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

# Quickest Intrusion Detection with Transient Analysis and Dynamic Models

SEEDS
CYBERSECURITY CENTER FOR
SECURE EVOLVABLE ENERGY DELIVERY SYSTEMS

*Increasing response efficiency to reduce damages and economic losses caused by cyberattacks*

This project develops quickest intrusion detection algorithms for power grid components with dynamic transient analysis, contributing to power grid cybersecurity through two main innovations. First, quickest intrusion detection minimizes detection delay while maintaining high detection accuracy. Conventional detection methods focus primarily on detection accuracy. Second, the algorithm uses transient analysis of the smart grid with dynamic models. A cyberattack will cause the power grid to deviate from its steady state. The signatures of cyberattack are embedded in the transient state. The transient analysis developed in this project allows security officers to track state transition and deviation in real time, enabling real-time intrusion detection.

## KEY TAKEAWAYS

- Operationalizes a transient data analysis protocol for real-time attack detection and mitigation
- Protects against bad data injection within supervisory control and data acquisition systems
- Responds to cyberattacks at high speed without sacrificing accuracy

## OUTCOME

Delivers a set of quickest intrusion detection algorithms that can identify malicious cyberattacks with minimum delays, while maintaining high detection accuracies. The algorithms can improve the cybersecurity of power grids.

| 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. |
| UNIVERSITY OF ARKANSAS | Develops quickest intrusion detection algorithms with dynamic models |

## CONTACT INFORMATION


**Initial Leads:**

**Carol Hawk**
Program Manager

**Jingxian Wu**
Principal Investigator
University of Arkansas
479-575-6584
wuj@uark.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