Chaos

Don't go chasing artificial waterfalls: Artificial line limits and cascading failures in power grids

Cite as: Chaos **29**, 113117 (2019); https://doi.org/10.1063/1.5115493
Submitted: 18 June 2019 . Accepted: 17 October 2019 . Published Online: 15 November 2019

J. Bourne, A. O'Sullivan, and E. Arcaute

Chaos ARTICLE scitation.org/journal/cha

Don't go chasing artificial waterfalls: Artificial line limits and cascading failures in power grids

Cite as: Chaos **29**, 113117 (2019); doi: 10.1063/1.5115493
Submitted: 18 June 2019 · Accepted: 17 October 2019 ·
Published Online: 15 November 2019 · Publisher error corrected: 19 November 2019

View Online Export Citation CrossMark

J. Bourne,[1,2,a] A. O'Sullivan,[1] and E. Arcaute[2]

AFFILIATIONS

[1] UCL Energy Institute, University College London, Gower Street, London WC1E 6BT, United Kingdom
[2] Centre for Advanced Spatial Analysis (CASA), University College London, Gower St, London WC1E 6BT, United Kingdom

Note: This paper is part of the Focus Issue on the Dynamics of Modern Power Grids.
[a] **Electronic mail:** ucabbou@ucl.ac.uk

ABSTRACT

Research on cascading failures in power-transmission networks requires detailed data on the capacity of individual transmission lines. However, these data are often unavailable to researchers. Consequently, line limits are often modeled by assuming that they are proportional to some average load. However, there is scarce research to support this assumption as being realistic. In this paper, we analyze the proportional loading (PL) approach and compare it to two linear models that use voltage and initial power flow as variables and are trained on the line limits of a real power network that we have access to. We compare these artificial line-limit methods using four tests: the ability to model true line limits, the damage done during an attack, the order in which edges are lost, and accuracy ranking the relative performance of different attack strategies. We find that the linear models are the top-performing method or are close to the top in all the tests we perform. In comparison, the tolerance value that produces the best PL limits changes depending on the test. The PL approach was a particularly poor fit when the line tolerance was less than two, which is the most commonly used value range in cascading failure research. We also find indications that the accuracy of modeling line limits does not indicate how well a model will represent grid collapse. The findings of this paper provide an understanding of the weaknesses of the PL approach and offer an alternative method of line-limit modeling.

The networked structure of power-transmission grids makes them susceptible to cascading failures. A cascading failure occurs when a single failure or a small number of failures propagate through a system, wreaking havoc. While major blackouts caused by cascading failures are rare, they affect a very large number of people and have significant financial consequences.[1–3] This paper considers the resilience of the power grid from the perspective of network science. In this context, cascading failures are not simulated using random failure but attacks that continue until the complete collapse of the network. The potential for such threats comes from either physical[4] or cyber-physical[5] attacks. The first known cyber-physical attack was in Ukraine which caused power loss to 200 000 people.[6] Since then the perceived threat of cyber-physical attacks has grown.[5] This paper explores a commonly used method to simulate cascading failures in the power grid, known as proportional loading, and finds that inaccurate estimation of the system tolerance produces modeling results that deviate substantially from the behavior of the grid under attack when using the real line limits.

I. INTRODUCTION

Power networks are an essential part of modern civilization. Power outages caused by either random failure or targeted attack can cascade through the power system and cause massive damage. In the last two decades, there have been several examples of cascading failures causing a loss of power to tens, sometimes hundreds of millions of people. In 2003, a major blackout in the northeast portion of the USA was estimated to have cost approximately \$6 billion.[1] In 2012, a cascading failure in the Indian power grid caused a loss of power to 600×10^6 people.[2] More recently, in 2019,[3] a failure in the interconnector between Argentina and Uruguay caused a blackout that affected nearly the entirety of both countries, which was close to 50×10^6 people. In addition to random failures, targeted cyber-physical attacks have become a growing threat to the power grid.[5,7] Cyber-physical attacks are so-called because they use cyber attacks to cause physical effects. The most successful cyber-physical attacks were against the Ukrainian power grid in 2015 and 2016 causing a loss of power to 200 000 people.[6,8] Given the potential magnitude of cascading failures and the threat posed by a deliberate attack, it is not surprising that researchers are looking for ways to reduce the impact and frequency of such failures. One method of understanding cascading failures is through network science, where cascading failures are stimulated using targeted attacks on network nodes or edges. Substantial work in this regard has focused on developing "vulnerability metrics" or "attack strategies" that identify the order in which nodes should be attacked to cause maximum damage to the power grid.

When researchers first began analyzing power grids using network science, the techniques applied used purely topological information about the power-grid structure.[9] As research developed, the power-grid's electrical properties were incorporated into the analysis, thereby creating the "extended topology."[10] Specifically, the extended topology integrates the power flowing in the network with the topological features. In most cases, electricity is transmitted through the power grid using alternating current (AC) at high voltage to reduce power loss, although direct current (DC) can be used point-to-point over long distances or underwater (e.g., the UK interconnectors to France, Ireland, and The Netherlands). However, as it is challenging to solve the AC power-flow equations, researchers often use DC power flow equations which can be solved using linear algebra. A recent literature review revealed that 81% of studies that involved power flow used DC power flow.[9] We use the DC power flow calculations, $\mathbf{f} = \mathbf{CA}(\mathbf{A}^{\mathrm{T}}\mathbf{CA})^{-1}\mathbf{p}$, described by Pepyne[11] and Arianos *et al.*[12] In this equation, $\mathbf{A}$ is the adjacency matrix with the slack bus removed to make the system invertible, $\mathbf{C}$ is a diagonal matrix of the line susceptance, and $\mathbf{p}$ is the power injected at each node. The slack bus absorbs or supplies additional power as demanded in order to ensure that the system is balanced.

Numerous studies create synthetic networks[11–14] or use the topological structure of a real power grid without the line limits.[13,15–18] It is necessary to know these limits to detect when a line has tripped in a simulation. Beyond cascading failure research, equivalencing is used to reduce large complex power networks to smaller sub grids in order to study local phenomena. In such cases, estimating the line limits of the equivalenced networks is important so as to be able to perform accurate analyses.[19–21] Although a few open-data solutions are being developed,[22,23] the lack of datasets with line limits remains a problem. Little modeling or simulation work has been done using real line limits[24] for this reason. If these limits are not available in the data, an estimate must be made. A few studies[25,26] have used statistical techniques to provide a distribution of possible line limits. However, a more common technique for this is to use proportional loading (PL). When using the PL approach, the line limits are set at a fixed proportion of the amount of power flowing in each line at initiation.[11,15,17,27–30] The PL of networks is usually defined as $f_i^{\max} = \alpha \left|f_i^c\right|$, where $\left|f_i^c\right|$ is the absolute power flow for line i under initial conditions, $f_i^{\max}$ is the line limit, and α is the tolerance factor. The PL assumes that the line limits of the network are proportional to the power flow; however, there is little evidence supporting this.

As there is no direct comparison between PL and real line limits, it is difficult to know how accurately PL and the simulations based on it reflect real-grid behavior or whether a more realistic method can be created. In this paper, we address this gap. We have access to a dataset that includes the generation and load nodes with capacities in megawatts, as well as the line limits in megawatts for a single base load profile of the power grid. The dataset is a simplified version of the UK power grid and is based on the Electrical Ten Year Statement (ETYS) produced by the national grid.

Using the base load profile, we compare the real line limits of the network against the PL values of α between 1 and 50, the results produced by two linear models, and topological analysis. We simulate random attacks on the power grid and analyze how well the artificial line limits model the damage caused by the attack as well as the order in which the edges are lost due to cascading. We also measure how well each line-limit method ranks the relative effectiveness of different grid-attack strategies. The findings of this paper provide an understanding of the weaknesses of the PL approach and provide an alternative method of line-limit modeling using linear models.

II. METHOD

1. We examine the network's real line-limit distribution. We then compare the accuracy of PL (proportional loading) and the modeled limits (using two different linear models) against the real line limits.
2. We simulate random attacks on the grid using the DC power flow model. We attack the grid until it collapses completely, repeating the process 100 times. We compare the mean damage and standard deviation of the artificial line limits and the real line limits at each stage of the attacks.
3. We compare the rank order in which edges are lost due to cascades between the artificial and real line limits. Then, we calculate the correlation coefficient, which shows us which artificial line-limit method most accurately represents the behavior of grid collapse.
4. In order to test whether the artificial line limits can compare vulnerability metrics, we attack the grid using five different strategies. We measure the ability of the artificial line limits to accurately represent the true ranking of each strategy using the real line limits.

The dataset we use in this paper describes the physical and electrical structures of a simplified version of the UK national grid. The dataset contains 512 nodes representing substations around the UK. The nodes are connected with 698 transmission lines that are rated 132 kV, 275 kV, and 400 kV. The network has a mean degree of 2.73, the average unweighted nodal distance is 11.7, and the clustering and mean normalized centrality are at 0.1. The low clustering coefficient, close to zero, suggests that the network tends to not form connected cliques, thereby making the network more vulnerable to disruption when individual nodes are lost. The dataset includes all the information required to perform the DC power flow calculations. This information includes line-node connections, line-reactance, base load node load/demand, and node generation. Unusually for a power-grid dataset, it also provides line limits, thereby making it possible to test the PL approach.

This paper defines the simulation using five parameters: physics model, element, attack type, removal method, and load profile. The physics model used in this analysis is DC flow or topological—that is, the power model uses DC power flow or is simply a topological analysis. The elements attacked are the nodes. The attack type is "fixed," meaning that the order in which the nodes will be removed

TABLE I. PEARL settings used in this paper.

Class	Types
Physics	Cascading DC, topological
Element	Node
Attack type	Fixed
Removal	Sequential
Load profile	Single

is generated before the attack begins. The order in which nodes are removed is sequential. This means that only a single node is targeted for removal each round. However, other nodes may be lost due to a cascading failure. A summary of the parameters is shown in Table I. These simulation parameters form the acronym PEARL. (The PEARL framework is discussed in greater depth in supplementary material S1.)

The last parameter of the PEARL settings is the load profile—although ideally we would use multiple demand load profiles for our analysis to explore the effects of time of day and seasonality, such data are unavailable to us. However, we do have a single load profile provided with the dataset, and we use this. This load profile is based on the year-round base load. The base-load data are provided by the UK power suppliers in their seven-year statements. In general, it is advisable to use multiple load profiles when performing cascading failure analysis on the power-grid, as cascade behavior can differ depending on line loading.[31] In this paper, we only have access to a single load profile; however, the goal of this paper is not to demonstrate any weaknesses of the UK power grid itself but to highlight the weaknesses of proportional loading. For such a goal, only a single line limit is necessary.

In this analysis, there are no restrictions on the generators. This implies that a generator of 100 MW in a subgraph with a load node of 1 MW will reduce its power output to balance the demands of the subgraph. This is a simplification and, in reality, there would be constraints on the output of the power station; however, that is beyond the scope of this paper.

A. Artificial line limits and real line limits

In order to understand how artificial line limits differ from real line limits, we use 13 α values for PL, the topological approach, and the line limits generated from two linear models. We use α values of 1.05, 1.1, 1.2, 1.3, 1.5, 2, 3, 5, 7, 10, 15, 20, and 50. The α values were selected on the basis of values used in other papers, typically 1 to 5, and extended until 50. The topological analysis is identical to an α level of infinity. With low values of α, node removal tends to cause larger cascading failures as the system has less spare carrying capacity; larger values of α tend to cause smaller cascades.

Line limits are caused by three main factors: thermal-limits, voltage drop, and steady state stability of frequency. In addition, certain line limits are imposed to prevent dynamic instability at a system level. These factors are all related to the line length and its voltage.[32] To keep the models similar to PL, we create a model that uses only the initial power flow on the line and a second model that uses initial power flow and the voltage, as voltage data are available in several open datasets.[33–35] The voltage power flow (volt PF) model has the form $y_i = \beta_0 1 + \beta_f x_{if} + \beta_v x_{iv}$, where y_i is the line limit of the ith power line to the log base 10, x_{if} is the initial power flow of the ith power line in megawatts, and x_{iv} represents the voltage level of line i. The coefficients are β_f and β_v, while β_0 is the model bias. The power-flow-only model (PF model) has the form $y_i = \beta_0 1 + \beta_f x_{if}$. The models are trained using 10-fold cross-validation, using ordinary least squares regression. Tenfold cross-validation is used as we only have access to the real line limits of a single power network. We train the model using 90% of the data and predict for the out of sample 10%; this will be repeated to predict for all parts of the network. The coefficients shown in this paper are the average across the ten folds. (For code details on model generation, see the section "Modeling Line Limits" of the GitHub code.[36]) These models will be compared to the PL approach throughout the paper. Ideally, we could use the models to predict the line limits of a separate network. However, we only have access to the real line limits of a single network. Since this is the case, we will use the line limits predicted in each of the validation sets as the predicted line limits for the attack simulation. The artificial line limits are compared to the real line limits using R^2, root mean square error (RMSE), and mean average percent error (MAPE).

The model we use is deterministic and based on the frequentest approach to statistics; this differs from the work of Kim and Motter[25] and Elyas and Wang[26] whose generative models use the Bayesian framework. The Bayesian approach to modeling can provide a better understanding of the range of possible results; however, it comes at the cost of greatly increased computation. In this paper, we do not seek to find an optimum line limit simulation model simply to create a statistical model to compare against PL. We use a simple linear model because it provides line limits that are based on a real system and are easily interpretable, with a low computational overhead.

B. Comparing attack damage between the PL approach and real line limits

We simulate the grid under attack by assigning a random-node attack rank to each network node. We then remove the node with Rank 1. Since node removal can cause overloading, we recalculate the power flow and remove any lines that exceed their maximum line limit. We then rebalance the power and load in the network. Line removal can cause the network to break into subcomponents; so, we remove any nodes that are in a subcomponent that has no power. We then recalculate power flow. This process continues until no further removals occur. We then find the node with the next lowest attack rank and remove it, repeating the process until no nodes remain in the network. The process is described in Algorithm 1 for graph G, the set of n nodes/vertices $\mathcal{V}$, and the set of m edges E. A schematic of the process is shown in Fig. 1.

During the attack simulation, two different damage metrics are used to analyze attack progression giant-component size, measured as the largest connected component, and blackout size, measured as total MW lost. These metrics are compared to the graph's original state using $\Delta P_x = \frac{P_1 - P_x}{P_1}$, where P_1 is the complete graph and P_x is the graph after attack x. This method of measuring damage returns a percentage between 0 (no damage) and 100 (complete grid collapse).

Algorithm 1 Attack the grid

procedure ATTACKTHEGRID(G)
  $\mathscr{V} \leftarrow V(G)$
  $E \leftarrow E(G)$
  while $\mathscr{V} \neq \emptyset$ **do**
    remove $\min_i(v_i)$ ▹ i is the order in which nodes will be attacked
    repeat
      calculate power flow in G
      for $e \in E$ **do**
        remove e if $f_e > f_e^{max}$ ▹ Power flow exceeds line limit
      end for
      rebalance generation and supply
      for $v \in \mathscr{V}$ **do**
        remove v if subgraph has no power
      end for
    until $f_e < f_e^{max}$ for all e
  end while
end procedure

Note that using the largest connected component as a measure might not be representative of the physical processes that occur on the power grid. For example, say we have a network that has 100 nodes but only two generators, where the first generator produces 99% of the electricity and the other generates the remaining 1%. If the big generator fails, the giant-component size is still 99%, thereby indicating that the network is almost unaffected even though there is only 1% of the necessary power. Despite this drawback, the metric's simplicity has made it a popular choice,[27,37–39] and, thus, it will be included here. Blackout size is a metric from the extended topology. It measures the loss of system power in megawatts. This metric is popular and has several different names with slightly different implementations that produce similar results. It has been called "loss of load,"[40] "blackout size,"[24] "load shed,"[41] "power supply,"[30] and "total loss of power,"[42] among other names. This metric does not suffer the problem described above regarding the size of the giant component.

C. Comparing the order in which edges are lost due to cascade

Accurately modeling the damage done in an attack provides substantial insight into a grid's vulnerability. Sometimes, however, it is also useful to know the order in which nodes or edges were lost, as this information is used in certain vulnerability metrics.[28,31,43] One caveat here, though, is that if the order of the nodes being lost differs depending on the line limits, the results of such analyses will not be reliable. In order to explore the robustness of loss order in relation to line limits, we correlate the order in which nodes are lost during an attack for artificial line limits with real line limits.

Tables II and III provide a toy example of how we compare node-loss order. First, k node-removal orders are generated. Then, all k simulations are run using each line-limit type. Table III shows Simulation 1 for the real line limits and a line limit of $\alpha = 3$. In the table, the bold numbers indicate a node that has been targeted for removal, while the other nodes are removed by the cascade. We find the similarity of network collapse by correlating the round lost of nodes that were lost to cascade. This implies we exclude nodes that were targeted for removal. As a result, in the example, only nodes F, G, and H can be compared.

For each of the k simulations, we use Spearman's correlation $\rho_k = \frac{\mathrm{cov}(\mathrm{rg}_{x,k}, \mathrm{rg}_{y,k})}{\sigma_{\mathrm{rg}_{x,k}} \sigma_{\mathrm{rg}_{y,k}}}$, where $\mathrm{rg}_{x,k}$ and $\mathrm{rg}_{y,k}$ are the rank of x_k and y_k, respectively, for the n nodes in the network, σ is the variance of the rank of the nodes, and cov() is the covariance of the rank of the nodes. In this case, x_k is the vector of the node-removal rounds of

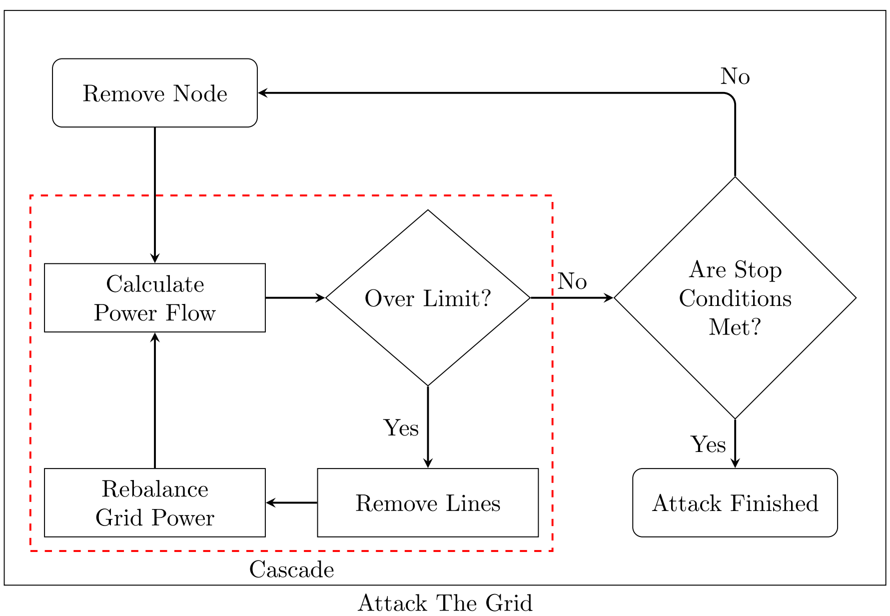

FIG. 1. Schematic of the node-removal process.

TABLE II. The node-removal orders are randomly generated k times.

Node ID	Sim 1	Sim 2	...	Sim k
A	1	4	...	3
B	2	2	...	8
C	3	1	...	7
D	4	6	...	6
E	5	5	...	1
F	6	7	...	2
G	7	8	...	5
H	8	3	...	4

TABLE III. The numbers indicate the round in which the node was lost in Simulation 1 for the real limits and $\alpha = 3$. Nodes that are shown bold were targeted for removal and so are not included when calculating removal similarity.

Node ID	Real limits	$\alpha = 3$
A	**1**	**1**
B	**2**	1
C	1	**2**
D	**3**	**3**
E	**4**	1
F	2	1
G	4	3
H	4	2

the artificial line limit for Simulation k and y_k is the vector of the node-removal round for the real line limits for Simulation k. In the example, this means $x_1 = 2, 4, 4$ and $y_1 = 1, 3, 2$, thereby yielding a correlation of 0.866.

For the real experiment, we generate 100 attack orders for the 512 nodes, producing 100 correlation scores per line limit method. This reveals the extent of similarity between the collapse order of the artificial line limits and that of the real line limits

D. Comparing vulnerability ranking accuracy

The choice of the attack strategy can have a substantial impact on results. Different strategies damage the network at different rates throughout the attack. When comparing attack strategies, it may be that only the relative performance is important. In this analysis, we compare the ability of different line-limit methods to accurately rank attack strategies. We compare five different attack strategies across eight α values, the modeled limits, and the topological limits. The α values used in this analysis are 1.05, 1.1,1.5, 2, 5, 10, 20, and 50.

The attack strategies we use in this analysis are a mixture of topological methods and extended topology. The strategies are entropic degree[10] using line limit, entropic degree using initial power flow, degree, centrality, and electrical centrality.[40] The centrality and degree attack strategies prioritize the most central nodes. Entropic degree using power flow and electrical centrality generally prioritize attacking the power sinks and the southern part of the UK. Entropic degree line-limit lies between the centrality and electrical centrality methods.

Using each attack strategy to define the node-removal order, we simulate an attack until we achieve complete grid collapse. After each attack round (node removed), we rank the strategies by total blackout size. The strategy that caused the most damage to the network is given

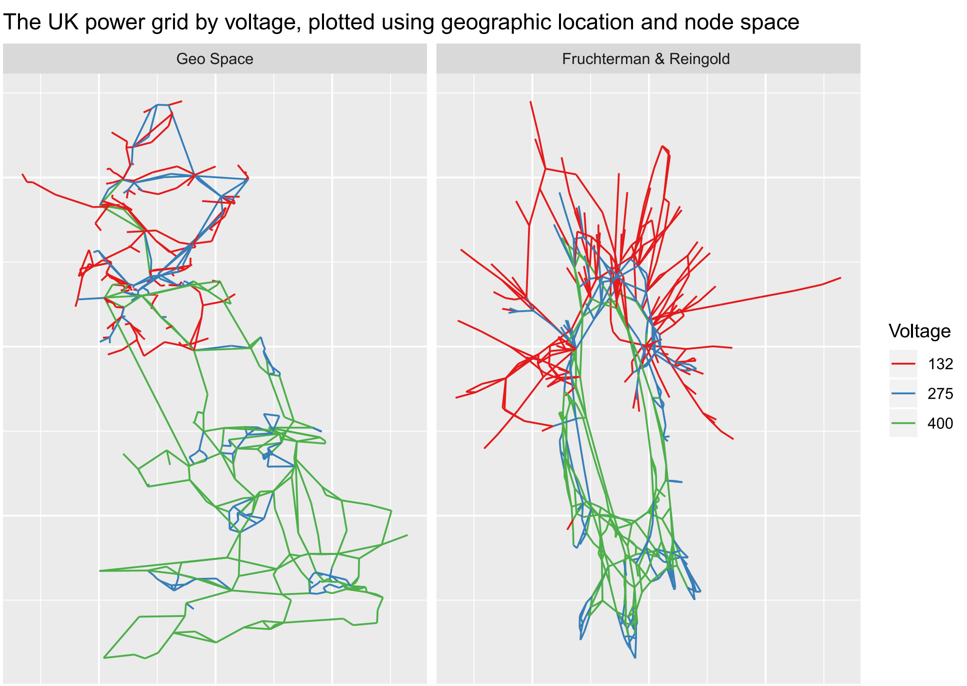

FIG. 2. UK power-grid voltage level shown in geographical space and graph space. The 132-V sections of the network are much less densely connected than the 275- and 400-V sections.

TABLE IV. Mean model coefficients from 10-fold cross-validation. Power flow and Voltage coefficients are in 1000 s. Model outputs are in a log base 10 scale.

	Coefficients	PF and Voltage model	PF model
1	Intercept	1.84	2.71
2	PF (MW)	0.21	0.76
3	Voltage (kV)	3.84	

TABLE V. Accuracy of modeling line limits.

	Model	R^2	RMSE	MAPE
1	Volt power flow	0.65	1026.00	0.45
2	Power flow	0.13	4446.96	1.07

Rank 1 and the strategy that caused the least damage is given Rank 5. We then compare the rankings obtained by each artificial limit with those obtained by the real line limits. Using RMSE, we evaluate which line-limit method has the lowest error relative to the real line limits.

III. RESULTS

The results are divided into two sections. The first section describes the results of the linear model used to generate line limits, and the second section compares the performance of different artificial line limits to the real line limits.

A. Modeling line limits

We first create a linear model that predicts line limits. The variables used are voltage and initial power flow. These variables create two models, the PF model (power flow model) and volt PF model (voltage power flow model). The network is represented in Fig. 2 and uses a UK geographical location and a graph space representation using force expansion. As we only have a single network, we use ten-fold cross-validation to train on 90% of the data and then predict using the remaining 10%. The model coefficients are all quite stable, with a proportionally small standard deviation. The coefficients were all positive across all folds. The volt PF model shows that as voltage increases so does the line limit. This is intuitive, as high-voltage cables are often used for bulk-power transmission (see Table IV).

B. Comparing the performance of different line limits

An inspection of the power-grid tolerance distribution under initial conditions shows that the system is not proportionally loaded. Figure 3 depicts the α distribution of the power grid under initial loading. The power grid has a mean of $\alpha = 5.12$ and a median of $\alpha = 6.12$. These tolerances are much higher than those used in the literature, which are typically less than two. We also compared the line capacity against line load and found a load capacity relationship similar to that found in Kim and Motter.[25] That pattern is $C - L \sim L^{\tau}$, where C is the capacity, L is the line load, and τ is the network exponential. This pattern persists when the data are broken out by voltage; further details can be found in supplementary material S2.

Correlating PL (proportional loading) limits with real limits yields an R^2 of 0.5. Using a range of α values, we find that the minimum MAPE (mean average percentage error) and RMSE (root mean

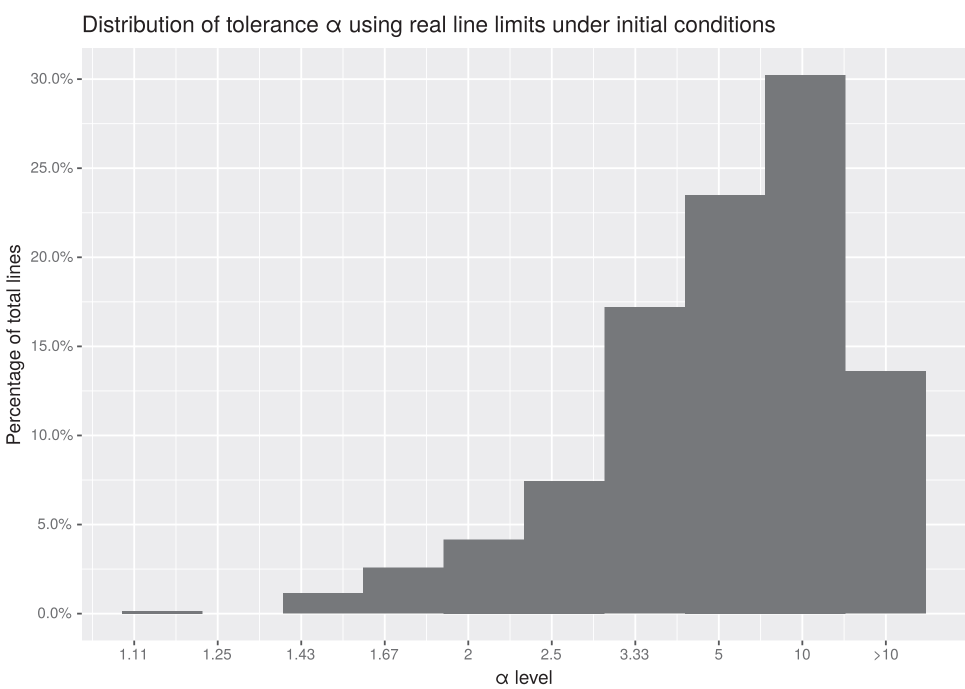

FIG. 3. The distribution of the loading is left-skewed with a mean α of 5.12.

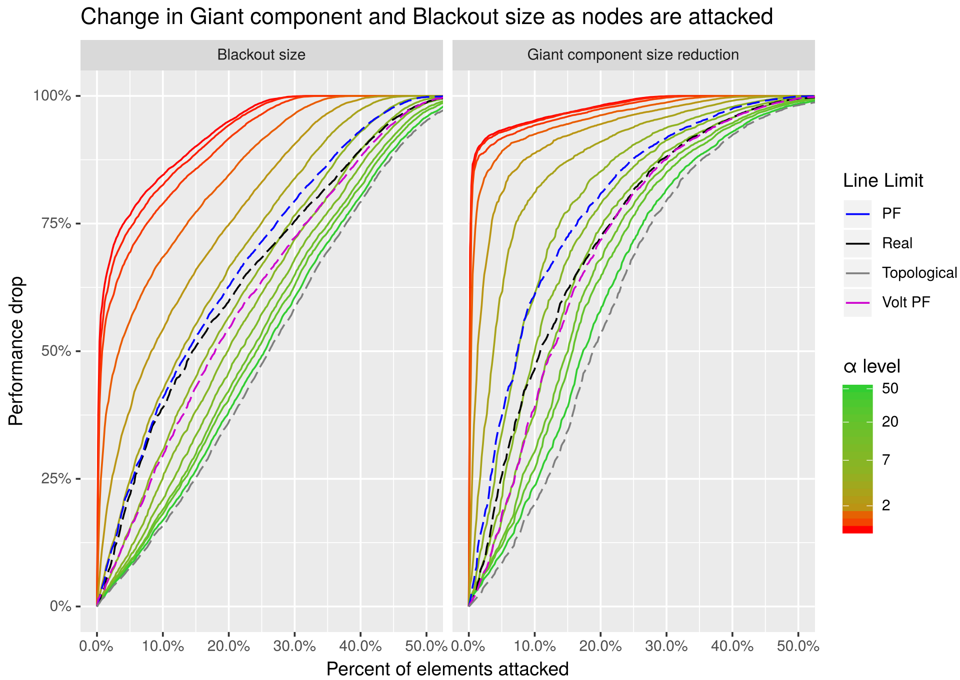

FIG. 4. Mean damage done in terms of giant-component and blackout size across 100 simulations, across all 13 α levels, and the linear models. There is a log relationship between α and damage done for a given number of elements attacked.

square error) are 0.52 and 1380 with α values of 3.6 and 3.5, respectively. The volt PF model greatly outperforms all PL models and the PF model (see Table V). The PF model has very poor performance across all three metrics, which shows that it is not an effective method to accurately represent line limits.

We explore the damage done during the random attack across different values of α. It is evident that α has a logarithmic relationship with the damage for a given number of attacks. Figure 4 illustrates that, for both damage metrics, the α levels only converge at grid collapse and do not cross each other before that.

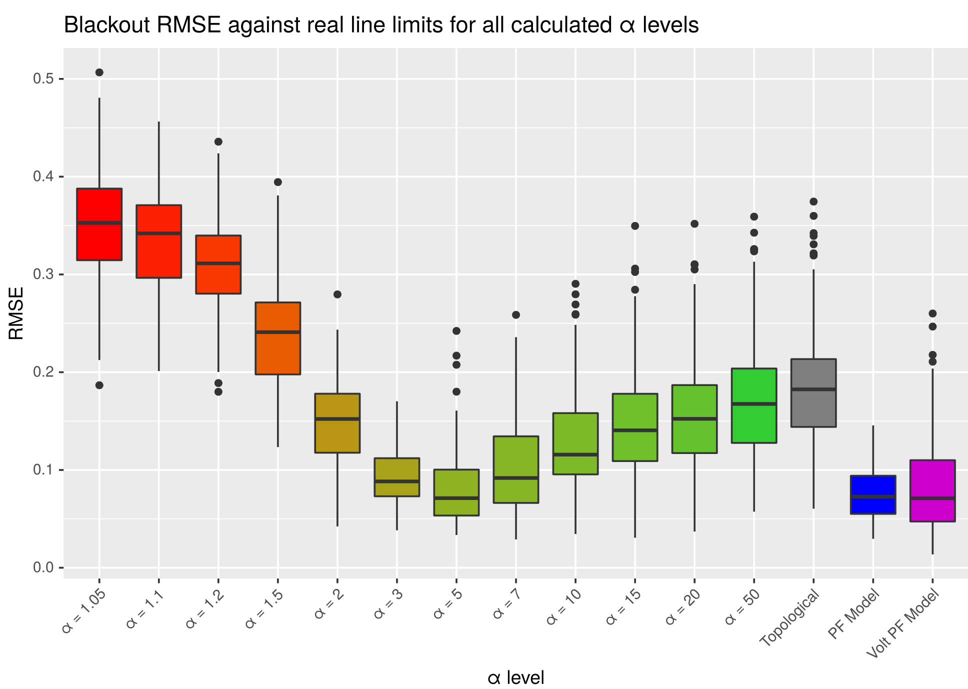

FIG. 5. The PF model has the lowest RMSE with the real limits. However, the volt PF model and $\alpha = 5$ follow closely.

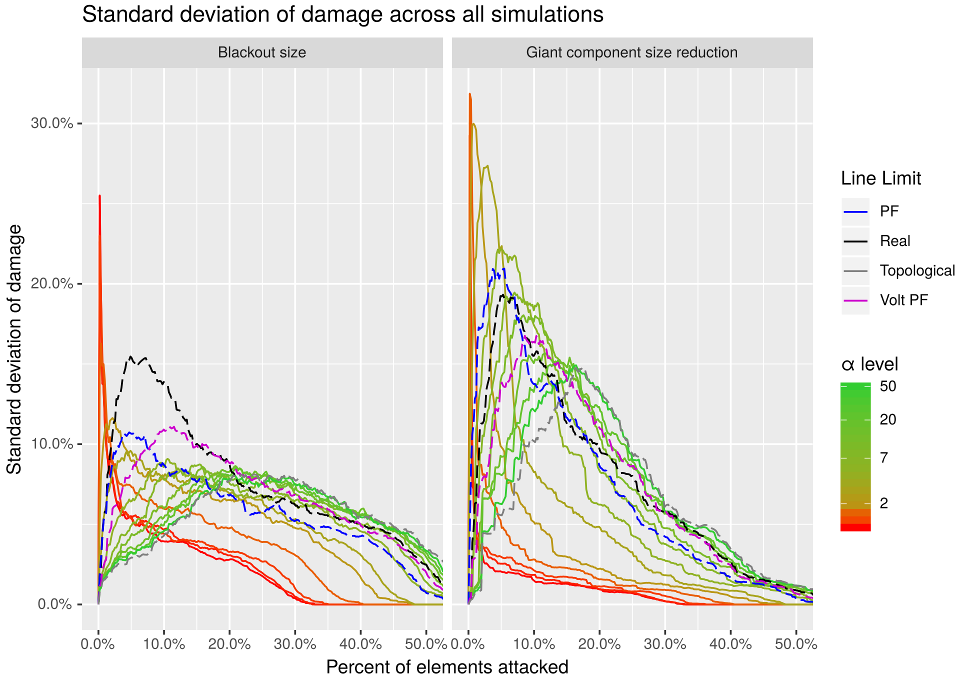

FIG. 6. The standard deviation of the attack damage across the 100 simulations.

Figure 5 shows that, despite its poor ability to accurately measure line limits, the PF model is the most accurate method of measuring blackout size, with an RSME of 0.077. The volt PF model performs slightly worse than the $\alpha = 5$ (the system mean) in terms of blackout size. These models have RMSE scores of 0.085 and 0.082, respectively.

For the giant component, the volt PF model is the best performer, with an RMSE error of 0.088. The volt PF model is

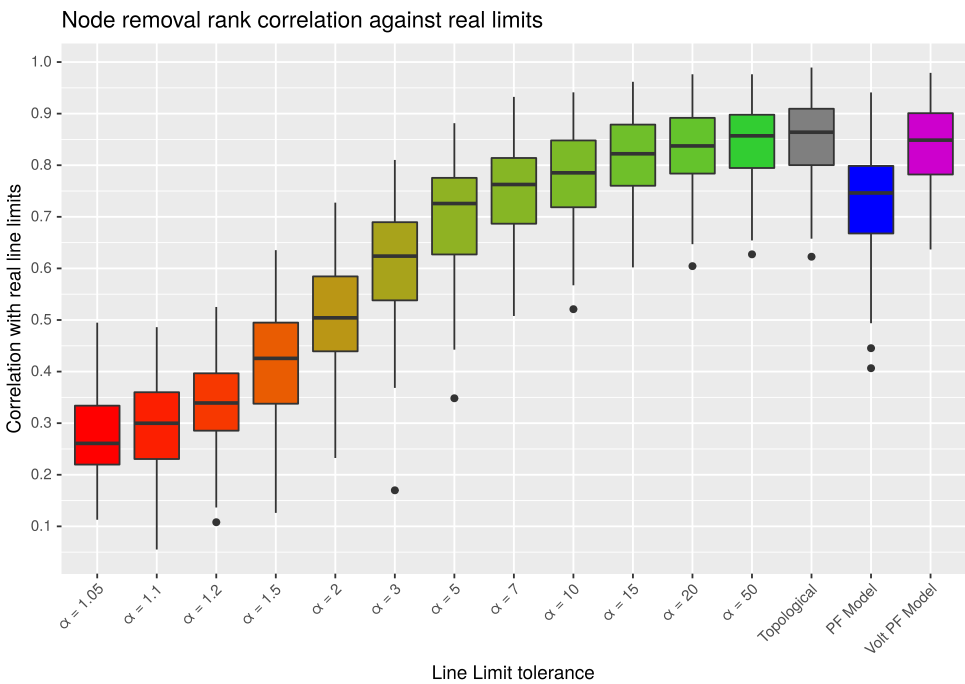

FIG. 7. The volt PF model has the highest correlation. Correlation of edge removal increases as α tends to infinity, which is identical to the topological analysis.

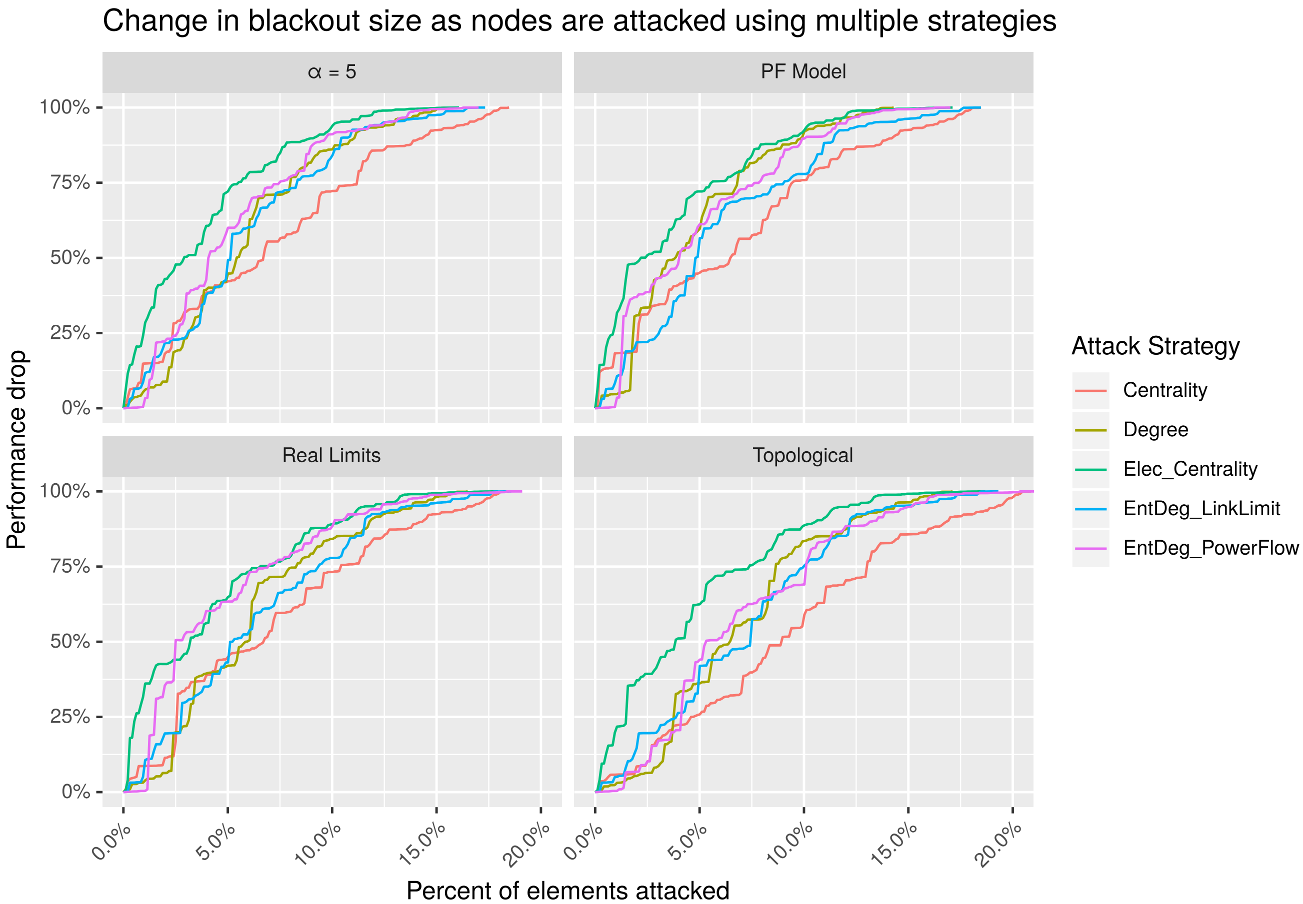

FIG. 8. The damage done to the power grid by each attack strategy by the percentage of the grid attacked. As can be seen, the strategy rank can change as a higher percentage of nodes is removed.

followed by $\alpha = 7$ and $\alpha = 10$, which have RMSE scores of 0.103 and 0.104, respectively. The PF model comes fourth with an RMSE score of 0.117.

The error relationship between blackout size and optimum α is intuitive, as it matches the average α of the real line limits. The reason for the giant-component optimum α is less apparent and may be linked to the topological structure. The linear models perform well in both cases.

Next, we compare the standard deviation of damage across all 100 simulations. The volt PF and the PF only models have very similar results with RMSE scores of 0.022 and 0.023, respectively. The accuracy of the linear models comes from the ability to represent the hump of the real limits shown in Fig. 6, something no value of α can replicate.

When examining the RMSE of the standard deviation of the damage of the giant component, we see that the volt PF model, the PF only model, and $\alpha = 7$ have similar scores, 0.018, 0.019 and 0.14, respectively.

We compare the correlation of the order of node loss between each artificial line limit and the real line limits. The correlation across all 100 simulations is shown in Fig. 7. The figure shows that, as α increases, the node-loss order similarity increases following a logarithmic growth curve with the topological analysis most similar to the real line limits. The topological analysis has a mean correlation of 0.853, more than three times as high as $\alpha = 1.05$, which has a mean of 0.277. The $\alpha = 50$ model narrowly outperforms the volt PF model, which have correlation scores of 0.847 and 0.842, respectively. The PF model has a significantly lower correlation score of 0.730.

Figure 8 shows plots of the damage caused by the five attack strategies in four of the ten line-limit scenarios. As can be seen, the rankings of the attack strategies change as the number of nodes removed increases. We analyze how well each line-limit method reflects the relative performance of the attack strategies. We find that the volt PF model (RMSE 0.638) comes out at the top, outperforming the $\alpha = 5$ (0.776), while the PF model (1.02) comes fifth, narrowly beaten by $\alpha = 2$ (0.971) and $\alpha = 10$ (0.987) (see Fig. 9). The values of α of 1.5 or less have a considerably greater error in ranking different attack strategies.

The fact that the low α values are much worse at ranking the performance of attack strategies is important, as the majority of PL

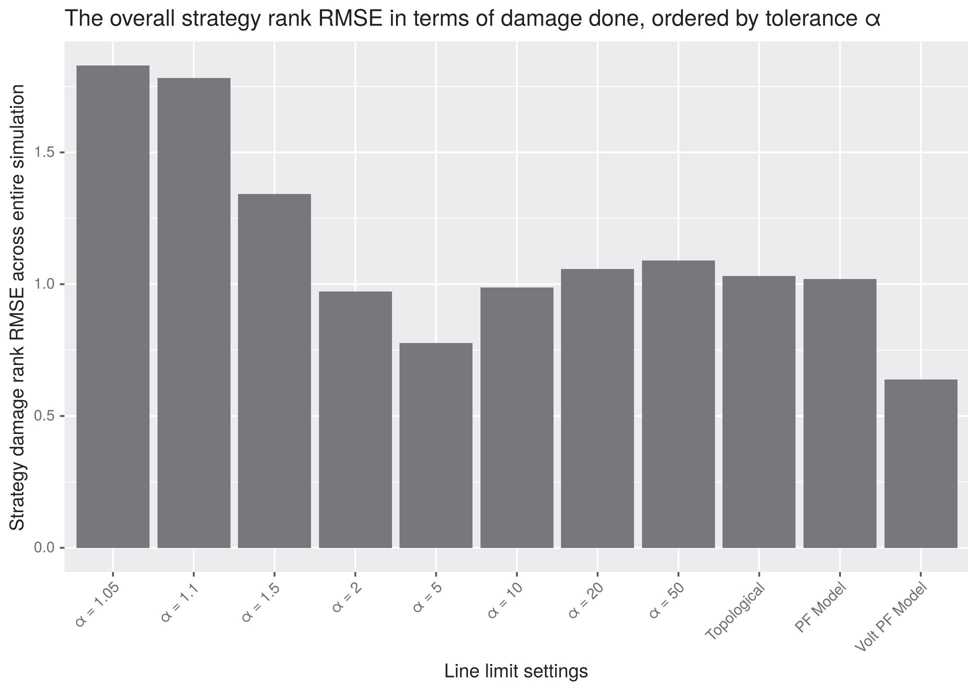

FIG. 9. The α values equal to or lower than two are particularly poor at ranking attack strategies.

papers use α values of less than five. One reason for this may be that the cascade size is bigger with lower α values.

An interesting finding is that in this specific case the change in α as the attack develops is minimized when the α is equal to the base case α of the system using the real line limits. Figure 10 shows a large drop in α during an attack, when the initial α of the system is much higher than the true system mean α of 5.1. In contrast, the load level $(\frac{1}{\alpha})$ shows a large drop, during an attack, when the initial α of the system is much lower than the true system α. When the initial α is set close to the true system α, the sum of the change in α and load level, $\Delta\text{Total} = \Delta\alpha + \Delta\frac{1}{\alpha}$, from initialization is minimized (see Fig. 11). This indicates that there may be a relationship between the position of an edge in the network topology and its line-limit, an idea related to Elyas and Wang.[26] Although no conclusions can be drawn from this single result, it is included as it may be of value to other researchers.

IV. DISCUSSION

This study found that using linear models to estimate power-grid line limits gives consistently high performance. The volt PF model (voltage and power flow model) performs very well across all tests, while the PF model (power flow only model) performs better than most α values but is not outstanding. We find that the optimum tolerance α is not consistent and changes depending on what is being measured. Although $\alpha = 5$, the value closest to the system mean of $\alpha = 5.12$ performed well; sometimes other α values, such as 7 or topological, provided the best performance in specific analyses. Results based on lower values of α may imply that the risk of cascading blackouts in some networks is greater than it actually is and provide a false indication of the robustness of power networks to cascading failure.

An interesting finding was that the ability of the linear model to measure line limits does not reflect the ability of the linear model to accurately represent power-grid collapse behavior. Although the volt PF model is much more accurate at estimating line limits, the PF is more accurate at modeling blackout size during grid collapse. This may be because the PF model makes large errors on edges that do not overload and smaller errors on edges that do. If a line is unlikely to overload, the limit is irrelevant. A complicating factor is that the PF model has relatively poor correlation with the order in which the nodes are lost. This result is probably related to the overloaded lines, of which the PF model has more on average than the volt PF model or the real line limits. Further research is needed to explore the relationship between modeling line limits and modeling collapse damage, particularly with regard to the importance of accurately identifying lines that may overload. Further details on model performance may be found in supplementary material S2.

A limitation of this paper is that it uses a static analysis of cascading failures. Work that uses transient analysis of cascading failures[15,17,18] can show networks to be more vulnerable than static analysis, as failures can occur due to synchronization issues. However, evidence suggests[18] that if this analysis was run using transient modeling, low values of α would be more affected. As such, we believe that the static nature of this analysis does not have a substantial outcome on the results.

In this paper, we explored how line limits affect the collapse behavior of the power grid using a single load profile which was the base case load profile. Ideally cascading failure research uses a range of load profiles, such as different time of day or season. Using different load profiles enables researchers to draw more generally applicable conclusions. However, this paper does not seek to find a solution to any possible weaknesses in the UK power grid topology

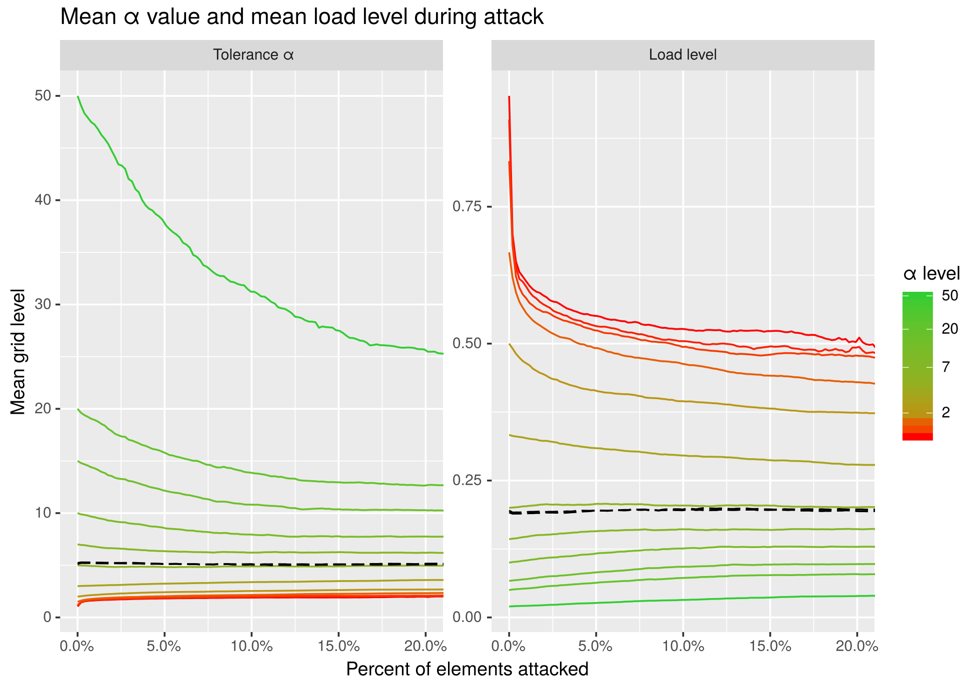

FIG. 10. When the PL value is much higher than the true system mean α, there will be a large drop in the observed α value as the attack develops. If the PL value is much lower than α, then there will be a drop in the $\frac{1}{\alpha}$ value as the attack develops. This indicates that there may be a link between the topology of the network and the edge line limit.

but instead to highlight the weaknesses of using proportional loading in power grid analysis. Consequently, the availability of only a single load profile is of less importance than it otherwise might have been, as we can demonstrate the weaknesses of α with only a single load profile.

Overall, we find that the line limits follow a simple linear model using voltage and initial power flow. Although the linear model has only been trained using a single load profile and only a single power network, it provides value as it is at a much more realistic system tolerance than arbitrarily selecting α because it uses the base load case

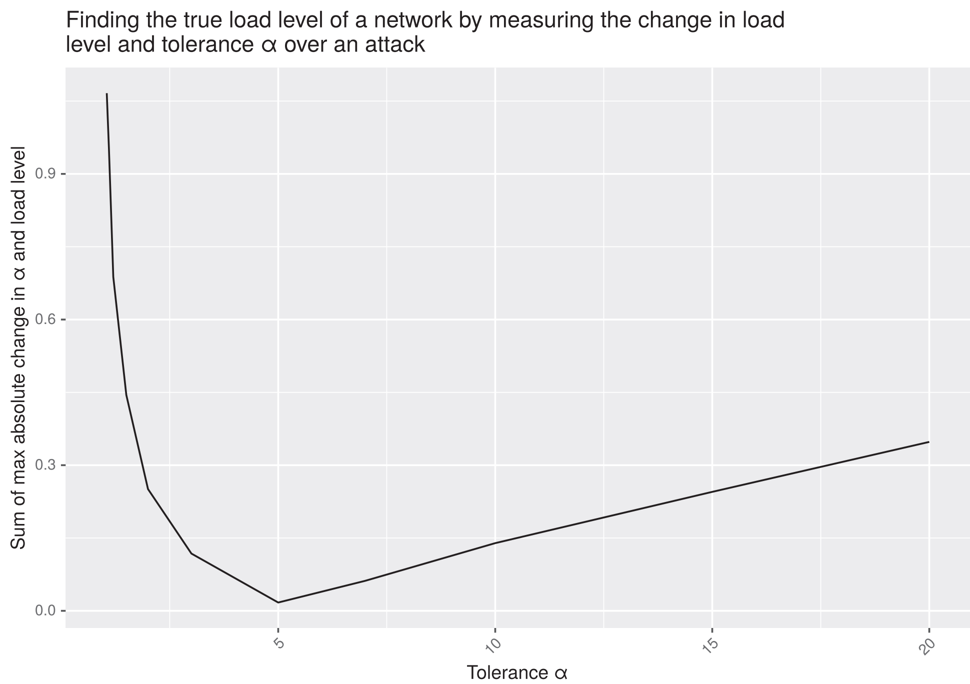

FIG. 11. By summing the absolute maximum difference in values for α and load level, we find that the minimum value is $\alpha = 5$, which is also the closest simulated value to the true mean α of 5.12.

for the UK grid. Moreover, the volt PF model uses the fact that higher voltage lines generally have more capacity to obtain information that is independent of the initial power flow state.

V. CONCLUSION

The title of this paper suggests that it is unwise to use artificial line limits when studying the collapse behavior of power grids under attack. In fact, given the importance of artificial line limits in this field, we merely propose that researchers must carefully consider how they set these artificial line limits. This is because, as we have shown, artificial line limits far from reality can produce results which themselves are far from reality and do not represent real-grid behavior. This study demonstrates the importance of using values based on real engineered systems rather than arbitrary representations when researching cascading failures on the power grid. In cases where researchers have no knowledge of the mean loading of the network and α will be selected arbitrarily, we recommend using the voltage power flow model developed in this study. Use of this linear model in conjunction with the network's base load profile will reduce the overall size of cascades (compared to a small value of α); however, the evidence presented in this paper suggests that the results of analyses using the model will be much more closely related to the real behavior of the grid.

SUPPLEMENTARY MATERIAL

This paper includes two additional sections in the form of supplementary materials S1 and S2. S1 provides more information on the PEARL analysis framework and acts as partial documentation for the associated R package. S2 provides a more in depth look at the performance of the models for researchers who are considering using them.

ACKNOWLEDGMENTS

This work was funded by the EPSRC International Doctoral Scholars - IDS grant (EP/N509577/1).

REFERENCES

[1] A. Walker, E. Cox, J. Loughhead, and J. Roberts, "Counting the cost: The economic and social costs of electricity shortfalls in the UK," Tech. Rep. (Royal Academy of Engineering, 2014).
[2] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," Renew. Sust. Energ. Rev. **80**, 9–22 (2017).
[3] BBC, "South America reels after massive outage," BBC News (2019).
[4] J. K. McGrath, "Will updated electricity infrastructure security protect the grid? A case study modeling electrical substation attacks," Infrastructures **3**, 53 (2018).
[5] C. Glenn, D. Sterbentz, and A. Wright, "Cyber threat and vulnerability analysis of the U.S. electric sector," Tech. Rep. INL/EXT-16-40692 [Idaho National Laboratory (INL), Idaho Falls, ID, 2016].
[6] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid table of contents," Tech. Rep. (E-ISAC, 2016).
[7] N. R. Council, *Terrorism and the Electric Power Delivery System* (National Academies Press, 2012).
[8] A. Cherepanov, "WIN32/INDUSTROYER: A new threat for industrial control systems," Tech. Rep. (ESET, 2017).
[9] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. Geem, "A critical review of robustness in power grids using complex networks concepts," Energies **8**, 9211–9265 (2015).
[10] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," Int. J. Crit. Infrastruct. Prot. **2**, 5–12 (2009).
[11] D. L. Pepyne, "Topology and cascading line outages in power grids," J. Syst. Sci. Syst. Eng. **16**, 202–221 (2007).
[12] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grids vulnerability: A complex network approach," Chaos **19**, 013119 (2009).
[13] D. Wu, F. Ma, M. Javadi, K. Thulasiraman, E. Bompard, and J. N. Jiang, "A study of the impacts of flow direction and electrical constraints on vulnerability assessment of power grid using electrical betweenness measures," Physica A **466**, 295–309 (2017).
[14] P. Hines and S. Blumsack, "A centrality measure for electrical networks," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, edited by R. Sprague, Jr. (IEEE, 2008), pp. 185–185.
[15] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," IEEE Trans. Power Syst. **30**, 285–297 (2015).
[16] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," Nature **464**, 1025–1028 (2010).
[17] R. Kinney, P. Crucitti, R. Albert, and V. Latora, "Modeling cascading failures in the North American power grid," Eur. Phys. J. B **46**, 101–107 (2005).
[18] B. Schäfer, D. Witthaut, M. Timme, and V. Latora, "Dynamically induced cascading failures in power grids," Nat. Commun. **9**, 1975 (2018).
[19] W. Jang and T. J. Overbye, "Equivalent line limit calculation using available thermal transfer capability," in *2017 IEEE Texas Power and Energy Conference (TPEC)* (IEEE, 2017), pp. 1–6.
[20] W. Jang, S. Mohapatra, T. J. Overbye, and H. Zhu, "Line limit preserving power system equivalent," in *2013 IEEE Power and Energy Conference at Illinois, PECI 2013* (IEEE, 2013), pp. 206–212.
[21] S. Mohapatra, W. Jang, and T. J. Overbye, "Equivalent line limit calculation for power system equivalent networks," IEEE Trans. Power Syst. **29**, 2338–2346 (2014).
[22] W. Medjroubi, U. P. Müller, M. Scharf, C. Matke, and D. Kleinhans, "Open data in power grid modelling: New approaches towards transparent grid models," Energy Rep. **3**, 14–21 (2017).
[23] A. B. Birchfield, T. Xu, and T. J. Overbye, "Power flow convergence and reactive power planning in the creation of large synthetic grids," IEEE Trans. Power Syst. **33**, 6667–6674 (2018).
[24] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?," Chaos **20**, 033122 (2010).
[25] D.-H. Kim and A. E. Motter, "Resource allocation pattern in infrastructure networks," J. Phys. A: Math. Theor. **41**, 224019 (2008).
[26] S. H. Elyas and Z. Wang, "Statistical analysis of transmission line capacities in electric power grids," in *2016 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (IEEE, 2016), pp. 1–5.
[27] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," Phys. Rev. E **66**, 065102(R) (2002).
[28] Y. Zhu, J. Yan, Y. Sun, and H. He, "Revealing cascading failure vulnerability in power grids using risk-graph," IEEE Trans. Parallel Distributed Syst. **25**, 3274–3284 (2014).
[29] Y. Koç, M. Warnier, P. V. Mieghem, R. E. Kooij, and F. M. Brazier, "The impact of the topology on cascading failures in a power grid model," Physica A **402**, 169–179 (2014).
[30] M. Ouyang, L. Zhao, Z. Pan, and L. Hong, "Comparisons of complex network based models and direct current power flow model to analyze power grid vulnerability under intentional attacks," Physica A **403**, 45–53 (2014).
[31] Y. Yang, T. Nishikawa, and A. E. Motter, "Vulnerability and cosusceptibility determine the size of network cascades," Phys. Rev. Lett. **118**, 048301 (2017).
[32] R. D. Dunlop, R. Gutman, and P. P. Marchenko, "Analytical development of loadability characteristics for EHV and UHV transmission lines," IEEE Trans. Power Apparatus Syst. **PAS-98**, 606–617 (1979).
[33] Entsoe-e, "Grid Map" (2019).
[34] J. Rivera, C. Goebel, D. Sardari, and H. A. Jacobsen, "Opengridmap: An open platform for inferring power grids with crowdsourced data," in *Lecture Notes in*

Computer Science, edited by S. Gottwalt, L. König, and H. Schmeck (Springer, Cham, 2015), Vol. 9424, pp. 179–191.
[35]OPenStreetMap Contributors: Planet Dump (2017), see https://planet.osm.org.
[36]J. Bourne, "ProportionalLoading" (2018).
[37]G. Andrea Pagani and M. Aiello, "Power grid complex network evolutions for the smart grid," Physica A **396**, 248–266 (2014).
[38]M. I. Rosas-Casals, S. Valverde, and R. V. So, "Topological vulnerability of the European power grid under errors and attacks," Int. J. Bifurcat. Chaos **17**, 2465–2475 (2007).
[39]G. A. Pagani and M. Aiello, "Towards decentralization: A topological investigation of the medium and low voltage grids," IEEE Trans. Smart Grid **2**, 538–547 (2011).
[40]K. Wang, B.-H. Zhang, Z. Zhang, X. Gen Yin, and B. Wang, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," Physica A **390**, 4692–4701 (2011).
[41]B. A. Carreras, D. E. Newman, and I. Dobson, "North American blackout time series statistics and implications for blackout risk," IEEE Trans. Power Syst. **31**, 4406–4414 (2016).
[42]C. Brancucci Martínez-Anido, R. Bolado, L. De Vries, G. Fulli, M. Vandenbergh, and M. Masera, "European power grid reliability indicators, what do they really tell?," Electric Power Syst. Res. **90**, 79–84 (2012).
[43]P. D. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," IEEE Trans. Power Syst. **32**, 958 (2017).