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

Anomaly Detection for Securing Communication in Advanced Metering Infrastructure

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Techniques to detect anomalies and improve power grid resiliency

This project identifies control decisions based on measurements in advanced metering infrastructure (AMI) that impact power grid resilience. A critical cyberattack model compromises the measurement data that drive control systems in a manner that leads to loss of resiliency. There are currently no tools for validating measurements before using them to make important control decisions. The research team is developing tools that help mitigate the impact of attacks designed to undermine system resilience. The tool differentiates non-malicious deviations in meter data from anomalies indicating cyberattacks on AMI communications so as to maximize system resiliency.

KEY TAKEAWAYS

- Validates advanced metering infrastructure data
- Allows energy delivery system operators to make informed control decisions to improve power grid resiliency
- Prevents distributed denial-of-service and data spoofing attacks on advanced metering infrastructure

OUTCOME

This research lays the groundwork for continued development and evaluation of new anomaly detection algorithms, as well as the processing time to meet real time constraints. The project advances operator understanding of metering data for long-term system resilience.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

William H. Sanders
Professor
Carnegie Mellon University
sanders@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 CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

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