U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Cybersecurity via Inverter-Grid Automated Reconfiguration (CIGAR)

Lawrence Berkeley National Lab (LBNL)

Sean Peisert and Daniel Arnold

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

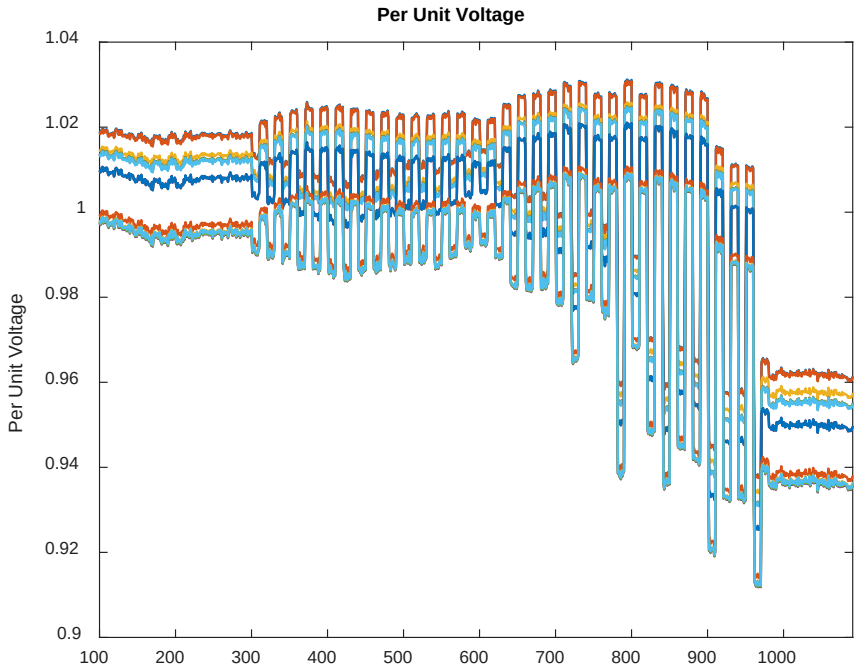
Summary: Project Title

Objective

- Ensure grid voltage stability due to manipulations of DER and legacy device control settings.

Schedule

- Project Dates: 4/1/18 – 4/1/21
- Deliverables (3): Task reports due April 1st (2019, 2020, 2021)
- Main Result: development of a tool to determine how to reconfigure a distribution grid in the event of a cyber attack on DER and/or legacy devices.



Total Value of Award:	**$2,500,000**
Funds Expended to Date:	**6%**
Performer:	**LBNL**
Partners:	**Arizona State Univ., Siemens, NRECA, Power Standards Lab**

Advancing the State of the Art (SOA)

- **Current SOA for defending inverters against cyberattacks looks at behavior of individual systems (DER, regulation & protection systems)**
  - Stability issues arising from complex interaction between these systems has not been addressed

- **CIGAR uses reinforcement learning to understand the holistic behavior of the entire system, in the context of cyber attacks against a subset of inverters, and adjust settings of remaining inverters to maintain grid stability.**
  - Example: Google DeepMind has applied reinforcement learning to reduce data center cooling by 40%

Advancing the State of the Art (SOA)

- **Improve Grid Cybersecurity Operations:**
  - CIGAR uses non-compromised distribution grid assets to mitigate instabilities caused by compromised DER, voltage regulation, and protection systems
- **Improve Grid Cybersecurity Planning:**
  - CIGAR reinforcement learning strategies will inform system hardening practices (e.g. adjusting control settings in voltage regulators)
- **Feasibility of our Approach:**
  - Existing examples of reinforcement learning optimizing complex systems (e.g., DeepMind),
  - Proof-of-concept simulations over life of project will demonstrate iterative refinements of success

Challenges to Success

Challenge: Observing Instabilities

- Q: How are cyber attacks distinguished in system telemetry?
- A: Developed instability observer to detect unstable oscillations in system voltage measurements

Challenge: Simulation Tool Physics

- Q: Can simulation tools recreate instabilities?
- A: Developed prototype simulation and compared to Open-DSS and GridLAB-D before scaling up

Challenge: Simulating a Cyber Attack

- Q: What combination of parameters creates an instability?
- A: Mathematical modeling of individual systems (DER, etc.)

Progress to Date

Major Accomplishments

- All subcontracts signed and IP agreement in place.
- Developed instability observer to detect unstable oscillations in system voltages and power flows
- Completed feedback control modeling of DER smart inverter control functions (Milestone – Oct. 1, 2018)
- Simulated 5 cyber attack & defense use cases for DER smart inverters on IEEE test feeders in Matlab and OpenDSS (each use case is an attack that is successfully mitigated by other DER)
- Prototyped 5 candidate reinforcement learning algorithms (after down-selection)
- Feedback control modeling of voltage regulation systems underway

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- CIGAR reinforcement learning agent will be integrated into NRECA Open Modeling Framework
- This will allow unique analysis for NRECA member utilities networks
- NRECA will recruit a cooperative utility advisory board, and work with them to create reports on use cases, feedback, and software enhancement requests
- Two workshops with industry steak-holders (Y2 and Y3)
- Paper publications and open-source code available on GitHub

Next Steps for this Project

Approach for the next year or to the end of project

- Development of feedback control models for voltage regulation systems (Dec. 2018)
- Development of feedback control models for voltage protection systems (April 2019)
- Integrated system (DER, voltage regulation, voltage protection) simulation (July 2019)
- Candidate reinforcement learning algorithms further down-selection and finalization (Fall 2019)
- OMF agent co-simulation framework development (April 2019)
- Development of reinforcement learning training framework (2019 ongoing)

Additional Slides – Motivation

Standardization of autonomous behavior of DER presents a cyber vulnerability

"800,000 Microinverters Remotely Retrofitted on Oahu—in One Day"

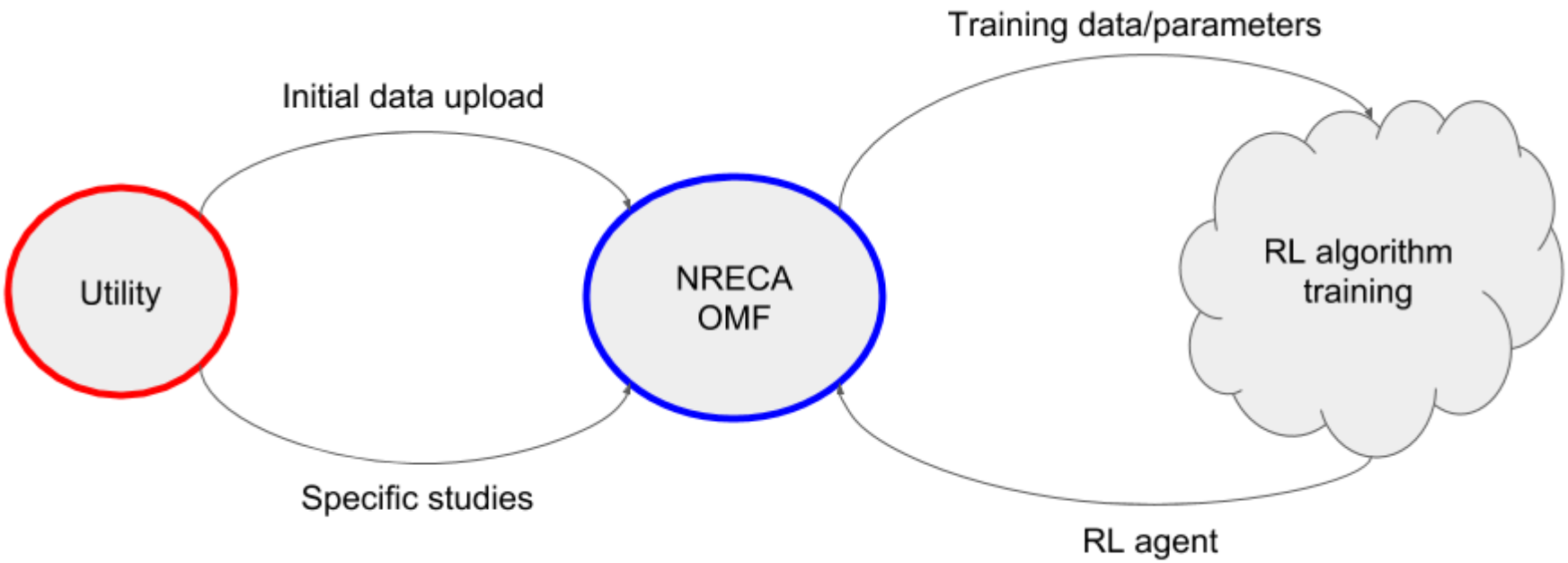
"…Enphase used built-in communications links to upgrade the grid-stabilizing capacity of four-fifths of Hawaii's rooftop solar systems"

If compromised, what would happen?

How can we defend against this?

https://spectrum.ieee.org/energywise/green-tech/solar/in-one-day-800000-microinverters-remotely-retrofitted-on-oahu

Tentative Architecture



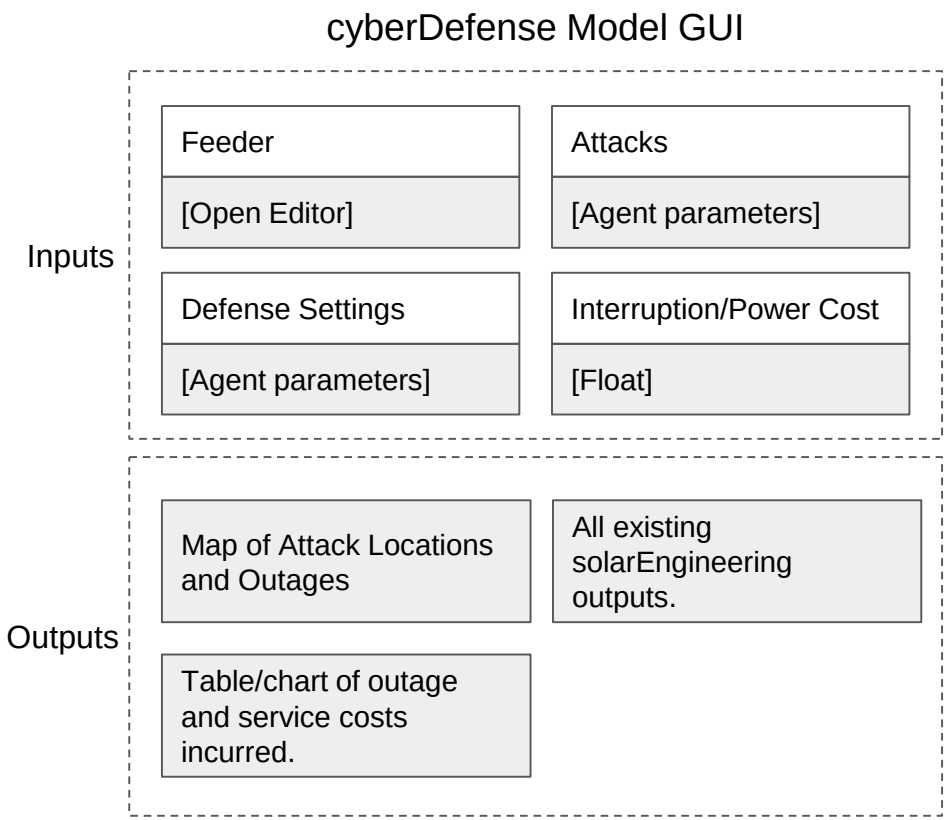
1. Initial data/parameters uploaded from the utility to the OMF
2. Training data passed to cloud for RL agent training
3. RL agent passed back to OMF (note: this architecture will house the RL agent within the NRECA OMF)
4. Utility can conduct simulations using the RL agent within the OMF using GridLAB-D

Facilitating Adoption

- Co-sim infrastructure will allow RL agent to be incorporated into the OMF
- NRECA will facilitate knowledge transfer with member utilities (Task 3.4)
- Recruit a cooperative utility advisory board with representation from at least three utilities
- Utilities will assist in creation of use cases, provide feedback, and software enhancement requests
- NRECA will provide outreach to 900 member utilities promoting the results of the project and application of the developed technologies.
- All developed algorithms to be made publicly available via GitHub
- Journal and conference publications, presentations

NRECA - GridLAB-D API

- Develop an API for GridLab-D that integrates existing OMF code (https://www.omf.coop) and new “attack” and “defense” agents acting in cosimulation.
- Use NESCOR list of utility attack scenarios to model different types of attacks to be represented by attack agents.
- Create a web-based GUI to run simulations based on specified attack and defense types.
- Simulations will help user determine the vulnerability of a grid to attacks and the effectiveness of implemented defense strategies.



ASU – Voltage Regulator Modeling

- Prior work using the DistFlow equations and linearization of the voltage square term shows the stability condition to be:

$$\lambda_{max}\left(\begin{bmatrix} C_pR & C_pX \\ C_qR & C_qX \end{bmatrix}\right) < 1$$

referring, the stability of the network depends upon the network parameters and droop control values of the inverters.

- The recent work of ASU team derived a new formulation using the actual voltage square term which is :

$$\sigma_{max}\left(C_s\left[1_2 \otimes \left\{diag^{-1}\left(\sqrt{\overline{v}^2 - Zs}\right)Z\right\}\right]\right) < \sqrt{2}$$

this shows that stability of the network depends on the network parameters, the droop control values as well as the network operation condition.

Siemens - Reinforcement Learning Platform

- Flexible: Support various RL algorithms, action spaces, neural network architectures and replay buffers.
- Scalable: Different agents can be clustered into one group and share the neural network parameters.
- Extensible: Users can arbitrarily change the number and strategies of attack and defense agents, which can be used to generate new attack scenarios and assess the vulnerability of the system.

Scenarios: / Control:	Attacker: None	Attacker: Blocked Setting	Attacker: RL
Rule-Based	Traditional	Traditional	Our work
RL	Our work	Our work	Our work

Scenarios explored in the project