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

Cyber-Physical Methods for Detecting and Localizing Date Falsification Attacks

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Applying physics and deep learning methods to detect and localize data falsification attacks in automatic generation control

This project addresses data forgery attacks in automatic generation control (AGC). First, it develops an understanding of the impact of data falsification attacks in AGC to the power grid. Second, it delivers a physics-based method for detecting data falsification attacks and localizing which data measurements are attacked. This method utilizes a more detailed model of the control system than currently used in control centers. Third, it delivers a learning-based method for detecting and localizing data forgeries leveraging recent advances in neural networks. This method utilizes data currently available in the AGC system and hence is easy to deploy. This project also tests the developed methods with real AGC operation data obtained from electric utilities.

KEY TAKEAWAYS

- Secures automatic generation control, a critical power grid control system that autonomous adjusts power generation in response to hard-to-predict area imbalances
- Ensures authentic and frequent system measurements as well as validated inter-area power exchange inputs
- Prevents data forgery attacks that lead to inaccurate power generation and significant operation problems

OUTCOME

Experiments over a synthetic dataset showed that the physics-based method detected all attacks. The learning-based method successfully detected 96% of the attacks and localized 94% of the attacks for reasonable scenarios. The accuracy improves in conjunction with the increasing severity of the observed attack. This introduces the potential to utilize available phasor measurement unit measurements for cybersecurity.

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.
Massachusetts Institute of Technology®	Develops physic-based method for attack detection and localization; assesses the impact of data forgery attacks in AGC to the power grid.
UNIVERSITY OF ARKANSAS	Develops learning-based methods for attack detection and localization.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Marija Ilic
Senior Research Scientist
Massachusetts Institute of Technology
412-260-2471
ilic@mit.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