U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Cyber Attack Detection and Accommodation for Energy Delivery Systems

Development of an automatic cyber-attack/anomaly detection and accommodation (ADA) system to reduce the probability of a successful attack

Background

Power plants need the ability to accommodate and survive should a cyber-attack penetrate the inner core and the surrounding Operational and Control Technology (OCT) layer that controls, manages, monitors and protects them, allowing the power plant to sustain critical functions throughout their operation. This research will develop protection of the inner control system, offering a detection and accommodation framework by engaging power system domain-expertise that embodies physics and operational knowledge of the power generation system. With such a strategy, pools of attackers can be reduced from a large group to a very small number of expert users, significantly reducing the impact to power plants and probability of damage in the event of a successful attack.

Objectives

The project team aims to develop a commercially viable, field demonstrated, self-learning and resilient cyber-attack detection and accommodation technology to provide uninterrupted, equipment safe, controlled power generation to the grid even in the presence of attacks. This automatic cyber-attack/anomaly detection and accommodation (ADA) system is integral to the defense-in-depth strategy to support improved resilience in the national critical energy infrastructure. In addition to providing attack detection, early warning, and accommodation, the technology will also supply critical real-time insight into plant operations and health data, which will be used by utilities and independent power producers to monitor malicious activities or tampering of control system parameters inside the power plants. ADA technology uses feature-based learning and control and estimation algorithms to detect and localize attacks with very low false positive rates with multiple heterogeneous data streams and attempts to mitigate its effects through accommodation algorithms operating within its physical capabilities while attacks are in progress.

Project Description

The project team will develop and demonstrate an ADA system for energy delivery systems initially with high fidelity models running on a threat simulator. The self-learning and resilient ADA system will be designed to continue to provide power to the grid.

The team will perform R&D on a threat simulator with field usable Mark VIe hardware and will demonstrate the technology on a real gas turbine with controlled attack experiments with active participation from GE Power, and then on a real power plant under normal operating conditions operated by the utility company, Inland Empire Energy Center (IEEC).

Benefits

- Enable power plants to detect, localize and accommodate to survive from cyber-attacks
- Anticipate impact on the power grid of an ADA-created detection, early warning and forecasting algorithms to adapt and survive a cyber-attack. For instance, make known in advance any expected deviations to the power grid frequency, voltage and damping ratio likely to develop as ADA changes power plant operations to ride-through a cyber-attack.

Partners

- General Electric Global Research (lead)
- GE Power
- Inland Empire Energy Center (IEEC)

Period of Performance

October 2016 – September 2019

Project Cost

Total: $4,143,496

Federal: $3,039,289

Cost Share: $1,104,207

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE
202-586-3247
carol.hawk@hq.doe.gov

Lalit K. Mestha
Principal Investigator
General Electric Global Research
518-387-6967
lalit.mestha@ge.com

For More Information:

http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity

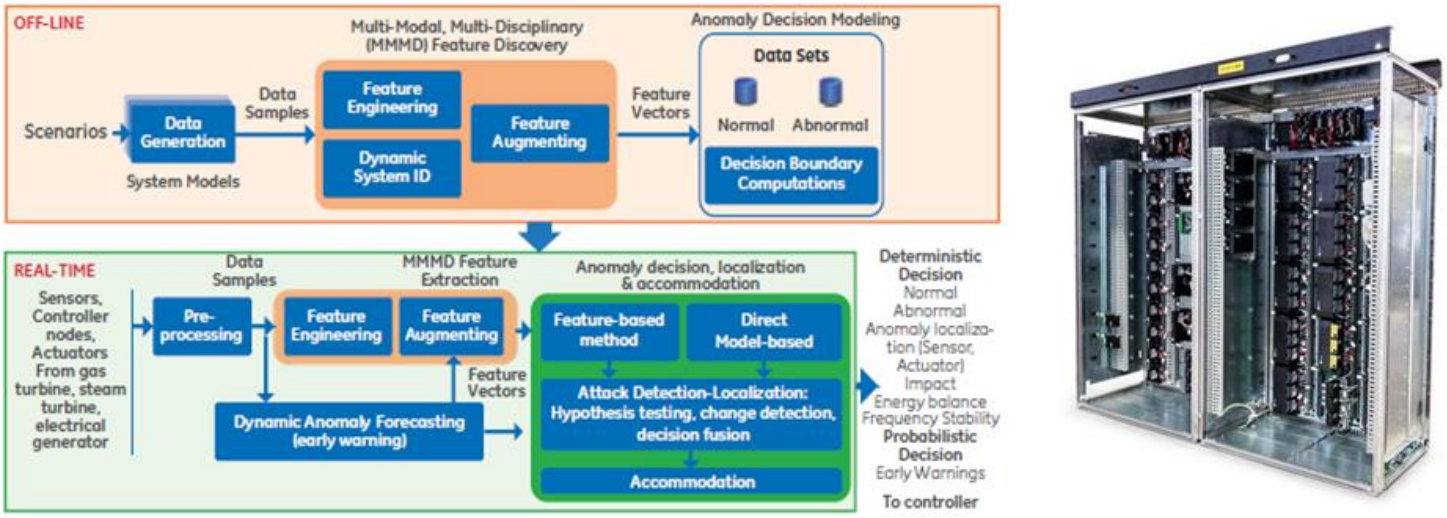

Figure 1: Off-line and Real-Time ADA System and Mark VIe

Technical Approach

Cyber-attack detection algorithms have always concentrated on the power grid, with some based on physics-based modeling and others on estimation theory. However, if the system is unobservable, conventional state estimation methods fail, requiring learning methods to solve this problem. Feature-based learning methods have shown improvements in minimizing false-positive rates when applied to anomaly detection and situational awareness of networked systems. Similarly, deep learning techniques have been shown to increase the performance of detecting anomalies in power generation equipment (<1% false positive rates). Therefore, the project team believes that attack detection is an anomaly detection problem, and requires a different approach from the current state of the art used for energy infrastructure such as the power grid.

The project team will attempt to address challenges to solving this problem as follows:

1. Domain threat points and attack simulations—It is difficult to simulate attacks in a real system. Therefore, the project team will leverage power plant models to simulate controlled attack experiments in the threat simulator.

2. Large-scale learning—Very high-dimensional space is a challenge and is difficult to solve with current methods. The project team will leverage their experience in large-scale learning and industrial Internet systems to extract features from time series signals with static/dynamic system components.

3. Anomaly decision, localization, and accommodation in real-time—Anomaly decision and localizing on-the-fly when an attack has occurred, and accommodating the system under attack is challenging. The project team will leverage experience in large-scale, feature-based learning, model-based approaches, resilient estimation and control theories and develop key algorithms.

4. Early warning and anomaly forecasting—In a physically constrained and stochastically driven system, forecasting future behavior is challenging because of improper estimation models. Models will be developed for short-, mid- and long-term forecasting of attacks.

5. Impact assessment on cybersecurity of energy infrastructure—Estimating anticipated impact after an attack to the power grid is challenging. The project team will demonstrate a method to estimate the impact of an attack while the power plants are operating in accommodation mode during an attack.

Anticipated Results

Project results will include the following:

- Proof of concept demonstration in a utility site
- Analysis of performance and impact to grid with accommodation algorithms
- Validation of anomaly detection, localization and accommodation algorithms, and a field demonstrated software system