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

Sequence Hopping Algorithm for Securing IEC 61850 Layer 2

SEEDS
CYBERSECURITY CENTER FOR SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

Advances data integrity through lightweight authentication and key management to secure new applications using IEC 61850 GOOSE messaging and other industrial protocols

The primary use of the International Electrotechnical Commission's (IEC) 61850 GOOSE messaging is for critical event-driven communication inside a substation. Since the standard does not cover GOOSE messaging security, the sequence hopping algorithm has been developed by Florida International University to address the authentication of GOOSE messaging inside substations. This project further develops the algorithm to support the extended IEC 61850 GOOSE messaging to include substation-to-substation and substation-to-control center communications. It implements the sequence hopping algorithm to authenticate GOOSE messages and prevents message spoofing, bad data injections, and replay attacks in substation communications.

KEY TAKEAWAYS

- Provides data integrity for GOOSE messages through a new lightweight authentication and signature algorithm
- Deploys cryptographic keys and digital certificates to devices across substations
- Extends the security algorithm to other control system protocols to maximize device and infrastructural interoperability

OUTCOME

Bump-in-the-wire solutions are seldom accepted by utility operators and vendors are skeptical about implanting algorithms that are not standardized. The project team is investigating avenues to transfer the proposed technology to practice and allow for its adoption in the IEC standard. The team built a demonstration that will be showcased during the next IEC interoperability testing program. A U.S. Patent has been awarded for this effort (Youssef T., El Hariri M., and Mohammed Osama, "Sequence hopping algorithm for securing goose messages". U.S. Patent number U.S. 9894080).

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.
FIU FLORIDA INTERNATIONAL UNIVERSITY	Research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Osama Mohammed
Distinguished Professor
Florida International University
305-348-3040
mohammed@fiu.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