Algorithms could stop an 'internet of things' attack from bringing down the power grid

24 September 2019, by Molly Sharlach

Credit: CC0 Public Domain

Last year, Princeton researchers identified a disturbing security flaw in which hackers could someday exploit internet-connected appliances to wreak havoc on the electrical grid. Now, the same research team has released algorithms to make the grid more resilient to such attacks.

In a paper published online in the journal *IEEE Transactions on Network Science and Engineering*, a team from Princeton's Department of Electrical Engineering presented algorithms to protect against potential attacks that would spike demand from high-wattage devices such as air conditioners—all part of the "internet of things"—in an effort to overload the power grid.

"The cyberphysical nature of the grid makes this threat very important to counter, because a large-scale blackout can have very critical consequences," said study author Prateek Mittal, an associate professor of electrical engineering.

Computerized control systems have greatly increased power companies' ability to tune and efficiently manage electric grids. But they also have created vulnerabilities. Operators rely on computers forecasting electricity demand to change the activity of generators and transmission lines over the course of the day. They use similar systems to respond to weather conditions and other factors. A spike in demand caused by a coordinated attack on internet of things devices could trigger a reaction by automated scheduling systems that leads to transmission line failures and blackouts. And unlike other threats to the power grid, such an attack would not require the adversary to have specific knowledge of a grid's structure.

The researchers' proposed solutions aim to optimize responses to a spike, said lead author and postdoctoral research associate Saleh Soltan. One set of algorithms automatically balances power provided by plants in ways that would prevent a line from getting overloaded in the event of an attack. Another, less costly approach would allow the grid to quickly recover after a power failure, thus avoiding larger, more sustained outages. Soltan and Mittal developed the strategies with co-author H. Vincent Poor, interim dean of the engineering school and the Michael Henry Strater University Professor of Electrical Engineering.

In 2016, the Mirai "botnet" (named Mirai after a Japanese anime series) of more than half a million internet of things devices around the world was used to jam traffic to some major computer networks, making websites such as Twitter and Netflix temporarily inaccessible. The attack took advantage of the fact that most internet of things devices use default usernames and passwords, and led the Princeton team to consider what might happen if an adversary could manipulate power usage by gaining access to a botnet of high-wattage internet of things devices within a geographic area.

Controlling 600,000 high-wattage devices would

"give the adversary the ability to manipulate around 3,000 megawatts of power in an instant," said Mittal—equivalent to the output of a large nuclear power plant. If not managed at the local level, this type of overload could cause cascading power failures—potentially as disruptive as the Northeast blackout of 2003 and a blackout earlier this year in Argentina and Uruguay.

"As opposed to computer networks that have routing algorithms, in power grids there is no notion of routing, so everything is based on physics," said Soltan. "This is why you can't really prevent a certain line overload if you don't change the supply and demand."

The team's algorithms take into account the capacity thresholds of transmission lines and the power generation capabilities of a grid, and use this information to compute solutions that redirect power flows and adjust generator activities to prevent line failures. The researchers tested the performance and computed the operating costs of using these algorithms on the New England 39-bus system, a power grid test case that reflects the structures of real power grids.

The researchers said the algorithms do add some cost to grid operations in exchange for increasing the safety margin. For example, they found, using the algorithm IMMUNE (for "Iteratively MiniMize and boUNd Economic dispatch") could, for a cost increase of about 6%, make a power grid robust against an attack that increases demand by 9%.

"What kind of safety margin you need is really an operations question, but our approach has been to have a theoretical framework to answer all these questions," said Soltan. For grid operators, "it's a tradeoff between how much you increase the cost and how much robustness you have against these attacks."

The federal government has recognized the security risks posed by the increasing digitization of the power grid, as the U.S. Senate recently passed the Securing Energy Infrastructure Act to move toward adding redundant analog control systems.

However, "even if you disconnect your grid, even if you make it 100% analog, since the internet of things devices are digital you can still have these types of attacks," said Soltan. "In a few years we will need to think about these types of vulnerabilities."

"This is a typical example of security research: As the environment changes, previous assumptions no longer hold and new attack vectors are discovered," said Edgar Weippl, an information security specialist and research director of SBA Research in Vienna. "As everything becomes 'a computer,' much higher electrical loads can now be centrally controlled. In addition, a higher share of renewable energy might reduce backup kinetic energy in the grid." Weippl, who was not involved in the study, added that smart grids and smart meters could help mitigate risks by automatically shutting off compromised devices.

In the future, the Princeton team hopes to collaborate with utility companies "as a testbed for some of these algorithms," said Mittal. "There's always a gap between theory and practice that real-world testbeds will help expose."

This work was supported by the Siebel Energy Institute, the National Science Foundation and the Office of Naval Research Young Investigator Program.

More information: Saleh Soltan et al. Protecting the Grid against MAD Attacks, *IEEE Transactions on Network Science and Engineering* (2019). DOI: 10.1109/TNSE.2019.2922131

Provided by Princeton University