NETWORK SCIENCE

Curtailing cascading failures

The failure of a small but variable set of links can bring down a supply network

By **Raissa M. D'Souza**

Cascading behaviors are ubiquitous, from power-grid failures (*1*) to "flash crashes" in financial markets (*2*, *3*) to the spread of political movements such as the "Arab Spring" (*4*). The causes of these cascades are varied with many unknowns, which make them extremely difficult to predict or contain. Particularly challenging are cascading failures that arise from the reorganization of flows on a network, such as in electric power grids, supply chains, and transportation networks. Here, the network edges (or "links") have some fixed capacity, and we see that some small disturbances easily dampen out, but other seemingly similar ones lead to massive failures. On page 886 of this issue, Yang *et al*. (*5*) establish that a small "vulnerable set" of components in the power grid is implicated in large-scale outages. Although the exact elements in this set vary with operating conditions, they reveal intriguing correlations with network structure.

One feature of cascading behaviors seen in systems as varied as electric blackouts, forest fires, financial markets, and firing of brain neurons (*1*, *6*, *7*) is that the sizes of the observed cascades follow a power-law distribution. The seminal "Bak-Tang-Wiesenfeld sandpile" model of self-organized criticality (*6*) provides a theoretical underpinning for this property. Here, discrete grains of sand, representing packets of load, are dropped at random on a network of nodes with limited capacity to hold sand. Once a node becomes overloaded, it "fails" and sheds all of its sand grains to neighboring nodes, which may then become overloaded and similarly fail in a cascading manner.

The model can be analyzed rigorously and reveals general mechanisms but fails to capture specific details. For example, it is a contact process. For a node to fail in a cascade, it must have a direct neighbor that has already failed, much like infectious diseases spread only through direct contact. By contrast, for electric grids, the failure of one power line can cause an indirectly connected line hundreds of kilometers away to fail next (*8*), and we lack a predictive framework for this (*9*).

Percolation theory, which considers the extent of systemwide connectivity, also provides an abstracted model of vulner-

Department of Computer Science and Department of Mechanical and Aerospace Engineering, University of California, Davis, Davis, CA, USA. Email: raissa@cse.ucdavis.edu

PHOTO: ISTOCK.COM/YANGPHOTO

Failures in the power grid can propagate hundreds of kilometers.

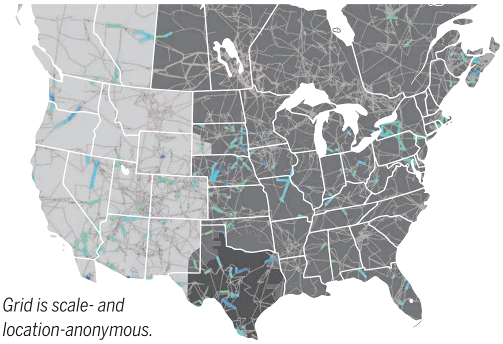
ability and cascades in the power grid (*10*, *11*) but neglects the dynamics of flows and the capacities on links, which can lead to different conclusions once accounted for (*10*, *12*, *13*). It also assumes that systemwide connectivity is essential for function, whereas in the power grid, "islanding" (breaking the grid up into smaller, self-sustaining subnetworks) is a control strategy used to prevent cascades (*14*).

Failure and the *k*-core

Yang *et al*. show that a small but variable set of vulnerable links in a power grid was disproportionately responsible for large failure cascades. The *k*-core structure of the network appears to be related to the redundancy of flow rerouting opportunities.

The links in the grid

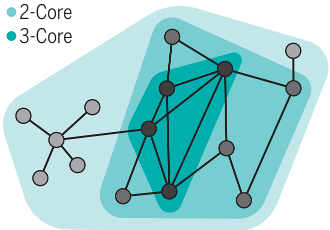
The contiguous span of the U.S.–South Canada electric grid, with shades of gray indicating the three main interconnections. Color is meant to convey example vulnerability for some operating condition.



Grid is scale- and location-anonymous.

Classifying culprits

The *k*-core structure classifies subnetworks by their increasing density of internal links. Links in higher *k*-cores (3, versus 2 and 1 in the sample graph) are more likely to fail from overloading due to flow rerouting.



To capture the real dynamics with higher fidelity, power engineers use models more specific to power-grid cascades [see, for example, (*15*)] and an arsenal of analytic tools and computer simulations. Of course, in any model, there are trade-offs. Increasing the detail of specific aspects still neglects the secondary effects that often amplify in this web of generators, transmission lines, consumers, and human operators, with nonlinear dynamics at many different time scales (*9*). Detailed models are also computationally expensive and thus restricted to regions that are quite small in comparison with the regional divisions of the continental United States power grid, whose interactions are vital to maintaining systemwide synchronization and stability.

The study by Yang *et al.* bridges the gap. They develop a simulation framework for analyzing the vulnerability of a continent-wide power system that captures the underlying physics of power flow, many standard operating practices (such as islanding), and cascading failures caused by power lines overheating. They validated their model with historical data on line outages and observed cascade sizes and then analyzed the vulnerability of the contiguous U.S.–South Canada power grid (see the figure). Specifically, they considered a small triggering perturbation on this grid, focused on how many links further fail because of a sequence of line overloads ("primary failures"), and aggregated this response over a broad range of system conditions.

They establish that the primary failure of a few links within or near a vulnerable set of links causes a disproportionate number of large cascades. Surprisingly, this vulnerable set is quite small, with only ~10% of all the links in the U.S.–South Canada power system ever undergoing a primary failure. Links in the vulnerable set are biased toward more densely populated geographic areas. They are also correlated with how central the link is in the *k*-core structure of the network, a method that reveals the subnetwork organization as characterized by increasing density of internal links (see the figure). The nodes in the *k*-core are determined by first removing all nodes of degree less than k, and their associated edges, and repeating the process, removing all nodes that now have degree less than k, and their associated edges, until all remaining nodes have degree at least k.

Yang *et al.* provide intriguing evidence that the *k*-core index of a link is related to the redundancy of paths available for flow rerouting, a result that should spark further theoretical investigations. Unfortunately, which exact links are in the vulnerable set varies based on the specific operating conditions, and no two cascades are identical. However, the vulnerable set is overall small with recurrent failures, and Yang *et al.* suggest that "failure-based" allocation of resources could be applied more selectively to lines seen to repeatedly undergo primary failures in an attempt to reduce cascades. They do use a level of abstraction to translate from the physical elements of the actual power grid into the "nodes" and "links" of their network. Also, they do not capture common failure modes that arise from instabilities. Still, they establish important insights for the power grid that should have wider-reaching implications.

A comprehensive theory of cascading failures across domains will require consideration of which quantities are conserved in the load-shedding process. The flow could be made of electrons in the power grid, packets on the internet, people on an airline network, or goods in supply chains, leading to vastly different constraints. Internet packets can be lost and readily resent, but each electron on the grid is conserved and transported somewhere, even short-circuiting to ground. Passengers on transportation networks are conserved, but unlike electrons, they have distinct source-destination pairs (and finite patience while waiting). Understanding how the different constraints and costs lead to different classes of cascading failures will be a key to eventually designing control interventions for avoidance and rapid recovery. ■

REFERENCES AND NOTES

1. I. Dobson, B. A. Carreras, V. E. Lynch, D. E. Newman, *Chaos* **17**, 026103 (2007).
2. P. Stafford, "Flash crash explanation questioned," *Financial Times*, 3 April 2013.
3. A. J. Menkveld, B. Z. Yueshen, *SSRN* 10.2139/ssrn.2243520 (2017).
4. C. D. Brummitt, G. Barnett, R. M. D'Souza, *J. R. Soc. Interface* **12**, 20150712 (2015).
5. Y. Yang, T. Nishikawa, A. E. Motter, *Science* **358**, eaan3184 (2017).
6. P. Bak, C. Tang, K. Wiesenfeld, *Phys. Rev. Lett.* **59**, 381 (1987).
7. P. Bak, M. Paczuski, *Proc. Natl. Acad. Sci. U.S.A.* **92**, 6689 (1995).
8. North American Electric Reliability Council (NERC), *System Disturbances–1996* (August 2002).
9. C. D. Brummitt, P. D. H. Hines, I. Dobson, C. Moore, R. M. D'Souza, *Proc. Natl. Acad. Sci. U.S.A.* **110**, 12159 (2013).
10. G. A. Pagani, M. Aiello, *Physica A* **392**, 2688 (2013).
11. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, S. Havlin, *Nature* **464**, 1025 (2010).
12. P. Hines, E. Cotilla-Sanchez, S. Blumsack, *Chaos* **20**, 033122 (2010).
13. M. Korkali, J. G. Veneman, B. F. Tivnan, J. P. Bagrow, P. D. H. Hines, *Sci. Rep.* **7**, 44499 (2017).
14. IEEE, *IEEE 1547.4-2011 Guide for Design, Operation, and Integration of Distributed Resource Island Systems with Electric Power Systems* (IEEE, 2011).
15. I. Dobson, B. A. Carreras, D. E. Newman, *Prob. Eng. Inf. Sci.* **19**, 15 (2005).

ACKNOWLEDGMENTS

I am grateful for support from Army Research Office Multidisciplinary University Research Initiative grant W911NF-13-1-0340, Army Research Laboratory grant W911NF-09-2-0053, and Defense Advanced Research Projects Agency grant W911NF-17-10077.

10.1126/science.aaq0474

GRAPHIC: V. ALTOUNIAN/*SCIENCE*; (MAP DATA) BOUCHECL/WIKIMEDIA COMMONS AND YANG *ET AL.*

Science

Curtailing cascading failures

Raissa M. D'Souza

Science **358** (6365), 860-861.
DOI: 10.1126/science.aaq0474