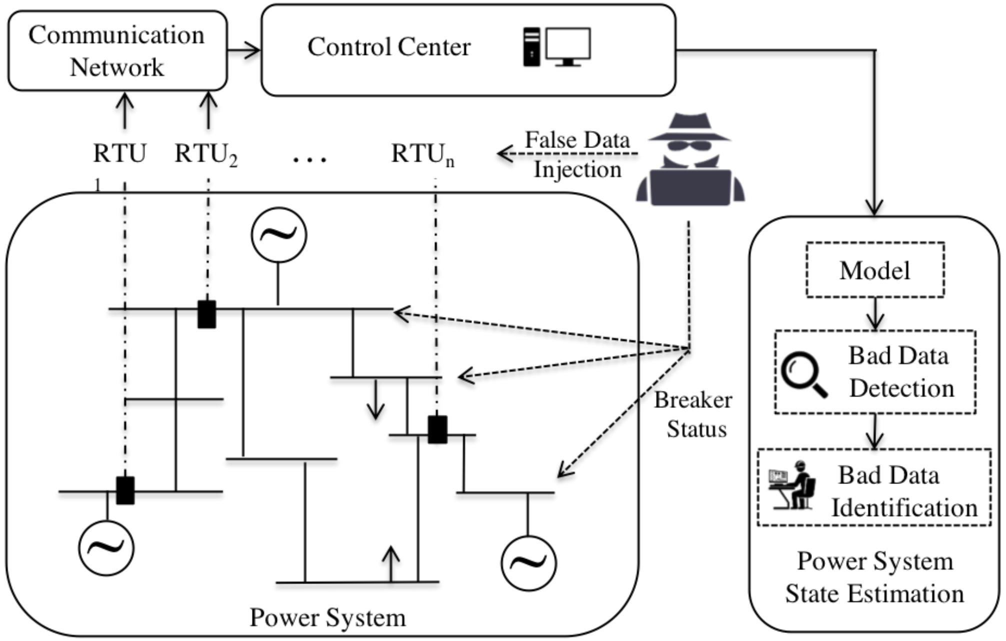
Multi-Model Resilient Observer Under False Data Injection Attacks

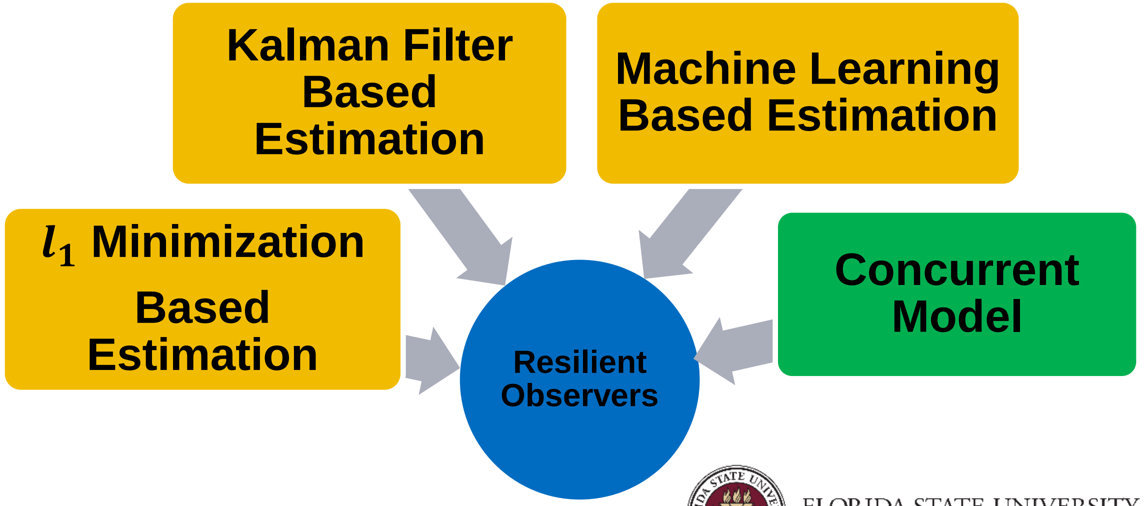
O. M. Anubi
C. Konstantinou
C. A. Wong*
S. Vedula

FLORIDA STATE UNIVERSITY
CENTER FOR ADVANCED POWER SYSTEMS

Motivation

- Existing resilient observers rely on model of the physical side mainly
- Cleverly crafted FDIA can bypass physics-based only detectors/monitors
- Integrating cyber-side and physical-side model for a resilient estimator is a challenging problem
- Concurrent model can improve state-of-the art resilient estimators
  - Data-Driven model for the cyber side
  - Physics-based model for physical side





Problem Statement

Setup

- Overview of Resilient Estimators:
  - Error correction problem
  - Compressive sensing problem
  - l_0 minimization (nonconvex) ⟶ l_1 minimization (convex)
  - Above relaxation holds under restricted isometric property (RIP)

- A globally convex approximation to the moving horizon compressive sensing problem with
  - The RIP condition
  - Linear time-invariant (LTI) system model
  - Auxiliary data-driven model

$$\underset{\mathbf{e}}{\text{Minimize:}}\ \|\mathbf{e}\|_{l_0} \quad \text{Subject to:} \quad \tilde{\mathbf{y}} = F\mathbf{e}.$$

$$\underset{\mathbf{e}}{\text{Minimize:}}\ \|\mathbf{e}\|_{l_1} \quad \text{Subject to:} \quad \tilde{\mathbf{y}} = F\mathbf{e}.$$

$$\begin{aligned} &\text{Minimize:} && \left\|\mathbf{y}_{(T)} - H_{(T)}\mathbf{u}_{(T-1)} - \Phi_{(T)}\mathbf{x}\right\|_1 \\ &\text{Subject to:} && \\ & && \left\|\Phi_T\mathbf{x} + H_T\mathbf{u}_{(T-1)} - \boldsymbol{\mu}(\mathbf{z_k})\right\|^2_{\Sigma^{-1}(\mathbf{z}_k)} \le \chi^2_m(\tau), \end{aligned}$$

$$\mathbf{y}_{(T)} = \begin{bmatrix} \mathbf{y}_{k-T+1} \\ \mathbf{y}_{k-T+2} \\ \vdots \\ \mathbf{y}_k \end{bmatrix} \in \mathbb{R}^{mT},\ \mathbf{u}_{(T-1)} = \begin{bmatrix} \mathbf{u}_{k-T+1} \\ \mathbf{u}_{k-T+2} \\ \vdots \\ \mathbf{u}_{k-1} \end{bmatrix} \in \mathbb{R}^{l(T-1)},$$

$$H_{(T)} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ CB & 0 & \dots & 0 \\ CAB & CB & \dots & 0 \\ \vdots & \vdots & & \vdots \\ CA^{T-2}B & CA^{T-3}B & \dots & CB \end{bmatrix} \in \mathbb{R}^{mT\times l(T-1)},\ \Phi_{(T)} = \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{T-1} \end{bmatrix} \in \mathbb{R}^{mT\times n}$$

Problem Statement

- Optimization Problem:
  - Formulation used for the numerical studies
  - Returns an estimate of the state vector
  - Current state estimate using physics based model and forward propagation

- Equivalent Optimization Problem:
  - If a receding horizon T is large enough and (A,C) is observable
  - Then there exists $F_{(T)}$ such that $F_{(T)}\Phi_{(T)} = 0$
  - Following is the representation for optimization problem discussed before

$$
\begin{aligned}
&\text{Minimize:} \quad \|\mathbf{e}\|_1 \\
&\text{Subject to:} \\
&\qquad \mathbf{f}_{(T)} = F_{(T)}\mathbf{e} \\
&\qquad \left\|\mathbf{y}_T + \mathbf{e}_T - \boldsymbol{\mu}(\mathbf{z_k})\right\|^2_{\Sigma^{-1}(\mathbf{z}_k)} \leq \chi^2_m(\tau),
\end{aligned}
$$

  - e_T, $y_T \in \mathbb{R}^m$ is the vector containing the last *m* elements of the respective vectors *e, y* in order.
  - Used in the proof of the main theorem

Results

Theorem 1 *Given a dataset $\mathcal{D} = \{\mathbf{Z}, \mathbf{Y}\}$ containing historical auxiliary variables $\mathbf{Z} \in \mathbb{R}^{p \times T}$ and corresponding sensor measurements $\mathbf{Y} \in \mathbb{R}^{m \times T}$. Suppose that the latent sensor measurement satisfies the data-driven GPR prior given and that there exists $\tau \in (0,\ 1)$ such that the true measurement $\mathbf{y}_k^*$ satisfies $p(\mathbf{y_k}^* | \mathbf{z}_k, \mathcal{D}) \geq \tau$. Consider the convex optimization problem discussed before. Let $\hat{\mathbf{e}}$ be the solution of the equivalent form in the previous slide. If $\delta_{2s}(F_{(T)}) < \frac{1}{\sqrt{2}}$, then, for any feasible sparse vector $\mathbf{e}$,*

$$\|\hat{\mathbf{e}}_T - \mathbf{e}_T\|_2 \leq K_1 sat_1 \left(K_2 \|\mathbf{e} - \mathbf{e}[s]\|_2 \right),$$

where

$$K_1 = \sqrt{2\chi_m^2(\tau)\overline{\sigma}(\mathbf{z}_k)}$$
$$K_2 = K_3 \sqrt{\frac{m - s}{2\chi_m^2(\tau)\overline{\sigma}(\mathbf{z}_k)}},$$

with

$$K_3 = \frac{2}{\sqrt{s}} \left(\frac{\delta_{2s} + \sqrt{\delta_{2s}\left(\frac{1}{\sqrt{2}} - \delta_{2s}\right)}}{\sqrt{2}\left(\frac{1}{\sqrt{2}} - \delta_{2s}\right)} + 1 \right)$$

and $\overline{\sigma}(\mathbf{z}_k)$ is the biggest singular value of $\Sigma(\mathbf{z}_k)$.

Results

Proof Sketch

- The probability of y_k^* given the auxiliary variable z_k and the dataset D must be greater than or equal to τ
- This implies a quadratic inequality
  - A function of composite measurements, y_T corrupted by the sparse error vector, e_T
- True measurement $y_{(T)}^*$ is a function of $\phi_{(T)}$
  - When multiplied by $F_{(T)}$ equals to zero
- Then using Theorem 1 from the paper,
  - The optimal $\hat{e}$ satisfies the following inequality
- With both the stated and quadratic inequalities
  - We can arrive at the stated conditions

$$\begin{aligned}\mathbf{y}_{(T)} &= \mathbf{y}_{(T)}^* + \mathbf{e}_{(T)} \\ &= \Phi_{(T)}\mathbf{x}_{k-T+1} + H_{(T)}\mathbf{u}_{(T-1)} + \mathbf{e}_{(T)}\end{aligned}$$

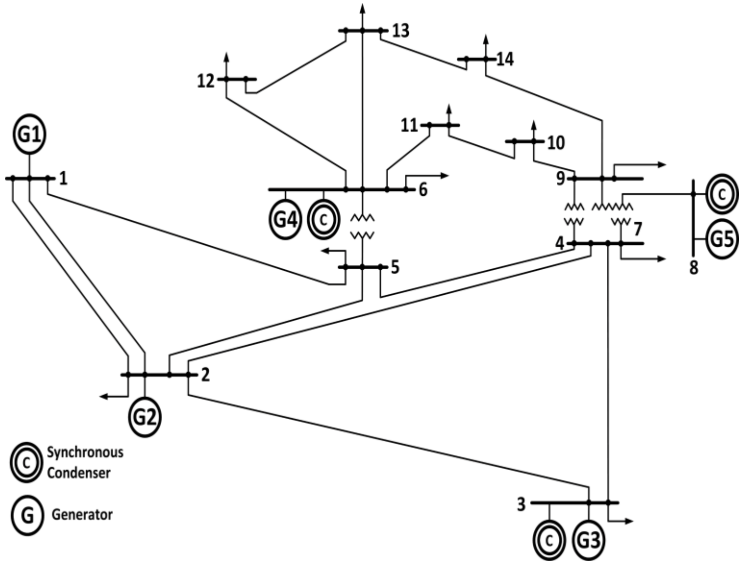
$$\begin{aligned}\mathbf{f}_{(T)} &= F_{(T)}\left(\mathbf{y}_{(T)} - H\mathbf{u}_{(T-1)}\right) \\ &= F_{(T)}\mathbf{e}_{(T)}\end{aligned}$$

$$\begin{aligned}\left\|\hat{\mathbf{e}}_{(T)} - \mathbf{e}_{(T)}\right\|_2 &\leq K_3\left\|\mathbf{e}_{(T)} - \mathbf{e}_{(T)}[s]\right\|_1 \\ &\leq K_3\sqrt{m-s}\left\|\mathbf{e}_{(T)} - \mathbf{e}_{(T)}[s]\right\|_2\end{aligned}$$

Numerical Simulation

System Model

- IEEE 14-bus system with 5 generators
- Linearized generator swing equations and power flow equations.
- State variables:
  - Generators rotor angles (δ)
  - Generators frequencies (ω)
  - Voltage bus angles (θ).
- Control inputs:
  - Generators mechanical input P_g with inner PI frequency regulation
  - Bus active power demand P_d .



$$\begin{bmatrix} I & 0 & 0 \\ 0 & M & 0 \\ 0 & 0 & 0 \end{bmatrix} \dot{x} = -\begin{bmatrix} 0 & -I & 0 \\ L_{gg} & D_g & L_{lg} \\ L_{gl} & 0 & L_{ll} \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ I & 0 \\ 0 & I \end{bmatrix} u$$

$$\theta(t) = -L_{ll}^{-1}(L_{lg}\delta(t) - P_d).$$

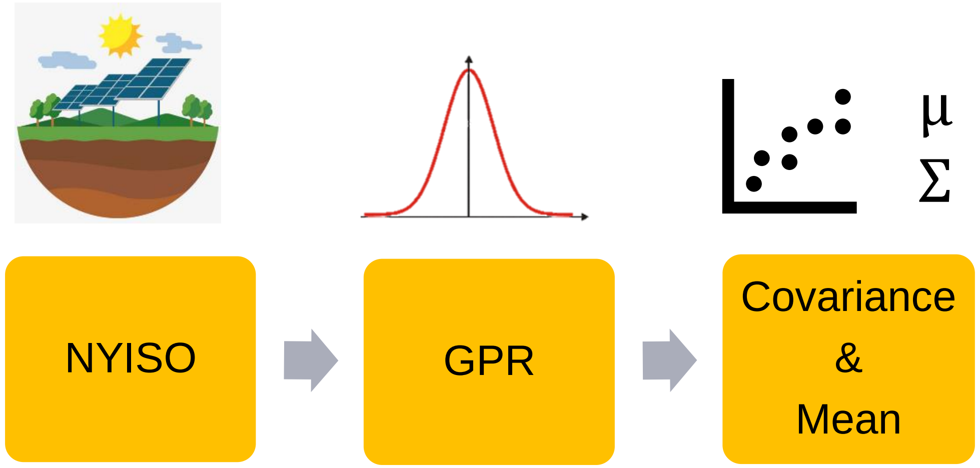
$$\begin{bmatrix} \dot{\delta}(t) \\ \dot{\omega}(t) \end{bmatrix} = \begin{bmatrix} 0 & I \\ -M^{-1}(L_{gg} - L_{gl}L_{ll}^{-1}L_{lg}) & -M^{-1}D_g \end{bmatrix} \tilde{x} + \begin{bmatrix} 0 & 0 \\ M^{-1} & -M^{-1}L_{gl}L_{ll}^{-1} \end{bmatrix} u,$$

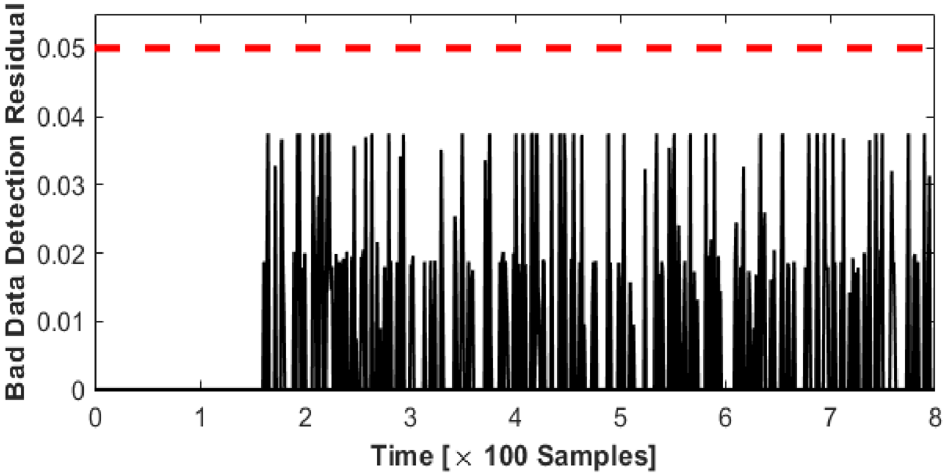
$$y(t) = \begin{bmatrix} 0 & I \\ -P_{\text{node}}L_{ll}^{-1}L_{lg} & 0 \end{bmatrix} \tilde{x} + \begin{bmatrix} 0 & 0 \\ -P_{\text{node}}L_{ll}^{-1} & 0 \end{bmatrix} u$$

Numerical Simulation

System Model

- Reduced System State Variables:
  - Generators rotor angles (δ)
  - Generators frequencies (ω)
- Measurement Channels y(t):
  - Generator frequency ω, it is also in PI feedback loop
  - The net power injected at each bus P_{net}
- Auxiliary Model:
  - Data collected from NYISO used to build GPR
  - Covariance matrix (Σ) is used to locate mean (μ) within three standard deviations from true values.
- Threat Model:
  - FDIA on at most 30% of the measurements
  - FDIA cannot be detected by BDD (5% threshold)

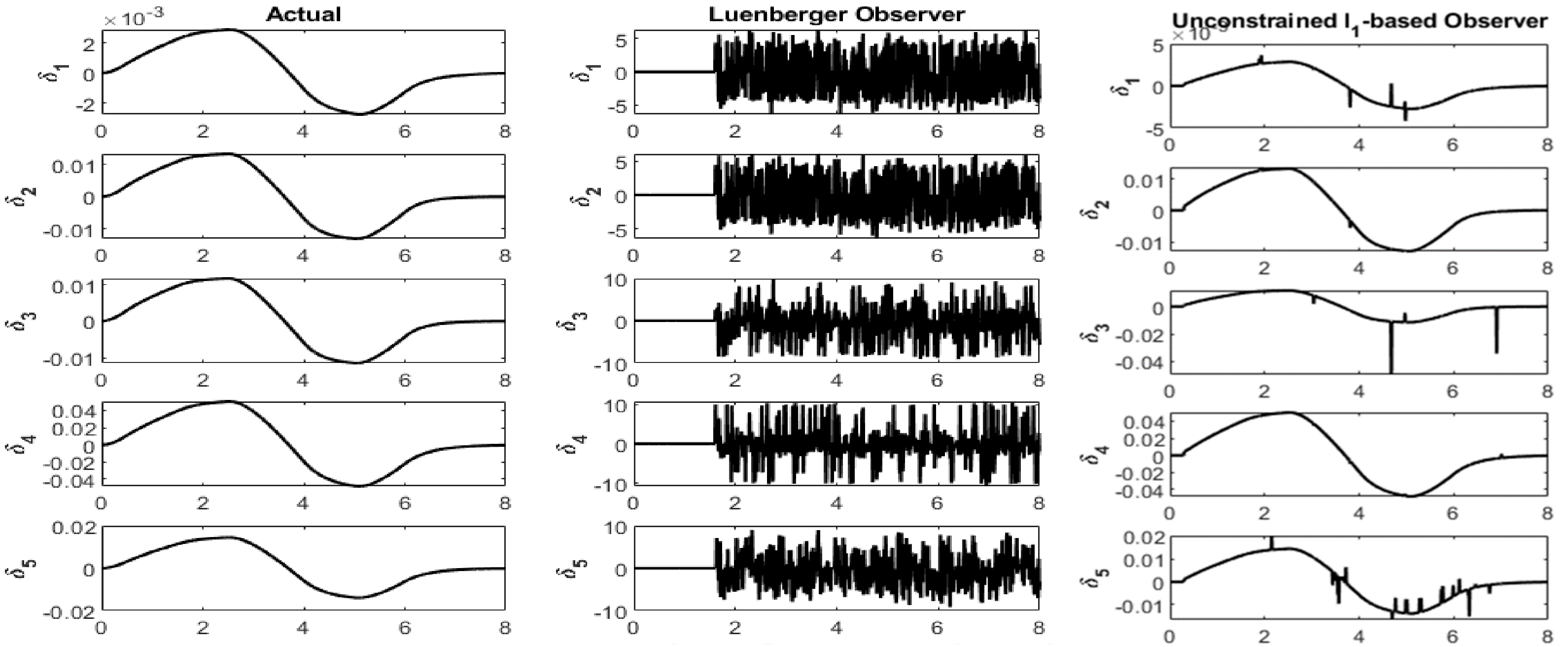




Numerical Simulation

Results

- The multi model observer is compared against:
  - Luenberger Observer:
    - Unable to reconstruct actual states under FDIA
  - l_1- Based Unconstrained Observer:
    - Most of the signals are reconstructed
    - Cascading controller might lead to instability
- The estimated generator rotor angle (δ) is used for comparison



Numerical Simulation

Results

- Outperforms both previous observers

- State Reconstruction:
  - More accurate compared to previous observers
  - Accuracy is due to constraint from auxiliary model

- Performance Analysis:
  - Root Mean Square value
  - Maximum absolute value of error

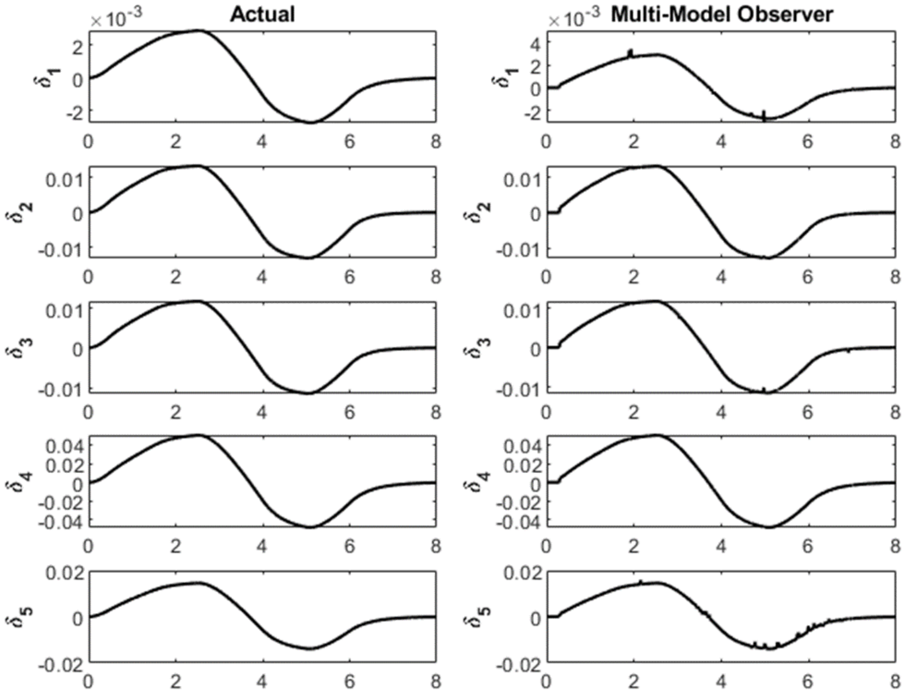


TABLE I

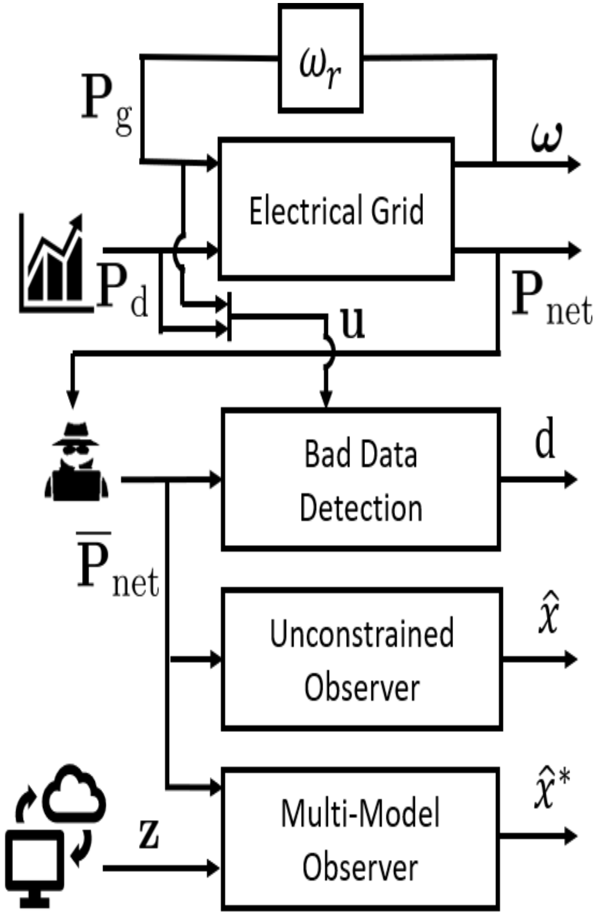
ERROR METRIC VALUES

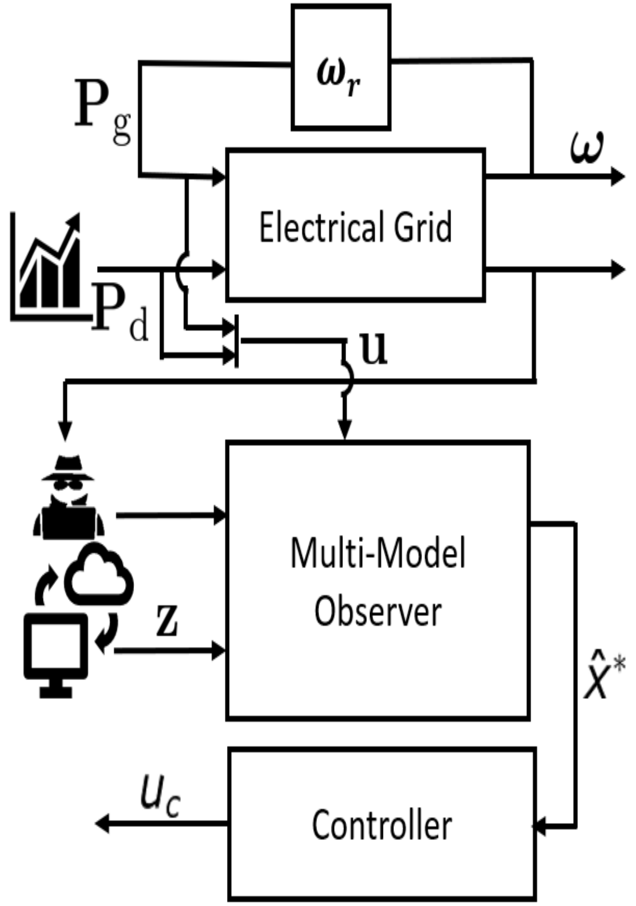
	RMS metric			Max. Abs. metric		
	LO	L1O	MMO	LO	L1O	MMO
δ_1	2.8801	0.0001	0.0001	6.4274	0.0028	0.0007
δ_2	2.7967	0.0002	0.0001	6.4437	0.0022	0.0013
δ_3	3.2746	0.0018	0.0001	9.7444	0.0387	0.0013
δ_4	3.4786	0.0004	0.0004	10.7019	0.0048	0.0042
δ_5	3.329	0.0011	0.0003	9.1387	0.0121	0.0024

LO: Luenberger Observer, **L1O**: Unconstrained ℓ_1-based Observer
MMO: Proposed Multi-Model Observer

Conclusion and Future Work

- **Conclusion:**
  - Novel data-driven constrained *l_1 minimization* based observer is developed.
  - Figure on the **left** represents implemented schematic.
- **Future Work:**
  - Cascading Controller:
    - Observer as filter
    - Feedback Loop with ***controller***
    - Figure on the **right** represents proposed schematic
  - Constraint:
    - Used Quadratic constraint
    - Develop sophisticated constraint
  - Uncertainties:
    - Study effect of FDIA under system uncertainties





THANK YOU

Olugbenga Moses Anubi – anubi@caps.fsu.edu

More information:

eng.famu.fsu.edu/~anubi/