Researchers protecting solar technologies from cyberattack

March 28 2022, by Mike Wooten

Wenzhan Song stands in front of a large solar panel. Credit: Dorothy Kozlowski/UGA

New research from the University of Georgia suggests a novel approach to safeguarding one possible target of a cyberattack—the nation's solar

farms. In a study published in *IEEE Transactions on Smart Grid*, a team in UGA's College of Engineering introduced a sensor system that monitors a key electrical component of solar farms for signs of cyber-intrusion in real time.

"A growing concern is that hackers may exploit the converters that connect solar farms with the power grid," said WenZhan Song, the Georgia Power Mickey A. Brown Professor in Engineering and the study's lead investigator. "In modern grid-connected solar farms, power electronics converters can be remotely controlled, but this internet connection also expands the potential for cyberattacks."

In general, power electronics use semiconductor switching devices to control and convert electrical power flow from one form to another. This technology has revolutionized modern life by streamlining manufacturing processes, increasing product efficiencies and improving the delivery of reliable power from utilities.

At a solar farm, power electronics devices convert direct current (DC) electricity generated by solar photovoltaic panels into alternating current (AC) electricity for use on the electrical grid. The U.S. Department of Energy estimates up to 80% of electricity could flow through power electronics devices by 2030.

To protect against cyber threats, the UGA researchers developed a system that can detect anomalies in a power electronic converter's operations in real-time using only one voltage sensor and one current sensor. Coupled with deep learning methods, the system can distinguish between normal conditions, open-circuit faults, short-circuit faults and cyberattacks.

"To our knowledge, this has not been attempted before," said Song.

A small, passive sensor device connected to the power converter collects data on electrical waveforms and feeds the information to a computer monitor. Even if an attack eludes the firewall or security software, the sensors would detect unusual activity in the electrical current of the power electronics device. The system also can run diagnostic tests to determine what type of problem has occurred.

"At your home, the power meter typically takes a reading once every 15 minutes," said Song. "Our system is taking 10,000 samples every second."

Compared to existing detection methods that only detect abnormal waveforms, the UGA researchers say their system proved more adept at identifying cyberattacks in testing using a solar farm model. The researchers also say their system can identify new types of cyberattacks that haven't been programmed into deep learning algorithms.

The researchers have filed a U.S. patent application for their approach, noting the sensor system could provide protection against cyberattacks for manufacturing systems, office buildings and even smart homes.

More information: Lulu Guo et al, Data-Driven Cyber-Attack Detection for PV Farms via Time-Frequency Domain Features, *IEEE Transactions on Smart Grid* (2021). DOI: 10.1109/TSG.2021.3136559

Provided by University of Georgia