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

Advanced Networking for Reliable Energy Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Enhanced security and service guarantees for energy delivery systems using software defined networks

This research delivers software defined network-based (SDN) solutions that improve energy delivery system (EDS) network consistency, while also enhancing quality-of-service (QoS) guarantees for control networks. SDNs provide a global view of the network and include mechanisms to manage data flows as a whole, enabling the creation and management of pre-engineered paths for packet flows in control networks, which increase network security and reliability. SDNs also isolate specific network components during disruptions or scheduled updates. However, SDN-based EDS networks currently lack guarantees for maintaining the consistency of network flows when the system needs to be updated. Current SDN implementations across EDS networks also lack QoS guarantees for critical flows, including end-to-end timeliness guarantees. Although SDNs can help address these problems, they require additional functionality to do so. The Advanced Networking for Reliable Energy Delivery Systems project addresses this gap by delivering actionable research in time-critical flows for EDS using SDNs and improves QoS guarantees in EDS control networks.

KEY TAKEAWAYS

- Enhances the consistency of software defined networks across energy delivery systems during security incident-induced updates
- Investigates hardware/software packet redirecting mechanisms
- Designs and develops dynamic real-time quality-of-service mechanisms for control networks

OUTCOME

With this SDN implementation, EDS networks no longer require system resets/restarts, thereby avoiding service disruptions, in the event of successful denial-of-service attacks. Increasing network visibility and responsiveness minimizes or removes this critical vulnerability within EDS infrastructure. The SDN solution also delivers on over a decade of research to operationalize QoS guarantees for EDS networks that have been otherwise difficult or impossible to implement.

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	Lead institution; performs research on algorithms and mechanisms for real-time delivery guarantees and leads experimental evaluation.
Oregon State University	Partner institution; collaborates and supports research on algorithms and mechanisms for real-time delivery guarantees. Supports experimental evaluation through review and feedback.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sibin Mohan
Research Assistant Professor
University of Illinois
217-300-3037
sibin@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