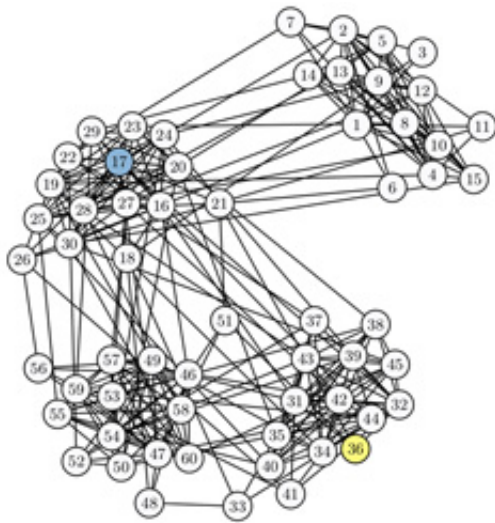# Researchers test distributed computing as defense against cyberattacks on power grids

May 21 2014, by Matt Shipman, North Carolina State University

This schematic diagram of a small power system network highlights the complexity of the grid. Credit: Aranya Chakrabortty

(Phys.org) —Imagine a cyberattack that does serious damage to the U.S. power grid. The results wouldn't be pretty.

The power grid is complicated, divided up into sections that cover everything from a single municipal area (like New York City) to large regions (like the entire state of California). But each of those sections is controlled by a single control center, which monitors the behavior of its piece of the grid to make sure things are operating normally, and makes whatever adjustments are necessary to keep the system running

smoothly.

But if that control center stops functioning, because of a cyberattack or for any other reason, it is no longer capable of monitoring and maintaining the grid. And that may result in severe instabilities in the system.

But a team of researchers from around the U.S. is working to address this and other power grid security concerns as part of the SmartAmerica Challenge, which kicked off in late 2013 to highlight U.S. research in the field of cyberphysical systems.

The Smart Energy Cyber-Physical Systems (Smart Energy CPS) team is focused on using sophisticated tools to test various scenarios (and solutions) related to cybersecurity in power grids. The Smart Energy CPS team includes researchers from NC State University, General Electric, Iowa State University, MITRE Corporation, National Instruments, NREL, Penn State, Scitor Corporation, UNC-Chapel Hill (UNC), and the University of Southern California (USC).

Because having a single control center for each section of the grid creates a significant vulnerability threat, the NC State and UNC group within the Smart Energy CPS team is pursuing the idea of creating a distributed computing system that would disseminate monitoring and control functions across multiple virtual machines in a cloud computing network that overlays the grid.

"The advantage here would be that if one element of the computing system gets compromised, the other virtual machines could step in to protect the system and coordinate their efforts to keep the grid functioning," says Aranya Chakrabortty, an assistant professor of electrical engineering who is leading the project from NC State. "We are working with USC's Information Sciences Institute to test this

distributed computing concept.

"Our early tests indicate that the distributed computing approach would make the grid more resilient against both physical attacks and cyberattacks," Chakrabortty adds. "Our next step is to scale up the collaboration to get more detailed analyses of different types of attacks. The more we understand about our potential vulnerabilities, the better controllers we'll be able to design to protect our infrastructure."

Chakrabortty says that NC State has extensive experimental resources for simulating the behavior of real-world power systems, but adds that "we're power systems experts, not cybercommunication experts. USC has a large testbed for emulating cyberattacks. By integrating our models with theirs, we can carry out more realistic scenarios." The team also includes Yufeng Xin of the Renaissance Computing Institute at UNC.

Provided by North Carolina State University

Citation: Researchers test distributed computing as defense against cyberattacks on power grids (2014, May 21) retrieved 18 April 2024 from https://phys.org/news/2014-05-defense-cyberattacks-power-grids.html