



Cascading Power Failure

John Ellis, Lawrence Livermore National Laboratory, Norfolk State University

Rafael Rivera Soto, Lawrence Livermore National Laboratory, Universidad del Turabo at Gurabo, Puerto Rico

Mentor: Jeffery Duffany, Universidad del Turabo at Gurabo, Puerto Rico

Celeste Matarazzo, Lawrence Livermore National Laboratory, Cyber Defenders



Abstract: Over the past century, the world has become dependent on power grids in order to receive electricity. With the rise of terrorist groups around the world, environmental activists that oppose large substations, and cyber warfare between the United States and its adversaries, there has become a need to analyze potential attacks, and the outcomes of said attacks. Our focus is cascading power failures due to node or edge based attacks. Failures like this could result in a total blackout similar to the 2003 Northeast Blackout that left 55 million people without power. The goal of our research is to simulate node and edge based attacks using R-Language. Due to their importance around the world, it is important to determine and secure the vulnerabilities of power grids.

Introduction:

A cascading power failure is a failure in which nodes in a grid become overloaded with power, and must redistribute the load the node holds in order to keep running. In turn, those nodes can become overloaded, causing the power to continuously redistribute to other nodes, until there aren't any left.

Methods:

To begin our research, we needed to gain an understanding on how power grids work, and why they're able to run. After learning that, we analyzed various models of cascading power failures. We used R-Language in order to simulate node and edge based failures in different types of networks such as Barabási-Albert (scale-free), Watts-Strogatz (small world), Erdős-Rényi (random) and mesh networks.

Results:

In order to understand and create simulations, we analyzed different formulas.

$$\Delta L_{ji} = L_i \frac{L_j}{\sum_{n \in \Gamma_i} L_n}$$

This equation represents the redistribution of the load once a node is removed. The load received by the neighboring node is proportional to its initial load.

$$L_i = \sum_{s \neq v \in EV} \frac{\sigma_{st}(v)}{\sigma_{st}}$$

This equation represents the load that a node will have at any period of time. The load in this case is the number of shortest paths that go to a node in any period of time.

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

The capacity is a percentage of the initial load of a node.

Discussion:

After extensive research, we found that the second model (fig. 2) was more successful than the first (fig. 1). Model 2 was more successful at creating a more realistic scenario of cascading failures. We also found that using a fixed threshold for the capacity was more realistic than using a percentage of the initial load.

References:

1. Wang, J. W., & Rong, L. (2009). Cascade-based attack vulnerability on the us power grid. *Safety Science*, 47, 1332-1336. Retrieved from <http://www.cse.psu.edu/~smclaugh/cse598e-f11/papers/wang.pdf>
2. Li, S., Li, L., Yang, Y., & Luo, Q. (2012). Revealing the process of edge-based-attack cascading failures. *Springer*, 69, 837-45. Retrieved from <http://link.springer.com/content/pdf/10.1007/s11071-011-0308-8.pdf>
3. Chen, Q., & Shi, D. (2003). The modeling of scale-free networks. *Physica A*, 335, 240-48. Retrieved from http://jupiter.engr.utk.edu/Projects/Mis/SEN/References/CS04_The_modeling_of_SFN.pdf

