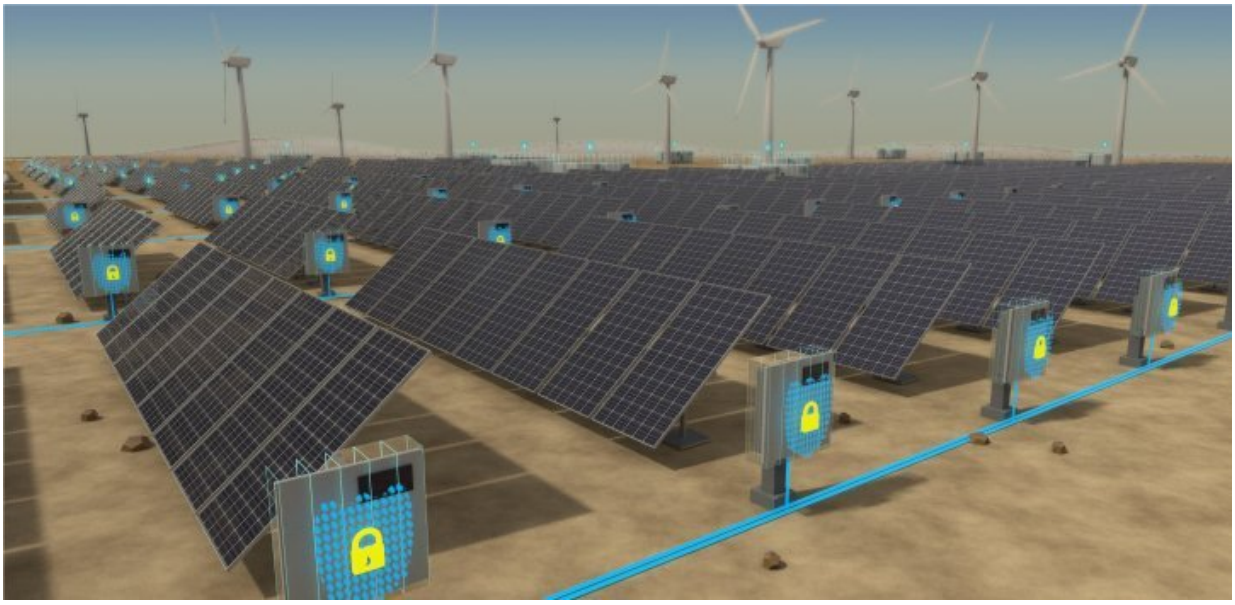
Simple hardware to defend against microgrid attacks

November 25 2022



Small-scale renewable energy systems can be vulnerable to cyberattacks. A team of KAUST researchers has devised a method to protect this critical infrastructure using low-cost hardware-based malware detection mechanisms. Credit: KAUST; Heno Hwang

An inexpensive piece of hardware integrated with solar panel controllers can protect isolated power networks from cyberattacks.

One advantage of small-scale renewable energy systems is that they can be arranged into networks that operate independently of the main

electric grid when required. Now, researchers at KAUST are developing ingenious ways of protecting these networks, known as microgrids, from cyberattacks.

"Microgrids are small 'power islands' that can provide electricity for critical services, such as health care, food and water, during emergencies," explains Ioannis Zografopoulos, who conducted the research with Charalambos Konstantinou at KAUST and co-workers at the University of Texas at Dallas, U.S. However, the relative simplicity and isolation of microgrids makes them attractive targets for cyberattacks aimed at disrupting communities.

In their latest efforts to improve microgrid security, the team employed hardware performance counters (HPCs)—special registers that are embedded within most computers to monitor events, such as how many times a certain command has been performed.

"HPCs were originally used for profiling purposes or to identify bottlenecks within code," says Zografopoulos. "However, we have utilized HPCs to detect code patterns that indicate the execution of malicious code on our devices: specifically, the embedded controllers of solar inverters that convert the output of solar photovoltaic panels into usable power for consumers."

The controllers in solar inverters do not come equipped with HPCs, for cost reasons. Zografopoulos and co-workers developed tailor-made HPCs that were able to monitor the commands occurring within the inverters, without interfering in their main job of converting solar energy to electricity. Crucially, the team added an extra layer of security by including time series classifiers; these are algorithms that correlate potentially malicious combinations of commands with the time sequence of HPC firing events.

"We can detect malware in inverter controllers with over 97 percent accuracy using a classifier trained on just a single custom-built HPC," says Zografopoulos. "This meets our original objective for a low-cost and low-complexity defense countermeasure."

The team also simulated malware attacks on a replica of the Canadian urban distribution system, containing four inverter-based distributed generators. Their HPC system was able to detect voltage, current and frequency instabilities that could lead to equipment damage or electricity interruptions.

"The main takeaway from our study is that embedded controllers can be equipped with hardware-based malware detection mechanisms (HPCs) that do not add complexity or require additional computational resources," says Zografopoulos. "The facilities at KAUST enabled us to evaluate our methodology in the lab using actual inverter controllers and simulate the potential impacts of cyberattacks."

The findings are published in *Energy Reports*.

More information: Ioannis Zografopoulos et al, Time series-based detection and impact analysis of firmware attacks in microgrids, *Energy Reports* (2022). DOI: 10.1016/j.egyr.2022.08.270

Provided by King Abdullah University of Science and Technology