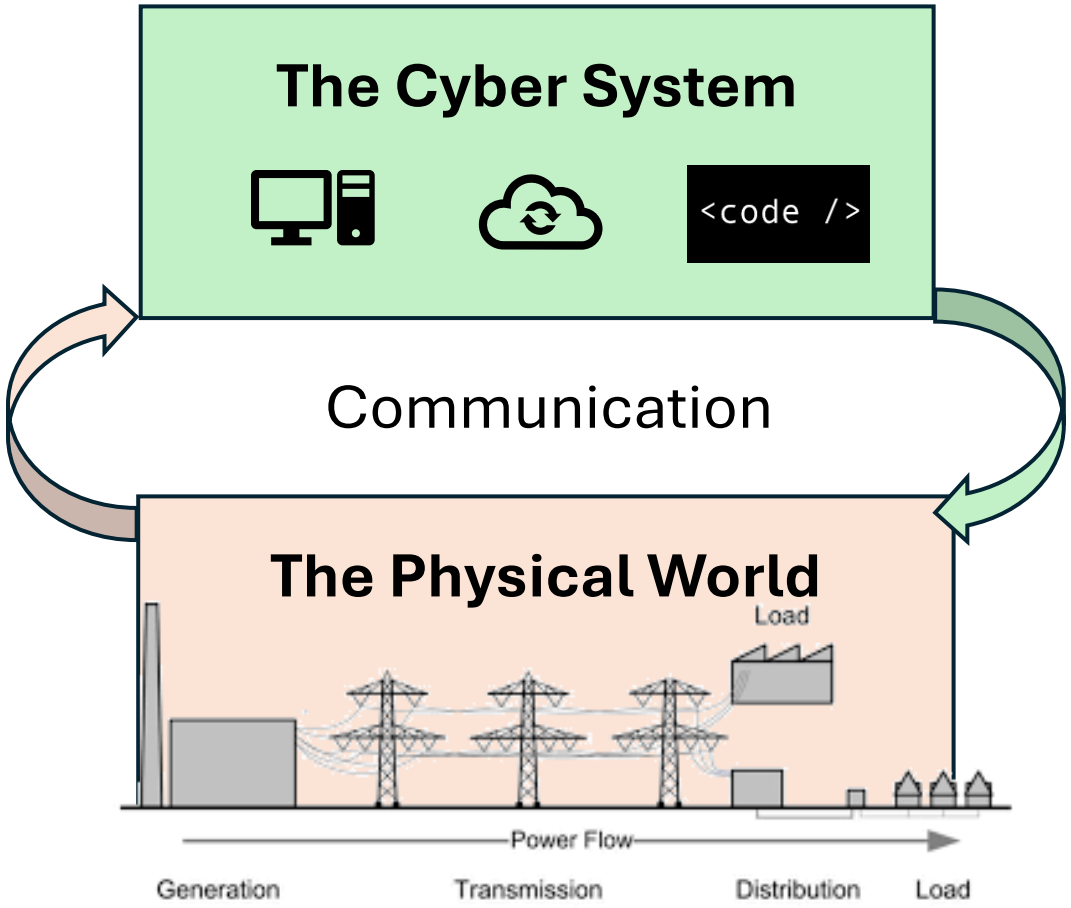
Carnegie Mellon University
Electrical & Computer Engineering

Exploiting sparse structures and synergy designs to advance power system situational awareness

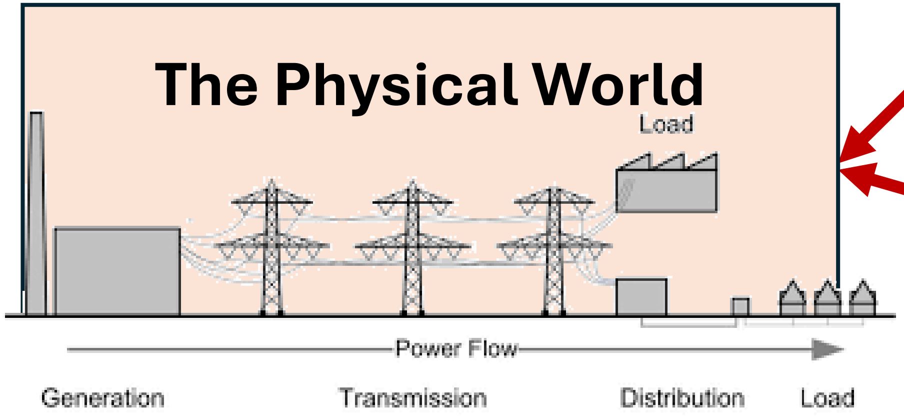
Shimiao (Cindy) Li
Carnegie Mellon University
Defense date: 11/15/2024

Today’s power grids: smart cyber-physical system



Natural threats to reliability and resiliency

More blackouts from extreme weathers and more fluctuations from renewables, microgrids, energy trading



Rising renewables penetration is a threat to grid reliability in some regions, NERC concludes

Published Dec. 18, 2020

*NERC: North American Electric Reliability Corporation

Adversarial threats to reliability and resiliency

The Cyber System



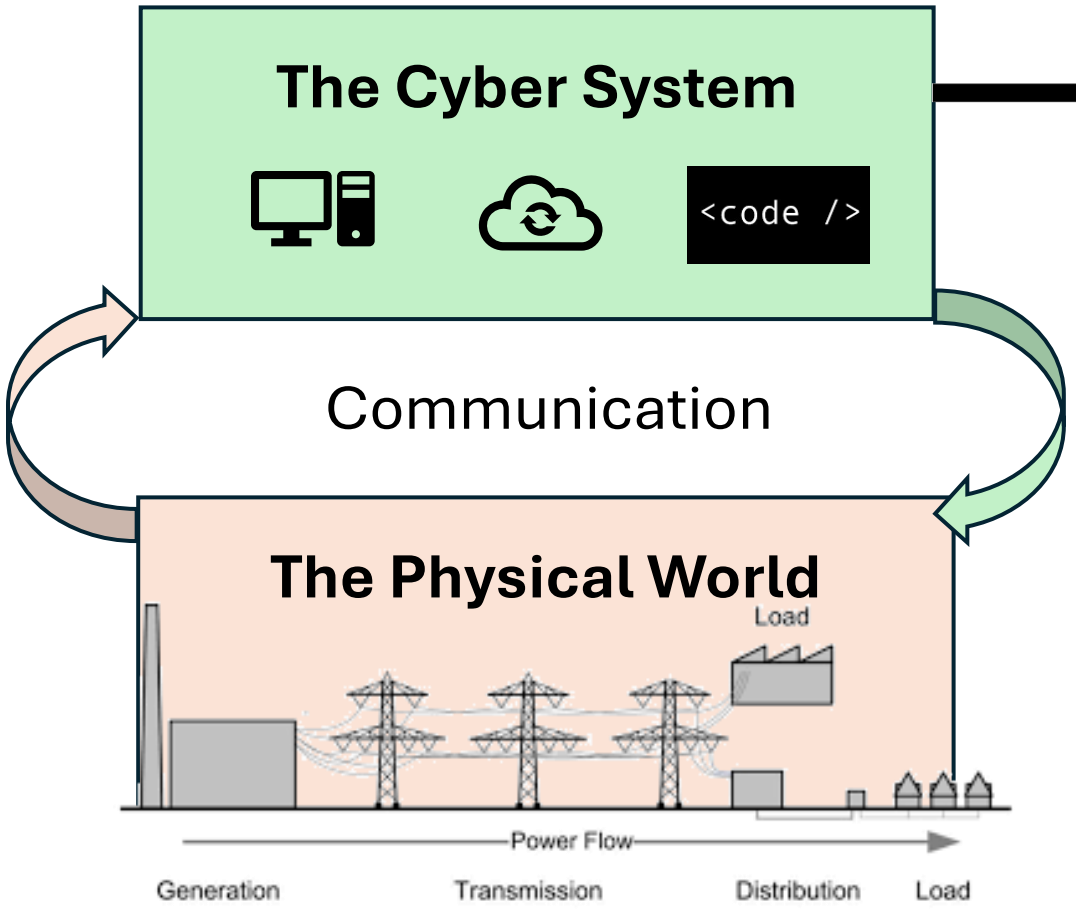
Cyberthreats: either brute-force blackouts or well-designed manipulations of system and data

False data injection attack in smart grid cyber physical system

MadIoT: How an IoT botnet could launch a major attack on the power grid


Graham CLULEY
August 21, 2018

Situational awareness key to addressing threats



Need Situational Awareness on the decision layer

*"The ability to perceive the system's **present** state and project its **future** behavior"*

Simulation and estimation tools key to situational awareness
This thesis focuses on steady-state horizon.

Estimation:

tells the real-time conditions from measurements

What are the bus voltages now?

What is the topology now?

Is there any anomalous data?

What anomalies are happening?

Simulation:

answers what-if questions

What if demand increases by 20%?

What if supply decreases by 20%?

What if there's a line outage?

Current gaps: robustness and efficiency

- **Not robust**: results become inaccurate, non-actionable, or meaningless under certain threats

Simulation not robust to blackout failures

Supply needs to meet demand at every node, giving system equations

$$\boldsymbol{F} = \begin{cases} \text{Node 1: } \boldsymbol{F_1(x, G, D) = 0} \\ \vdots \\ \text{Node N: } \boldsymbol{F_N(x, G, D) = 0} \end{cases}$$

$\boldsymbol{G}$: generation
$\boldsymbol{D}$: demand
$\boldsymbol{x}$: voltage magnitude |V| & phase angles

Simulation reaches a feasible solution to system equations

Normal condition

Solution doesn't exist upon blackout!
Simulator diverges!

2003 Blackout in the Northeast

Estimation not robust to anomalous data

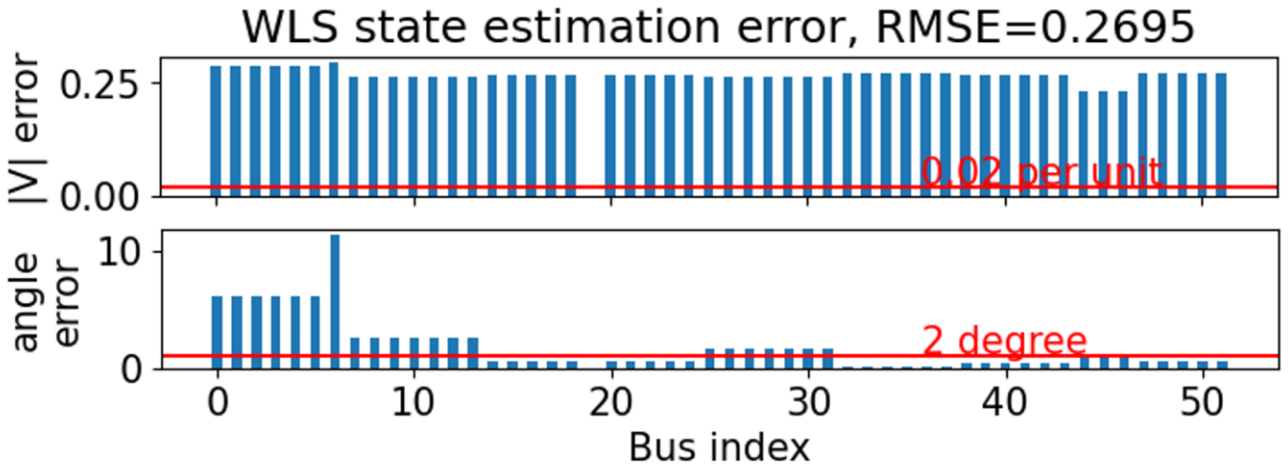
Steady-state estimation solves state $\boldsymbol{x}$ from measurements $\boldsymbol{z}$ using weighted least squares (WLS)

$$\min_{x} w_i\left(z_i - f_i(\boldsymbol{x})\right)^2$$

$\boldsymbol{x}$: voltage magnitude |V| & phase angles

f_i: measurement – state relationship

A 52-bus system with 1 bad data and 2 topology errors. Large estimation errors occur.



Current gaps: robustness and efficiency

- **Not robust**: results become inaccurate, non-actionable, or meaningless under certain threats
- **Not efficient**: large systems are slow or non-converging

Simulation problem

$$\boldsymbol{F} = \begin{cases} \text{Node 1: } \boldsymbol{F_1}(\boldsymbol{x}, \boldsymbol{G}, \boldsymbol{D}) = \boldsymbol{0} \\ \vdots \\ \text{Node N: } \boldsymbol{F_N}(\boldsymbol{x}, \boldsymbol{G}, \boldsymbol{D}) = \boldsymbol{0} \end{cases}$$

$\boldsymbol{F_i}$ **nonlinear** on branches

Estimation problem

$$\min_x w_i\left(z_i - f_i(\boldsymbol{x})\right)^2$$

f_i **nonlinear** for measurements of power

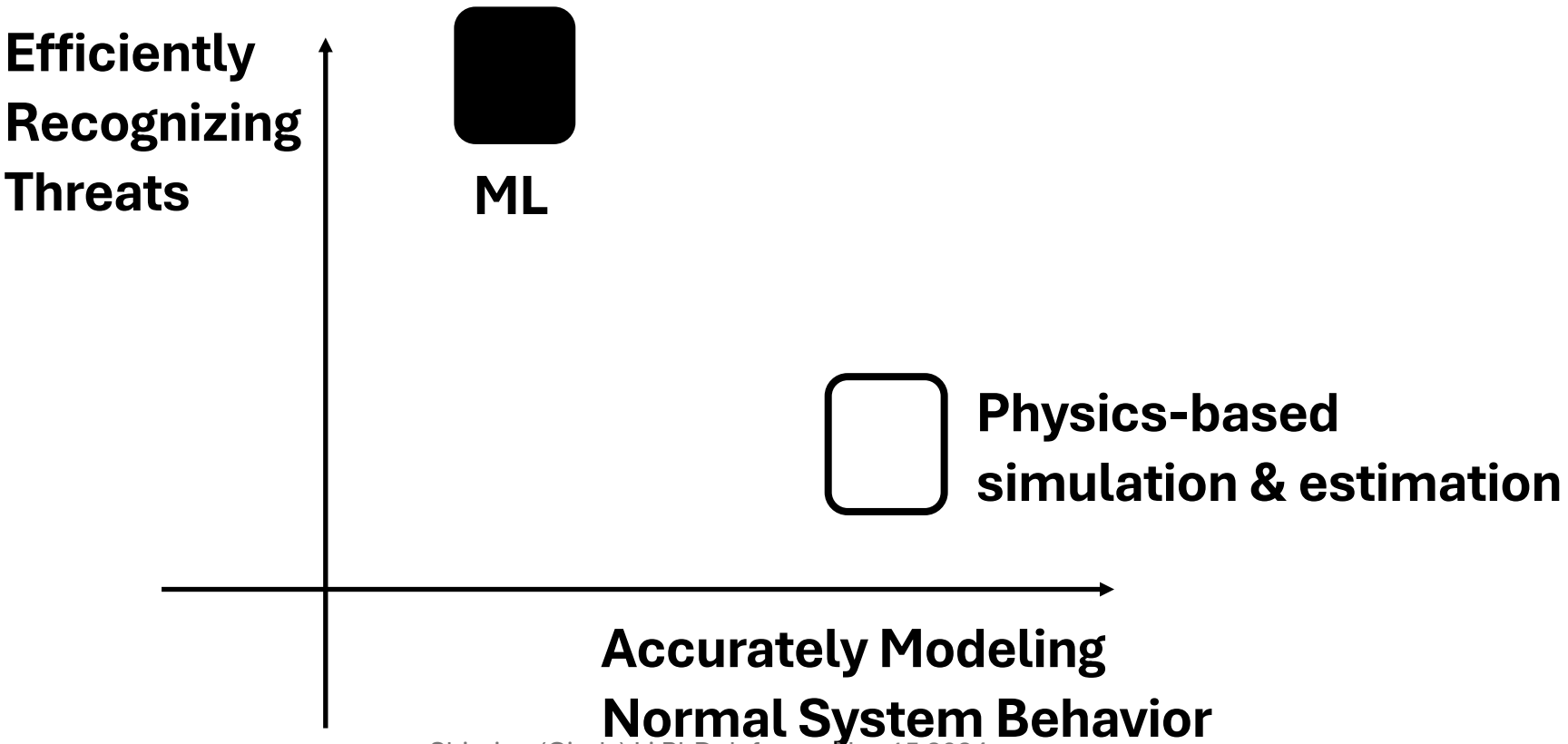
Data-driven approaches using machine learning (ML)

- Anomaly detection / identification methods
- Data-driven alternatives to simulators and estimators
  - Aim at faster speed & comparable accuracy

Gaps on heavily-constrained power systems: not generalizable, not scalable, not interpretable

Physics-based VS Data-driven: an either-or question?

- The two worlds have pros and cons (at state-of-the-art).



My research: fill the gaps with a synergy of both

- Address inherent limitations in physics-based and ML worlds
- Develop Physics-ML Synergy to merge their complementary benefits

Physics-based
Robustness gap
Efficiency gap

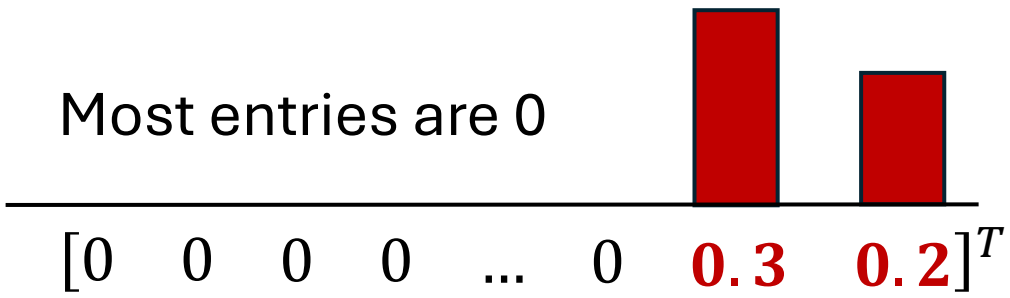
Data-driven (ML)
Generalization
Scalability
Interpretability

Interconnection

Key enabler: sparsity-exploiting optimizations

- A small fraction of non-zero values – carrying essential information
- Most entries are zero – ignorable without losing significant accuracy.

Sparse vector



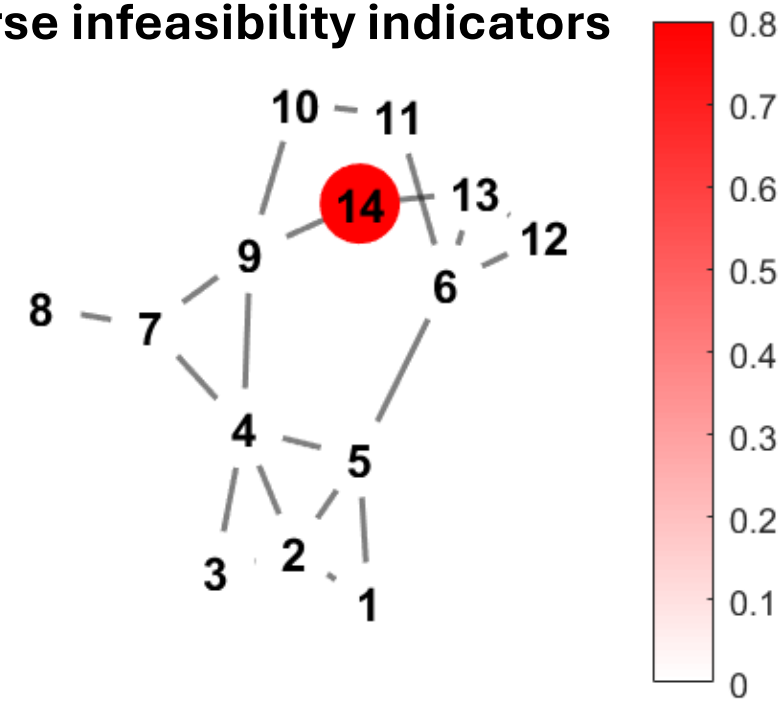
Sparse matrix

$$\begin{bmatrix} \mathbf{1} & \mathbf{2} & 0 & 0 & 0 & 0 \\ \mathbf{2} & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & \mathbf{3} & 0 \\ 0 & 0 & 0 & \mathbf{2} & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix}$$

Key enabler: sparsity-exploiting optimizations

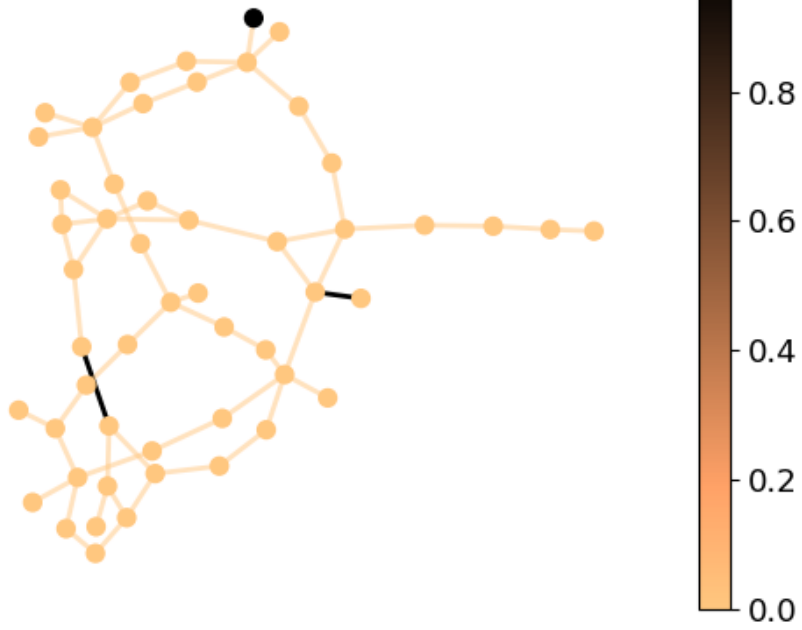
- Making physics-based tools intrinsically **robust to random threats**

Simulation with sparse infeasibility indicators



Dominant sources of blackout are sparse.

Estimation with sparse error indicators

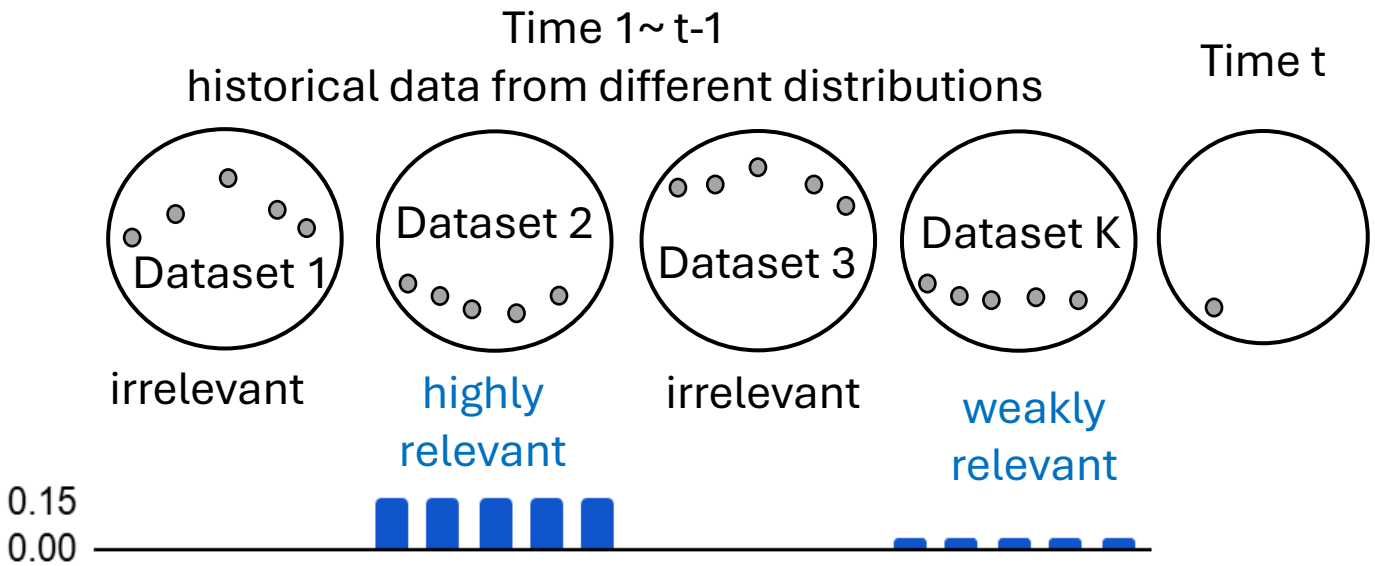


Anomalous data are sparsely distributed

Key enabler: sparsity-exploiting optimizations

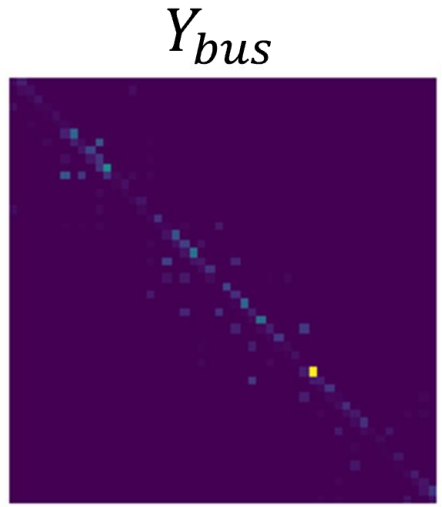
- Developing lightweight ML that is **generalizable and scalable**

Temporal sparsity



Relevant data are sparsely distributed among all historical data;
Sparse weights pinpoint relevant data.

Spatial sparsity



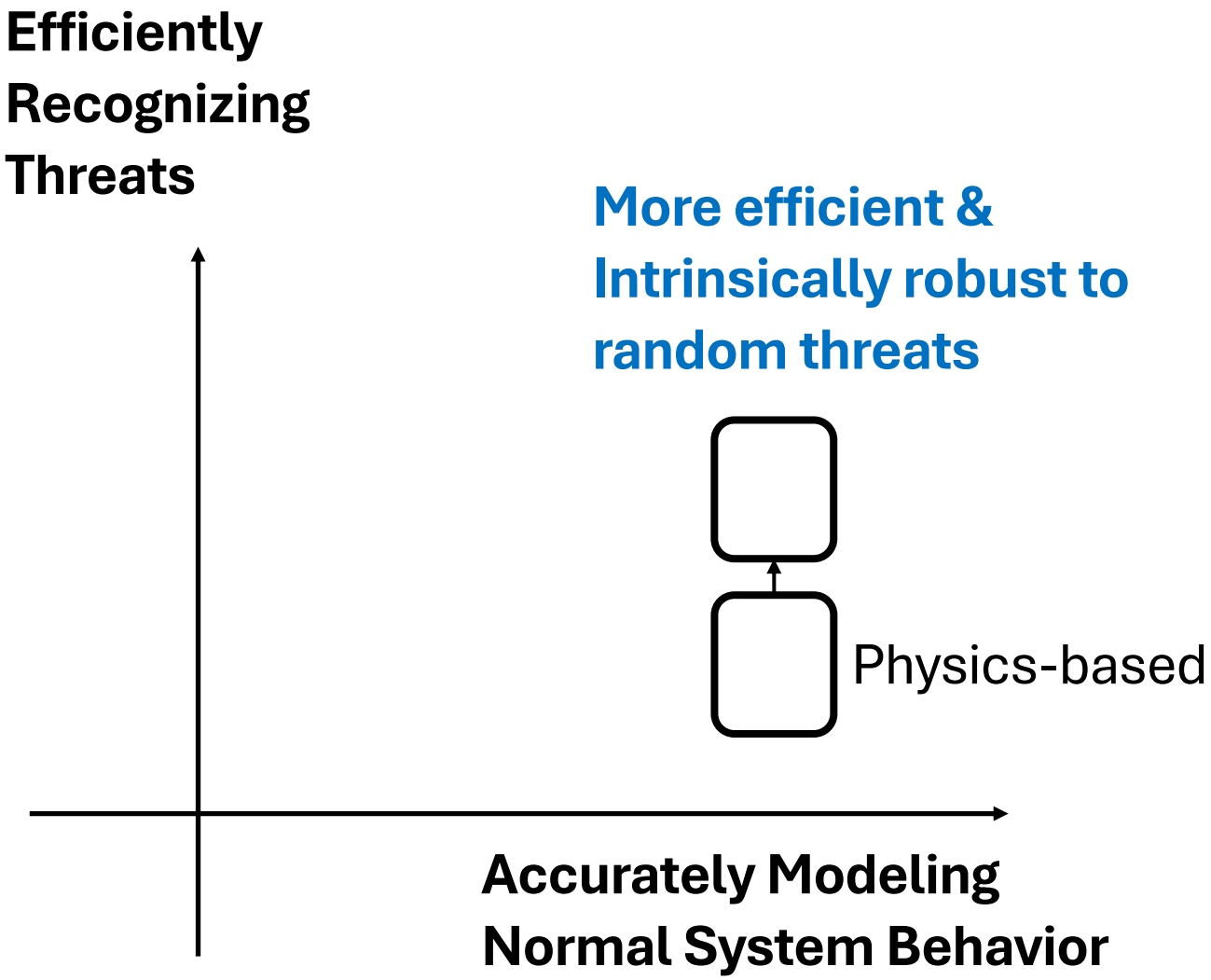
Power grid is a sparsely-connected graph;
Sparse model has low complexity

Outline

- Part 1: Physics-based tools – efficient & robust to random threats
- Part 2: Lightweight ML – generalizable, scalable & interpretable
- Part 3: Physics-ML Synergy – efficient & robust to cyberthreats

Part 1: Physics-based tools

- Building efficiency & robustness to random threats

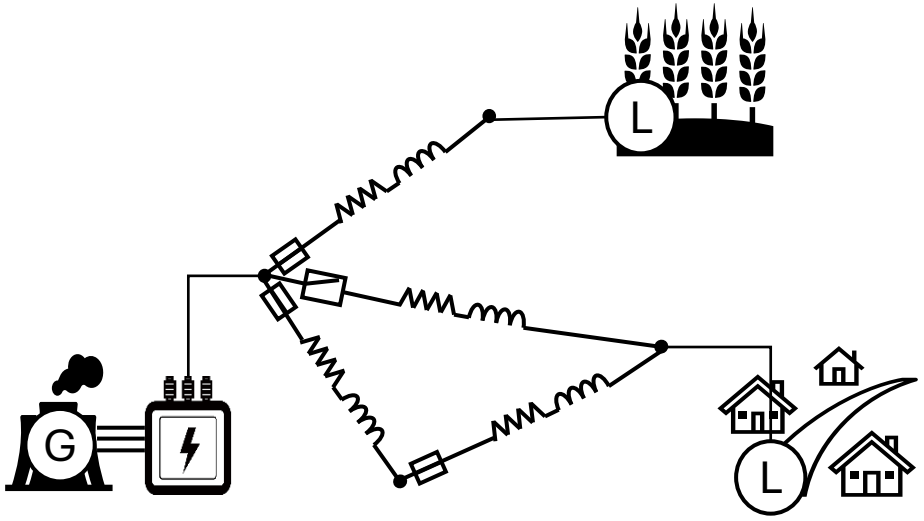


Our approaches are developed with circuit-based formulations

- A unified framework for transmission (T) and distribution (D) systems
- Decades of research in circuit simulation have developed mature heuristics for solving large-scale (nonlinear) circuit with fast speed

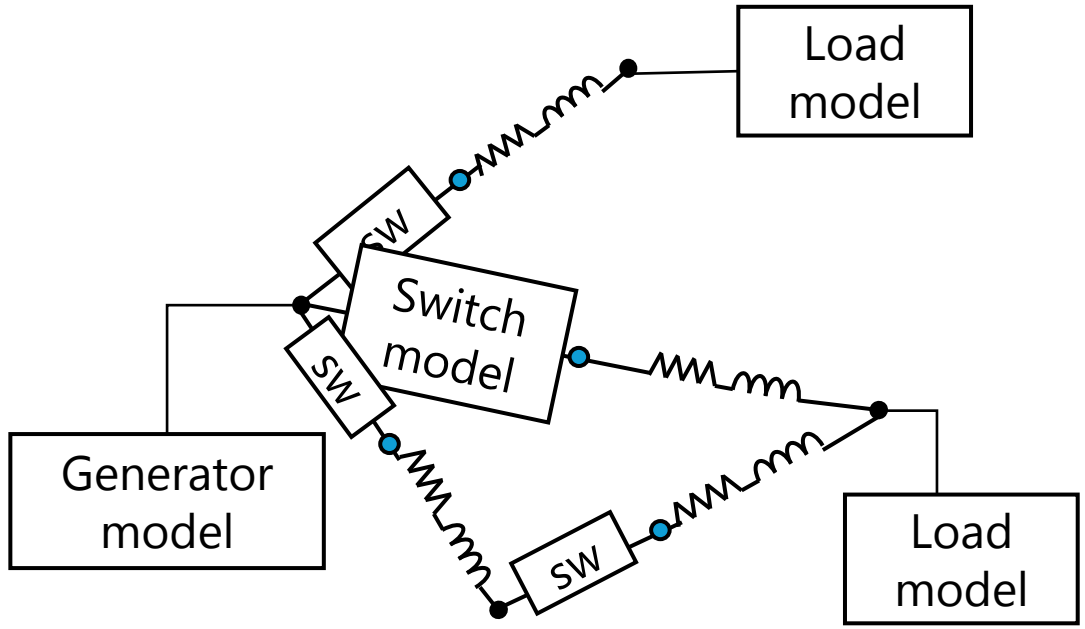
Adopting a circuit viewpoint to simulation and estimation

- Power system can be mapped to a circuit for simulation analysis



Closed switch Open switch

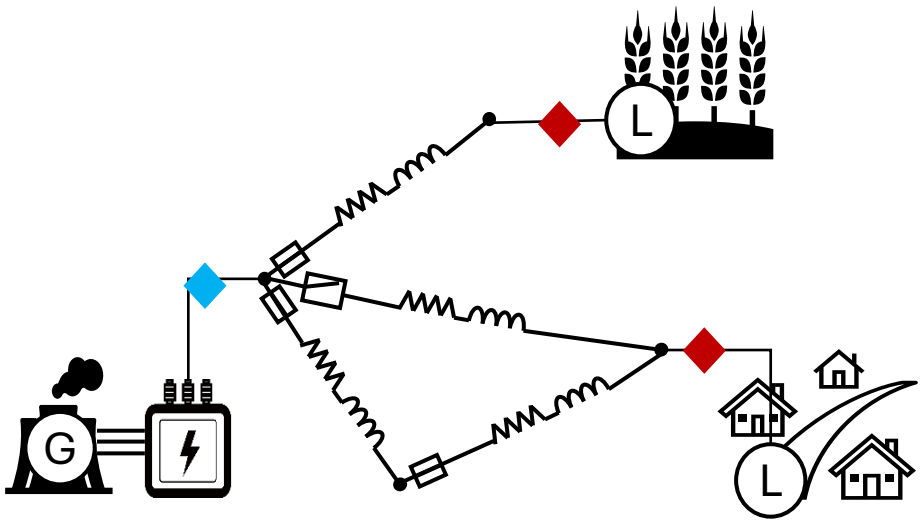
G Generator L Load



- Behavior-based models
- Simulation is to find a feasible solution to the circuit system
- Blackout makes this infeasible!

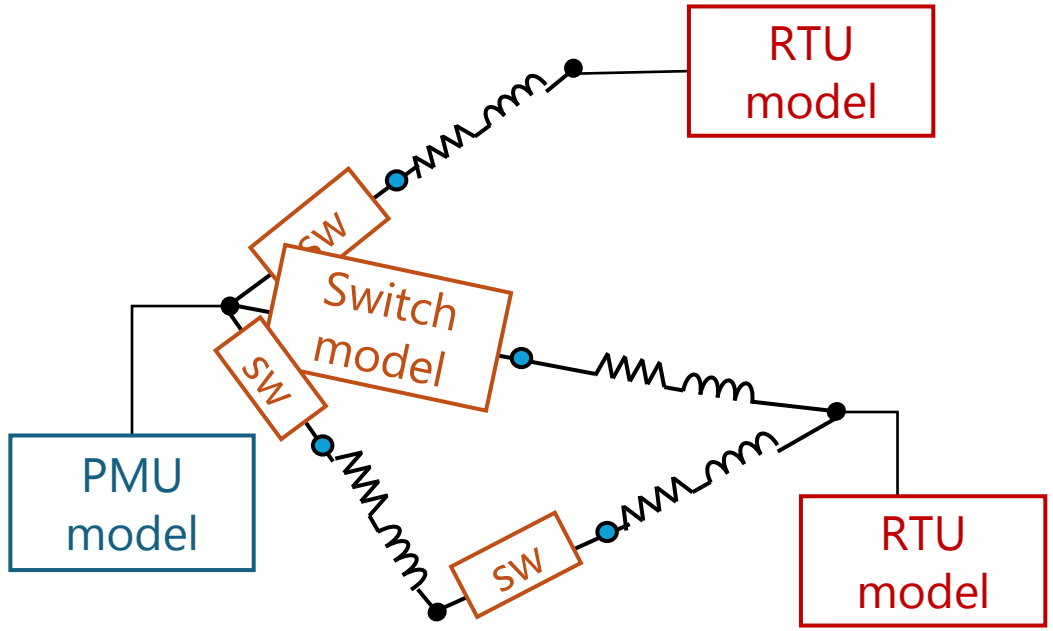
Adopting a circuit viewpoint to simulation and estimation

- The same idea extends to estimation



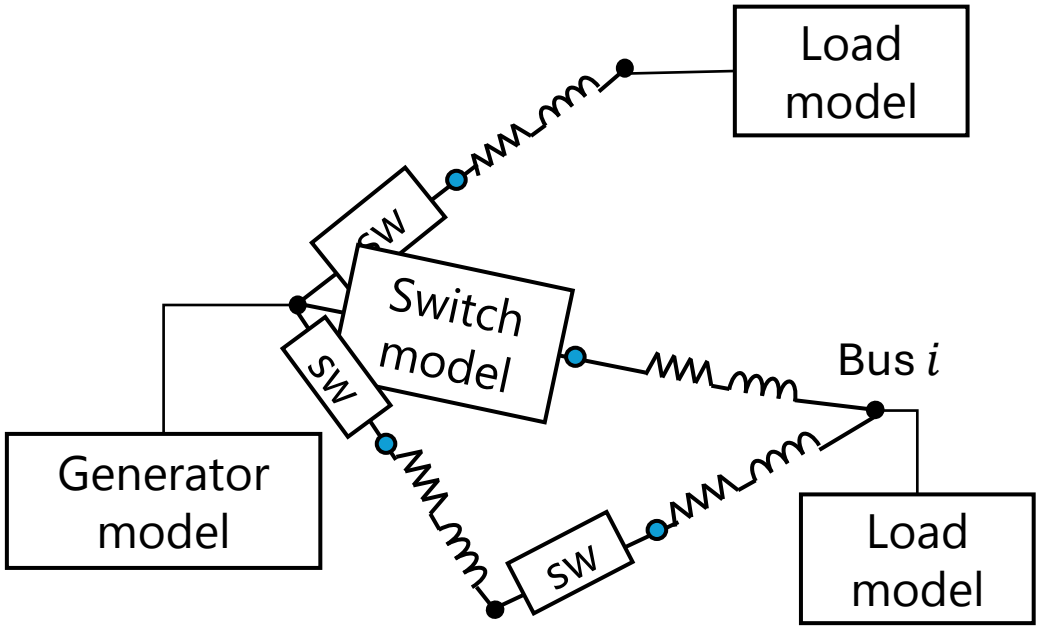
PMU meter

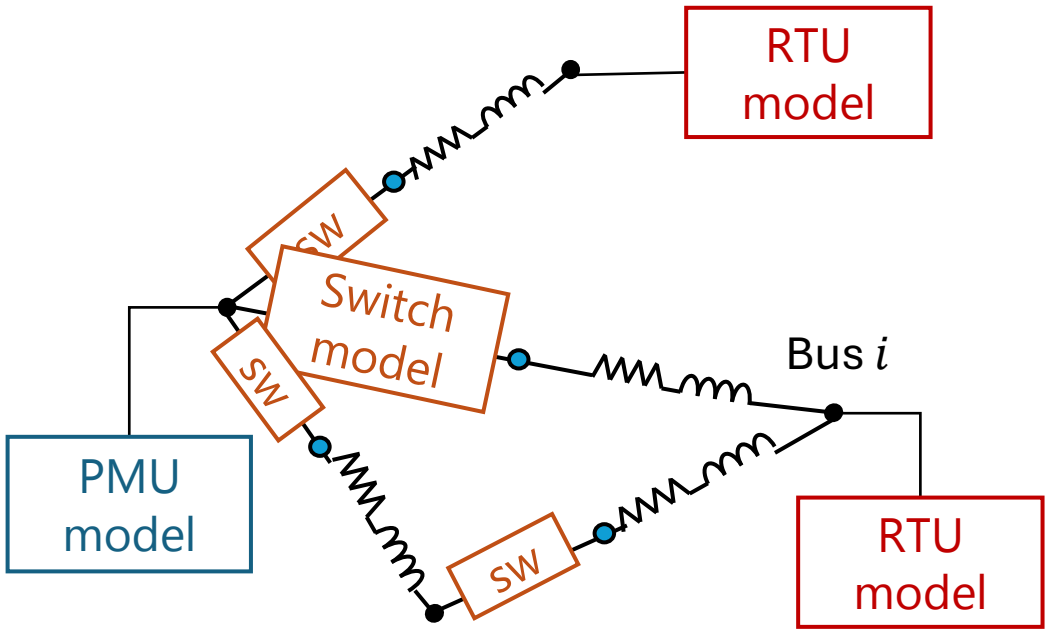
RTU meter



- Measurement-based models
- Estimation is to find a feasible system whose behavior is consistent with the observed data
- Data errors makes this infeasible

Opportunities to efficiency



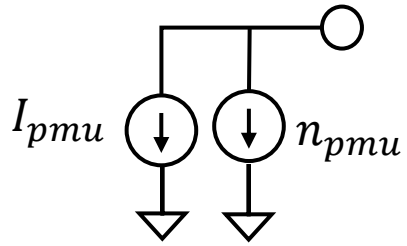


- Branches are linear; nonlinearity exists at generators/loads
- Prior works applied circuit simulation heuristics to advance efficiency

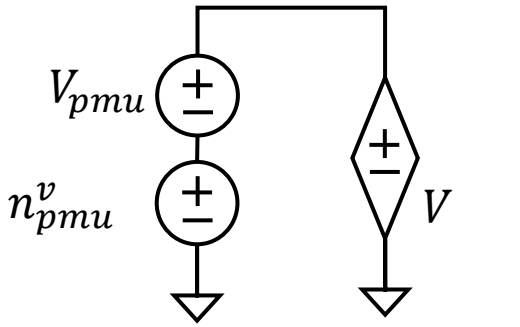
- What if these measurement-based models are all linear? A linear system!

My research: building linear measurement models

- PMU, RTU, and switch models

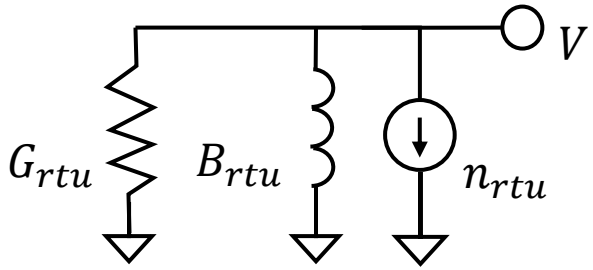


(Current phasor)

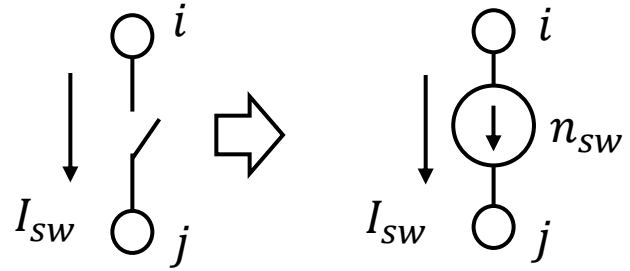


(Voltage phasor)

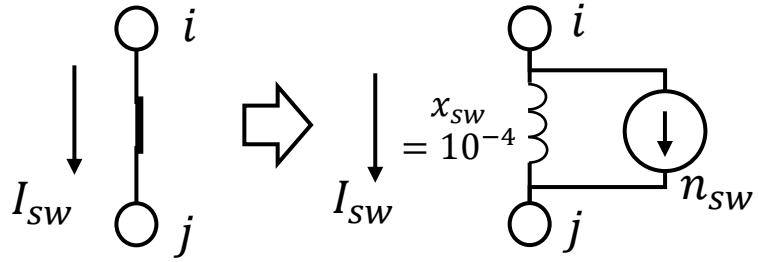
PMU model



RTU model

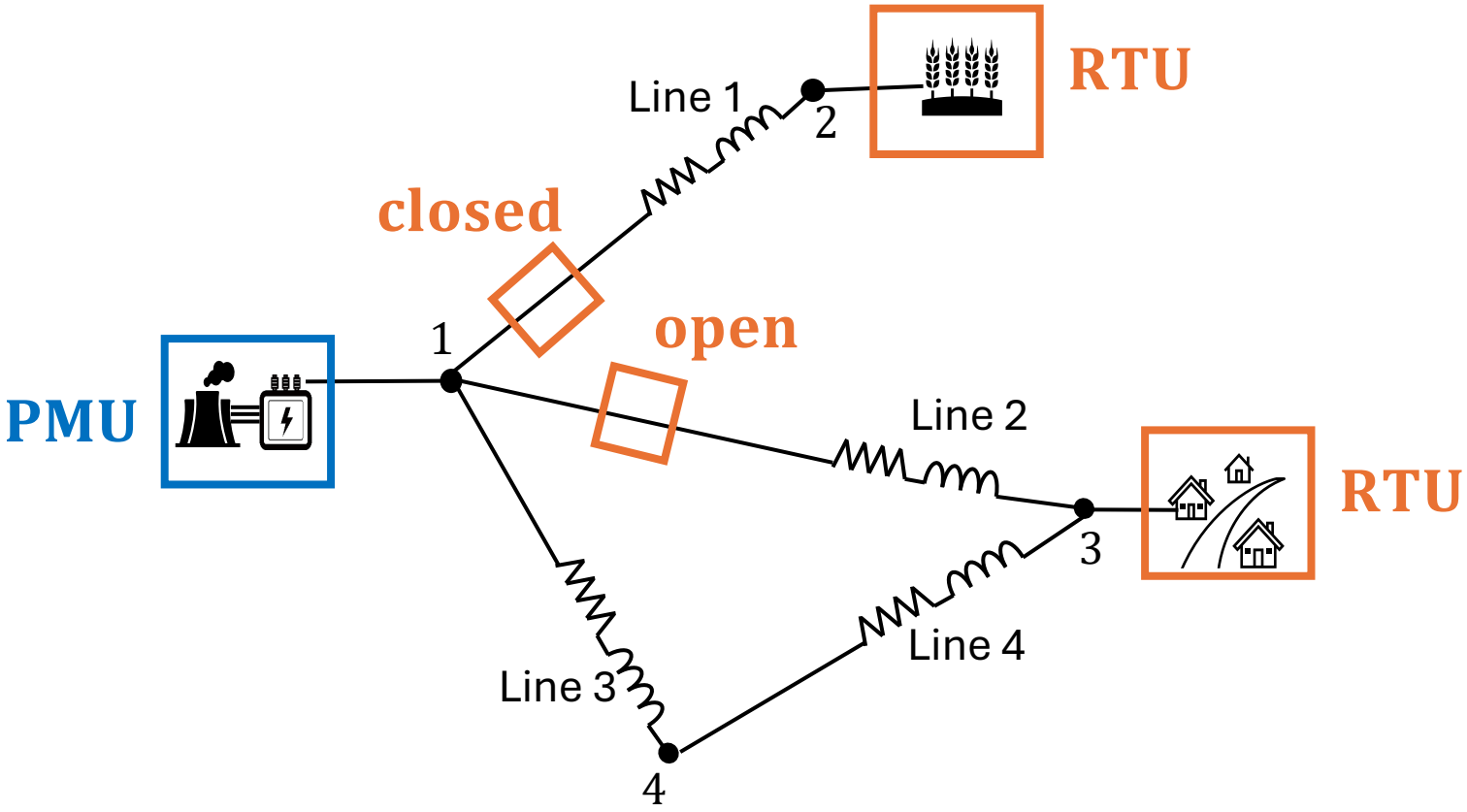


Open switch model



Closed switch model

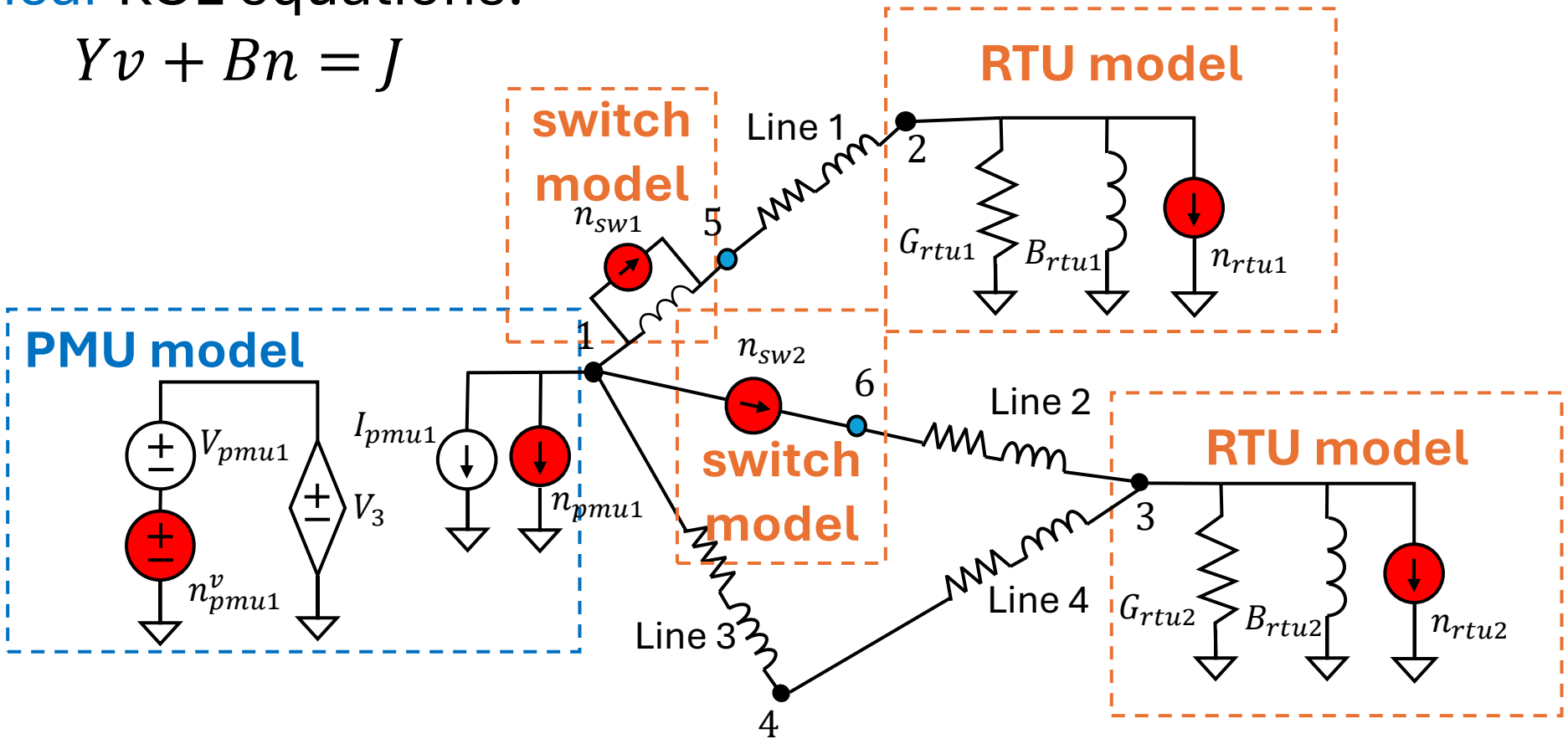
Now given any system with measurements



Equivalently representing measured system into a linear circuit

Linear KCL equations:

$$Yv + Bn = J$$



Convex estimation with closed-form solution

- Minimize measurement noises subject to network constraints

$$\min_{v,n} \frac{1}{2} n^T W n$$

$$Yv + Bn = J$$

$$\begin{bmatrix} x^* \\ n^* \\ \lambda^* \end{bmatrix} = \begin{bmatrix} Y & B & 0 \\ 0 & 0 & Y^T \\ 0 & W & B^T \end{bmatrix}^{-1} \begin{bmatrix} J \\ 0 \\ 0 \end{bmatrix}$$

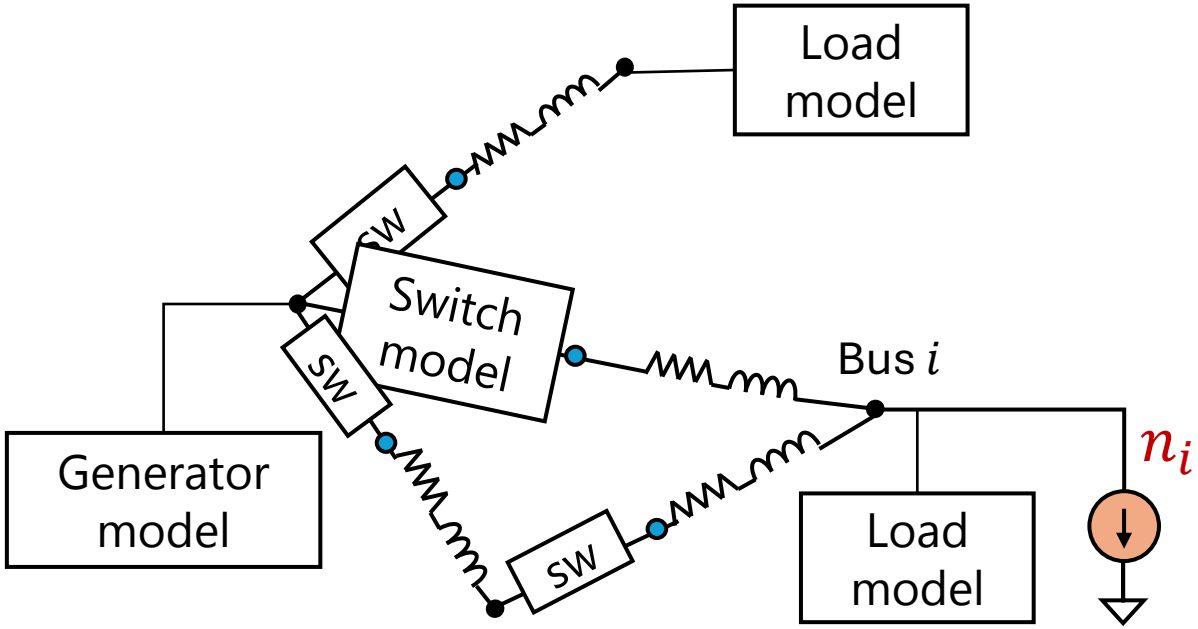
Nonlinear estimators need iterative solvers

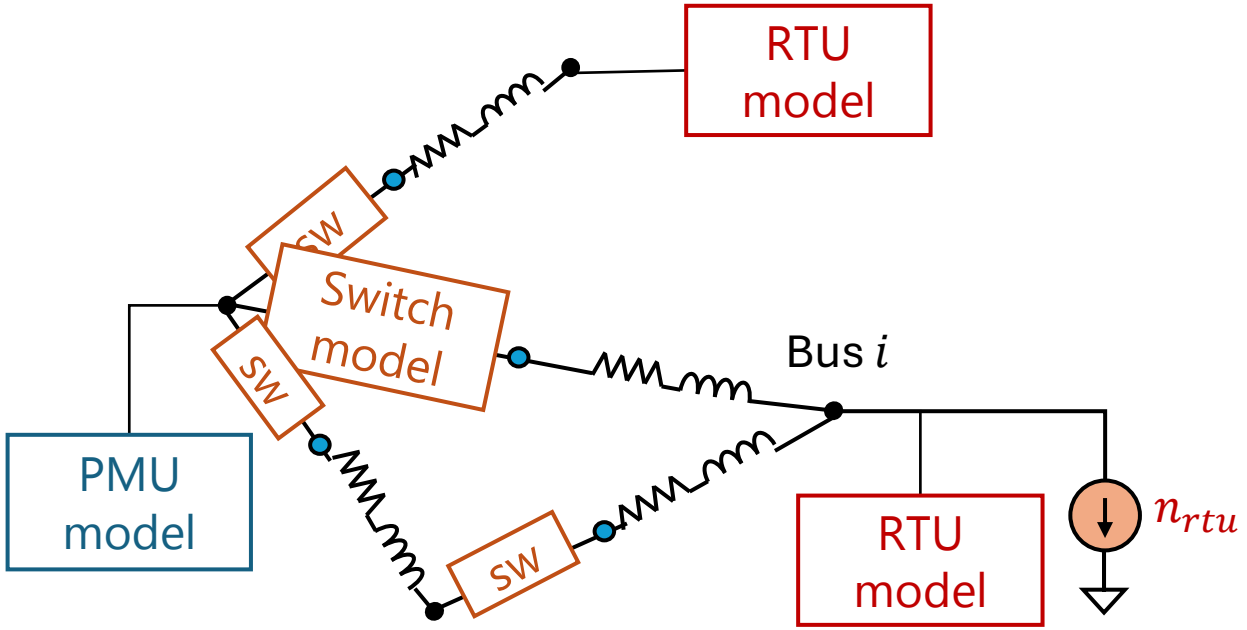
Case name	Num of iterations to converge		
	Traditional, case start	Traditional, flat start	Circuit-based
case14	4	5	1
case118	4	6	1
case2383wp	diverge	6	1
case3375wp	5	diverge	1
case6468rte	7	diverge	1
case9241pegase	11	diverge	1
ACTIVSg25k	diverge	diverge	1

We just need one linear solve!

Robustness remains a concern!

Opportunity to robustness: threat indicators

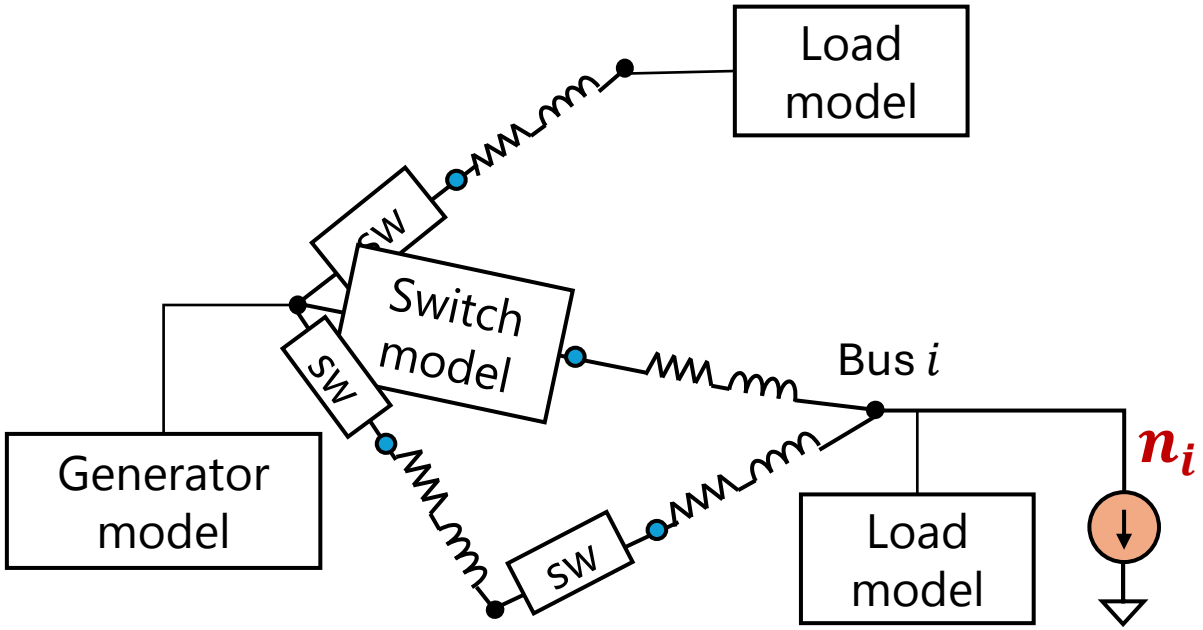




n_i : threat indicator of power deficiency at bus i.

n_{rtu} : threat indicator of measurement error at RTU bus i

Application 1: towards robust and actionable simulation



n_i : threat indicator of power deficiency at bus i.

Network balance at bus i:

$$\boldsymbol{F_i(V, G, D) + n_i = 0}$$

$\boldsymbol{n_i}$ compensates power deficiency, and now supply meets demand at this bus

Making the unsolvable cases solvable

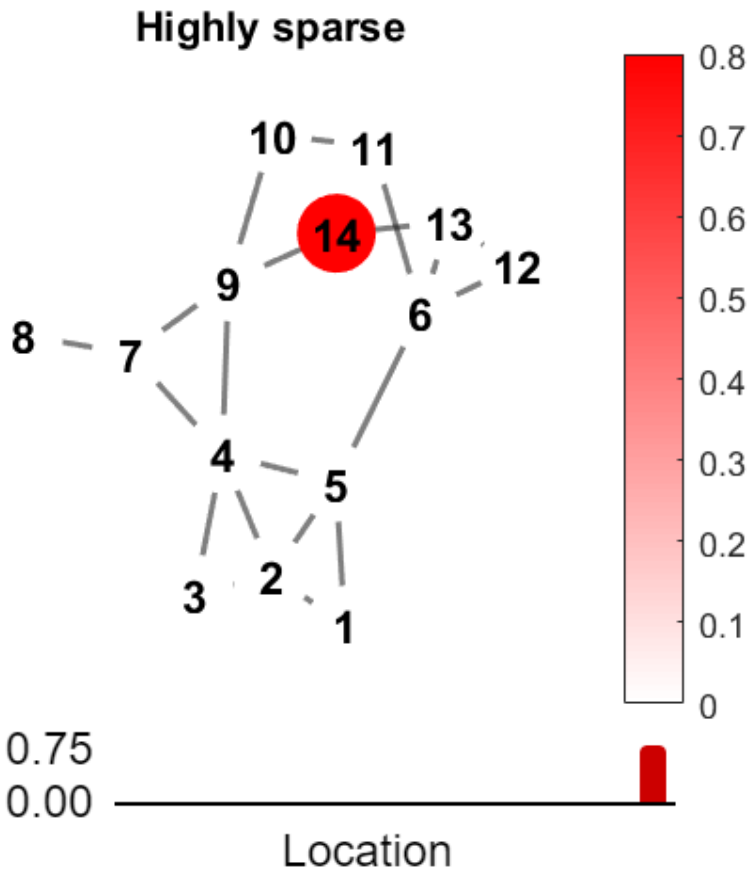
No feasible solution exist
(Simulation diverges)

With compensations everywhere
There exist (infinite) solutions $[V, n]$.

$$\boldsymbol{F} = \begin{cases} \text{Node 1: } \boldsymbol{F_1(V, G, D) = 0} \\ \vdots \\ \text{Node N: } \boldsymbol{F_N(V, G, D) = 0} \end{cases} \longrightarrow \begin{cases} \boldsymbol{F_1(V, G, D) + n_1 = 0} \\ \vdots \\ \boldsymbol{F_N(V, G, D) + n_N = 0} \end{cases}$$

My research: a robust actionable simulation

- A variant of LASSO to enforce high sparsity



c_i: bus-wise sparsity enforcer

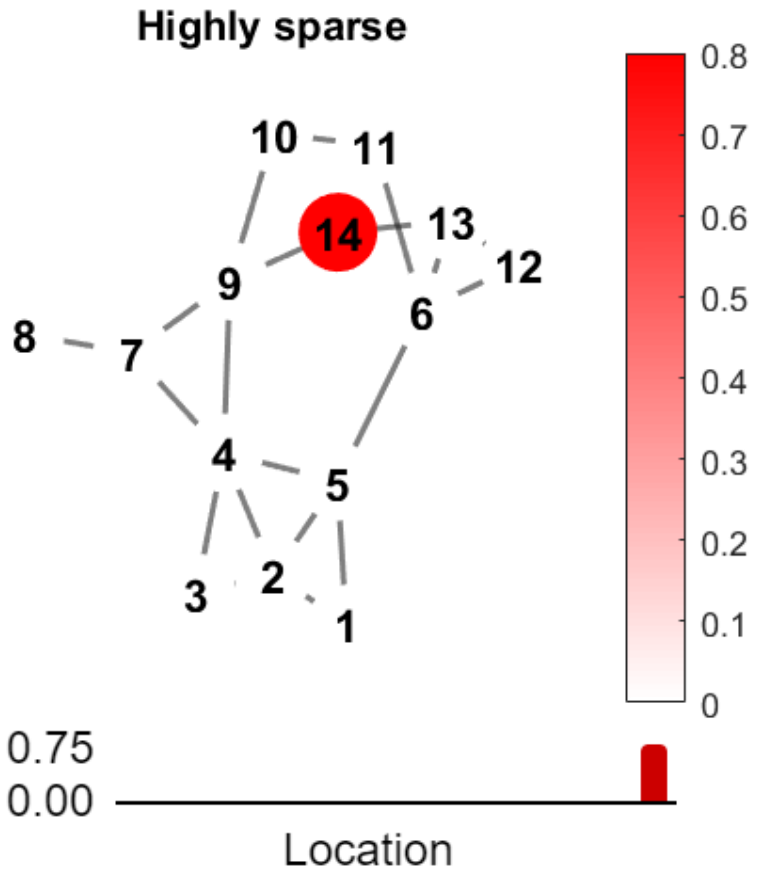
$$\min_{V} \frac{1}{2}\left|\left|n\right|\right|_2^2 + \sum_{i=1}^{N} c_i \left|\left|n_i\right|\right|_1$$

s.t.

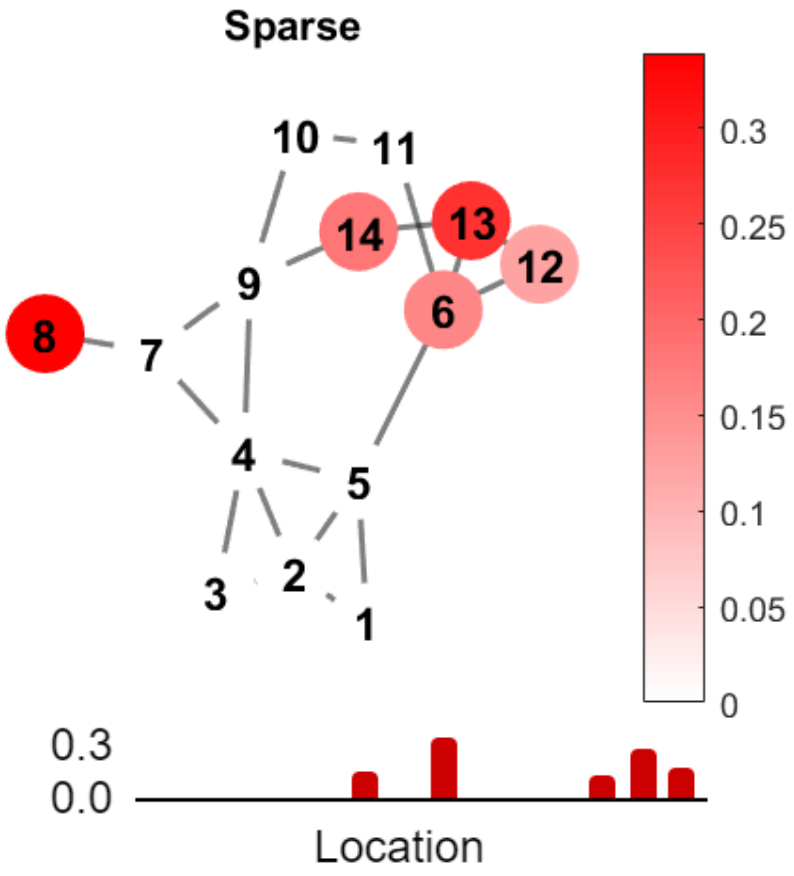
$$F_1(V, G, D) + n_1 = 0$$
$$\vdots$$
$$F_N(V, G, D) + n_N = 0$$

Dominant sources of blackout is pinpointed.
Severity of blackout can be quantified.

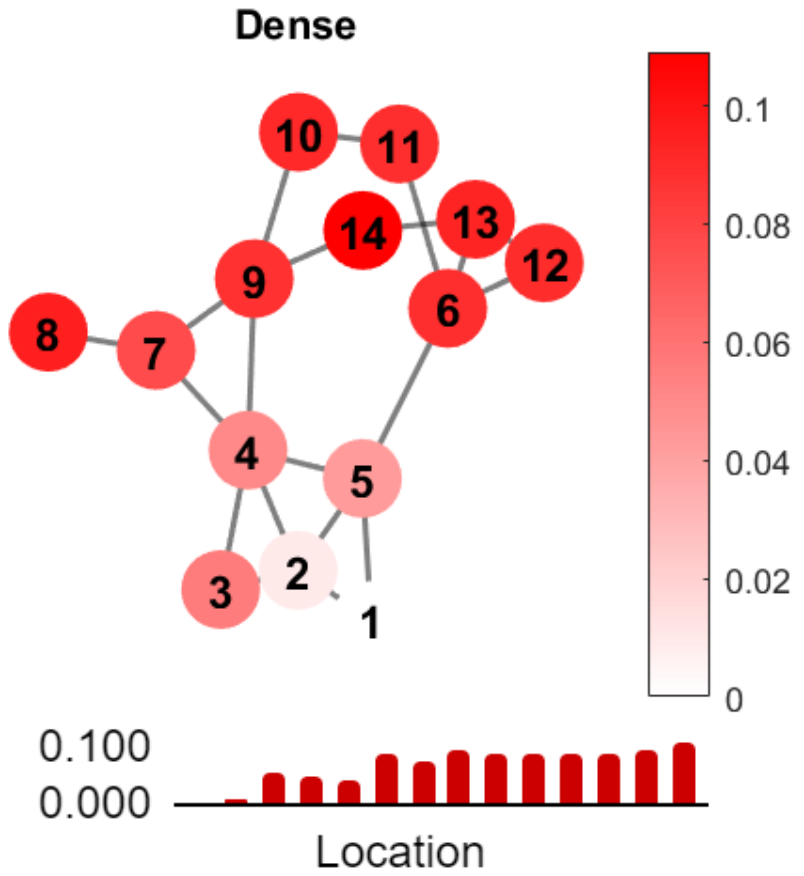
Sparse indicators pinpoint key locations to fix blackouts



Need 1 power plant to fix it.

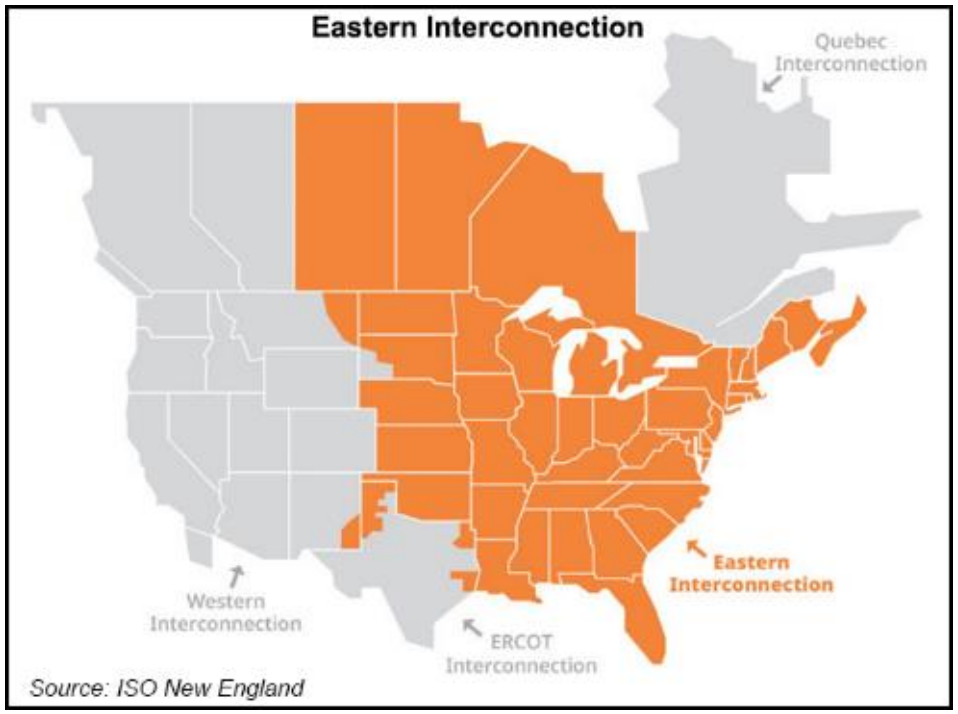


Need 5 power plants to fix it.



Need new plants everywhere

On large-scale Eastern Interconnection System

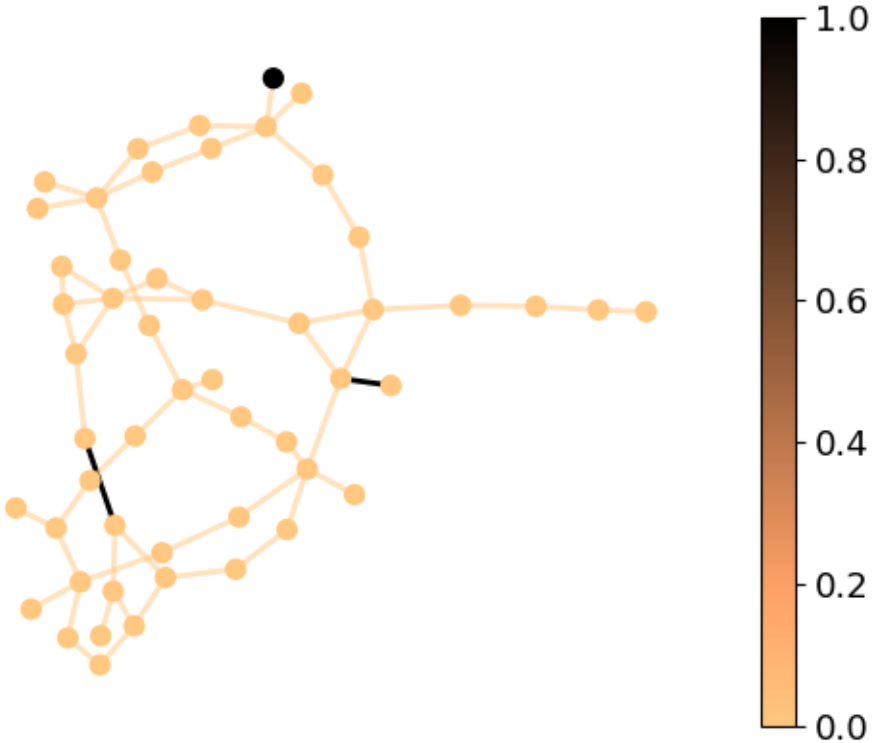


Eastern Interconnection Case
(80K-bus system)

Pinpoint dominant failure source at **only 1 bus**, when we increase load by 7%

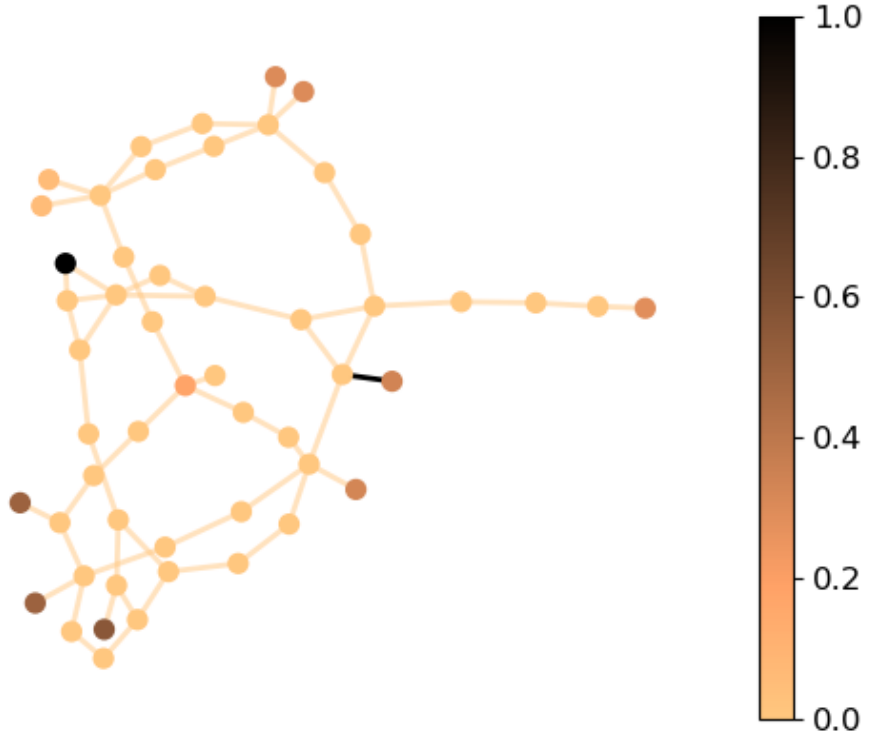
Application 2: towards robust convex estimation
Sparse error indicators pinpoint **random** data errors

Robust estimator



1 bad data and two topology errors are located accurately

Non-robust estimator



Data errors cannot be located accurately

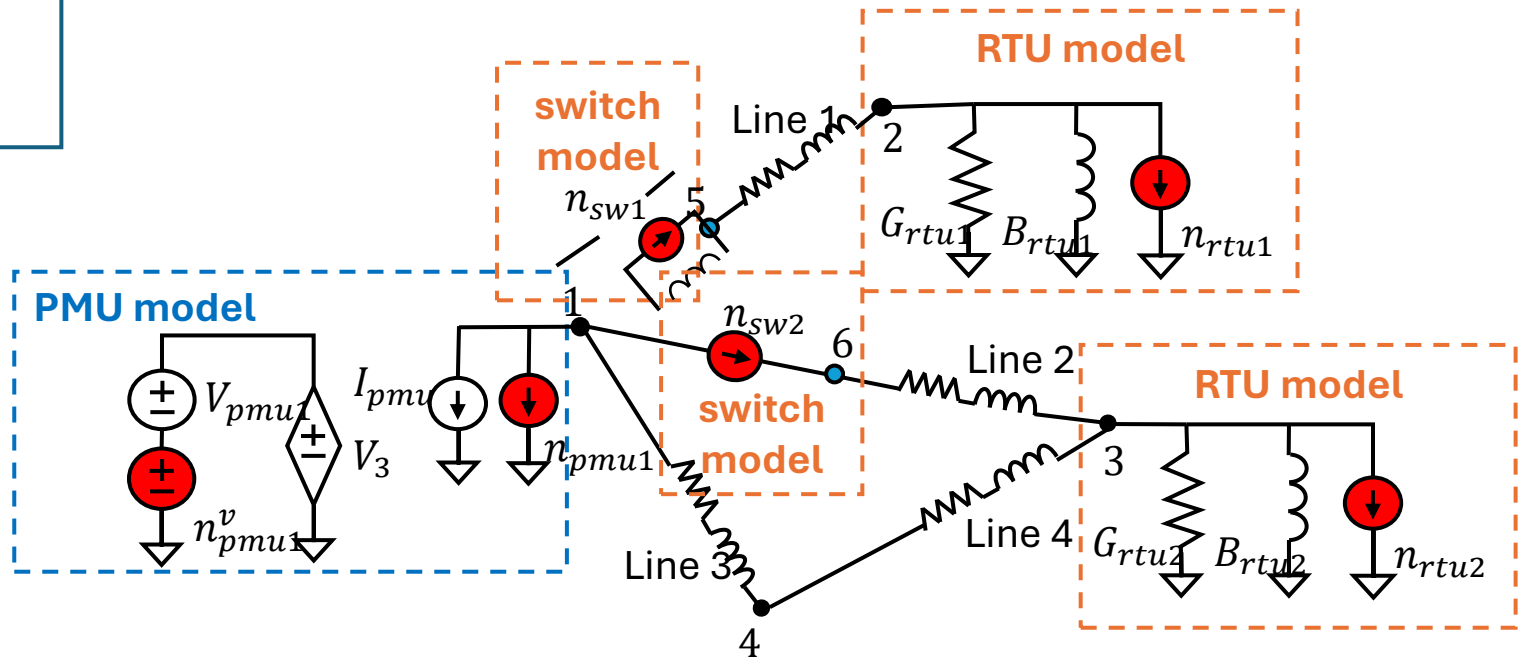
Methodology: a robust convex estimator

- A linear programming problem

$$\min_{v,n} ||n||_1$$

$$Yv + Bn = J$$

- Objective function enforces sparsity
- Affine constraints written from linear KCL equations

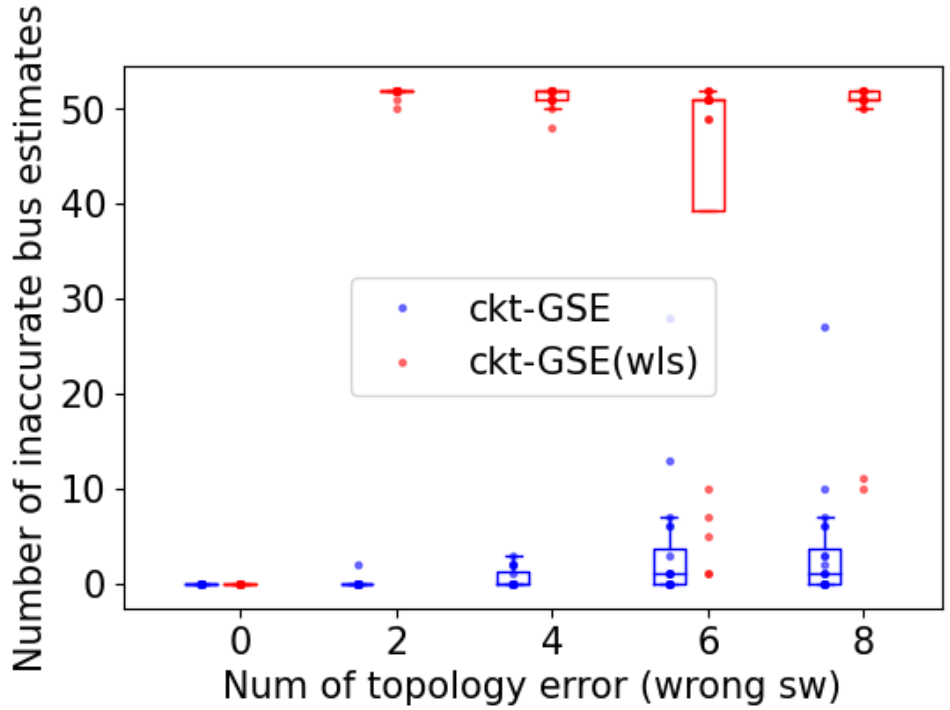


Accurate estimation of states (a 52-bus system with 49 switches)

Num. of buses whose voltage solutions are inaccurate

(err >0.02pu, 2 deg)

The lower the better

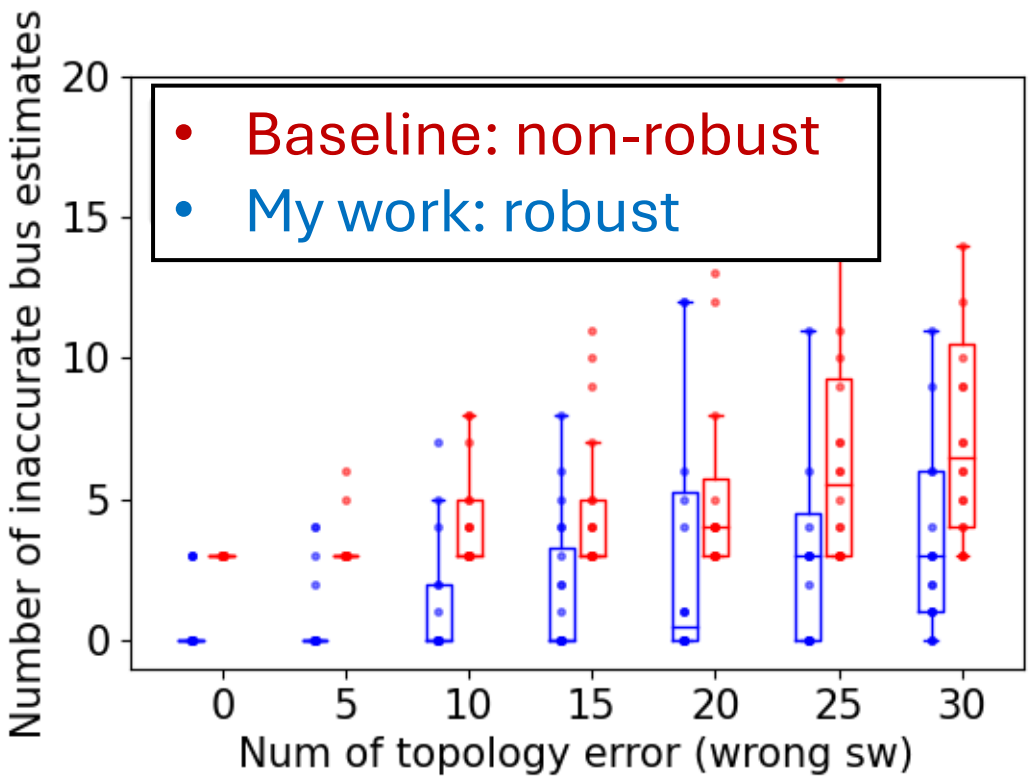


- Baseline: non-robust
- My work: robust

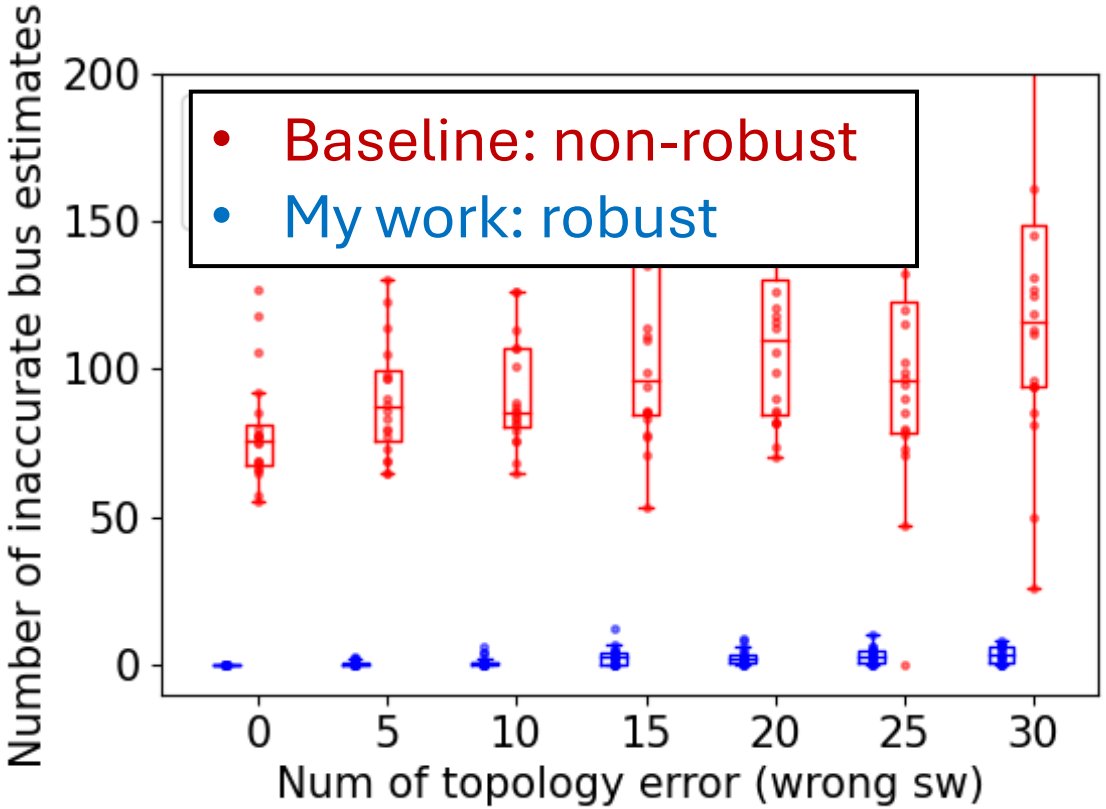
The number of data error increases

Accurate estimation of states (large scale systems)

>1.6k buses, 1.8k switches

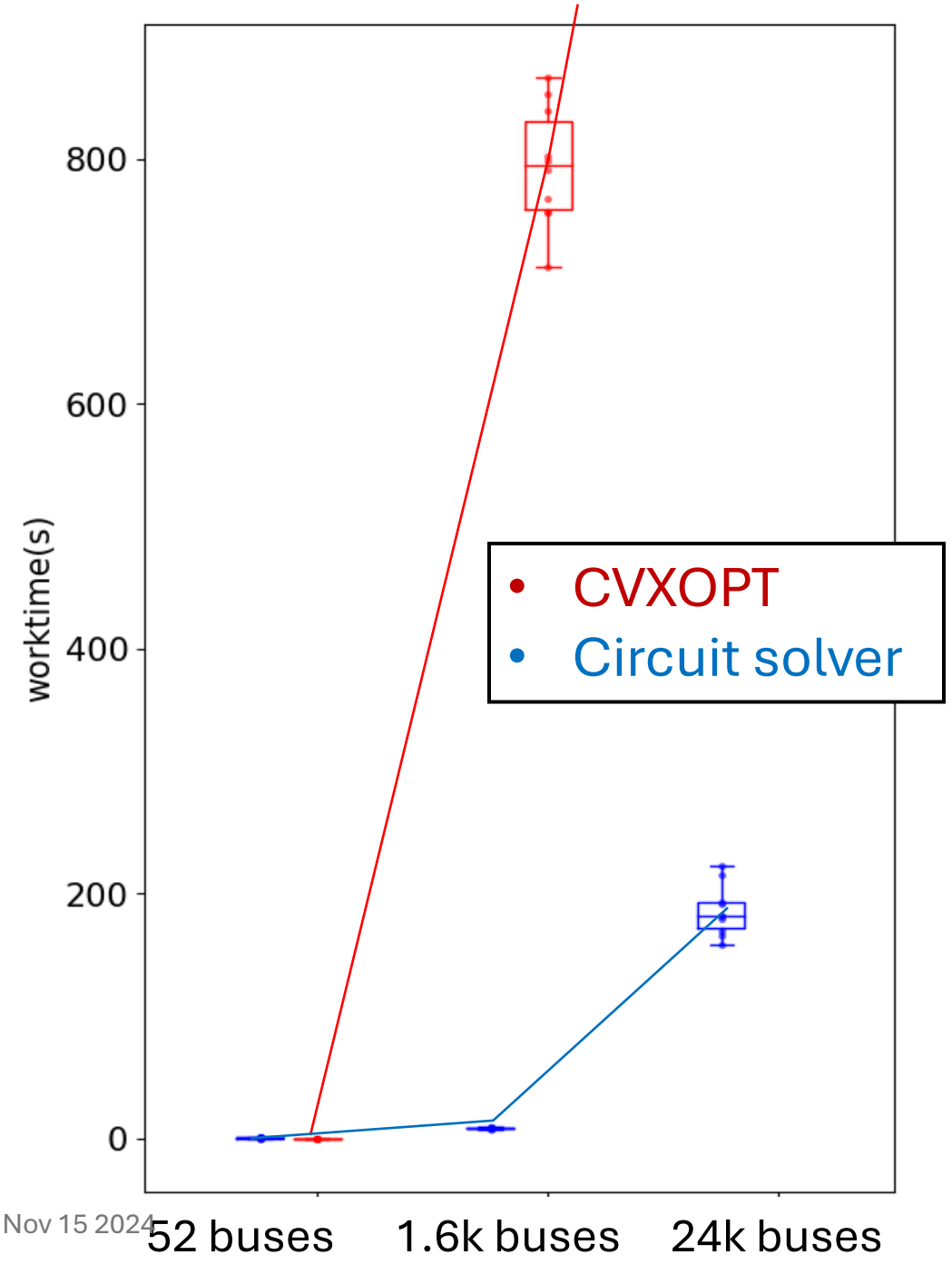


>24k buses, 23k switches



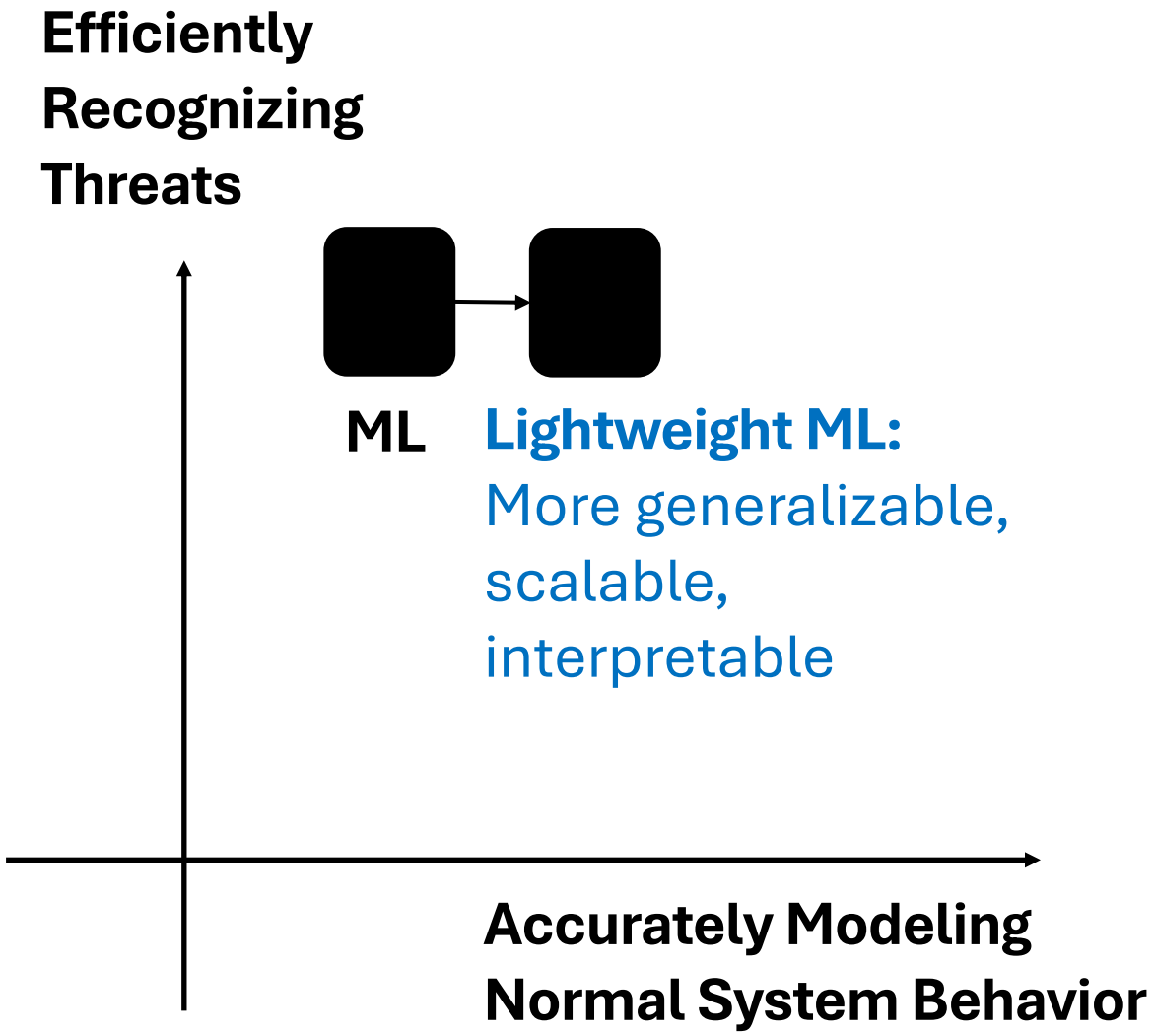
Faster speed than standard tools

When solving Linear Programming, our circuit-theoretic solver is much faster than standard Interior Point Method (CVXOPT)



Part 2: Lightweight ML

- Capabilities complement physics-based tools
- Inherent limitations addressed



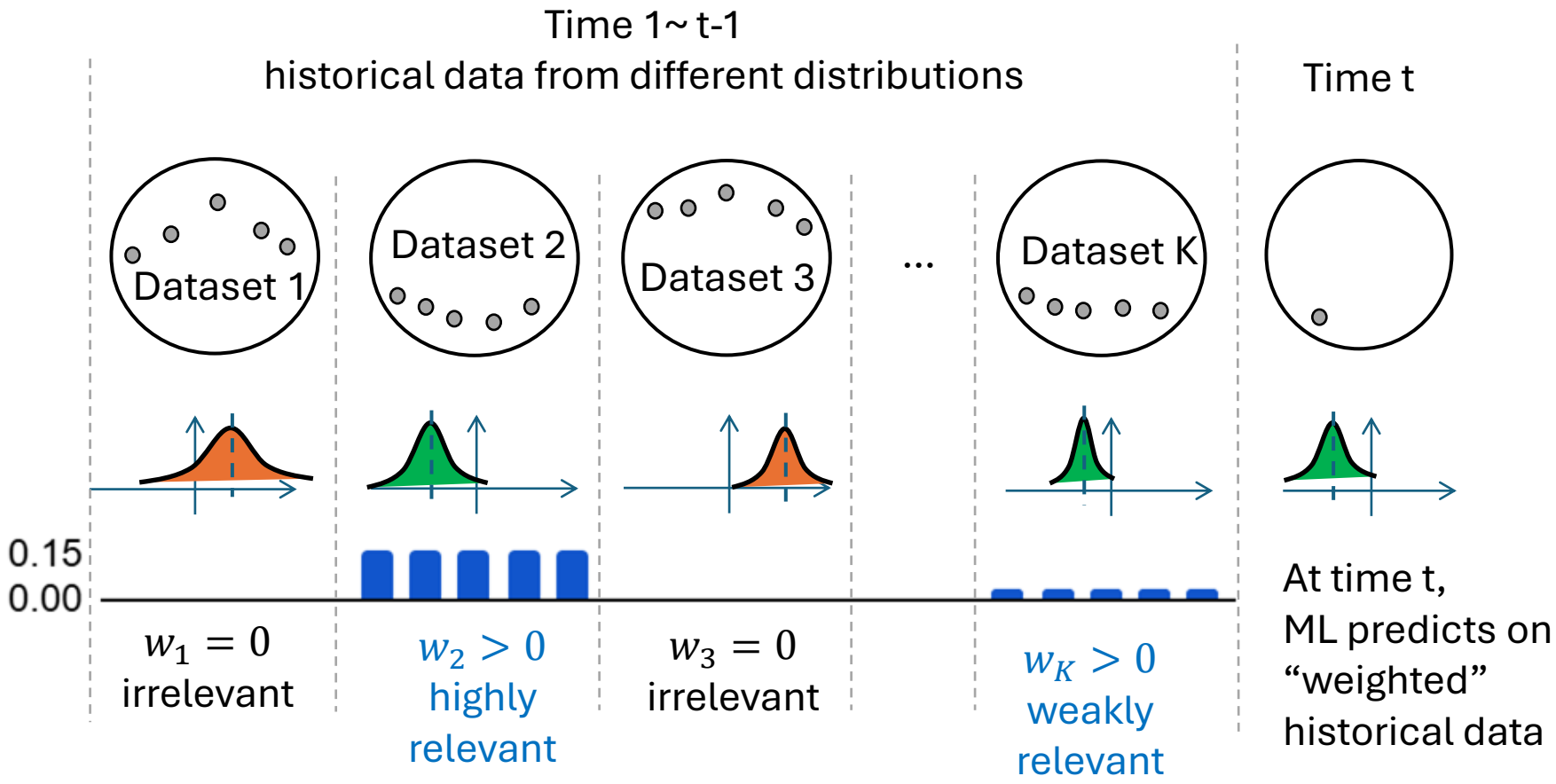
Application 1: time-series ML prediction & detection

- Part 1 has advanced estimation: **random** data errors are identified and rejected efficiently
- Remaining gap: not robust to advanced threats (e.g, cyberattacks)

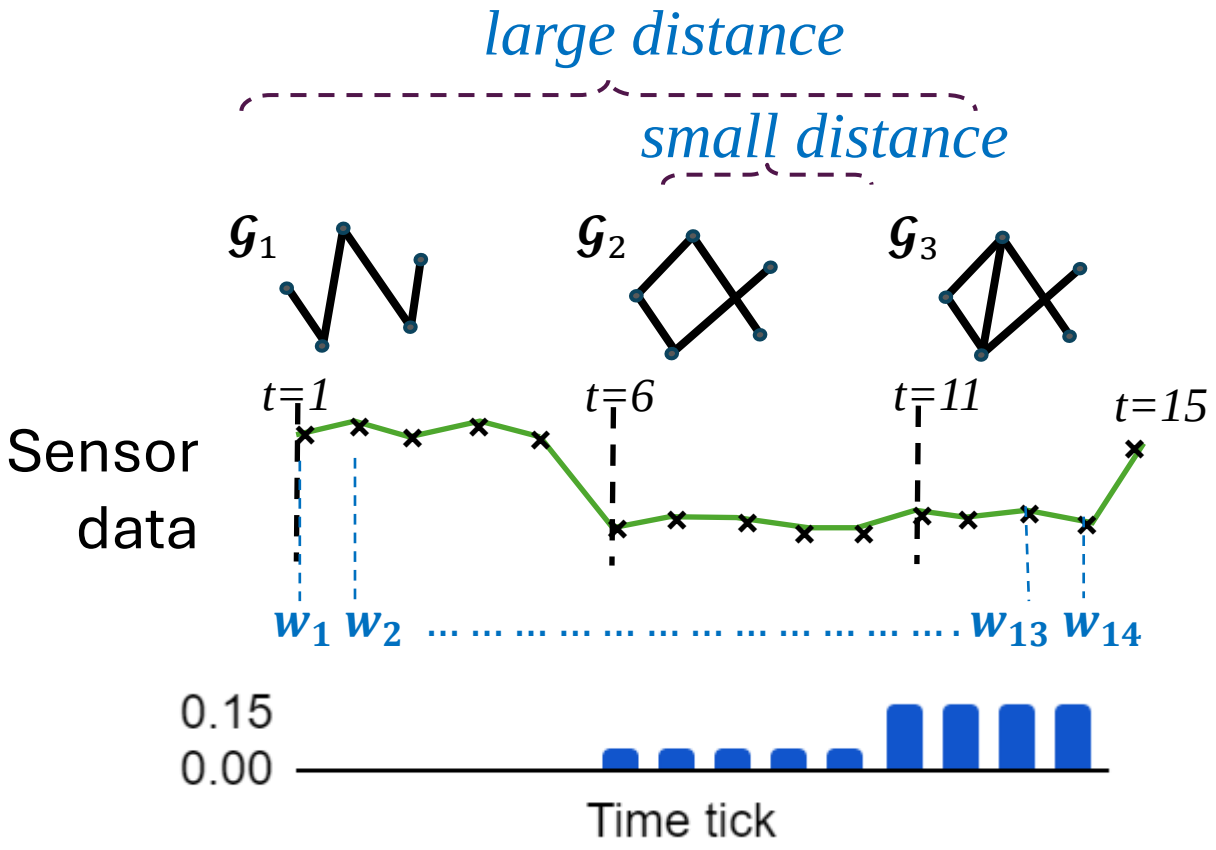
Physics-based estimator
Only consider random threats

Data-driven (ML)
More threats detectable from temporal patterns

Generalize to different distributions via a sparse recommendation



Power system example: topology changes induce dynamic graphs and different sensor data distributions



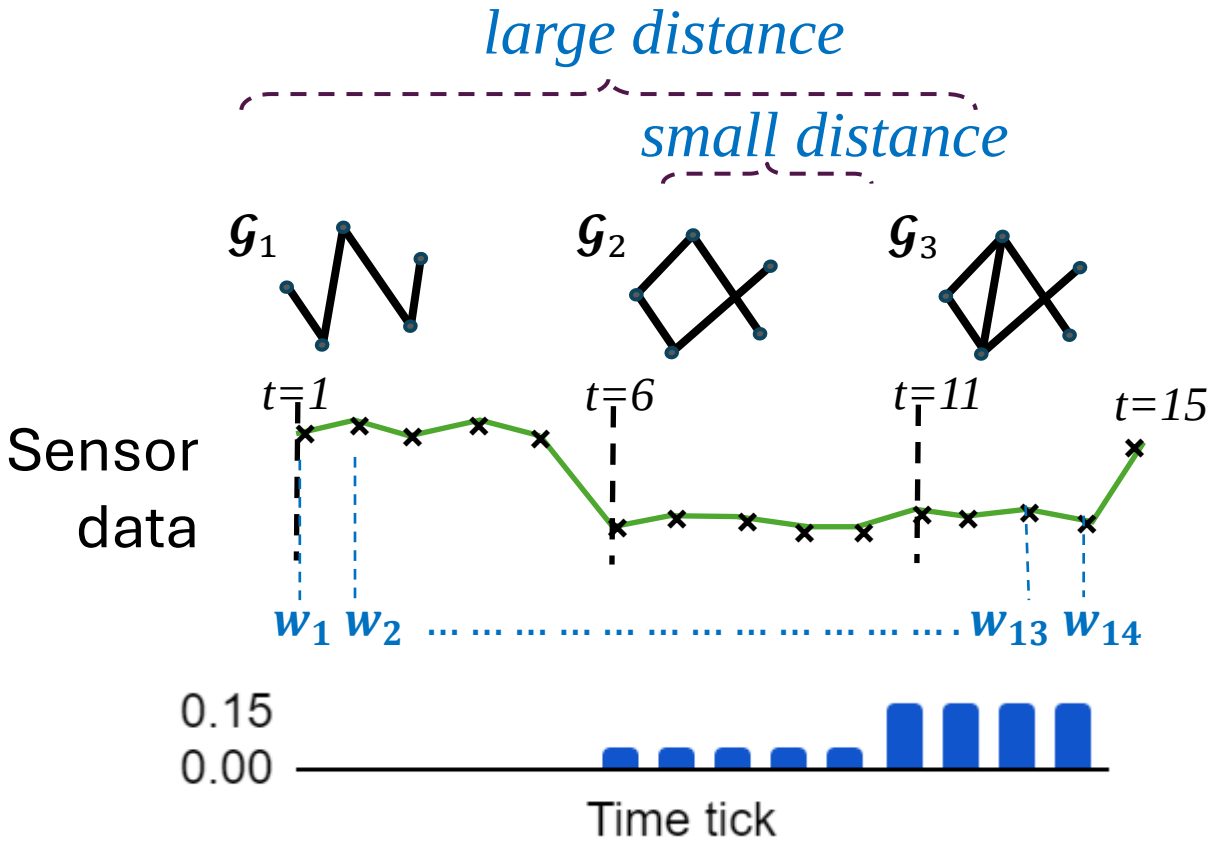
True distributions unknown, but Graph Distance can measure the differences:

Larger distance

Means irrelevant data

Means smaller weights

DynWatch: A distance-based sparse temporal weighting



Solve a **bias-variance trade-off:**

$$\min_w \underbrace{\sum_t w_t d_t}_{\text{bias}} + \underbrace{\beta \frac{1}{2} w^T w}_{\text{variance}}$$

$$\text{s.t.} \quad \sum_t w_t = 1$$

$$w_t \geq 0, \forall t$$

$$= \sum_t |w_t| d_t$$

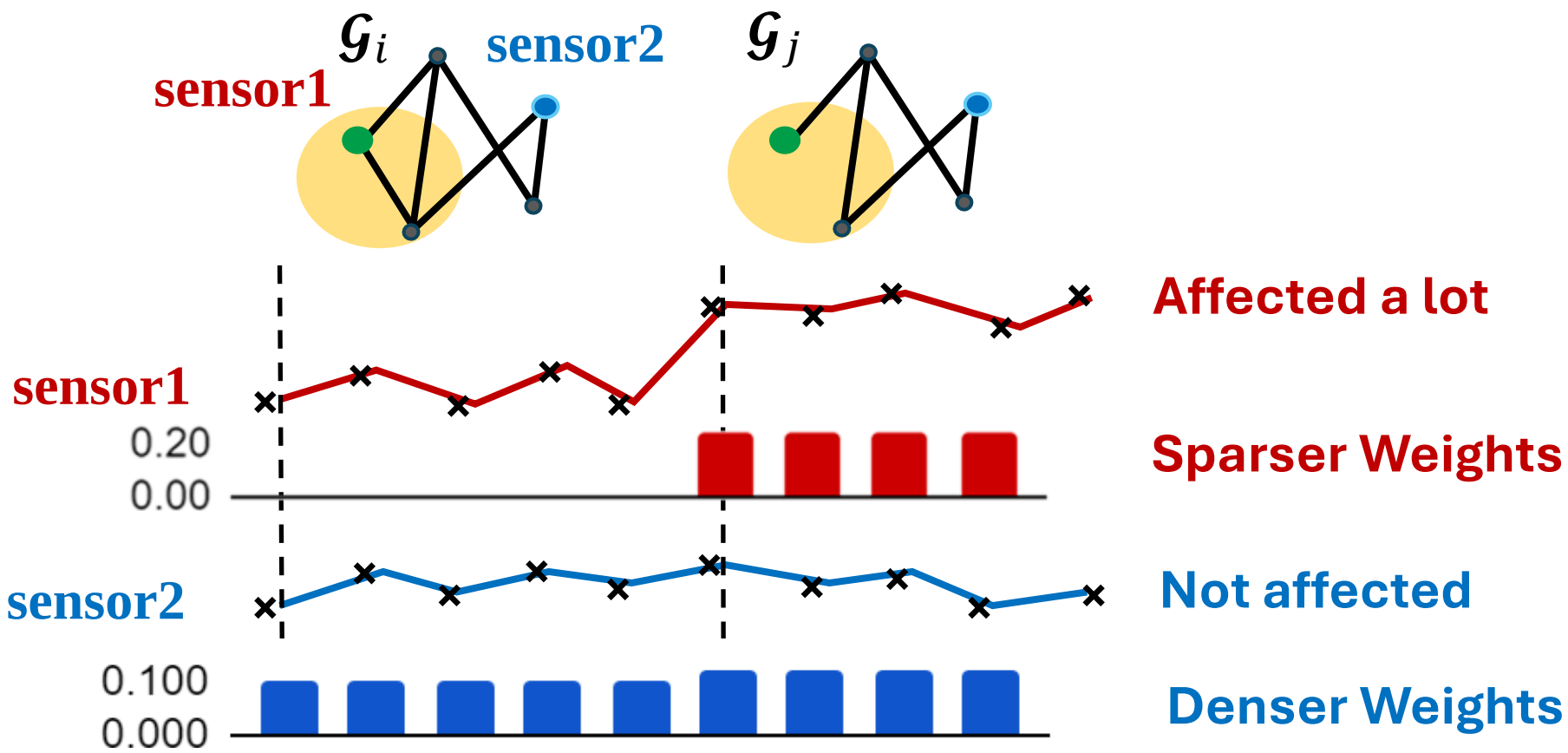
L1 regularization
Enforces sparsity

Weights need appropriate sparsity

Too dense → bias; Too sparse → variance

DynWatch-local: extension to large systems

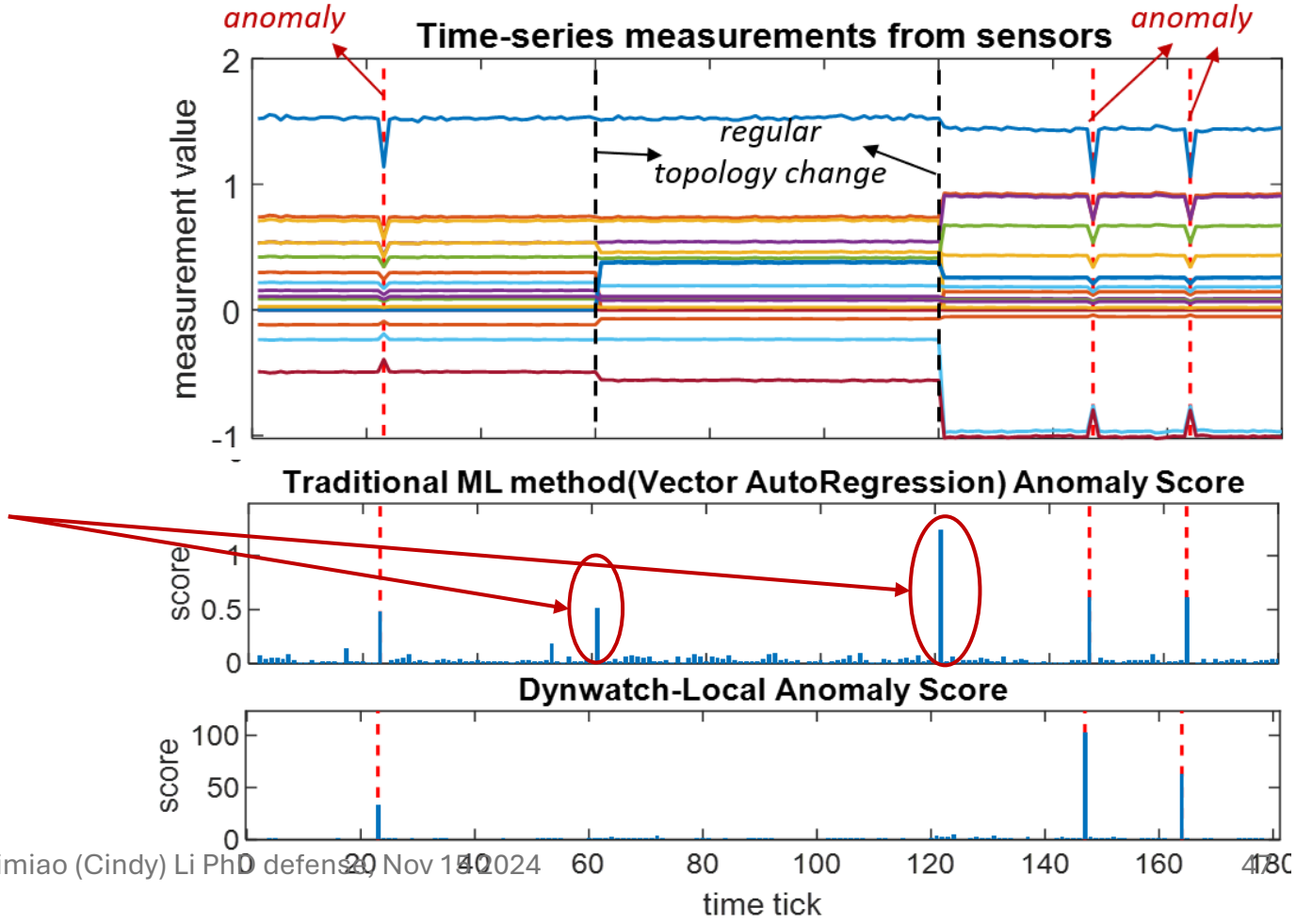
- Distances and weights will be **local-sensitive**



DynWatch: generalizable to dynamic graphs

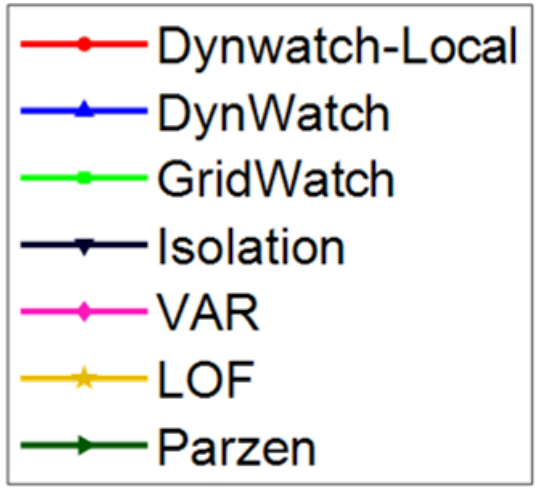
- Anomaly detection: predict distribution from weighted historical data; then calculate anomaly scores

Traditional methods produce false alarms when there's a regular topology change

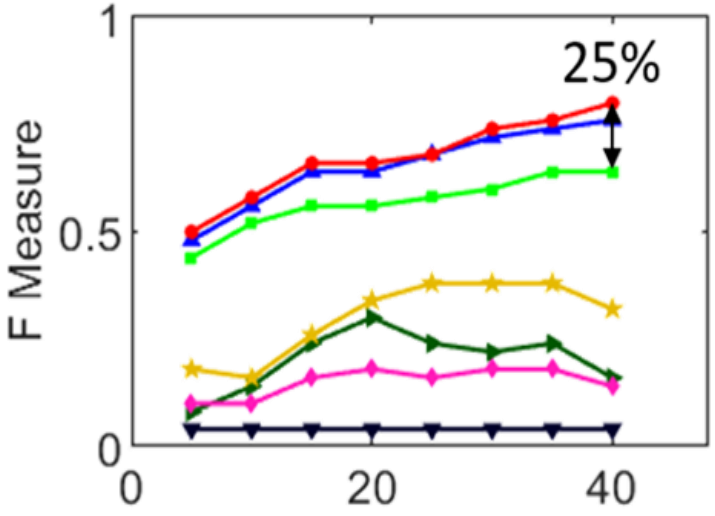


DynWatch: generalizable to dynamic graphs

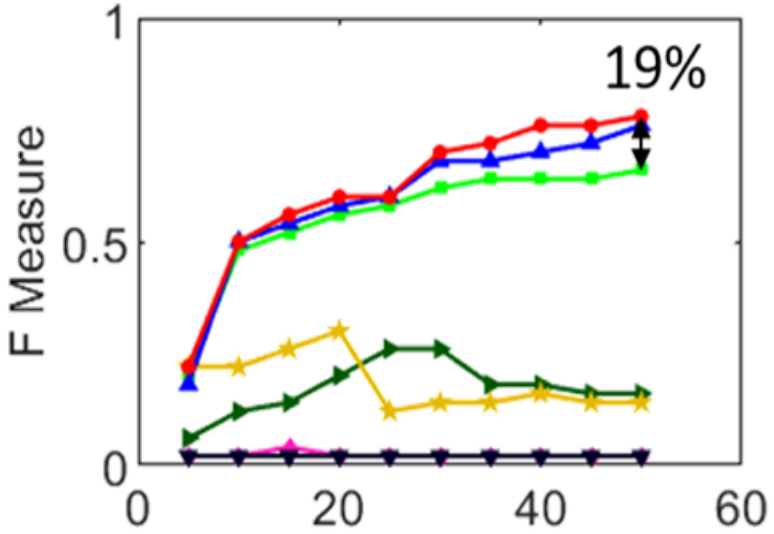
- Better F-measure



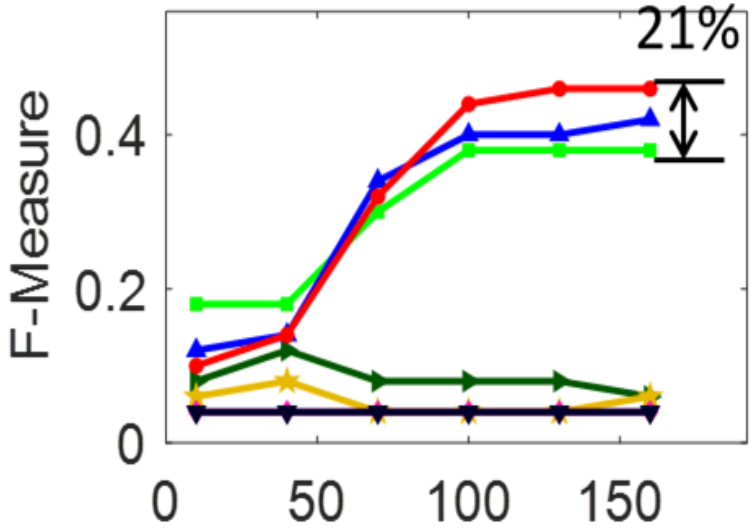
Case2383wp
(2383 buses)



Case2869pegase
(2869-buses)

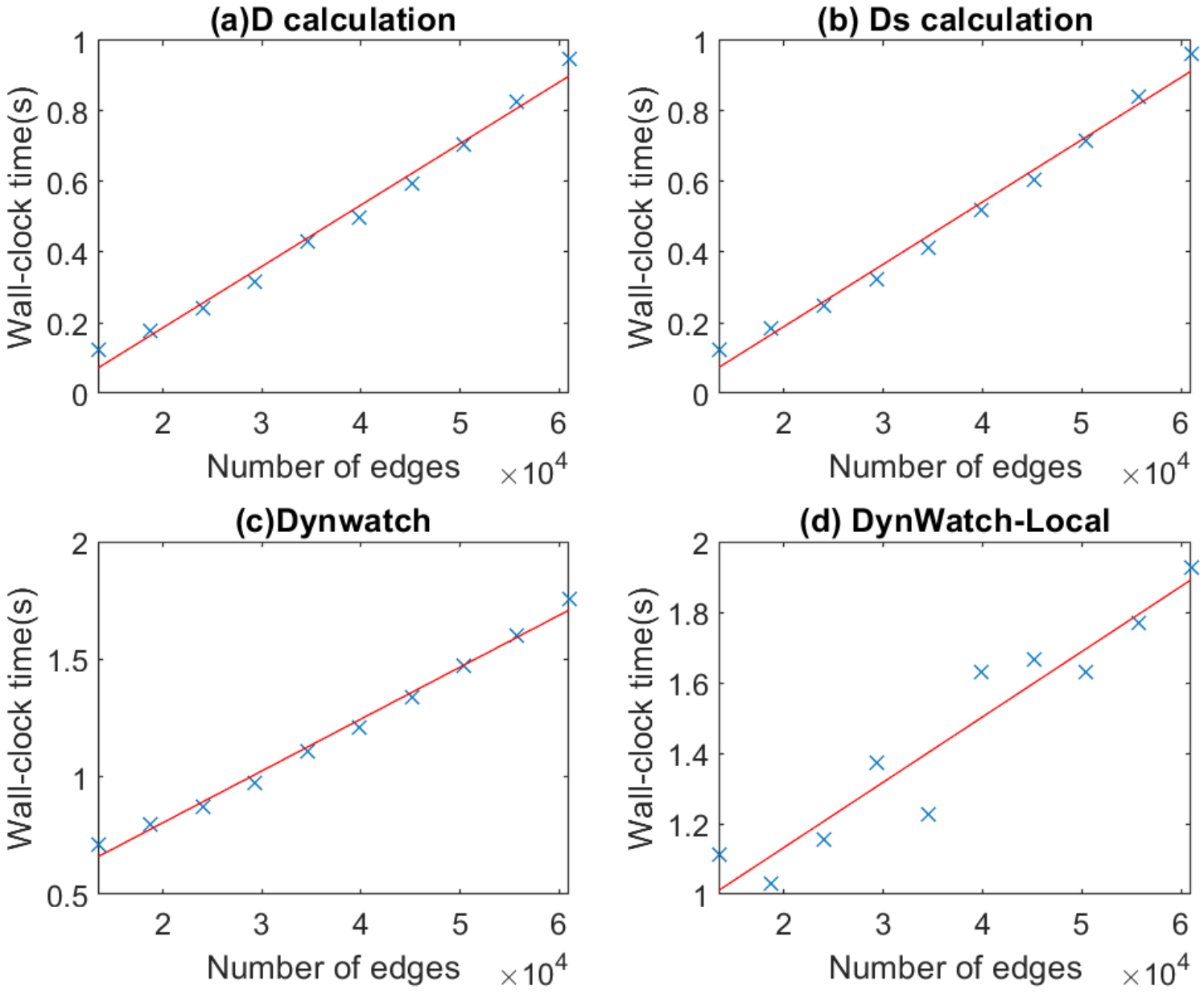


ActivSg25k
(25k buses)



DynWatch: scalable

- Method scales almost linearly.



Application 2: Spatial ML prediction

- Part 1 has advanced simulation robustness: unsolvable cases are made solvable and resilient.
- Remaining gap: large systems are slow to converge when good initial conditions are unavailable

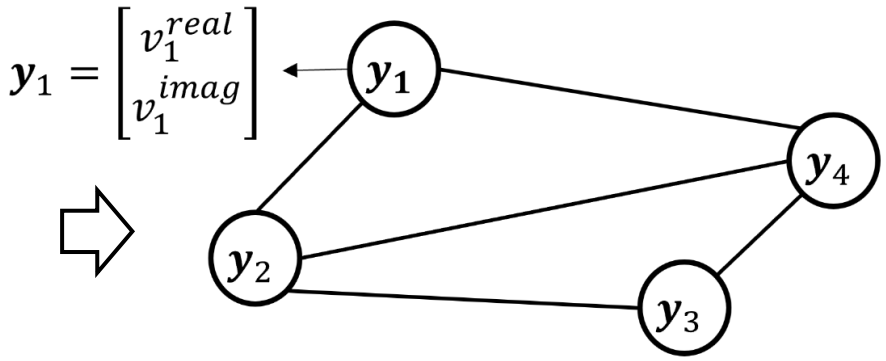
Physics-based simulation
Slow

Data-driven (ML)
Fast in predicting the impact of a what-if scenario

GridWarm: exploiting sparse graphical structure

Input $\boldsymbol{x}$:

- System info.
- Disturbance info.



Output y:

- State after disturbance

Pairwise Markov Random Field models the relationship on graph

$$P(\boldsymbol{y_1}, \ldots, \boldsymbol{y_N}|\boldsymbol{x}, \boldsymbol{\theta}) = \frac{1}{Z} \prod_{i=1}^{N} \Psi_i(\boldsymbol{y_i}; \boldsymbol{x}, \boldsymbol{\theta}) \prod_{(s,t)\in\mathcal{E}} \Psi_{(s,t)}(\boldsymbol{y_s}, \boldsymbol{y_t}; \boldsymbol{x}, \boldsymbol{\theta})$$

Parameters that maps x to y

Node potential

Edge potential

Sparse parameters to learn

Assuming Gaussian potentials:

Models & parameters to learn are sparse and location-specific

Node potential at node i:

$$\Psi_i(\boldsymbol{y_i}|\boldsymbol{x},\boldsymbol{\theta}) = \boldsymbol{e}^{-\frac{1}{2}\boldsymbol{y_i^T}\boldsymbol{\Lambda_i}\boldsymbol{y_i}+\boldsymbol{\eta_i^T}\boldsymbol{y_i}} \longrightarrow \textbf{Node-specific parameters: } \boldsymbol{\Lambda_i}, \boldsymbol{\eta_i}$$

Edge potential at edge (s,t) :

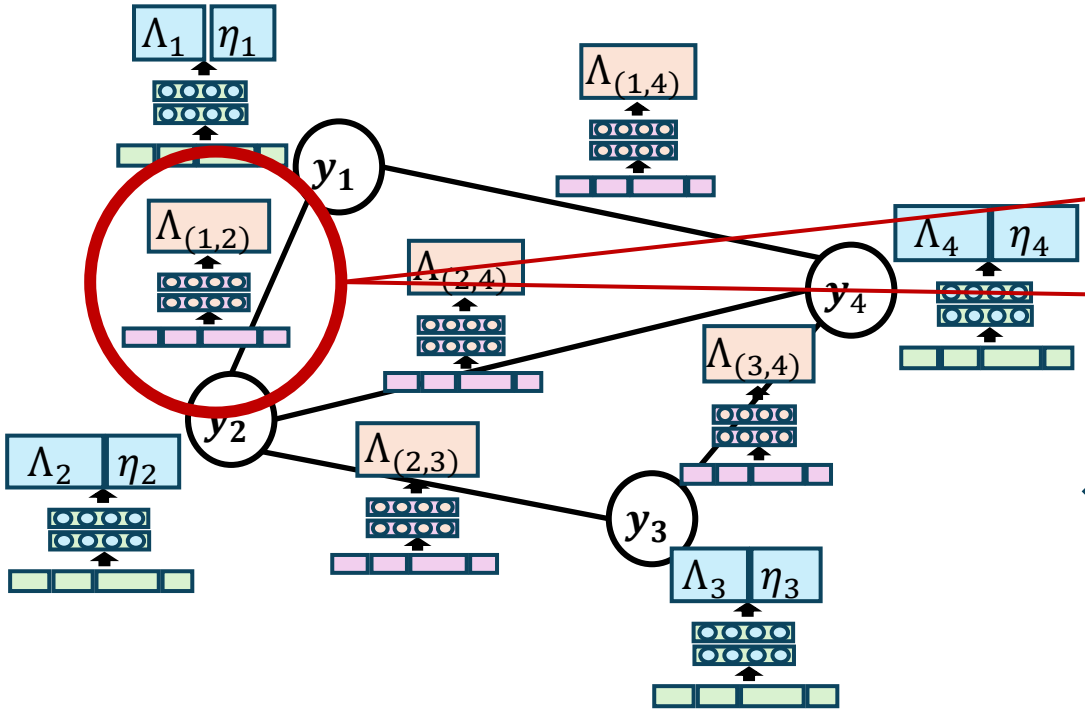
$$\Psi_{(s,t)}(\boldsymbol{y_s},\boldsymbol{y_t}|\boldsymbol{x},\boldsymbol{\theta}) = \boldsymbol{e}^{-\frac{1}{2}\boldsymbol{y_s^T}\boldsymbol{\Lambda_{(s,t)}}\boldsymbol{y_s}} \longrightarrow \textbf{Edge-specific parameters: } \boldsymbol{\Lambda_{(s,t)}}$$

Sparse graphical structure enables lightweight ML

Minimize log-likelihood loss to learn parameters

$$-\sum_{(x,y)\in Data} logP(y|x,\theta)$$

Forward ⇑ ⇓ Backpropagation

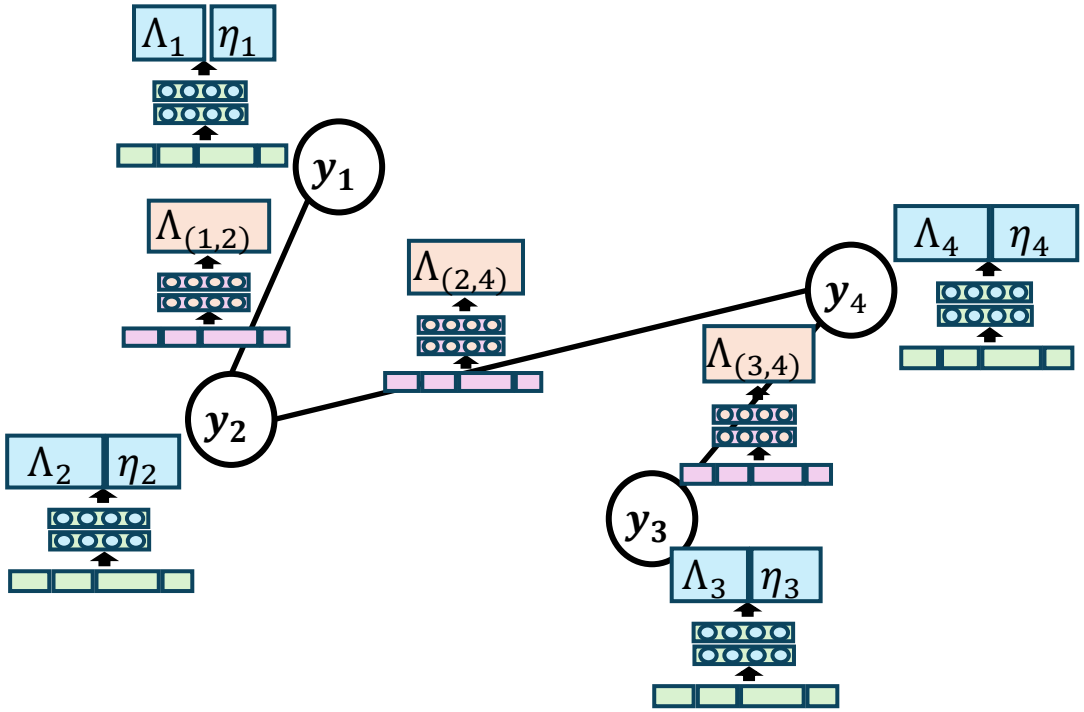


$$\Lambda = \begin{bmatrix} \Lambda_1 & \frac{1}{2}\Lambda_{(1,2)} & 0 & \frac{1}{2}\Lambda_{(1,4)} \\ \frac{1}{2}\Lambda_{(1,2)}^T & \Lambda_2 & \frac{1}{2}\Lambda_{2,3} & \frac{1}{2}\Lambda_{(2,4)} \\ 0 & \frac{1}{2}\Lambda_{(2,3)}^T & \Lambda_3 & \frac{1}{2}\Lambda_{(3,4)} \\ \frac{1}{2}\Lambda_{(1,4)}^T & \frac{1}{2}\Lambda_{(2,4)}^T & \frac{1}{2}\Lambda_{(3,4)}^T & \Lambda_4 \end{bmatrix}, \eta = \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \end{bmatrix}$$

Λ is a sparse matrix;

Local lightweight NNs to learn local Λ entries

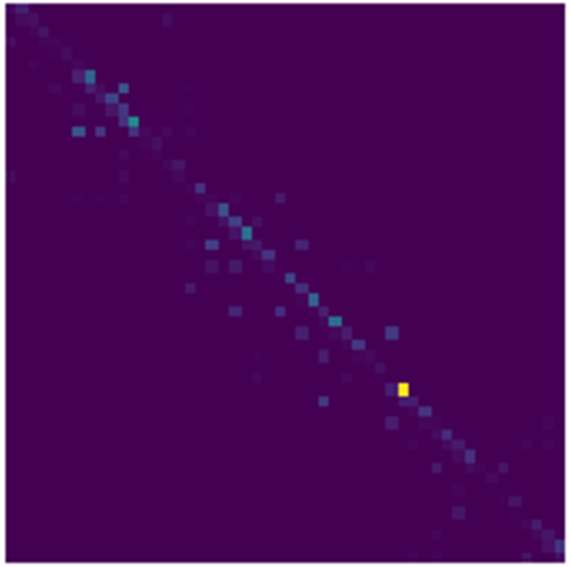
GridWarm: generalizable to different topologies



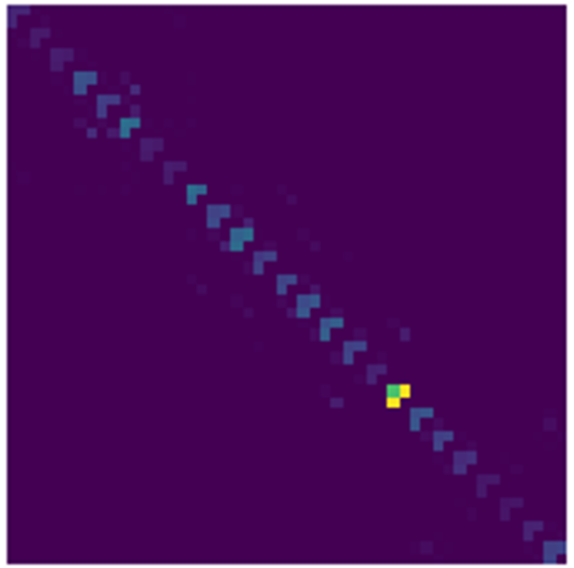
$$\boldsymbol{\Lambda} = \begin{bmatrix} \boldsymbol{\Lambda_1} & \frac{1}{2}\boldsymbol{\Lambda_{(1,2)}} & \boldsymbol{0} & \boldsymbol{0} \\ \frac{1}{2}\boldsymbol{\Lambda_{(1,2)}^T} & \boldsymbol{\Lambda_2} & \boldsymbol{0} & \frac{1}{2}\boldsymbol{\Lambda_{(2,4)}} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{\Lambda_3} & \frac{1}{2}\boldsymbol{\Lambda_{(3,4)}} \\ \boldsymbol{0} & \frac{1}{2}\boldsymbol{\Lambda_{(2,4)}^T} & \frac{1}{2}\boldsymbol{\Lambda_{(3,4)}^T} & \boldsymbol{\Lambda_4} \end{bmatrix}, \boldsymbol{\eta} = \begin{bmatrix} \boldsymbol{\eta_1} \\ \boldsymbol{\eta_2} \\ \boldsymbol{\eta_3} \\ \boldsymbol{\eta_4} \end{bmatrix}$$

GridWarm: interpretable with ML parameters structurally similar to true system physics

Y_{bus}



Λ



True linearized system:

$$Y_{bus}y = J$$

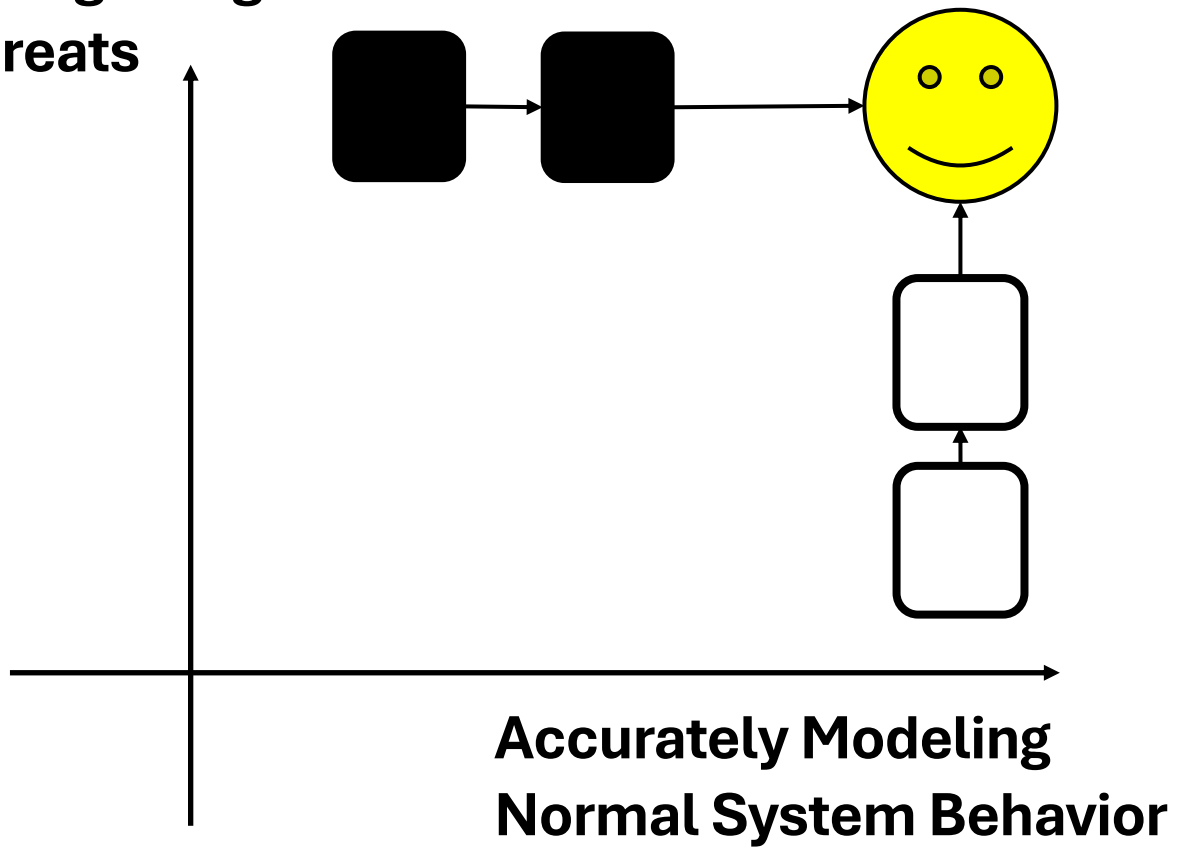
ML learns a linear proxy:

$$\Lambda\widehat{y_{test}} = \eta$$

Part 3: Physics-ML Synergy

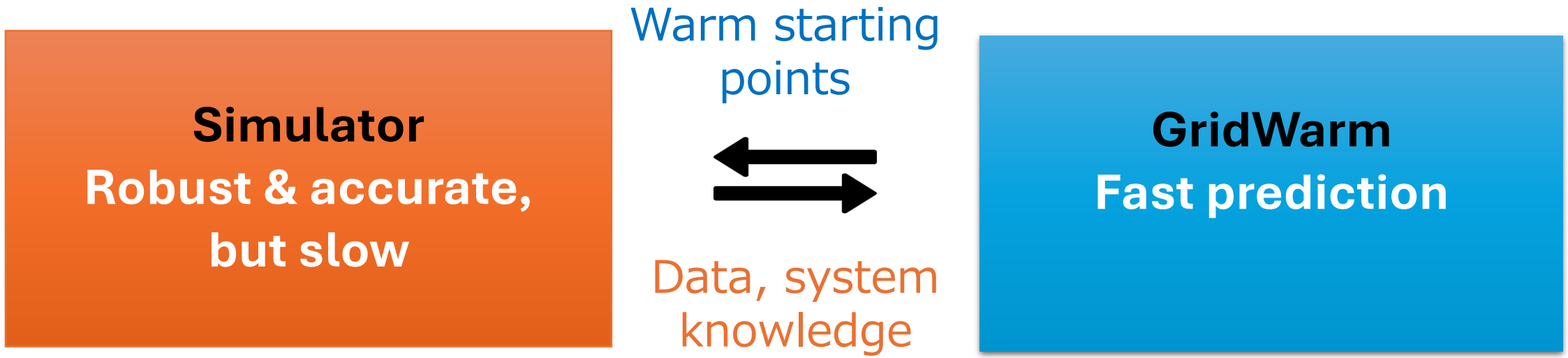
- Bringing efficiency & robustness further against cyberthreats

Physics-ML Synergy: More efficient & robust to modern cyberthreats

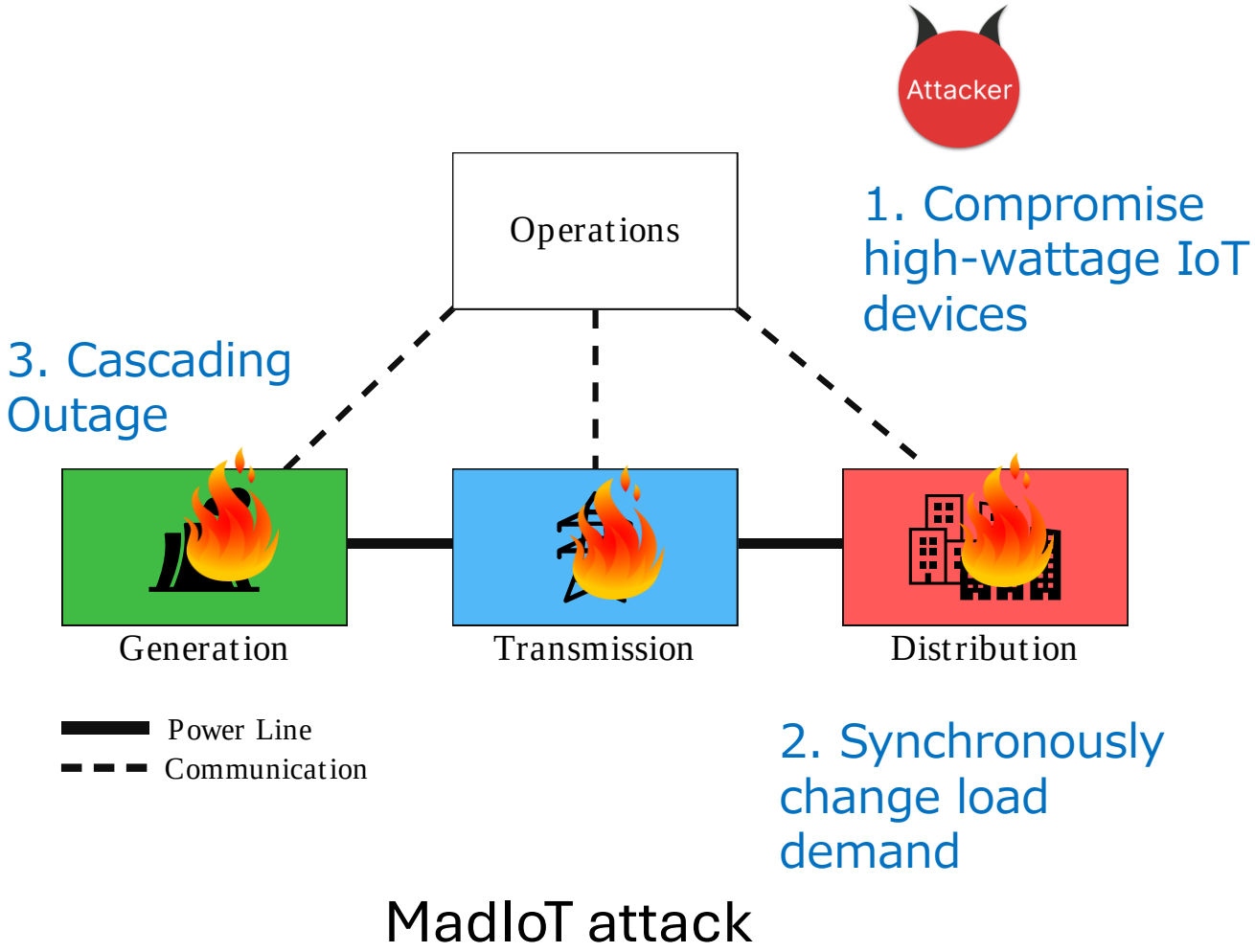


Application 1: Physics-ML Synergy for simulation

- Interconnection gives a ML-aided simulation.



Simulating MadIoT attack scenarios for cyber resiliency

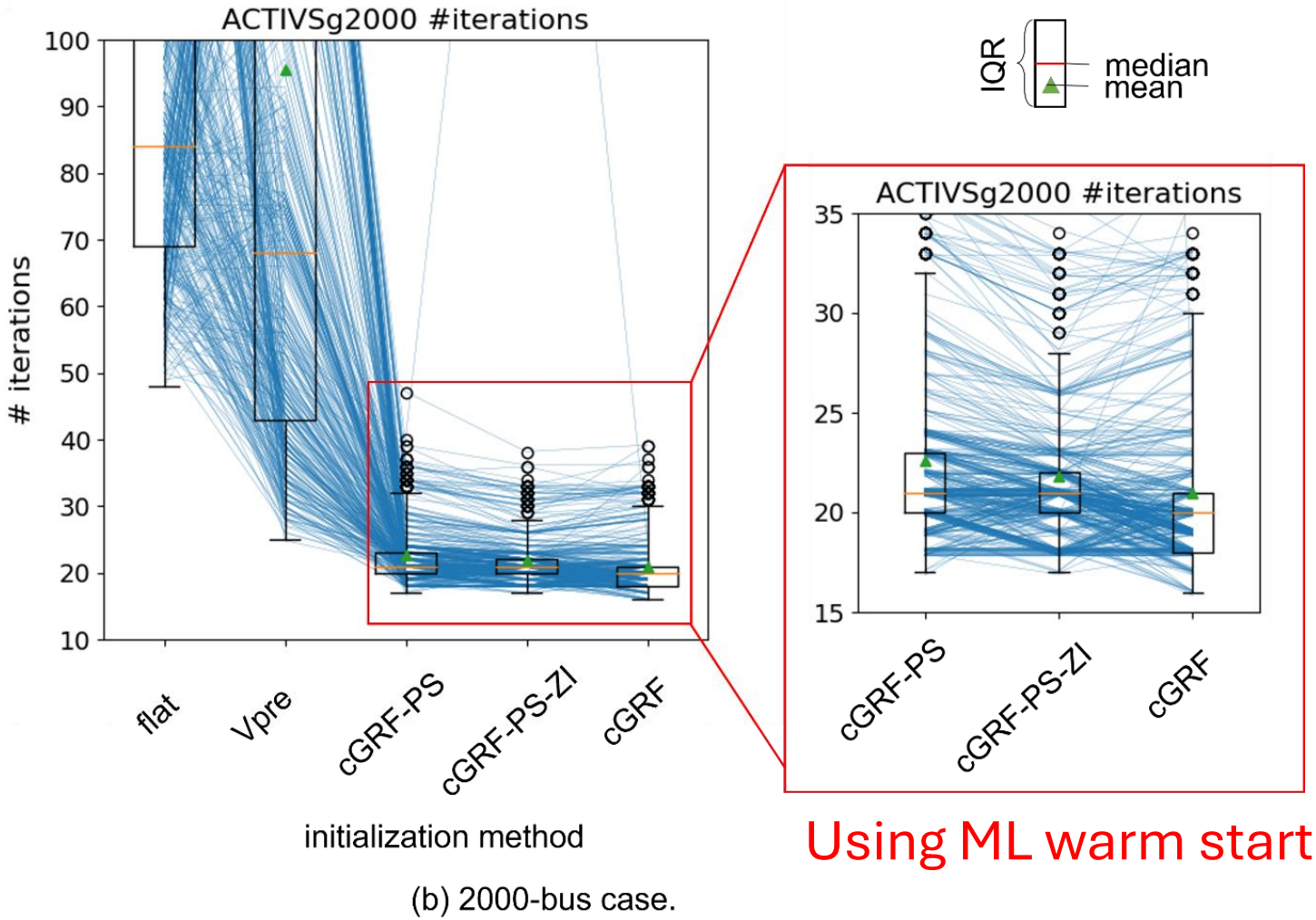


MadIoT attack

- Multiple-location disturbance.
- Causing significant impact
- A large amount of scenarios

Need fast simulation to evaluate them in real time.

ML-aided simulation: >3x faster for MadIoT on 2000-bus system



(b) 2000-bus case.

Using ML warm starter

Three variants of GridWarm with different domain knowledge

Domain Knowledge	cGRF	cGRF-PS	cGRF-ZI
Graph structure	Y	Y	Y
Parameter Sharing	N	Y	Y
Zero Injection Nodes	N	N	Y

Application 2: Physics-ML Synergy for estimation

- Interconnection by prior distributions gives ML-augmented estimation.

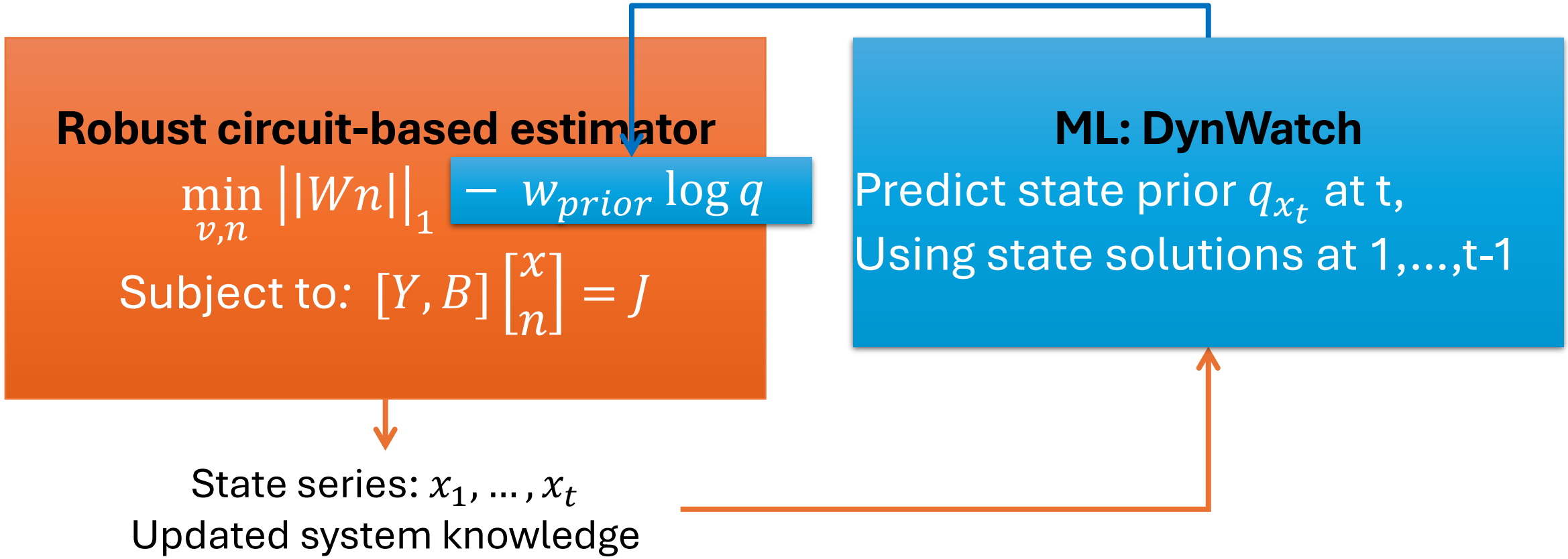
Estimator
Robust to random threats
But vulnerable to cyberattacks

Prior distributions

Data, system knowledge

DynWatch
Predict normal behavior and detect attack

Prior distribution in the form of regularization



Estimating with False Data Injection Attack (FDIA)

Experiment setting:

- Attackers mislead system operators into thinking the load demand decreases by 20%

$$\begin{bmatrix} |V_1| \\ P_1 \\ Q_1 \\ \vdots \\ |V_i| \\ \theta_i \\ |I_i| \\ \phi_i \\ \vdots \\ s_{i,j} \\ \vdots \end{bmatrix}$$

False data injection attack (FDIA)

$$\boldsymbol{\Delta z = H(V_{attacked}) - H(V_{true})}$$

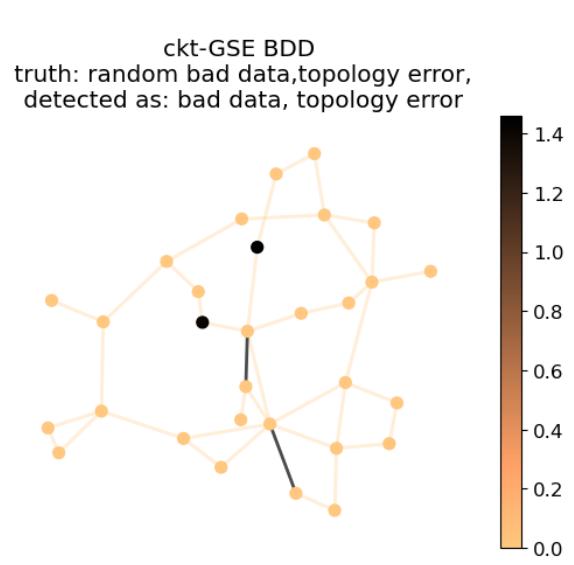
$$\begin{bmatrix} |V_1|' \\ P_1' \\ Q_1' \\ \vdots \\ |V_i|' \\ \theta_i' \\ |I_i|' \\ \phi_i' \\ \vdots \\ s_{i,j}' \\ \vdots \end{bmatrix}$$

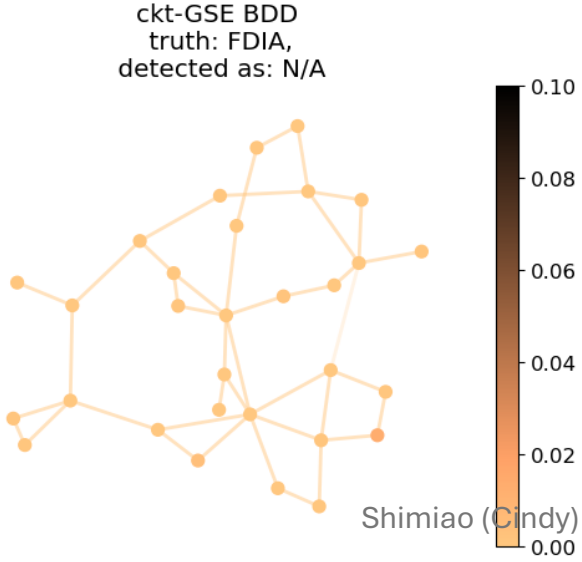
$$\boldsymbol{z = H(V_{true}) + n} \qquad \boldsymbol{z' = H(V_{attacked}) + n}$$

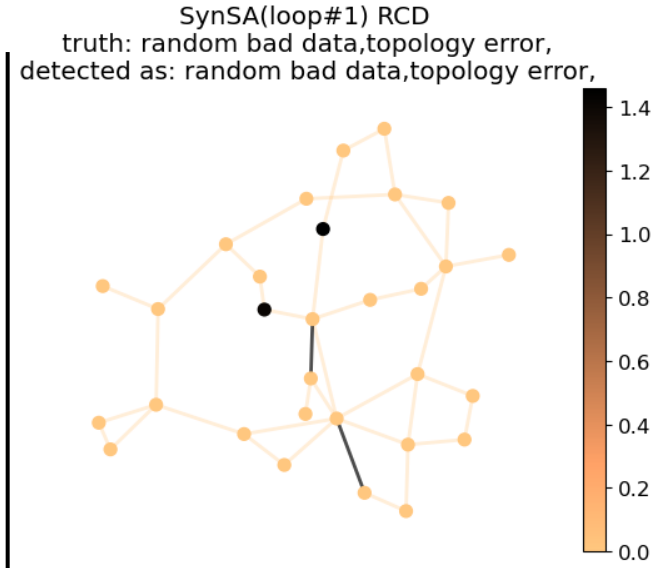
ML-augmented estimation: robust to FDIA cyberattack

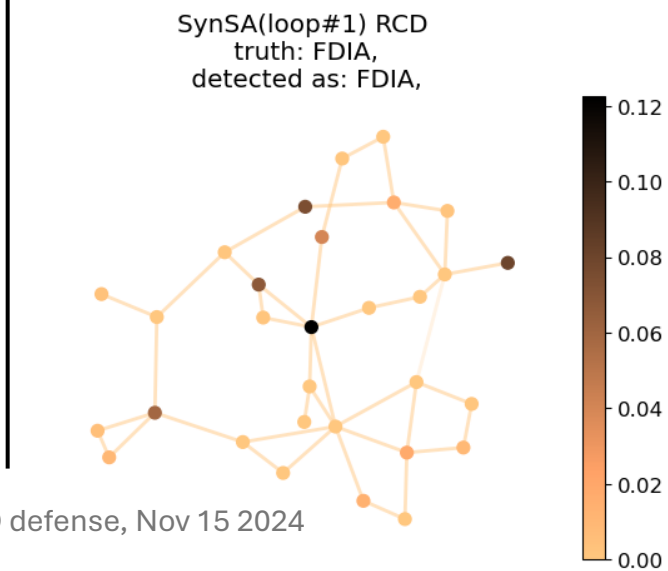
Circuit-based estimator
Can identify random threats

But not cyberattack







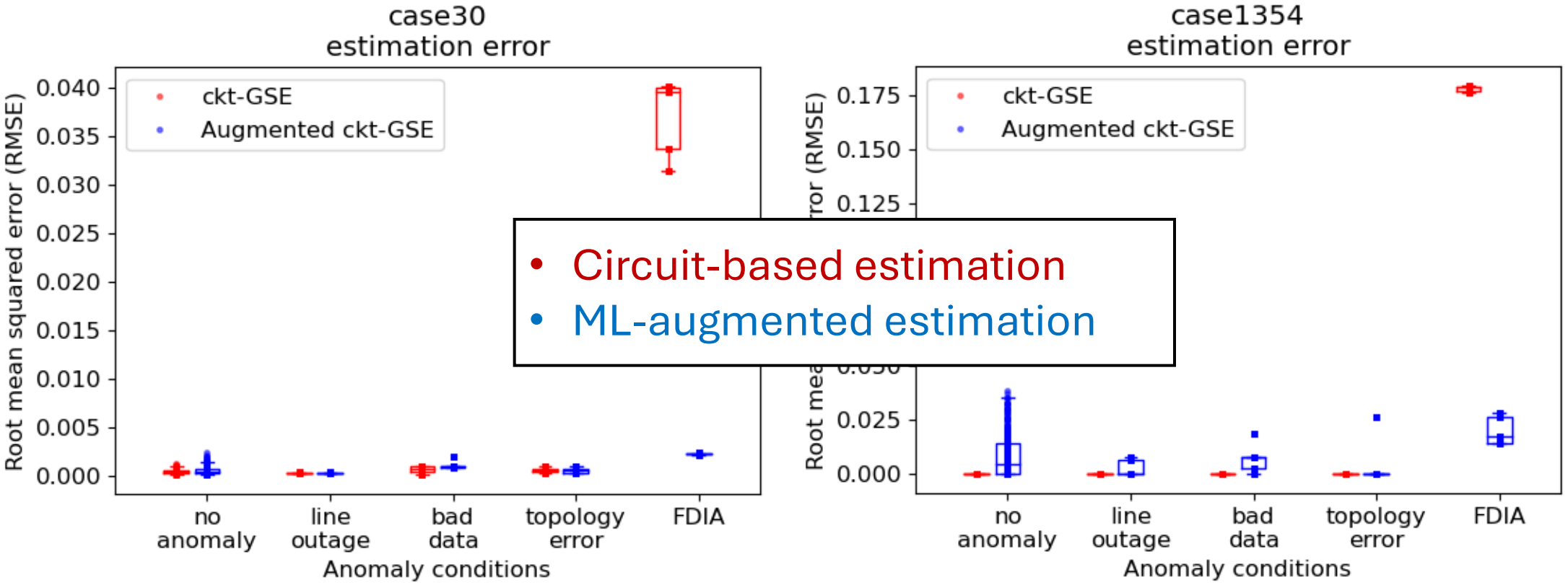


ML-augmented estimation
Can identify random threats

And also FDIA cyberattacks

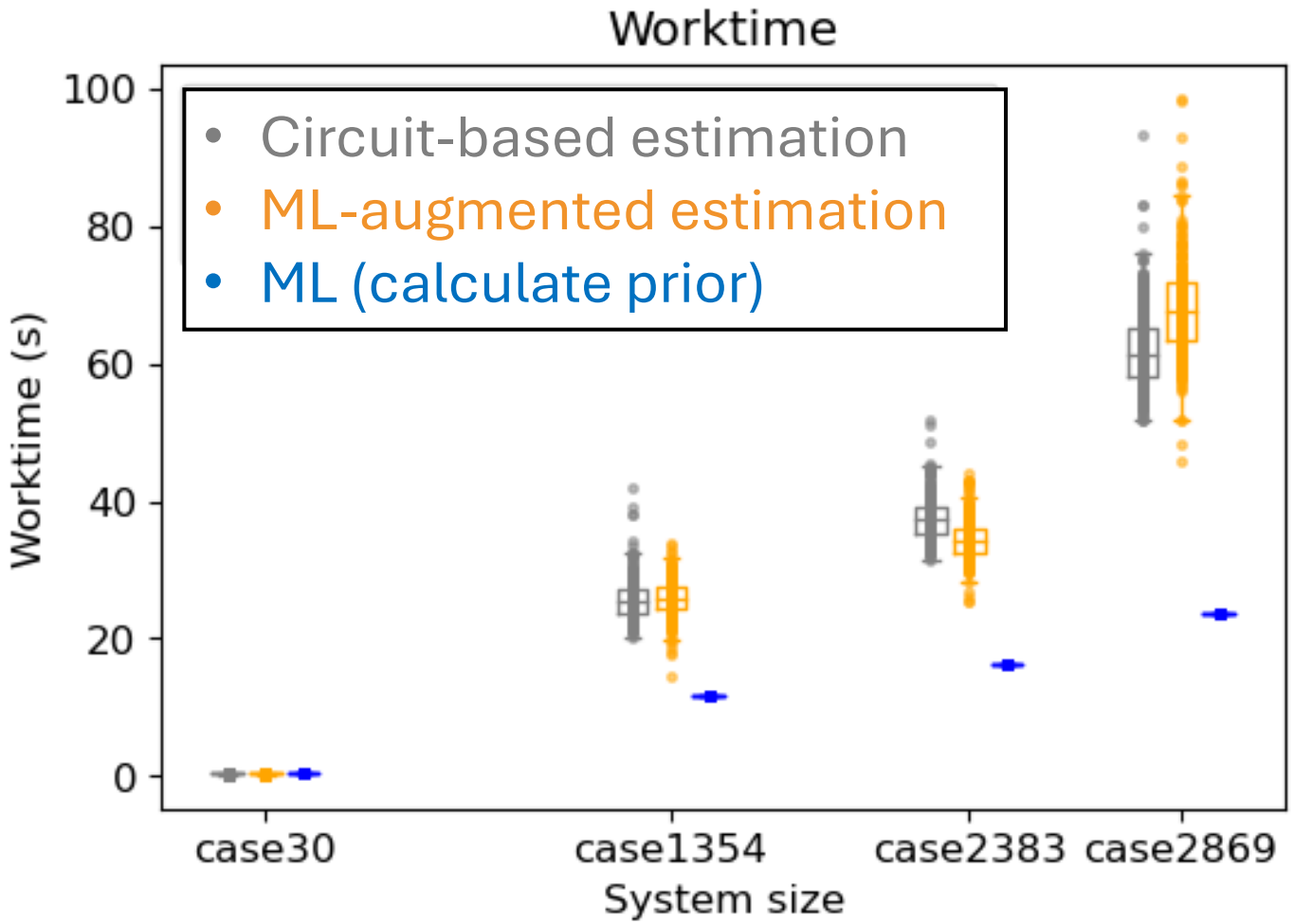
ML-augmented estimation: robust to FDIA cyberattack

- Minimize the intended damage of the FDIA attack



- Circuit-based estimation
- ML-augmented estimation

ML-augmented estimation: scalable



*System size = number of nodes + number of edges.

Conclusions

- **Grand Challenge Problem:** *Advance situational awareness to deal with natural and adversarial threats*
- **Limitations of status quo:** *Robustness and efficiency gaps*

- **My work: fill the robustness and efficiency gaps**
  - *Sparsity-exploiting optimizations advance physics-based & ML tools*
  - *Physics-ML Synergy merges the benefits of two worlds*

- **We see exciting opportunities in Physics-ML synergy**

Future works of Physics-ML Synergy

- Dealing with a broader range of modern threats.
- Leveraging ML to complement missing physics.
- Applying to broader range of analytical tools and other cyber-physical systems

Thanks!

- Thanks to all committee members: Prof. Larry Pileggi, Vyas Sekar, Soummya Kar, Bryan Hooi, Guannan Qu.

- Thanks to my amazing collaborators, colleagues, and friends!