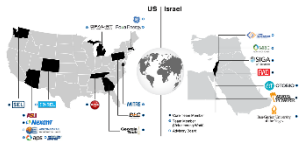


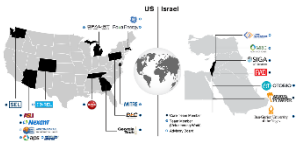
Enhancing Cybersecurity of Grid Operations

Lalitha Sankar
Associate Professor
Arizona State University

28 September 2022

ARIZONA STATE UNIVERSITY

Enhancing Cybersecurity of Grid Operations

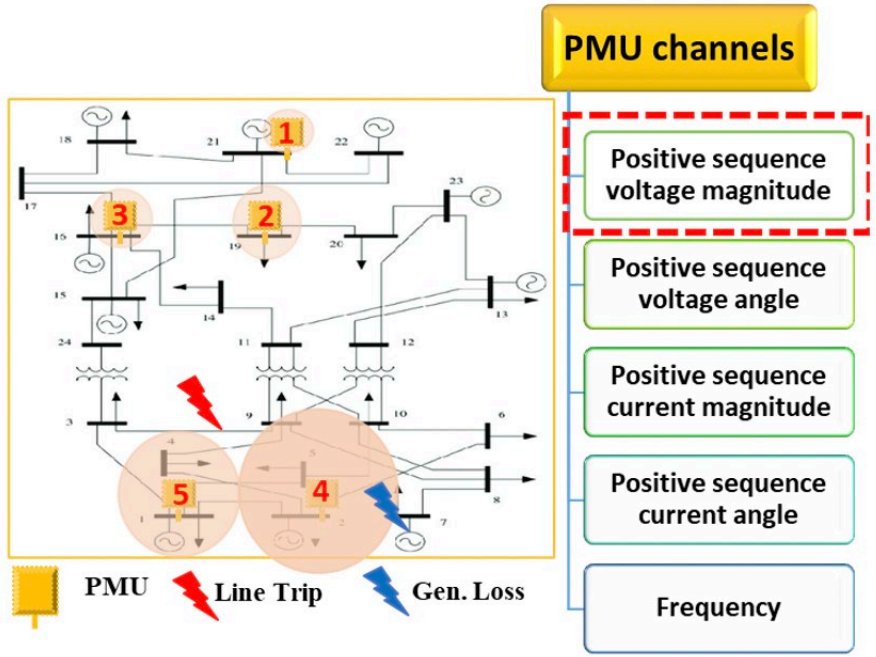


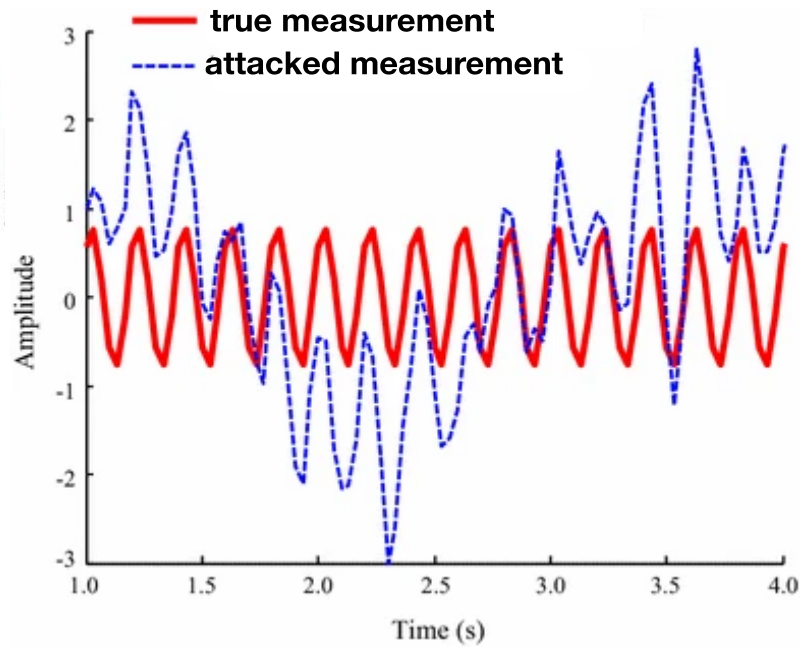
Task 5: Generate event-mimicking attacks

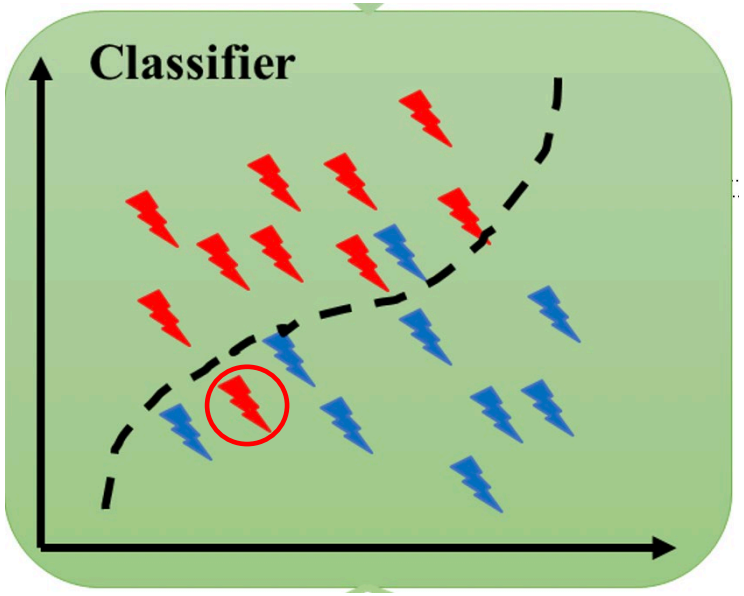
Task 8: Detect event-mimicking attacks ✓

Commercialization: Evaluate attacks on Nexant's (Resource Innovations) EMS Platform ✓

Task 5: Recap





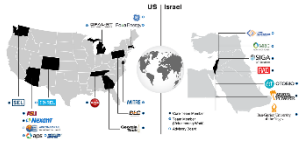


Challenge: Adding white noise or some arbitrary mode is not sufficient

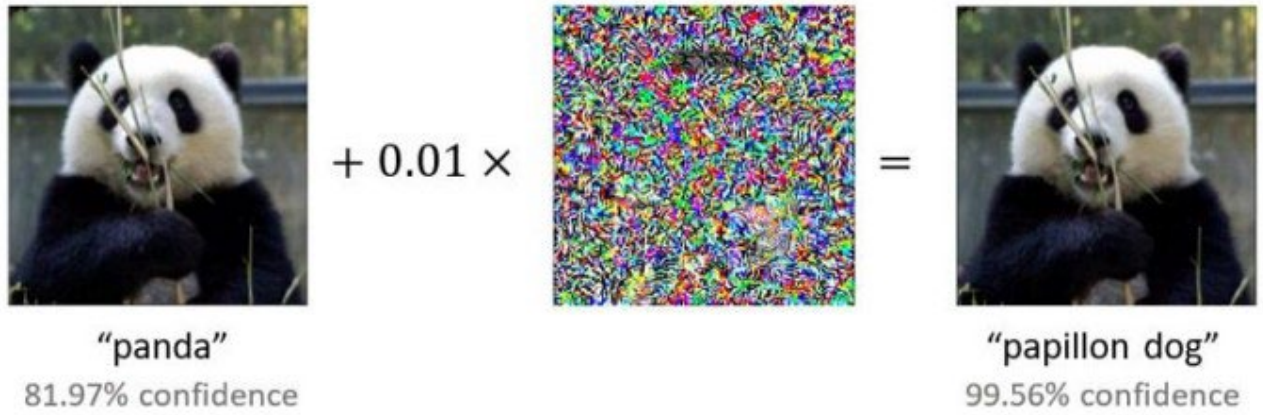
Work in progress:

- Extend existing binary classifier to multi-class classifier to include attacks
- Identify the key set of features that can change normative data to mimic an event
- Integrate new synthesized attacks to the existing database

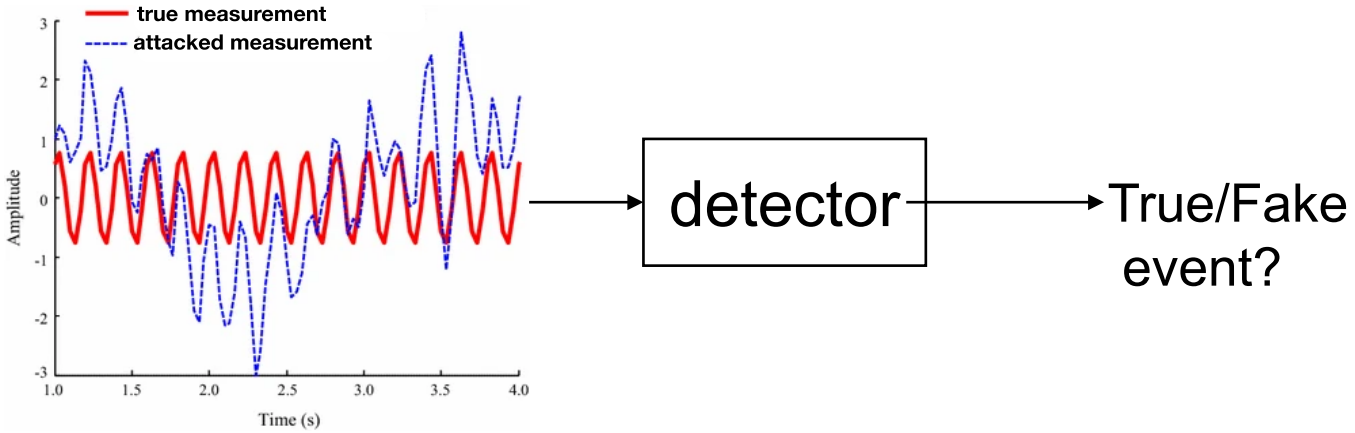
Task 8: Detect Sophisticated (Mimicking) Attacks



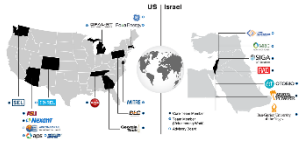
- Existing robust detectors of static data



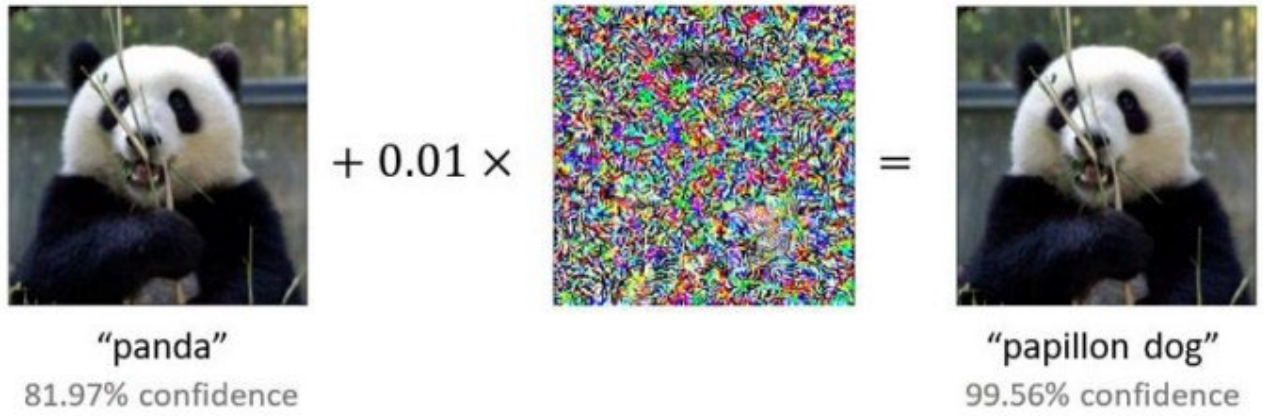
- Power system data is dynamic?



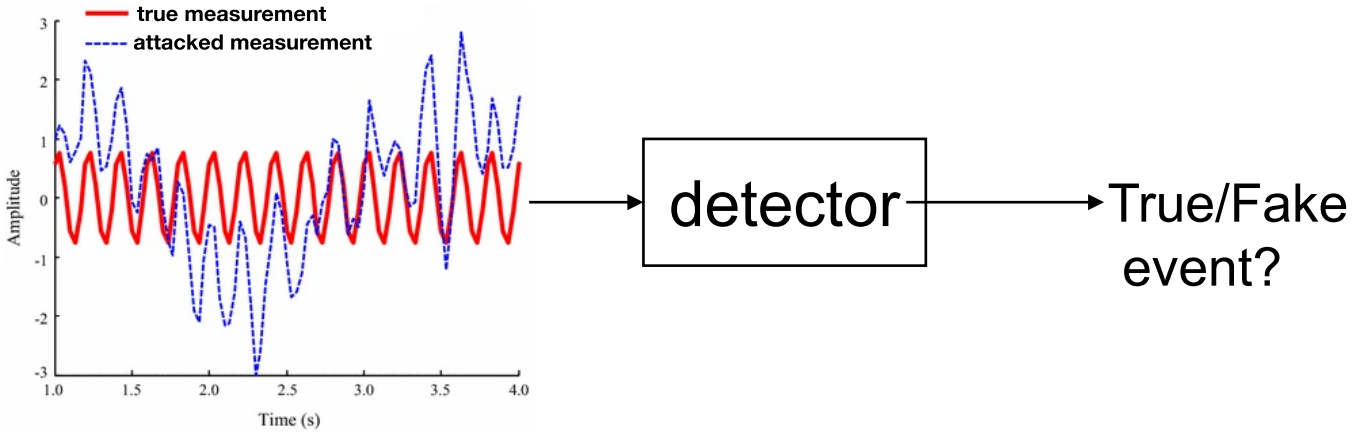
Task 8: Detect Sophisticated (Mimicking) Attacks



- Existing robust detectors of static data



- Power system data is dynamic?



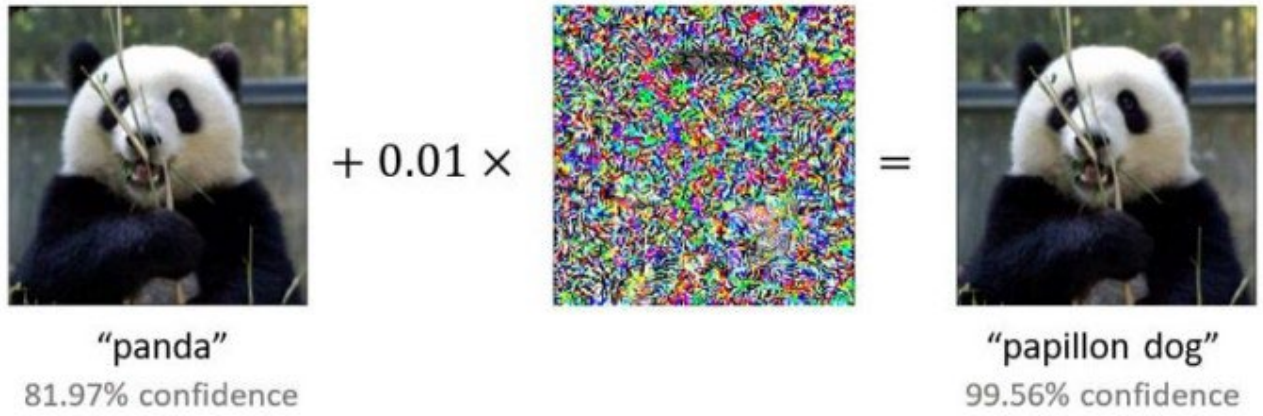
Objective: Design modular detectors capable of detecting anomalies via PMU measurements

Our Method: Online ML detector that exploits **event features** to:

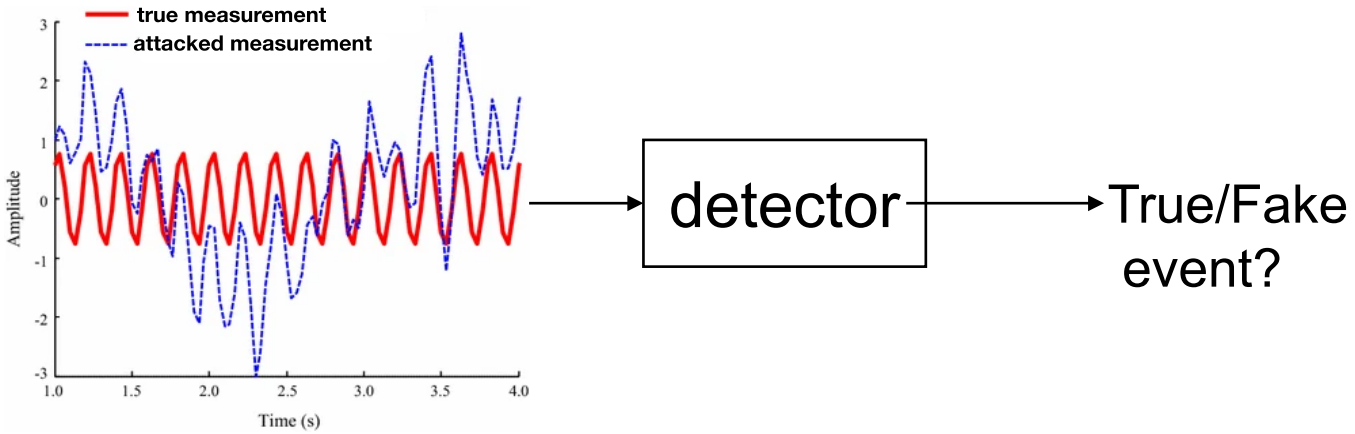
- compare *features* of true events against fake events

Task 8: Detect Sophisticated (Mimicking) Attacks

- Existing robust detectors of static data



- Power system data is dynamic?



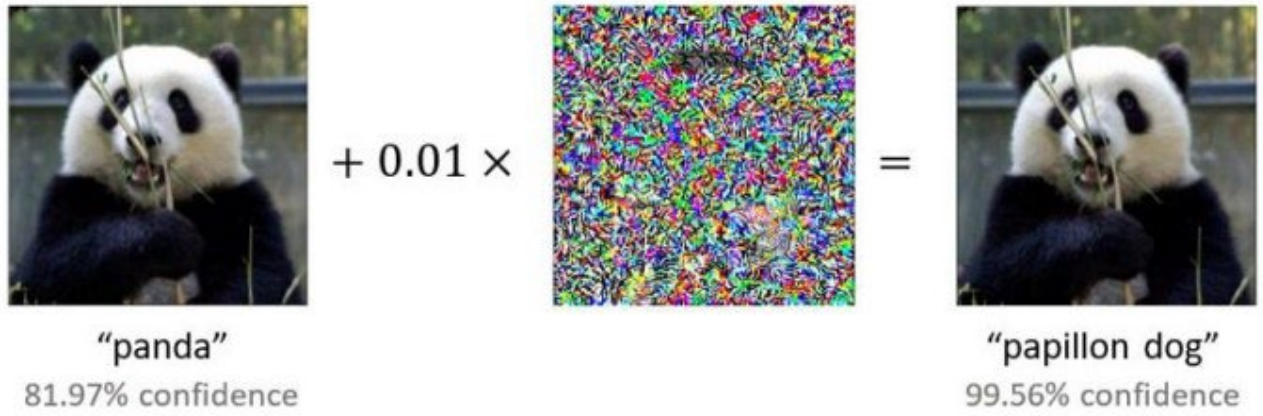
Objective: Design modular detectors capable of detecting anomalies via PMU measurements

Our Method: Online ML detector that exploits **event features** to:

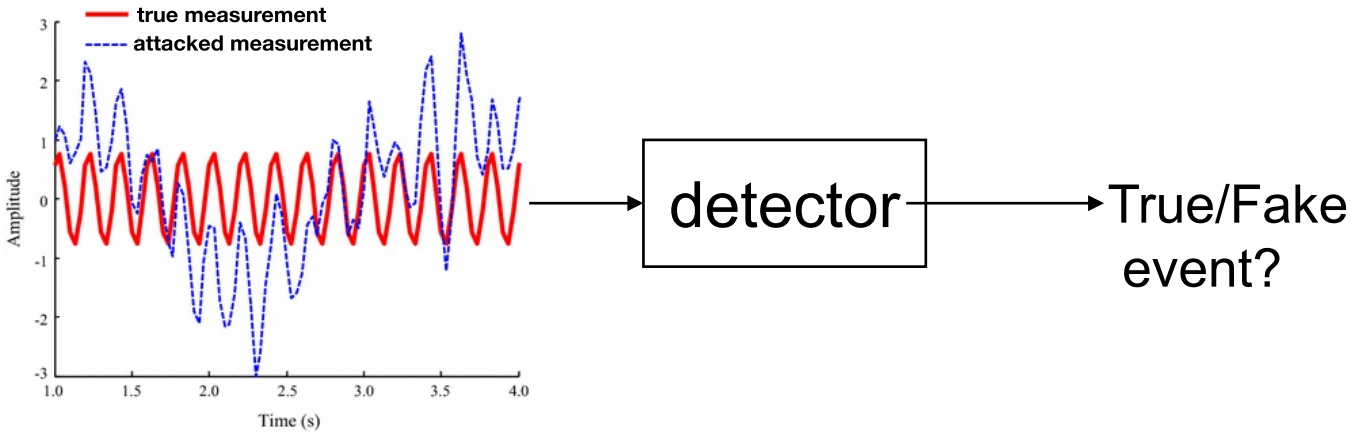
- compare *features* of true events against fake events
- Incorporate (*physics-based*) *priors* to make detectors robust

Task 8: Detect Sophisticated (Mimicking) Attacks

- Existing robust detectors of static data



- Power system data is dynamic?

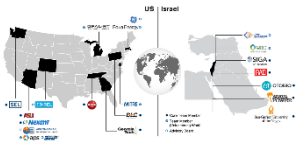


Objective: Design modular detectors capable of detecting anomalies via PMU measurements

Our Method: Online ML detector that exploits **event features** to:

- compare *features* of true events against fake events
- Incorporate (*physics-based*) *priors* to make detectors robust
- Include *spatio-temporal characteristics* (e.g., frequency, event source) for distinguishability

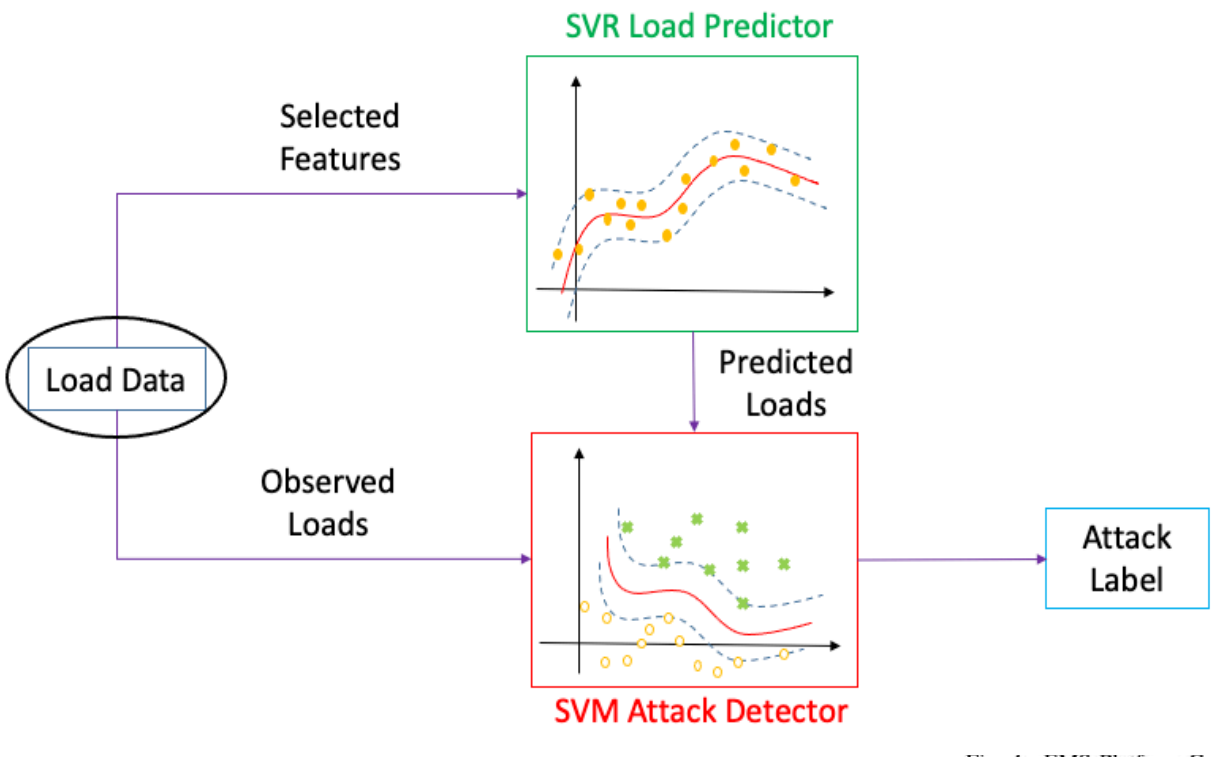
Summary and Future of Task 8



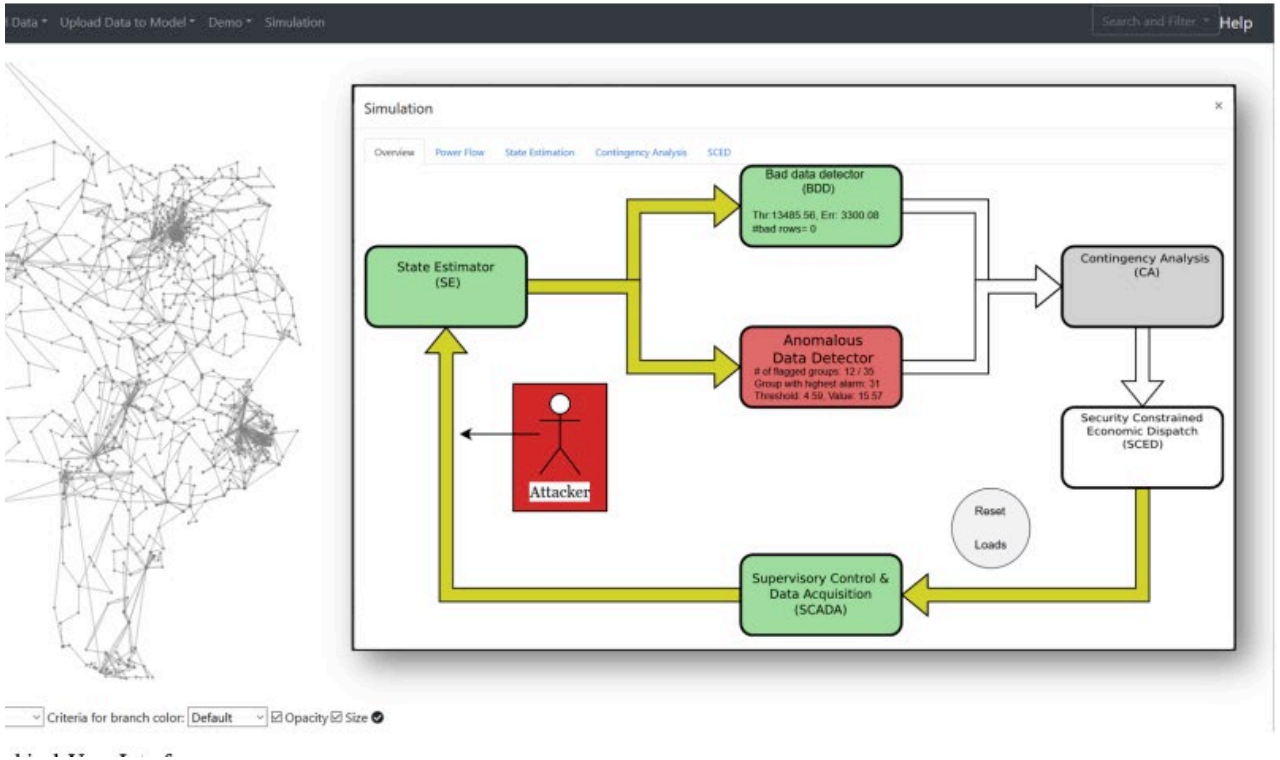
Task 8	Status (Work in progress)	Work to be done
• Design robust detectors and test it against attacks • Explore commercialization	• Detector design in progress (for events) • Testing its efficacy to attacks (in progress)	• Evaluate detectors from Task 5 with new attacks (Q3) • Incorporate prior knowledge: - (i) Use prior (historical) data to identify if event pattern is meaningful (e.g., k- NN on event features) (Q5) - (ii) Design a risk predictor method for operators. (Q7) • Work with Resource Innovations on Commercialization

Commercialization

Prior OT Software Incorporate (*physics-based*) *priors* to make detectors robust



(a) SVM and SVR based detector to detect load altering attacks.



(b) Cyber attack detector on Energy Management Systems (EMS)

[1] C. Zhigang, O. Kosut, and L. Sankar. "Detecting load redistribution attacks via support vector models." *IET Smart Grid*, 2020
[2] A. Pinceti, L. Sankar, and O. Kosut. “Detection and Localization of Load Redistribution Attacks” *J. of Modern Power Systems and Clean Energy, 2021*

Task 5 (a): Learn Event Signatures from Measurements