New algorithm quickly identifies most dangerous risks in a power grid amid millions or billions of possible failures

July 1 2013, by Jennifer Chu

Credit: CHRISTINE DANILOFF/MIT

Each summer, power grids are pushed to their limits, as homes and offices crank up the air conditioning in response to rising temperatures. A single failure in the system—such as a downed power line or a tripped relay—can cause power outages throughout a neighborhood or across entire towns.

For the most part, though, a failure in one part of the grid won't bring

down the entire network. But in some cases, two or more seemingly small failures that occur simultaneously can ripple through a power system, causing major blackouts over a vast region. Such was the case on Aug. 14, 2003, when 50 million customers lost power in the northeastern United States and Ontario—the largest blackout in North American history. Even more recently, in July 2012, India experienced the largest power outage ever, as 700 million people—nearly 10 percent of the world's population—went without power as a result of an initial tripped line and a relay problem.

To help prevent smaller incidents from snowballing into massive power failures, researchers at MIT have devised an algorithm that identifies the most dangerous pairs of failures among the millions of possible failures in a power grid. The algorithm "prunes" all the possible combinations down to the pairs most likely to cause widespread damage.

The researchers tested their algorithm on data from a mid-sized power grid model consisting of 3,000 components (in which there are up to 10 million potential pairs of failures). Within 10 minutes, the algorithm quickly weeded out 99 percent of failures, deeming them relatively safe. The remaining 1 percent represented pairs of failures that would likely cascade into large blackouts if left unchecked.

The speed with which the researchers' algorithm works is unmatched by similar existing alternatives, according to one of its co-developers, Konstantin Turitsyn, the Esther and Harold E. Edgerton Assistant Professor in MIT's Department of Mechanical Engineering.

"We have this very significant acceleration in the computing time of the process," Turitsyn says. "This algorithm can be used to update what are the events—in real time—that are the most dangerous."

Turitsyn and graduate student Petr Kaplunovich will present their work,

supported by the MIT Skoltech Initiative, in a paper at the IEEE Power and Energy Society Meeting in July.

A zero missing rate

In power systems lingo, a pair of failures is referred to as an "N minus 2 contingency"—"N" being the number of components in a system, and "2," the number of failures in a power grid at any given moment. In recent years, researchers have been developing algorithms to predict the most dangerous N-minus-2 contingencies in an electric grid. But while such algorithms successfully identify dangerous pairs of failures, Turitsyn says that most of them don't guarantee that these pairs are the only failures of concern. In other words, there may be failures that these algorithms missed.

"They don't provide guarantees that the ones you assume to be safe are really safe," Turitsyn says. "If you want to have some guarantees that the system is safe, you want the system to rely on algorithms that have zero missing rates."

Taking this angle of approach, Turitsyn and Kaplunovich developed an algorithm to comb through all possible pairs of component failures in a power grid (for example, a downed transmission line, or a generator short-circuit), weeding out failures that don't result in any overloads and are unlikely to cause widespread damage, and certifying them as safe. The pairs that are left can be flagged as potentially dangerous.

On a qualitative level, the algorithm essentially identifies spheres of influence around a power failure. While every part of a grid responds in some way to a single failure, the intensity of the response centers on a few grid components, and may only be felt locally, within a single neighborhood, or local region. If two failures are relatively "close," spheres of influence can overlap, intensifying the response and

increasing the likelihood of a catastrophic cascade.

The algorithm essentially identifies all the pairs of failures that are separated by a reasonable distance where their effects would not overlap; the algorithm then certifies these pairs as safe.

The pairs that overlap in their local effects, however, are classified as potentially dangerous.

Reinforcing the weakest links

To test the algorithm, the researchers worked with data from the power grid of Poland—the largest grid of any power system where its data is publicly available. The country's electric grid consists of 3,000 components, making up nearly 10 million potential pairs of failures. In 10 minutes of regular laptop computations, the algorithm trimmed those pairs down to 5,000 that were of potential concern.

Turitsyn says grid operators may use such information to modernize the system and "reinforce the weakest links," designing sensors and communication technologies to improve system reliability and security. If two failures deemed to be dangerous do in fact occur, operators can shed the load in nearby regions or, for example, temporarily reduce the use of air conditioners, to provide some relief to the system and prevent a cascade of failures.

Understanding how vulnerabilities in a power grid arise is an intricate problem, says Daniel Bienstock, a professor of industrial engineering and operations research at Columbia University. Algorithms such as Turitsyn's, he says, are needed to help predict and prevent power failure cascades.

"This algorithm, if massively deployed, could be used to anticipate

events like the 2003 blackout by systematically discovering weaknesses in the power grid," Bienstock says. "This is something that the power industry tries to do, but it is important to deploy truly agnostic algorithms that have strong fundamentals."

In the future, Turitsyn plans to test the algorithm on large-scale system models, such as the power grid that supplies the northeastern United States, a system that consists of more than 100,000 components—up to five billion potential pairs of failures.

"The number of ways in which a grid can fail is really enormous," Turitsyn says. "To understand the risks in the system, you have to have some understanding of what happens during a huge amount of different scenarios."

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology