Scientists put forth a smarter way to protect a smarter grid

March 4 2024

Credit: Pixabay/CC0 Public Domain

There's a down side to "smart" devices: They can be hacked.

That makes the electric grid, increasingly chock full of devices that interact with one another and make critical decisions, vulnerable to bad actors who might try to turn off the power, damage the system or worse.

But smart devices are a big part of our future as the world moves more toward renewable energy and the many new devices to manage it. Already, such tools play a big role in keeping the power humming. The portion of the grid owned by utilities has thousands of devices that can be targeted, including transformers and generators. And then there are devices owned by customers, municipalities and others, such as solar panels and charging stations. With so many devices as well as an array of partners who have a stake in the grid, it's becoming more taxing than ever to prevent or stop every potential attack.

At the recent annual meeting of the Association for the Advancement of Artificial Intelligence in Vancouver, Canada, a team of experts at the Department of Energy's Pacific Northwest National Laboratory put forth a new approach to protect the grid.

The team, led by data scientist Sumit Purohit, is trying to leapfrog current practices and create a better level of protection. Instead of protecting the electric grid and its tens of thousands of components piece by piece, the team is creating a tool that sorts and prioritizes cyber threats on the fly. The idea is to give grid operators a clear blueprint to identify and address the biggest threats first and to protect against them without a mad scramble for resources down the road.

"A great deal of effort is put forth every day into addressing specific vulnerabilities, but that can be overwhelming," said Purohit. "We're putting forth a longer-term solution. What do you need to be looking at, not just today or tomorrow, but years down the road, as the grid is changing?

"It's important to deal with today's problems, but let's also think about tomorrow's challenges. We need to plan for things down the line as more smart devices like batteries, inverters, generators and hybrid cars are connected to the grid," Purohit added.

It's a bit like the difference between addressing ailments one at a time compared to embarking on decades of preventive health. A person might break a hip falling at home one year, end up in the ER with a bad case of pneumonia a few years later, and then have a heart attack. Of course, getting the best treatment for each condition is critical.

An alternate path is to map out the most critical wellness behaviors early on and to give those high priority throughout life. That might include staving off osteoporosis by eating a healthy diet and being active, receiving vaccines to prevent as much illness as possible, and avoiding smoking and eating less fat to keep the heart healthy.

Mapping cyberattack paths

The team's formula is based on a model known as hybrid attack graphs, a mathematical approach that is becoming more popular as the cyber and physical worlds become interconnected. The approach gives users flexibility to map out and follow multiple attack routes as they evolve and as defenders and attackers give and take ground. The team uses optimization and data from actual grid cyberattacks to train the model.

The project is one of hundreds of efforts at PNNL to improve artificial intelligence or apply it to address the nation's greatest challenges. The research led by Purohit is an example of work on energy resilience, an important mission area of the Center for AI @ PNNL.

The research draws on research previously done by MITRE Corp. that links high-level objectives of adversaries with the techniques they have used as well as ways to prevent attacks. But the framework does not include information about the "cost" to an organization, in terms of effort or money, to implement those protections. The PNNL team is trying to change that by addressing the cost of implementing solutions.

"This approach would allow a utility to quickly assess its cyber risk as they are planning their future grid expansion," said Purohit. "If you plan to connect more smart devices in the future, you need to be prepared to address the risks. There are thousands of ways to attack utility operations. By looking at historical events and using reinforcement learning, we have reduced that to fewer than 100 that need the most attention."

Data scientist Rounak Meyur, who worked on the project, added that "Our work aims not only to maximize available resources but also to consider what might need to be done to augment or improve existing capabilities."

A key part of the team's work is making sure the work is "explainable"—that grid operators and cyber analysts understand the reasons why the model prioritizes and makes the recommendations it does.

"If your favorite movies aren't recommended by a streaming service, and you don't understand why, that's inconvenient but not a real problem," said Purohit. "But grid operators must keep the power on, and they need to understand the reasoning behind every action they might take."

The team is working to improve the model and plans to work with power grid and cybersecurity experts to better measure the impacts of adversarial actions on cyber-physical systems.

PNNL researcher Braden Webb also contributed to the project. The research is part of a Laboratory project called Resilience through Data-driven, Intelligently Designed Control, where cybersecurity scientist Thomas Edgar and others are part of the effort.

"Right now, in some ways, keeping power flowing and keeping the grid

safe is more art than science," said Edgar. "Our approach is grounded in science and would help the utility know in a more definitive way where to invest to get the most bang for its buck in terms of protecting itself from attack."

Provided by Pacific Northwest National Laboratory