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

Topology Attacks: Detection and Localization

SEEDS
CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Detection and localization of topology attacks on electricity transmission and distribution systems

A topology cyberattack occurs when incorrect information about the network topology is transmitted to the system operator, possibly by manipulating system topology databases or through malicious reporting of instantaneous topological states. Such attacks, if not detected and localized, leads to incorrect state monitoring and understanding of system physical dynamics, thus, potentially triggering incorrect control actions with disastrous consequences. This project to develops fast decentralized methods for topology attack detection in transmission and distribution systems, specifically taking into account the distributed cyber-physical nature of the power network, its large-scale nature, traditionally limited integration of measuring devices with system physical models, as well as the possibility of coordinated multi-point attacks. It further develops optimal sensor placement algorithms to guarantee real-time observability of the network and topology attack identifiability. The tools developed can be readily integrated as non-intrusive software add-ons in existing utility systems and services such as state estimation and protection modules.

KEY TAKEAWAYS

- Develops algorithms and software for detecting and localizing multi-point topology attacks on transmission and distribution networks
- Optimizes sensor placement and integration solutions for real-time network observability, attack detection, and outage analysis
- Develops decentralized implementations for scalable and resource-efficient topology attack analyses and monitoring

OUTCOME

This project develops a framework for power system topology monitoring and attack detection, based on optimal sensor placement, measurement data integration and fast decentralized attack analysis algorithms. The tools developed can be integrated with existing utility system modules, to enable reliable state and topology monitoring, protection and outage analysis in the face of malicious cyberattacks.

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.
Carnegie Mellon University Electrical & Computer Engineering	Responsible for developing the topology attack analysis algorithms, their performance analysis, and validation.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Soummya Kar
Professor
Carnegie Mellon University
412-268-8962
soummyak@andrew.cmu.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