Combination of old and new yields novel power grid cybersecurity tool

7 March 2018, by Kathy Kincade

Developed at Power Standards Lab under a project led by UC Berkeley and funded by the Department of Energy's ARPA-E program, µPMUs are designed to increase situational awareness at the power distribution grid level. Credit: Power Standards Lab

An innovative R&D project led by Berkeley Lab researchers that combines cybersecurity, machine learning algorithms and commercially available power system sensor technology to better protect the electric power grid has sparked interest from U.S. utilities, power companies and government officials.

Launched in 2015, the three-year project is now moving into the tech transfer stage, according to project lead Sean Peisert, a computer scientist in Berkeley Lab's Computational Research Division and a cybersecurity expert. In addition to receiving funding support from the Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) program in the Office of Electricity Delivery and Energy Reliability, the team has been working closely with key industry partners, including EnerNex, EPRI, Riverside Public Utilities and Southern Company.

"This project has, from the outset, been designed with technology transfer in mind," said Peisert. who is also chief cybersecurity strategist for CENIC and associate adjunct professor of computer science at the University of California, Davis. "We have sought input from equipment vendors and power utilities to help ensure that the techniques developed are grounded in reality and are more likely to be implemented and used in practice."

Enhancing Grid Resiliency

A more modernized electricity grid will result in better reliability and resilience and faster restoration of service when disruptions occur. Creating innovative tools and technologies to reduce the risk that energy delivery might be disrupted by a cyber incident is vital to making the nation's electric power grid resilient to cyber threats.

The power distribution grid was developed with careful consideration of ensuring safe and reliable operation; as the grid is modernized to further advance reliability, new features must be designed for cyber-resilience to prevent cyberattacks via IP networks. While IT security approaches developed for business systems to deal with malware and other cyberattacks include traditional intrusion detection systems, firewalls and encryption, these techniques may leave a gap in safety and protection when applied to cyber-physical devices because they do not consider physical information known about the device they are protecting.

To address this vulnerability, starting in 2014 Peisert and his collaborators—who include Ciaran

Roberts (Berkeley Lab), Anna Scaglione (Arizona State University), Alex McEachren (Power Standards Laboratory), Chuck McParland (Berkeley Lab retiree), and Emma Stewart (now with Lawrence Livermore National Laboratory)—embarked on a series of projects that take a unique approach to grid security by integrating traditional computer security and safety engineering techniques. Their ultimate goal was to develop a security monitoring and analysis framework that enhances resiliency of the grid system.

"The more we looked into this, the more we realized that the people responsible for computer security and the people responsible for safety engineering are often not in the same parts of the organization and very often do not talk to each other," Peisert said. "So we began to wonder if there was a way we could bridge the gap between the physical world and the cyber world, and the safety engineering world and the cybersecurity world, and create a single system in which the cybersecurity system takes into account the physics of the device and the physical limitations of that device."

Toward this end, their current project has focused on designing and implementing an architecture that can detect cyber-physical attacks on the power distribution system network. To do this they are using micro phasor measurement units (?PMUs) to capture information about the physical state of the power distribution grid. They then combine this data with SCADA (supervisory control and data acquisition, commonly used in electric grid monitoring) information to provide real-time feedback about system performance.

"The idea is if we could leverage the physical behavior of components within the electrical grid, we could have better insight in terms of whether there was a cyberattack that sought to manipulate those components," Peisert explained. "These devices provide a redundant set of measurements that give us a high-fidelity way of tracking what is going on in the power distribution grid, and either by looking at those measurements alone or by comparing those measurements to what the equipment itself was reporting and looking for discrepancies, we might have some indication of certain kinds of attacks against components in the power distribution grid."

Creating innovative tools and technologies to reduce the risk that energy delivery might be disrupted by a cyber incident is vital to making the nation's electric power grid resilient to cyber threats. Credit: US Department of Energy

?PMUs versus PMUs

Phasor measurement units (PMUs) are used to measure the electrical state of the power grid and provide situational awareness to transmission system operators. Typically installed at high-voltage substations, PMUs are considered an important measurement device in power systems, providing snapshots of the power network at a much higher rate than SCADA by calculating and reporting voltage and current phasors (a complex number that represents the magnitude and phase angle of the of sinusoidal waves that characterize AC electrical networks).

However, PMUs have some characteristics—namely size and cost—that limit their deployment at the distribution grid level. This is where ?PMUs come in. Developed at Power Standards Lab under a project led by UC Berkeley and funded by the Department of Energy's ARPA-E program, ?PMUs are designed to increase situational awareness at the distribution level. Because they are much

smaller and potentially less expensive, multiple ?PMUs can be deployed at points along the distribution grid, providing a much higher resolution (120 measurements/sec) of the grid and alerting operators to potential attacks on that grid in real time.

"Our approach—which actually uses only a small number of sensors—utilizes both SCADA and ?PMU measurements, and there is incredible value in being able to cross-check between the two to look for discrepancies," Peisert said. "Individually it might be possible for an attacker to manipulate what is being represented by any single sensor or source of information, which could lead to damage of the power grid. This approach provides the redundancy and therefore resilience in the view that is available to grid operators."

Machine Learning Aids Detection

To make this happen, the research team employed a modified version of the Cumulative Sum (CUSUM) algorithm, first introduced in 1954, for sequential analysis of the data and automated anomaly detection. The result is, in essence, a form of machine learning.

"The algorithm enables the software to adaptively learn the normal behavior of the quantities being measured, and through that process learn to identify abnormal and normal behavior by detecting fast changes in the physical environment, such as current magnitude and active and reactive power," said Berkeley Lab's Roberts, an energy systems engineer in the Energy Technologies Area. "All the computing is done in real time during the physical data collections, and the algorithms are designed to run in real time."

At present data is being collected from ?PMUs placed in multiple locations around Berkeley Lab (which has its own power distribution substation) and analyzed using a compute cluster and a web presence (powerdata.lbl.gov) the team set up specifically for this project.

"We had to build our own infrastructure to collect all the sensor data in a single place and run the algorithms over it to determine if there was an event of interest," Peisert said. "And we have graphical front-ends to that system that can be used by the broader research community as well."

As the R&D component of this project winds down, the team is preparing its final report and actively meeting with their industry partners and other utilities and power companies across the U.S. to introduce them to this unique grid security framework. They are also sharing their findings through presentations at events such as the EPRI Power Delivery & Utilization Winter 2018 Program Advisory & Sector Council Meeting, held in February in San Diego, and the OSIsoft PI World Users Conference in April.

"Using high resolution sensors in the power distribution grid and a set of machine learning algorithms that we have developed, in conjunction with only a simple model of the distribution grid, our work can be deployed by utilities in their distribution grid to detect cyberattacks and other types of failures in the grid," Peisert said. "That's a novel accomplishment that we don't think has been done before."

Provided by Lawrence Berkeley National Laboratory