Discovery of false data injection attacks on power grid frequency controllers with reinforcement learning

Romesh Prasad,
Dr. Malik Hassanaly, Dr. Xiangyu Zhang
ALIS, Computational Science

Introduction: Cyber security in power grid

Present Grid
- Conventional generation
- Synchronous generator

Future Grid
- More renewable energy
- Inverter based resources

- ✚ Hundreds of generators
- ✚ High Mechanical Inertia
- ▬ Linear control law
- ▬ Inflexible control

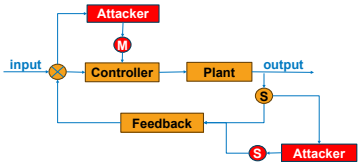
- ▬ Millions of inverters
- ▬ Low Inertia
- ✚ Flexible control
- ✚ Arbitrary control law

Long term advantage
Cleaner energy

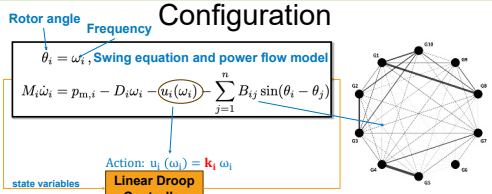
Long term security concern
Need more communication channels

Introduction: False data injection attack

- **Feedback loop assumption**
  - **Sensor value observed is unbiased**
- **False data injection attack**
  - **State estimation is modified**
  - **Modified control logic**



Configuration



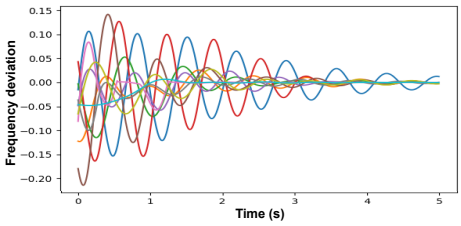
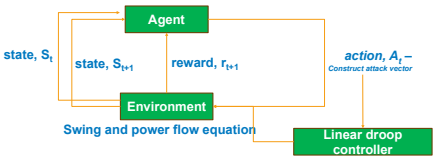


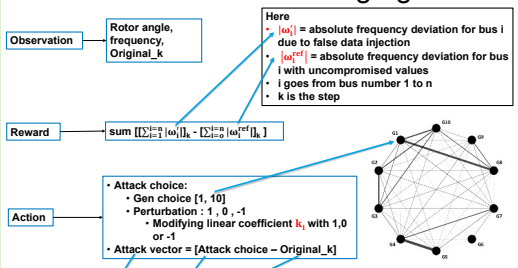
Fig 1: Linear droop controller for frequency deviation of reduced 10 bus system

Methodology



Assumption:
- Agent has access to the frequency, rotor angle and original linear droop coefficient value (Original_k)
- The agent chooses one generator to perturb with one attack choice at one time step
- Episode terminates at 5s i.e., 500 timesteps

Reinforcement learning agent



Manual false data injection attack

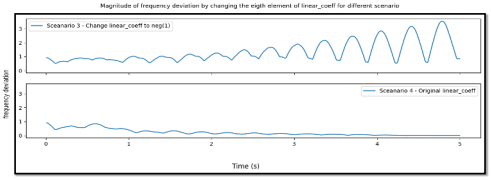


Fig 2: Manual FDI on generator 8 with perturbation of -1

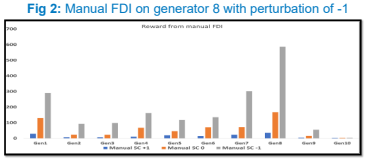


Fig 3: Reward earned by manual perturbation of each generator for different scenario

Results

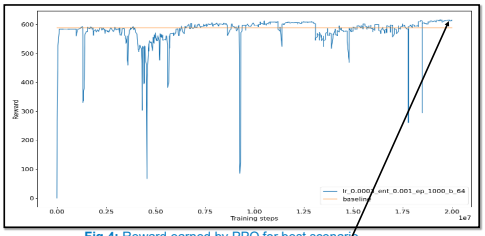


Fig 4: Reward earned by PPO for best scenario

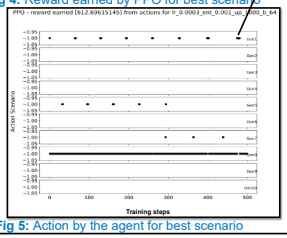


Fig 5: Action by the agent for best scenario

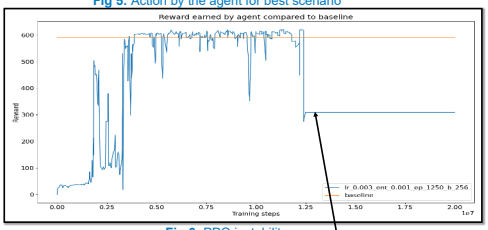


Fig 6: PPO instability

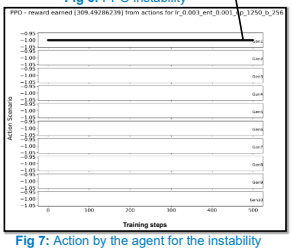


Fig 7: Action by the agent for the instability

Conclusion

- **Agent discovered that how to perturb a combination of generators**
- **Agent discovered perturbing generator 10 and 9 has no impact**
- **In some cases, agents demonstrated sign of "catastrophic forgetting"**
- **In future, we would like to add more complexity to the environment**
  - **Agent should avoid detection**
  - **Partially observable states**

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. This work was supported by the Laboratory Directed Research and Development (LDRD) Program at NREL. The research was performed using computational resources sponsored by the Department of Energy's Office of Energy Efficiency and Renewable Energy and located at the National Renewable Energy Laboratory. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

August 11, 2023
NREL/PO-2C00-87148