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

Cybersecurity via Inverter-Grid Automatic Reconfiguration

BERKELEY LAB

Uses reinforcement learning to control non-compromised distributed generation to mitigate the effect of attacks on solar photovoltaic systems

The project team is developing supervisory control algorithms to counteract cyber-physical attacks that compromise multiple independent systems in the electric grid. This research begins by analyzing the stability of different types of feedback control systems such as distributed energy resources (DER) and voltage regulation and protection systems in the electric grid to determine what parameters an attacker would change if these control systems were compromised. Then, the project team develops adaptive control algorithms that adjust critical parameters in non-compromised systems to actively fight the cyber-physical attack. Finally, the project uses reinforcement learning techniques to simultaneously develop new attack methodologies and defense strategies tailored to specific sections of the electric grid.

KEY TAKEAWAYS

- Develops a state observer that detects the presence and severity of cyberattacks on solar photovoltaic control systems
- Creates a reinforcement learning-based controller that adjust settings of distributed energy resource smart inverters to mitigate the effect of cyber-physical attacks in real time
- Integrates reinforcement learning agents into open-source distribution grid simulation tool allowing utilities to explore different attack scenarios

OUTCOME

This technology protects distributed generation and other DER against cyberattacks that threaten grid stability. Reinforcement learning-based algorithms adjust the settings of non-compromised DER inverter controllers to mitigate cyber-physical attacks on DER. Analysis of derived attack and defensive strategies will highlight specific system vulnerabilities and determine recommended upgrades to enhance system cybersecurity.

PARTICIPANTS	ROLE
BERKELEY LAB	Electric grid modeling and simulation, development of reinforcement learning algorithms
SIEMENS	Leverages expertise in reinforcement learning algorithm development
NRECA America's Electric Cooperatives	Integration of reinforcement learning algorithms into open source grid simulation tool (Open Modeling Framework)
ASU Arizona State University	Leverages expertise in electric grid optimization and control

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Sean Peisert
Principal Investigator
Lawrence Berkeley National Lab
510-486-4706
sppeisert@lbl.gov

Daniel Arnold
Co-Principal Investigator
Lawrence Berkeley National Lab
510-486-5564
dbarnold@lbl.gov

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

Period of Performance: October 2017 – March 2021

Total Award Value: $2,500,000
DOE Share: $2,500,000
Cost Share: $0

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