CREDC

From Data Falsification to Cascading Failure: Feasibility and Security Measures

Attack-Resilient Machine Learning for Power Grid Control

Carter J. Lassetter, Eduardo Cotilla-Sanchez, and Jinsub Kim

GOALS

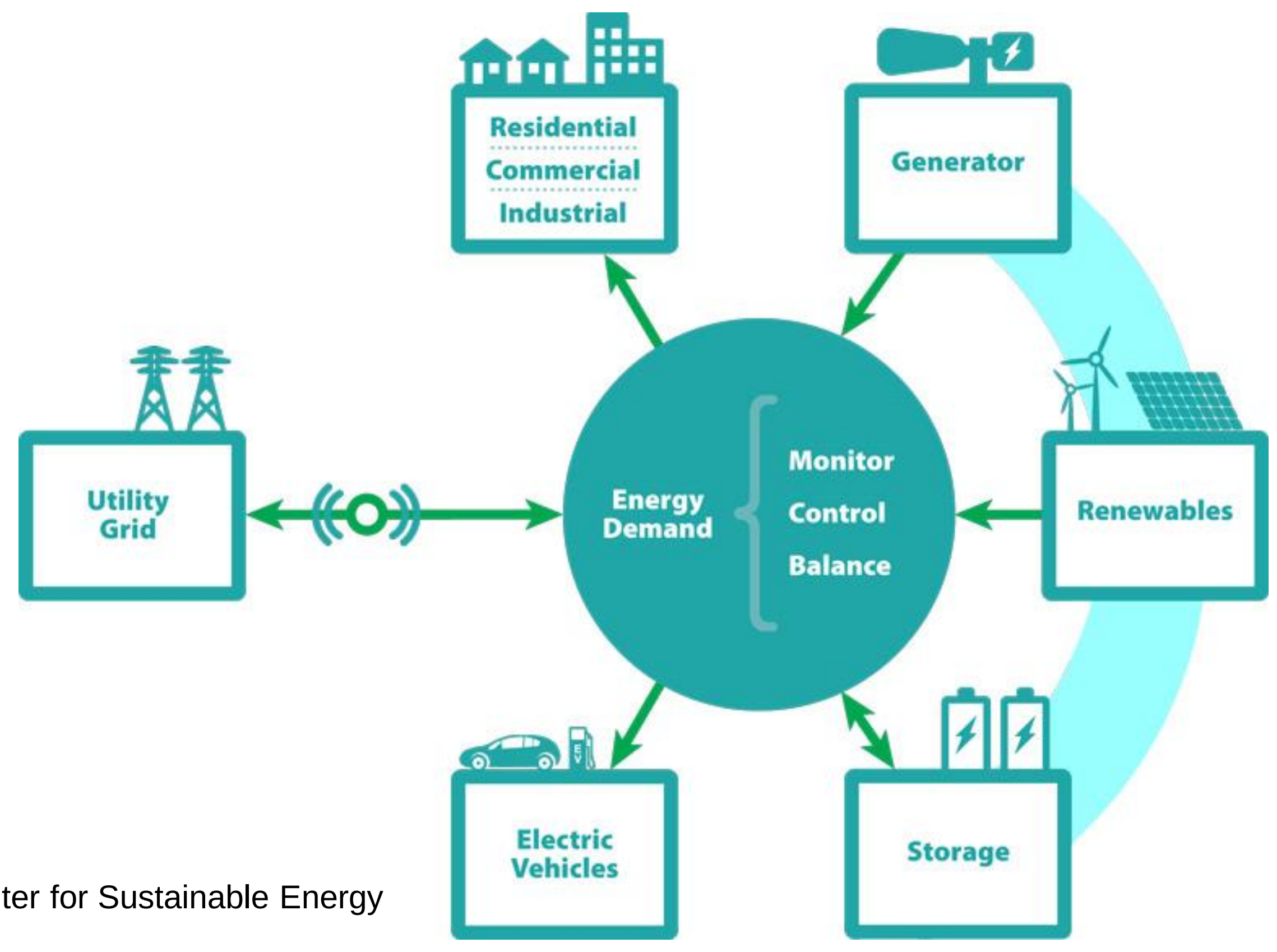
- We aim to develop *attack-resilient* machine learning algorithms to aid power system operators in making real-time control decisions.
- The objective is to design a robust machine learning algorithm such that it can perform consistently even in the presence of cyber attacks. Of particular interest is a scenario in which some real-time test data are falsified by cyber attack.
- The current application of our interest is real-time identification of stable reconnection timings for an islanded microgrid (or a larger balancing area) based upon phasor measurement unit (PMU) data streams.

FUNDAMENTAL QUESTIONS/CHALLENGES

- Success of machine learning algorithms relies heavily on the integrity of training and test data. In practice, because of limited security resources, perfect data integrity cannot be guaranteed in the smart grid.
- There are several challenges that we need to address:
  - **Designing a good machine learning algorithm itself is a challenging task**. A proper dimensionality reduction technique is needed to reduce computation and avoid overfitting.
  - A unique challenge of machine learning for assisting power grid control comes from **difficulty of acquiring real-world training data**.
  - Third, **identifying falsified portions of data or nullifying their effect is a nontrivial task**, especially as we do not want to impose restrictive assumptions on attacks.

RESEARCH PLAN

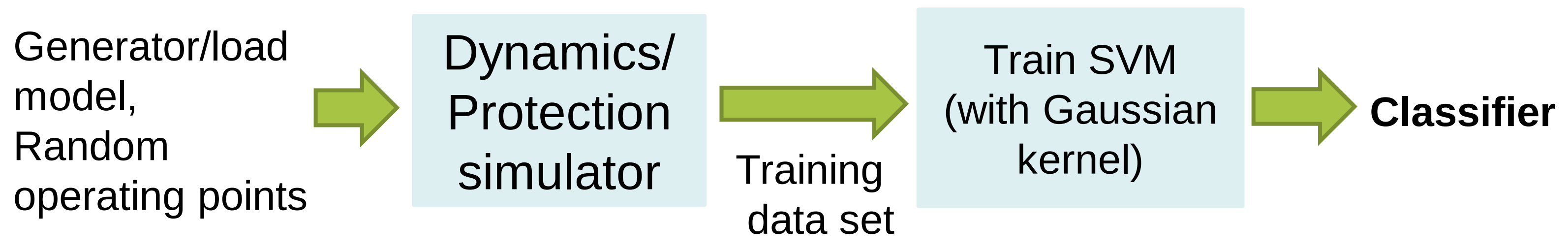
- Current application: **Machine learning for identifying stable reconnection timings of an islanded microgrid**:



© Center for Sustainable Energy

  - Depending on the current operating conditions, reconnection of an islanded microgrid may lead to a new stable operating point or an unstable condition, such as voltage collapse. We are developing a classifier that can advise us, based on PMU data streams, whether reconnection at a certain (current or future) time point will result in stable reconnection or not.

- **Task 1**: Train a classifier using power system dynamics and protection simulator.
  - In order to create training examples, we utilize a power system dynamics simulator that integrates customized protection schemes. We use both our own open-source code, the Cascading Outage Simulator with Multiprocess Integration Capabilities (COSMIC)[1], and a commercial simulator (Siemens PSS/E) with customized interface and protections.
  - Train a support vector machine (SVM) classifier with simulated data:


Generator/load model, Random operating points

Dynamics/ Protection simulator

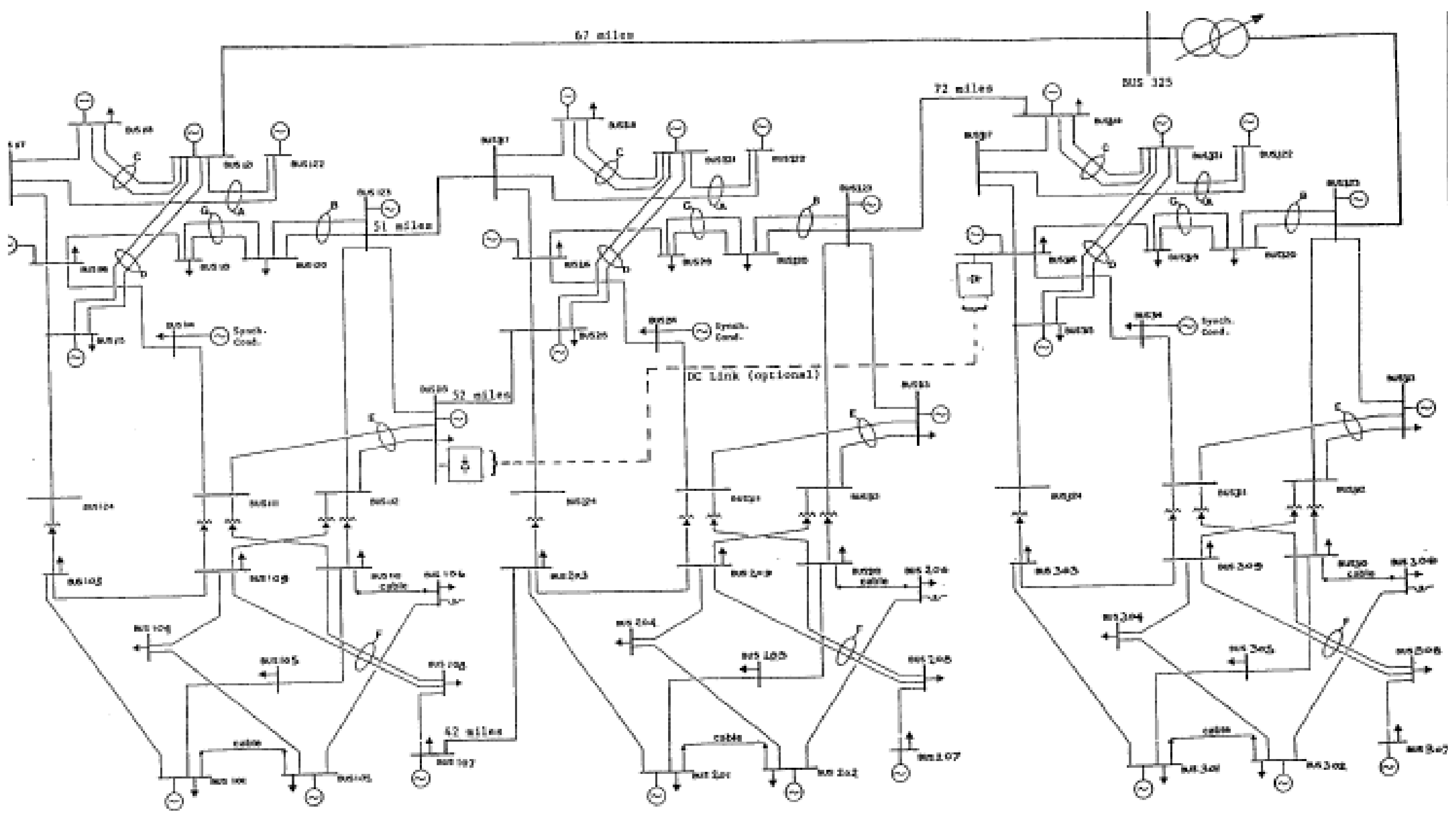
Training data set

Train SVM (with Gaussian kernel)

Classifier

- **Task 2**: Optimal security resource allocation: classifier based on a trusted subset of PMUs.
  - We envision two modes of the classifier. When no false data are detected, the classifier will utilize all PMU data streams. However, if false data are detected, the classifier will utilize only the trusted subset of PMUs.
  - We aim to find a subset of PMUs that are critical for our application.
- **Task 3**: Detection and localization of falsified data.
  - A statistical anomaly detector to detect abnormal PMU data streams.
  - We will consider a GPS signal-spoofing attack.

RESEARCH RESULTS



© IEEE, Reliability Test System Task Force, "The IEEE Reliability Test System – 1996", *IEEE Trans. Power Systems*, vol. 14, no. 3, 1999.

- **Classification performance**: When applied to RTS-96 system, the proposed SVM classifier resulted in 91.4% accuracy in classifying stable reconnection timings as "stable" and 86.3% accuracy in classifying unstable reconnection timings as "unstable."

BROADER IMPACT

- Security aspect of machine learning applications in power systems:
  - Investigate vulnerability of machine learning applications to potential adversaries.
  - Countermeasures to make them attack-resilient.
- Advances in power system dynamics and protection simulator:
  - There are several open questions about what are good levels of fidelity for cascading failure models in order to capture the propagation mechanisms of interest.
  - We will investigate the particular cascading mechanisms that result from cyber attacks.
- Through the project, we aim to provide new insights into the following fundamental problems of machine learning:
  - Impact of data corruption on machine learning algorithms.
  - Design of robust machine learning algorithms.
  - Machine learning based on the simulated data.

INTERACTION WITH OTHER PROJECTS

- For practical validation of PMU data streams that have been compromised and their impact for the system, we will leverage a network of relay units with synchrophasor capabilities installed across the Oregon State University – Corvallis campus with support from the Bonneville Power Administration, TIP #328.

FUTURE EFFORTS

- We plan to consider other control and protection applications in power systems that can benefit from the proposed secure machine learning approach. For instance, we will investigate load shedding schemes and substation relaying configurations under emergency operations due to cyber attack.

[1] https://github.com/ecotillasanchez/cosmic

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY