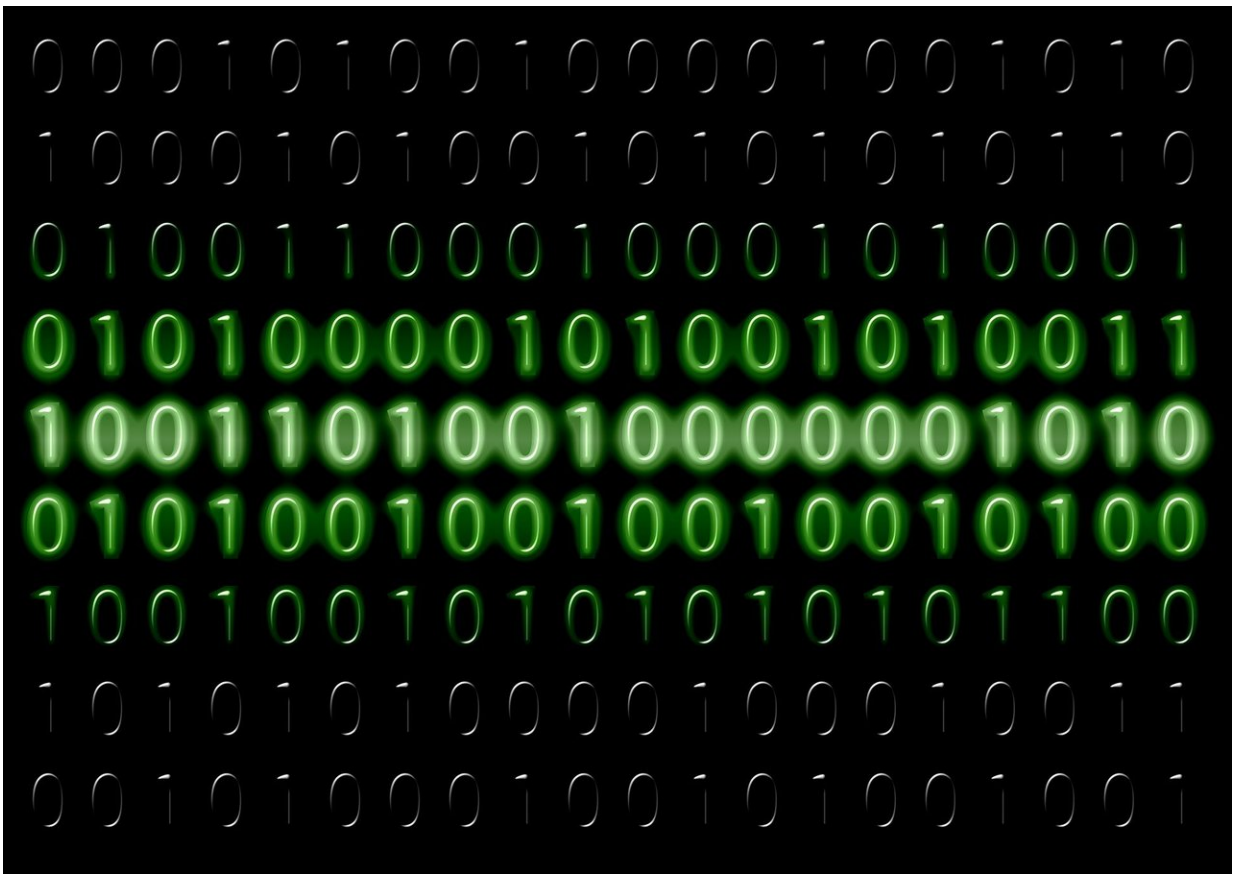
Team suggests a way to protect autonomous grids from potentially crippling GPS spoofing attacks

July 20 2018, by James Badham



Credit: CC0 Public Domain

Not long ago, getting a virus was about the worst thing computer users

could expect in terms of system vulnerability. But in our current age of hyper-connectedness and the emerging Internet of Things, that's no longer the case. With connectivity, a new principle has emerged, one of universal concern to those who work in the area of systems control, like João Hespanha, a professor in the departments of Electrical and Computer Engineering, and Mechanical Engineering at UC Santa Barbara. That law says, essentially, that the more complex and connected a system is, the more susceptible it is to disruptive cyber-attacks.

"It is about something much different than your regular computer virus," Hespanha said. "It is more about cyber physical systems—systems in which computers are connected to physical elements. That could be robots, drones, smart appliances, or infrastructure systems such as those used to distribute energy and water."

In a paper titled "Distributed Estimation of Power System Oscillation Modes under Attacks on GPS Clocks," published this month in the journal *IEEE Transactions on Instrumentation and Measurement*, Hespanha and co-author Yongqiang Wang (a former UCSB postdoctoral research and now a faculty member at Clemson University) suggest a new method for protecting the increasingly complex and connected power grid from attack.

The question that arises in any system that incorporates many sensors for monitoring is, what if someone intercepts the communication between two sensors that are trying to assess the health of the system? How does the system know not to believe—and act on—the false information?

Hespanha explained, "In the power grid, you have to be able to identify what the voltage and the current are at specific, highly precise points in time" for multiple points along the grid. Knowing the speed at which electricity moves, the distance between sensors, and the time it takes an oscillation to move between sensors, one can determine whether the

oscillation is real.

Making these precise, high-resolution measurements anywhere in the grid is possible through the use of phase measurement units (PMUs)—devices that are aligned with the atomic clocks used in GPS. With the energy grid becoming increasingly distributed, power providers now have to monitor the system more, and PMUs are among the most important devices for doing so. While PMUs could be used to inform autonomous control systems, so far, they have seen limited use for one simple reason: they are vulnerable to GPS spoofing attacks.

"There is the possibility," Hespanha said, "that someone will hack the system and cause a catastrophic failure."

The attack could be as simple as someone taking a GPS jammer to a remote power-distribution station and tricking the system into providing false measurements, leading to a cascade effect as false readings ripple through the system and incorrect actions are taken. Since it is virtually impossible to prevent a hacker from getting close enough to a remote substation to jam its GPS, Hespanha said, "What you need is a control system that can process the information to make good decisions. The system has to keep hypothesizing that what it is reading is not real."

How It Can Work

"The power-supply system is a distributed system, so measurements are being made in many places," Hespanha explained. "If one of them starts to give erratic or unexpected measurements—a sudden current surge or a voltage drop—you should be able to determine whether those measurements make sense."

In the case of an actual fluctuation, such as when many people in Los Angeles are using their air-conditioning on a hot summer day, the result

may be a slight drop in the alternating-current frequency in the city. That drop creates a disturbance which propagates along the power grid stretching from western Canada south to Baja California in Mexico and reaching eastward over the Rockies to the Great Plains. As the disturbance travels through the grid, the power stations that feed the grid try to counteract it by generating extra power if the frequency is too low or decreasing production if the frequency becomes too high.

"You're going to start by seeing oscillation on the grid," Hespanha explained. "That's exactly what the PMUs are looking for. You then compare the precise time you saw the disturbance in Los Angeles to the time you saw it in Bakersfield and then at other sensors as it continues north. And if those readings don't reflect the physics of how electricity moves, that's an indication something's wrong. The PMUs are there to see oscillations and to help dampen them to prevent them from developing."

But, if someone fooled an automated system, instead of damping the oscillations, the PMUs could create them instead.

So how would such an attack be recognized and stopped? To illustrate, Hespanha draws an electrical line running between Los Angeles and Seattle, with many smaller, ancillary lines running off to the sides. "If power is going in a certain direction, you should also be able to see any oscillation in the side lines in that direction. And you know the physical model of what things should do, so an attacker who changed the measurement on the main line would also have to mess up a lot of other measurements on the side lines along the way. And that would be very difficult."

Testing suggests that Hespanha's system would be resistant to attack and remain effective even if one-third of the sensor nodes were compromised. "That would allow for a much more autonomous system;

that's the next big step," said Hespanha. "This is an enabling technology that will be needed to make a lot of this control come online. And it will be needed soon, because the system gets more complex all the time and is therefore more susceptible to attack."

More information: Yongqiang Wang et al. Distributed Estimation of Power System Oscillation Modes Under Attacks on GPS Clocks, *IEEE Transactions on Instrumentation and Measurement* (2018). DOI: 10.1109/TIM.2018.2801018

Provided by University of California - Santa Barbara