U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector

A lightweight, decentralized, mobile agent-based approach to enhance cybersecurity in the Smart Grid

Background

Energy delivery systems face unique threats and challenges as greater numbers of smart grid technologies are adopted and deployed. Smart grid technologies must be protected from cyber threats that aim to disrupt or deny the use of key energy delivery system components. Coordinated attacks that exploit previously unknown vulnerabilities (so called "zero-day") may be used against a large number of smaller devices (such as smart meters) in an attempt to manipulate the grid maliciously. In addition, the legacy grid will still be operational for many years and must also be protected against advanced and evolving cyber attacks.

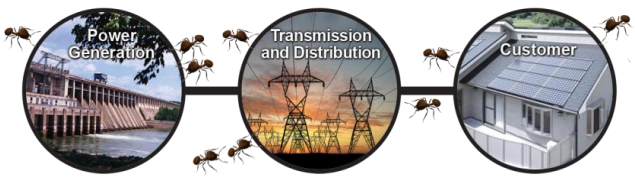
Barriers

- Electric sector system architectures are complex and widely distributed across multiple entities
- Cybersecurity solutions must not introduce latency issues
- Electricity delivery systems are costly to install and replace and therefore have long lifetimes
- Cybersecurity solutions must accommodate the often limited computing resources of legacy control systems

Project Description

This project will demonstrate that Digital Ants (a biologically-inspired solution developed by the Pacific Northwest National Laboratory) can be successfully deployed across multiple organizational and technological boundaries found in smart grid architectures to correlate activities, produce emergent behavior, and draw attention to anomalous conditions that indicate a potential cyber incident. The project will address component-level and "zero-day" threats. It will also develop a lightweight and dynamic framework that can operate on both legacy and smart grid systems.

The Digital Ants architecture will use swarm intelligence to identify potential cyber threats. Digital Ants will wander through computer networks and will leave digital trails whenever they find evidence of an anomaly or threat. The digital trails will attract additional Ants to the same location, their collective emergent behavior alerting operators of a potential cyber incident.

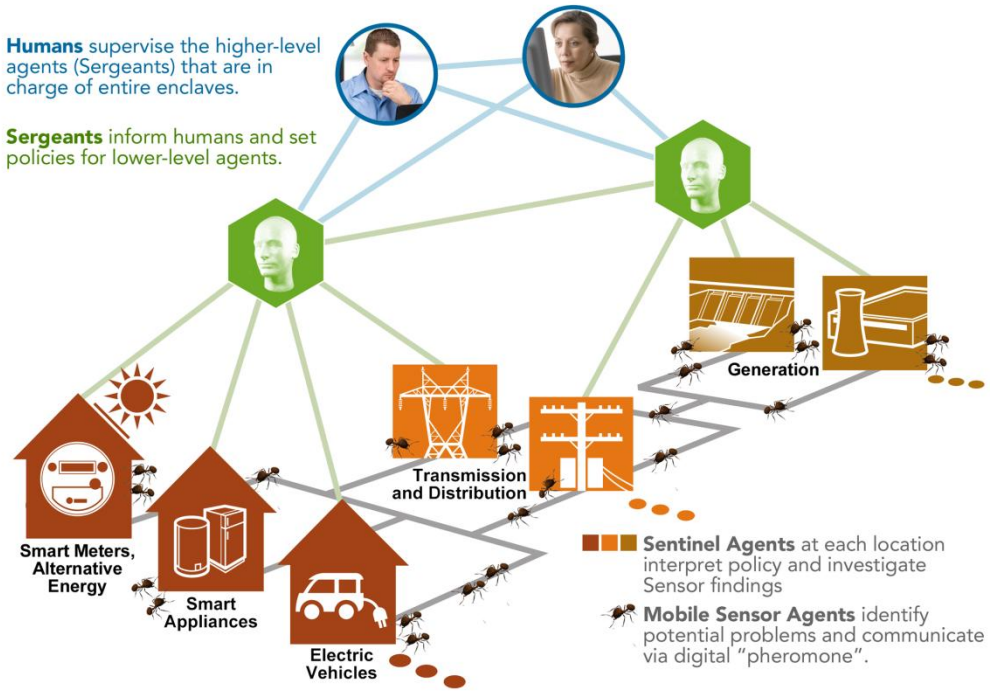


Benefits

- Adapts rapidly to changing threats
- Supports legacy devices and systems
- Enables lightweight, mobile agents (Digital Ants) to move across multiple organizational boundaries
- Discovers anomalies and provides feedback as to whether the anomaly is concentrated at a key system component or widely distributed across a large system and multiple entities
- Scales well for use in large and complex networks

Partners

- Pacific Northwest National Laboratory
- Wake Forest University
- Argonne National Laboratory
- SRI International



Technical Objectives

This project will adapt Digital Ants to the unique constraints and cyber threats of the smart grid while developing an approach for identifying Digital Ant signatures, learning rates and appropriate support hierarchies for use within the smart grid.

Phase 1: Research and Development

- Engage the subject matter expert community to validate the need for this new approach
- Adapt the Digital Ant infrastructure to support as much of the legacy electric power grid as feasible
- Design a reference implementation of smart grid-aware Digital Ants
- Test the proposed implementation both with laboratory-based experiments and embedded operational security assessments

Phase 2: Demonstration

- Evaluate Digital Ants in real hardware and in large-scale simulation environments:
  - Simulations in a GridLAB-D™ test bed will focus on energy delivery factors
  - Additional simulations in the cyber-Defense Technology Experimental Research laboratory (DETERlab) test bed will focus on information technology and networking factors
- Gather metrics from simulations and demonstrations using smart grid models and scenarios

End Results

Project results will include:

- More rapid identification of potential cyber threats
- A decentralized approach to cybersecurity that still allows for human control and interpretation
- Enhanced cybersecurity for legacy systems
- A scalable solution for use in large and interconnected smart grid systems

Content last updated: August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

David McKinnon
Senior Research Scientist
Pacific Northwest National Laboratory
509-375-3968
david.mckinnon@pnnl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov