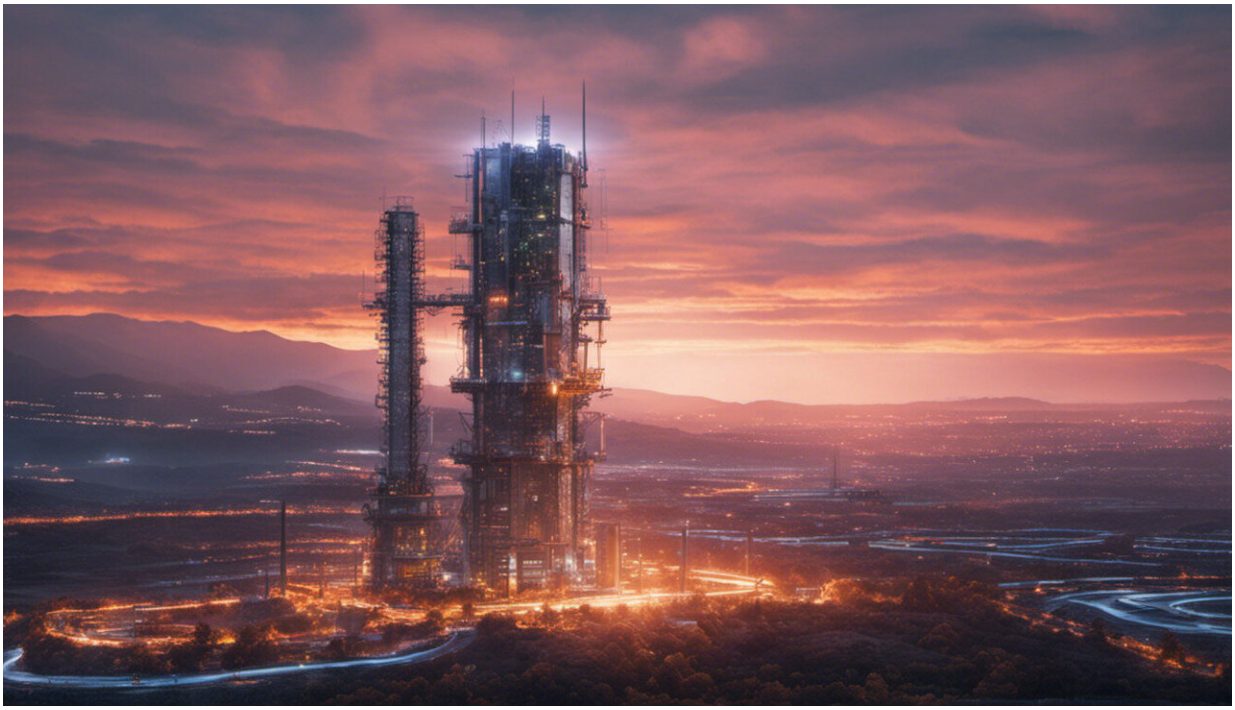
A beautiful defense for smart grids

November 2 2015



Credit: AI-generated image (disclaimer)

The physical infrastructure of the U.S. electric grid is aging, overburdened and vulnerable to natural hazards.

That's not the bad news.

The bad news is that efforts to solve these issues have opened the door to new vulnerabilities.

New approaches that transform how energy is produced, delivered and consumed have created increased reliance on complex data flows, interconnected systems and sophisticated technologies—i.e., the new smart grid.

But with smarter systems come equally smart hackers.

Cyberattacks can come in many forms, all with the real risk of physical harm to the system. This was demonstrated in the 2007 Aurora project, where a staged cyberattack revealed critical vulnerabilities in the power grid.

To stay one step ahead of cyberattacks, engineers and scientists funded by the National Science Foundation (NSF) are exploring innovative new ways to operate and secure the grid, using the tools of game and control theory.

Control at the periphery

The smart grid is evolving to look like a vast ant colony, with each node of the grid collecting and acting on its own measured data. While inconsequential in isolation, those individual actions can result in collective behavior that has profound effects on the power grid as a whole.

Smart meters, smart appliances, electric vehicles, and the increasing number of devices connected through the Internet of Things offer users and grid operators new opportunities to control the usage of power at a scale never seen before.

"Essential to the reliable operation of the grid is the need to balance supply and demand on a sub-second timescale," says Eilyan Bitar, a Cornell University engineer who designs algorithms for control of large-

scale systems. "Traditionally, we schedule supply to follow demand. There is, however, a considerable flexibility in demand that remains largely untapped. So, why not tailor demand to follow supply?"

For instance, in the U.S., the power grid is designed to operate at a frequency of 60 hertz. Deviations in frequency from this nominal value indicate an imbalance between supply and demand in the system.

Instead of relying entirely on large centralized generators to balance the system, your smart refrigerator could sense an imbalance between supply and demand by simply measuring the frequency of its local voltage.

If there is excess demand on the system, the refrigerator could automatically allow its its interior temperature to increase by a degree or two to decrease its energy use—not enough to spoil your milk, but enough to alleviate load on the system and save energy.

Multiple devices could be doing this simultaneously throughout your house and your neighbors' houses, creating a dynamic network of devices acting in concert.

This is what Bitar calls a "grid with an intelligent periphery."

Such a decentralization of control authority across millions of end-point devices would give rise to a far more efficient power grid and lessen the danger of a single catastrophic failure (natural or malicious) taking down the whole system; however, it also opens up more points of entry.

A beautiful defense

The most insidious type of cyberattack that researchers are looking to thwart is one in which grid operators may themselves be unwitting participants.

Within a power grid are natural fluctuations in energy: perturbations that seem normal.

Notably abnormal perturbations—those caused by lightning strikes or an equipment malfunction—are picked up by sensors. Controllers then adjust the energy flow accordingly, and all is well.

But what grid monitors worry about are perturbations that seem natural but aren't.

It's possible for malicious hackers to purposefully feed bad data to controllers, who may mistakenly believe the energy flow needs to be adjusted, essentially fooling the control system into disrupting its own state.

Cedric Langbort, a University of Illinois Urbana-Champaign engineer who uses game theory to develop secure control algorithms, says the challenge is that "you don't know what you don't know."

"Remember the movie about John Nash?" Langbort says, referring to the film A Beautiful Mind. "There's a scene where Nash and his friends discuss how if they all go for the same girl, no one will get the girl. But if they cooperate and know each other's strategies, they have a good chance of succeeding.

"My decision influences your outcomes and vice versa," he says. "It's basic Nash equilibrium."

For Langbort, cybersecurity is more than preventing hackers from getting into the system. He assumes a hacker will find a way in—especially in a system with more and more distributed entry points.

The challenge is how to detect those seemingly innocuous perturbations

and develop countermeasures for an attack in progress.

Theoretically, a hacker can meddle with information and influence decision-making without anyone ever realizing it. That's where game theory may come in handy.

"What I do affects what you get to know about the game," says Langbort. "That makes it more difficult because now there are things that you don't know that I know."

Those things can include whether the attacker has altered the sensor signals to provide incorrect measurements—maybe not enough to trigger an alarm about an "unnatural" perturbation, but enough so the controller unnecessarily adjusts the energy flow. Once that happens, the system is compromised.

Langbort is developing an algorithm that would help people make decisions when information is incomplete or even purposefully misleading.

"There is a lot of interest in cybersecurity right now," he says. "Because these are difficult, fundamental problems. These types of games that involve partial information are not well understood."

He is even playing both sides of the game in his research, setting up smart control systems and then trying to hack them. He's doing so to identify the weaknesses, as well as potential methods to exploit weaknesses, and use them to build a new control theory system.

Langbort, Bitar and other NSF-funded researchers are exploring vital issues that have immediate impacts tied to long-term implications for the power grid. With millions of new points of control, there is tremendous potential to improve efficiency and resiliency, and enormous need to

explore innovative methods to secure them.

Cybersecurity of control systems is one of the major research challenges in the smart grid, according to Radhakishan Baheti, program director for the Energy, Power, Control and Networks Program at NSF. "Future control systems will include cybersecurity as the design requirement to guarantee the resilience of power grids against cyber attacks," he said.

Provided by National Science Foundation