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

Toward Attack-Resilient PMU Data Analytics

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Mitigating hard-to-prevent system interference to expand and secure data analytics capabilities for energy delivery systems

Phasor measurement units (PMU) stand out as the most popular data source for conducting advanced data analytics to aid decision making in power grid operations including system monitoring, control, and protection. PMUs provide high-frequency, high-resolution, direct measurements in real time, but their data are susceptible to falsification from attack vectors such as jamming or spoofing or GPS synchronization, which can be executed without triggering typical security controls. While some countermeasures exist to make GPS clock synchronization more robust to spoofing attacks, their performance and guarantees are limited, especially when the adversary can design and inject sophisticated spoofing signals at multiple PMU locations. This project develops and validates real-time data correction and adversarial machine learning techniques that leverage the physical grid model to mitigate the impact of spoofing attacks on PMU data analytics decisions. This technique distributes data correction capabilities across the power grid to accurately identify and correct falsified data, deploys machine learning capabilities to recognize and more effectively protect against adversarial attack approaches, and visualizes the results of PMU data correction to better understand attack behaviors and enhance preparedness measures.

KEY TAKEAWAYS

- Develops a data correction approach for mitigating phasor measurement unit GPS spoofing attacks
- Deploys adversarial machine learning to mitigate the impact of falsified data on energy delivery system performance
- Operationalizes a visualization platform to enable training and preparedness against future attacks

OUTCOME

This project overcomes a critical barrier to securing and validating PMU data and increasing its reliability for power grid analytics and decision making. The developed techniques will be deployable on all Schweitzer Engineering Laboratories real-time automation controllers in operation across existing energy delivery infrastructure.

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.
Oregon State University	Leads research, development, and testing
SEL SCHWEITZER ENGINEERING LABORATORIES	Validates the techniques in practical environments; develops, tests, and verifies wide area monitoring application integration

CONTACT INFORMATION

Initial Leads:

Jinsub Kim
Assistant Professor
Oregon State University
541-737-3304
Jinsub.kim@oregonstate.edu

Eduardo Cotilla-Sanchez
Assistant Professor
Oregon State University
541-737-8926
ecs@oregonstate.edu

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