Oregon State University

Towards Attack Resilient Data Analytics for Power Grid Operations

Travis Hagan, Shashini De Silva

Advisors: Dr Eduardo Cotilla-Sanchez, Dr. Jinsub Kim

April 27, 2018

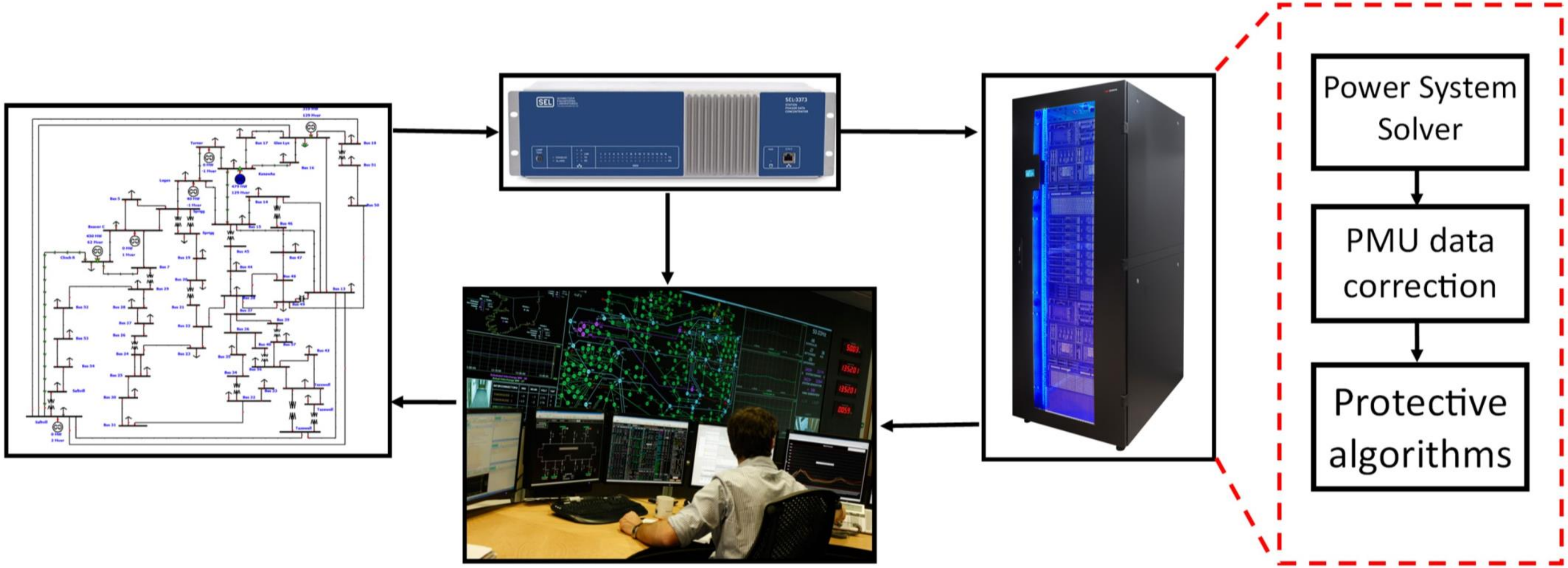
Oregon State University
College of Engineering

Motivation

- Modernizing power grid
- Bad data = bad decisions
- Blackouts
- Why GPS attacks?

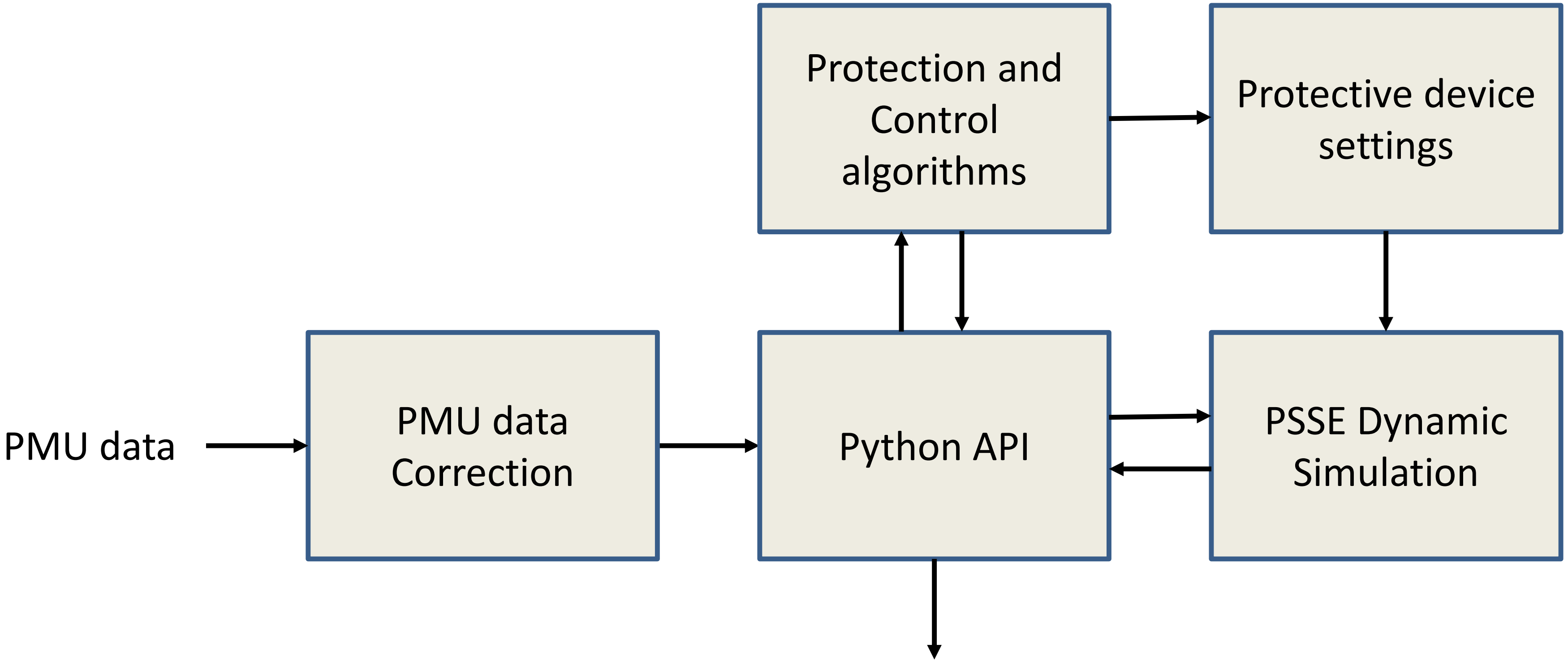
Oregon State University
College of Engineering

Project Description



Oregon State University
College of Engineering

Overview of Approach



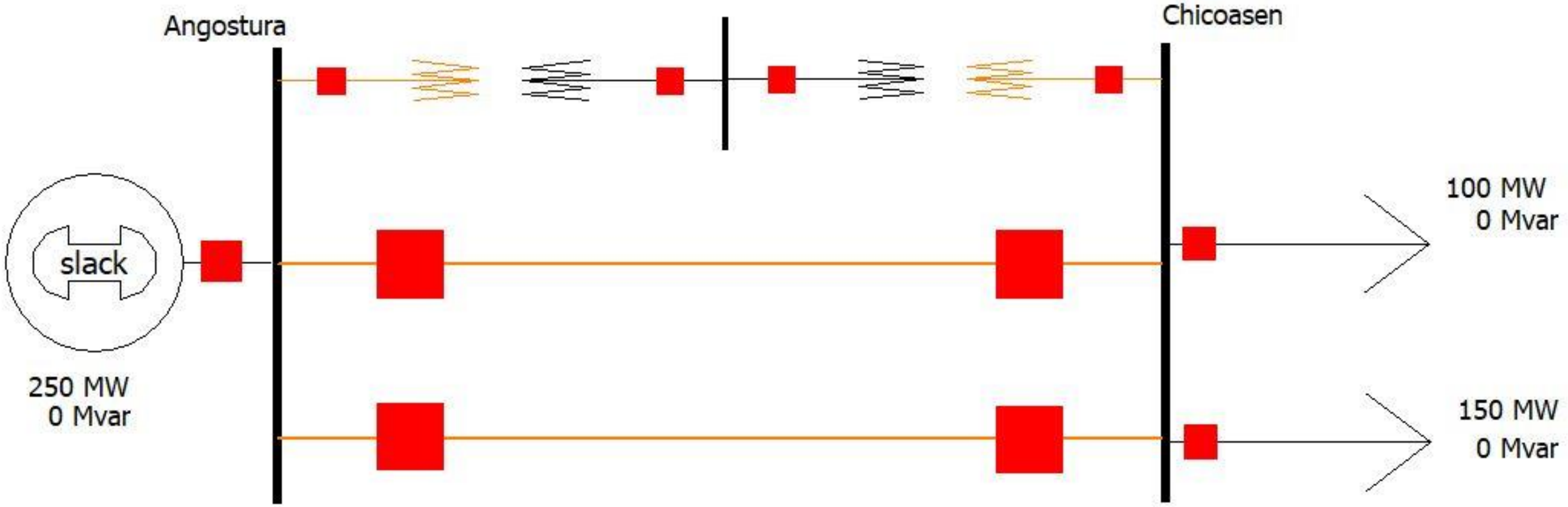
Control Actions:
- Update relay settings
- Load shedding
- Line/Generator disconnect

Realistic attacks on PMU devices

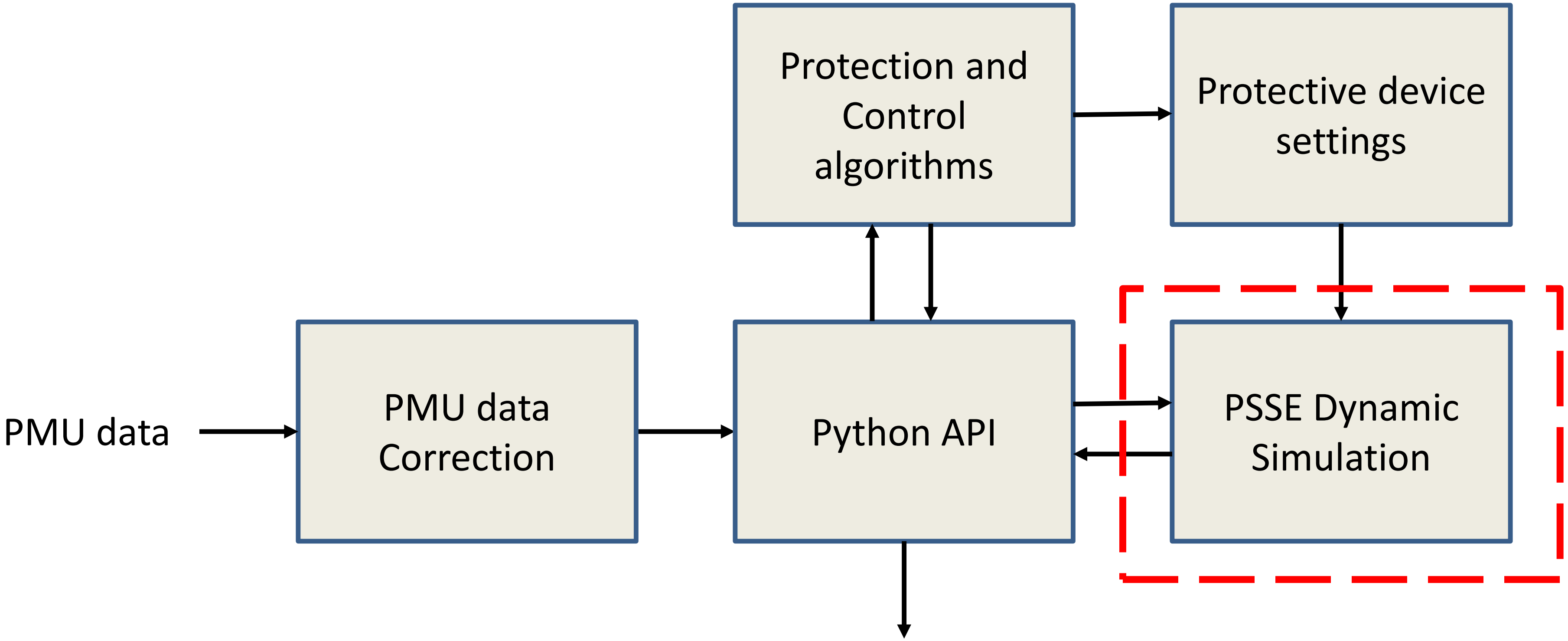
- Removing from service
- Hacking PMU to PDC connection
- GPS Jamming
- Spoofing

Case Study: Chicoasen-Angostura transmission line

- Carry away clock
- If PMU data goes through PDC, max error is 200 ms



Overview of Approach

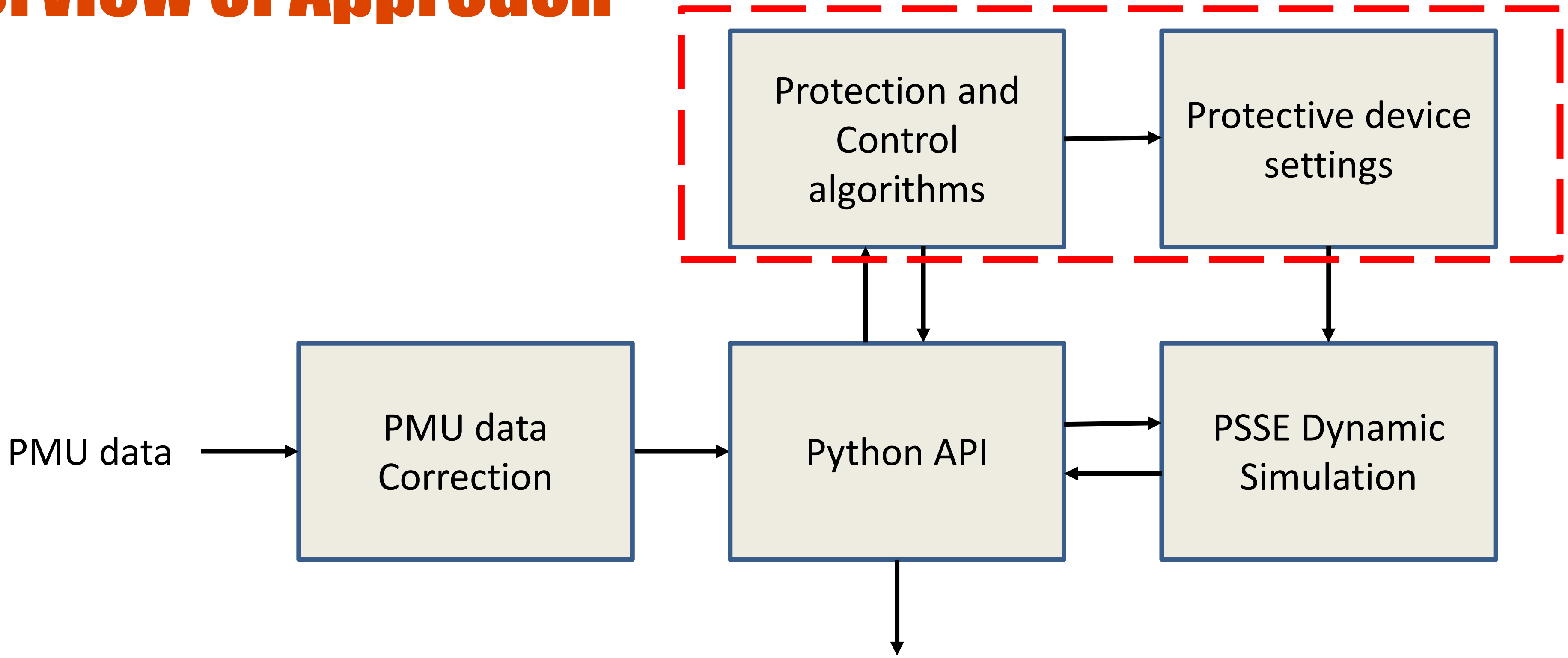


Control Actions:
- Update relay settings
- Load shedding
- Line/Generator disconnect

PSS®E Simulation

- RTS 1996
- Creating a realistic power grid
  - Primarily based on BPA recommendations and current grid operations
  - Implementing an angle change attack

Overview of Approach



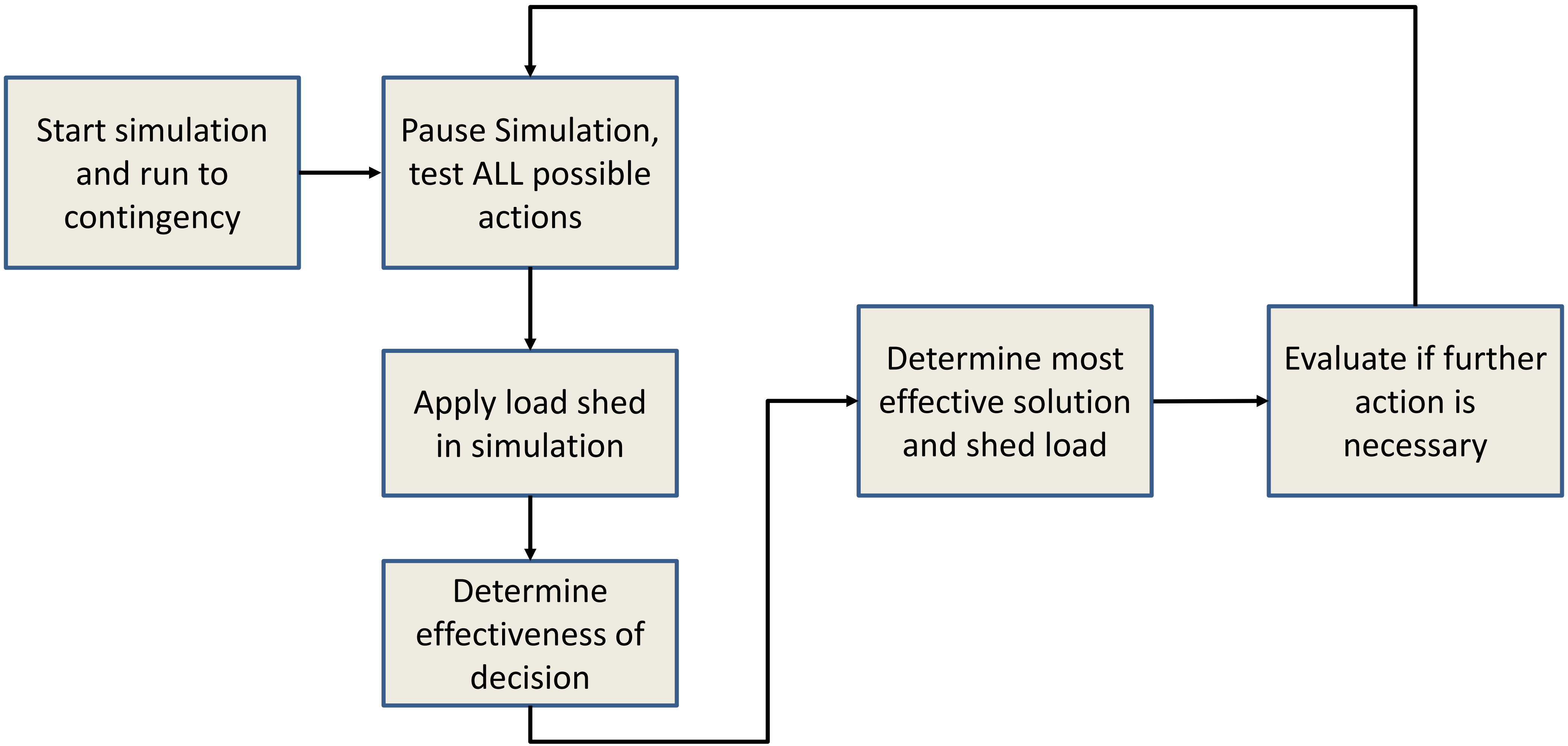
Control Actions:
- Update protection settings
- Load shedding
- Line/Generator disconnect

Simulation - Protective devices

- Overcurrent relay
- Frequency/voltage relay
- Distance relay
- Volts/Hertz relay
- Load shedding relay
- No differential relay in PSSE

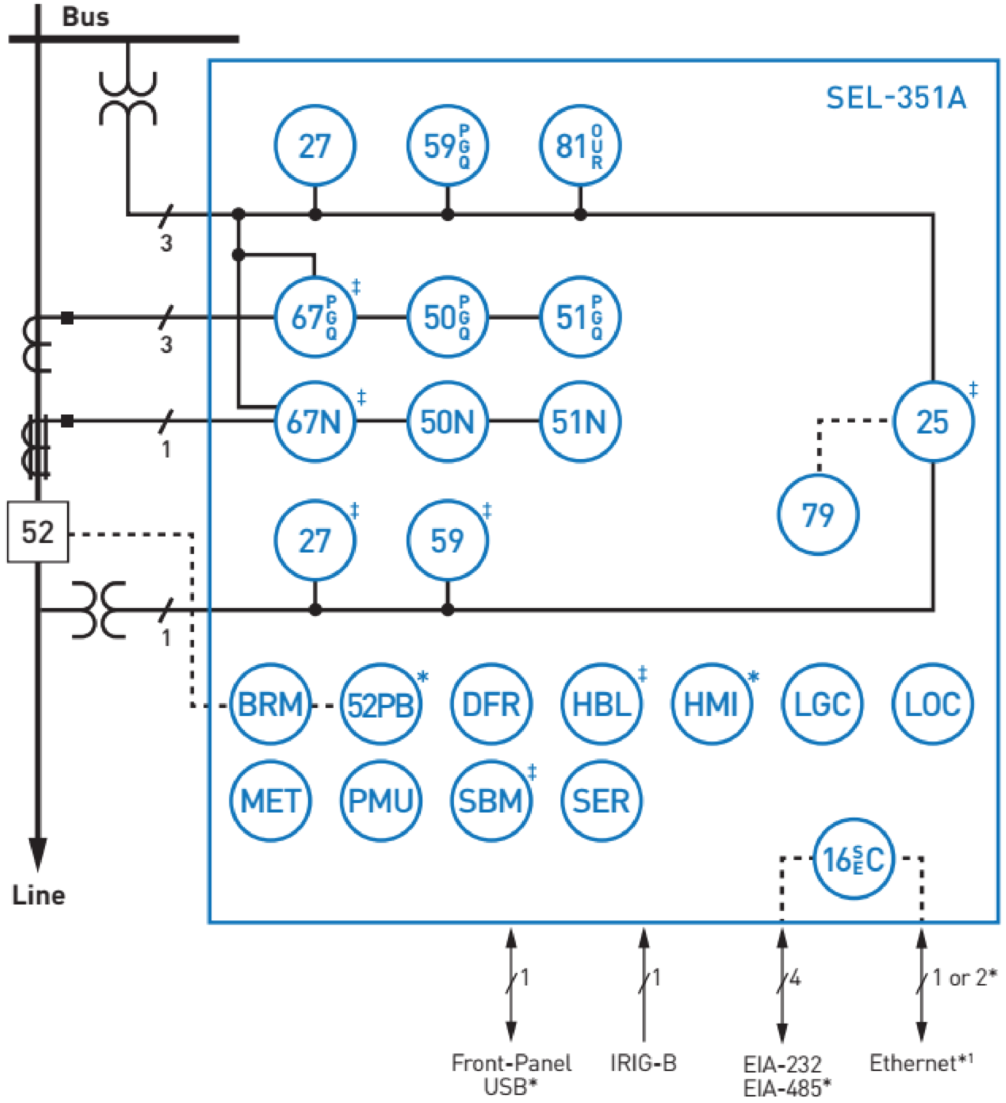
Devices	Count	Protective devices (typ)	Protective device (sim)	
Buses	73	2	0	0
Loads	51	2	1	51
Generators	99	2	5	495
Branches	105	3	2	210
Transformers	16	3	1	16
Total				772

Simulation – Rollout Policy



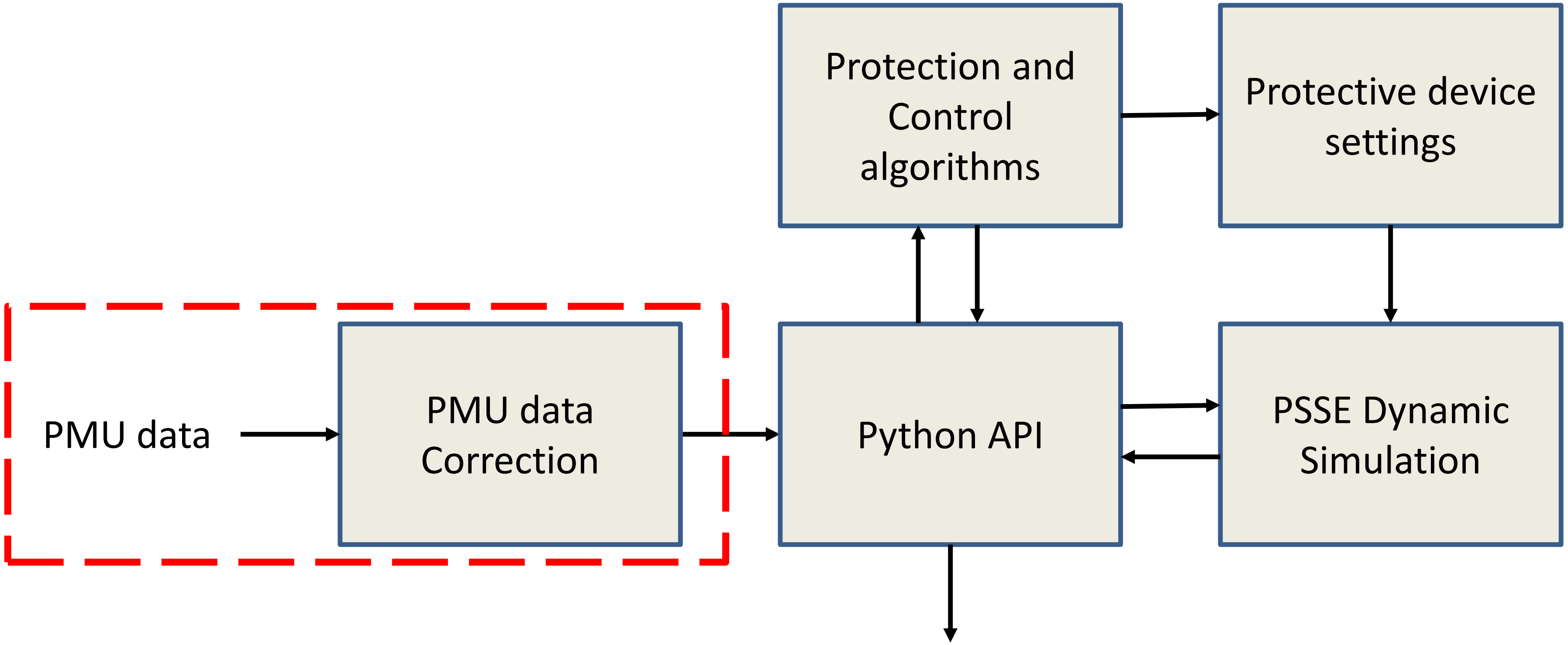
Connection to real devices

- PMUs and relays
- Six settings groups
- USB, Ethernet, Serial



Oregon State University
College of Engineering

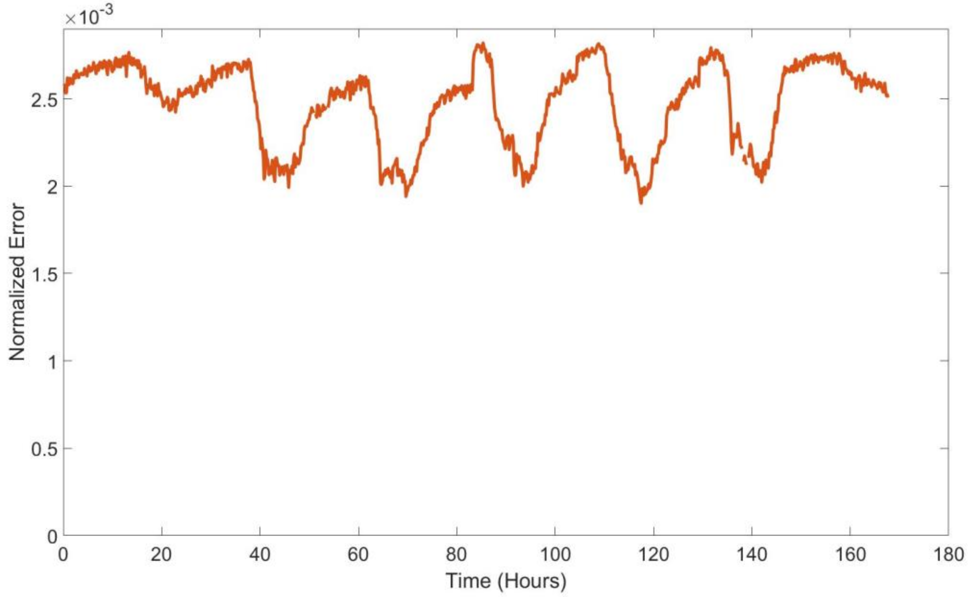
Overview of Approach



Control Actions:
- Update protection settings
- Load shedding
- Line/Generator disconnect

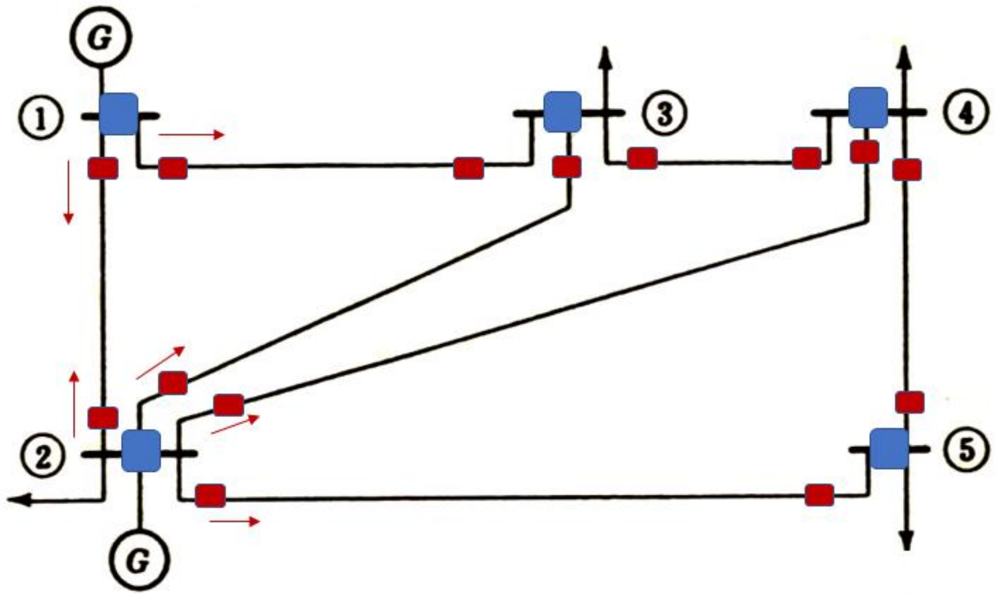
Motivation

- Observing a low dimensional subspace for real time PMU data



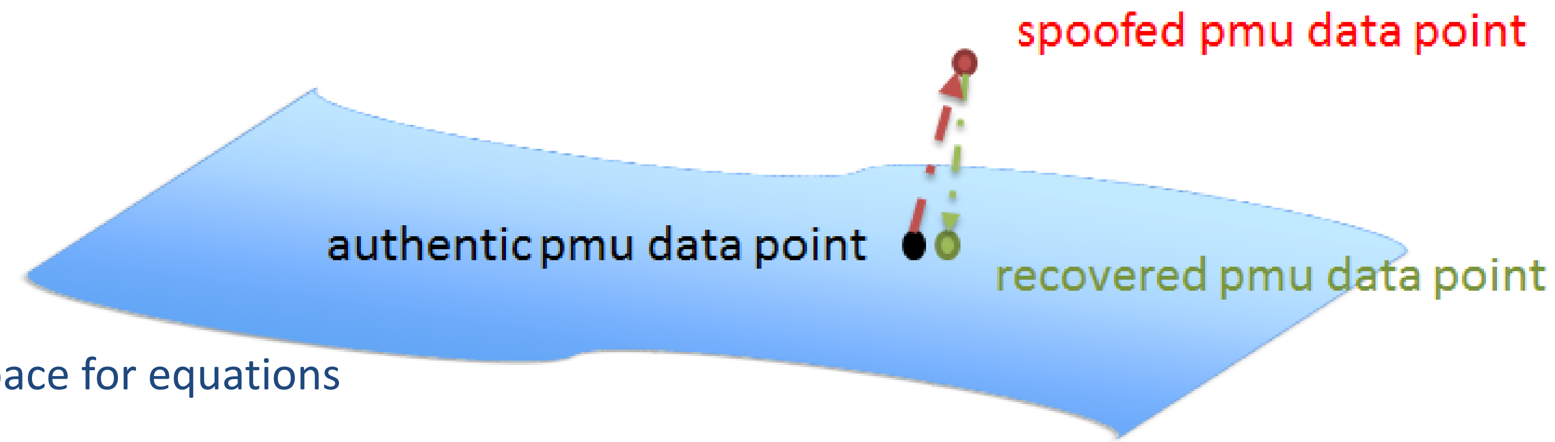
Motivation Contd.

- Measurements collected from the power network are constrained by Kirchoff laws.



High-level Idea

- Use the knowledge of the solution space to detect and mitigate the effect of data attacks



Solution space for equations

PMU Measurement model

- Voltage phasor and outgoing power flow measurements collected from sparsely deployed PMUs

$$y = h(\theta) + e + a$$

$y =$ PMU measurement vector

$\theta =$ State vector

$a =$ Attack vector

$h(.) =$ Nonlinear measurement function

$e =$ Gaussian random noise vector

Oregon State University
College of Engineering

SCADA Measurement model

- Outgoing power flow and power injection measurements collected from a **trustworthy** set of SCADA meters

$$b = g(\theta) + e$$

b = SCADA measurement vector

$g(.)$ = Nonlinear measurement function

θ = State vector

e = Gaussian random noise

Data Correction Approach

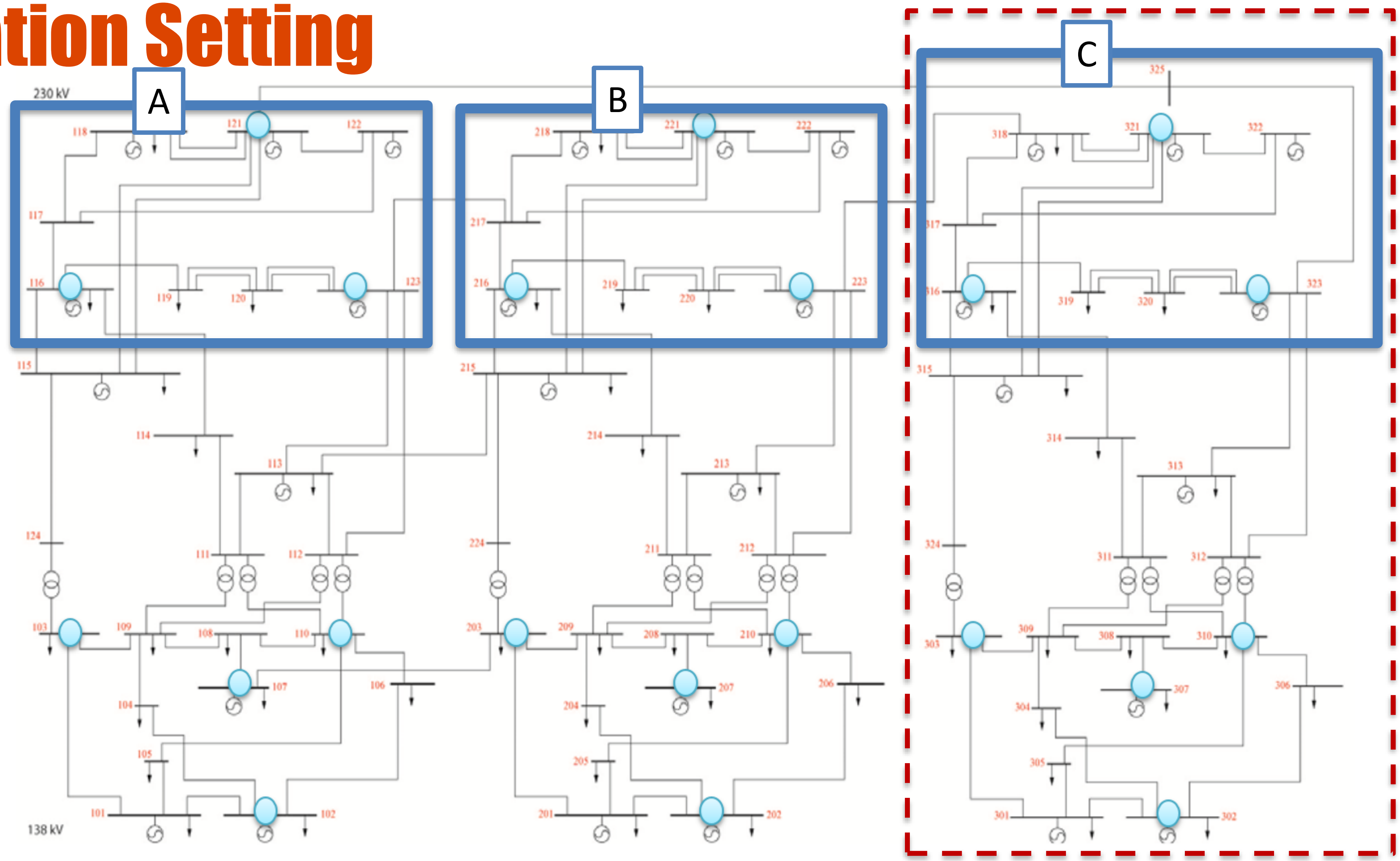
- Leverage both PMU and SCADA measurements

$$\theta^* = \text{argmin}_\theta \left\| \begin{bmatrix} y \\ b \end{bmatrix} - \begin{bmatrix} h(\theta) \\ g(\theta) \end{bmatrix} \right\|_2$$

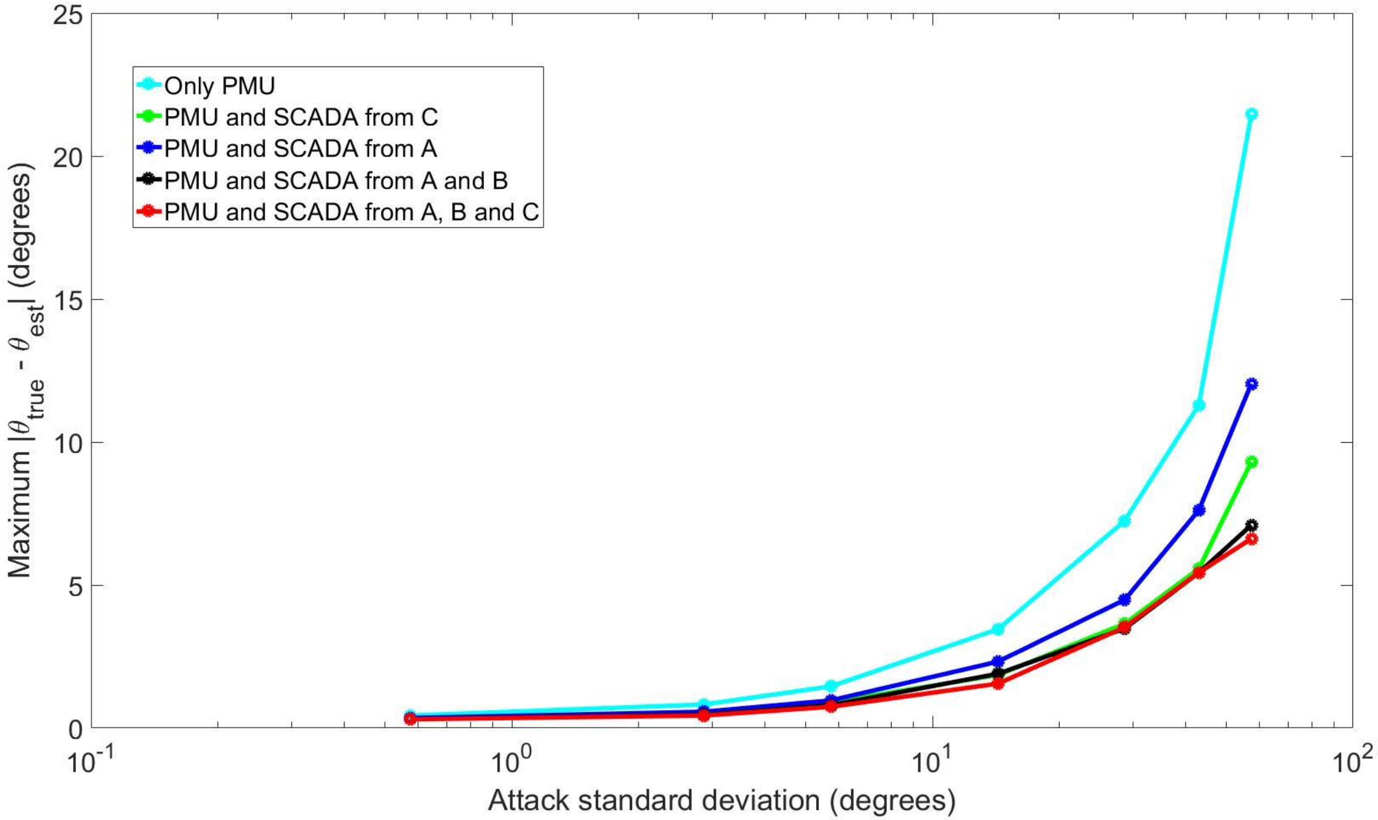
$$\hat{y} = h(\theta^*)$$

Oregon State University
College of Engineering

Simulation Setting



Simulation Results



Oregon State University
College of Engineering

Future Steps

- Validate protection settings
- Integrated framework

Oregon State University
College of Engineering

Questions