RESEARCH ARTICLE

Topological vulnerability of power grids to disasters: Bounds, adversarial attacks and reinforcement

Deepjyoti Deka [1] *, **Sriram Vishwanath** [2], **Ross Baldick** [2]

1 Center for Non-Linear Studies, Los Alamos National Laboratory, Los Alamos, United States of America,
2 Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, United States of America

* deepjyoti@lanl.gov

Abstract

Natural disasters like hurricanes, floods or earthquakes can damage power grid devices and create cascading blackouts and islands. The nature of failure propagation and extent of damage, among other factors, is dependent on the structural features of the grid, that are distinct from that of random networks. This paper analyzes the structural vulnerability of real power grids to impending disasters and presents intuitive graphical metrics to quantify the extent of topological damage. We develop two improved graph eigen-value based bounds on the grid vulnerability. Further we study adversarial attacks aimed at weakening the grid's structural robustness and present three combinatorial algorithms to determine the optimal topological attack. Simulations on power grid networks and comparison with existing work show the improvements of the proposed measures and attack schemes.

Introduction

The structure of the power grid is an important feature that affects the delivery of electricity [1]. From an economic perspective, the capacity of transmission lines and the graphical properties (whether tree-like or loopy) affect the locational marginal electricity prices as well as the convergence of Optimal power flow algorithms [2]. At a faster time-scale, structure of the grid affects controllability of ambient fluctuations [3]. From a reliability perspective, the grid structure is one of the factors that influence the extent of damage following a natural or man-made disaster. In particular, it affects the propagation of failures and the formation of islands. Over the years, natural disasters like earthquakes, floods, hurricanes have caused extensive power outages due to damage of grid equipment and loss of network connectivity [4, 5]. Such disasters also directly and indirectly affect other co-located and interdependent networks like the transportation and communication infrastructure. Thus there is a greater need to quantify the effect of the grid structure on failure propagation in the grid following a natural disaster and to incorporate the insights gained into transmission planning techniques to improve grid resilience.

There is existing work that studies the impact of different grid features including structure on grid reliability, under different regimes of operation. Reference [6] describes a DC model

for the propagation of equipment (nodes and links) failures in cascading outages in the power grid. Here, the propagation process begins with an initial failure of a network node or link which leads to a redistributing of the power flows for optimal dispatch. Subsequently in [7], the authors incorporate recovery mechanism for the tripped transmission lines into the failure model and show that the size of blackout has a power-law distribution. Reference [8] analyzes the problem of finding the optimal k lines in the grid that can be used for interdiction in the grid to create failures. Power flow based analysis has been done to analyze geographically correlated failures in [9]. Similarly, an interdiction based analysis on grid resilience considering short term impacts is discussed in [10]. These models utilize laws governing power flows and generator dispatch to solve optimization problems such as Optimal Power Flow (OPF). Such dispatch decisions are effective in the range of $5 - 15$ minutes in realistic power grid operations. At time-scales below the minute level, voltage and frequency fluctuations represented by swing equations affect the stability of the grid. In that regime, control-theoretic measures [3, 11, 12] have been used to analyze grid resilience and suggest improvements to prevent damage. Indeed inclusion of accurate models for generator dynamics, load response and system operator's control efforts into the analysis improve the characterization of the physics of failure propagation and enable an accurate study. Such analysis, however, seldom leads to a closed form expression of a metric to quantify the resilience of the power grid to failures, one of the objectives of this paper. Moreover perspective gained from an detailed optimization based quantification of grid vulnerability may not be transferable from one network to another. Further it needs to be mentioned that power grid dynamics in the regime of an extreme event like cascading outage is highly non-linear and may not be accurately represented by dynamical equations approximated for small ambient fluctuations.

In a separate line of work, efforts have been made to study probabilistic failure propagation in power grids and related networks using techniques from percolation theory and random graph theory. In this approach, failures based on connectivity as against power flows are studied. Initial failures induced by external events are supposed to propagate probabilistically from source to neighboring nodes and edges in the grid graph. The final state will often include greater number of failures than the initial state and efforts are made to study the effect of the grid structure in influencing the spread. References [13, 14] study the effect of removing nodes and edges from power grid graphs based on their centrality and degree measures and their effect on network connectivity. The authors of [15, 16] analyze the propagation of structural failures in complex random networks based on similar neighborhood propagation rules. This approach has been extended to study interdependent networks failures as well [17–20] where nodes of two different networks may depend on one another for survivability. Similarly, references [21, 22] have analyzed node and edge percolation based techniques to understand failure propagation in random graphs generated by stochastic geometry. An interaction graph based model is presented in [23] where power flow based cascading information is used to study the inter-nodal dependencies on cascades. For mitigation of cascading failures, a capacity sharing protections scheme is proposed in [24]. A good review of works pertaining to grid resilience to natural disasters can be found in [25] and [26].

It is worth mentioning that parallel analytical graph-theoretic techniques are also used in studying social and biological networks for information dissemination, spread of viruses as well as synchronization of dynamic processes [27–29]. Existing work [1, 30–34] has demonstrated that the structure of finite-sized real power grids create deviations in observed parameters from those predicted in random graphs. For example, sharp breakdown thresholds that emerge in analysis of topological failures on random graphs [17, 19] are seldom observed in simulations of failures on real grids and IEEE test cases [35]. Further, structural reinforcements derived from random graph analysis [19] include fractional network changes (relative to size of the

entire grid) where effects of nodes of similar degree or connectivity are not distinguished. Such changes are not easily extended to determine finite (optimal k) network upgrades as they do not use the exact topology of the grid that is available with the grid controller.

In this work, we focus on power grid failures induced by large natural disasters like hurricanes and earthquakes that create disconnected islands in the grid. Our work pertains to graph-theoretic analysis of connectivity based failure models in power grids. This is similar to mentioned prior work on probabilistic failures in power grids but has a key difference. We use knowledge of the finite sized power grid graphs in our analysis and show that this leads to non-trivial results and improved understanding of network vulnerabilities. For grids affected by a disaster, we study the post-disaster network and present justification for using the size of the largest connected component as a valid metric for the functioning grid. We then extend probabilistic analysis of grid failures to known real grid graphs and popular IEEE test cases and determine computable graphical parameters (eg. eigenvalues of the grid adjacency matrix) that can be used to quantify grid robustness. It is noteworthy that these bounds are not realized from random graph constructions in prior work that do not consider the known finite structure of the grid. More importantly, we also present a novel construction of a modified graph based on the original grid graph that can be used to develop improved bounds on the extent of damage created by the disaster. The efficacy of the graphical parameter based bounds and soft thresholds are demonstrated by simulations of failures on publicly available grid data-sets.

The final contribution of the paper is in determining grid components that affect its vulnerability. We use the graphical metrics of grid resilience mentioned above to identify k critical transmission lines (graph edges) that maximally affect the grid robustness. In particular, we study removal of transmission lines by an adversary that aims to maximize the expected damage to network connectivity following a natural disaster. As this problem is NP-hard in general, we present three novel approximate algorithms to determine the optimal edges in the adversary's target set. The first two algorithms are based on perturbation based analysis of eigen-values of the grid adjacency matrix while the third algorithm is based on greedy trace minimization of a higher power of the adjacency matrix. Note that all three developed approaches rely on the global properties of the finite-sized grid structure. Crucially, such algorithms do not emerge from random graph based prior work where nodal degrees and centrality measures may be used to determine vulnerable locations. The performance of our algorithms for attack design in reducing grid resilience is demonstrated through simulations. Further comparison from other random graph based topological techniques in literature [14] are presented to elucidate the benefits derived from our approach. From the system operator or grid controller's perspective, these algorithms can be used to determine the critical lines that need to be protected to build resilience before any impending natural disaster.

To summarize, we present a framework to *analytically quantify the 'topological' resilience of real power grids to natural disasters*, and develop *novel algorithms to determine critical transmission lines that can prevent adversarial deterioration*. The rest of the paper is organized as follows. In the next section, we develop our intuitive graph theoretic quantification of network failure. Next, in Section 1 we analyze failures in actual grid graphs (non-random) and present our preliminary bound on the threshold of network breakdown. We proceed to present our novel modified graph construction to develop improved bounds on the threshold and size of the network damage in Section 1. We also discuss simulation results of developed bounds on IEEE test cases and real power grids. In Section 1, we study adversarial attacks on transmission lines aimed at weakening grid resilience to natural disasters and present three approximate methods to determine the critical transmission lines. Simulation results on our designed algorithms and comparison with existing work highlight the benefits of our approach in Section 1.

Limitations of our current approach and directions of improvements are discussed in Section. Finally, we discuss the insights gained and prospective future work in Section.

Failure model in power grids

We begin by describing the power grid and the topological failure model considered in this paper.

Network Model

We denote the grid by a graph $\mathcal{G} = (V, E)$, where sets V and E represent the nodes/buses and the undirected edges/lines respectively. Let the total number of buses in the system be N. We denote the adjacency matrix of the graph $\mathcal{G}$ by $A_{\mathcal{G}}$ that is assumed to be known and not generated by a probabilistic model. Each edge (ij) in E is represented by a value of 1 for $A_{\mathcal{G}}(i, j)$ and $A_{\mathcal{G}}(j, i)$ in the binary adjacency matrix. As an example, the IEEE 39 bus test system [35] is given in Fig 1. We assume nodes in the grid to have generation resources that may be provided
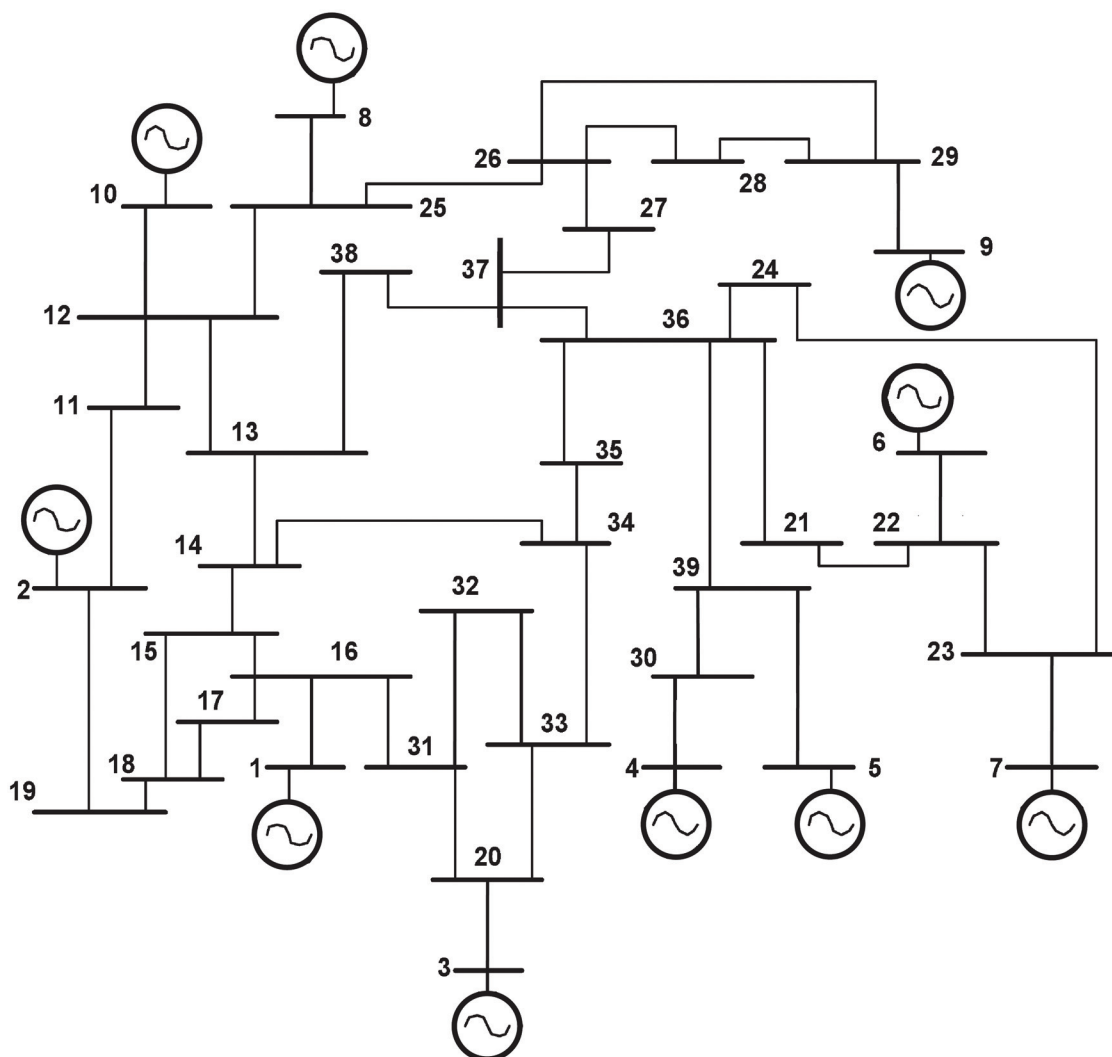

Fig 1. IEEE 39-bus test system [35].

by renewables (solar, wind etc.) or by conventional resources. Further, under normal operating conditions, the lines are assumed to have sufficient transmission capacity to transfer power from one part of the network to another. This is done as the objective of the paper is to study only topological (not electrical) features of the grid and their effects on grid resilience.)

Failure Model

As described in the Introduction, we consider a natural disaster that causes a probabilistic failure on all nodes in the system, with independent *initial probability of failure* denoted by p_0. The initial failure probability p_0 depends on the nature of the natural disaster (Eg. earthquake scale, wind speed of hurricane etc.) as well as geography (Eg. topography of the land). Such probabilities are computed by agencies like the National Hurricane Center and used to predict the scale of damage and help in planning for evacuation strategies [36]. For small grids with small or moderate geographical coverage, the assumption of identical initial probability of failure is valid. For a grid in a large area with diverge topographical conditions, the initial probability of failure will vary from node to node. In this work, we only consider cases where the initial probability of failure on all nodes is the same. The case with different initial failure probabilities for nodes is briefly discussed in comments and will be a subject of our following work. Under the failure model, the nodes can fail in two ways. One, nodes may fail under the initial failure probability—we term such failures as *'primary' failures*. Second, nodes fail as they get disconnected from the rest of the network due to failures at all neighboring nodes. Such failures are termed as *'secondary' failures*. Both these kind of failures are depicted in Fig 2. As described in subsequent discussion, we consider a node to be disconnected if it is separated from the largest connected component in the surviving network. Note that the chance of overall failure of a node depends on both the initial probability of failure p_0 and the probability of being disconnected which in turn depends on the network structure. Next we describe our measure of network damage following the natural disaster.

Measure of network damage

We assume that transmission line capacities are sufficient to satisfy all load in the system provided enough generating resources are online and connected. Thus in the post event network,
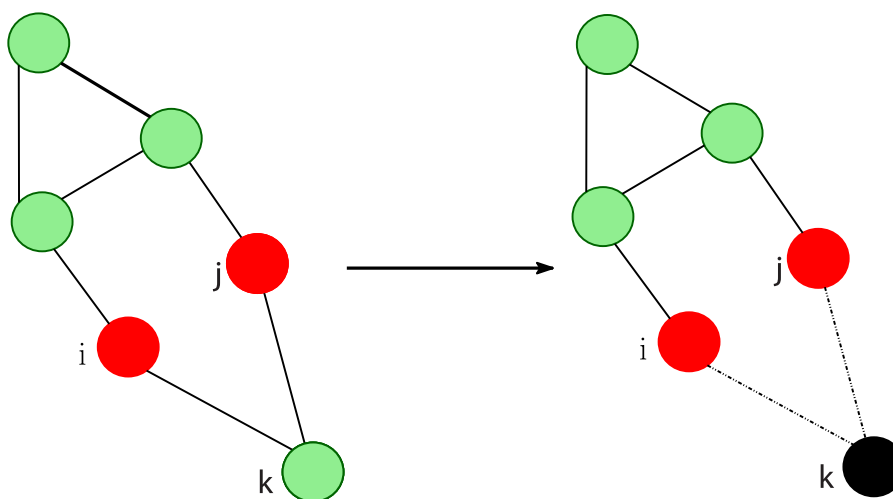

Fig 2. Primary failures, colored red, at nodes *i* and *k*. Secondary failure, colored black, at node *j* as it is disconnected from the network due to failures at its neighboring nodes. The surviving nodes are colored green.

loads are not served only if they are not connected to sufficient generation resources. In this work we restrict our discussion to strictly topological measures of network damage. In Section 1 we discuss possible ways of integrating other schemes of network damage into our models.

Let N_s denote the size of the largest connected component of surviving nodes after the disaster. We consider $N - N_s$ to be the *measure of network damage* caused by the natural disaster in this paper. It is worth mentioning that outside of the largest component, smaller groups of nodes can be functional as well. However, we select $N - N_s$ as the measure of network damage as it has a key characteristic as described next.

Let Δ_i^P denote the net power (generating capacity minus load) of node i in the network, where nodal generating capacity and load are both random variables. Note that net power may be positive or negative. We model each Δ_i^P by an independent Gaussian random variable with mean $\mu \geq 0$ and variance σ^2, as commonly used in literature [37, 38]. The variance of the Gaussian random variable reflects the uncertainty with nodal injections.

If node i is disconnected from the rest of the network, the probability q_0^i that its local load is served is then given by:

$$q_0^i = \mathbb{P}(\Delta_i^P \geq 0) = \int_0^\infty \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/\sigma^2} dx$$

$$\Rightarrow \quad q_0^i = .5 + \int_0^\mu \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/\sigma^2} dx \quad \text{as } \mu \geq 0 \tag{1}$$

On the other-hand, if node i is connected to a group of N_k nodes, the probability $q_{N_k}^i$ that node i satisfies its load is given by:

$$q_{N_k}^i = \mathbb{P}(\sum_{i=1}^{N_k} \Delta_i^P \geq 0) = \mathbb{P}(\sum_{i=1}^{N_k} \Delta_i^P/N_k \geq 0)$$

$$= .5 + \int_0^\mu \frac{1}{\sqrt{2\pi\sigma^2/N_k}} e^{-\frac{(x-\mu)^2}{\sigma^2/N_k}} dx \tag{2}$$

where Eq (2) follows from the fact that $\sum_{i=1}^{N_k} \Delta_i^P/N_k$ is a Gaussian($\mu, \sigma^2/N_k$) random variable. Note that its variance decreases with increase in N_k, the size of the connected set that node i belongs to. For $1 \leq N_k \leq N_s$, using properties of the exponential function it follows that

$$\int_0^\mu \frac{1}{\sqrt{2\pi\sigma^2/N_k}} e^{-\frac{(x-\mu)^2}{\sigma^2/N_k}} dx \leq \int_0^\mu \frac{1}{\sqrt{2\pi\sigma^2/N_s}} e^{-\frac{(x-\mu)^2}{\sigma^2/N_s}} dx \tag{3}$$

Using Eqs (1), (2) and (3), we have $q_1^i \leq q_{N_k}^i \leq q_{N_s}^i$.

Thus, *the probability of a nodal load being served is maximum when it belongs to the largest set of connected nodes.* This justifies our usage of N_s (size of the largest connected component of surviving nodes) to quantify the functional network and correspondingly of $N - N_s$ to measure the scale of network damage. Note that prior literature includes the use of the largest connected component in simulation based studies [39] of grid resilience. However the motivation behind its usage in power grids is not clearly stated or justified. In the next section, considering the largest component as the surviving network, we analyze the effects of network structure on the extent of failures and determine a preliminary bound on the probability of initial failure p_0 beyond which the network fragments.

Failure analysis and preliminary bound

As shown in Fig 2, we consider primary failures and secondary failures in the grid. The overall survival probability of each node depends on the absence of both failure cases and thus depends on the probability of initial failure and network structure. Let $\lambda^V(i)$ denote the survival probability of node i in set V. Due to the neighborhood based dependence of secondary failures, $\lambda^V(i)$ satisfies the relation

$$\lambda^V(i) = (1 - p_0)\mathbb{P}[\bigcup_{j:(ij)\in E} \{\text{node } j \text{ survives}\}] \tag{4}$$

$$\Rightarrow \lambda^V(i) \leq (1 - p_0) \sum_{j:(ij)\in E} \lambda^V(j) \tag{5}$$

$$\Rightarrow \lambda^V \leq (1 - p_0)A_{\mathcal{G}}\lambda^V \text{ (in vector form)} \tag{6}$$

Note that $1 - p_0$ is the probability of i surviving the primary failure, while the rest of the terms in Eq (4) denote the probability of at least one surviving neighbor node that connects it to the largest component and prevents secondary failure. Here Eq (5) follows from the Union Bound [40] for probabilities. Note that the union bound is not replaceable by an equality for grid graphs as failures at different nodes are correlated due to sharing common paths for connectivity. This is distinct from prior work in random graph models [17] where equality is assumed based on locally tree-like structural assumptions on the grid structure. In a related setting with varying initial probabilities of failures for different nodes (p_0^i for node i), we modify Eq (6) to compute the overall probability of failure. In particular, $(1 - p_0)$ on the right side of Eq (6) is replaced by a diagonal matrix with $(1 - p_0^i)$ as the ith diagonal entry. In the remaining sections, we limit our discussion to a constant $p_0^i = p_0 \forall i$ as we are interested in deriving thresholds based on it. Note that one can derive an upper bound on the value of λ^V by computing fixed point iterations of relation (6) till the values converge. Using that we have the following upper bound on the initial probability of random failures (p_0) beyond which the grid fragments.

Theorem 1 *Let $\beta_{A_{\mathcal{G}}}$ be the largest eigenvalue of the adjacency matrix $A_{\mathcal{G}}$. If $p_0 > 1 - 1/\beta_{A_{\mathcal{G}}}$, the grid fragments following the natural disaster.*

The proof follows immediately from the fact that if $(1 - p_0)\beta_{A_{\mathcal{G}}} < 1$, then $\lambda^V \to \mathbf{0}$. Thus, we have an **upper bound** on p_0. Note that this is indeed a bound and not an exact threshold due to correlated final probability of failures at different nodes. Further the current formulation does not specify the extent of damage in the region $p_0 < 1 - 1/\beta_{A_{\mathcal{G}}}$. In the next section, we present a novel modified graph construction based on the true grid graph that overcomes this and helps generate tighter bounds.

Modified graph for improved bounds

In our failure model, the survival of any node depends on the existence of edges that connect it to the largest connected component. We now analyze a node's survivability by modeling the probability of its connectivity through operational edges in the grid graph. This is done by construction of a '*modified*' graph based on the true grid graph. To motivate this approach better, consider node i and its neighbor j in the grid as shown in Fig 3(a). Let $B^E(ij)$ be the event that i is connected to the surviving nodes in the largest component through edge (ij). Let the probability of $B^E(ij)$ be denoted by $\lambda^E(ij)$. Similarly, such events can be defined for every neighboring node of node i. Note that node i's survivability requires at least one of these events to be true.
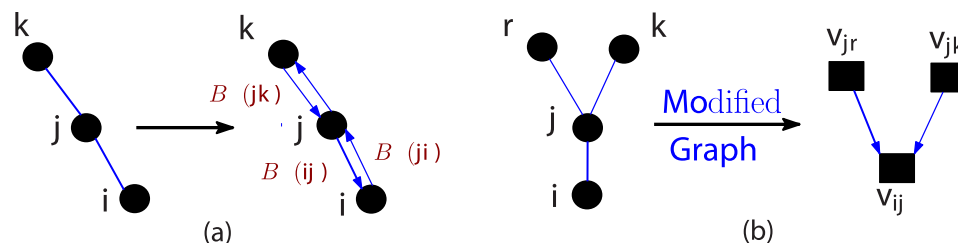
Fig 3. (a) Each undirected edge results in two survival probabilities, one in each direction. (b) Modified graph $\mathcal{G}^E$ formation from $\mathcal{G}$.

Thus, the probability of node i surviving is given by:

$$\lambda^V(i) = (1 - p_0)\mathbb{P}[\bigcup_{j:(ij)\in E} [B^E(ij)] \text{ where } \mathbb{P}[B^E(ij)] = \lambda^E(ij) \tag{7}$$

Here, the $(1 - p_0)$ term arises from the probability of node i surviving a primary failure, while the remaining terms correspond to the survivability due to at least one connecting edge. In a similar way, we define event $B^E(ji)$ of probability $\lambda^E(ji)$ for node j surviving through the edge with node i. This event is reciprocal to $B^E(ij)$. Thus, every edge gives rise to two probabilities of survival, one along each direction as shown in Fig 3(a). If nodes i, j and k are connected as shown in Fig 3(a), the event $B^E(ij)$ (node i surviving via edge (ij)) depends on node j not failing initially and events $B^E(jk)$ (j surviving through edge (jk)) for all neighbors k of node j. In terms of their probabilities, we write this relation mathematically $\forall i, j$ such that $(ij) \in E$ as

$$\lambda^E(ij) = (1 - p_0)\mathbb{P}[\bigcup_{k:(jk)\in E, k\neq i} B^E(jk)]$$
$$\Rightarrow \quad \lambda^E(ij) \leq (1 - p_0) \sum_{k:(jk)\in E, k\neq i} \lambda^E(jk) \quad \text{(using Union Bound)} \tag{8}$$

In Eq (8), the $(1 - p_0)$ comes from the fact that if node j fails initially, then node i cannot survive through edge (ij). Eq (8) is the motivation behind our construction of a **modified directed graph** $\mathcal{G}^E$ based on the power grid graph $\mathcal{G}$. The objective of constructing this graph is to demonstrate the analysis of $\lambda^E(ij)$ that denote the probability of survival via paths to the largest connected component. As demonstrated, this leads to better estimates of the scope of network failures. The construction is depicted in the following steps:

Graph Construction for directed graph $\mathcal{G}^E$ from grid $\mathcal{G}$:

- Each edge (ij) in E gives rise to two nodes v_{ij} and v_{ji} in $\mathcal{G}^E$, that represent orientations $i \rightarrow j$ and $j \rightarrow i$ in (ij).

- Two nodes v_{ij} and v_{kl} in $\mathcal{G}^E$ are connected by an edge directed from v_{kl} towards v_{ij} if $k = j$ and $l \neq i$ (see Fig 3(b)).

It is worth mentioning that $\mathcal{G}^E$ is similar in structure to a line graph for grid graph $\mathcal{G}$ as nodes in $\mathcal{G}^E$ arise from edges in $\mathcal{G}$. However, there is a slight difference in that $\mathcal{G}^E$ has lesser number of edges as a pair of nodes v_{ij} and v_{ji} are *not* neighbors in $\mathcal{G}^E$, though they would be in a standard line graph construction. The number of nodes in $\mathcal{G}^E$ is thus equal to twice the number of edges in $\mathcal{G}$. The size of A_E, the adjacency matrix of $\mathcal{G}^E$, is $2|E| \times 2|E|$. Note that both

graphs $\mathcal{G}$ and $\mathcal{G}^E$ represent the same network but the later is able to model higher number of probabilities due to considering directional effects. In particular, each node v_{ij} in $\mathcal{G}^E$ can be associated with probability of failure $\lambda^E(ij)$ that affects connectivity of node i through edge (ij) in the original graph $\mathcal{G}$. Thus, we can write Eq (8) in a vector form using the adjacency matrix of the modified graph $\mathcal{G}^E$ as follows:

$$\lambda^E \le (1 - p_0) A_E \lambda^E \tag{9}$$

Extending the analysis in the previous section to Eq (9), we get the following theorem that provides a **second upper bound** on the threshold on p_0, beyond which the grid fragments.

Theorem 2 *If β_{A_E} (the largest eigenvalue of A_E) satisfies $p_0 > 1 - 1/\beta_{A_E}$, then the grid disintegrates following the natural disaster.*

This follows as $\lambda^E \to \mathbf{0}$ and thus $\lambda^V \to \mathbf{0}$ when p_0 is greater than the value in Theorem 2. We compare the first upper bound in Theorem 1 with this second upper bound for different IEEE test-cases and real grids and observe that in all cases the second upper bound is smaller in magnitude and hence provides an improved and tighter bound on the failure threshold. The comparisons are noted in simulation results later in this section. This improvement is due to a more nuanced modeling of the failure process through directed graph $\mathcal{G}^E$ as compared to the original graph $\mathcal{G}$.

We now use the modified graph $\mathcal{G}^E$ and Eq (7) to analyze the extent of damage in the grid. In particular, we are interested in estimating the number of failures over the entire range of initial probability of failure p_0, even below the bounds derived earlier. For this, we use the basic failure definition that states that a node fails eventually if it suffers an initial failure or if it gets disconnected from the largest component. In other words, the probability of *not* surviving (given by $1 - \lambda^V(i)$ for node i in graph $\mathcal{G}$) depends on the initial probability of failure and also on the probability that *none* of its edges connect it to the largest component. Let $[B^E(ij)]^c$ denote the event of node i *not surviving* through edge (ij). Using the notation in Eq (7), $\mathbb{P}[B^E(ij)]^c = 1 - \lambda^E(ij)$. Mathematically, we have

$$1 - \lambda^V(i) = p_0 + (1 - p_0)\mathbb{P}[\bigcap_{j:(ij)\in E} [B^E(ij)]^c] \tag{10}$$

$$\le p_0 + (1 - p_0) \min_{j:(ij)\in E}(1 - \mathbb{P}[B^E(ij)]) \tag{11}$$

$$\le p_0 + (1 - p_0) \sum_{j:(ij)\in E} \frac{1 - \lambda^E(ij)}{d_i} \tag{12}$$

where d_i is the number of neighbors of node i in $\mathcal{G}$. Eq (10) follows from the failure definition where p_0 denotes the initial failure probability for original node i. Eq (11) follows from $\mathbb{P}[A \cap B] \le \min(\mathbb{P}[A], \mathbb{P}[B])$ while Eq (12) follows from the fact that the minimum of a set of numbers is less than their average. Summing over all nodes, the upper bound on the expected number of node failures in the gird (N_f) is given by:

$$N_f = \sum_{i=1}^{N}(1 - \lambda^V(i))$$

$$\Rightarrow \quad N_f \le p_0 N + (1 - p_0)\sum_{i=1}^{N} \sum_{j:(ij)\in E} \frac{1 - \lambda^E(ij)}{d_i} \tag{13}$$

Note that N_f depends on λ^E. Previously Eq (8) gave an upper bound on λ. Here we require an upper bound on $1 - \lambda^E$. For that we use a similar analysis as Eqs (10–12) and derive expressions for $(1 - \lambda^E(ij))$ for failure probabilities in the modified graph.

$$1 - \lambda^E(ij) = p_0 + (1 - p_0)\mathbb{P}[\bigcap_{k:(jk)\in E, k\neq i}[B^E(jk)]^c] \tag{14}$$

$$\leq p_0 + (1 - p_0)\sum_{k:(jk)\in E, k\neq i}\frac{1 - \lambda^E(jk)}{d_{ij}} \tag{15}$$

where d_{ij} is the number of neighbors of node v_{ij} in modified graph $\mathcal{G}^E$. Writing it in vector form, we get

$$\mathbf{1} - \lambda^E = p_0(\mathbb{I}_{2|E|} - (1 - p_0)D_E^{-1}A_E)^{-1} \tag{16}$$

where $\mathbb{I}_{2|E|}$ is the identity matrix of dimension $2|E|$ (number of nodes in $\mathcal{G}^E$). D_E is the diagonal matrix of node degrees (d_{ij}) in $\mathcal{G}^E$, while A_E is its adjacency matrix. We can now compute the **upper bound** on node failures as summarized in the following theorem.

Theorem 3 *Consider grid graph $\mathcal{G}$ with edge set E and modified directed graph $\mathcal{G}^E$. Let A_E and D_E respectively be the adjacency and degree matrices of $\mathcal{G}^E$. The expected number of nodal failures N_f after a natural disaster that induces an initial failure probability p_0 is upper bounded by the right side of* Eq (13), *where* $\mathbf{1} - \lambda^E$ *is given by* Eq (16).

To demonstrate the performance of our bounds, we present simulations of random failures on known power grid graphs.

Comparison of bounds through simulations

The performances of the upper bound on network failure over all values of p_0 and the two upper bounds on critical value of p_0 beyond which the network disintegrates are shown through simulations on the IEEE 118 and 300 bus test systems [35] in Fig 4(a) and 4(b) respectively. Subsequently we also consider publicly available power grid topologies pertaining to the grid under the Union for Coordination of Transmission of Electricity (UCTE) in Europe. The power grid of the UCTE has 1254 buses and 1811 lines [41, 42]. Failure propagation simulation and determined bounds for this network are shown in Fig 4(c). All simulations have been carried out in Matlab 2008 on a windows 8 machine.

In all the power grid cases, we consider the grid to have fragmented if the size of the largest connected component of surviving nodes is less than $2 \log N$, where N is the initial size of the network. This follows from the usage of logarithm of the original network size as a popular scale in graph percolation to signify total fragmentation [43]. It is true that for operational paradigms in power grids where additional information of nodal type and control architectures are available, percolation based notions of fragmentation may not present the entire picture. However we restrict ourselves to such bounds as we are strictly concerned with topological vulnerabilities in this paper and only analyze the affect of grid structure. In future work, we plan to merge topological notions of failure with operational and power flow based features.

In Fig 4(a)–4(c), it can be clearly observed that the novel second upper bound $(1 - 1/\beta_{A_E})$ on the threshold on p_0 (initial probability of failure) derived from the modified graph is lower and hence tighter than the first upper bound $(1 - 1/\beta_A)$ derived using the original graph. Next we discuss the upper bound on number of grid failures given by Theorem 3. Note that the upper bounds given by Eqs (13) and (16) is tighter for higher values of p_0 compared to smaller values. The gaps between the simulated number of failures and the upper bound arise due to
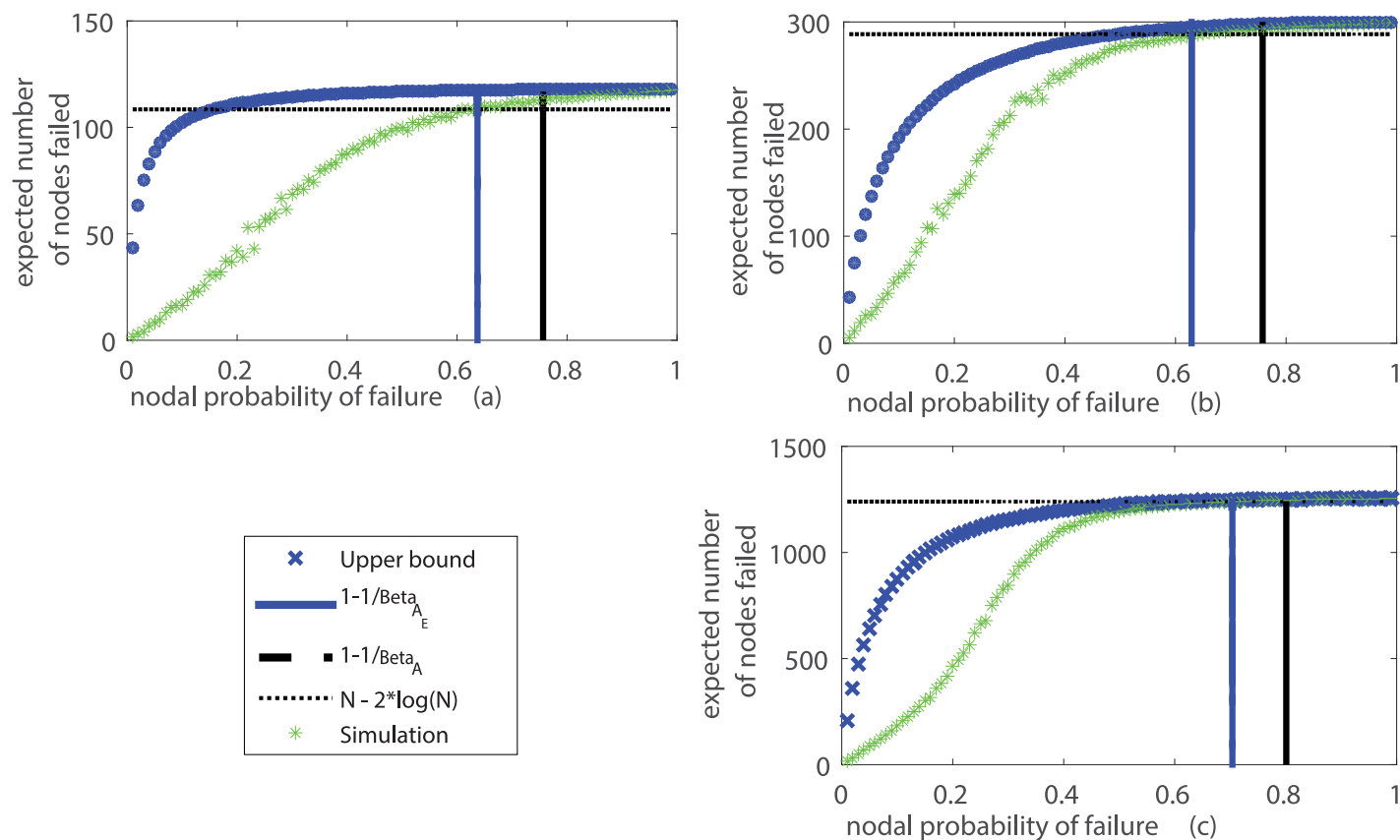
Fig 4. Upper bounds for number of failed nodes and bounds on p_0 in (a) IEEE 118 bus system (b) IEEE 300 bus system (c) UCTE power grid.

the presence of loops/cycles in the power grid graphs. These loops creates multiple paths between nodes and enhances grid robustness to fragmentation after the disaster. However the connectivity through the multiple paths are correlated and hence the inequalities described in Eqs (6) and (15) are weaker. In the absence of cycles, the grid graph is radial/tree-like where unique paths exist between any two nodes or between a node and the largest component. In this setting the upper bound given by Eqs (13) and (16) closely reflects the actual number of failures and will be tight.

The crucial advantage of the modified graph based analysis is the non-trivial upper bound on number of failures for values of p_0 below the threshold that are not captured by the original graph and in random graph based prior work. This is in addition to the tighter bound on threshold for network breakdown. As mentioned in the Introduction, one of the chief advantages of using topology information in determining measures of grid failure is in understanding vulnerable grid components that can help in securing the grid against adversarial attacks. This is particularly useful compared to random graph based models on power grids where specific nodes' effects on the grid vulnerability cannot be directly measured.

In the next section, we present algorithms to determine critical transmission lines that may be attacked by an adversary interested in weakening the grid resilience to natural disasters.

Critical lines for adversarial attack on grid resilience

We consider an adversary that aims to maximally weaken the grid structure to make it more vulnerable to failures during natural disasters. The adversary does so by attacking and

removing a fixed number (k_{max}) of transmission lines in the grid. As mentioned in prior sections, relations involving the eigenvalues of adjacency matrix of the grid graph or the modified graph provide upper bounds on the probability of failure beyond which grid connectivity diminishes greatly. *Decreasing* these upper bounds will enhance the vulnerability of the network to disasters. In the remainder of this section, we focus on the first upper bound $(1 - 1/\beta_{A_\mathcal{G}})$ given in Theorem 1. Techniques based on the modified graph in Eq (9) will be the focus of a future work. Let normalized eigenvector u_1 correspond to the largest eigenvalue $\beta_{A_\mathcal{G}}$ of adjacency matrix $A_\mathcal{G}$. By definition

$$\max_{\|x\|_2=1} x^T A_\mathcal{G} x = u_1^T A_\mathcal{G} u_1 = \beta_{A_\mathcal{G}} \tag{17}$$

The Perron-Frobenius theorem [44] states that eigenvector u_1 is a positive vector. From Eq (17), it is thus clear that removing edges from graph $\mathcal{G}$ (or deleting 1s from $A_\mathcal{G}$) leads to a reduction in the magnitude of its largest eigenvalue. Hence, we formulate the adversary's objective as follows.

Attack Problem: Identify and damage k_{max} edges in the graph to minimize $\beta_{A_\mathcal{G}}$, where $\beta_{A_\mathcal{G}}$ is the largest eigenvalue of the adjacency matrix $A_\mathcal{G}$.

This is a known NP-hard problem. Here, we present three approximate techniques to determine the critical lines that will be included in the adversary's target set.

Eigen-Perturbation based attack

In this attack scheme, we use perturbation analysis [44] to approximate the change in eigenvalues of adjacency matrix $A_\mathcal{G}$ following removal of edges. Let the new adjacency matrix of the grid after removal of edges be given by $A_\mathcal{G} - \Delta A_\mathcal{G}$. The change in adjacency matrix $\Delta A_\mathcal{G}$ has the following structure:

$$\Delta A_\mathcal{G}(i,j) = \begin{cases} 1 & \text{if edge } (ij) \in E \text{ is removed,} \\ 0 & \text{otherwise,} \end{cases} \tag{18}$$

Let the largest eigenvalue of new adjacency matrix be $\beta_{A_\mathcal{G}}^\Delta$. From Eq (17), we have

$$\begin{aligned}
\beta_{A_\mathcal{G}}^\Delta &= \max_{\|x\|_2=1} x^T (A_\mathcal{G} - \Delta A_\mathcal{G}) x \\
\Rightarrow \quad \beta_{A_\mathcal{G}}^\Delta &\geq u_1^T (A_\mathcal{G} - \Delta A_\mathcal{G}) u_1 = \beta_{A_\mathcal{G}} - u_1^T \Delta A_\mathcal{G} u_1 \\
\Rightarrow \quad \beta_{A_\mathcal{G}} - \beta_{A_\mathcal{G}}^\Delta &\leq u_1^T \Delta A_\mathcal{G} u_1 \\
\Rightarrow \quad \Delta \beta_{A_\mathcal{G}} &\approx \sum_{\text{removed } (ij)} 2 u_1(i) u_1(j) \quad (\text{using Eq (18)})
\end{aligned} \tag{19}$$

where $\Delta \beta_{A_\mathcal{G}} = \beta_{A_\mathcal{G}} - \beta_{A_\mathcal{G}}^\Delta$ denotes the change in the maximum eigen-value.

The optimal transmission lines in the attack are then determined by maximizing the linear expression in Eq (19). Next, we use this to design a modified attack scheme.

Iterative Eigen-Perturbation based attack

In this scheme, the adversary does not select all k_{max} lines together by maximizing Eq (19). Instead, it selects them iteratively, one at a time. In each iteration, it computes u_1, the eigenvector corresponding to the largest eigenvalue, removes line to maximize Eq (19) and refines the adjacency matrix. As shown later, the iterative scheme provides far greater reduction in grid

resilience than selecting the k_{max} lines all at once, though it leads to an increase in computational complexity.

Complexity: The computation of the eigenvector u_1 takes $O(N^3)$ steps via Singular Value Decomposition (SVD) of $A_{\mathcal{G}}$ [45]. Given that the maximization of Eq (19) takes $k_{max}|E|$ steps which is less than $O(N^3)$, computing the k_{max} critical lines by the first non-iterative approach takes $O(N^3)$. On the other hand, the iterative scheme needs k_{max} SVD computations and hence has a complexity of $O(k_{max}N^3)$. Finally, we describe another technique for attack design that depends on trace minimization.

Trace minimization based attack

The trace of a square matrix refers to the sum of its diagonal elements and is equal to the sum of its eigenvalues [44]. Consider the $2r^{th}$ power of the adjacency matrix $A_{\mathcal{G}}$, where $2r$ is an even positive integer. The eigenvalues of $A_{\mathcal{G}}^{2r}$ are the $2r^{th}$ powers of the eigenvalues $(\beta_{A_{\mathcal{G}}} = \beta_1 > \beta_2, \ldots \geq \beta_N)$ of $A_{\mathcal{G}}$. We thus have the following relation for its trace

$$trace(A_{\mathcal{G}}^{2r}) = \sum_{i=1}^{N} \beta_i^{2r} = \beta_{A_{\mathcal{G}}}^{2r}\left(1 + \left(\frac{\beta_2}{\beta_{A_{\mathcal{G}}}}\right)^{2r} + \ldots + \left(\frac{\beta_N}{\beta_{A_{\mathcal{G}}}}\right)^{2r}\right) \qquad (20)$$

$$\Rightarrow \lim_{r \to \infty} trace(A_{\mathcal{G}}^{2r})/\beta_{A_{\mathcal{G}}}^{2r} \approx 1 \qquad (21)$$

where $\beta_{A_{\mathcal{G}}} = \beta_1$ is the largest eigenvalue of the adjacency matrix. Eq (21) follows as $\left|\frac{\beta_i}{\beta_{A_{\mathcal{G}}}}\right| < 1 \forall 2 \leq i \leq N$. Thus, for large values of r, the largest eigenvalue and trace of the $2r^{th}$ power of $A_{\mathcal{G}}$ are approximately equal. In this attack design, we thus remove lines to reduce the trace of $A_{\mathcal{G}}^{2r}$ instead of the largest eigenvalue $\beta_{A_{\mathcal{G}}}$ or its higher power $\beta_{A_{\mathcal{G}}}^{2r}$. Optimal minimization of the trace of $A_{\mathcal{G}}^{2r}$ is computationally hard as well, however it has certain advantages as discussed in the next result.

Theorem 4 *The trace of $A_{\mathcal{G}}^{2r}$, where $A_{\mathcal{G}}$ is the adjacency matrix of grid graph $\mathcal{G}$ is a supermodular function of the constituent edges in the graph.*

Note: A real-valued function f defined over set S is *supermodular* [46] if $f(A \cup C) - f(A) \geq f(B \cup C) - f(B)$ for $B \subset A$ and A, B, C are subsets of S. In other words, the returns due to addition of C are not diminishing.

Proof: Let a cycle of length $2r$ in $A_{\mathcal{G}}$ refer to a graph path with $2r$ hops (repetition allowed) that begins and ends at the same node. Note that the ith diagonal element in $A_{\mathcal{G}}^{2r}$ is equal to the number of cycles of length $2r$ that begin and end at node i. This can be shown by direct checks or by mathematical induction. Thus, the trace of $A_{\mathcal{G}}^{2r}$ is given by the total number of cycles of length $2r$ formed on all nodes in the grid graph. To show that trace of $A_{\mathcal{G}}^{2r}$ is a supermodular function, we consider edge sets $A, B = A \bigcup \{(lm)\}, C = \{(ij)\}$ for edges $(lm), (ij) \notin A$. We argue that the increase in the number of cycles of length $2r$ in edge set A is less than the increase observed in set B due to addition of edge (ij). This is true as presence of edge (lm) in $B \cup C$ produces cycles having both edges (lm) and (ij) that cannot be formed in $A \cup C$. The trace of $A_{\mathcal{G}}^{2r}$ is thus a supermodular function of the graph edges.

It is a known that greedy minimization of a supermodular function is equivalent to greedy maximization of a submodular function and is provably at least $1 - 1/e$ ($\approx 63\%$) close to the optimal solution [46]. Thus, the adversary's attack policy in this scheme is **to greedily remove k_{max} edges that minimizes the trace of $2r^{th}$ power of the adjacency matrix of the grid graph.**

Complexity: The $2r^{th}$ power of the symmetric adjacency matrix is computed efficiently using Singular Value Decomposition (SVD) as $A_{\mathcal{G}}^{2r} = U\beta_{A_{\mathcal{G}}}^{2r}U^T$ where columns of U are the eigenvectors and $\beta_{A_{\mathcal{G}}}^{2r}$ is the diagonal matrix with $2r^{th}$ powers of the eigenvalues. Note that matrix multiplication and SVD are computed in $O(N^3)$ while computing $\beta_{A_{\mathcal{G}}}^{2r}$ takes complexity $O(N \log r)$. Since we greedily minimize the trace, the selection of one edge takes $O(|E|(N^3 + N \log r))$. The overall complexity of computing k_{max} optimal edges by this scheme is thus $O(k_{max}|E|(N^3 + N \log r))$. This expression implies that increasing r to improve the accuracy of this approach will at most lead to a logarithmic increase in the complexity.

Resilience: From the grid controller's perspective, these techniques can be used to determine the critical transmission lines for enhancing security and reinforcement to prevent adversarial manipulation aimed at disrupting grid resilience to natural disasters. In the next section, we look at the performance of these approaches as an adversarial tool.

Simulation results of adversarial attacks

We consider all approaches (eigen perturbation, iterative eigen perturbation and trace minimization) for determining the optimal k_{max} edges to minimize the largest eigenvalue of the adjacency matrix of the grid graph and thereby reduce the resilience of the grid to natural disasters. Note that each of these methods use global properties of the network in determining the most vulnerable edges. To demonstrate the improvements from our schemes, we compare them with two alternate schemes: one where an adversary removes edges randomly, and another where an adversary removes edges in the decreasing order of their betweenness centralities suggested in prior work [14]. We plot our results for the IEEE 118 and 300 bus test systems and the UCTE power grid network in Fig 5(a), 5(b) and 5(c) respectively. Note that both algorithms outperform random and betweenness based attacks [19, 31] to reduce the eigenvalues. It can also be noted that iterative eigen perturbation reduces the largest eigenvalue further than edge removal based on a single perturbation computation as mentioned in the previous section. Further, it can be observed from Fig 5(a) and 5(b) that increasing the value of $2r$, the power of the adjacency matrix, leads to an improvement in the trace minimization based scheme as it approximates the largest eigenvalue better as noted in Eq (21). These plots highlight the benefit derived from utilizing the structural information of the network in studying the vulnerable components of the grid.

Limitations and extensions

In this section, we discuss simplifications in our model in comparison to other techniques and present a path forward to its incorporation into general grid resilience research. As the primary objective of the work is in understanding topological effects on grid vulnerability, we limit our study to connectivity based failures where we show improved performance over general random graph based prior work. It needs to be mentioned that studying size of largest connected component in a grid is realistic when looking at distributed placement of similar controllers or generators throughout the network. In the dynamic regime, the larger the connected component is, the greater is its ability to withstand fluctuations in voltage and frequency. However including dynamics models of power flows in the analysis is important. Note that cascading failures in the grid are complex processes that begin at slower time-scales with overloading of lines etc. and eventually at faster time-scales due to frequency and voltage based automatic tripping of different components. At different scales, different models for network flow are applicable and hence a single method is not sufficient to understand vulnerability to failures. Further different components (generators/loads) may have differing failure models. One
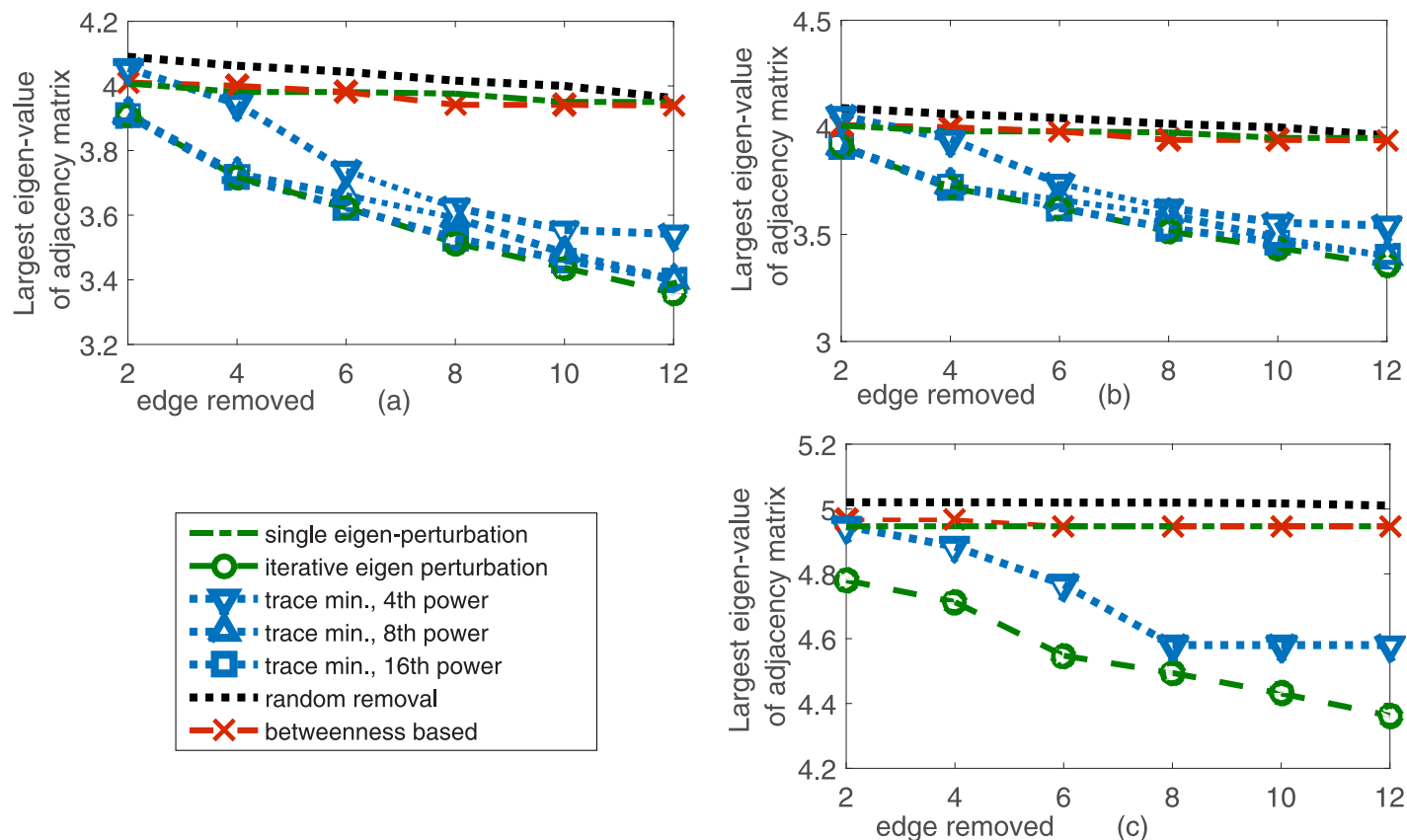
Fig 5. Comparison of adversarial schemes to reduce maximum eigenvalue of grid adjacency matrix in (a) IEEE 118 bus test system (b) IEEE 300 bus test system (c) UCTE power grid.

potential way of extending our methodology to multiple component types would include keeping different probabilities of nodal failures and dependence on neighbors.

In future extensions, nodal types (generator/load/distributor) and system constraints (line limits/nodal voltage limits/power capacities) should be included to in the topological failure model, though analytic formulae for thresholds may be harder to derive. Further if knowledge of node type is available, grid failures can be studied at group levels (sub-networks) that can self-sustain if disconnected. It is unlikely that a single method of vulnerability analysis can approximate the failure propagation in the full-scale power grid model. Hence a judicious combination of topological models, static power flow based and grid dynamics based models should be utilized to determine optimal actions and reinforcements to enable the protection of the grid.

Conclusion

We analyze topological vulnerability of power grids to probabilistic failures introduced by natural disasters in this paper. We analyze the evolving failure process that originates at nodes with initial failures. Based on the adjacency matrix of the grid, we present two bounds on the critical initial probability of node failures beyond which the grid fragments. We also derive a new non-trivial upper bound on the expected number of total failures after the disaster. We present the performance of our derived bounds on two IEEE test cases and a real grid data set. Finally, we discuss adversarial attacks on the power grid aimed at damaging transmission lines

to minimize the grid's resilience to natural disasters. We develop approximate algorithms to identify the critical lines that will enable such adversarial attacks—the first two based on perturbation analysis of the eigenvalues of the adjacency matrix, and the third algorithm based on minimization of the trace of a higher power of the adjacency matrix. We analyze the complexity of both algorithms and demonstrate their performance against random and centrality based attacks studied in literature through simulations.

Moving forward, we plan to generalize our failure models with respect to diversity of nodes and initial probability of failures. Further we plan to incorporate our model with existing work as mentioned in the preceding section.

In future work, we plan to build upon the techniques developed in this paper to incorporate more realistic features of grid operations.

Author Contributions

Conceptualization: Deepjyoti Deka, Sriram Vishwanath, Ross Baldick.

Data curation: Deepjyoti Deka.

Formal analysis: Deepjyoti Deka, Sriram Vishwanath, Ross Baldick.

Investigation: Deepjyoti Deka, Ross Baldick.

Methodology: Deepjyoti Deka, Sriram Vishwanath.

Resources: Deepjyoti Deka.

Software: Deepjyoti Deka, Sriram Vishwanath.

Supervision: Sriram Vishwanath, Ross Baldick.

Validation: Deepjyoti Deka, Sriram Vishwanath, Ross Baldick.

Visualization: Deepjyoti Deka, Sriram Vishwanath, Ross Baldick.

Writing – original draft: Deepjyoti Deka.

Writing – review & editing: Deepjyoti Deka, Sriram Vishwanath, Ross Baldick.

References

1. Deka D, Vishwanath S, Baldick R. Analytical Models for Power Networks: The case of the Western US and ERCOT grids. IEEE Transactions on Smart Grid. 2016 Mar 22.

2. Lavaei J, Low SH. Zero duality gap in optimal power flow problem. IEEE Transactions on Power Systems. 2012 Feb; 27(1):92–107. https://doi.org/10.1109/TPWRS.2011.2160974

3. Deka, D., Nagarajan, H. and Backhaus, S., 2017. Optimal Topology Design for Disturbance Minimization in Power Grids. InIEEE American Control Conference. 2017 May.

4. Kwasinski A, Weaver WW, Chapman PL, Krein PT. Telecommunications power plant damage assessment for hurricane katrina–site survey and follow-up results. IEEE Systems Journal. 2009 Sep; 3 (3):277–87. https://doi.org/10.1109/JSYST.2009.2026783

5. Kantha L. Time to replace the Saffir-Simpson hurricane scale?. Eos, Transactions American Geophysical Union. 2006 Jan 3; 87(1):3–6. https://doi.org/10.1029/2006EO010003

6. Dobson I, Carreras BA, Lynch VE, Newman DE. An initial model for complex dynamics in electric power system blackouts. In Proceedings of the Annual Hawaii International Conference on System Sciences 2001 Jan 3 (pp. 51–51)

7. Dobson I, Carreras BA, Lynch VE, Newman DE. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2007 Jun; 17(2):026103. https://doi.org/10.1063/1.2737822

8. Bienstock D, Verma A. The nk problem in power grids: New models, formulations, and numerical experiments. SIAM Journal on Optimization. 2010 Jun 3; 20(5):2352–80. https://doi.org/10.1137/08073562X

9. Bernstein A, Bienstock D, Hay D, Uzunoglu M, Zussman G. Power grid vulnerability to geographically correlated failures—analysis and control implications. InINFOCOM, 2014 Proceedings IEEE 2014 Apr 27 (pp. 2634–2642). IEEE.

10. Wang Y, Baldick R. Interdiction analysis of electric grids combining cascading outage and medium-term impacts. IEEE Transactions on Power Systems. 2014 Sep; 29(5):2160–8. https://doi.org/10.1109/TPWRS.2014.2300695

11. Kundur Prabha, Balu Neal J., and Lauby Mark G. Power system stability and control. Vol. 7. New York: McGraw-hill, 1994.

12. Motter Adilson E., Seth A. Myers, Marian Anghel, and Takashi Nishikawa. Spontaneous synchrony in power-grid networks. Nature Physics 9, no. 3 (2013): 191–197.

13. Albert R, Jeong H, Barabási AL. Error and attack tolerance of complex networks. nature. 2000 Jul 27; 406(6794):378–82. https://doi.org/10.1038/35019019 PMID: 10935628

14. Motter AE, Lai YC. Cascade-based attacks on complex networks. Physical Review E. 2002 Dec 20; 66(6):065102. https://doi.org/10.1103/PhysRevE.66.065102

15. Wang JW, Rong LL. Cascade-based attack vulnerability on the US power grid. Safety Science. 2009 Dec 31; 47(10):1332–6. https://doi.org/10.1016/j.ssci.2009.02.002

16. Wang JW, Rong LL. Robustness of the western United States power grid under edge attack strategies due to cascading failures. Safety science. 2011 Jul 31; 49(6):807–12. https://doi.org/10.1016/j.ssci.2010.10.003

17. Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature. 2010 Apr 15; 464(7291):1025–8. https://doi.org/10.1038/nature08932 PMID: 20393559

18. R. Parshani, S. V. Buldyrev, and S. Havlin, "Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition", *Physical Review Letters*, 2010.

19. Yagan O, Qian D, Zhang J, Cochran D. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. IEEE Transactions on Parallel and Distributed Systems. 2012 Sep; 23(9):1708–20. https://doi.org/10.1109/TPDS.2012.62

20. Sun S, Wu Y, Ma Y, Wang L, Gao Z, Xia C. Impact of Degree Heterogeneity on Attack Vulnerability of Interdependent Networks. Scientific Reports. 2016; 6.

21. Kong Z, Yeh EM. Resilience to degree-dependent and cascading node failures in random geometric networks. IEEE Transactions on Information Theory. 2010 Nov; 56(11):5533–46. https://doi.org/10.1109/TIT.2010.2068910

22. Xiao H, Yeh EM. Cascading link failure in the power grid: A percolation-based analysis. InCommunications Workshops (ICC), 2011 IEEE International Conference on 2011 Jun 5 (pp. 1–6). IEEE.

23. Qi J, Sun K, Mei S. An interaction model for simulation and mitigation of cascading failures. IEEE Transactions on Power Systems. 2015 Mar; 30(2):804–19. https://doi.org/10.1109/TPWRS.2014.2337284

24. Wang J. Robustness of complex networks with the local protection strategy against cascading failures. Safety Science. 2013 Mar 31; 53:219–25. https://doi.org/10.1016/j.ssci.2012.09.011

25. Hines P, Cotilla-Sanchez E, Blumsack S. Do topological models provide good information about electricity infrastructure vulnerability?. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2010 Sep; 20(3):033122. https://doi.org/10.1063/1.3489887

26. Wang Y, Chen C, Wang J, Baldick R. Research on resilience of power systems under natural disasters—A review. IEEE Transactions on Power Systems. 2016 Mar; 31(2):1604–13. https://doi.org/10.1109/TPWRS.2015.2429656

27. Miller JC, Hyman JM. Effective vaccination strategies for realistic social networks. Physica A: Statistical Mechanics and its Applications. 2007 Dec 15; 386(2):780–5. https://doi.org/10.1016/j.physa.2007.08.054

28. Boguná M, Pastor-Satorras R, Vespignani A. Epidemic spreading in complex networks with degree correlations. InProceedings of the XVIII Sitges Conference on Statistical Mechanics, Lecture Notes in Physics, Springer, Berlin 2003 Jan 10.

29. Sun S, Li R, Wang L, Xia C. Reduced synchronizability of dynamical scale-free networks with onion-like topologies. Applied Mathematics and Computation. 2015 Feb 1; 252:249–56. https://doi.org/10.1016/j.amc.2014.12.044

30. Parshani R, Buldyrev SV, Havlin S. Interdependent networks: reducing the coupling strength leads to a change from a first to second order percolation transition. Physical review letters. 2010 Jul 21; 105(4):048701. https://doi.org/10.1103/PhysRevLett.105.048701 PMID: 20867893

31. Cotilla-Sanchez E, Hines PD, Barrows C, Blumsack S. Comparing the topological and electrical structure of the North American electric power infrastructure. IEEE Systems Journal. 2012 Dec; 6(4):616–26. https://doi.org/10.1109/JSYST.2012.2183033

32. Wang Z, Scaglione A, Thomas RJ. Generating statistically correct random topologies for testing smart grid communication and control networks. IEEE Transactions on Smart Grid. 2010 Jun; 1(1):28–39. https://doi.org/10.1109/TSG.2010.2044814

33. Deka D, Vishwanath S. Generative growth model for power grids. InSignal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on 2013 Dec 2 (pp. 591–598). IEEE.

34. Sun S, Ma Y, Wu Y, Wang L, Xia C. Towards structural controllability of local-world networks. Physics Letters A. 2016 May 20; 380(22):1912–7. https://doi.org/10.1016/j.physleta.2016.03.048

35. Athay T, Podmore R, Virmani S. A practical method for the direct analysis of transient stability. IEEE Transactions on Power Apparatus and Systems. 1979 Mar(2):573–84. https://doi.org/10.1109/TPAS.1979.319407

36. Krishnamurthy V, Kwasinski A. Empirically validated availability model of information and communication technologies facilities under hurricane conditions. InTelecommunications Energy Conference (INTELEC), 2014 IEEE 36th International 2014 Sep 28 (pp. 1–8). IEEE.

37. Dvorkin Y, Lubin M, Backhaus S, Chertkov M. Uncertainty sets for wind power generation. IEEE Transactions on Power Systems. 2016 Jul; 31(4):3326–7. https://doi.org/10.1109/TPWRS.2015.2476664

38. Lee D, Baldick R. Short-term wind power ensemble prediction based on Gaussian processes and neural networks. IEEE Transactions on Smart Grid. 2014 Jan; 5(1):501–10. https://doi.org/10.1109/TSG.2013.2280649

39. Schneider CM, Moreira AA, Andrade JS, Havlin S, Herrmann HJ. Mitigation of malicious attacks on networks. Proceedings of the National Academy of Sciences. 2011 Mar 8; 108(10):3838–41. https://doi.org/10.1073/pnas.1009440108

40. Grimmett G, Stirzaker D. Probability and random processes. Oxford university press; 2001 May 31.

41. Zhou Q, Bialek JW. Approximate model of European interconnected system as a benchmark system to study effects of cross-border trades. IEEE Transactions on power systems. 2005 May; 20(2):782–8. https://doi.org/10.1109/TPWRS.2005.846178

42. Approximate Model of European Interconnected System. Available from: http://www.see.ed.ac.uk/jbialek/Europe%20load%20flow/.

43. Durrett R., "Random graph dynamics", Cambridge University Press, 2006.

44. Stewart GW. Matrix perturbation theory.

45. Golub GH, Van Loan CF. Matrix computations. JHU Press; 2012 Dec 27.

46. Nemhauser GL, Wolsey LA, Fisher ML. An analysis of approximations for maximizing submodular set functions—I. Mathematical Programming. 1978 Dec 1; 14(1):265–94. https://doi.org/10.1007/BF01588971