On the robustness of power systems: optimal load-capacity distributions and hardness of attacking

Evangelos Chatziafratis
Computer Science Department
Stanford University
Palo Alto, CA 94305
Email:vaggos@stanford.edu

Yingrui Zhang
Department of ECE
Carnegie Mellon University
Moffett Field, CA 94035
Email: yingruiz@andrew.cmu.edu

Osman Yağan
Department of ECE
Carnegie Mellon University
Moffett Field, CA 94035
Email: oyagan@ece.cmu.edu

***Abstract*— We consider a power system with N transmission lines whose initial loads (i.e., power flows) $L_1, \ldots, L_N$ and capacities $C_1, \ldots, C_N$ are independent and identically distributed with the joint distribution $P_{LC}(x, y) = \mathbb{P}[L \leq x, C \leq y]$; the capacity C_i defines the maximum flow allowed on line i. We survey some results on the robustness of this power system against random attacks (or, failures) that target a p-fraction of the lines, under a democratic fiber bundle-like model. Namely, when a line fails, the load it was carrying is redistributed equally among the remaining lines. We then consider the case where an adversary can launch a targeted attack, and present several results on the hardness of attacking optimally.**

I. Introduction

Electrical power systems have been an integral part of our daily lives for decades, and our quality of life largely depends on the continuous availability of an electrical power supply. This is expected to be further amplified in the near future due to the increasing market share of electric vehicles and increasing integration of major national infrastructures to the power grid; e.g., water, transport, communications, etc. All of these point to a future where the reliability of the power systems will be paramount with the central research question being how we can design a power system in a robust and reliable manner.

A major problem with the existing power systems is the seemingly unexpected large scale failures. Although rare, the sheer size of such failures has proven to be very costly, at times affecting hundreds of millions of people [15], [2]; e.g., the recent blackout in India [25], [20]. Such events are often attributed to a small initial shock getting escalated due to intricate dependencies within a power system [3], [22], [8]. This phenomenon, also known as cascade of failures, has the potential of collapsing an entire power system as well as other infrastructures that depend on the power grid [11], [7], [24]. Therefore, understanding the dynamics of failures in power systems and mitigating the potential risks are critical for the successful development and evolution of many critical infrastructures.

In this paper, we study the robustness of power systems under a simple model based on equal redistribution of load upon the failure of a power line. Namely, we consider a power system with N transmission lines with initial loads $L_1, \ldots, L_N$ and capacities $C_1, \ldots, C_N$. If a line fails (for any reason), its load is assumed to be redistributed equally among all lines that are *alive*. Thus, the load carried by a line i may exceed its initial value L_i over time due to load-redistribution. The capacity C_i defines the maximum flow allowed on the line i, meaning that if the load carried by i exceeds this capacity at any time, the line will be tripped (i.e., disconnected) by means of automatic protective equipments so as to avoid costly damages to the system. Subsequently, the load that was carried by line i before failure will be redistributed to remaining lines, which in turn may cause further failures, possibly leading to a *cascade* of failures.

It was recently suggested by Pahwa et al. [13] that equal load redistribution can be a reasonable assumption (in the mean-field sense) due to the long-range nature of Kirchhoff's law, especially under the DC power flow model; the DC model is known [12], [19] to approximate the AC model well in many cases. With these in mind, our main goal is to understand the robustness of power systems under the equal load redistribution model described above against *random* and *targeted* attacks. The former case was recently studied by Yağan [23] under the assumptions that initial loads $L_1, \ldots, L_N$ are independent and identically distributed with $P_L(x) = \mathbb{P}[L \leq x]$ and that capacities are given by

$$C_i = (1 + \alpha)L_i, \quad i = 1, \ldots, N,$$

where $\alpha > 0$ denotes the *tolerance factor*; in [23] all lines assumed to have the same tolerance factor. There, Yağan studied the robustness of the system against *random* attacks that target a p-fraction of the lines; system robustness was quantified by the *final* (i.e., steady-state) fraction $n_\infty(p)$ of *non-failed* lines. Among other results, it was shown that the system robustness, is maximized if all lines are given the same initial load, for a given fixed mean load value $\mathbb{E}[L]$.

Recently, Zhang and Yağan [26] extended the results in [23] to the more general case where lines can have varying tolerance parameters. Namely, they let

$$C_i = L_i + S_i, \quad i = 1, \ldots, N,$$

with S_i denoting the free-space (or, redundancy) available at line i; under this setting, the tolerance factor is given

by $\alpha_i = S_i/L_i$ and may vary from one line to another. Under the assumption that load-'free space' pairs (L_i, S_i) are independent and identically distributed with the joint distribution $P_{LS}(x, y) = \mathbb{P}[L \leq x, S \leq y]$, they studied again the robustness of the system against random attacks that target a p-fraction of the lines. Their main result is that, with the mean values $\mathbb{E}[L]$ and $\mathbb{E}[S]$ are fixed, the robustness metric $n_\infty(p)$ is uniformly maximized for all p values if all nodes are given the same free space $\mathbb{E}[S]$, regardless of how the loads are distributed. More precisely, they showed under the enforced constraints that $n_\infty(p)$ is maximized if

$$P_{LS}(x, y) = P_L(x)\mathbf{1}[y \leq \mathbb{E}[S]],$$

where the choice of $P_L(x)$ is arbitrary. This leads to the counterintuitive conclusion that that lines with higher initial load shall be assigned smaller tolerance factors to maximize robustness.

With the case of random attacks being relatively well-understood, we shift our attention in this paper to the case of *targeted* attacks. As before, the main goal would be to derive design strategies (in the form of optimal load-'free space' distributions) that would lead to maximum robustness, this time against a knowledgable adversary attacking to a carefully selected set of lines. However, for this optimization problem to be well-defined one has to have a good understanding of the problem from an adversary's perspective. With this in mind, this paper aims to reveal *good* attack strategies that lead to maximal damage to the system for a given number of lines that can be attacked.

Formally, we consider the following optimization problem. Given N lines with loads $L_1, \ldots, L_N$ and free spaces $S_1, \ldots, S_N$, we seek to find the optimal set A of k lines that the adversary should attack in order to minimize the final fraction $n_\infty(A)$ of alive lines. We provide optimal solutions via greedy algorithms in three special cases: i) when all lines have the same load; ii) when $S_i = \alpha L_i$ for each $i = 1, \ldots, N$ (as considered in [23]); and iii) when all lines have the same free space, i.e., when $S_1 = \cdots = S_N$. The last case is of particular interest as it is known to lead to maximum robustness against random attacks. Then, we consider a variation of the problem with an additional constraint on the total load of the lines attacked; i.e., when the adversary is further constrained with $\sum_{i \in A} L_i \leq Q$ for some Q. We show that this variation of the optimal attack problem is in fact NP-Complete, meaning that no polynomial-time algorithm can find the optimal set A that minimizes $n_\infty(A)$, unless $P \equiv NP$. Our proof is based on a polynomial time reduction to the *k-Subset Sum* problem, i.e., to the problem that seeks to find whether a sequence of integers has a subset of size k whose sum equals Q.

The rest of the paper is organized as follows: We describe the system model in details in Section II. In Section III, we give a detailed survey of the recent results by Zhang and Yağan [26] concerning the robustness of power systems against random attacks. These results characterize the robustness of the power system under any load-'free space' distributions and any attack size p, explain the *order* (i.e., first vs. second) under which the system undergoes a complete breakdown, and show the distributions that lead to maximum robustness. Then, we consider targeted attacks and start our discussion on optimal attack strategies in Section IV. There, we start by demonstrating why certain greedy algorithms fail to give the optimal solution in general. Then, in Section V we consider some special cases of interest where greedy algorithms are shown to find optimal attack sets. Finally, in Section VI we prove a hardness result showing that a variation of the optimal attack problem is NP-Complete.

We close with a word on notation in use. The random variables (rvs) under consideration are all defined on the same probability space $(\Omega, \mathcal{F}, \mathbb{P})$. Probabilistic statements are made with respect to this probability measure $\mathbb{P}$, and we denote the corresponding expectation operator by $\mathbb{E}$. The indicator function of an event E is denoted by $\mathbf{1}[E]$. For a discrete set A we write $|A|$ for its cardinality.

II. System Model

We consider a power system with N transmission lines $\mathcal{L}_1, \ldots, \mathcal{L}_N$ with initial loads (i.e., power flows) $L_1, \ldots, L_N$. The *capacity* C_i of a line $\mathcal{L}_i$ defines the maximum power flow that it can sustain, and is given by

$$C_i = L_i + S_i, \qquad i = 1, \ldots, N, \tag{1}$$

where S_i denotes the *free-space* (or, redundancy) available to line $\mathcal{L}_i$. The capacity of a line is typically set [10], [21], [9], [4] to be a fixed factor of the line's original load, i.e.,

$$C_i = (1 + \alpha_i)L_i$$

with $\alpha_i > 0$ defining the *tolerance* parameter for line $\mathcal{L}_i$. Put differently, the free space S_i is often given in terms of the initial load L_i with $S_i = \alpha L_i$. It is assumed that a line *fails* (i.e., outages) if its load exceeds its capacity at any given time. In that case, the load it was carrying before the failure is redistributed *equally* among all remaining lines.

Throughout we assume that the pairs (L_i, S_i) are independently and identically distributed with $P_{LS}(x, y) := \mathbb{P}[L \leq x, S \leq y]$ for each line $i = 1, \ldots, N$. The corresponding probability density function is given by $p_{LS}(x, y) = \frac{\partial^2}{\partial x \partial y} P_{LS}(x, y)$. Let L_{min} and S_{min} denote the minimum values for load L and free space S; i.e.,

$$L_{min} = \inf\{x : P_L(x) > 0\}$$
$$S_{min} = \inf\{y : P_S(y) > 0\}$$

We assume that $L_{min}, S_{min} > 0$. We also assume that the marginal densities $p_L(x)$ and $p_S(y)$ are continuous on their support.

Our main goal is to characterize the robustness of this power system against i) *random* attacks that result initially with a failure of a (randomly selected) p-fraction of the lines; or *targeted* attacks that initially fail a specific set A of lines. The initial set of failures leads to redistribution of power flows from the failed lines to *alive* ones (i.e., non-failed lines), so that the load on each alive line becomes equal to its initial

load plus its equal share of the total load of the failed lines. This may lead to the failure of some additional lines due to the updated flow exceeding their capacity. This process may continue recursively, generating a *cascade of failures*, with each failure further increasing the load on the alive lines, and may eventually result with the collapse of the entire system.

Throughout, we let $n_\infty(p)$ denote the *final* fraction of alive lines when a p-fraction of lines is randomly attacked. The robustness of a power system will be evaluated by the behavior of $n_\infty(p)$ as the attack size p increases, and particularly by the critical attack size $p^\star$ at which $n_\infty(p)$ drops to zero. In the case where a specific set A of lines are attacked, we define $n_\infty(A)$ as the final fraction of alive lines. Throughout we will seek to derive *optimal* attack strategies, i.e., to find the set A of lines that minimizes $n_\infty(A)$ under certain constraints; e.g., the size $|A|$ being fixed.

The equal redistribution model described above is inspired by the democratic fiber bundle model [1], [6], where N parallel fibers with random failure thresholds $C_1, \ldots, C_N$ (i.e., capacities) drawn independently from $P_C(x)$ share equally an applied total force of F; see also [5], [18], [14], [17]. This model has been recently adopted by Pahwa et al. in the context of power systems with F corresponding to the total load that N power lines share equally.

The problem formulation considered here was introduced by Yağan [23] and Zhang and Yağan [26]. This formulation differs from the original democratic fiber-bundle model in that i) it does not assume that the total load of the system is fixed at F; and ii) it allows for power lines to carry different initial loads. In addition, [13] is concerned with failures in the power system that are triggered by increasing the total force (i.e., load) applied. Instead, our formulation allows analyzing the robustness of the system against external attacks or random line failures, which are known to be the source of system-wide blackouts in many interdependent systems [16], [3], [24]. In addition, unlike the democratic fiber bundle model where all lines start with the same initial load, power lines in real systems are likely to have different loads at the initial set-up although they may participate equally in taking over the load of those lines that have failed.

III. Defender's Perspective: A Survey of Existing Results [23], [26] on Optimization of Robustness

We now survey existing results obtained by Yağan [23] and Zhang and Yağan [26] on the robustness of power systems under equal redistribution of loads. These works are interested in the problem from a defender's perspective and provide means to characterize, improve, and optimize the robustness of the system, assuming in most cases that the adversary will launch a *random* attack to a certain fraction of lines. With the randomness involved in the attack model, as well as load-capacity values, both [23] and [26] rely on *mean-field* analysis and aim to characterize the *mean* (or, average) performance of the underlying systems in the asymptotic regime where N approaches infinity.

A. Final system size as a function the attack size

The first main result in [26] characterizes the robustness of power systems under any distribution of initial load L and free space S, and any attack size p.

Theorem 3.1 ([26]): Let L and S denote generic random variables following the same distribution with initial loads $L_1, \ldots, L_N$, and free space $S_1, \ldots, S_N$, respectively. Then, with $x^\star$ denoting the smallest solution of

$$\mathbb{P}\left[S > x\right]\left(x + \mathbb{E}\left[L \mid S > x\right]\right) \geq \frac{\mathbb{E}\left[L\right]}{1-p}. \tag{2}$$

over the range the $x^\star \in (0, \infty]$, the final system size $n_\infty(p)$ is given by

$$n_\infty(p) = (1-p)\mathbb{P}\left[S > x^\star\right]. \tag{3}$$

For a graphical solution of $n_\infty(p)$, one shall plot $\mathbb{P}\left[S > x\right]\left(x + \mathbb{E}\left[L \mid S > x\right]\right)$ as a function of x (e.g., see Figure 1(a)), and draw a horizontal line at the height $\mathbb{E}\left[L\right]/(1-p)$ on the same plot. The leftmost intersection of these two lines gives the operating point $x^\star$, from which we can compute $n_\infty(p) = (1-p)\mathbb{P}\left[S > x^\star\right]$. When there is no intersection, we set $x^\star = \infty$ and understand that $n_\infty(p) = 0$.

B. The "Critical" Attack Size

In many practical cases, one would be interested in the variation of $n_\infty(p)$ as a function of p. This would help understand the response of the system to attacks of varying magnitude. Of particular interest will be to derive the critical attack size $p^\star$ such that for any attack with size $p > p^\star$, the system undergoes a complete breakdown leading to $n_\infty(p) = 0$. The next result specifies this critical attack size for arbitrary system parameters.

Theorem 3.2 ([26]): The maximum attack size $p^\star$ is related to the global *maximum of the function $\mathbb{P}\left[S > x\right]\left(x + \mathbb{E}\left[L \mid S > x\right]\right)$. In particular, we have*

$$p^\star = 1 - \frac{\mathbb{E}\left[L\right]}{\max_x\{\mathbb{P}\left[S > x\right]\left(x + \mathbb{E}\left[L \mid S > x\right]\right)\}}. \tag{4}$$

C. No-cascade Condition

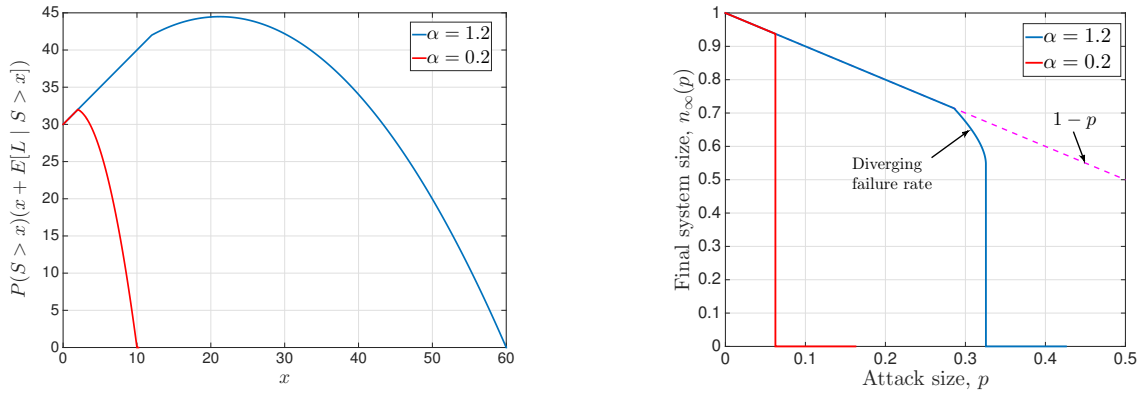
For extremely critical power systems it is desirable to characterize the "no-cascade" condition under which the final system size equals $1 - p$, when p-fraction of the lines are taken down by an attacker. In other words, it would be useful to obtain conditions such that no single line fails other than the pN lines that went down as a result of the initial attack. The next result provides exactly that.

Theorem 3.3 ([26]): For any attack size p, the no-cascade condition is given by

$$S_{min} > \frac{p\mathbb{E}\left[L\right]}{1-p}. \tag{5}$$

where S_{min} denotes the minimum free space that a line can have in the system.

This result establishes (5) as the *condition for no cascade of failures*, which can be of significant use in capacity provisioning, i.e., in determining the line capacities needed for robustness against p-size attacks.



(a) (b)

Fig. 1. *We demonstrate the distinction between an abrupt first-order rupture, and a first-order rupture that is preceded by a diverging failure rate.* $p_L(x)$ *is assumed to be of uniform density over the range* $[L_{min}, L_{max}] = [10, 50]$*, and we assume that the free space of a line is given by* $S_i = \alpha L_i$ *for some* $\alpha > 0$*; i.e., the joint density is given by* $p_{LS}(x, y) = p_L(x)\delta(y - x\alpha)$ *where* $\delta(\cdot)$ *denotes the Dirac-delta function. In both plots, red (lower) curves stand for the case where* $\alpha = 0.2$*, whereas blue (upper) curves represent* $\alpha = 1.2$*. Figure 1(a) shows* $\mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])$*, whereas Figure 1(b) plots the corresponding variation of* $n_\infty(p)$ *with attack size* p*. We observe that for* $\alpha = 0.2$ *(Red),* $\mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])$ *takes its maximum at the point* $x = S_{min} = 2$*. As a result, we see an abrupt first-order transition of* $n_\infty(p)$ *as it suddenly drops to zero at the point* $p = p^\star = 0.0625$*, while decaying linearly as* $1 - p$ *up until that point. The case where* $\alpha = 1.2$ *is clearly different as* $\mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])$ *is now maximized at* $x = 21.1 > 12 = S_{min}$*. As expected from our discussion, this ensures that the total failure of the system occurs after a diverging failure rate is observed. This divergence is clearly seen in Figure 1(b) where the dashed line corresponds to the* $1 - p$ *curve.*

D. Understanding the "Phase Transition": Rupture Condition

It is of significant interest to understand the behavior of the system near the *phase transition*; i.e., when the attack size is very close to but smaller than the critical value $p^\star$. One main questions here is whether $n_\infty(p)$ decays to zero continuously (i.e., through a second-order transition), or discontinuously (i.e., through a first-order transition). The practical significance of this is that continuous transitions suggest a more stable and predictable system behavior with respect to attacks, whereas with discontinuous transitions, system behavior becomes more difficult to predict based on past data.

The next result shows that the total breakdown of the system for the model considered here will always be through a first-order (i.e., discontinuous) transition.

Theorem 3.4 ([26]): Under the enforced assumptions, the system always undergoes a first-order *(i.e., discontinuous) transition at the point* $p^\star$*; i.e., we have*

$$n_\infty(p^{\star^-}) > 0,$$

while by definition it holds that

$$n_\infty(p^{\star^+}) = 0;$$

here $p^{\star^\pm} = p^\star \pm \epsilon$ *with* $\epsilon > 0$ *arbitrarily small.*

An interesting question is whether this first order rupture at the point $p^\star$ will have any early indicators at smaller attack sizes; e.g., a *diverging* failure rate leading to a non-linear decrease in $n_\infty(p)$. An *abrupt* first-order transition is said to take place if the linear decay of $n_\infty(p)$ is followed by a sudden discontinuous jump to zero at the point $p^\star$. Those cases are reminiscent of the real-world phenomena of unexpected large-scale system collapses; i.e., cases where seemingly identical attacks/failures leading to entirely different consequences. A distinction is demonstrated in Figure 1.

The result provides conditions for an abrupt rupture to take place.

Theorem 3.5 ([26]): For the system to go through an abrupt first order breakdown (e.g., see the below line shown in red in Figure 1(b)) the function, we must have

$$\arg\max_{x>0} \{\mathbb{P}[S > x](x + \mathbb{E}[L \mid S > x])\} = S_{min}$$

E. Achieving Optimal *Robustness*

Perhaps the most important question from a defender's perspective is concerned with deriving the *universally optimum* distribution of initial loads $L_1, \ldots L_N$ and free spaces $S_1, \ldots, S_N$ when the mean values $\mathbb{E}[L]$ and $\mathbb{E}[S]$, respectively, are fixed. For the time being, we consider the maximization of robustness against random attacks or failures as our optimality criterion, where maximization of robustness is defined as the maximization of the critical attack size $p^\star$. Later, we shall check whether maximizing $p^\star$ also maximizes the entire robustness curve $n_\infty(p)$ vs. p. Zhang and Yağan obtained [26] the answer to this important question, and the corresponding result is presented next; see also [23] for a similar result when $S_i = \alpha L_i$ for all $i = 1, \ldots, N$.

Theorem 3.6 ([26]): For any initial load distribution, it holds that

$$p^\star \leq \frac{\mathbb{E}[S]}{\mathbb{E}[S] + \mathbb{E}[L]} = \frac{\mathbb{E}[S]}{\mathbb{E}[C]}. \tag{6}$$

In words, this result states that the critical attack size can never be larger than the ratio of mean free space (or, redundancy) and mean capacity. In addition, the *optimal* robustness given at (6) can be achieved by a *Dirac* delta distribution of free space, regardless of how loads are distributed. More

precisely, let $p^\star_{\text{dirac}}$ denote the critical attack size when $S_1 = \cdots = S_N = \mathbb{E}[S]$. We have

$$p^\star_{\text{dirac}} = \frac{\mathbb{E}[S]}{\mathbb{E}[S] + \mathbb{E}[L]}.$$

Thus far, we have seen that the equal distribution of free space leads to the largest possible critical attack size, hereafter denoted $p^\star_{\text{opt}}$. It is clear that the final system size after an attack of size p is always less than $1-p$. With this in mind, the next result establishes the optimality of the Dirac-delta distribution of free-space in the sense of maximizing the robustness of power systems *uniformly* over all attack sizes.

Theorem 3.7 ([26]): With Dirac-delta distribution of initial free spaces, the breakdown of the system is always through an abrupt first order rupture. Namely, with $S_1 = S_2 = \cdots = S_N$ we have

$$n_\infty(p) = \begin{cases} 1-p & \text{for } p < p^\star_{opt} \\ 0 & \text{for } p \geq p^\star_{opt} \end{cases}$$

Hence, the Dirac-delta distribution maximizes $n_\infty(p)$ *over the entire range* $0 \leq p \leq 1$.

These findings suggest that under the democratic fiber bundle-like model considered here, power systems with homogenous distribution of redundant space are significantly more robust against random attacks and failures, as compared to systems with heterogeneous distribution of redundancy. Interestingly, this suggests that the optimal robustness is achieved when the tolerance factor $\alpha_i = S_i/L_i$ decreases with increasing load, leading to the counterintuitive conclusion that the lines carrying the highest load should have the smallest tolerance factor to achieve maximum robustness.

IV. Attacker's Perspective: Optimal Attack Strategies

A. The Main Optimization Problem: ER-k

The Equal Redistribution (ER) problem with k attacks is the problem in which we are interested in finding a set A of k lines such that attacking A leads to the maximum number of total line failures (as a result of load redistribution and cascading failures), among all possible attack sets with size k. Put differently, we seek to find A with $|A| = k$ such that $n_\infty(A)$ is minimized. This problem is now stated formally.

INPUT: A list of n pairs of non-negative rational numbers in the form (L_i, C_i) indicating the load and the capacity of each line, an integer $0 < k \leq n$, an integer $0 < k' \leq n$ and a rational number L. We suppose $C_i > L_i$ so that no line fails initially at its own load.

OUTPUT: We are interested in knowing whether or not there is an attack set A with size exactly k, and total sum of loads $\sum_{i\in A} L_i \leq L$, so that at the end of the cascading failures the number of failed nodes is at least k'.

B. Greedy Algorithms that Fail

Here we will present three intuitive greedy algorithms and give concrete examples demonstrating their poor performance for the optimization problem described above. In doing so, we will focus on the special case where $k' = N$ meaning that the goal of the attack is to destroy the whole system.

In what follows, we often find it useful to view the problem as a fun game, where we have N water containers with capacities $C_1, \ldots, C_N$, and initial water levels $L_1, \ldots, L_N$. As in the democratic fiber-bundle model, when a container is "attacked" its content is redistributed equally to the remaining containers. Also, if the water level in a container exceeds its capacity, we assume that it has failed and redistribute its content, again equally, to the remaining containers.

An important observation is that the following greedy algorithms do not work and actually can deviate significantly from the optimal solution.

a) Attacking the container with greatest load: This strategy aims to maximize the load that we will redistribute in each attack round by maximizing the nominator L_0 of $L_0/(n-1)$. This strategy is not optimal in general because it fails to recognize the opportunity to eliminate containers with very large capacities that will otherwise be difficult to fail by redistributing the load. The worst-case deviation from the optimal (in terms of the number of lines need to be attacked for whole system failure) is $\Theta(n)$; e.g., see Figure 2.

b) Attacking the container with greatest capacity: This strategy attacks the container that has the maximum capacity in each round. The idea here is that by taking out large containers, the remaining, supposedly small, containers will be destroyed due to load redistribution. This strategy is not in general optimal either, because there may be containers with *large* capacities but small (or, even almost zero) loads, rendering an attack to such containers very ineffective in terms of triggering failures by means of load redistribution. The worst-case deviation from the optimal is again $\Theta(n)$ as demonstrated in Figure 3.

c) Attacking the container with largest free space (i.e., $(capacity - load)$ difference): It is clear from the previous two cases that the optimal attack strategy will be one that considers both the loads and capacities of the containers involved. The greedy approach that targets containers with largest free space (i.e., $(capacity - load)$ difference) falls into this category, and is based on the fact that containers with largest free space will fail the *latest* in the course of a cascading failure; e.g., see Section IV-C for a discussion of this fact. Therefore, it is sensible to eliminate those containers with a direct attack. On the other hand, containers with small free space are already on the verge of failing and therefore can be taken down of by means of redistribution of loads. Although this greed strategy is sensible (and in fact optimal in some special cases), it fails to be the optimal solution in general. The main reason is that this approach does not take into account the loads of the containers directly. For example, a container may have a large $(capacity - load)$ difference but it may be the case that its load is negligible comparably to the other containers' capacities, making it ineffective to attack it. The worst-case deviation from the optimal is $\Theta(n)$ (attacked: n versus optimal: 1) as demonstrated in Figure 4.

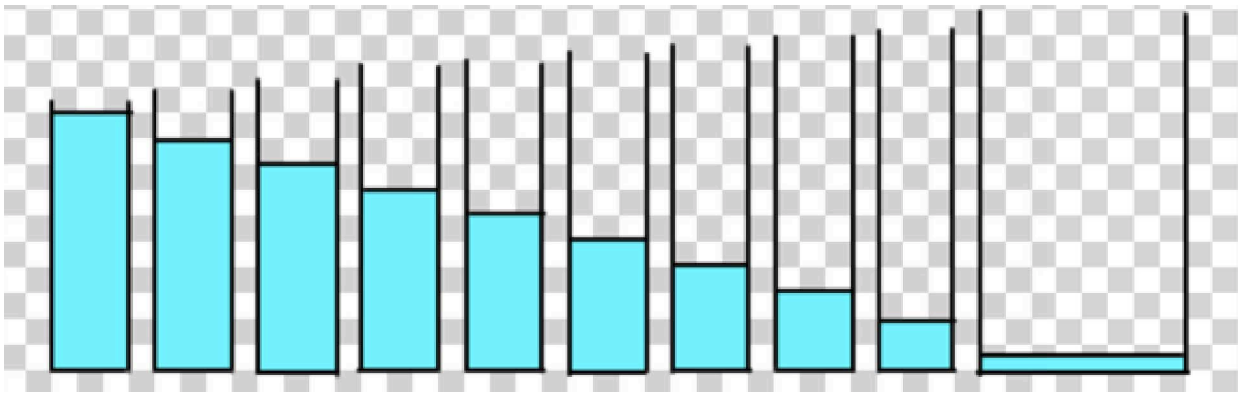


Fig. 2. *In this example (for the greedy maximum-load attack) we have (load, capacity) values given by* $(10, 10+1/10), (9, 9+10/9+\epsilon), (8, 8+19/8+\epsilon), (7, 7+27/7+\epsilon), (6, 6+34/6+\epsilon), (5, 5+40/5+\epsilon), (4, 4+45/4+\epsilon), (3, 3+49/3+\epsilon), (2, 52/2+\epsilon), (1, 1+54/1+\epsilon)$ *where* $\epsilon > 0$ *is arbitrarily small. The greedy will output* $k = 10$ *since it will start attacking the first/leftmost container with load* $L_1 = 10$ *and no cascading failures will happen and then it will continue towards the right. The optimal solution is* $k = 1$ *by attacking the last container because then the cascading failures will take place (the first container will then fail since it will have* $L_1 > C_1$*), thus destroying the whole system. We can generalize this counterexample to the case with* n *containers with the greedy algorithm's output being* $k = n$ *while the optimal solution being* $k = 1$.

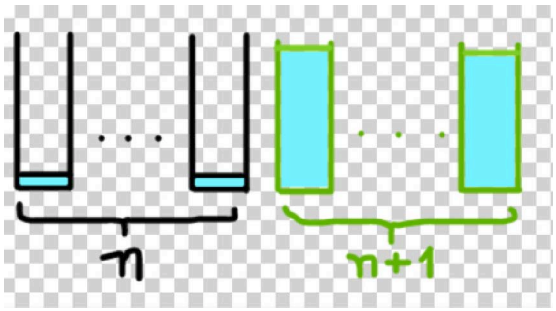


Fig. 3. *In this example (to the max capacity attack) we have* $2n+1$ *containers where (load, capacity) values are given by* (ϵ, M) *for the first* n *containers and* $(M-2\epsilon, M-\epsilon)$ *for the last* $n+1$ *containers; here* $\epsilon > 0$ *is arbitrarily small. The greedy approach will output* $k = n+1$ *since it will start attacking the first* n *containers with the highest capacity, but no cascading failures will take place until a container that has slightly less capacity but is almost full is attacked; at that point all containers will fail. On the other hand, the optimal solution is* $k = 1$ *as it takes to attack only one of the containers with* $(M-2\epsilon, M-\epsilon)$ *to trigger a cascading failure that will overfill the small containers along with the big but empty containers.*

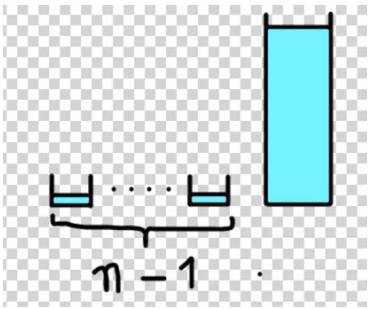


Fig. 4. *In this example (to the max* $(capacity - load)$ *attack) we have* n *containers with (load, capacity) values* $(\epsilon, (n+1)\epsilon)$ *for the first* $n-1$ *containers and* $(M, M+(n-1)\epsilon)$ *for the last container, where* $\epsilon > 0$ *is arbitrarily small and* M *satisfies* $M > (n^2-n)\epsilon$*. The greedy will output* $k = n$ *since it will start attacking the leftmost containers first and no cascading failures will happen and then it will continue towards the right. The algorithm must destroy all the containers in order for the system to break down. The optimal solution is obviously* $k = 1$ *by attacking the last container.*

C. Observations towards Designing a Smart Algorithm

We now present three main observations that shall be useful in designing a smart algorithm to the aforementioned optimization problem.

a) Order of failures during the cascading process: Assume that containers are sorted by increasing free space, $Z_i = (C_i - L_i)$. Given that any failed load is redistributed *equally* among the remaining containers, it is clear that this ordering will remain the same throughout the course of cascading failures; the containers that are attacked directly at the beginning are excluded from this discussion. Therefore, in the process of recursive load redistribution, containers will fail (due to their free space diminishing to (below) zero) in this exact same order; the one with smallest free space will fail first, and so on and so forth.

b) A sufficient (but not necessary) condition to destroy the system: Let $\mathcal{C}$ denote the set of all containers and A denote those that are attacked; i.e., A is the set of containers our algorithm chooses at the beginning to destroy. We observe that a sufficient condition to achieve our goal of destroying the whole system is the following: $\sum_{i\in A} L_i \geq \sum_{i\in\mathcal{C}\setminus A}(C_i - L_i)$. This means that the total load of the containers we are currently attacking exceeds the sum of the empty spaces of the remaining containers, and hence all containers will fail after redistribution of the failed loads (though, not necessarily simultaneously).

This condition can be seen to be *not* necessary for the whole system to fail. What is instead necessary is that $\sum_{i\in A'(t)} L_i \geq \sum_{i\in\mathcal{C}\setminus A'(t)}(C_i - L_i)$ should hold *at some point* $t = 0, 1, \ldots$ during the cascade of failures. Here, we define $A'(t)$ as the set of all containers that have failed until stage $t = 0, 1, \ldots$ of the cascade of failures. More precisely, we have $A'(0) = A$, and

$$A'(t) = A'(t-1) \cup \left\{ j : C_j - L_j < \frac{\sum_{i\in A'(t-1)} L_i}{|\mathcal{C}| - |\mathcal{A}'(t-1)|} \right\},$$

for each $t = 1, 2, \ldots$. Therefore, it is possible to start with a small number of containers attacked, and by recursive redistribution and failures, ultimately reach a point where the aforementioned condition is satisfied.

With these in mind, we find it useful to refer to the attack projection of a set of containers A as $proj(A)$, defined as the set of the attacked containers union the containers that will be destroyed after all cascading failures have stopped. Our main problem then reduces to finding a seed set A such that $proj(A) = \mathcal{C}$. The attack projection is calculated step by step by Algorithm 1.

c) The order of attack does not matter: In the equal redistribution scheme the order with which we launch our attack will not affect the final set of failed containers. This is because the load of the attacked nodes will be distributed to all of the remaining nodes so at the end an amount of $\sum_{i \in A} L_i$ will end up in the remaining containers (leading to new failures or not) irrespective of the order we chose to attack the containers in A.

V. Greedy Algorithms that Succeed

We now consider some special cases of the ER-k problem and provide greedy algorithms that yield the *optimal* attack strategies in these special cases. To aid this discussion, we describe two algorithms below, namely the ER-Attack Projection algorithm that finds the impact an attack set A has, and the Max-X (X=Load or Capacity) Greedy Algorithm for Special Cases that attacks the container with maximum X value first.

Algorithm 1 ER-Attack Projection $proj(A)$

Require: Input is sorted according to FreeSpace: $Z_i = L_i - C_i$ for the $binarySearch$
Require: $binarySearch$ returns all containers with free space less than extra_load
procedure $proj$(A)
  new_set= A
  repeat
    previous _set = new_set
    extra_load = $\sum_{i \in previous\_set} L_i$ / $(n - |previous\_set|)$
    new_set= $binarySearch$(extra_load)$\cup$previous_set
  until new_set = previous_set
  Return new_set
end procedure

A. Same Loads

An interesting situation arises when initial loads are the same for all containers while capacities differ. This reflects situations in which all lines in the power system are given the same initial load, but have different capacities owing to the physical constraints or material used. We show that a greedy algorithm finds the optimal solution in this special case. The ER-k-Same Loads Problem is defined formally as follows.

Algorithm 2 Max-X (X=Load or Capacity) Greedy for Special Cases

Require: Input is sorted according to Loads
procedure max-X GREEDY(k)
  repeat
    Attack=arg**max**(X_i)
    Failed=$proj$(attack)$\cup$Failed
    Input=Input$\backslash$Failed ▷ we discard the failures
    $k = k - 1$
  until $k = 0$ or |failed|$= n$
end procedure

INPUT: A non-negative rational number L for the common load and a list of n non-negative rational numbers C_i indicating the capacity of each line. We suppose $C_i > L, \forall i$, so that no line fails initially at its own load. The integer k represents the number of attacks we can launch.

OUTPUT: The maximum damage we can give to the system with the k available attacks; i.e., the maximum number of lines that can be failed in total (initial attack plus cascading failures).

In the above scenario the algorithm that we call $max - C$-Greedy finds the optimal solution. We give the proof to the following theorem:

Theorem 5.8: The max-C-Greedy Algorithm is optimal for the ER-k-Same Loads Problem.

Proof: A key observation is that since the failed load is always redistributed *equally* among *alive* lines, this system will preserve the "equal load" property through the cascading failures. Namely, at any stage the load of a line that is functioning will be given by $L(1 + \frac{M}{N-M})$ where M is the number of failed lines (out of a total N lines) thus far. In addition the sequence of attacks doesn't affect the final state of the system as discussed before. Therefore, the claim would follow for general attack sizes k, if we establish it for $k = 1$. This is because after a single line is attacked, the system will again be one with equal loads and the optimization problem will repeat itself with $k - 1$ additional lines to be attacked. Continuing in this manner, we see that the optimal attack strategy in this case would be a combination of *optimal* single-line attacks launched sequentially.

Assume now that $k = 1$, i.e., the goal is to attack the line that will lead to the maximum damage (i.e., number of failed lines) to the system. Since all loads are equal, the lines that fail as a result of this attack will be (with A_0 denoting the line chosen)

$$\{A_0\} \cup \{\ell \in \{1, 2, \ldots, N\}/A_0 : C_\ell \leq LN/(N-1)\} \quad (7)$$

The goal is then to find A_0 that maximizes the cardinality of this set, namely $|proj(A_0)|$. Let $\mathcal{L}_i$ and $\mathcal{L}_j$ be arbitrary distinct lines. From (7) we have

$$|proj(\mathcal{L}_i)| - |proj(\mathcal{L}_j)| = \mathbf{1}\left[C_j \leq LN/(N-1)\right] - \mathbf{1}\left[C_i \leq LN/(N-1)\right]$$

which automatically gives

$$|proj(\mathcal{L}_i)| \geq |proj(\mathcal{L}_j)| \quad \text{if} \quad C_i \geq C_j. \tag{8}$$

Since i and j are arbitrary, this shows that

$$\arg\max_{i=1,\ldots,N} |proj(\mathcal{L}_i)| = \arg\max_{i=1,\ldots,N} C_i.$$

In other words, the total number of failed lines $|proj(\mathcal{L}_i)|$ is maximized by attacking the line $\mathcal{L}_i$ with the maximum capacity. ∎

B. Same Free Spaces

Sometimes it might be the case that the containers have arbitrary load and capacity but they have a fixed free space. In [26], this was in fact shown to be the optimal design that gives maximum robustness against random attacks. We refer to the corresponding problem as the ER-k-Same Free Spaces and give a greedy algorithm that finds the optimal solution. The formal definition of the problem is as follows.

INPUT: A list of n non-negative rational numbers L_i indicating the load of each advertiser and a positive rational number Z indicating the common free space.

OUTPUT: Find out which is the minimum number k of attacks in order to destroy the system.

We changed the output here from having a fixed number of lines to be attacked to inflict the maximum damage, to the case where we aim to destroy the whole system with the minimum number of attacks. This is because in the case where every container has the same free space, there are no intermediate cascading failures. In all cases, the system will either fail completely, or no single line will fail other than those attacked directly. We now show that the $max-L$-Greedy algorithm that targets lines with the largest loads finds the optimal solution.

Theorem 5.9: The max-L-Greedy Algorithm is optimal for the ER-k-Same Loads Problem.

Proof: As in the case of the previous Theorem, the key here is to observe that the optimization problem can be reduced to finding the optimal single-line attack, and repeating this recursively. Again, the reason is that since failed load is equally redistributed, the system will maintain to have the same free space (among all alive lines) throughout the cascade process. Given also that the order of the attack does not matter, it remains to find the optimal single-line attack, i.e., the case where $k = 1$. Similar to (7), we have

$$proj(A_0) = \{A_0\} \cup \{\ell \in \{1, 2, \ldots, N\}/A_0 : Z_\ell \leq L_{A_0}/N\}$$

where A_0 is the line that is attacked. Since all lines have equal free space Z, this gives

$$|proj(A_0)| = N\mathbf{1}\left[Z \leq L_{A_0}/N\right].$$

It is now clear that $|proj(A_0)|$, i.e., the total number of lines failed by attacking A_0, is monotone increasing in the load L_{A_0} of A_0. Therefore, $|proj(A_0)|$ is maximized by attacking the line with the maximum load. Repeating this argument recursively, we see that in ER-k-Same Free Spaces, the optimal strategy is to attack lines with largest loads. ∎

C. Capacities Proportional to Loads

In many cases, the capacities and the loads of power lines are related in a particular way. Namely, the capacity of a line is often set to be proportional to its load. For example with $\alpha > 0$ denoting the *tolerance factor*, we have $C_i = (1+\alpha)L_i$ for each line $i = 1, \ldots, N$. In this variation, we will also show that there is a greedy algorithm achieving the optimal solution. The ER-k-$(C \propto L)$ Problem is defined formally as follows.

INPUT: A list of n non-negative rational numbers L_i indicating the load of each line and a positive rational number α as the tolerance parameter.

OUTPUT: The maximum damage we can cause to the system with the k available attacks, that is which nodes to attack to destroy the maximum number of nodes in total.

In the above scenario the $max - L$-Greedy algorithm that targets the lines with the largest loads gives the optimal solution.

Theorem 5.10: The max-L-Greedy Algorithm is optimal for the ER-k-$(C \propto L)$ Problem.

Proof: The key observation about the ER-k-$(C \propto L)$ Problem is that, given $C_i = (1+\alpha)L_i$, the load, capacity, and free spaces of lines all follow the same order. Namely, the lines with the largest loads, whom are tempting to attack to shed more load on others, are also the ones with the largest free spaces, whom are also tempting to attack given the difficulty of failing them by load redistribution. This eliminates the trade-off faced in the optimal attack problem and simplifies it greatly.

In this setting, the problem does not repeat itself as cascading failures take place since after load redistribution, it may no longer be the case that all lines have the same tolerance factor (i.e., the ratio of free space to load). However, the aforementioned key property will be maintained throughout. For instance, assume without loss of generality that initial loads are ordered as $L_1 \leq L_2 \leq \cdots \leq L_N$. Then, at any stage of the cascading failures, L_i, C_i, and Z_i will all be in increasing order for all $i = 1, 2, \ldots, N$ that are still alive.

With these in mind, we will first show the optimality of max-L-Greedy Algorithm for single line attacks in any system whose loads $L_1, L_2, \ldots, L_N$ and free spaces $Z_1, \ldots, Z_N$ follow the same ordering. Since this property will be preserved throughout the cascades and the sequence of attacks doesn't affect the final state of the system, the proof of Theorem 5.10 will be completed.

We now consider the case of $k = 1$, i.e., the case where a single-line A_0 is to be attacked to maximize the number $|proj(A_0)|$ of failed lines. This time, we have

$$proj(A_0) = \{A_0\} \cup \{\ell \in \{1, 2, \ldots, N\}/A_0 : Z_\ell \leq L_{A_0}/N\}$$

With $\mathcal{L}_i$ and $\mathcal{L}_j$ denoting arbitrary distinct lines we have

$$|proj(\mathcal{L}_i)| - |proj(\mathcal{L}_j)| = \sum_{\ell \in \{1,\ldots,N\}/\{i,j\}} (\mathbf{1}[Z_\ell \le L_i/N] - \mathbf{1}[Z_\ell \le L_j/N]) + \mathbf{1}[Z_j \le L_i/N] - \mathbf{1}[Z_i \le L_j/N]$$

Now, if $L_i \ge L_j$, we clearly have

$$\mathbf{1}[Z_\ell \le L_i/N] - \mathbf{1}[Z_\ell \le L_j/N] \ge 0, \;\; \ell \in \{1,\ldots,N\}/\{i,j\}.$$

Since $Z_i = \alpha L_i$ in the ER-k-($C \propto L$) Problem, $L_i \ge L_j$ also implies $Z_i \ge Z_j$. Together, these inequalities also give

$$\mathbf{1}[Z_j \le L_i/N] - \mathbf{1}[Z_i \le L_j/N] \ge 0.$$

Combining, we find

$$|proj(\mathcal{L}_i)| \ge |proj(\mathcal{L}_j)| \quad \text{if} \quad L_i \ge L_j,$$

and this establishes the optimality of attacking the line with the highest load in any setting where loads and free spaces follow the same ordering. Given that this ordering will prevail through the cascade process, we establish the optimality of the max-L-Greedy Algorithm. ∎

VI. Hardness Reductions

In this Section, we will prove that a variation of the ER-k Problem is NP-Complete. In particular, we consider the ER-k-k'-$\min \sum L$ problem, defined formally as follows.

INPUT: A list of n pairs of non-negative rational numbers in the form (L_i, C_i) indicating the load and the capacity of each line, an integer $0 < k \le n$, an integer $0 < k' \le n$ and a rational number L. We suppose $C_i > L_i$ so that no line fails initially at its own load.

OUTPUT: We are interested in knowing whether or not there is an attack set A with size exactly k, and total sum of loads $\sum_{i \in A} L_i \le L$, so that at the end of the cascading failures the number of failed nodes is at least k'.

It is clear that the objective is two-fold here and that there is an inherent tradeoff: by attacking lines with larger initial loads we can shed more load on other lines and have a better chance to trigger a cascade of failures that would destroy the whole system. However, the optimization problem requires minimizing the total load of the attacked containers. This *knapsack-like* tradeoff is what makes the problem NP-complete as we now show. Our proof is based on the reduction of the ER-k-$\min \sum L$ problem to the *k-Subset Sum* variant defined as follows: *Given a set of integers and a target sum Q, is there any subset of size k whose sum is Q?*

Theorem 6.11: The ER-k-$\min \sum L$ Problem is NP-Complete.

Proof: First, we show that ER-k-k'-$\min \sum L$ Problem is in NP: The certificate is a list of the k containers we need to attack. We can check in polynomial time (see the ER-Attack Projection algorithm) whether all lines in the system fail or not. Since we have a certificate that can be checked in polynomial time, ER-k-k'-$\min \sum$QL is in NP!

Given an instance of the k-Subset Sum problem we will create an instance of the ER-k-k'-$\min \sum L$ problem: Given a set of N integers $a_1, a_2, ..., a_N$, the k-Subset Sum problem asks whether there exists k members of the set whose some equals Q. If $k = N$, we can check if $\sum_{i=1}^{N} a_i = Q$ and respond accordingly. From now on, we suppose $k < N$ and create an equivalent version of the ER-k-k'-$\min \sum L$ problem in the following manner. Let lines $\mathcal{L}_1, \ldots, \mathcal{L}_N$ have loads $L_1 = a_1, L_2 = a_2, ..., L_n = a_N$ and consider the ER-k-N-Q problem; i.e., we seek to find a set A of k lines such that $\sum_{i \in A} L_i \le Q$ and that attacking A leads to failure of all N lines in the system. We also set $C_i = L_i + S_i$ where the free space is $S_i = \frac{Q}{N-k}$ for each $i = 1, \ldots, N$. This last constraint ensures two things. First, as discussed in Section V-B, when all lines have the same free space then attacking k lines can only have two consequences: either only those k lines that are attacked fail, or all N lines fail. In either case, there is no *cascade* of failures and the system reaches a steady-state immediately. Thus, with equal free space among all lines, the ER-k-k'-Q problem with $k' > k$ is equivalent to ER-k-N-Q problem. Secondly, under the enforced assumptions it is clear that a complete system failure will take place if and only if the total load failed by the initial attack A is larger than the sum of the free spaces of those that are not in the attack set A; i.e., if and only if

$$\sum_{i \in A} L_i \ge \sum_{j \in \{1,\ldots,N\}/A} S_j = (N-k)\frac{Q}{N-k} = Q.$$

Here, the first equality follows from the facts that $|A| = k$ and $S_i = \frac{Q}{N-k}$ for each $i = 1, \ldots, N$. Recalling that ER-k-N-Q problem seeks to find A such that $\sum_{i \in A} L_i \le Q$, this leads to $\sum_{i \in A} L_i = Q$. Therefore, the created instance of the ER-k-N-Q problem indeed seeks to find a subset A of $\{a_1, \ldots, a_N\}$ such that $|A| = k$ and $\sum_{i \in A} L_i = Q$, rendering it equivalent to the k-Subset Sum instance that we have started with. For the reverse direction, assume that the ER-k-N-Q problem has a solution with k lines $\mathcal{L}^{(1)}, \ldots, \mathcal{L}^{(k)}$. Then the loads of these lines constitute a solution to the k-Subset-Sum problem.

The above reduction can be constructed in polynomial time (linear time to be exact), so if there was a polynomial algorithm that could solve the ER-k-k'-$\min \sum L$, then the k-Subset Sum would be in P, which is wrong unless P=NP. Thus, we conclude that the ER-k-k'-$\min \sum L$ Problem is NP-complete. ∎

VII. Conclusion

In this paper, we seek to develop a framework towards mitigating cascading failures that cause large-scale blackouts in electrical power systems. We consider an equal load-redistribution based cascading failure model, and study it from i) a designer's perspective that aims to achieve optimal robustness under system constraints; and ii) an attacker's perspective that seeks to fail as many lines as possible by attacking a given number of lines. For the former case, we survey several results from [23] and [26] concerning the final system size as a function of the size of *random* attacks, the critical attack size

above which the system breakdowns completely, and optimal load-capacity distributions that maximize robustness. In the latter case, we study the constrained optimization problem of finding k initial lines to be attacked to minimize the final number of alive lines in the system. We give optimal greedy algorithms in several special cases, and prove that a variation of the problem (with a bound on the total load of the initial attack set) is NP-Complete.

There are several interesting directions one might consider for future work. First of all, the complexity of the optimal k-line attack problem (without a bound on the total load of those attacked) is still unknown. Also, given that even polynomial algorithms may be prohibitively complex in practical applications, it would be interesting to design *heuristic* attack strategies that give close-to-optimal solutions. Last but not least, with the results of this paper shedding some light on *good* attack strategies, one might turn to the defender's side and seek optimal design strategies of the power system (e.g., in the form of load-capacity distributions) against the *targeted* attacks developed here.

ACKNOWLEDGMENT

This research was supported in part by the National Science Foundation through grant CCF #1422165, and in part by the Department of Electrical and Computer Engineering at Carnegie Mellon University. O. Yağan also acknowledges the Berkman Faculty Development Grant from Carnegie Mellon. This work was done when E. Chatziafratis was at the National Technical University of Athens.

REFERENCES

[1] J. V. Andersen, D. Sornette, and K.-t. Leung. Tricritical behavior in rupture induced by disorder. *Phys. Rev. Lett.*, 78:2140–2143, Mar 1997.

[2] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, et al. Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *Power Systems, IEEE Transactions on*, 20(4):1922–1928, 2005.

[3] 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.

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

[5] R. da Silveira. Comment on "tricritical behavior in rupture induced by disorder". *Phys. Rev. Lett.*, 80:3157–3157, Apr 1998.

[6] H. Daniels. The statistical theory of the strength of bundles of threads. i. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, 183(995):405–435, 1945.

[7] I. Dobson, B. A. Carreras, V. E. Lynch, and D. E. Newman. Complex systems analysis of series of blackouts: Cascading failure, critical points, and self-organization. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 17(2):026103, 2007.

[8] R. Kinney, P. Crucitti, R. Albert, and V. Latora. Modeling cascading failures in the north american power grid. *The European Physical Journal B-Condensed Matter and Complex Systems*, 46(1):101–107, 2005.

[9] B. Mirzasoleiman, M. Babaei, M. Jalili, and M. Safari. Cascaded failures in weighted networks. *Physical Review E*, 84(4):046114, 2011.

[10] A. E. Motter and Y.-C. Lai. Cascade-based attacks on complex networks. *Phys. Rev. E*, 66:065102, Dec 2002.

[11] T. D. O'Rourke. Critical infrastructure, interdependencies, and resilience. *BRIDGE-WASHINGTON-NATIONAL ACADEMY OF ENGINEERING-*, 37(1):22, 2007.

[12] T. J. Overbye, X. Cheng, and Y. Sun. A comparison of the ac and dc power flow models for lmp calculations. In *Proceedings, 37th Hawaii International Conference on System Sciences*, 2004.

[13] S. Pahwa, C. Scoglio, and A. Scala. Abruptness of cascade failures in power grids. *Scientific reports*, 4, 2014.

[14] S. Pradhan and B. K. Chakrabarti. Failure properties of fiber bundle models. *International Journal of Modern Physics B*, 17(29):5565–5581, 2003.

[15] M. Rosas-Casals and R. Solé. Analysis of major failures in europes power grid. *International Journal of Electrical Power & Energy Systems*, 33(3):805–808, 2011.

[16] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, and R. Setola. Modelling interdependent infrastructures using interacting dynamical models. *International Journal of Critical Infrastructures*, 4(1):63–79, 01 2008.

[17] C. Roy, S. Kundu, and S. Manna. Fiber bundle model with highly disordered breaking thresholds. *Physical Review E*, 91(3):032103, 2015.

[18] D. Sornette, K.-T. Leung, and J. Andersen. Conditions for abrupt failure in the democratic fiber bundle model. *arXiv preprint cond-mat/9712313*, 1997.

[19] B. Stott, J. Jardim, and O. Alsac. Dc power flow revisited. *Power Systems, IEEE Transactions on*, 24(3):1290–1300, Aug 2009.

[20] Y. Tang, G. Bu, and J. Yi. Analysis and lessons of the blackout in indian power grid on july 30 and 31, 2012. In *Zhongguo Dianji Gongcheng Xuebao(Proceedings of the Chinese Society of Electrical Engineering)*, volume 32, pages 167–174. Chinese Society for Electrical Engineering, 2012.

[21] W.-X. Wang and G. Chen. Universal robustness characteristic of weighted networks against cascading failure. *Phys. Rev. E*, 77:026101, Feb 2008.

[22] D. J. Watts. A simple model of global cascades on random networks. *Proceedings of the National Academy of Sciences*, 99:5766–5771, 2002.

[23] O. Yağan. Robustness of power systems under a democratic-fiber-bundle-like model. *Phys. Rev. E*, 91:062811, Jun 2015.

[24] O. Yağan, D. Qian, J. Zhang, and D. Cochran. Optimal allocation of interconnecting links in cyber-physical systems: Interdependence, cascading failures, and robustness. *IEEE Transactions on Parallel and Distributed Systems*, 23(9):1708–1720, Sept 2012.

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

[26] Y. Zhang and O. Yağan. Optimizing the robustness of electrical power systems against cascading failures. In preparation for submission to *Scientific Reports*.