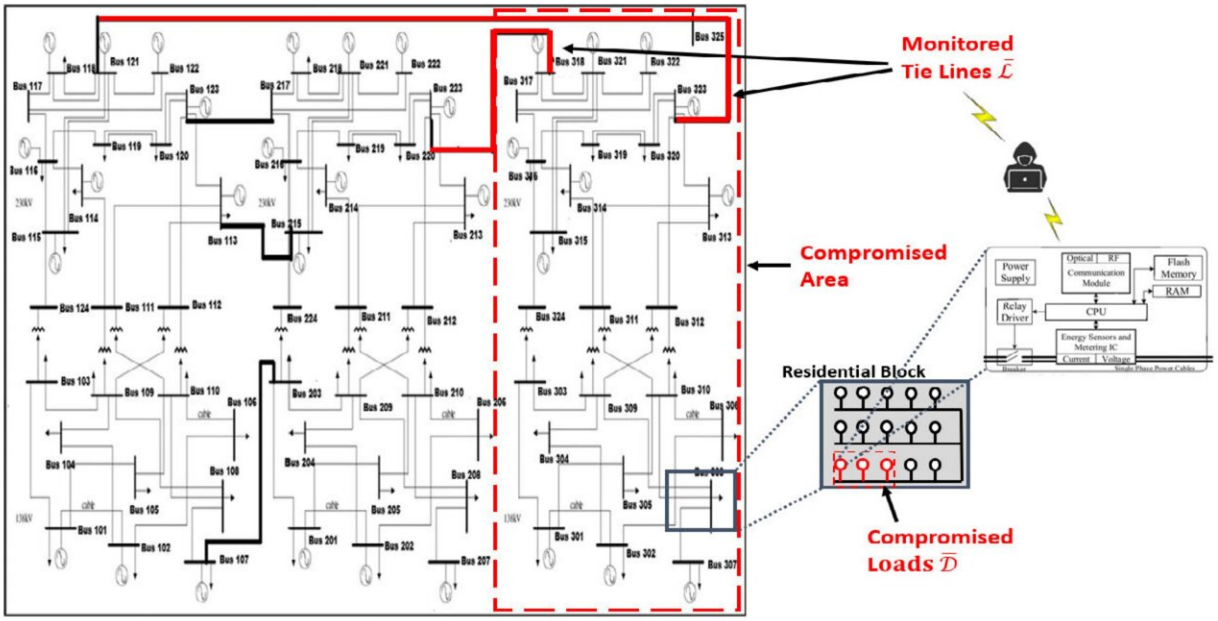
Research shows how hackers can target smart meters to destabilize electricity grid

May 3 2023, by Steve Lundeberg



Adapted IEEE RTS-96 bus system and its smart meter components. Credit: *IEEE Access* (2023). DOI: 10.1109/ACCESS.2023.3266249

A power transmission grid can be destabilized by hackers who manipulate smart meters to create an oscillation in electricity demand, researchers in the Oregon State University College of Engineering have shown.

Findings were published in *IEEE Access*.

The study is important because understanding where a grid's vulnerabilities lie and what they look like is the first step in designing protection mechanisms, says associate professor of electrical engineering and computer science Eduardo Cotilla-Sanchez, who led the project with graduate student Falah Alanazi.

A smart meter is a digital device that collects electricity usage data and sends it to a local utility through a telecommunications connection. The meters can help customers learn more about their electricity use, and they can also be used to remotely shut off customers' power, such as in the case of unpaid bills.

Like circuit breakers in a household panel, power grid components can "trip" and shut off when demand, or load, is too high or problematic for some other reason. The result is load being passed on to other parts of the grid network, which may also shut down, creating the possibility of a domino effect that can lead to a blackout.

In this study, conducted with OSU College of Engineering associate professor Jinsub Kim, researchers used a model known as a time-domain grid protection simulator to demonstrate how causing load to vary back and forth in a regular pattern—known as a load oscillation attack—can compromise transmission.

"New technologies have been introduced to make our aging electricity infrastructure more efficient and more reliable," Cotilla-Sanchez said. "At the distribution level, upgrades have included communication systems, distribution automation, local control and protection systems, and advanced metering infrastructure. The bad news is, the upgrades also introduce new dimensions for attacking the power grid."

One of the types of attacks made possible by the new technologies involves hacking into the advanced metering infrastructure, often

abbreviated as AMI, and controlling the smart meter switches to cause load oscillations.

"Imagine calling everyone you know and saying, 'OK, at 6 p.m. we are all going to turn the lights on," Cotilla-Sanchez said. "Even if you got a couple thousand people to do that, it would be unlikely to cause much instability because the grid is able to absorb fairly big changes in supply and demand—for example solar panels at the end of the day do not produce electricity and we are able to anticipate and compensate for that.

"But if a person were to remotely coordinate a large number of smart meters to switch customers on and off at a particular frequency, that would be a problem."

That type of incident would start with someone performing reconnaissance by "poking" a couple of locations in a grid and using the information gained to estimate the grid's destabilizing oscillation frequency, he said. After determining which customer meters to turn on and off at that frequency—less than 1 Hertz or cycle per second—the attacker would be ready to launch an assault.

And comparatively speaking, an attack doesn't need to involve that many meters.

"We juxtaposed our work with related recent grid studies and found that a well-crafted attack can cause grid instability while involving less than 2% of the system's load," Cotilla-Sanchez said.

The findings, while unsettling, provide a jump-off point for grid operators to develop countermeasures, he added.

"For example, if they detect this type of oscillation on the load side, they

could take lines A and B out of service, intentionally islanding the affected area and thus avoiding propagation of the instability to a broader area of the grid," he said.

"Another solution, which could be complementary, might be to change the generation portfolio enough—for example, curtail some wind generation while ramping up some hydro generation—so the overall dynamic response is different to what the attack was designed toward, so the impact will be smaller and won't be enough to tip the system."

Either technique, he said, will require additional research and development to serve as an effective mechanism of protection, "but understanding the nature of possible attacks I would say is a good start."

More information: Falah Alanazi et al, Load Oscillating Attacks of Smart Grids: Vulnerability Analysis, *IEEE Access* (2023). DOI: 10.1109/ACCESS.2023.3266249

Provided by Oregon State University