Towards Attack Resilient Data Analytics for Power Grid Operations

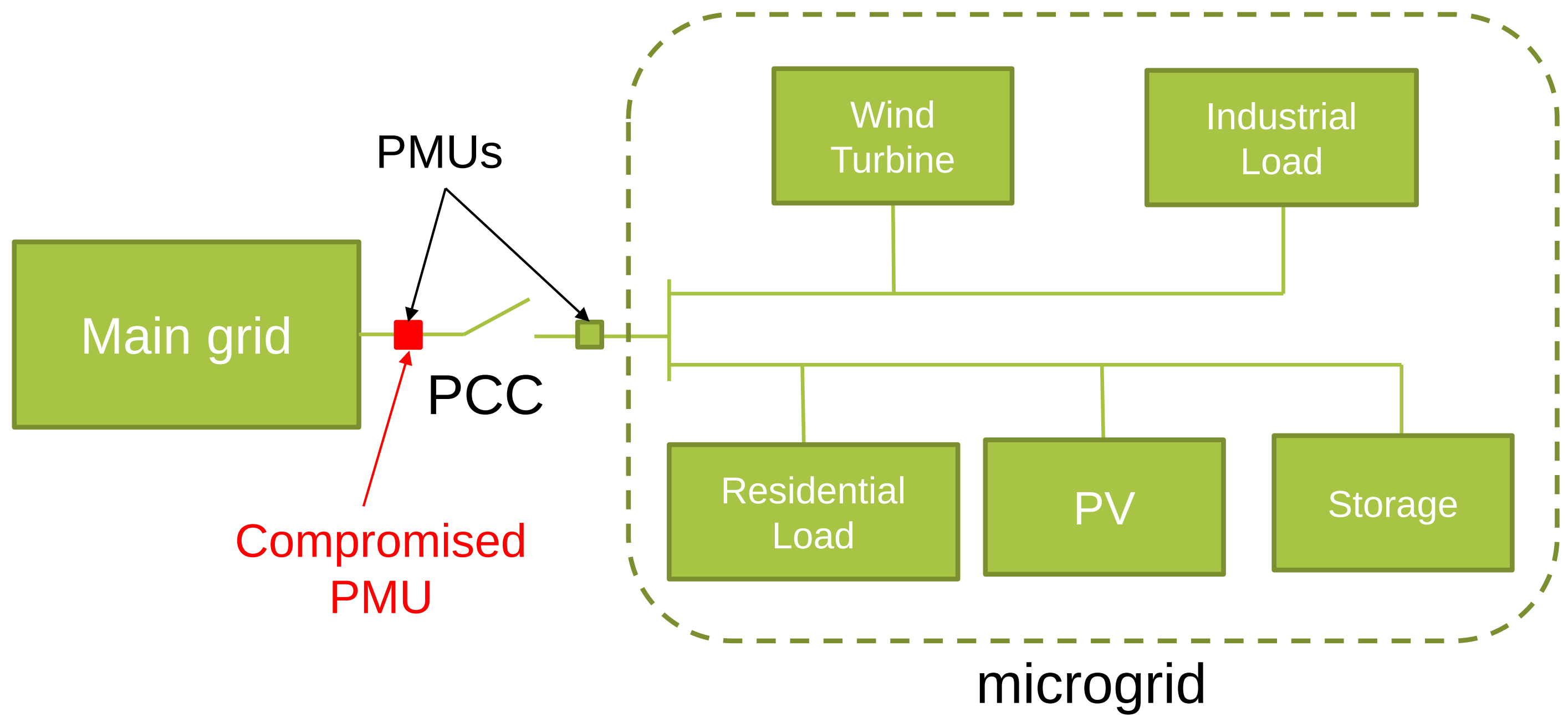
Carter J. Lassetter, Eduardo Cotilla-Sanchez, and Jinsub Kim

GOALS

- **To develop attack resilient data analytics** for power grid operations that can advise operators with proper control decisions even in the presence of **data integrity attacks**. Such techniques are essential for assuring that power system control and protection schemes can function properly to isolate faults, mitigate damage, and recover lost components, in the presence of an on-going attack.
- To develop attack-resilient data analytics to aid **microgrid islanding/ reconnection** and **protective relay control** based on **PMU** data.
- **To establish academe-industry collaboration** for prototyping and potential deployment

FUNDAMENTAL QUESTIONS/CHALLENGES

- Critical power system control and protection decisions such as microgrid islanding, relay tripping, and load shedding are inherently data-dependent, and they are vulnerable to data integrity attacks.



< Manually synchronizing PCCs relying on local PMUs>.

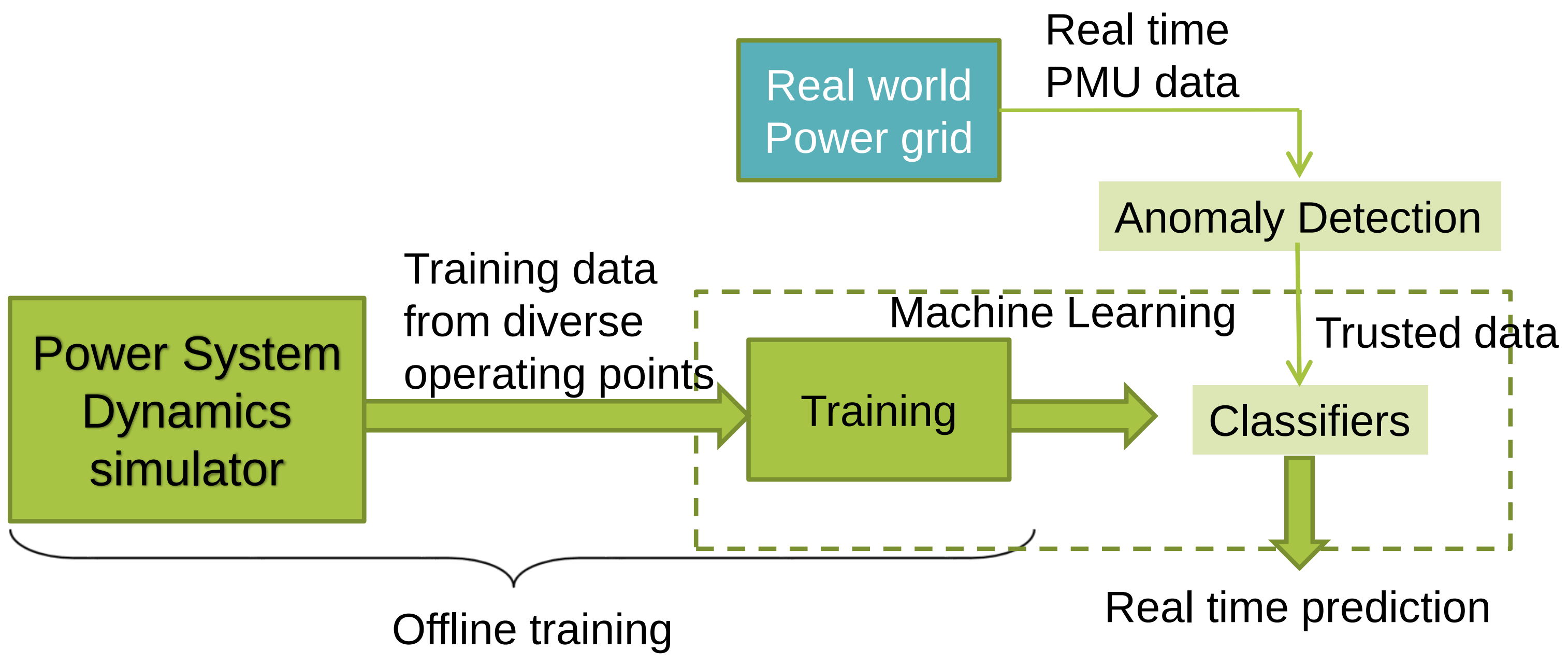
- Data integrity attacks can be carried out as a part of a larger attack effort.
- In order to mitigate the attack impact, the grid needs to be equipped with resilient data analytics that can advise the operators with proper mitigating actions even when part of the input data are compromised.
- Fundamental questions we aim to address are:
  - (*Vulnerability assessment*) How vulnerable are existing power system protection and microgrid control schemes?
  - (*Resilient analytics development*) How can we design data analytics for grid operations such that they can be resilient to partial corruption or loss of input data?
  - (*Real world deployment*) How can we make the proposed approach practically feasible? We aim to make our technique satisfy practical requirements such as latency constraints, accuracy, reliability, etc.

RESEARCH PLAN

- In order to build attack resilient analytics for microgrid islanding/ reconnection and power system protection:

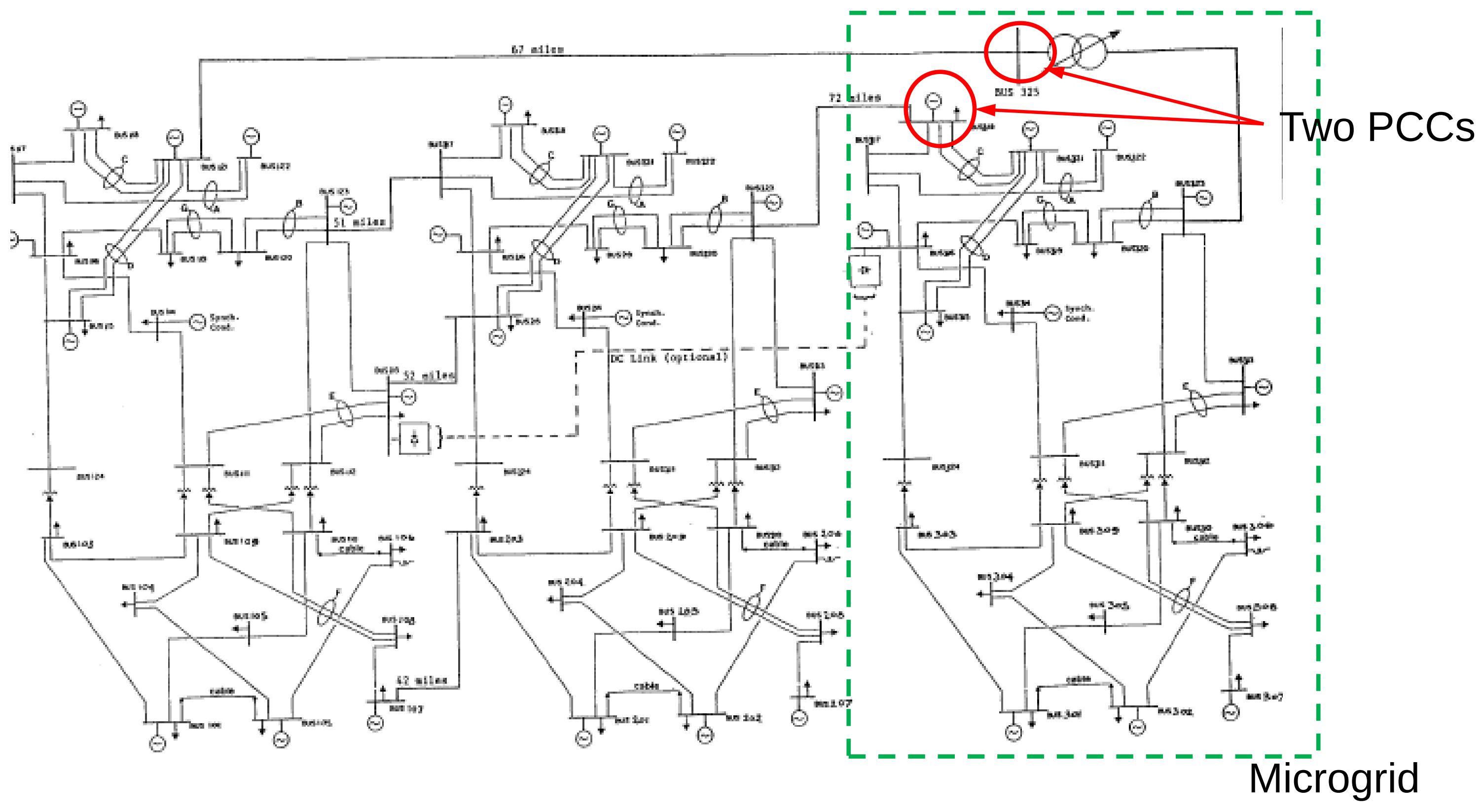
  Unlike the benchmark approaches of feedback control based on a fixed set of local measurements, we will:
  - enlarge the input dataset,
  - incorporate machine learning techniques,
  - incorporate an adaptive input data selection (anomaly detection)

  to improve the resiliency to falsified input data as well as the accuracy.



- **Task 1:** Vulnerability assessment of existing microgrid control and power system protection schemes.
- **Task 2:** Develop data analytics for power system protection (load shedding/protective relay operations) that is resilient to data integrity attacks
- **Task 3:** Performance evaluation under practical attack scenarios (e.g., PMU spoofing attack)
- **Task 4:** Work with industry partners for verification and validation

RESEARCH RESULTS



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

- Developed an attack-resilient data analytics to *predict timings for stable reconnection of an islanded microgrid*.
  - An anomaly detector based on low-rank PMU data matrix estimation processes PMU data
  - The trusted subset of PMU data is passed to a support vector classifier as inputs.
- GPS spoofing attacks on PMUs were considered for evaluation.
- **RTS-96 Performance:** 87% accuracy in predicting unstable reconnection. When tested with the RTS-96 case, our prediction algorithm achieved around 92% accuracy in predicting stable reconnection.
- **Poland Performance:** To test the performance on a large-scale grid, we tested the analytics with the Poland test case. To test scalability, we trained our analytics using training data from only a few operating points and tested it with input data generated from unseen operating points. The classifier was able to predict stable cases with an accuracy of 82.6% and unstable cases with 83.9% accuracy.

BROADER IMPACT

- The results of this project are expected to contribute to improving resiliency of the nation's grid to cyber-adversarial attempts to induce a cascading failure. Developed analytics will be able to advise reliable mitigating actions under an ongoing attack.
- The developed framework is expected to be applicable to other energy sectors to improve resiliency of the delivery systems to cyber attacks.
- The developed techniques are expected to improve the state-of-the-art of power system protective schemes in terms of robustness to sensor failure.

INTERACTION WITH OTHER PROJECTS

- For practical validation of compromising PMU data streams, 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 #380.

FUTURE EFFORTS

- Plan to improve the classification and anomaly detection accuracy by leveraging other learning schemes such as deep neural network.
- Seeking industry collaborators to validate our technique in a real-world environment and work together to realize its real-world deployment.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY