $\alpha_i \in [\alpha_{min} + (i-1)\Delta_\alpha, \alpha_{min} + i\Delta_\alpha]$. Since the maximum value of DS is 1, $(\alpha_{max} - \alpha_{min})$ refers to the maximum possible area below the robustness curve ensuring that the value of r is between 0 and 1. Evaluation of equation (7) for the robustness curve results in the experimental robustness level of a power grid with respect to cascading failures.

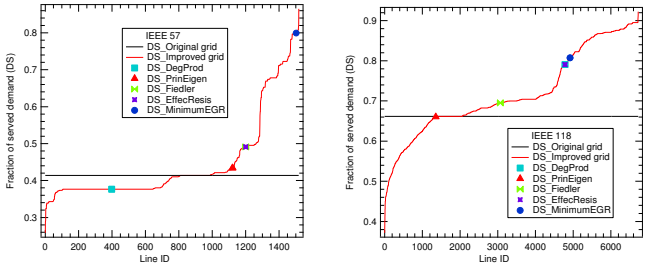
VI. Numerical Analysis

This section investigates the effectiveness of the effective graph resistance as a metric for line addition, the impact of structures on the Braess's paradox, and the performance of the four strategies. First, the power grid is expanded by adding single links according to the minimization of the effective graph resistance, and the criteria of the four strategies. Then, the robustness of the improved power grid is assessed quantitatively under targeted attacks.

A. Assessing effectiveness of the effective graph resistance

Exhaustively adding all the possible links provides us all the possibly improved grids. Quantifying the cascading damages of all the improved grids under targeted attacks provides the benchmark for the evaluation of the effective graph resistance. The reactance value on each added line is assumed to be the average of all the existing transmission lines. The simulations are performed by MATCASC [15], a MATLAB based cascading failures analysis tool implementing the model in Section II.

Figure 1 shows the performance of the effective graph resistance on identifying a critical link under a fixed tolerance parameter $\alpha = 2$ in IEEE 57 and 118 power systems. The original and improved power systems are attacked based on the node significance centrality computed by equation (4). In Figure 1, the horizontal line (i.e. the black line) is the served demand DS for the original power grid after cascading failures. The curve is the served demand for each improved power grid after adding each possible line. The curve above the horizontal line shows an increase of the robustness after a link addition, while the curve below the horizontal line presents a decrease of the robustness by adding a link. This counter-intuitive phenomenon is linked to Braess's paradox known for traffic networks, stating that adding extra capacity or links to a network occasionally reduces the overall performance of a network [3].



(a) IEEE 57 (b) IEEE 118

Fig. 1: The performance of the effective graph resistance in IEEE 57, IEEE 118 power system with the tolerance parameter $\alpha = 2$.

Braess's paradox generally occurs in most complex networks, such as oscillator networks [35], mechanical and electrical networks [6], hydraulic networks and other networks that obey Kirchhoff's laws [22]. In particular, Braess's paradox also exists in power systems [1], [35]. Our results are in line with the occurrence of Braess's paradox in power systems.

The performance of the effective graph resistance as a metric for link addition and the performance of strategies are labeled in the Figure 1 with markers. The added line that minimizes the effective graph resistance increases the robustness from 0.41 to 0.80. Compared to the possibly maximal increase 0.86 by a single link addition, the effective graph resistance achieves 93% accuracy in the IEEE 57 power system. Similarly, the effective graph resistance achieves 87% accuracy in the IEEE 118 power system. The simulation results in Figure 1 validate the effectiveness of the effective graph resistance to identify a critical link. The addition of the critical link improves the robustness of power grids regardless of the fact that the robustness can be decreased according to Braess's paradox. Moreover, the increase of the grid robustness by adding the critical link according to the effective graph resistance is over 87% of the upper bound of increase for a single link addition.

B. Assessing the impact of the grid topology on Braess's paradox

Braess's paradox in this paper refers to the decrease of grid robustness by placing additional links. The relationship between the grid topology and the Braess's paradox in power grids is investigated.

The Wheatstone bridge graph (shown in Figure 2) refers to a graph consisting of four nodes, with four links creating a quadrilateral. A fifth link connects two opposite nodes in the quadrilateral, splitting the graph into two triangles [4]. We consider the subgraph with four nodes and four links as the Wheatstone subgraph and the fifth link as the Wheatstone link. Braess's paradox indicates that the construction of the Wheatstone bridge graph by adding the Wheatstone link occasionally decreases the robustness of power grids. Let $P_{\text{Wheatstone}}$ represent the percentage of the Wheatstone links and P_{Paradox} be the percentage of the links, whose addition results in Braess's paradox. In order to investigate the impact of the Wheatstone bridge graph on Braess's paradox, the correlation between the percentages $P_{\text{Wheatstone}}$ and P_{Paradox} is quantified. The number of Wheatstone links is computed by the number of Wheatstone bridge subgraphs detected by FANMOD [34], a tool for fast network motif detection.

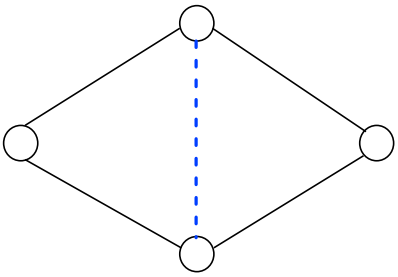
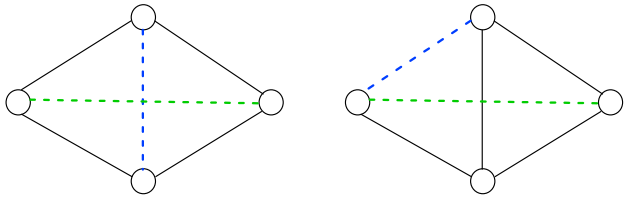


Fig. 2: Wheatstone bridge graph

Figure 3 shows two types, Type I and Type II, of Wheatstone subgraphs from which a Wheatstone bridge graph is built by adding the Wheatstone link (the dashed line). For each subgraph, the number of the Wheatstone links is two times the total number of subgraphs of Type I and Type II. The percentage $P_{\text{Wheatstone}}$ of Wheatstone links in all the possible added links L_c is computed by $P_{\text{Wheatstone}} = \frac{2(N_{\text{TypeI}}+N_{\text{TypeII}})}{L_c}$, where N_{Typek} is the number of subgraphs of Type k. Table II shows the percentage $P_{\text{Wheatstone}}$ of Wheatstone links and the percentage P_{Paradox} in Figure 1. The correlation between $P_{\text{Wheatstone}}$ and P_{Paradox} is 0.96 suggesting the criticality of the Wheatstone bridge graph (see Figure 2) to the occurrence of Braess's paradox.



(a) Type I (b) Type II

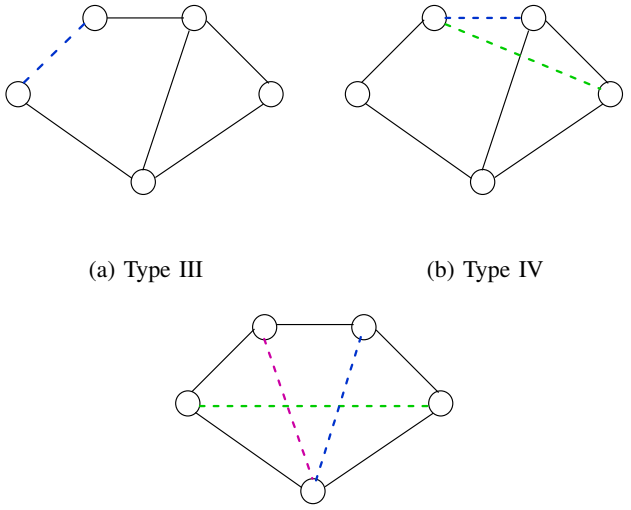
Fig. 3: Two types of subgraphs to build a Wheatstone bridge graph by adding the Wheatstone link. The dashed lines are the possible Wheatstone links.

Besides the Wheatstone bridge graph that occasionally introduce Braess's paradox as shown in several literatures [1], [6], [22], we further investigate other sub-structures that may lead to the Braess's paradox. Figure 4 shows other three types, Type III to Type V, of subgraphs resulting in Braess's paradox when a single link is added. The dashed lines in Figure 4 are the possible links that cause the Braess's paradox. Table III shows the percentages $P_{\text{Wheatstone}}$ and P_{Paradox} after considering the number of links added into Type III, IV and V. The percentage $P_{\text{Wheatstone}}$ increases from 6.73% to 25.00% in IEEE 57 power system. An increase of the $P_{\text{Wheatstone}}$ from 4.53% to 15.44% is also observed in IEEE 118 and from 1.34% to 4.11% in IEEE 247 power system. Accordingly, the correlation between $P_{\text{Wheatstone}}$ and P_{Paradox} increases to 0.971. The results indicate that the subgraphs from Type I to Type V provide an effective indication for the occurrence of the Braess's paradox in power grids. The impact of other characteristics of power grids, such as the reactance values and the loading profiles, on the occurrence of Braess's paradox is still an open question.

	IEEE57	IEEE118	IEEE247
L_c	1516	6717	30026
N_{TypeI}	0	20	30
N_{TypeII}	51	132	171
$P_{\text{Wheatstone}}(\%)$	6.73	4.53	1.34
P_{Paradox} $(\%)$	53.16	20.67	4.57

TABLE II: The percentage $P_{\text{Wheatstone}}$ and P_{Paradox} in IEEE power systems

Based on the Wheatstone bridge graph, we analyze the impact of the reactance value of the Wheatstone link (see for example the dashed line in Figure 2) on the Braess's paradox. Figure 5 shows the relation between the reactance value and the percentage P_{Paradox} of the links that decrease the robustness.



(a) Type III (b) Type IV

(c) Type V

Fig. 4: Three types of subgraphs resulting in Braess's paradox by adding an extra link.

	IEEE57	IEEE118	IEEE247
L_c	1516	6717	30026
N_{TypeIII}	95	256	299
N_{TypeIV}	91	216	255
N_{TypeV}	0	15	8
$P_{\text{Wheatstone}}(\%)$	25.00	15.44	4.11
P_{Paradox} (%)	53.16	20.67	4.57

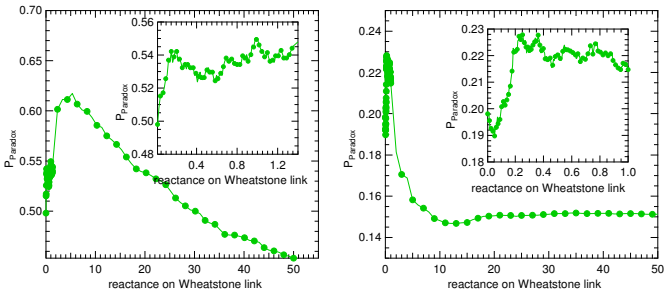
TABLE III: The percentage $P_{\text{Wheatstone}}$ and P_{Paradox} in IEEE power systems

The inserted figure shows that as the reactance increases from the minimum to the maximum reactance of all the existing links, the percentage P_{Paradox} first increases and then starts to fluctuate. The difference between P_{Paradox} in the inserted figure is 0.06 in IEEE 57 and 0.04 in IEEE 118 power systems. Consequently, the average reactance value of all the existing links is considered as the reactance value of the Wheatstone link in this paper. By continuously increasing the reactance value on the Wheatstone link, the percentage P_{Paradox} decreases due to the descent of the power flow in the Wheatstone link. At a certain point of the reactance, the percentage P_{Paradox} converges to a constant value in IEEE 118 system.

C. Assessing the effectiveness of strategies

To assess the effectiveness of the four strategies in Section IV, the IEEE 118 power system, consisting of 118 buses and 186 lines, is considered as a use case. For each line identified by each strategy, equation (6) is evaluated and its impact on the effective graph resistance is determined. Table IV shows the lines to be added identified by strategies and their impact on the decrease of R_G.

In Table IV, the strategy based on the Fiedler vector selects the line connecting bus 111 and bus 117 and its addition causes 11.3% decrease of the effective graph resistance. Strategies based on the degree product and the effective resistance have



(a) IEEE 57 (b) IEEE 118

Fig. 5: The percentage P_{Paradox} under different reactance values in IEEE 57, IEEE 118 power system.

Strategy	line ID	$\Delta R_G^l(\%)$
DegProd	l_{87-117}	9.0
PrinEigen	l_{87-111}	4.2
Fiedler	$l_{111-117}$	11.3
EffectiveResis	l_{87-117}	9.0

TABLE IV: Added lines identified by the strategies and their impact on the decrease of R_G.

an equal performance that decrease the effective graph resistance by 9%. The strategy based on the principle eigenvector decreases the effective graph resistance by 4.2%. Compared to other strategies, the strategy based on the Fiedler vector performs the best.

To validate the results from Table IV, the original and improved IEEE 118 power systems are attacked based on the electrical node significance and the link betweenness, and damages after cascading failures are quantified. Figures 6 and 7 show the robustness curves for improved power grids under an interval of tolerance parameters $[\alpha_{min}, \alpha_{max}]$ with $\Delta_\alpha = 0.05$, and highlight the improvement of the grid robustness. In order to quantify the performance of the four strategies in improving the grid robustness, the robustness value r in equation (7) for each robustness curve is shown in Table V.

Figure 6 and Table V show the performance of the strategies in the IEEE 118 power grid under the attack based on the node significance. The strategy based on the Fiedler vector has a robustness value $r = 0.777$ which is an increase by 1.8% compared to the original grid robustness (i.e. 0.763). The strategy based on the degree product and on the effective resistance have an equal performance. These two strategies have the same robustness value $r = 0.769$ and increase the robustness by 0.8%. The strategy based on the principle eigenvector has the lowest performance and its robustness value is $r = 0.757$ that decreases the robustness by 0.8%.

Figure 7 and Table V present the performance of the strategies under the betweenness based attack. The strategy based on the Fiedler vector has the highest robustness value $r = 0.991$, which is an increase by 8.2% compared to the original grid robustness (i.e. 0.916). The strategy based on the degree product and on the effective resistance have an equal performance with the same robustness value $r = 0.949$. The robustness is increased by 3.6% compared to the original

grid robustness. In contrast, the strategy based on the principle eigenvector with $r = 0.915$ slightly decreases the robustness by 0.1%. The performance order of the strategies shown in Figures 6 and 7 and Table V is in agreement with the theoretical results in Table IV.

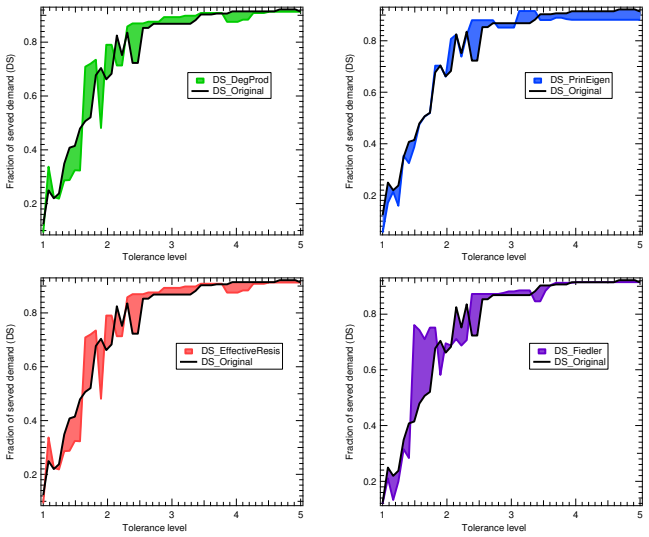


Fig. 6: The performance of the four strategies in IEEE 118 power system under different tolerance parameters. The attack strategy is based on the node significance centrality.

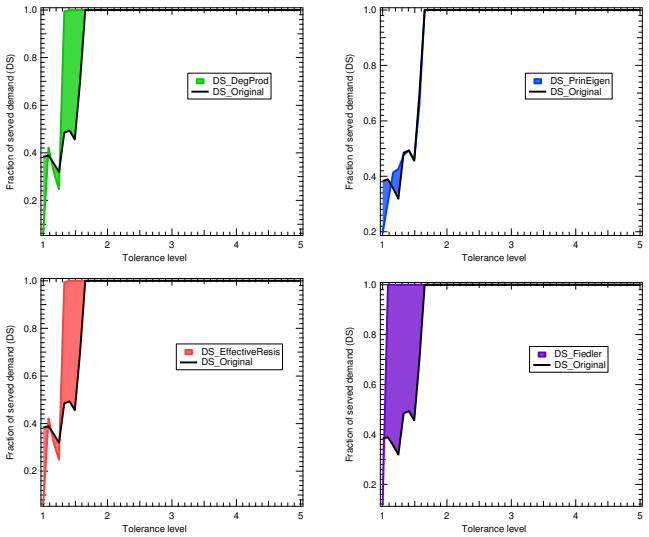


Fig. 7: The performance of the four strategies in IEEE 118 power system under different tolerance parameters. The attack strategy is based on betweenness centrality.

When the computational cost for finding the optimal links to add is prohibitive, the strategy based on the Fiedler vector with the highest performance is preferable compared to other strategies. Assuming that computing the Fiedler vector for large grids is not an option, the strategy based on the degree product can be an alternative. The degree based strategy is more likely to be chosen than the strategy based on the effective resistance due to the fact that these two strategies have comparable performance, while the strategy based on the degree product has lower computational complexity.

Strategy	line ID	r (Node Siginificance attack)	r (Betweenness attack)
DegProd	l_{87-117}	0.769	0.949
PrinEigen	l_{87-111}	0.757	0.915
Fiedler	$l_{111-117}$	0.777	0.991
EffectiveResis	l_{87-117}	0.769	0.949

TABLE V: Critical lines identified by the four strategies and the robustness value r in IEEE 118 power system.

VII. Conclusion and Discussion

This paper investigates the effective graph resistance as a metric for network expansions to improve the grid robustness against cascading failures. The effective graph resistance takes the multiple paths and their ability to accommodate power flows into account to quantify the robustness of power grids. The experimental verification on IEEE power systems demonstrates the effectiveness of the effective graph resistance to identify single links that improve the grid robustness against cascading failures. Additionally, when computational cost for finding optimal links is prohibitive, strategies that optimize the effective graph resistance can still identify an added link resulting in a higher level of robustness. Specifically, the strategy based on the Fiedler vector performs the best compared to other strategies and increases the robustness by 8.2% in IEEE 118 power system under the betweenness based attack, while reduces the computational complexity from $O(N^5)$ to $O(N^3)$.

The occurrence of Braess's paradox in power grids suggests that the robustness can be occasionally decreased by placing additional links. In particular, a badly designed power grid may cause enormous costs for new lines that actually reduce the grid robustness. The experimental results in this paper provide insights in designing robust power grids while avoiding the Braess's paradox in power grids.

Acknowledgment

This research was supported by the China Scholarship Council (CSC) and by the NWO project RobuSmart, grant number 647.000.001.

References

[1] S. Blumsack, L. B. Lave, and M. Ilić. A quantitative analysis of the relationship between congestion and reliability in electric power networks. *The Energy Journal*, pages 73–100, 2007.

[2] D. Braess. Über ein Paradoxon aus der Verkehrsplanung. *Unternehmensforschung*, 12(1):258–268, 1968.

[3] D. Braess, A. Nagurney, and T. Wakolbinger. On a paradox of traffic planning. *Transportation science*, 39(4):446–450, 2005.

[4] B. Calvert and G. Keady. Braess's paradox and power-law nonlinearities in networks. *The Journal of the Australian Mathematical Society, Series B. Applied Mathematics*, 35(01):1–22, 1993.

[5] L. Chang and Z. Wu. Performance and reliability of electrical power grids under cascading failures. *International Journal of Electrical Power & Energy Systems*, 33(8):1410–1419, 2011.

[6] J. E. Cohen and P. Horowitz. Paradoxical behaviour of mechanical and electrical networks. *Nature*, 352:699–701, 1991.

[7] I. Dobson. Cascading network failure in power grid blackouts. In *Encyclopedia of Systems and Control*, pages 1–5. Springer London, 2014.

[8] G. Dong, J. Gao, R. Du, L. Tian, H. E. Stanley, and S. Havlin. Robustness of network of networks under targeted attack. *Physical Review E*, 87(5):052804, 2013.

[9] W. Ellens, F. M. Spieksma, P. Van Mieghem, A. Jamakovic, and R. E. Kooij. Effective graph resistance. *Lin. Algebra Appl.*, 435(10):2491–2506, 2011.

[10] M. Fiedler. Algebraic connectivity of graphs. *Czech. Math. J.*, 23(2):298–305, 1973.

[11] J. G. F. Francis. The QR transformation - part 2. *Comput. J.*, 4(4):332–345, 1962.

[12] J. J. Grainger and W. D. Stevenson. Power system analysis. *McGraw-Hill series in electrical and computer engineering*, 1994.

[13] P. Hines, K. Balasubramaniam, and E. C. Sanchez. Cascading failures in power grids. *Potentials, IEEE*, 28(5):24–30, 2009.

[14] B. Karrer, M. E. J. Newman, and L. Zdeborová. Percolation on sparse networks. *Phys. Rev. Lett.*, 113:208702, 2014.

[15] Y. Koç, T. Verma, N. A. M. Araujo, and M. Warnier. MATCASC: A tool to analyse cascading line outages in power grids. In *Intelligent Energy Systems (IWIES), IEEE International Workshop on*, pages 143–148. IEEE, 2013.

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

[17] Y. Koç, M. Warnier, P. Van Mieghem, R. E. Kooij, and F. M. T. Brazier. The impact of the topology on cascading failures in a power grid model. *Physica A: Statistical Mechanics and its Applications*, 402:169–179, 2014.

[18] V. Latora and M. Marchiori. Vulnerability and protection of infrastructure networks. *Physical Review E*, 71(1):015103, 2005.

[19] C. Li, H. Wang, and P. Van Mieghem. Bounds for the spectral radius of a graph when nodes are removed. *Linear Algebra and its Applications*, 437(1):319–323, 2012.

[20] J. Martín-Hernández, H. Wang, P. Van Mieghem, and G. D'Agostino. Algebraic connectivity of interdependent networks. *Physica A: Statistical Mechanics and its Applications*, 404:92–105, 2014.

[21] M. E. J. Newman. Community detection and graph partitioning. *EPL(Europhysics Letters)*, 103(2):28003, 2013.

[22] C. M. Penchina and L. J. Penchina. The Braess Paradox in mechanical, traffic, and other networks. *American Journal of Physics*, 71(5):479–482, 2003.

[23] J. G. Restrepo, E. Ott, and B. R. Hunt. Approximating the largest eigenvalue of network adjacency matrices. *Phys. Rev. E*, 76:056119, 2007.

[24] S. Trajanovski, J. Martín-Hernández, W. Winterbach, and P. Van Mieghem. Robustness envelopes of networks. *Journal of Complex Networks*, 1(1):44–62, 2013.

[25] D. Van Hertem, J. Verboomen, K. Purchala, R. Belmans, and W. L. Kling. Usefulness of DC power flow for active power flow analysis with flow controlling devices. In *AC and DC Power Transmission, The 8th IEE International Conference on*, pages 58–62, 2006.

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

[27] P. Van Mieghem. Epidemic phase transition of the SIS type in networks. *EPL (Europhysics Letters)*, 97(4):48004, 2012.

[28] P. Van Mieghem. *Performance analysis of complex networks and systems*. Cambridge University Press, 2014.

[29] P. Van Mieghem, C. Doerr, H. Wang, J. Martín-Hernández, D. Hutchison, M. Karaliopoulos, and R. E. Kooij. A framework for computing topological network robustness. *Delft University of Technology, Report20101218*, 2010.

[30] P. Van Mieghem, D. Stevanović, F. Kuipers, C. Li, R. van de Bovenkamp, D. Liu, and H. Wang. Decreasing the spectral radius of a graph by link removals. *Physical Review E*, 84(1):016101, 2011.

[31] H. Wang and P. Van Mieghem. Algebraic connectivity optimization via link addition. In *Proceedings of the 3rd International Conference on Bio-Inspired Models of Network, Information and Computing Sytems*, page 22. ICST, 2008.

[32] 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.

[33] X. Wang, E. Pournaras, R. E. Kooij, and P. Van Mieghem. Improving robustness of complex networks via the effective graph resistance. *The European Physical Journal B*, 87(9):1–12, 2014.

[34] S. Wernicke and F. Rasche. FANMOD: a tool for fast network motif detection. *Bioinformatics*, 22(9):1152–1153, 2006.

[35] D. Witthaut and M. Timme. Braess's Paradox in oscillator networks, desynchronization and power outage. *New Journal of Physics*, 14(8):083036, 2012.

[36] G. Zhang, Z. Li, B. Zhang, and W. A. Halang. Understanding the cascading failures in Indian power grids with complex networks theory. *Physica A: Statistical Mechanics and its Applications*, 392(15):3273–3280, 2013.