Interdependent Causal Networks for Root Cause Localization

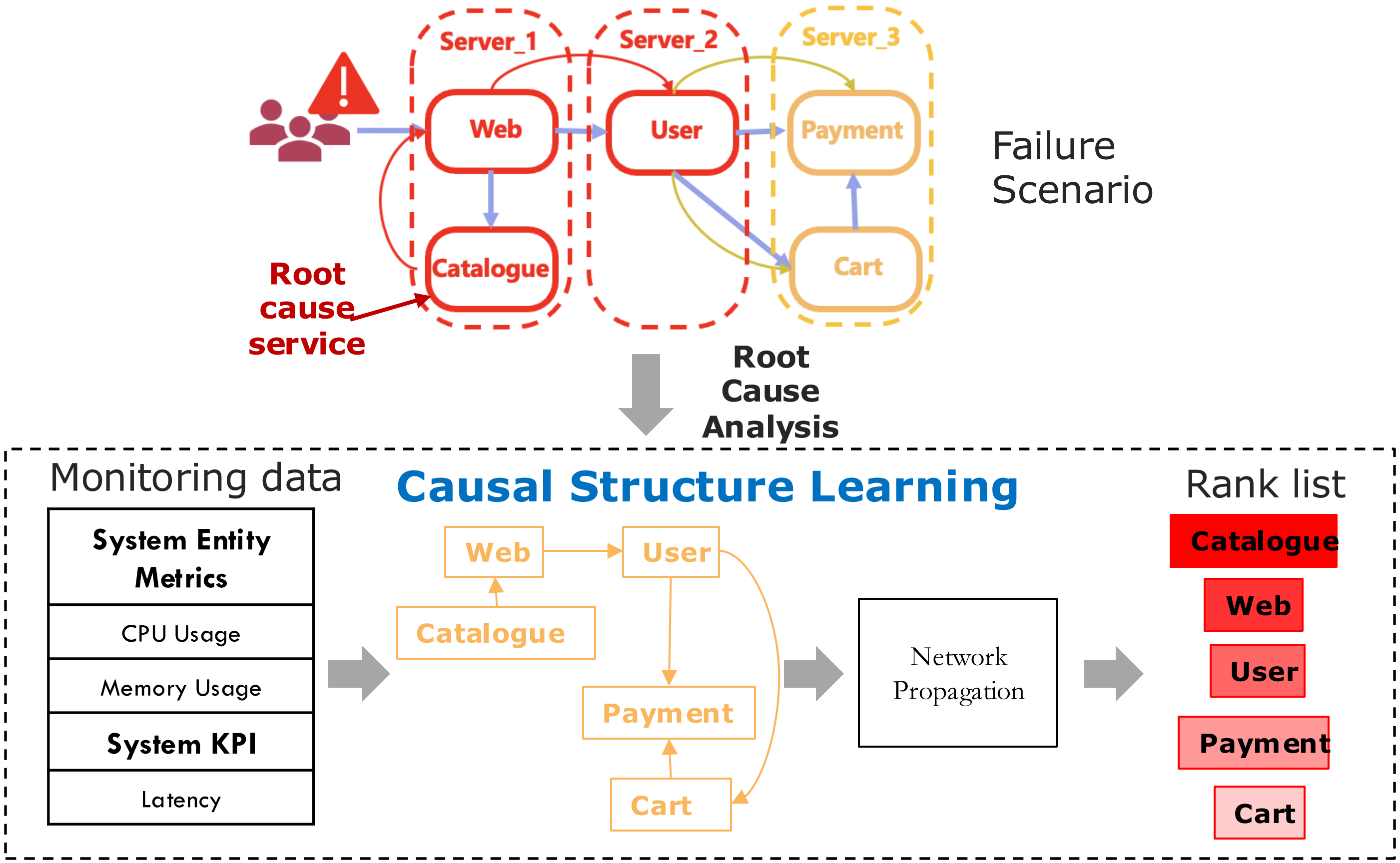
Dongjie Wang, Zhengzhang Chen, Jingchao Ni, Liang Tong, Zheng Wang, Yanjie Fu, Haifeng Chen

NEC Laboratories America

University of Central Florida 1963

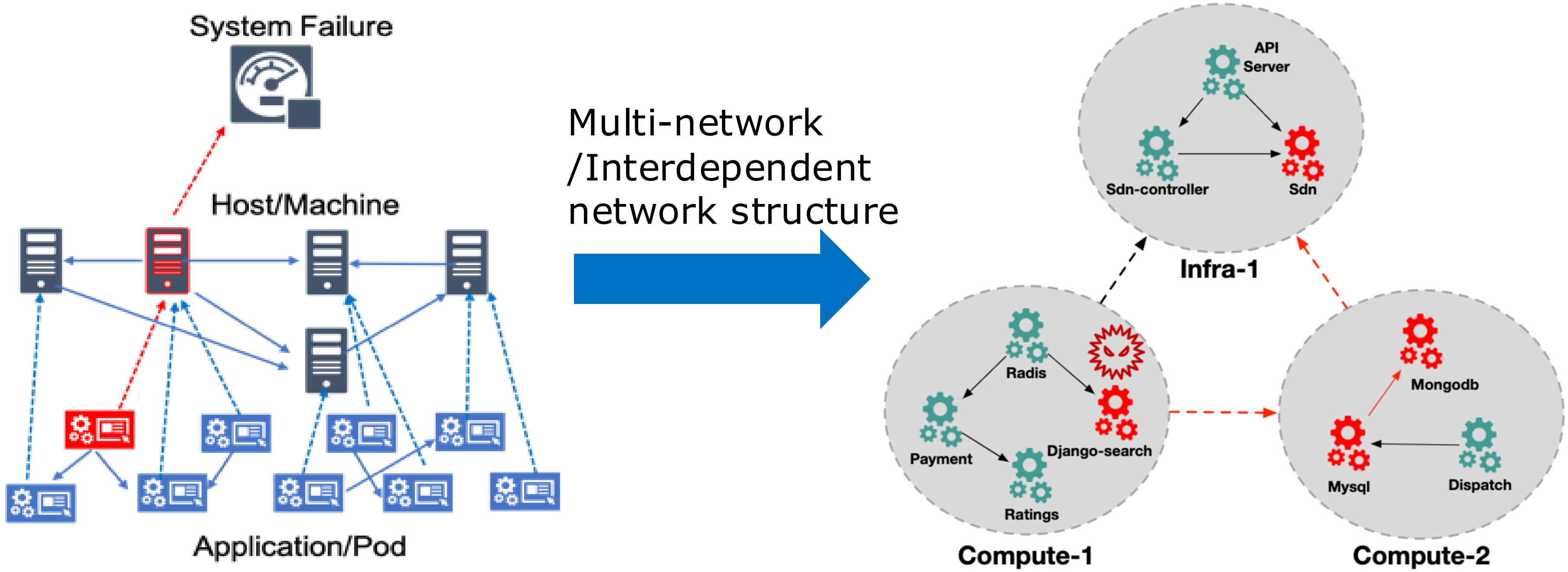
The University of Utah

Background: Root Cause Analysis



- Microservice Example
  - Input: System entity metrics and system KPI (i.e., multi-variate time series)
  - Output: Top-k possible root causes (i.e., malfunctional system entities)
- Effective **root cause analysis** (RCA) can greatly accelerate system failure recovery

Interdependent Networks



[1]: "Catastrophic cascade of failures in interdependent networks," **Nature**, vol. 464, no. 7291, pp. 1025–1028, 2010.

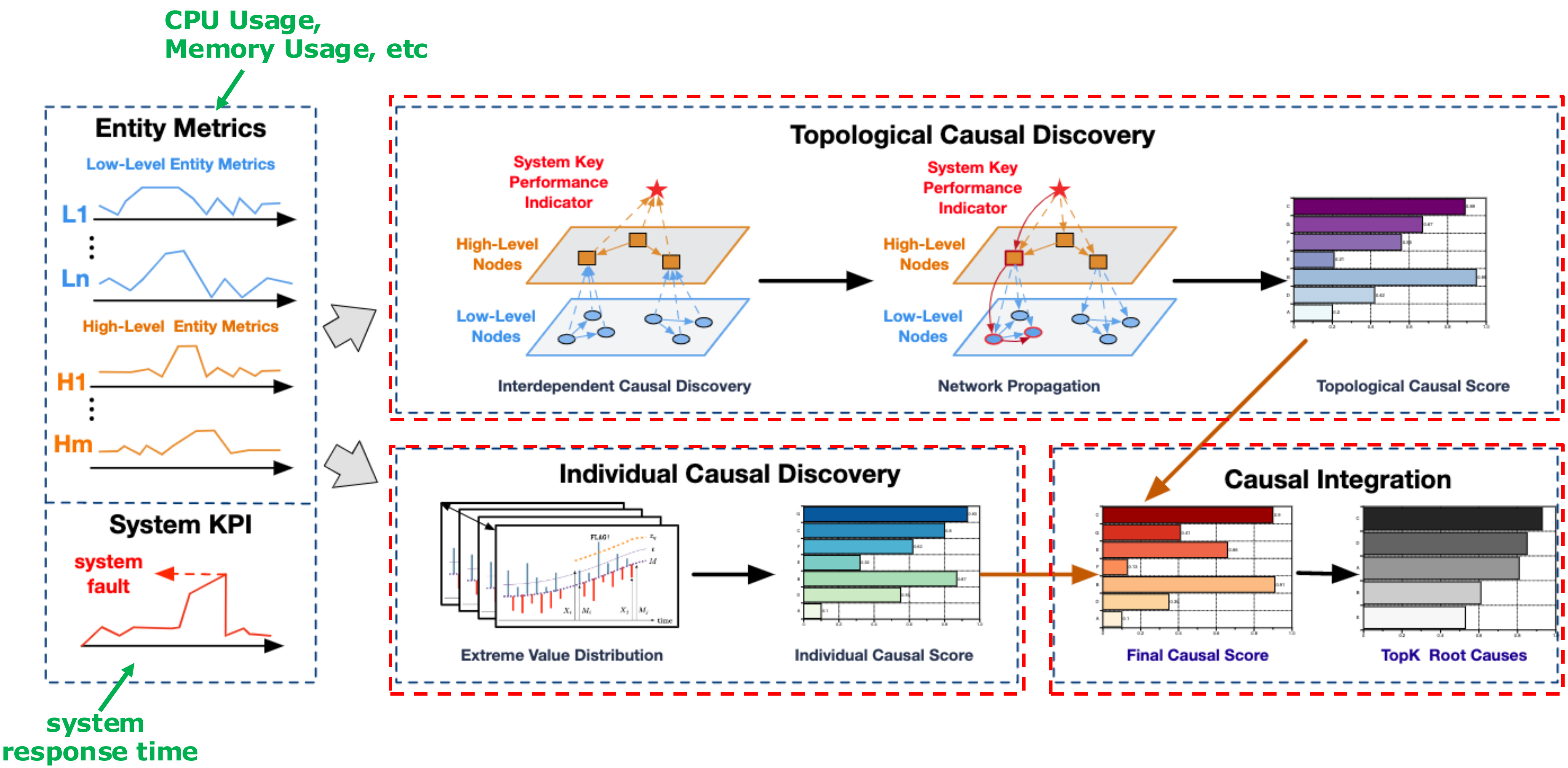
- Real-world systems are complex and exhibit **interdependent structures**
  - Multiple networks of a system are interconnected by cross-network links
- **Cascading failures**[1]: The malfunctioning patterns of problematic system entities can **propagate across different networks** or different levels of system entities

Research Challenges

How can we learn the **inter-level** and **intra-level** causal relationships from monitoring data for effectively capturing **cascading patterns**?

How can we accurately capture **abrupt change patterns** from the metrics data of an **individual system entity** for accurate RCA?

Proposed Framework REASON



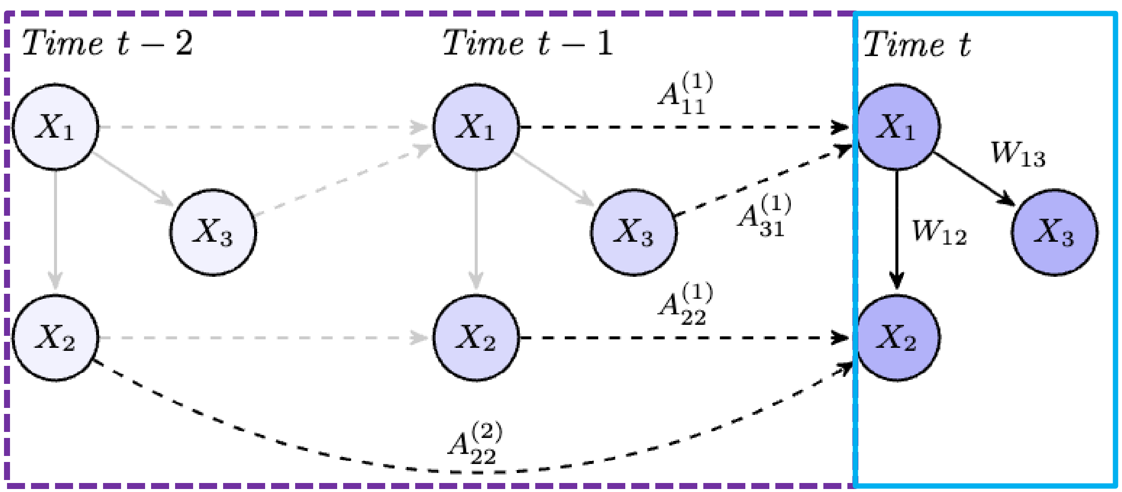
REASON consists of three major steps: **topological causal discovery, individual causal discovery, and causal integration.**

Structural Vector Autoregressive (SVAR)

- SVAR Equation

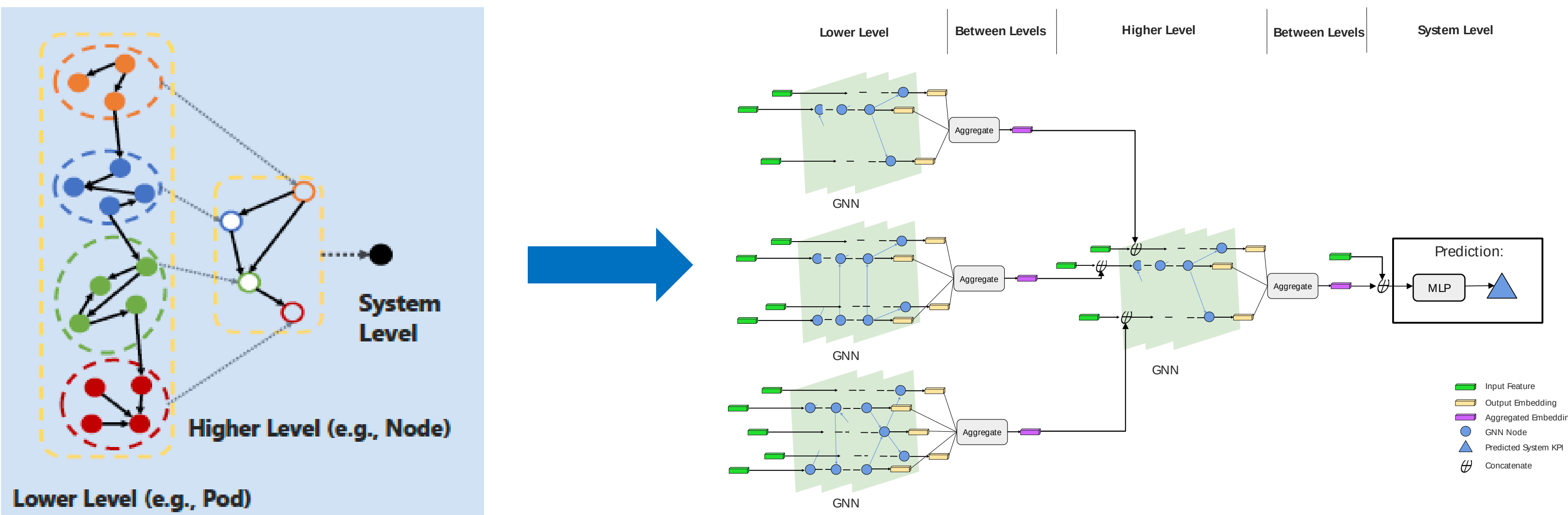
$$\mathbf{X} = \mathbf{X}\overbrace{\boxed{\mathbf{W}}}^{\text{Contemporaneous Causation}} + \mathbf{Y}\underbrace{\boxed{\mathbf{A}}}_{\text{Time-lagged Causation}} + \mathbf{Z}$$

Time-lagged Causation



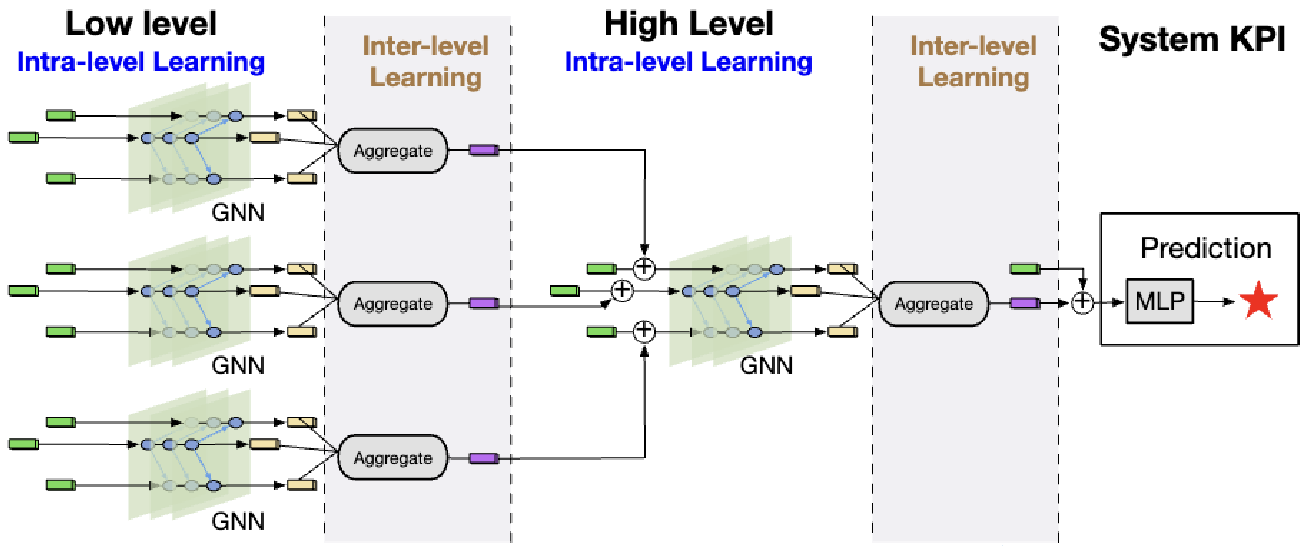
Contemporaneous Causation

Topological Causal Discovery



- **Topological causal learning in two levels**
  - **Intra-level Learning**
    - Captures causal relations within the same-level system entities
  - **Inter-level Learning**
    - Aggregates low-level information to high-level for constructing cross-level causal relations

Hierarchical Graph Neural Networks



Adjacency matrix elements, j->i

Activation function

Original input

Contributions to higher level

$$h_i^{(l+1)} = \mathrm{Act}\left(\underbrace{W_i^{(l)}\mathrm{Cat}\left(h_i^{(l)}, \sum_{j=1}^{n} \alpha_{ji}^{(l)} h_j^{(l)}\right)}_{\text{Concatenation Aggregation}}\right)$$

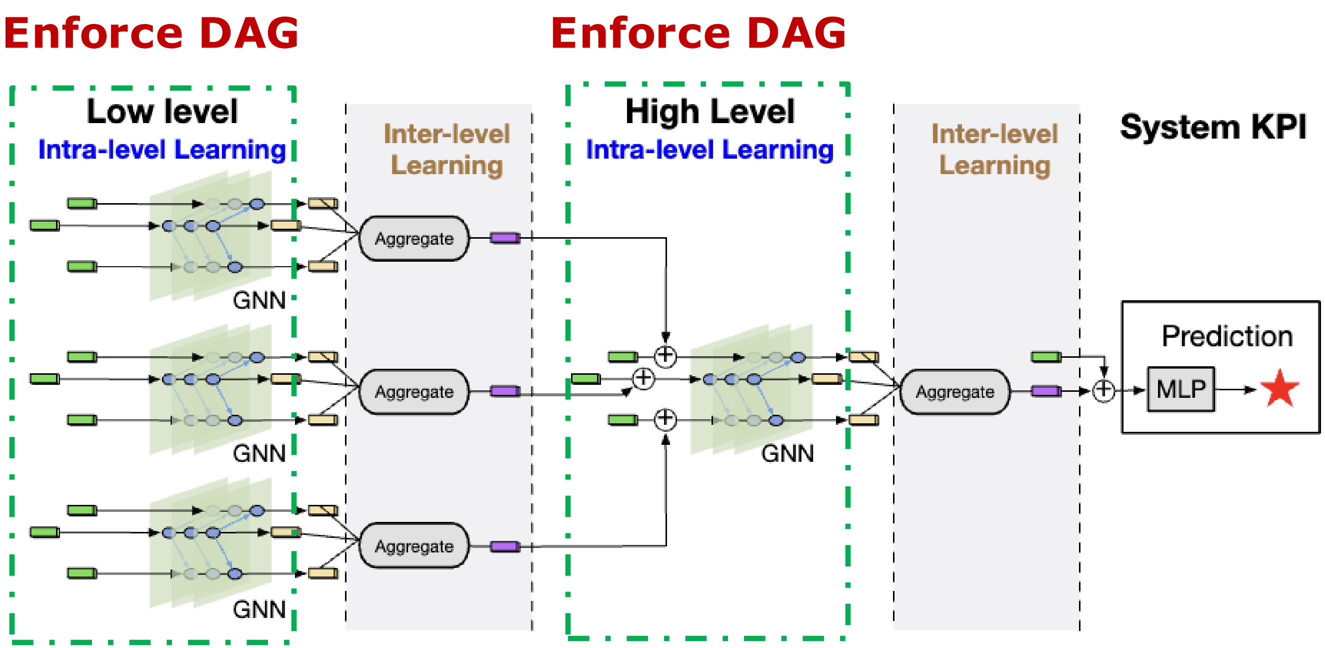
$$\hat{h}_i^{(0)} = \mathrm{Cat}\left(h_i^{(0)}, \sum_{m=1}^{M} \beta_m s_m^{(L)}\right)$$

Embedding in layer (l+1) for node i

Augmented input

Lower-level embeddings

Topological Causal Discovery



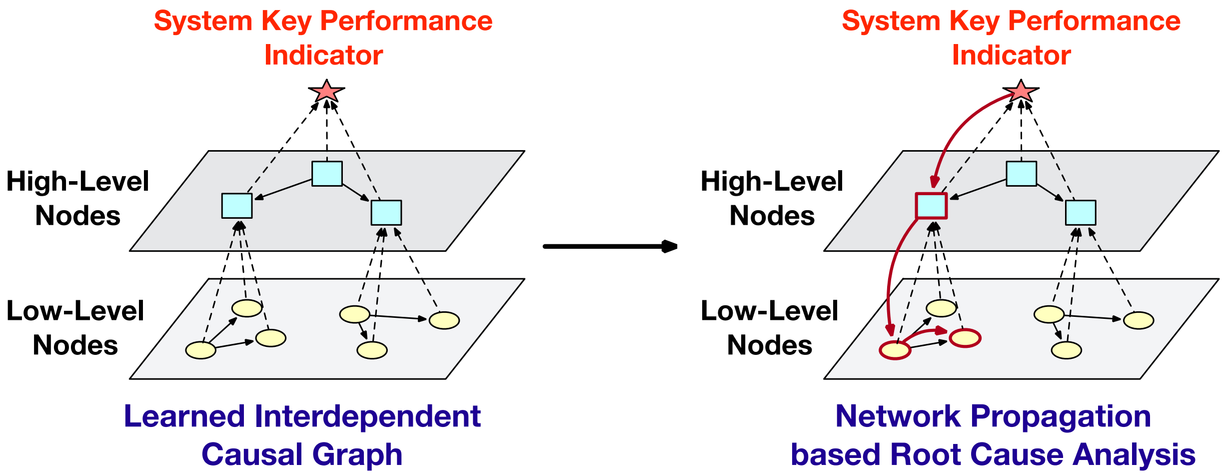
- **Learning Objectives**
  - Minimize the prediction error at each level

$$\mathcal{L} = \frac{1}{m}\sum_{t}(\mathbf{x}_t - \check{\mathbf{x}}_t)^2$$

  - Enforce the learned structure to be a DAG, (NOTEARS Constraint)

$$h(\mathbf{W}) = tr(e^{\mathbf{W}\circ\mathbf{W}}) - d = 0$$

Network Propagation based RCA



- **Network propagation-based root cause analysis**
  - The moving probability among nodes in the same level:

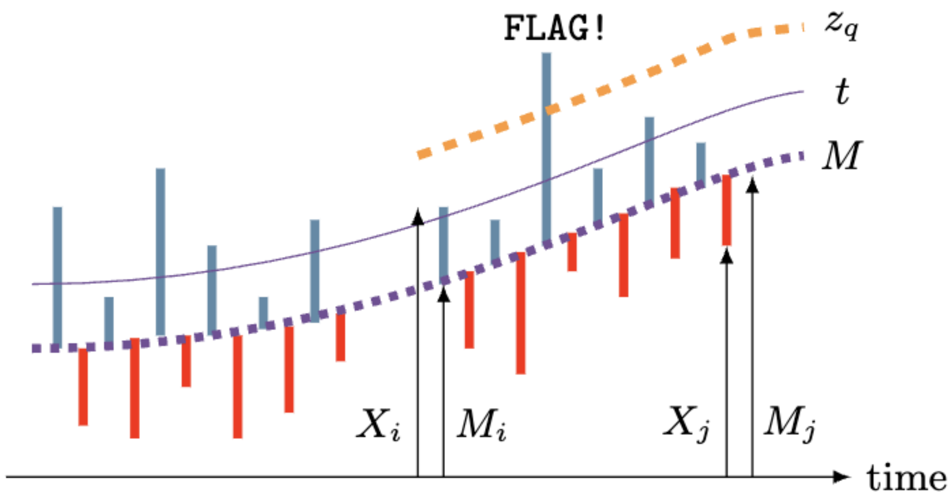
$$H_{\mathbf{GG}}(i,j) = (1-\Phi)\mathbf{G}^{\top}(i,j) / \sum_{k=1}^{g} \mathbf{G}^{\top}(i,k)$$

  - The moving probability among nodes across the level:

$$H_{\mathbf{G}\mathcal{A}}(i,b) = \Phi \mathbf{W}(i,b) / \sum_{k=1}^{gd} \mathbf{W}(i,k)$$

  - When the visiting probability distribution converges, the nodes' probability scores serve as their causal scores for ranking.

Individual Causal Discovery



- **Individual causal learning via Extreme Value Theory**
  - t is the probability threshold for the peak value, which typically set at 98%.
  - z_q is the threshold for the real anomaly case, which is determined by the extreme value distribution.
  - As the increase of time points, the time window will move and the corresponding value of t and z_q will be updated as well.

Evaluation

Baselines

- PC
  - is a classic constraint-based method, which first decides skeleton, then directions.
- C-LSTM
  - captures the nonlinear Granger causality by using LSTM neural networks.
- Dynotears
  - is a score-based method that uses SVAR to construct dynamic Bayesian networks.
- GOLEM
  - employs a likelihood-based score function to relax hard DAG constraints in NOTEARS..
- GNN
  - the model variant of REASON, which only captures the low-level causal relations.
- REASON-I
  - the model variant of REASON, which removes the individual part.
- REASON-T
  - the model variant of REASON, which removes the topological part.

Datasets

- Swat
  - 6 high-level nodes, 51 low-level nodes, 16 faults
- WADI
  - 3 high-level nodes, 23 low-level nodes, 15 faults
- AIOps
  - 5 high-level nodes, 234 low-level nodes, 5 faults

Evaluation Metrics

$$\text{PR@K} = \frac{1}{|\mathbb{A}|} \sum_{a \in \mathbb{A}} \frac{\sum_{i<K} R_a(i) \in V_a}{min(K, |V_a|)},$$

$$\text{MAP@K} = \frac{1}{K|\mathbb{A}|} \sum_{a \in \mathbb{A}} \sum_{1 \le j \le K} \text{PR@j},$$

$$\text{MRR} = \frac{1}{\mathbb{A}} \sum_{a \in \mathbb{A}} \frac{1}{rank_{R_a}},$$

Experimental Results

Table 1: Overall performance *w.r.t.* SWaT dataset.

	PR@1	PR@3	PR@5	PR@7	PR@10	MAP@3	MAP@5	MAP@7	MAP@10	MRR
REASON	**25.0%**	**28.13%**	**66.67%**	**76.04%**	**84.38%**	**23.96%**	**35.0%**	**46.73%**	**57.60%**	**40.99%**
GNN	18.75%	19.79%	43.75%	52.08%	62.50%	18.06%	27.92%	33.63%	41.88%	34.77%
PC	12.5%	13.54%	34.38%	47.92%	58.33%	12.85%	20.42%	26.64%	35.0%	26.16%
C-LSTM	12.5%	13.54%	28.13%	40.63%	52.08%	13.89%	17.71%	23.81%	31.88%	29.35%
Dynotears	12.5%	29.17%	32.29%	34.38%	42.71%	20.14%	24.38%	26.93%	30.83%	27.85%
GOLEM	6.25%	7.29%	12.5%	39.58%	47.92%	7.64%	9.58%	16.96%	25.0%	22.36%

Table 2: Overall performance *w.r.t.* WADI dataset.

	PR@1	PR@3	PR@5	PR@7	PR@10	MAP@3	MAP@5	MAP@7	MAP@10	MRR
REASON	**28.57%**	**59.52%**	**65.0%**	**76.19%**	**79.76%**	**42.46%**	**50.62%**	**57.41%**	**63.76%**	**53.35%**
GNN	14.28%	26.19%	34.28%	42.86%	54.76%	21.83%	25.31%	30.15%	37.54%	32.71%
PC	7.14%	27.38%	35.0%	44.05%	50.0%	16.27%	23.90%	28.47%	34.57%	27.74%
C-LSTM	0%	20.24%	35.0%	47.62%	51.19%	11.51%	18.55%	25.83%	32.73%	24.40%
Dynotears	7.14%	14.29%	30.00%	29.76%	47.62%	10.71%	17.43%	20.95%	26.81%	22.23%
GOLEM	0%	19.05%	40.0%	46.43%	53.57%	9.92%	20.38%	27.82%	34.83%	23.48%

Table 3: Overall performance *w.r.t.* AIOps dataset.

	PR@1	PR@3	PR@5	PR@7	PR@10	MAP@3	MAP@5	MAP@7	MAP@10	MRR
REASON	**80.0%**	**80.0%**	**100.0%**	**100.0%**	**100.0%**	**80.0%**	**84.0%**	**88.57%**	**92.0%**	**84.0%**
GNN	20.0%	40.0%	40.0%	40.0%	60.0%	26.67%	32.0%	34.29%	38.0%	30.65%
PC	0%	20.0%	20.0%	40.0%	40.0%	13.33%	16.0%	22.86%	28.0%	14.0%
C-LSTM	0%	20.0%	20.0%	20.0%	20.0%	13.33%	16.0%	17.14%	18.0%	10.82%
Dynotears	20.0%	40.0%	40.0%	40.0%	40.0%	33.33%	36.0%	37.14%	38.0%	30.79%
GOLEM	20.0%	40.0%	40.0%	40.0%	40.0%	33.33%	36.0%	37.14%	38.0%	31.22%

The Impact of Network Propagation

Table 4: The influence of network propagation in terms of MAP@10

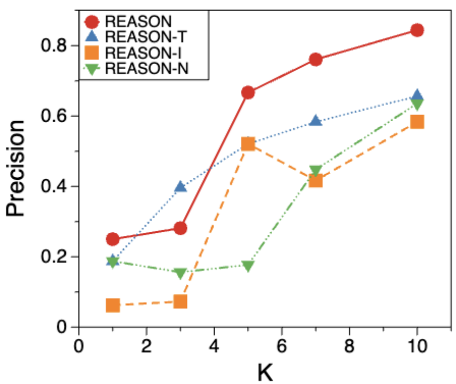
	PC		GLOEM		Dynotears		C-LSTM		GNN	
	Original	Propagate	Original	Propagate	Original	Propagate	Original	Propagate	Original	Propagate
SWaT	35.0%	**37.39%**	25.0%	**33.44%**	30.83%	**37.08%**	31.87%	**34.16%**	41.87%	**49.16%**
WADI	34.57%	**35.71%**	34.83%	**38.05%**	26.81%	**33.76%**	32.72%	**42.61%**	37.53%	**45.98%**
AIOPS	28.0%	**30.0%**	38.0%	**54.0%**	38.0%	**58.0%**	18.0%	**48.0%**	38.0%	**60.0%**

Table 5: The influence of network propagation in terms of MRR

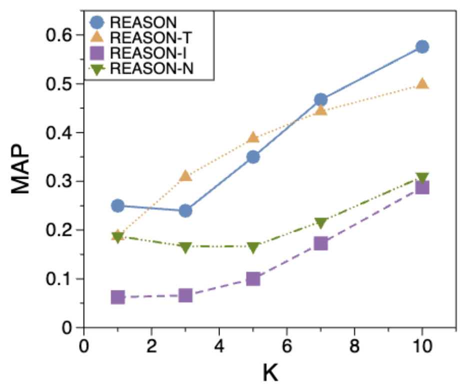
	PC		GLOEM		Dynotears		C-LSTM		GNN	
	Original	Propagate	Original	Propagate	Original	Propagate	Original	Propagate	Original	Propagate
SWaT	26.16%	**32.27%**	22.36%	**30.42%**	27.85%	**33.98%**	29.35%	**32.85%**	34.77%	**40.43%**
WADI	27.74%	**30.74%**	23.48%	**25.89%**	22.22%	**34.28%**	24.39%	**33.27%**	32.71%	**36.40%**
AIOPS	14.0%	**25.35%**	31.22%	**37.74%**	30.79%	**50.77%**	10.82%	**24.73%**	30.65%	**62.48%**

- Network propagation can **significantly improve the performance** of root cause localization.
- The reason for the improvement is that the network propagation **captures the propagated patterns** of system failures among different system entities.

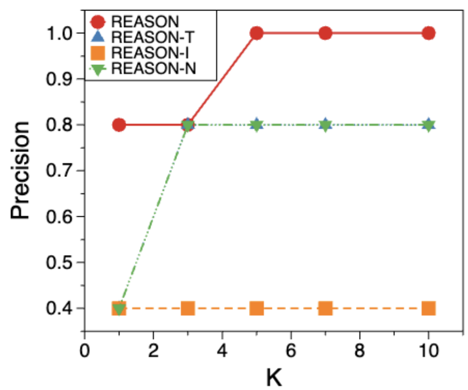
Ablation Studies for REASON



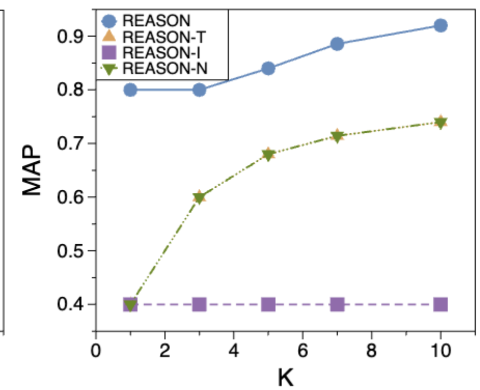
(a) Precision@K for SWaT



(b) MAP@K for SWaT



(c) Precision@K for AIOps



(d) MAP@K for AIOps

- **Definitions**
  - REASON-T, which solely keeps the topological causal discovery.
  - REASON-I, which only keeps the individual causal discovery.
  - REASON-N, which removes the inter-level learning in topological causal discovery while keeping the intra-level learning of low-level system entities, network propagation and individual causal discovery.

The integration of topological causal discovery and individual causal discovery is important for keeping a good RCA performance.

The inter-level learning component will help learn robust causation among high-level nodes by integrating the causal information in the low-level nodes.

Conclusion and Future Work

- **Conclusion**
  - We propose an offline RCA framework by learning **interdependent causation** among system entities.
  - **Network Propagation** based method can capture the propagated patterns of system failures for accurate RCA.
  - **Capturing both topological and individual causal pattern** are helpful to maintain a good RCA performance.
  - The proposed framework has been deployed in **real industrial systems** and plays an important role in keeping security.
- **Future Work**
  - We will extend our framework to online setting for quickly and efficiently locating root causes of system failures.

Thanks for Listening!