Resilient Energy Systems
Mission Campaign

POWER SYSTEM VULNERABILITY IDENTIFICATION AND DEFENSE THROUGH DEEP REINFORCEMENT LEARNING

Inefficiencies of power system operation centers and generators underscore the need for dynamic stabilization capabilities. This project will leverage Deep Reinforcement Learning to generate mitigation strategies for an adversarial power system control model.

THE CHALLENGE

We seek to develop a Deep Reinforcement Learning (DRL) algorithm to reveal operational vulnerabilities and generate defensive strategies for an adversarial power systems scenario. New features of our implementation method will include advances in machine learning which will be applied to networked infrastructure systems. Our novel method will provide new capabilities to identify vulnerabilities and learn defensive strategies. Our work will dramatically advance the resilience of networked infrastructure systems, permitting the discovery of potential cyber-physical vulnerabilities and the development of possible mitigation strategies.

APPROACH

This research will develop a customized DRL algorithm applied to a gamified scenario. Our scenario defines a two-player "game" where a compromised distributed energy resource (DER) is maliciously controlling the DER equipment, trading turns with a utility operator attempting to maintain system stability. Through repeated play-throughs, the algorithm will simultaneously identify key system vulnerabilites and risks, and recommend defensive mitigation strategies.

Recent cyber threats to power system operation centers underscore the need for dynamic response. An effective response to cyberattacks requires an automated strategy. DRL is uniquely suited to this problem space due to its revolutionary success in learning strategies for complex adversarial scenarios. DRL will solve the problem of modeling at scale. Our DRL implementation plan requires several new contributions to extend it to infrastructure systems.

1. We will create a deep-learning model to best operate networked power system infrastructure.
2. We will develop a methodology to enable emergent co-evolution within an asymmetric competitive environment.
3. We will implement our model to take best advantage of Sandia's high performance computing (HPC) capabilities.

EXPECTED RESULTS

Evaluating progress requires a clear metric for success. Our adversarial scenario is defined as a two-player game, where the attacker must destabilize the system within a certain number of turns in order to win. To demonstrate learning, we will evaluate our trained agents against four static opponents. Learning will be demonstrated through improved relative performance against all four opponents. Successful completion of each research objective will result in a functional prototype to maintain stability in the face of an adversarial attack. This result will represent a new capability for Sandia with multiple potential impacts.

1. We will have a trained agent, capable of performing automated defense strategies.
2. We will have a trained attacker, capable of identifying key vulnerabilities.
3. Finally, we will have a new methodology that can be extended to other interconnected infrastructure systems.

Recent breakthroughs applying Deep Reinforcement Learning to the game of Go suggest a new approach to improve energy system stability and analysis.

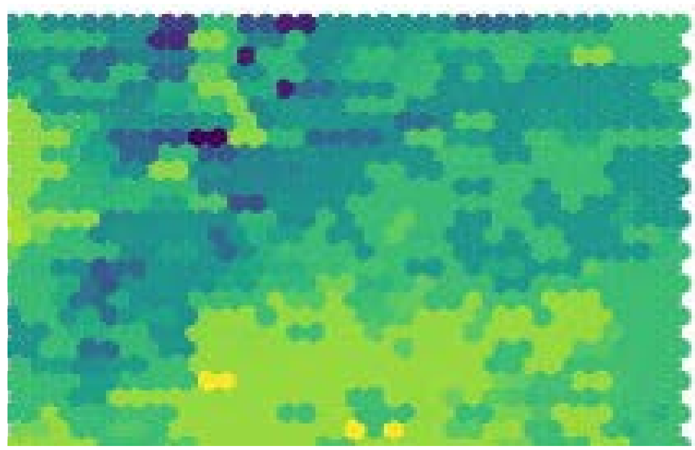
EXPECTED IMPACT OF THIS RESEARCH

A functional prototype applied to our power systems model will reveal unique vulnerabilities arising from cyber-physical control systems' interactions. This research will position Sandia as a leader in the use of high-performance DRL to develop resilient defensive strategies for critical infrastructure systems.

RESILIENT ENERGY SYSTEMS

Sandia's investment in this project is part of the Resilient Energy Systems portfolio of projects, coordinated R&D that addresses the resiliency of the nation's energy systems and other critical infrastructures to threats.

Specifically, we will utilize state-of-the-art DRL artficial intelligence methods to reveal key vulnerabilities and risks of the modeled system. This research will provide new methodology to further investigate diverse and integrated types of infrastructure through the use of novel artificial intelligence methods (DRL and Graph Convolutional Neural Networks) to address scaling issues inherent to the modeling of complex interconnected infrastructure systems.



Deep learning can help uncover the complex shape of the power system stability manifold.

CONTACT:

resilience@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2020-13373 O