GLOBAL SECURITY

LAWRENCE LIVERMORE NATIONAL LABORATORY

DRAGON: Deep Reinforcement Learning for Autonomous Grid Operation and Attack Detection

Dec. 7, 2022

PRESENTED BY:

Matthew Landen
Georgia Tech

Keywhan Chung
LLNL

Moses Ike
Georgia Tech

Sarah Mackay
LLNL

JP Watson
LLNL

Wenke Lee
Georgia Tech

Lawrence Livermore National Laboratory

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

LLNL-PRES-843151

National Nuclear Security Administration

Cyber Physical Attacks

- **Cyberattacks on industrial control systems are on the rise**
  - >2x more vulnerabilities published in 2021 as 2020
  - 19% published without a mitigation
- **Sophisticated attackers will gain access to power grid control systems**
- **Systems need to respond to both the cyber and physical effects of an attack**

Goal

- **A system that detects cyberattacks while maintaining reliable power**

Approach

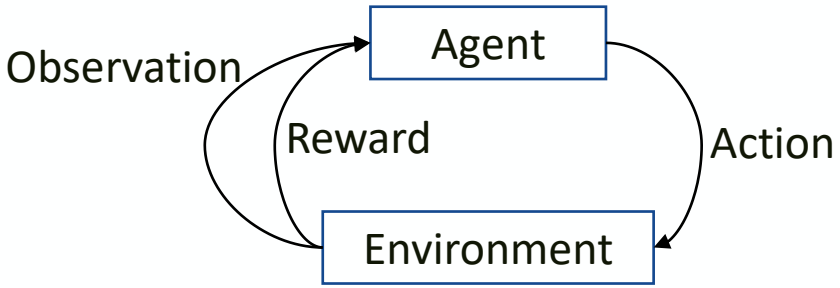
- **Dragon trains reinforcement agents to:**
  1. Detect cyberattacks
  2. Maintain reliable power grid operations

Ref: https://www.dragos.com/year-in-review/

Background

Reinforcement learning

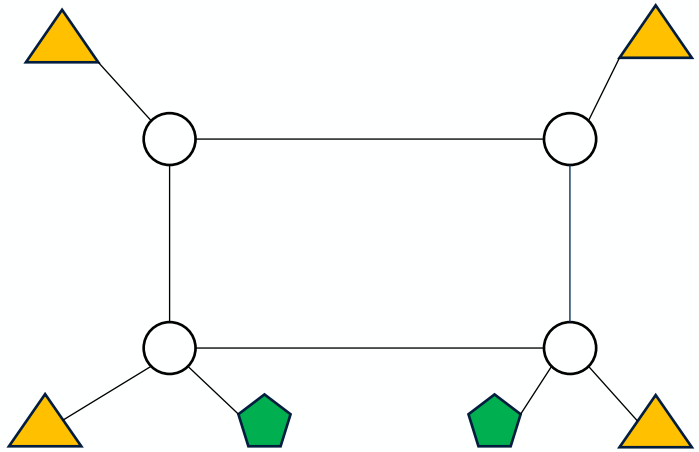
- Technique to learn decision making to accomplish a task, defined as a Partially observable Markov decision process (POMDP)



- Given an observation of the environment O, an agent learn a policy P that predicts actions A, which maximizes the total reward, R
- Agents learn the value of actions, given observations and chose the action with maximum value

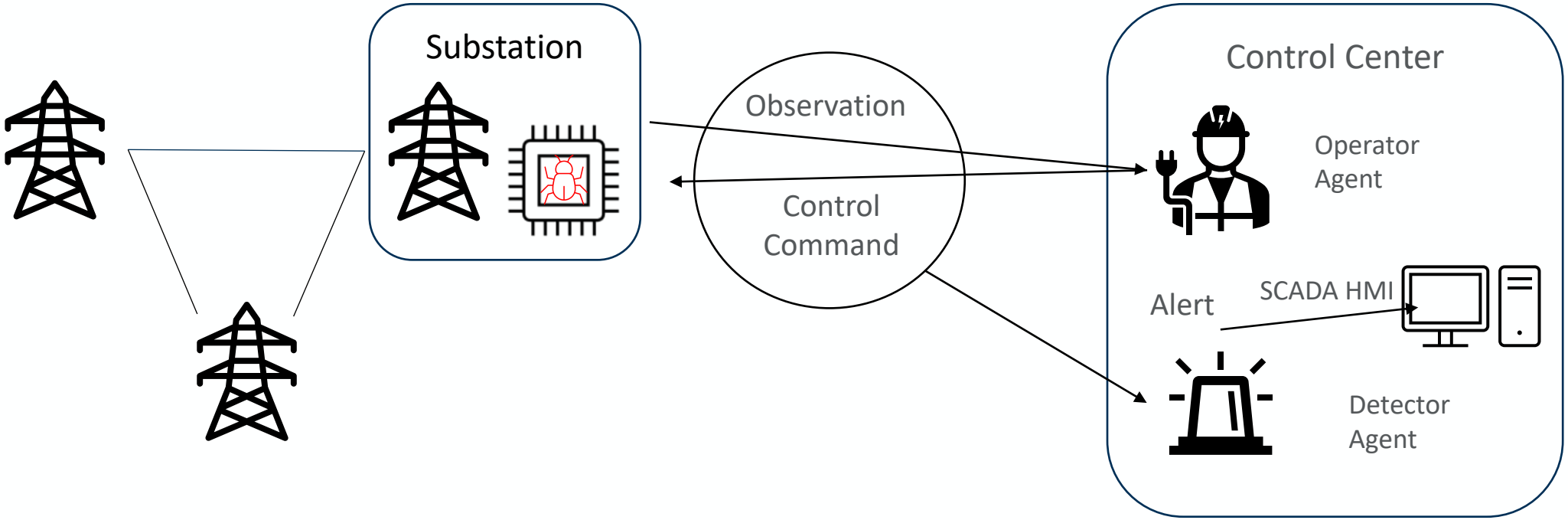
Power Grids

- Structure where power lines connect substations that carry power from generators (green) to loads (yellow)



- Lines carrying more power than their thermal limits are disconnected

Overview of Dragon



Threat Model

- Attacker can disconnect power lines for a maximum of 4 hours
- The line to target is selected randomly, weighted by current power flows
- Duration of attack is either
  - fixed (weighted random attacker)
  - randomly sampled (geometric attacker)
- Attacker can also inject false measurements into grid observations (FDIA)

Power Operator Agent

Observation

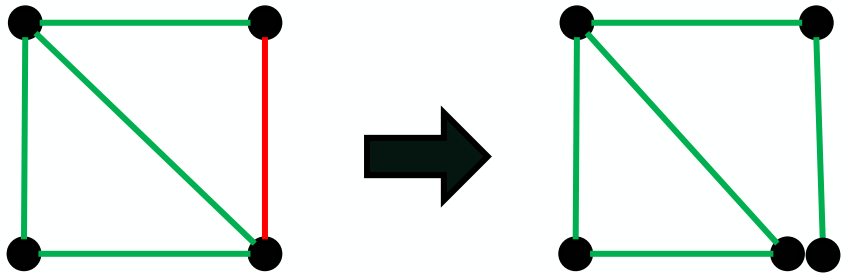
- Load, generator, line attributes

Actions (179 total)

- Reconnect power lines
- Bus switching

Rewards

- All loads receive power
- Lines obey their thermal limits



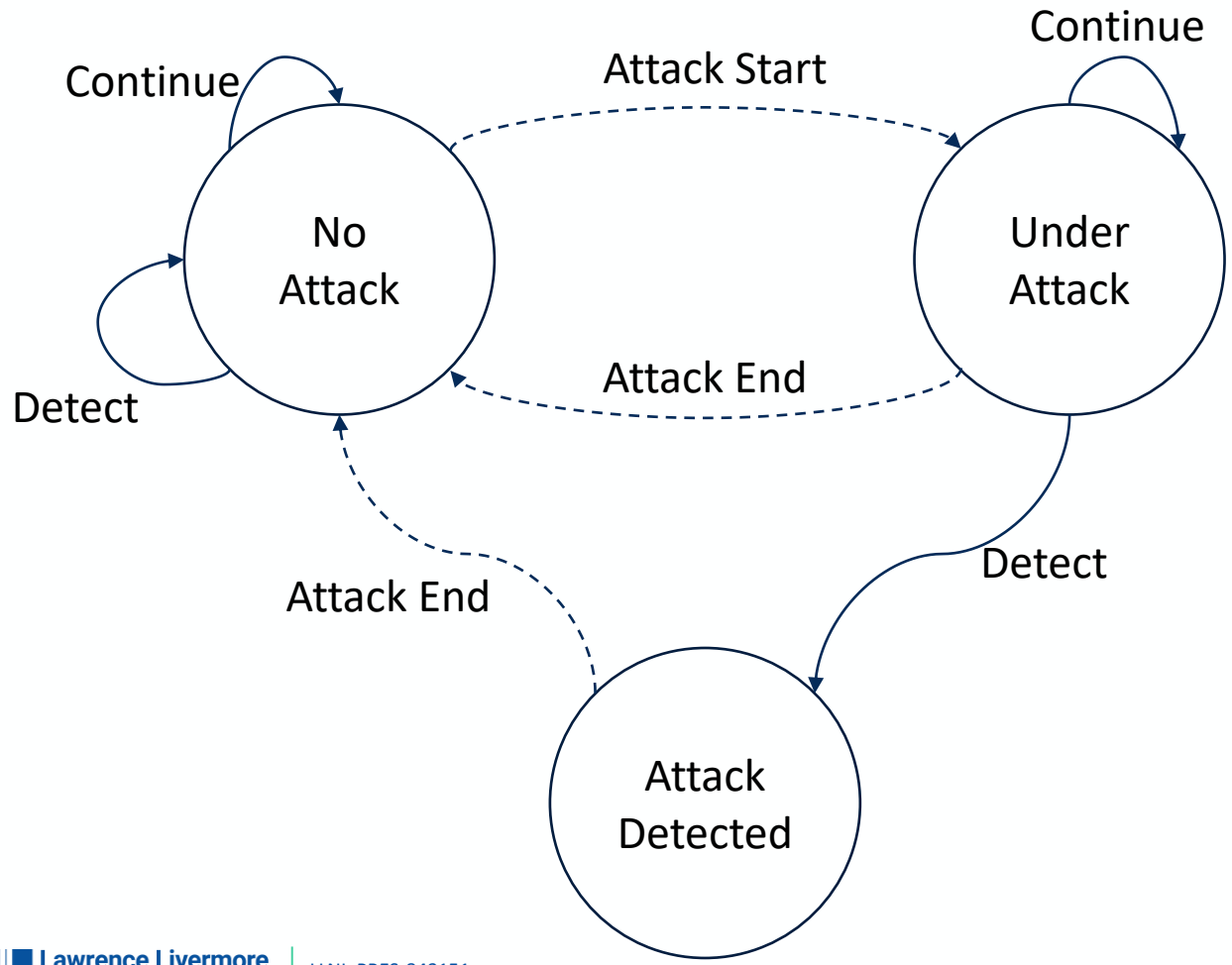
Bus Switch Action

Control Command Selection

1. Reconnect any lines
2. Sample potential commands from estimated action values
3. Simulate commands and rank them

Attack Detector Agent

Environment



Observation

- Previous and current grid observations
- Operator's control command

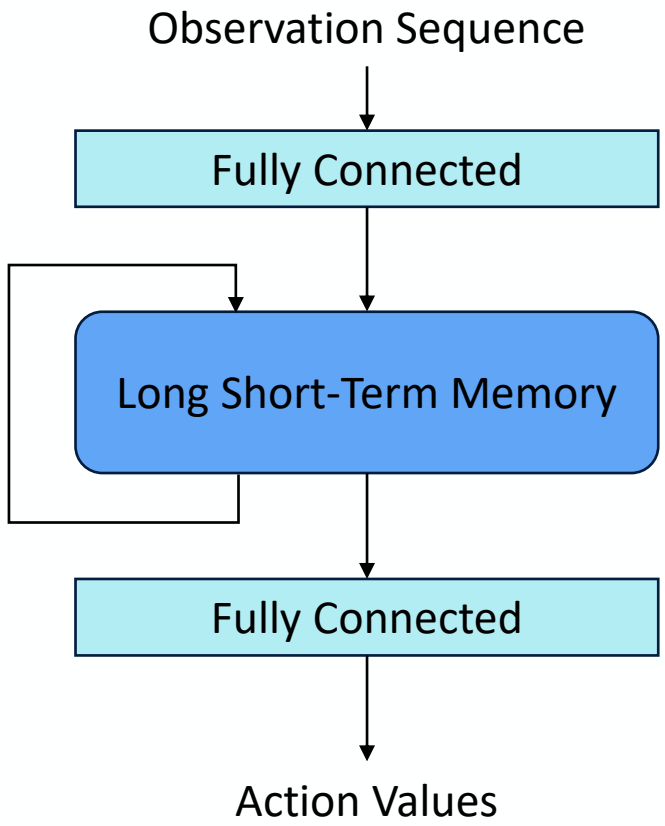
Actions

- Detect attack
- Continue normal operation

Rewards

- Penalize false positives and false negatives

Training Process



Training

- Agent uses recurrent neural networks as policies
- Agents are trained with the Deep Recurrent Q Network algorithm
- Trained for a set number of backpropagation passes

GLOBAL SECURITY

Evaluation

Lawrence Livermore National Laboratory

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

LLNL-PRES-843151

National Nuclear Security Administration

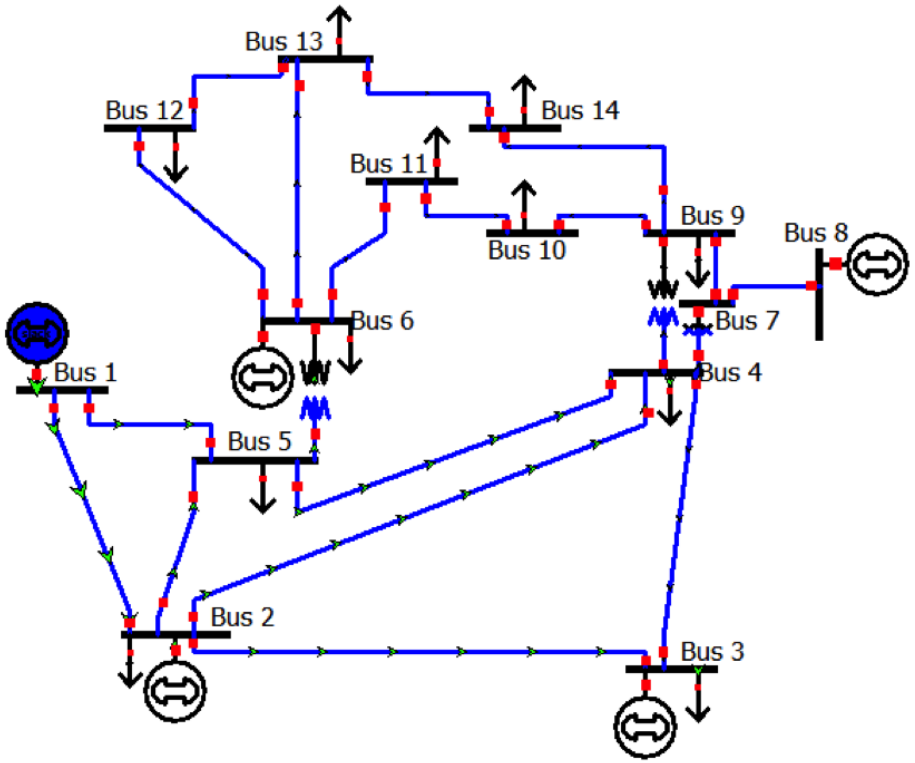
Evaluation Setup

Evaluation

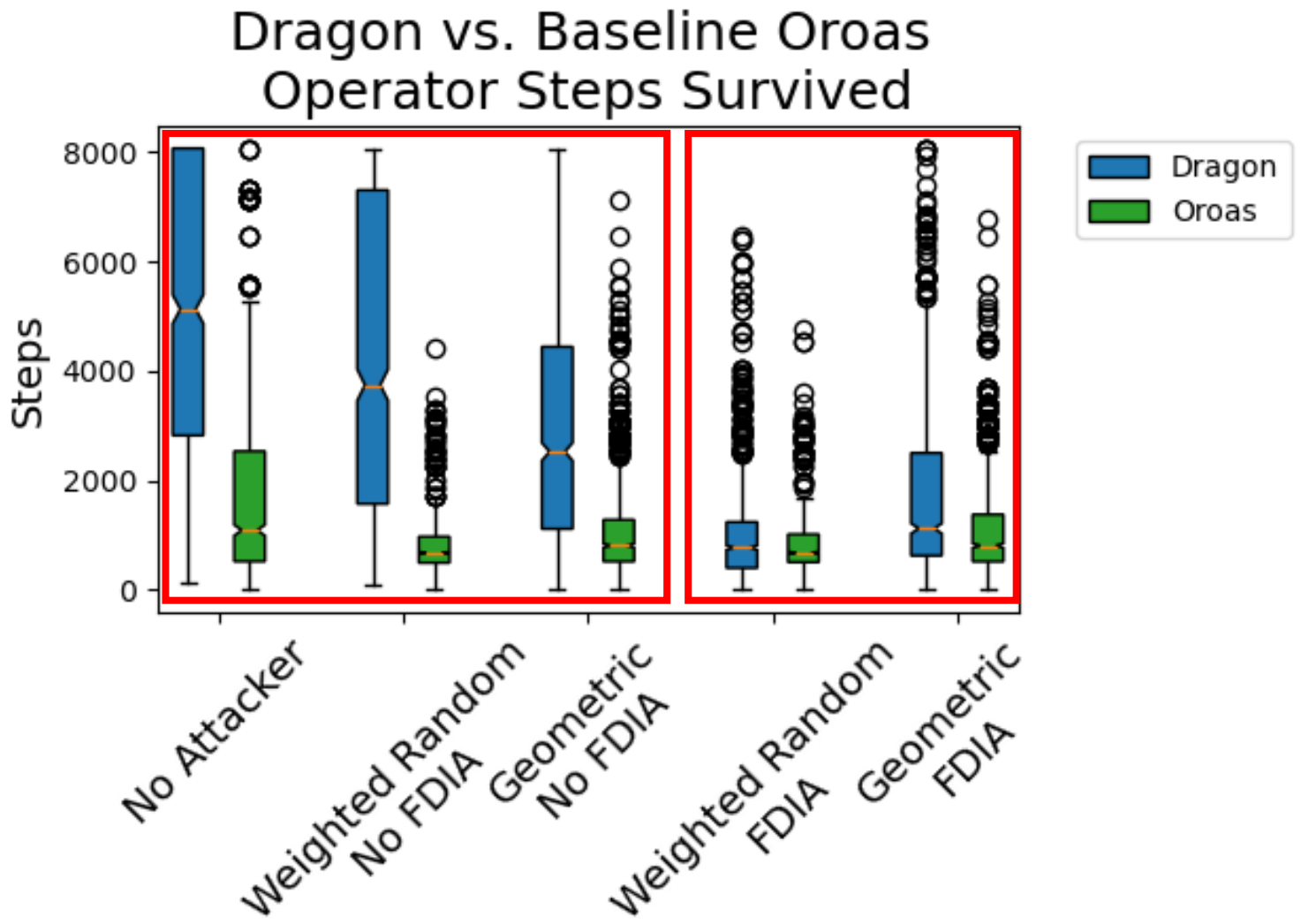
- IEEE 14 bus power grid with 1,110 load/generation profiles spanning all months and different years
- Ran hyperparameter optimization with 2% of the profiles for validation
- Applied 3-fold cross validation for training/evaluation

Baselines

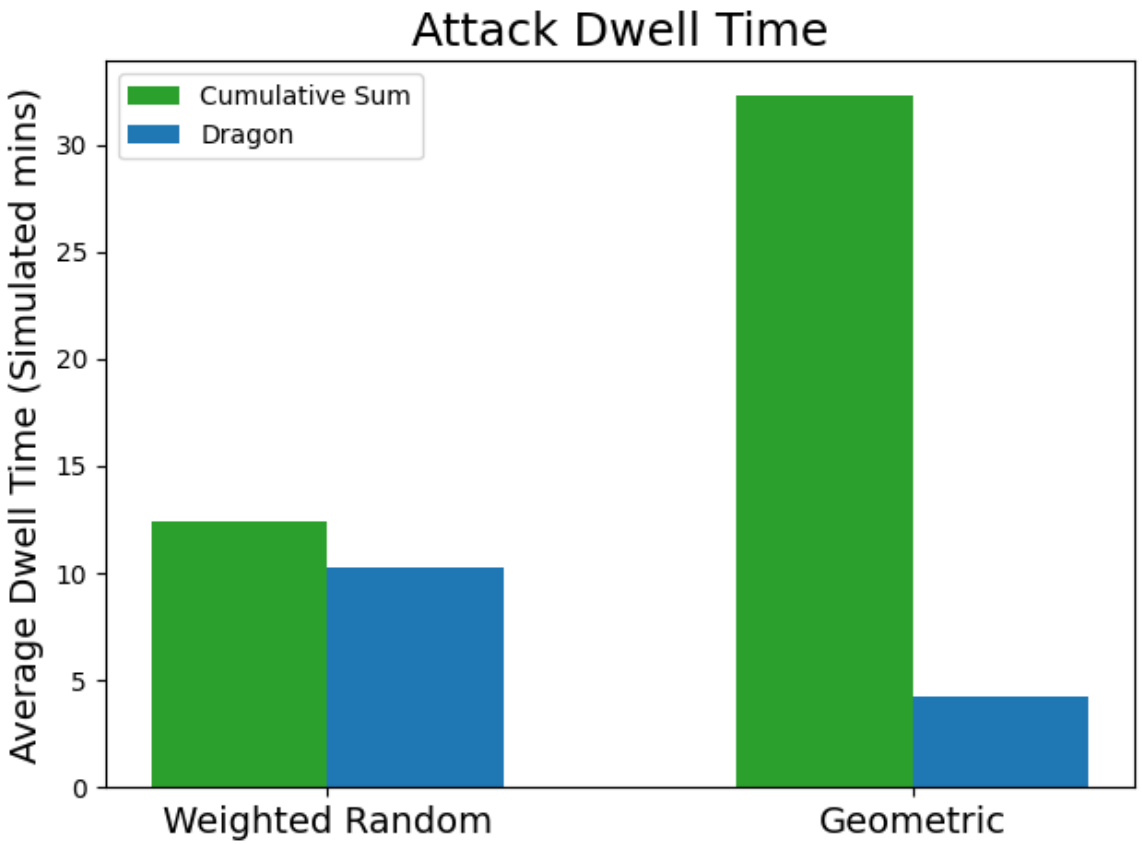
- Operator
  - Second place team (Oroas) from recent autonomous grid operation competition
- Detector
  - Cumulative sum of residuals algorithm

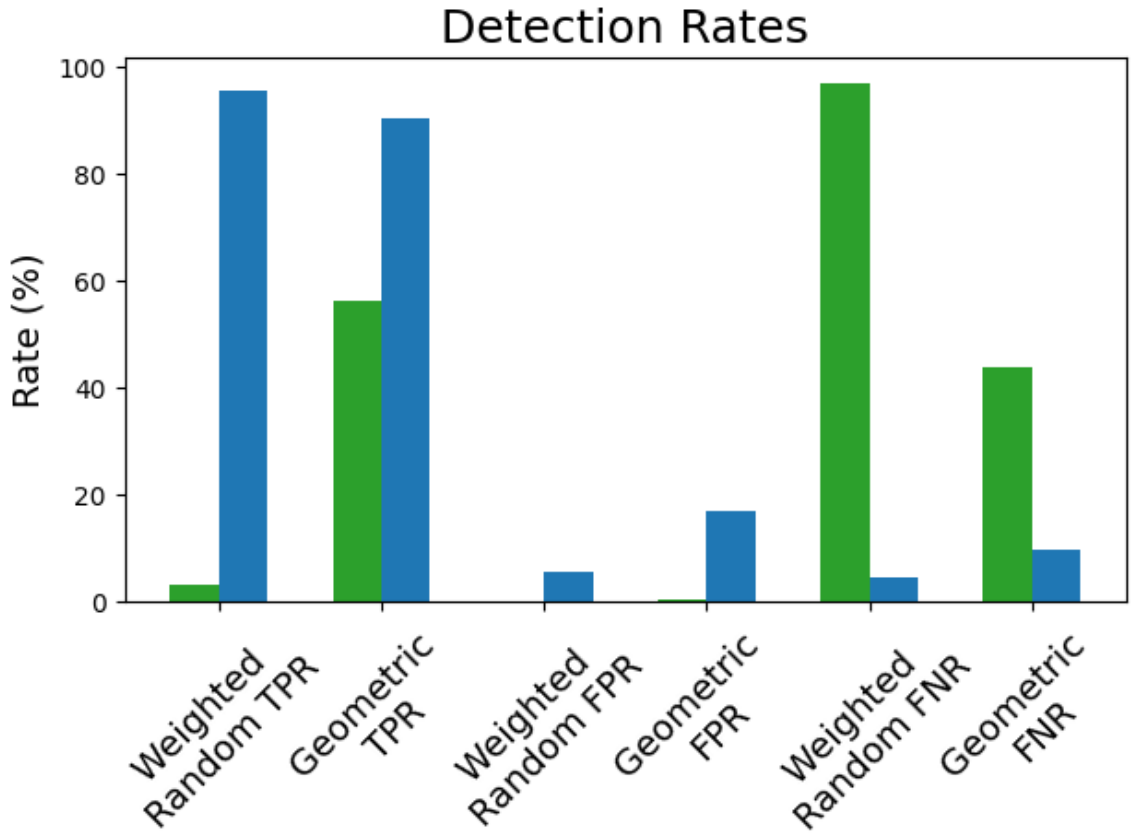


Operator Evaluation



Detector Evaluation





Discussion

Limitations

- Operator relies on the ability to execute commands to maintain grid reliability
- Small grid used during evaluation

Future Work

- Investigate how the two agents can benefit from each other's knowledge

GLOBAL SECURITY

Thank you
Q&A

Lawrence Livermore National Laboratory

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

LLNL-PRES-843151

National Nuclear Security Administration


Lawrence Livermore
National Laboratory

DISCLAIMER