U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Secure Time-Critical Communications

SEEDS
CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Assessing the resilience of time-critical communications in electric substations to cyberattacks

Critical control messages in electric substations need to be delivered extremely fast. Such communications are vulnerable to flooding attacks that can delay messages. The team is experimentally studying how flooding attacks affect the delivery of time-critical messages protected by commonly used authentication schemes in wireless and wired networks. The team has discovered that a practical intelligent attack can significantly increase the delivery delay in a wired network with a very small number of attack packets. Building on this discovery, the team is developing a scheme to detect intelligent, delay-increasing attacks. This scheme will be integrated into a detection tool that will be implemented and tested.

KEY TAKEAWAYS

- Develops solutions to remediate flooding attacks against time-critical communications within electric substations

OUTCOME

The detection method for intelligent delay-increasing attacks has very high accuracy (over 95% in practical settings). It will be able to detect multiple coordinated attackers. The tool is easy to integrate into existing network security and intrusion detection devices/software.

PARTICIPANTS	ROLE
SEEDS CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS	This project is part of the Secure Evolvable Energy Delivery Systems (SEEDS) academic consortium. SEEDS researches and develops innovative cybersecurity technologies, tools, and methodologies to advance the energy sector's ability to survive cyber incidents while sustaining critical functions.
UNIVERSITY OF ARKANSAS	Research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Qinghua Li
Associate Professor
University of Arkansas
479-575-6416
qinghual@uark.edu

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

This is a subproject sponsored by the SEEDS academic consortium, led by the University of Arkansas.

SEEDS Period of Performance: October 2015 – March 2022

SEEDS Total Award Value: $15,309,114
DOE Share: $12,226,504
Cost Share: $3,082,610

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021