Mitchell Lehman
Andrew Nyffeler
Wyatt Ward
Team 07
Advisor: Tu N. Nguyen

CS46500 Final Report

Introduction

A modern electrical grid is different from its earlier forbears; it possesses sensors and computer systems that can choose to route power to quickly restore operation in the event of failure of a few components (making it "smart").

However, this might be exploitable for a potential attacker, as happened in Ukraine in late 2015. By intelligently choosing which parts of a grid to attack, one may be able to cause a "domino effect" which can potentially cause large swaths of the grid to go offline. Such attackers need to operate within the budgets they have; this means making everything they attack count as much as possible, with minimal waste. Our project sought to find a method to predict what points can be used to trigger a domino effect, accounting for the varying costs of attacking a given part.

Literature Survey

Three articles were given by our advisor as a jumping-off point for this project. The first of these was “Price Modification Attack and Protection Scheme in Smart Grid” [1], which covered some suggested techniques for protecting smart grid systems from a slew of attacks and described the idea of ‘cascading failure’ in detail.

This paper uses two attack models: the first is to maximize the number of downed (failed) transmission lines, and the second is to rank the lines by the ability to induce a cascade, and then attacking the line with the highest benefit-to-cost ratio. The success or failure of these two models

(along with random attacks, as a control) is performed on three electrical models: the IEEE 57-bus system (AEP's grid from "the early 1960s"), a contrived model, and a simulation of the Summer 2004 Polish grid from the MATLAB package MATPOWER.

Interestingly, the cascade-targeting attack method result in a higher percentage of downed lines in all three simulated grids. While this is likely due to its risk-reward accounting nature, it does reinforce the idea that targeting metrics that consider both a targeted node and the consequences of attacking it are more likely to be successful.

The second paper we read for background, "Catastrophic Cascading Failures in Power Networks" [2], covered the topic of cascade in much greater depth than the first, which merely touched on it as one aspect of the overall scope of the report. This one is comparatively much narrower, and several of the researchers who were involved in this paper were also involved in the first.

This paper uses a model of the Western North American (WNA) power grid from a 1998 issue of Nature. This model does not natively come with load and capacity values, however, so the authors create these values. The load used of a node is based off the number of attached nodes, and the capacity is equal to the load times a system-wide tolerance factor.

Tests of a variety of different attack priority algorithms of the WNA grid reveal that despite containing nearly 5000 nodes, the entire grid can nearly collapse with the fall of far less. A system tolerance factor of 2.0 (i.e. 50% usage), for example, would see around 4500 nodes fail (91%) after just 10 attacks. Stepping up to 2.2 (45% usage) decreases 10-node attack failure to about 3400 (70%). The paper continues with more values, ranging from 1.2 to 2.6 in 0.2 increments, but a pattern becomes visible: While most increments cause equally small differences in grid failure, tolerance factors starting from 2.4 begin to have wider gaps between them.

While half the WNA grid can be brought down with just 5 attacks for tolerance factors of 2.2 or below, 2.4 requires 10, and 2.6 requires nearly 25. While tolerance factor 2.6's usage rate of 38% may be dauntingly small, a much nicer value of 75% corresponds to a tolerance factor (~1.3) that will bring the entire grid down on a **single** well-placed attack.

The third article is "An Entropy-based Metric to Quantify the Robustness of Power Grids Against Cascading Failures" [3] and it focused on ways to measure how prepared smart grids are for attempts at causing cascading failure chains. Like the others, this paper uses a real-life accurate model, specifically the IEEE's 30-bus system, which represents AEP's grid in December 1961 (slightly earlier the 57-bus model mentioned above). The paper also considers seasonal variation of the grid, when people turn on AC unit in the summer and heaters in the colder winters.

These papers gave us the background knowledge we needed in order to proceed with confidence in the months that followed.

Description of Methods

Initially the primary concern was determining at what point a system would suffer a cascading failure. In order to do this, it was decided to approach the problem as an attacker would, with special attention being paid to the real-world logistical problems faced by attackers. Our model uses elements of graph theory to analyze smart grid networks to demonstrate the effects an attack can have on the system, even with limited resources; a graph of a smart grid might have power plants (suppliers), transmission lines, and transformers that distribute and change power for consumption. Each of these elements of the graph has its own set of properties with respect to how they can fail and information

that might be relevant in picking the best ones to target. Since power flows directionally, a graph must therefore be directed. In Figure A, an example of such a graph is presented.

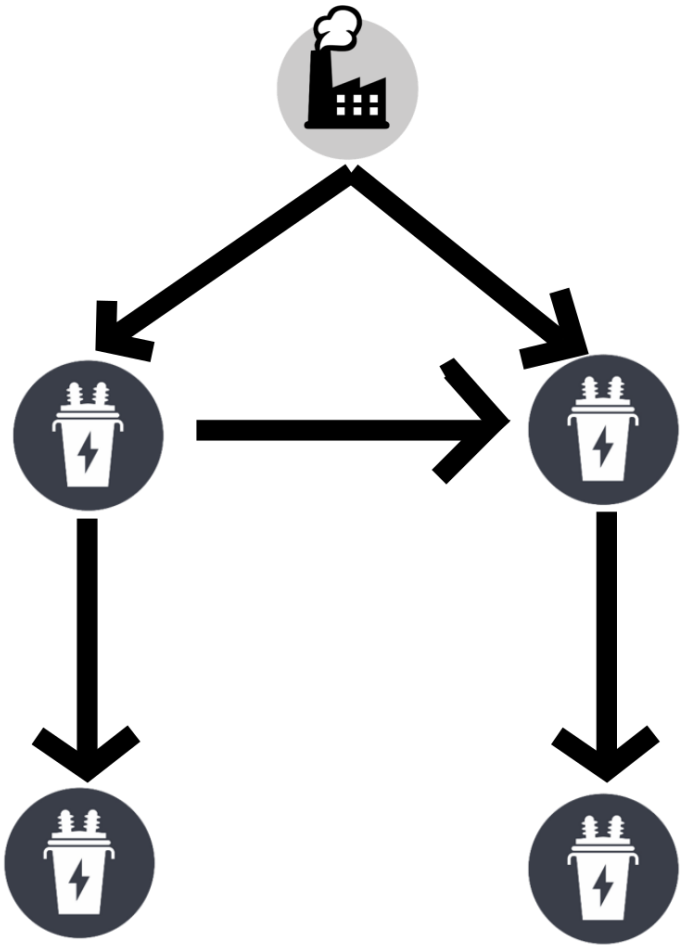

Fig. A: an example graph, sans properties of the elements.

The factors an attacker would include in analysis of a grid include the cost of mounting an attack on a given target within the grid, as well as the amount of 'value' that is associated with bringing down individual parts of the grid. This value attribute is essentially based on consequences deemed as having desirable properties for the attacker. To an attacker, bringing down a hospital or government building potentially causes more havoc, and is thus a better target than bringing down a suburban neighborhood's power on a weekday.

Much as the grid itself has a maximum load it can carry, so too does every individual part of a grid. As more parts start to fail, the remaining parts' operating margins shrink as they are forced to work ever harder. The implication of this is by simply taking down one or two cheaper parts of the grid tangential to the actual, costlier target, the remaining work to cause an expensive target to fail is reduced. In this way, it can be easier to mount one or several smaller attacks instead of a direct, all-out assault on the final target. Figure B demonstrates how the remaining ability of a given part to cope (area above the curve) decreases when other failures occur and the part is forced to shoulder heavier burdens.

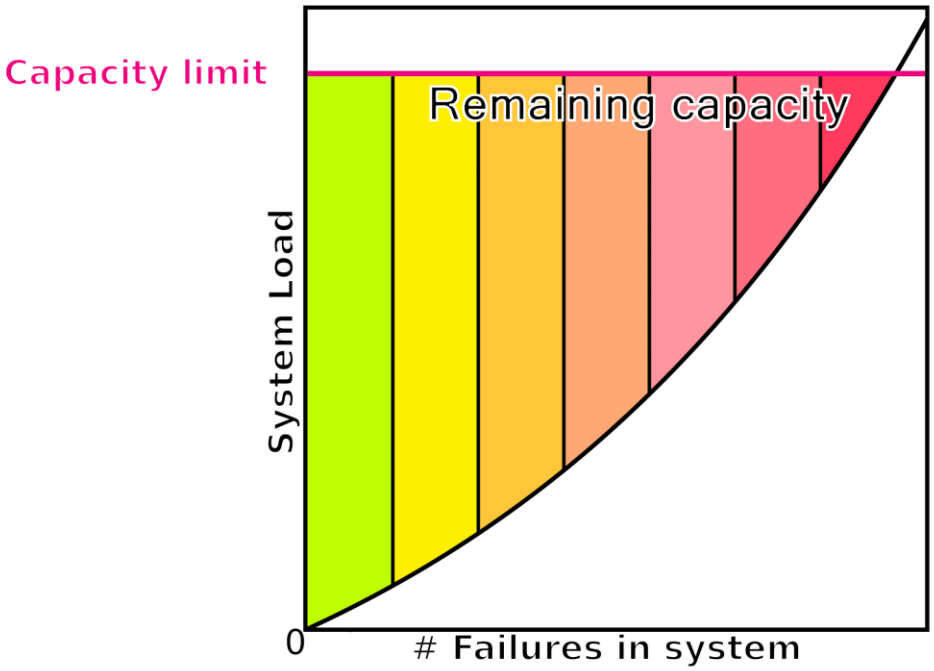

Fig. B: Failure of other parts in a smart grid decreases the operating margins of the remaining parts.

All of this implies three major properties to consider for each element on a grid: those of weight, capacity, and cost. They can be formed into a mathematical relationship for divining the most best attack points, which is useful if it isn't cost-effective to directly attack a desired target. This property is termed the 'metric' (M) of an element. Figure C shows a similar graph to the one from Figure A, in the light of this new additional information, and also provides the metric equation referred to earlier. The

numbers by each element represent capacity to show how load from a part propagates ‘up-stream' to the plant, accumulating at midpoints.

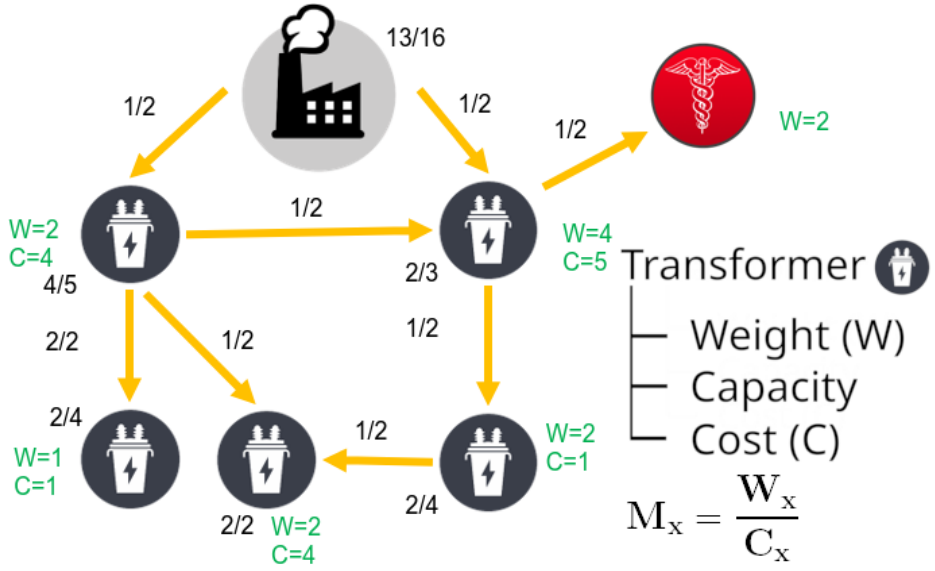

Fig. C: A full graph with all data. Fractions show current versus maximum load.
‘x’ can represent any individual node on the graph.

Results and Analysis

Using figure C’s data, the attacker desirability metrics for each of these points can be determined. It is then seen that despite the high weight on the transformer connecting to the hospital, the equation states that better use of money-for-weight would be attacking the transformer to the south. The hospital’s transformer has an M-value of 0.8 (4/5), and the best transformer (according to the metric) has an M-value of 2.0 (2/1). When this point is brought off-line, it increases the load on the remaining parts of the system, resulting in more failures. The transmission line connecting it to the hospital’s transformer is overrun (3/2 the designed load), and more importantly the hospital transformer itself is brought up to 4/3 capacity, causing its failure as well. In this way, disabling the 2-metric transformer is the only action needed to take out the 0.8-metric for no extra costs (figure D).

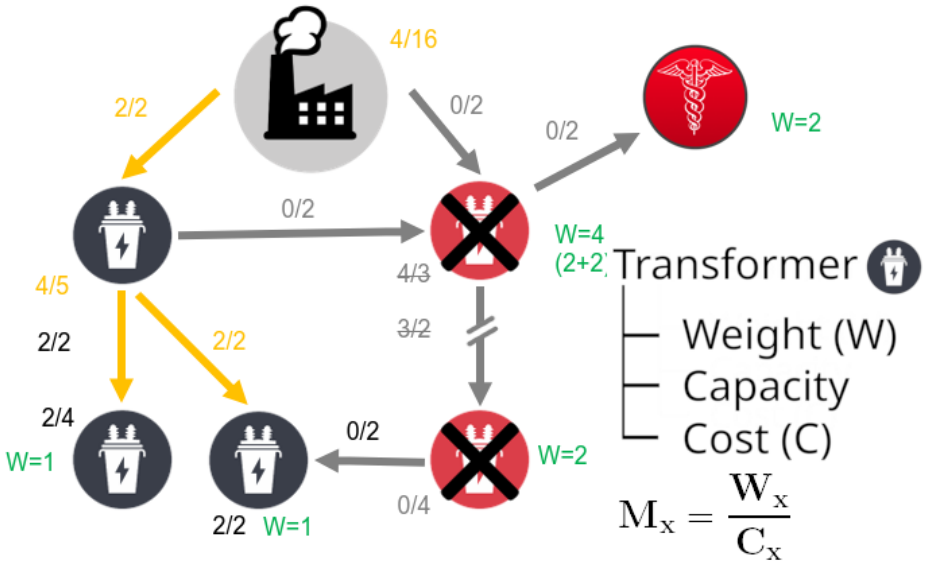

Fig. D: Disabling the M_x=2 node causes the failure of the W_x=4 node and the transmission line connecting them.

This particular example demonstrates the power of this concept; by aiming for the target with the highest M_x rather than the highest weight, expenses were reduced to knock out the same node by instead finding a different primary target.

Hypothetical Future Works

The current model does not perfectly match real systems. This is to be expected for simplicity's sake, but a hypothetical future model may be more accurate. Included details in this more realistic idea would be resistance of transmission lines (and their altering value with load, temperature, and line length), quantification of a node's physical and digital attack surfaces, and seasonal (and even daily) variation in load by consumers.

To be highly topical, the current pseudo-quarantine brought about by COVID-19 has likely drastically altered the terrain of the electrical grid as stay-at-home workers shift electrical load from commercial facilities to a far larger number of residences. This would result in changes to node weights, where areas commonly populated by large numbers of people (such as universities) are now far less

productive to target. Correspondingly, places such as medical facilities, fabric stores (for homemade masks), and groceries all make significant leaps on target priority lists.

The implementation of all these changes only complicates the process of target data collation and analysis, however. A more immediate future adjustment would be to add automation to the project, such that the grid analysis can be done far faster and more accurately than any human. Later stages of automation could very well include giving the program the ability to acquire the weights and benefits from attacking specific nodes without user input. Neural network models can also be integrated. Their convolutional nature is an out-of-the-box approach that could detect otherwise hidden weaknesses in the electrical grid.

References

[1] S. Mishra, X. Li, T. Pan, A. Kuhnle, M. T. Thai and J. Seo, "Price Modification Attack and Protection Scheme in Smart Grid," IEEE Transactions on Smart Grid, vol. 8, no. 4, pp. 1864-1875, 4 July 2017.

[2] J. Seo, S. Mishra, X. Li and M. T. Thai, "Catastrophic cascading failures in power networks," Theoretical Cpmputer Science, vol. 607, pp. 306-319, 2015.

[3] Y. Koç, M. Warnier, R. E. Kooij and F. M. Brazier, "An entropy-based metric to quantify the robustness of power grids against cascading failures," Safety Science, vol. 59, pp. 126-134, 2013.