Blocking microgrid cyberattacks to keep the power flowing

February 10 2022

Charalambos Konstantinou (left) and Ioannis Zografopoulos (right) are developing effective methods to increase the resilience of power grids to cyberattacks. Credit: KAUST

Power grids have become far more complex in recent decades due to

energy demands, environmental regulations and small-scale renewable energy systems that turn businesses and individuals into combined consumer-producers. One way to ensure that power supplies remain resilient is to create small groups of sources and loads called microgrids. Microgrids can operate independently of the main grid when required, such as supporting hospitals during natural disasters, for example.

As microgrids grow more complex, they require sophisticated computer networks to coordinate, control and distribute different sources of power. Like any network, they are vulnerable to cyberattacks. To prepare for such events, KAUST researchers have been running simulations of possible attacks, assessing the impact that they might have and developing methods to detect and suppress malicious behavior.

"The microgrid system that we considered was the Canadian urban distribution model, comprised of four inverter-based distributed generations (DGs)," says Ph.D. student Ioannis Zografopoulos, who worked on the project alongside Charalambos Konstantinou, assistant professor of computer science. "The Canadian model is ideal to effectively capture the system dynamics and interdependencies between the four DGs and exhibit how a malicious event affecting one DG can propagate to the rest of the system."

While previous studies into microgrid attacks assumed that attackers have a good knowledge of the power grid's internal components and structure, Zografopoulos and Konstantinou took a more realistic approach. Instead, they adopted a model where the attacker has limited knowledge but is able to design attacks based on historical measured data about the grid's performance.

The researchers considered three different types of attack. Zografopoulos explains, "the first scenario involved altering the measurement data that the microgrid system operator uses to coordinate

the power generation of the DGs, the second involved modifying the control signals that regulate power conversion within the DG controllers, while the third involved sudden changes in load, causing grid instabilities."

The simulations showed that all three scenarios could have damaging effects that cascade through the power system, inducing large costs, power losses and damage to equipment. However, the researchers also identified effective methods to quickly and accurately detect the anomalous conditions associated with an incoming attack.

"Our future work will focus on identifying disruptive events and mitigating them via the preventive isolation of microgrid subsystems, safeguarding their crown-jewel components," says Zografopoulos. "We envision that our contributions will pave the way for resilient microgrids, automating the detection of attacks and supporting defensive and self-healing strategies."

More information: Ioannis Zografopoulos et al, Detection of Malicious Attacks in Autonomous Cyber-Physical Inverter-Based Microgrids, *IEEE Transactions on Industrial Informatics* (2021). DOI: 10.1109/TII.2021.3132131

Provided by King Abdullah University of Science and Technology