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

Robust and Secure GPS-Based Timing for Power Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Securing GPS time signals to enhance the precision and security of smart grid energy delivery systems

The GPS time-synchronized readings of Phasor Measurement Units (PMUs) provide assistance with real-time operations and off-line analysis to improve the reliability and efficiency of the bulk electric system. They deliver precise measurements that are required for regional-scale, high-resolution grid state estimation and potential early-stage detection of destabilizing conditions as part of the grid Wide Area Measurement System. However, the GPS signal is weak and vulnerable to jamming, interception, and spoofing, causing concern that GPS-based time synchronization of PMUs may be a potential point of entry for attacks on the power system. To address this, the research team is developing a multi-layer scheme for the reliable, robust, and secure GPS-based time transfer to PMUs, including the application of Direct Time Estimation (DTE) to authenticate GPS signals up to 10x faster than the current standard. The team is also developing a GPS simulator testbed to investigate spoofing attacks and mitigation schemes specific to PMUs.

KEY TAKEAWAYS

- Secures and authenticates highly vulnerable GPS-based time signals to maintain synchronicity of wide area measurement and control
- Maintains device synchronization under potential attack for high-precision network operations
- Simulates sensor device use cases to determine and mitigate risks prior to live implementation

OUTCOME

This research enhances the security and resiliency of smart grid infrastructure, upon which energy delivery systems (EDS) are increasingly reliant for automated and precise operations. The resulting techniques will allow PMUs to verify the authenticity of GPS-based data, enabling EDS networks to implement novel smart grid operations for advanced performance.

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

Grace Gao
Assistant Professor
University of Illinois
217-333-6360
gracegao@illinois.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