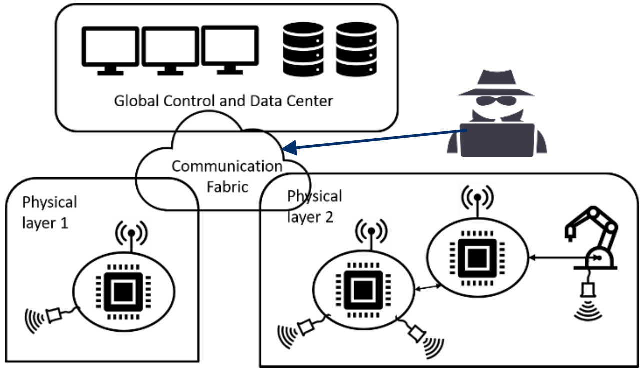
Attack-Resilient Weighted L1 Observer with Prior Pruning

Yu Zheng
Olugbenga M. Anubi

FLORIDA STATE UNIVERSITY
CENTER FOR ADVANCED POWER SYSTEMS

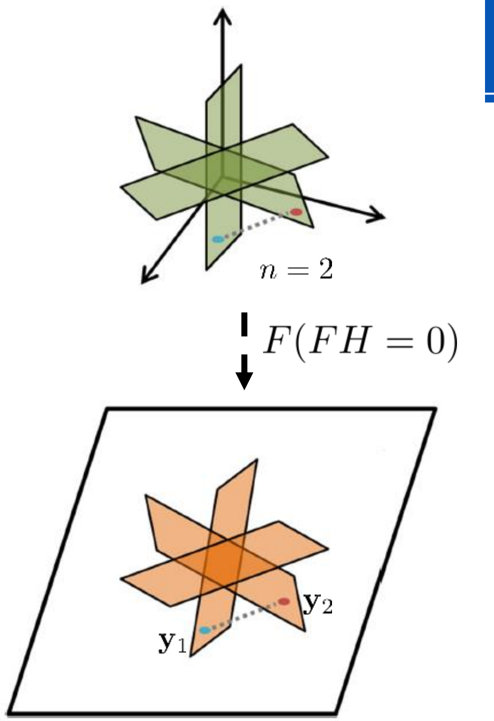
Motivation

- Secure Operation on Cyber Physical System



- False Data Injection Attacks
  - Erroneous measurements maliciously combined with systems measurement to disrupt performance/stability
  - Bypasses bad data detection mechanisms
  - Properties: time-varying, possibly unbounded, sparse
- Resilient Observers Limitations
  - Examples: event-triggered Luenberger observer, Gramian-based estimator, Robust estimator (local estimator + global fusion), L1 decoder …
  - If there is k attacks, the system should be at least 2k-detetable/observable

Preliminary



L0-L1 Minimization Program

$$\mathbf{y} = H\mathbf{x} + \mathbf{e}, \quad \mathbf{e} \in \mathcal{R}(H)$$

$$\begin{array}{rl} min & \|\mathbf{e}\|_0 \\ s.t. & \mathbf{y} = H\mathbf{x} + \mathbf{e} \end{array} \quad \Longleftrightarrow \quad min \ \ \|\mathbf{y} - H\mathbf{x}\|_0$$

↑ Restricted Isometry Property (RIP)

$$min \ \ \|\mathbf{y} - H\mathbf{x}\|_1$$

Pre-requirement: Less than half of measurements are attacked

Prior

- State prior [**16**]
- Measurement prior [**7,15**]
- Support prior [**5**]

Linear System Case

- Physical Model with decoder-detector

$$\begin{aligned} \mathbf{x}_{i+1} &= A\mathbf{x}_i & \mathbf{x}_i \in R^n,\, \mathbf{y}_i \in R^m (m > n) \\ \mathbf{y}_i &= C\mathbf{x}_i + \mathbf{e}_i & \mathbf{e}_i \in R^m \end{aligned}$$

➡

$$\mathbf{y}_T = H\mathbf{x}_{i-T+1} + \mathbf{e}_T$$

$$H = \begin{bmatrix} CA^{T-1} \\ CA^{T-2} \\ \vdots \\ CA \\ C \end{bmatrix} = [U_1 \;\; U_2] \begin{bmatrix} \sum_1 \\ 0 \end{bmatrix} V$$

- Decoder

$$\hat{\mathbf{x}} = \mathcal{D}(\mathbf{y}_T) = V\Sigma_1^{-1}\text{argmin}\|\mathbf{y}_T - U_1\mathbf{z}\|_1$$

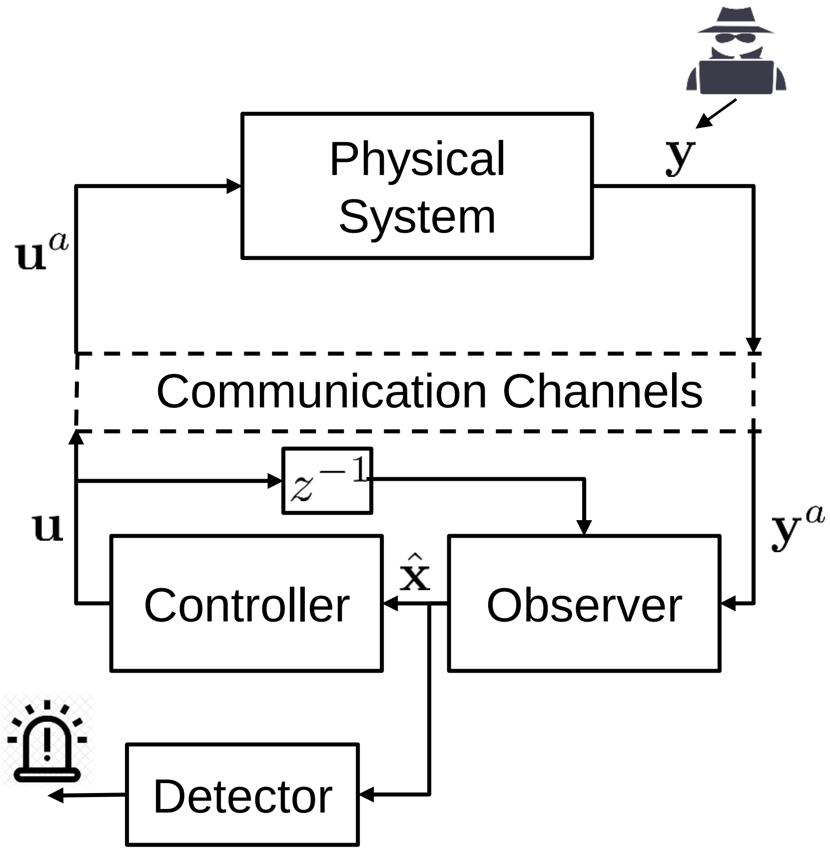
- Detector

$$\mathcal{D}_\epsilon(\mathbf{y}_T) = \begin{cases} 1 & \text{if } \|\mathbf{y}_T - H\mathcal{D}(\mathbf{y}_T)\|_1 > \epsilon \\ 0 & \text{otherwise} \end{cases}$$

False Data Injection Attacks

Threat Model

Successful FDIA: $\|\mathbf{x}^\star - \mathcal{D}(\mathbf{y}_T)\|_2 \geq \alpha, \;\; \mathcal{D}_\epsilon(\mathbf{y}_T) = 0$



Successful FDIA Design

Theorem 2.1: Given the support sequence $\mathcal{T} = \{\mathcal{T}_i \;\; \mathcal{T}_{i-1} \cdots \mathcal{T}_{i-T+1}\}$ with $|\mathcal{T}_i| \leq k$. Let $\mathbf{z}_e$ be an optimal solution of the optimization program

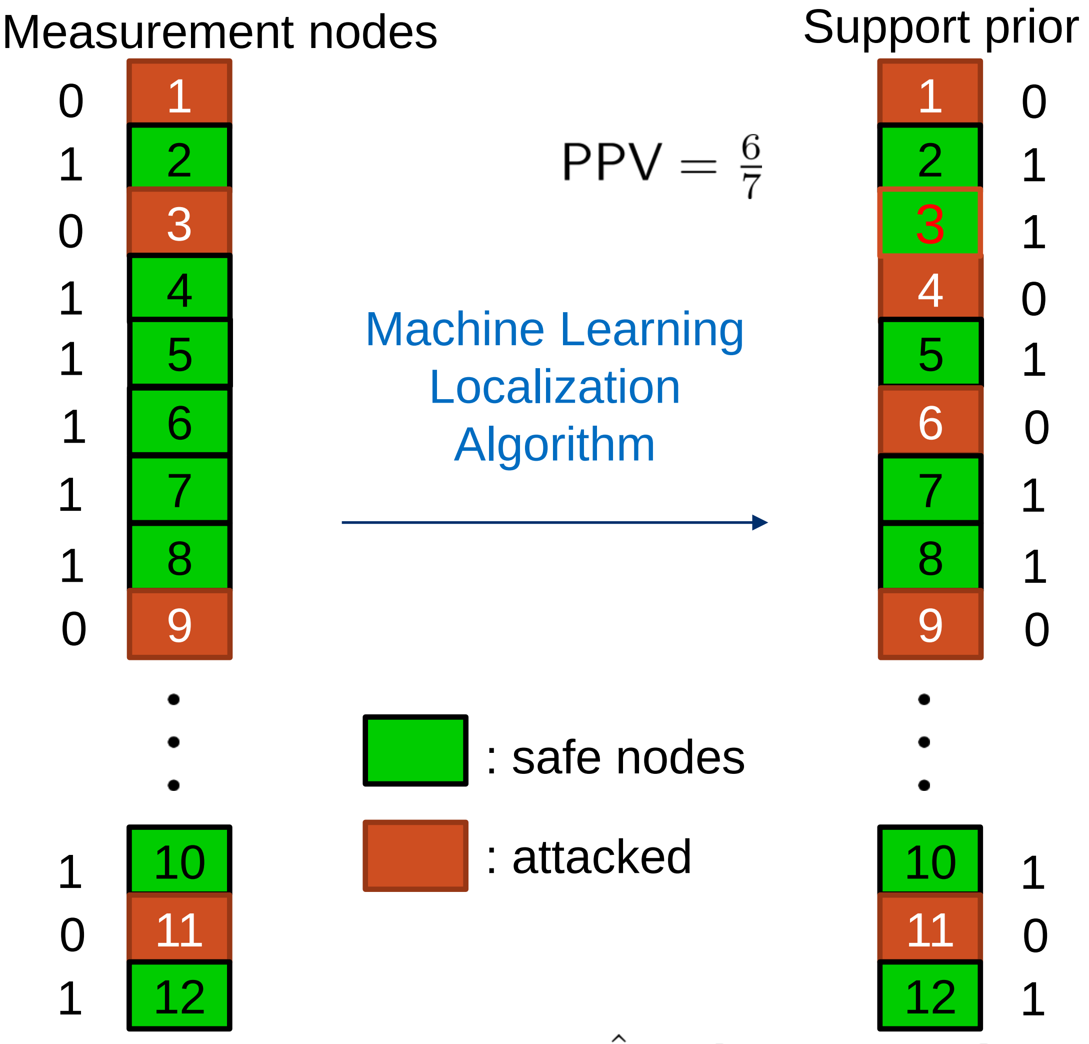
$$\begin{aligned} \text{Maxmize}: \quad & \|U_1 \mathbf{z}\|_2, \\ \text{Subject to}: \quad & \|U_{1,\mathcal{T}^c}\mathbf{z}\|_2 \leq \frac{\varepsilon}{\sqrt{Tm - |\mathcal{T}|}}. \end{aligned} \qquad (7)$$

If $\|U_{1,\mathcal{T}^c}\|_2 < \frac{1}{2\sqrt{Tm - |\mathcal{T}|}}$, then the FDIA

$$\mathbf{e}_{\mathcal{T}} = (U_{1,\mathcal{T}})\mathbf{z}_e, \;\; \mathbf{e}_{\mathcal{T}^c} = \mathbf{0} \qquad (8)$$

Measurement Prior

- Prior model



Measurement nodes

Support prior

0	🟥 1	🟥 1	0
1	🟩 2	🟩 2	1
0	🟥 3	🟩 3	1
1	🟩 4	🟥 4	0
1	🟩 5	🟩 5	1
1	🟩 6	🟥 6	0
1	🟩 7	🟩 7	1
1	🟩 8	🟩 8	1
0	🟥 9	🟥 9	0
⋮	⋮	⋮	⋮
1	🟩 10	🟩 10	1
0	🟥 11	🟥 11	0
1	🟩 12	🟩 12	1

$\text{PPV} = \frac{6}{7}$

Machine Learning Localization Algorithm

🟩 : safe nodes

🟥 : attacked

$\mathbf{q}$ $\mathcal{T} = [1, 3, 9, 11]$

$\mathcal{T}^c = [2, 4, \cdots, 8, 10, 12]$

$\hat{\mathcal{T}} = [1, 4, 6, 9, 11]$ $\hat{\mathbf{q}}$

$\hat{\mathcal{T}}^c = [2, 3, 5, 7, 8, 10, 12]$

Def (Indicator):

$$\mathbf{q}_i = \begin{cases} 1 & \text{if } i \in \mathcal{T}^c \\ 0 & \text{otherwise} \end{cases}$$

Def (Precision of estimation):

$$\text{PPV} = \frac{\|\mathbf{q} \circ \hat{\mathbf{q}}\|_{\ell_0}}{\|\hat{\mathbf{q}}\|_{\ell_0}}$$

Uncertainty model:

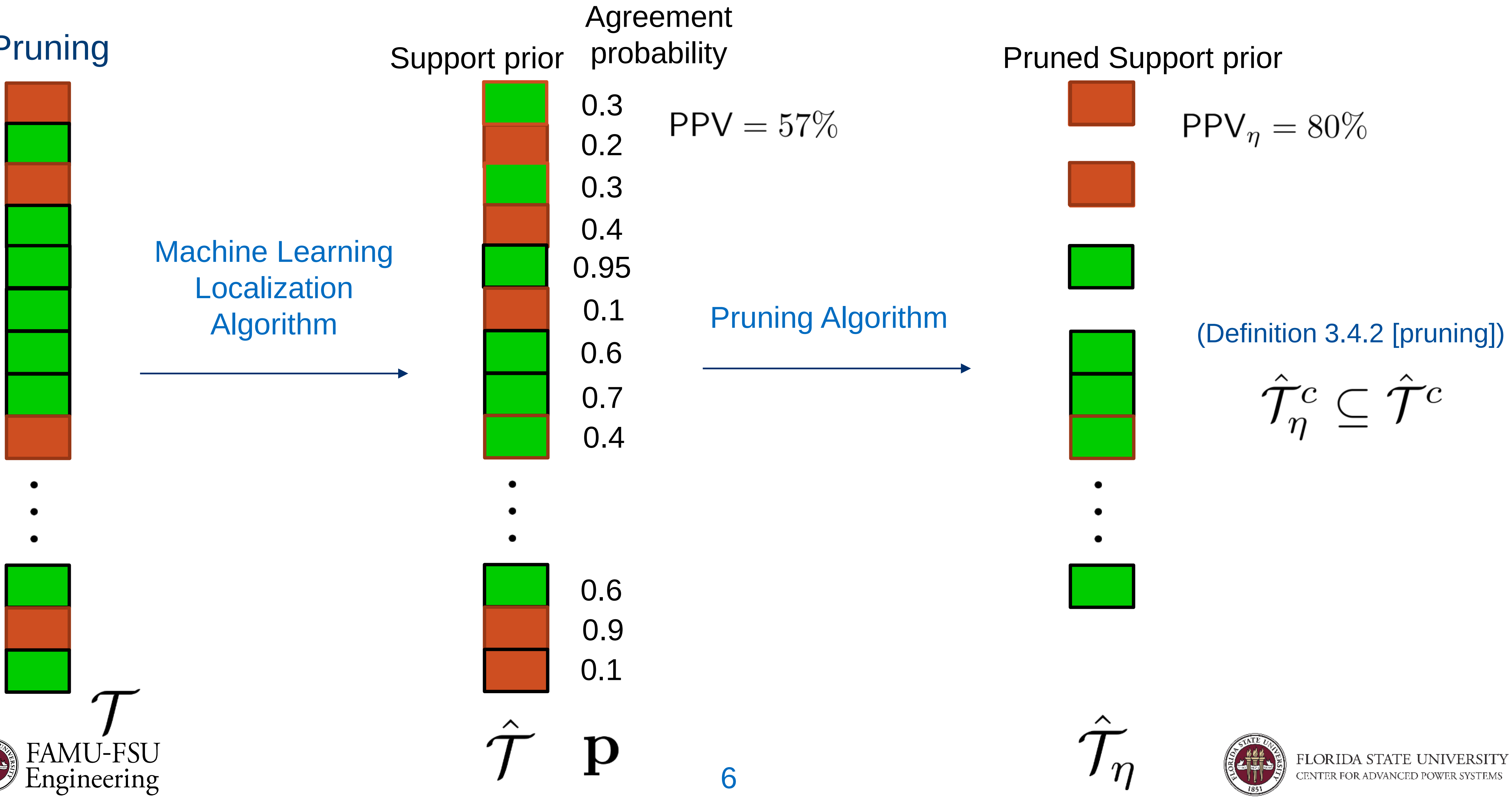
$$\mathbf{q}_i = \epsilon_i \hat{\mathbf{q}}_i + (1 - \epsilon_i)(1 - \hat{\mathbf{q}}_i)$$

$\epsilon_i \sim \mathcal{B}(1, \mathbf{p}_i)$, with known $\mathbf{p}_i \in R_+$
given by $\mathbf{p}_i = E[\epsilon_i] = \Pr\{\epsilon_i = 1\}$

1. Uncertainty
2. Training price

Weighted L1 Observer with Prior Pruning

- Pruning



$\mathcal{T}$

Machine Learning Localization Algorithm

Support prior

$\hat{\mathcal{T}}$

Agreement probability

$\mathbf{p}$

0.3
0.2
0.3
0.4
0.95
0.1
0.6
0.7
0.4
0.6
0.9
0.1

$\text{PPV} = 57\%$

Pruning Algorithm

Pruned Support prior

$\hat{\mathcal{T}}_\eta$

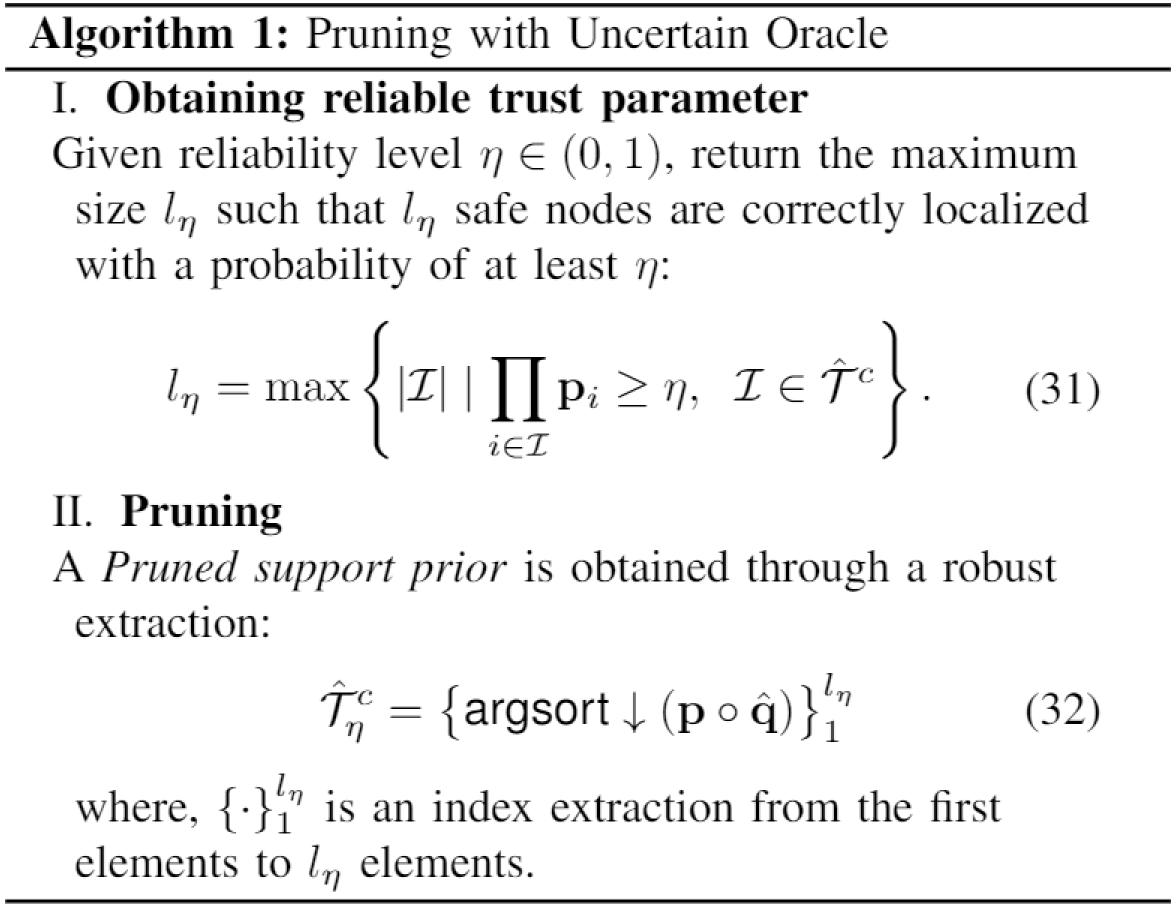
$\text{PPV}_\eta = 80\%$

(Definition 3.4.2 [pruning])

$$\hat{\mathcal{T}}_\eta^c \subseteq \hat{\mathcal{T}}^c$$

Weighted L1 Observer with Prior Pruning

- Pruning



Algorithm 1: Pruning with Uncertain Oracle

I. **Obtaining reliable trust parameter**

Given reliability level $\eta \in (0,1)$, return the maximum size l_η such that l_η safe nodes are correctly localized with a probability of at least η:

$$l_\eta = \max\left\{ |\mathcal{I}| \mid \prod_{i \in \mathcal{I}} \mathbf{p}_i \geq \eta,\ \ \mathcal{I} \in \hat{\mathcal{T}}^c \right\}. \qquad (31)$$

II. **Pruning**

A *Pruned support prior* is obtained through a robust extraction:

$$\hat{\mathcal{T}}_\eta^c = \{\mathsf{argsort}\downarrow(\mathbf{p} \circ \hat{\mathbf{q}})\}_1^{l_\eta} \qquad (32)$$

where, $\{\cdot\}_1^{l_\eta}$ is an index extraction from the first elements to l_η elements.

$$\Rightarrow \quad \Pr\left\{\mathsf{PPV}_\eta = 1\right\} \geq \eta.$$

Lemma 3.1

Weighted L1 Observer with Prior Pruning

- Weighted L1 Observer

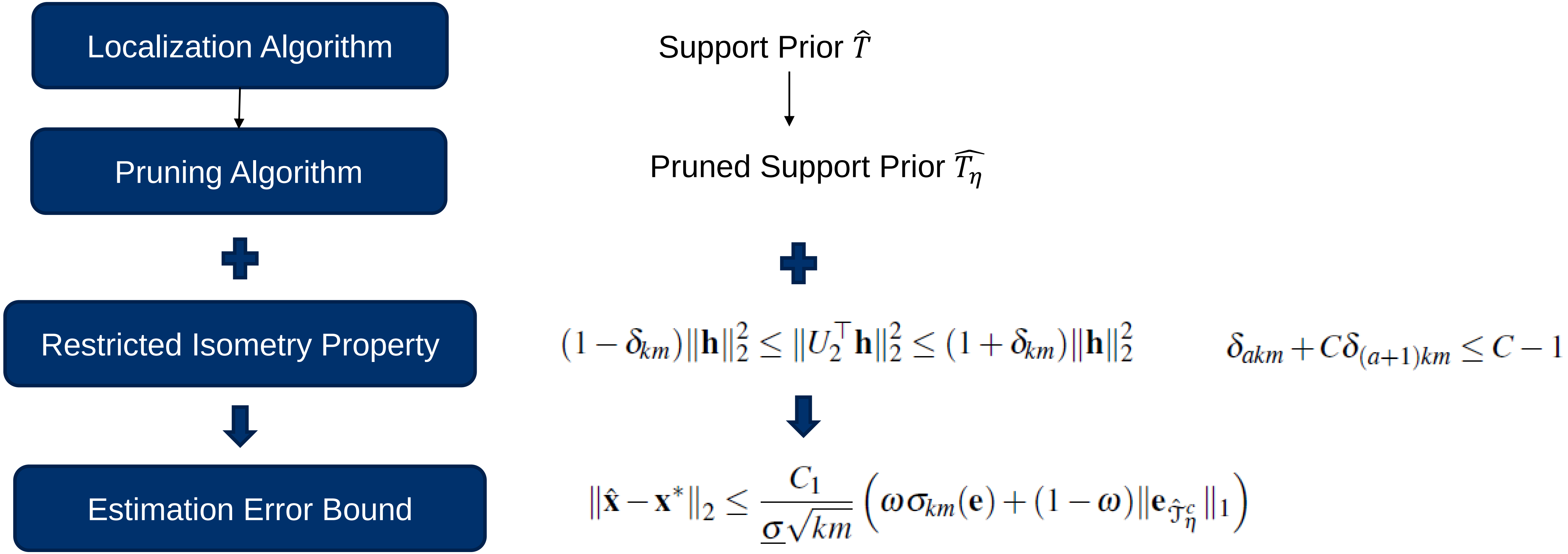
$$\begin{aligned} \text{Minimize} \quad & \sum_{p=i-T+1}^{i} \|\mathbf{y}_p - C\mathbf{z}_p\|_{1,w} \\ \text{Subject to} \quad & \mathbf{z}_{p+1} - A\mathbf{z}_p = 0, \\ & \qquad p = i-T+1, \cdots, i-1 \\ & w = \begin{cases} 1, & j \in \hat{\mathcal{T}}_\eta^c \\ \omega, & j \in \hat{\mathcal{T}}_\eta \end{cases} \end{aligned}$$

$\|\mathbf{z}\|_{1,w} = \sum_i w_i |\mathbf{z}_i|$ is the weighted 1-norm

$$\text{Minimize } \|\mathbf{y}_T - H\mathbf{z}\|_{1,\mathrm{w}}, \text{ with } w = \begin{cases} 1, & j \in \hat{\mathcal{T}}_\eta^c \\ \omega, & j \in \hat{\mathcal{T}}_\eta \end{cases}$$

Weighted L1 Observer with Prior Pruning

- Main Theorem (Theorem 3.2)



Localization Algorithm

Pruning Algorithm

Restricted Isometry Property

Estimation Error Bound

Support Prior $\hat{T}$

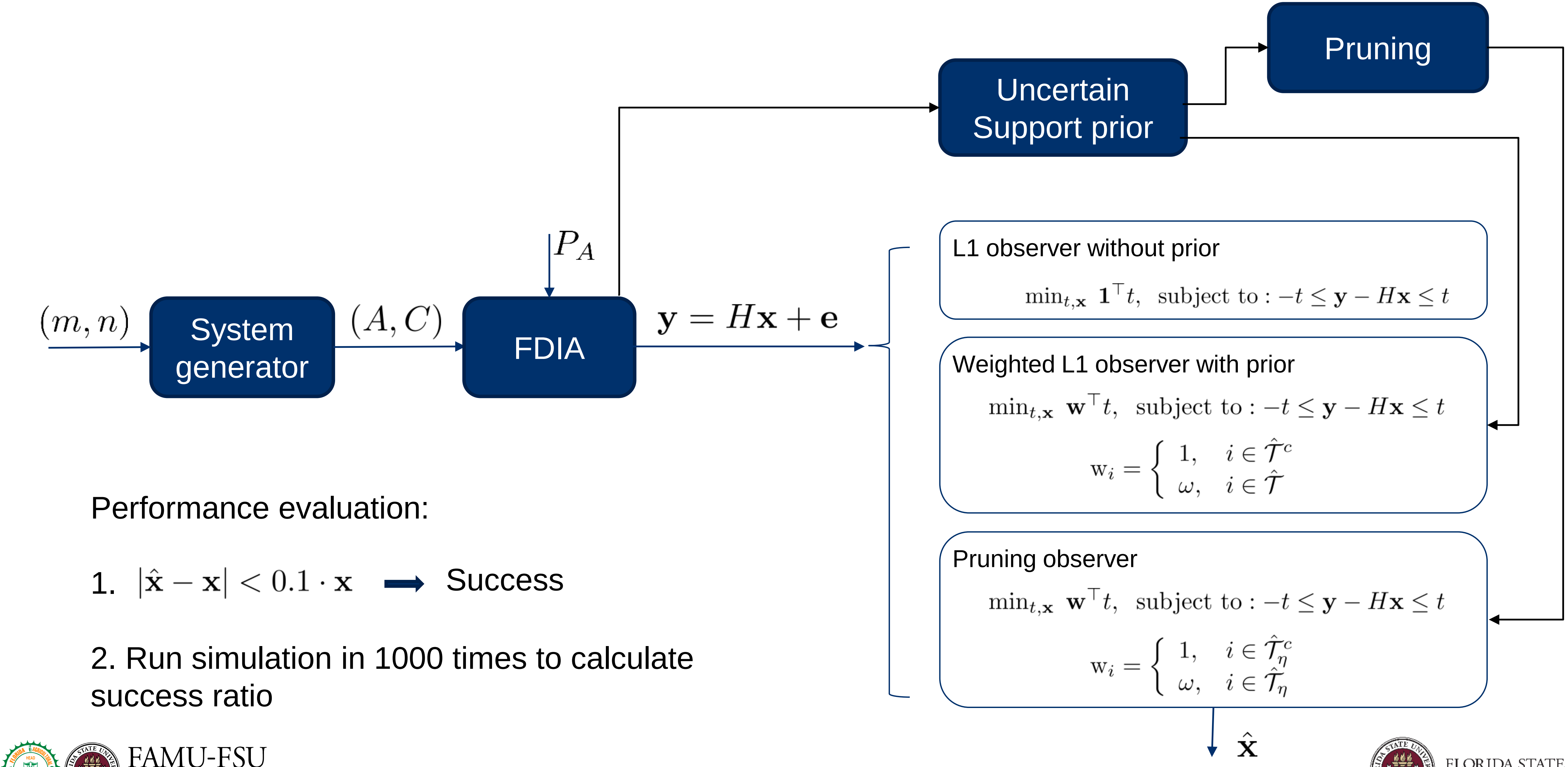
Pruned Support Prior $\widehat{T_\eta}$

$$(1-\delta_{km})\|\mathbf{h}\|_2^2 \leq \|U_2^\top \mathbf{h}\|_2^2 \leq (1+\delta_{km})\|\mathbf{h}\|_2^2$$

$$\delta_{akm} + C\delta_{(a+1)km} \leq C - 1$$

$$\|\hat{\mathbf{x}} - \mathbf{x}^*\|_2 \leq \frac{C_1}{\underline{\sigma}\sqrt{km}} \left(\omega\sigma_{km}(\mathbf{e}) + (1-\omega)\|\mathbf{e}_{\hat{\mathfrak{T}}_\eta^c}\|_1 \right)$$

Numerical Simulation



(m, n)

System generator

(A, C)

P_A

FDIA

$\mathbf{y} = H\mathbf{x} + \mathbf{e}$

Uncertain Support prior

Pruning

L1 observer without prior

$$\min_{t,\mathbf{x}} \ \mathbf{1}^\top t, \ \ \text{subject to} : -t \leq \mathbf{y} - H\mathbf{x} \leq t$$

Weighted L1 observer with prior

$$\min_{t,\mathbf{x}} \ \mathbf{w}^\top t, \ \ \text{subject to} : -t \leq \mathbf{y} - H\mathbf{x} \leq t$$

$$\mathrm{w}_i = \begin{cases} 1, & i \in \hat{\mathcal{T}}^c \\ \omega, & i \in \hat{\mathcal{T}} \end{cases}$$

Pruning observer

$$\min_{t,\mathbf{x}} \ \mathbf{w}^\top t, \ \ \text{subject to} : -t \leq \mathbf{y} - H\mathbf{x} \leq t$$

$$\mathrm{w}_i = \begin{cases} 1, & i \in \hat{\mathcal{T}}_\eta^c \\ \omega, & i \in \hat{\mathcal{T}}_\eta \end{cases}$$

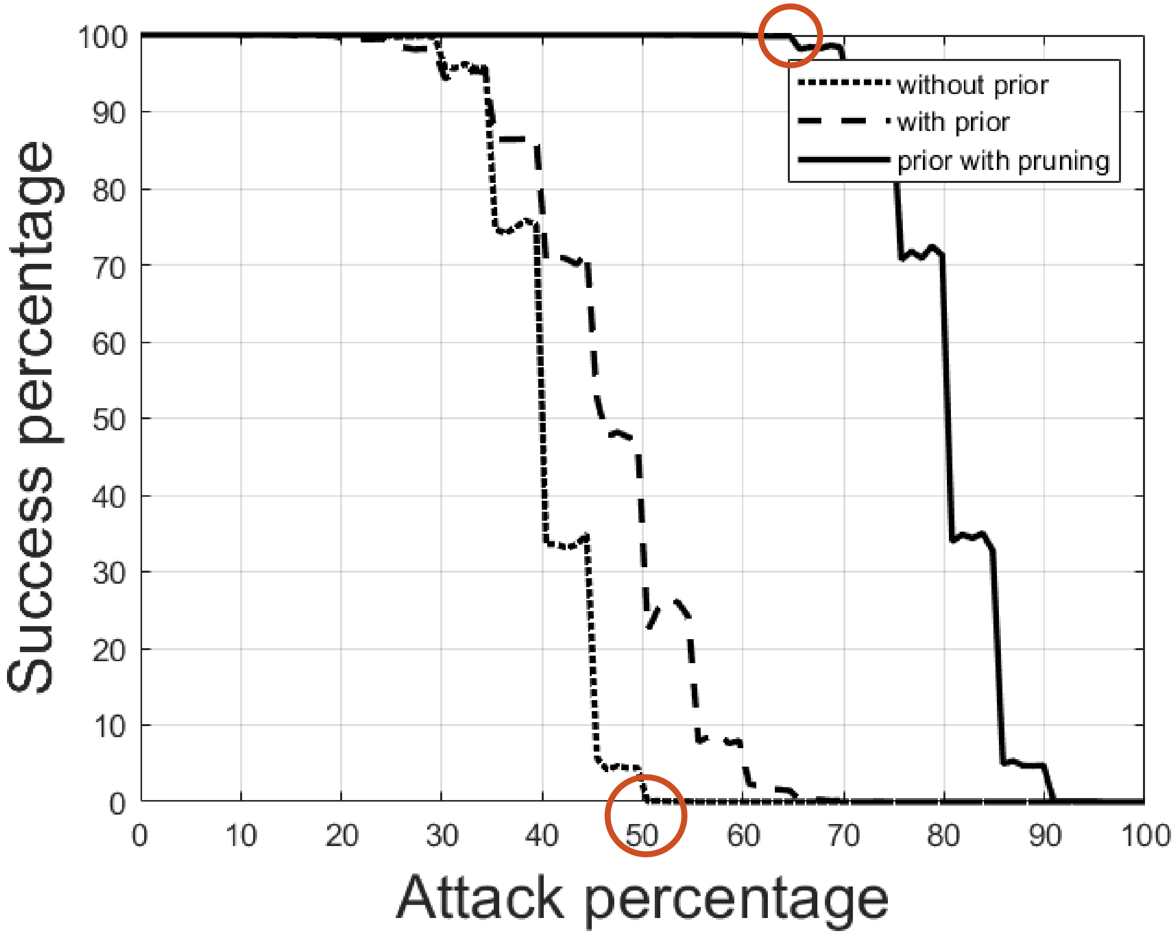
$\hat{\mathbf{x}}$

Performance evaluation:

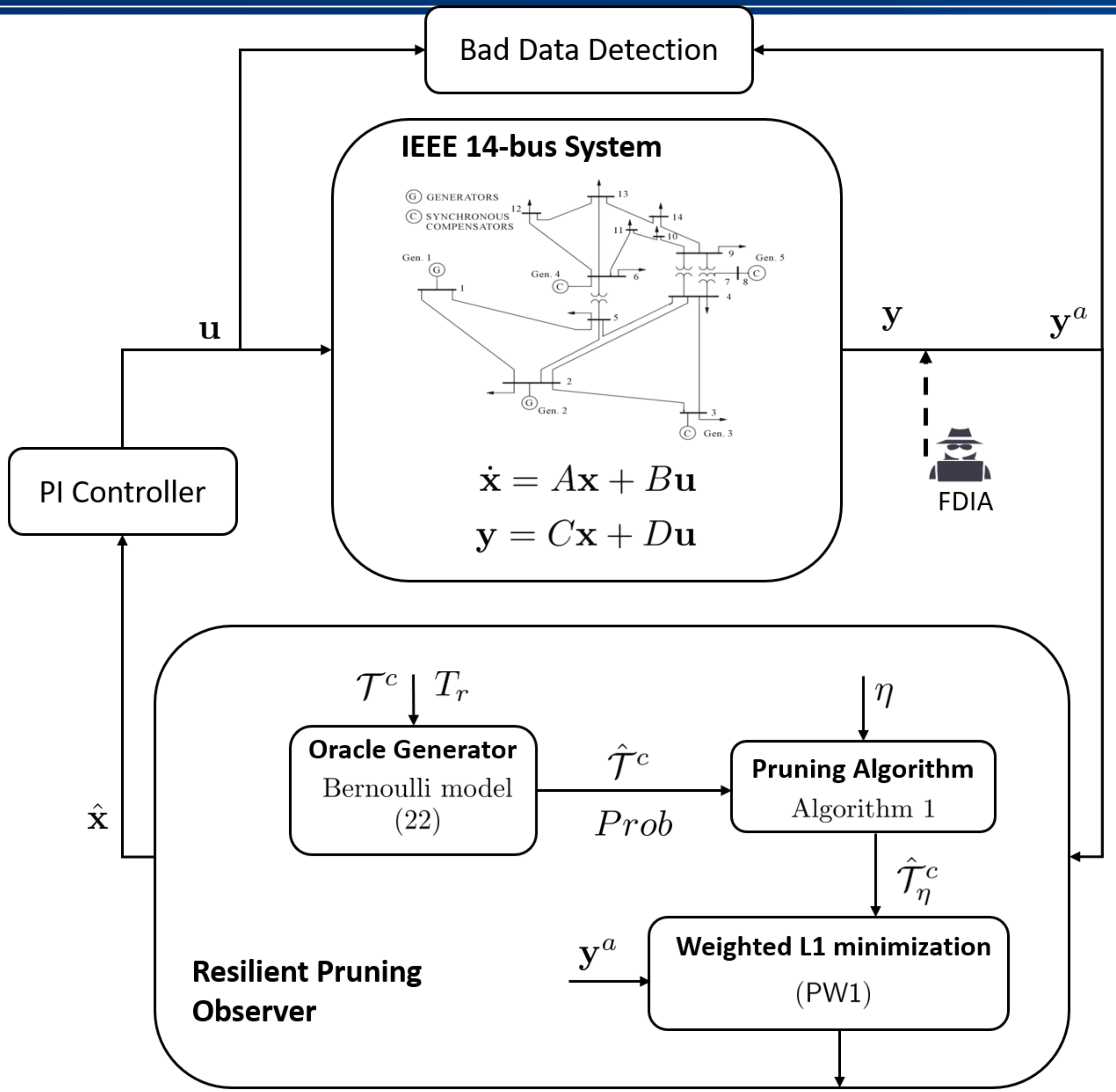
1. $|\hat{\mathbf{x}} - \mathbf{x}| < 0.1 \cdot \mathbf{x}$ ➡ Success

2. Run simulation in 1000 times to calculate success ratio

Numerical Simulation



Application Example



Bad Data Detection

IEEE 14-bus System

$$\dot{\mathbf{x}} = A\mathbf{x} + B\mathbf{u}$$

$$\mathbf{y} = C\mathbf{x} + D\mathbf{u}$$

$\mathbf{u}$

$\mathbf{y}$

$\mathbf{y}^a$

FDIA

PI Controller

$\hat{\mathbf{x}}$

$\mathcal{T}^c$ T_r

Oracle Generator

Bernoulli model (22)

$\hat{\mathcal{T}}^c$

$Prob$

η

Pruning Algorithm

Algorithm 1

$\hat{\mathcal{T}}^c_\eta$

$\mathbf{y}^a$

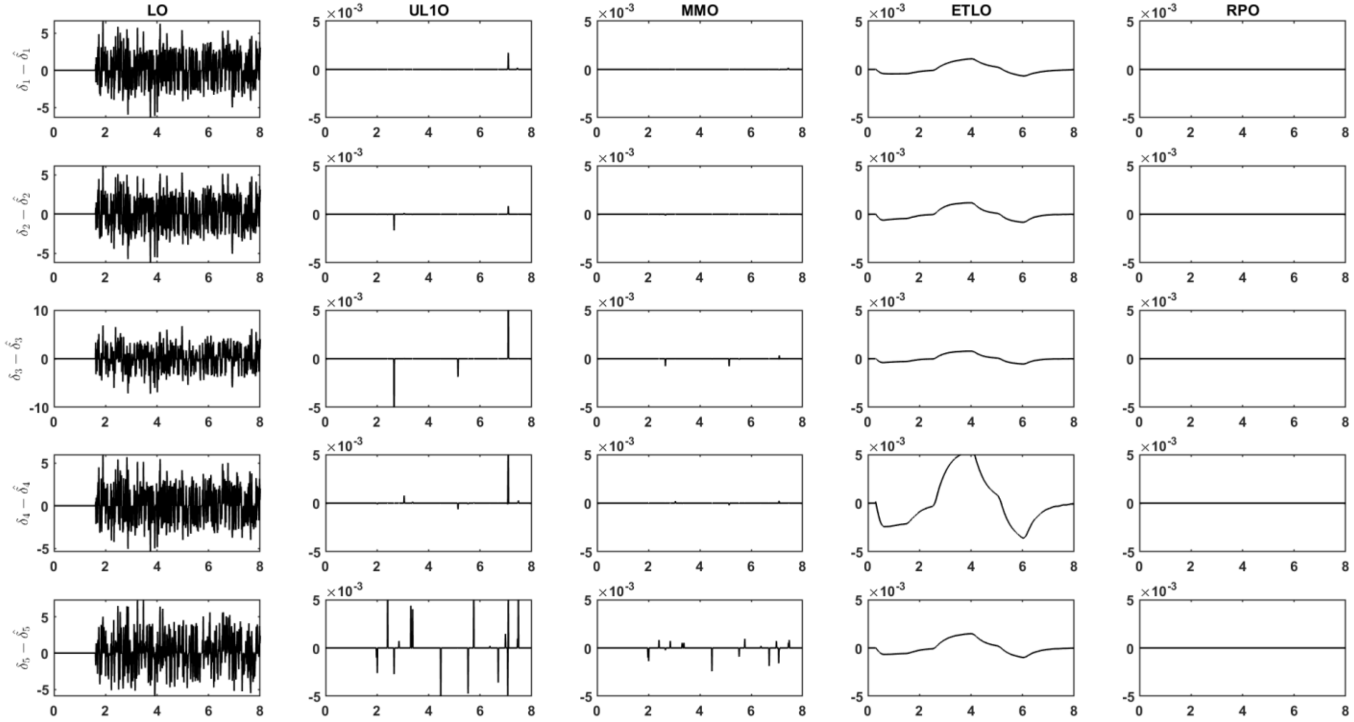
Weighted L1 minimization

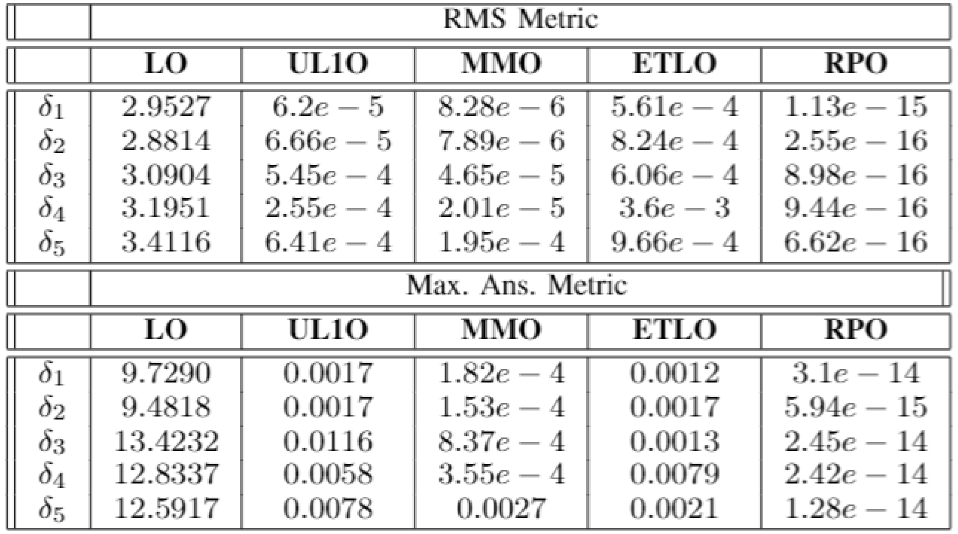
(PW1)

Resilient Pruning Observer

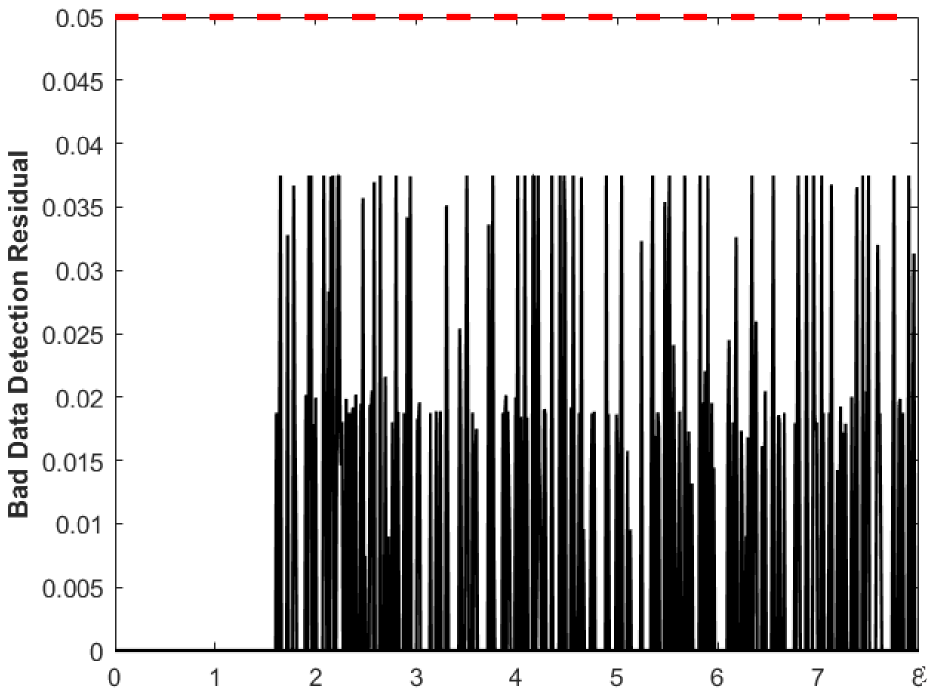
Application Example

Estimation error on bus angles





	RMS Metric				
	LO	UL1O	MMO	ETLO	RPO
δ_1	2.9527	$6.2e-5$	$8.28e-6$	$5.61e-4$	$1.13e-15$
δ_2	2.8814	$6.66e-5$	$7.89e-6$	$8.24e-4$	$2.55e-16$
δ_3	3.0904	$5.45e-4$	$4.65e-5$	$6.06e-4$	$8.98e-16$
δ_4	3.1951	$2.55e-4$	$2.01e-5$	$3.6e-3$	$9.44e-16$
δ_5	3.4116	$6.41e-4$	$1.95e-4$	$9.66e-4$	$6.62e-16$
	Max. Ans. Metric				
	LO	UL1O	MMO	ETLO	RPO
δ_1	9.7290	0.0017	$1.82e-4$	0.0012	$3.1e-14$
δ_2	9.4818	0.0017	$1.53e-4$	0.0017	$5.94e-15$
δ_3	13.4232	0.0116	$8.37e-4$	0.0013	$2.45e-14$
δ_4	12.8337	0.0058	$3.55e-4$	0.0079	$2.42e-14$
δ_5	12.5917	0.0078	0.0027	0.0021	$1.28e-14$



LO: Luenburger Observer
UL1O: Unconstrained L1 Observer
MMO: Multi-model Observer
ETLO: Event triggered Luenbueger Observer
RRO: proposed Pruning Observer

Conclusion

Resilient weighted L1 observer with prior pruning against False data Injection attacks

Pruning: a way to improve the precision of results of localization algorithm without training
Observer: can cope with big percentage of attacks
Weighted L1: provide a chance to reduce the sacrifice of measurements redundancy

THANK YOU

Olugbenga Moses Anubi – anubi@caps.fsu.edu

Open source codes: https://github.com/ZYblend/Resilient-Pruning-Observer-Design-for-CPSs-under-FDIA