# New technology shows promise in detecting and blocking grid cyberattacks

20 July 2021

To demonstrate the ability of the Constrained Cyber Communication device to block a cyberattack on the power grid, researchers constructed a 36-foot long mobile substation and connected it to INL's full-scale Power Grid Test Bed. Credit: Chris Morgan, Idaho National Laboratory

Researchers from Idaho National Laboratory and New Mexico-based Visgence Inc. have designed and demonstrated a technology that can block cyberattacks from impacting the nation's electric power grid.

During a recent live demonstration at INL's Critical Infrastructure Test Range Complex, the Constrained Cyber Communication Device (C3D) was tested against a series of remote access attempts indicative of a cyberattack. The device alerted operators to the abnormal commands and blocked them automatically, preventing the attacks from accessing and damaging critical power grid components.

"Protecting our critical infrastructure from foreign adversaries is a key component in the department's national security posture," said Patricia Hoffman, acting assistant secretary for the U.S. Department of Energy. "It's accomplishments like this that expand our efforts to strengthen our electric system against threats while mitigating vulnerabilities. Leveraging the capabilities of Idaho National Laboratory and the other national laboratories will accelerate the modernization of our grid hardware, protecting us from cyberattacks."

The C3D device uses advanced communication capabilities to autonomously review and filter commands being sent to protective relay devices. Relays are the heart and soul of the nation's power grid and are designed to rapidly command breakers to turn off the flow of electricity when a disturbance is detected. For instance, relays can prevent expensive equipment from being damaged when a power line fails because of a severe storm.

However, relays are not traditionally designed to block the speed and stealthiness of a cyberattack, which can send wild commands to grid equipment in milliseconds. To prevent this kind of attack, an intelligent and automatic filtering technology is needed.

"As cyberattacks against the nation's critical infrastructure have grown more sophisticated, there is a need for a device to provide a last line of defense against threats," said INL program manager Jake Gentle. "The C3D device sits deep inside a utility's network, monitoring and blocking cyberattacks before they impact relay operations."

A picture of the Constrained Cyber Communication device (top) next to a power grid protective relay and a laptop running monitoring software. Credit: Chris Morgan, Idaho National Laboratory

Several members of the research team responsible for designing and testing the Constrained Cyber Communication device stand next to their invention. Credit: Chris Morgan, Idaho National Laboratory

To test the technology's effectiveness, researchers spent nearly a year collaborating with industry experts, including longtime partners from Power Engineers, an international engineering and environmental consulting firm. INL and the Department of Energy also established an industry advisory board consisting of power grid and cybersecurity experts from across the federal government, private industry and academia.

After thoroughly assessing industry needs and analyzing the makeup of modern cyber threats, researchers designed an electronic device that could be wired into a protective relay's communication network. Then they constructed a 36-foot mobile substation and connected it to INL's full-scale electric power grid test bed to establish an at-scale power grid environment.

With the entire system online, researchers sent a sudden power spike command to the substation relays and monitored the effects from a nearby command center. Instantly, the C3D device blocked the command and prevented the attack from damaging the larger grid.

The development of the device was funded by DOE's Office of Electricity under the Protective Relay Permission Communication project. The technology and an associated software package will undergo further testing over the next several months before being made available for licensing to private industry.

Provided by DOE/Idaho National Laboratory

APA citation: New technology shows promise in detecting and blocking grid cyberattacks (2021, July 20) retrieved 31 July 2021 from https://techxplore.com/news/2021-07-technology-blocking-grid-cyberattacks.html