

'Digital ants' seek viruses to protect computer networks

May 30 2011

As the nation's electrical power grid becomes more interconnected through the Internet -- from the nuclear power plant in California to transmission lines in Texas to the microwave in your kitchen -- the chances of cyber attacks increase as well. Errin Fulp, a professor of computer science at Wake Forest University, is training an army of "digital ants" to turn loose into the power grid to seek out computer viruses trying to wreak havoc on the system.

If the approach proves successful in safeguarding the [power grid](#), it could have wide-ranging applications on protecting anything connected to SCADA (Supervisory Control and Data Acquisition) networks, computer systems that control everything from water and sewer management systems to mass transit systems to manufacturing systems.

Fulp is working this summer with scientists at Pacific Northwest National Laboratory (PNNL) in Richland, Wash., on the next steps in the digital ants technology, developed by PNNL and Wake Forest over the last several years. The approach is so promising that it was named one of the "ten technologies that have the power to change our lives," by Scientific American magazine last year.

The power grid is probably more vulnerable to [cyber attacks](#) than security experts would like to admit, said Fulp, an expert in security and computer networks. As the grid becomes more and more interconnected, it offers hackers more points to enter the system; for instance, inserting a virus or computer worm into a low security site, such as in your home's smart grid, to gain access to more secure systems up the line.

"When that network connects to a power source, which connects to the smart grid, you have a jumping off point" for [computer viruses](#), he said. "A [cyber attack](#) can have a real physical result of shutting off power to a city or a [nuclear power plant](#)."

The digital ants technology could transform cyber security because it adapts rapidly to changing threats, said Fulp, who has received nearly \$250,000 in grants from PNNL/Battelle Memorial Institute for his ongoing research.

Unlike traditional security approaches, which are static, digital ants wander through computer networks looking for threats such as [computer worms](#), self-replicating programs designed to steal information or facilitate unauthorized use of computers. When a digital ant detects a threat, it summons an army of ants to converge at that location, drawing the attention of human operators to investigate.

"The idea is to deploy thousands of different types of digital ants, each looking for evidence of a threat," Fulp said. "As they move about the network, they leave digital trails modeled after the scent trails ants in nature use to guide other ants. Each time a digital ant identifies some evidence, it is programmed to leave behind a stronger scent. Stronger scent trails attract more ants, producing the swarm that marks a potential computer infection."

The concept has proven successful in testing on a small scale, but will it still work when it's scaled up to protect something as large and complex as the nation's power grid? Fulp and two of his students -- computer science graduate students Michael Crouse and Jacob White -- are working this summer with scientists at PNNL and from the University of California at Davis to answer that question. But even using PNNL's vast computer platforms, they can only rely on computer simulations to predict the ants' "behavior" up to a point.

That's where Fulp's colleague, Ken Berenhaut, an associate professor of mathematics at Wake Forest and an expert in mathematical modeling and simulation, comes in. Berenhaut, along with Wake Forest graduate student Ross Hilton, will use modeling to help determine what will happen as the ants move about the smart grid from the hot water heater in your house to the electrical substation to the power plant.

Among the questions to be answered: How do the ants migrate across different computer platforms and systems operating at different speeds? How many ants should you have patrolling a system? How long do they live? How do the ants scale up to identify a threat and then ramp back down?

"In nature, we know that [ants](#) defend against threats very successfully," Fulp said. "They can ramp up their defense rapidly, and then resume routine behavior quickly after an intruder has been stopped. We're trying to achieve that same framework in a computer system."

Provided by Wake Forest University

Citation: 'Digital ants' seek viruses to protect computer networks (2011, May 30) retrieved 24 April 2024 from <https://phys.org/news/2011-05-digital-ants-viruses-networks.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.