Mitigation of malicious attacks on Californian power transmission network

Patrick Soltis

Introduction

As electrical infrastructure in the US ages and power consumption becomes more complex, the grid becomes increasingly vulnerable to failure. As the 2003 and 2011 US blackouts showed, a single transmission line failure can cascade into a grid failure spanning multiple states and leaving millions without power for days. Important lessons were learned from these episodes (1,2).

In the mainland US, random failures have not caused the grid to spiral out of control in the past 9 years. Transmission lines form a highly interconnected network, which proves robust against randomly failing components. However, a coordinated attack could still prove deadly. Targeting a relatively small number of hub-like substations, those of which join a relatively large number of transmission lines, could disconnect large swaths of the transmission network. Reducing reliance on a small number of substations is imperative. Any attacker would require more attacks and therefore more time to take out a larger number of substations. More time means a greater chance of stopping the attack before the network fails.

Investment in updated grid infrastructure has been minimal over the past few decades. However, with an incoming presidential administration that prioritizes an energy overhaul, there is hope that some long-awaited investment is coming. Any updates to the transmission grid structure should be made to prolong the stability of the transmission network in the case of targeted attacks.

In this project, I identify a handful of transmission lines that could be replaced to make California's transmission network more robust. I use a process developed by Schneider, et al to measure and improve robustness (3). These authors were motivated by the same questions of grid robustness, with the goal of improving robustness using the fewest changes possible.

While many studies have quantified robustness of the power transmission network in various countries, this study is notable in that it proposes a process for improvement (4,5). They improve the network by rewiring select transmission line edges to new substation nodes. (This process is described in detail in the *Methods & Results* section.) The investigation finds that the robustness of the EU transmission grid significantly increases when only 5% of the lines are rewired. I will repeat this process for California's grid, and will assess whether the proposed replacements are sensible.

I refer to "transmission network" and not "grid" because the grid is comprised of both transmission and distribution lines, while this study focuses solely on transmission. Transmission lines are significantly more important for grid robustness than distribution. Additionally, data describing distribution networks are typically restricted to grid operators. Data describing the transmission network came from Homeland Infrastructure Foundation-Level Data (HIFLD), a service of the US Department of Homeland Security.

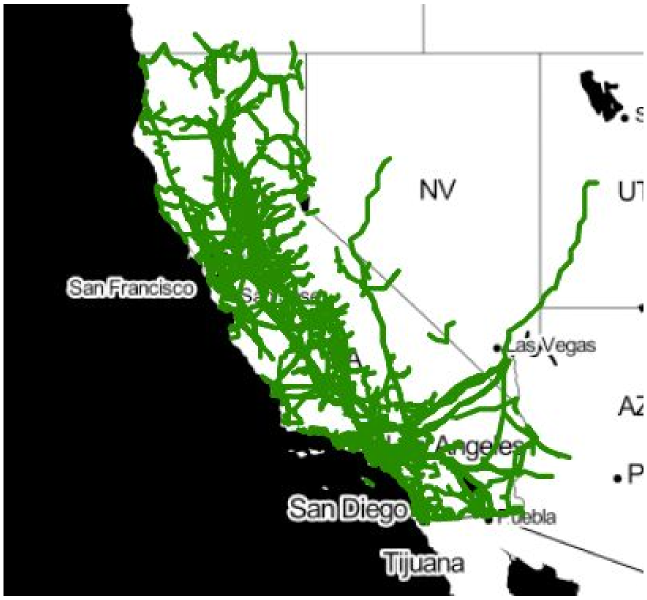


Fig. 1. A visualization of all power transmission lines with at least one end in California. Only lines that lie entirely in California are included in this study.

My study focuses on transmission lines supervised by the California ISO (Independent System Operator) in the state of California (Figure 1).[1] This is the largest relevant connected transmission network for the state.

In the next section, I describe the processes that Schneider et al used for measuring and improving the grid's robustness. I discuss how I adapted it for my study, as well as how I improved upon the model.

Methods & Results

The Schneider et al study measures robustness based on damage done to the network in a simulated "attack" sequence. To simulate deliberate destruction, the attack sequence starts by targeting a node of the highest degree. This node is removed. To determine the next target node, the degree of all nodes are recalculated. Every subsequent node is targeted based on the highest degree after the previous node is removed.

Q represents the number of nodes that have been removed from the original network. The fraction of total nodes $\frac{Q}{N}$ removed is represented as q. The health of the network is described in the value $s(q)$, which is the fraction of nodes (relative to the original graph) in the largest connected component after Q nodes were removed. This fraction is used because, in the case of the transmission network, operators will attempt to stabilize all significantly large connected components of the network. The only meaningful "collapses" in the transmission network are blackouts and equipment failures that cause injury, none of which the topology of the network can meaningfully indicate. Thus, the size of the largest operational unit provides a useful proxy for indicating overall health.

---

[1] Some sections of the grid in California are supervised by a different ISO, and the California ISO also supervises portions of the grid in Nevada. Neither of these grid sections are included in this study.

The attack ends when *s(q)* falls below a predetermined limit. This limit is arbitrarily set at 0.1 for both the previous study and my project.

The robustness of the network, *R*, is defined as:

$$R = \frac{1}{N} \sum_{Q=1}^{N} s(q)$$

Essentially, the values of *s(q)* after every node removal are added together and divided by *N*, the number of nodes in the original graph.[2] To expedite the time required to calculate *R*, I adjusted the definition to only add in *s(q)* only as long as $s(q) > 0.1$. R is still larger when larger components remain intact for longer periods of time, so R is still a useful measure even with this adjustment.

A stronger network was identified by trial and error. In each iteration, 2 links were randomly selected. If the 2 links A and B met some practical criteria, they were removed. 2 links were drawn that each connected one point formerly on link A and one point formerly on link B, as shown in figure 2.

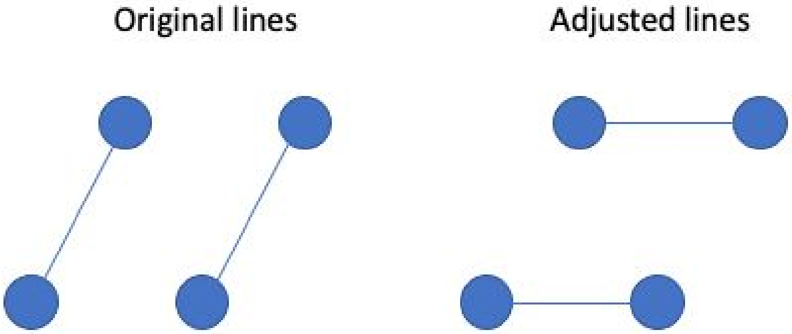


Fig. 2. A toy example of how transmission lines are adjusted.

This process for adjusting the network reflects the practical limitations of power infrastructure. Utilities cannot add dozens of transmission lines to increase network connectivity due to budget and landscape limitations. However, replacing two lines with two new lines is more within the realm of possibility. Also to this effect, the lines were not replaced unless the combined length of the proposed lines was less than the combined length of the original lines. I also made use of the voltage rating for each line available in the HIFLD data. To make sure a substation is not connected to a transmission line with an dangerous voltage level, a pair of lines was only replaced if they had the same voltage rating.

After changing a pair of links, the adjusted network was then subjected to an attack sequence to determine the *R*. The adjustments were accepted if *R* increased, and denied if *R* failed to increase. The process was repeated until *R* failed to increase after 20 attempts.

---

[2] Normalizing by N helps make this measure relevant for comparison between networks of different sizes.

Hundreds of substations pairs had multiple transmission lines running between them. I included these multiple lines as multiple edges between the relevant nodes. Combining these multi-edges into single edges would make it impossible to compare voltage ratings when adjusting links. Additionally, the multi-edge network behaved significantly differently under the attack sequence than the combined edge network (Figure S1). Since the multi-edge network more closely resembles the real transmission network, using the combined edge network would thus significantly increase inaccuracy.

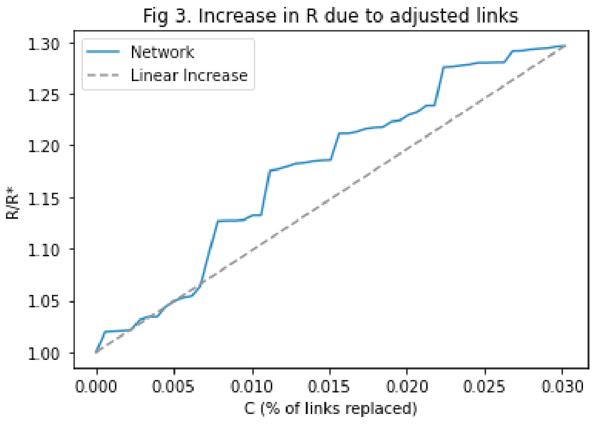
The strengthening process fizzled out after adjusting 108 transmission lines, about 3% of the total. Although small compared to the overall Californian transmission network, these adjustments led to a 30% increase in the network robustness measurement R (Figure 3).

This is a significant increase, although the process appeared slightly more effective for the European grid modeled in Schneider et al. At 3% link adjustment, the EU grid achieved closer to 40% increase in R.

The plot of *s(q)* may prove a more intuitive representation of the network's improvements (Figure 4). Both the original and the improved network experience a dramatic dropoff between 1% and 2% of nodes being removed. However, this drastic dropoff occurred after 1.3% node removal in the original network but after 1.6% node removal in the improved network. This improvement of 0.3% corresponds to about 10 additional substations that would have to be knocked offline before this first disaster. There is a more dramatic increase in the number of nodes - over 1%, or 33 nodes - which must be removed before *s(q)* drops below 0.1.

Conclusions & Future Work

Interestingly, the improvement in R relative to C follows a roughly linear relationship connecting the R-values of the initial and final improved networks (Figure 3). This shows that, on average, each link replaced provides a similar boost to robustness. In Menczer et al, we see that real networks are more



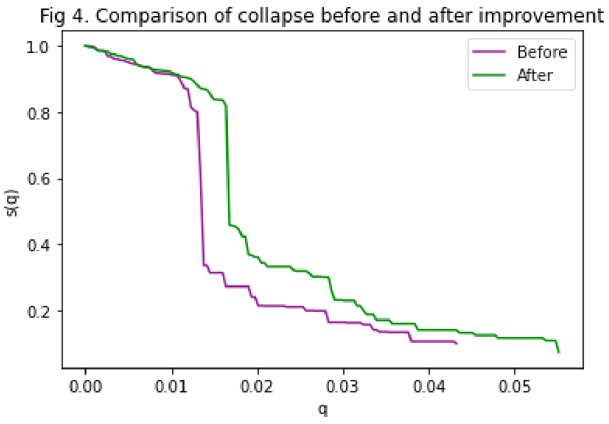


Fig. 3. Increase in robustness *R* as percentage of links replaced *(C)* increases. *R* is normalized by *R**, the robustness of the initial network before any link replacements. The gray line runs from the first point to the last point, showing a theoretical linear increase for comparison.

Fig. 4. Collapse of the transmission network under the attack sequence, before and after the network improvement process. *Before* represents the initial network, and *After* represents the network with 108 transmission lines redrawn.

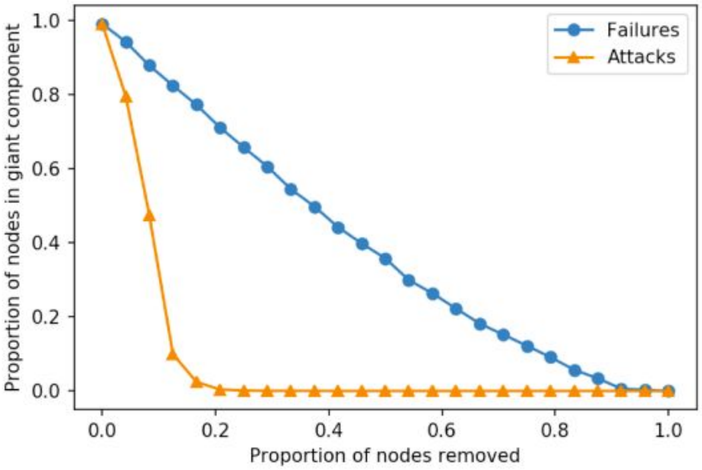


Fig. 5. Real networks are robust against random failures but fragile against targeted attacks (6).

robust against random failures than targeted attacks (6). The value of R is similar to the sum of the area under each curve in Figure 5. The *After* curve in Figure 4 indeed captures a greater area. If the linear trend in Figure 3 continues, it is possible that every good adjustment will continue to prove network robustness as well as the previous adjustment. However, the trend in Figure 3 also appears to begin flattening out between C = 0.02 and C = 0.03. Identifying some critical point at which the improvement in R switches from linear to a decaying function would be useful. This would indicate a practical number of lines to replace before the improvements are no longer worth the cost.

Further research or consultation with grid security experts is necessary to determine whether either of these features are significant improvements. For example, rerouting over 100 transmission lines only increased the number of substations that needed to go down by 10. The cost to switch so many lines may be prohibitively expensive for improvements of such a size. In addition, there have been no successful coordinated attacks on the US transmission network in the past 10 years, which suggests that the system may already be sufficiently robust.

Although the EU grid became significantly more robust through the strengthening process, this is not sufficient to conclude that the EU grid is more robust than California's. For example, it is not clear whether the EU study modeled the grid as a combined edge or a multi-edge graph, or if the EU grid even has the need to be represented by a multi-edge graph. Additionally, my study restricted the link adjustment by voltage rating, which might stifle improvements in any grid. Finally, my simplification of the R calculation might also affect the relative improvement, even if both studies normalize by the R of the original network.

Because the identifiers for each transmission line are preserved, a future investigation could review in more detail the 108 transmission lines that were adjusted. Such a review could clarify how practical this method is for measuring and improving robustness. For example, although the strengthening process did not net any increase in total transmission line length, the length of the lines replaced is still important. Longer lines would be more costly to replace, and likely more disruptive to the grid's normal operating paradigm. As a result, replacements of shorter lines that can improve the robustness are more relevant.

Additionally, some of the new lines may require impossible or prohibitively expensive routes, such as crossing the peak of a mountain or a body of water.

If the removed lines have been identified as vulnerabilities by other studies or by operators, this process could potentially gain credibility as a performance enhancing tool. More importantly, such an investigation could draw attention to potentially shiftable transmission links and prompt real improvements to grid stability.

My results draw from one simulation, due to the limited time and computing power I could access for this project. Aggregating multiple runs would smooth out the variability in the improvement sequence, which may be disproportionately affected by the specific links selected at random.

The study's accuracy is limited by the availability of grid data. While I can analyze the structure of transmission lines, the real system is in a constant state of shifting voltage and current. The model would be significantly improved if data representing real time-dependent use of the system could be integrated. For example, location of major loads and generation sources at peak usage hours could be used to infer the directionality of current flow at this critical moment (7).

On the other hand, this study does not even make full use of the data available through HIFLD. This database contains information for every transmission line in the United States. Running this analysis on a larger portion of the country, or even the full country, could render more broad-reaching insights. Such an analysis could even be more accurate, as this study considers California's transmission network as an island when in fact it could be modeled more accurately as part of a larger system.

References

1. US-Canada Power System Outage Task Force (2004). "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations."
2. Federal Energy Regulatory Commission and North American Electric Reliability Corporation staff (2012). "Arizona-Southern California Outages on September 8, 2011."
3. Schneider, CM; Moreira, AA; Andrade JS; Havlin, S; Herrmann HJ (2011). "Mitigation of malicious attacks on networks." *PNAS* 108 (10), 3838-3841. https://doi.org/10.1073/pnas.1009440108.
4. Rosato, V; Bologna, S; Tiriticco, F (2007). "Topological properties of high-voltage electrical transmission networks." *Electric Power Systems Research* 77 (2), 99-105. Elsevier. https://doi.org/10.1016/j.epsr.2005.05.013.
5. Albert, R; Albert, I; Nakarado, GL (2004). "Structural vulnerability of the North American power grid." *Phys. Rev. E* 69, 025103(R), APS. https://doi.org/10.1103/PhysRevE.69.025103.
6. Menczer, F; Fortunato, S; Davis, CA (2020). *A First Course in Network Science*. Cambridge University Press. cambridgeuniversitypress.github.io/FirstCourseNetworkScience
7. Shahparia, A; Khansaria, M; Moeinib, A (2019). "Vulnerability analysis of power grid with the network science approach based on actual grid characteristics: A case study in Iran." *Physica A* 513*,* 14-21. Elsevier. https://doi.org/10.1016/j.physa.2018.08.059.

Supplementary/Appendix

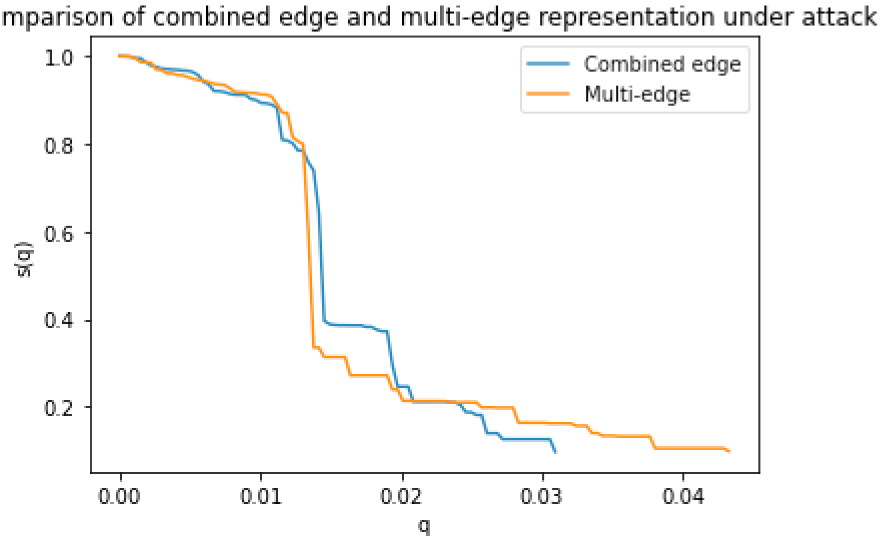


Fig. S1. Comparing the differences in network breakdown between a combined edge representation and multi-edge representation of the initial transmission network. A substantial difference in behavior exists. Similar to Fig 4, except comparing two different versions of the unadjusted network.

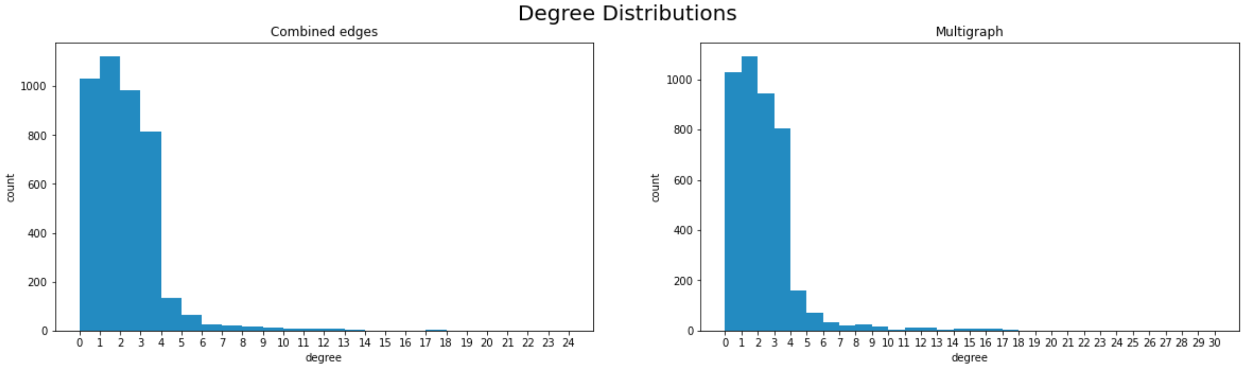


Fig. S2. Degree distributions of combined edge and multigraph representations of the California power transmission grid were overall very similar.

Table S1. Comparison of basic network characteristics between the combined edge and multi-edge representations of the power transmission network. These statistics are for a network representing all transmission lines in California, before the CalISO supervised region was isolated.

Characteristic	*Combined Edge*	*Multi-edge*
N (number nodes)	4260	4260
L (number links)	3689	3974
<k> (average degree)	1.73	1.9
k max (maximum degree)	24	30
Node(s) with k max	id=70932	id=70932