Fact Sheet

December 2023

NRECA Research Project Overview:
MAGIC
Mitigation via Analytics for Grid-Inverter Cybersecurity

Project Description

The increased proliferation of Distributed Energy Resources (DER) into the electric distribution system simultaneously presents challenges and opportunities for maintaining the cybersecurity of both DER and the grid itself. The remote update capability of DER has the potential to change the behavior of large aggregations of individual units, which can substantially alter grid conditions and there is recognition that this functionality constitutes a significant expansion of the cyber attack surface. On the other hand, DER devices can also be leveraged to mitigate the effect of cyber attacks on both DER and the electric grid in real time. In order to enable this capability, mechanisms must be created to perform analytics on DER/electric grid operational technology (OT) data to:

1) identify the onset of cyber attack, and
2) adjust the behavior of DER and legacy grid components to mitigate the attack in its earliest stages.

Project MAGIC will develop Artificial Intelligence/Machine Learning (AI/ML) algorithms to detect and mitigate cyberattacks on aggregations of DER and the electric grid, and will deploy and test these algorithms (through hardware-in-the-loop experiments) on the Siemens Spectrum Power Microgrid Management System (MGMS). Additionally, project MAGIC will integrate AI/ML algorithms into the National Rural Electric Cooperative (NRECA) Open Modeling Framework (OMF), allowing electric-cooperatives to conduct simulations of cyber attack detection and mitigation strategies for their specific networks.

The AI/ML approaches developed in this project will be tested by an independent red team and will be designed to be resistant to both data poisoning and input attacks. Project MAGIC will utilize the physics of both the electric grid and DER in the attack detection mitigation processes and will determine ways to reconfigure DER to mitigate disruptions to normal grid operations, thereby promoting the cyber-resiliency of the power system.

Project Goals

Project MAGIC will develop secure Artificial Intelligence/Machine Learning (AI/ML) tools to both detect and mitigate cyber attacks on aggregations of Distributed Energy Resources (DER) in electric power distribution systems and microgrids. In doing so, MAGIC will facilitate detecting cyber attacks on DER in their earliest stages and ameliorating the effect of attacks immediately.

The objectives of the project are to:

1. Develop secure AI/ML algorithms to detect cyber attacks on aggregations of DER and distinguish attacks from normal operating conditions.
2. Extend a reinforcement learning framework developed in previous RMT/CEDS projects to mitigate the effect of cyber attacks on DER in a wide array of operating conditions.
3. Integrate the attack detection and mitigation algorithms into a commercially available substation/microgrid management platform for algorithm demonstration.
4. Create an open source simulation tool allowing electric utilities to determine rules to detect and mitigate cyber attacks designed to severely disrupt normal grid operations or cause voltage instabilities.
5. Develop a software test harness to assess the security of AI/ML algorithms for electric grid attack detection and mitigation.

Project Partners

- Lawrence Berkeley National Laboratory
- National Renewable Energy Laboratory
- Siemens Corporate Technologies
- Cornell Tech

Contact

Lisa Slaughter
Research Software Engineer and Data Scientist
NRECA Research
Lisa.Slaughter@nreca.coop
571.422.2756