Towards application of network topology information to network causal log analysis

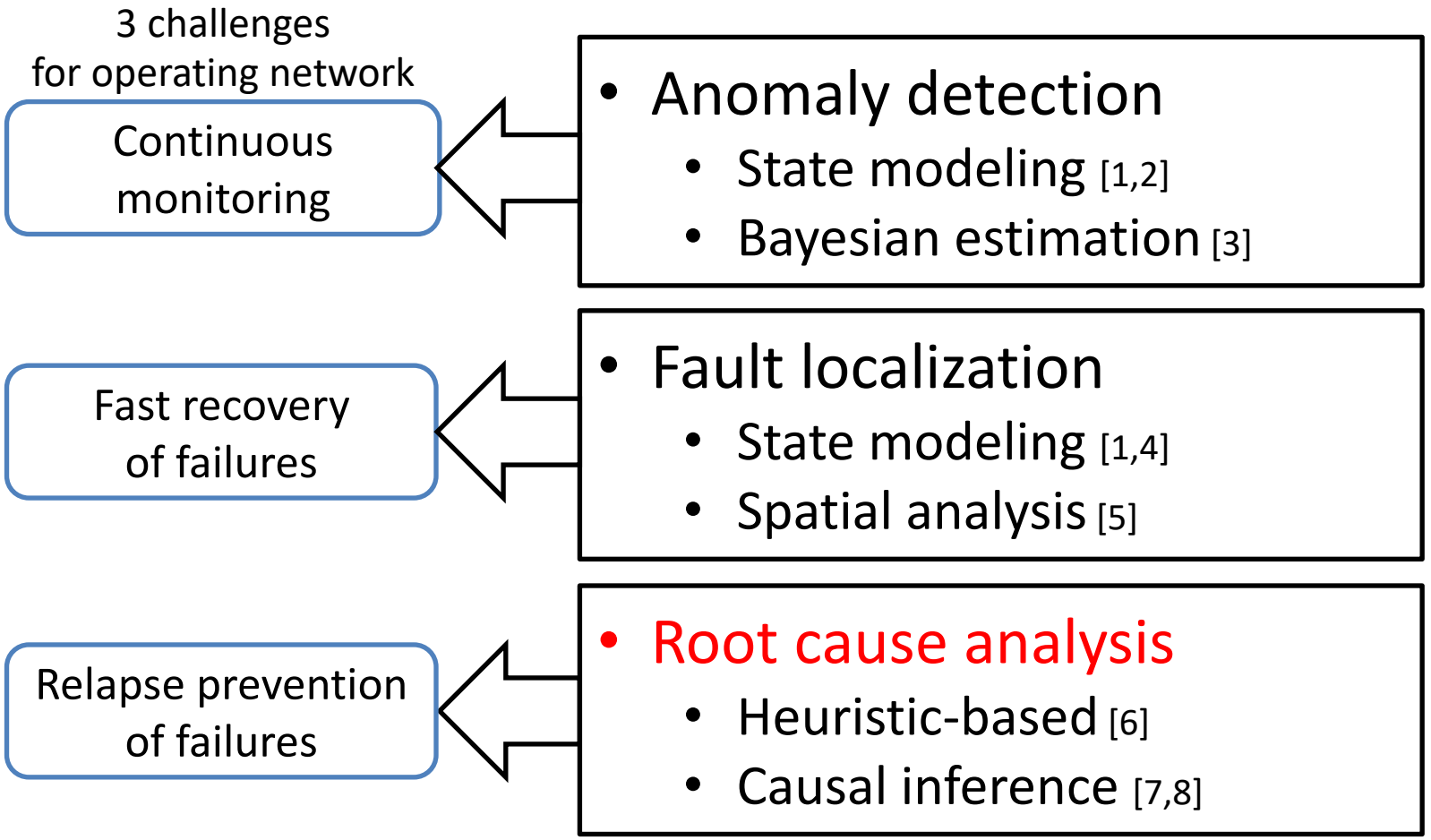
National Institute of Informatics
Project Researcher
Satoru Kobayashi
Dec 13, 2018

Difficulty of leveraging system log

- Huge dataset
  - Large scale and complicated systems
  - 150,000 lines / day in SINET 5
  - Automated analysis required

- Difficult to analyze automatically
  - Free-format
  - Mixture of frequent and sparse logs
  - Lengthy / Repeated data

Automated analysis of system log



[1] K. Yamanishi et al. "Dynamic syslog mining for network failure monitoring". In ACM KDD'05, p. 499, 2005.
[2] F. Salfner et al. "Using hidden semi-Markov models for effective online failure prediction". In IEEE SRDS, pp. 161–174, 2007.
[3] P. Chen et al. "Causeinfer: Automatic and distributed performance diagnosis with hierarchical causality graph in large distributed systems". In IEEE INFOCOM, pp. 1887–1895, 2014.
[4] I. Beschastnikh, et al. "Inferring Models of Concurrent Systems from Logs of Their Behavior with CSight." In ICSE 2014, 468-479, 2014.
[5] T. Kimura et al. "Spatio-temporal factorization of log data for understanding network events". In IEEE INFOCOM, pp. 610–618, 2014.

Causal analysis of system log

- Graph-based causal inference [9]
  - PC algorithm: causal structure estimation
  - Exploratory analysis in contrast to existing approaches [7, 8]
- Challenges
  - Processing time
  - Reliability of detected information

➢ Improve causal analysis based on topology knowledge

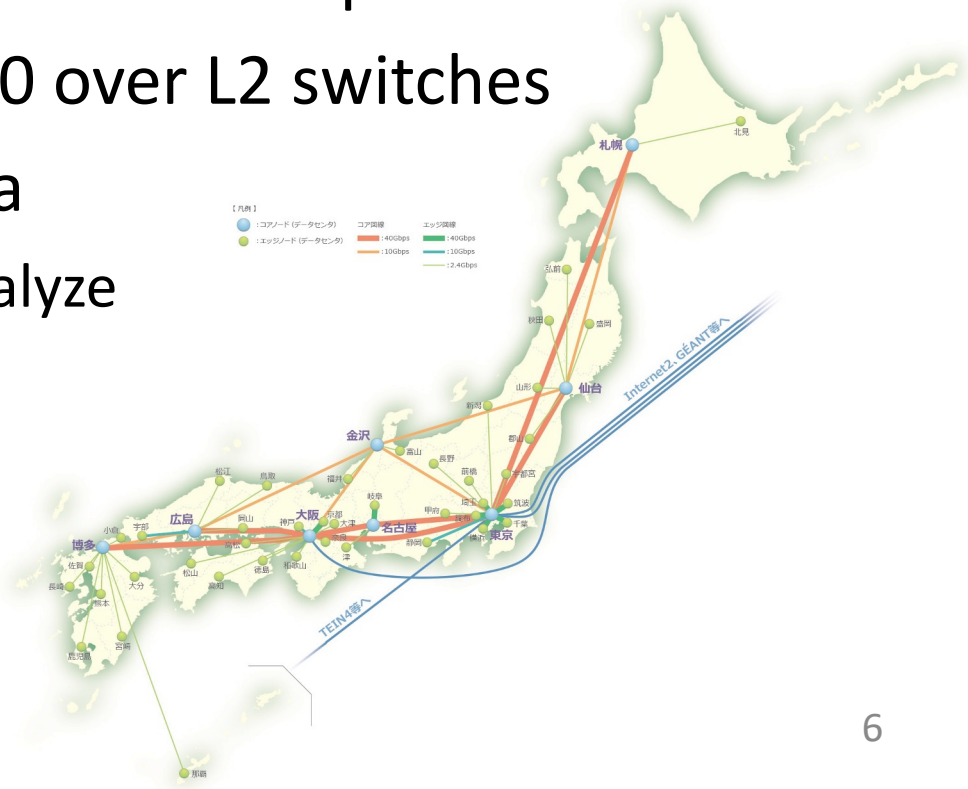
[6] B. Tak et al. "LOGAN: Problem Diagnosis in the Cloud Using Log-Based Reference Models," in IEEE IC2E, 2016, pp. 62-67.
[7] Z. Zheng et al. "3-Dimensional root cause diagnosis via co-analysis," in ACM ICAC, 2012, pp. 181.
[8] A. Mahimkar et al. "Towards automated performance diagnosis in a large iptv network," in ACM SIGCOMM, 2009, pp. 231–242.
[9] S. Kobayashi et al. "Mining causality of network events in log data", IEEE TNSM, vol. 15, no.1, pp. 37–67, 2018.

Goal

- Extract causality of events in system logs efficiently
  - Based on causal inference (PC algorithm)
  - Using network topology knowledge
- Provide reliable information for system management and troubleshooting
  - More accurate information
  - Less redundant (or meaningless) information

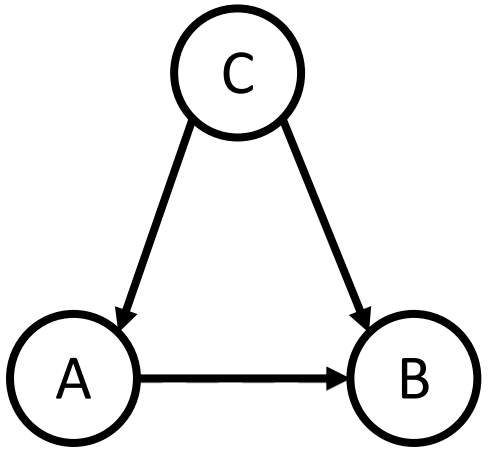
Dataset

- SINET4
  - https://www.sinet.ad.jp/en/top-en
  - A nation-wide R&E network in Japan
  - 8 core routers and 100 over L2 switches
  - 15 months syslog data
    - 3.5 million lines to analyze



Causal Inference

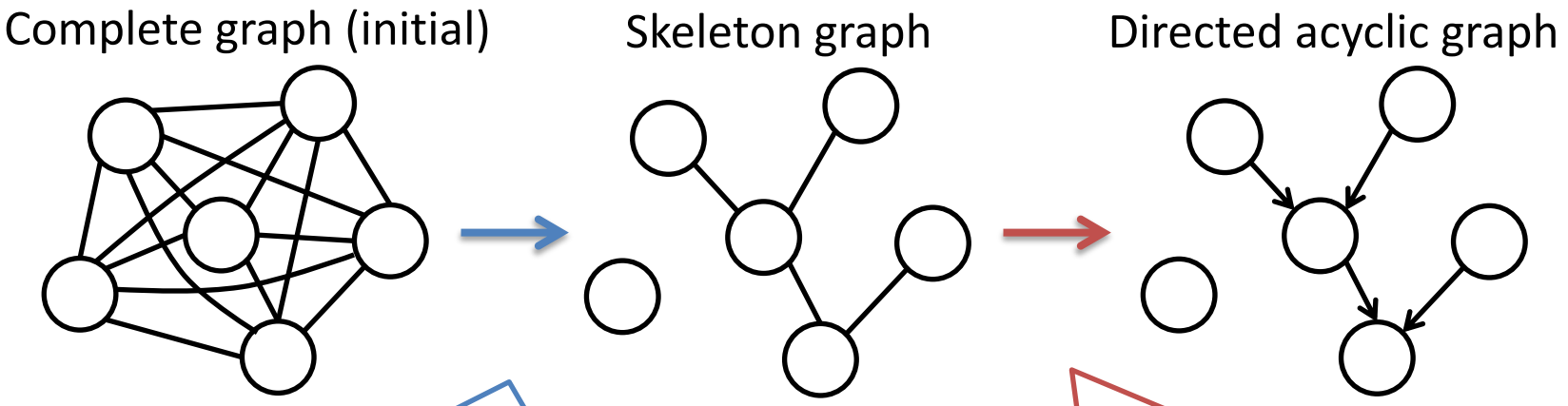
- Conditional Independence
  - A and B are independent if the effect of confounder C is excluded
  - A and B are conditionally independent given C
- PC algorithm [10]
  - Directed acyclic graph (DAG)
  - Explore conditional independence and remove false edges



$$P(A|C)P(B|C) = P(A, B|C)$$

[10] P. Spirtes et al. "An algorithm for fast recovery of sparse causal graphs", Social science computer review, vol. 9, pp. 62–72, 1991.

Flow of PC algorithm

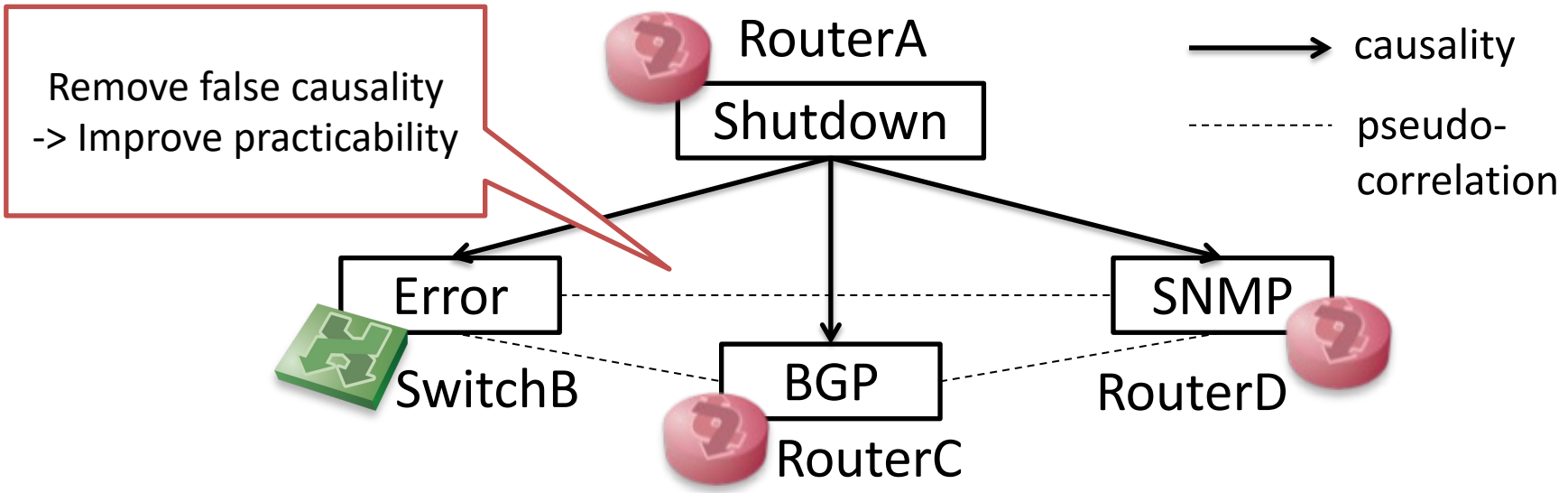


- Remove edges of conditional independence
- Statistical test for conditional independence [11] s) [12]
  - G2 test (for binary or multi-level data)
  - Fisher-Z test (for continuous data)

[11] R. E. Neapolitan. "Learning Bayesian Networks." Prentice Hall Upper Saddle River, 2004.
[12] T. Verma, et al. "An algorithm for deciding if a set of observed independencies has a causal explanation". In Proceedings of UAI'92, pp. 323–330, 1992.

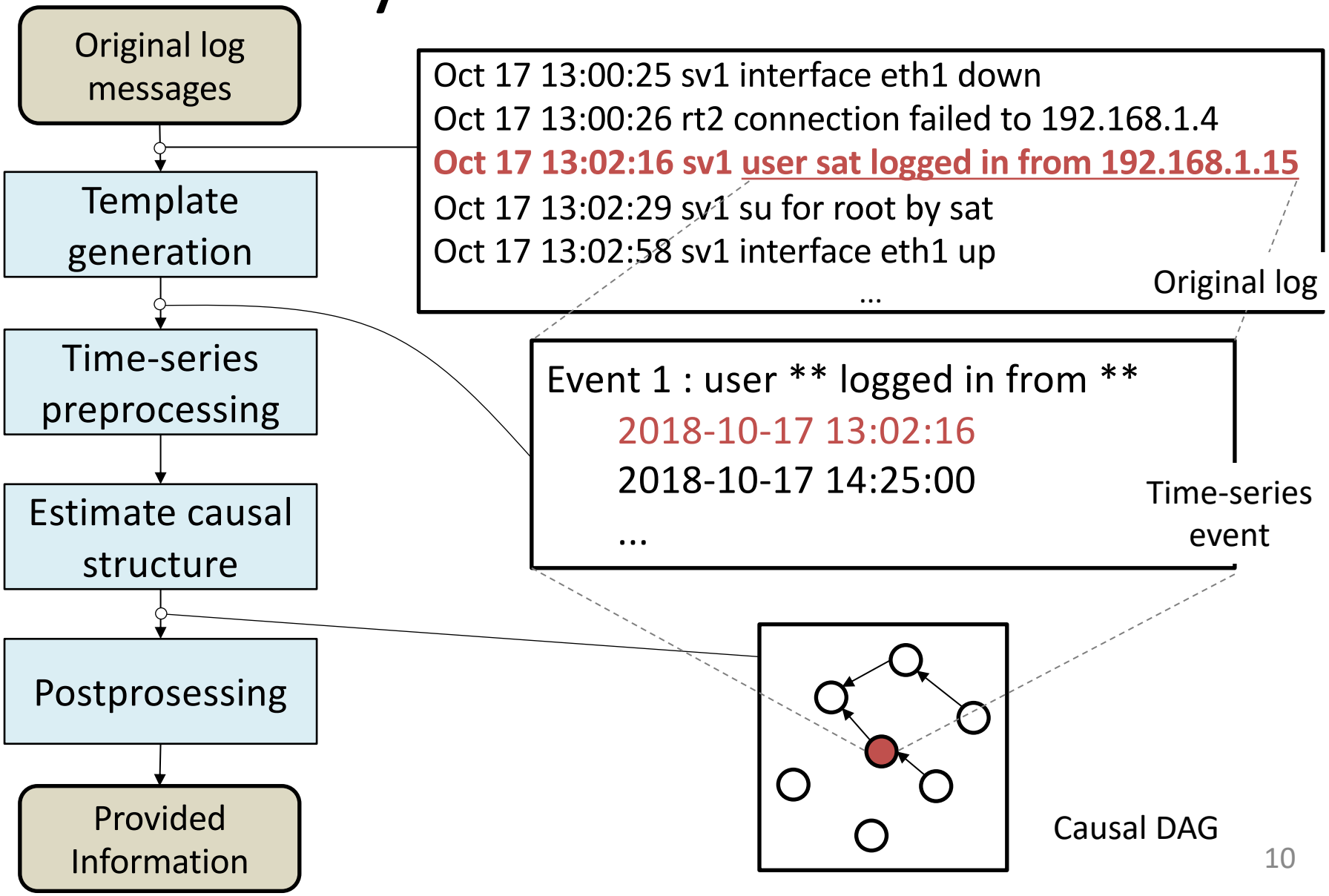
Log analysis and causal inference [9]

Oct 17 17:00:00 routerA System shutdown by root
Oct 17 17:00:05 switchB Error detected on eth0
Oct 17 17:00:15 routerC BGP state changed from Established to Idle
Oct 17 17:00:15 routerD SNMP trap sent to routerA
……

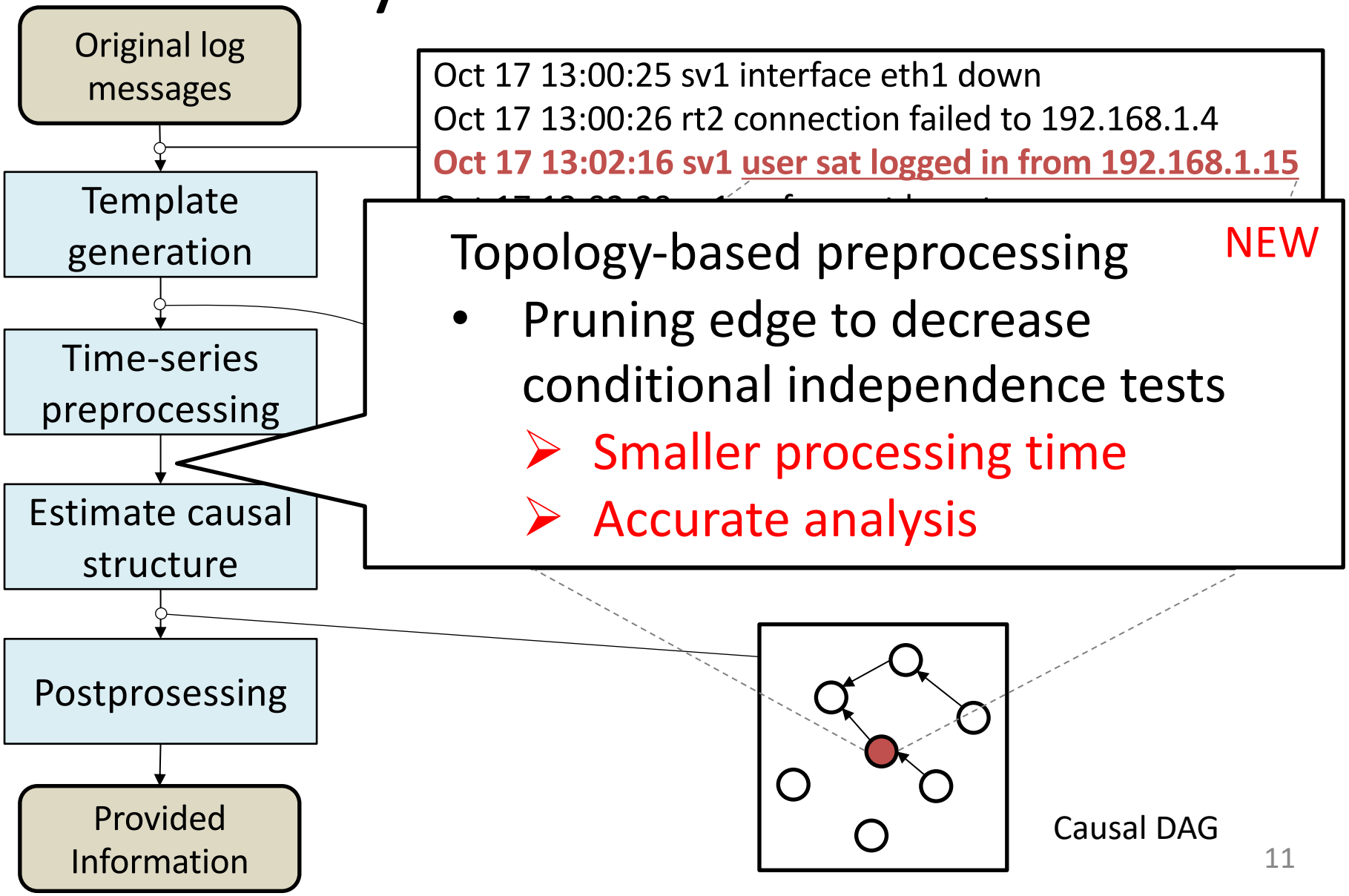


[9] S. Kobayashi et al. "Mining causality of network events in log data", IEEE TNSM, vol. 15, no.1, pp. 37–67, 2018.

System architecture

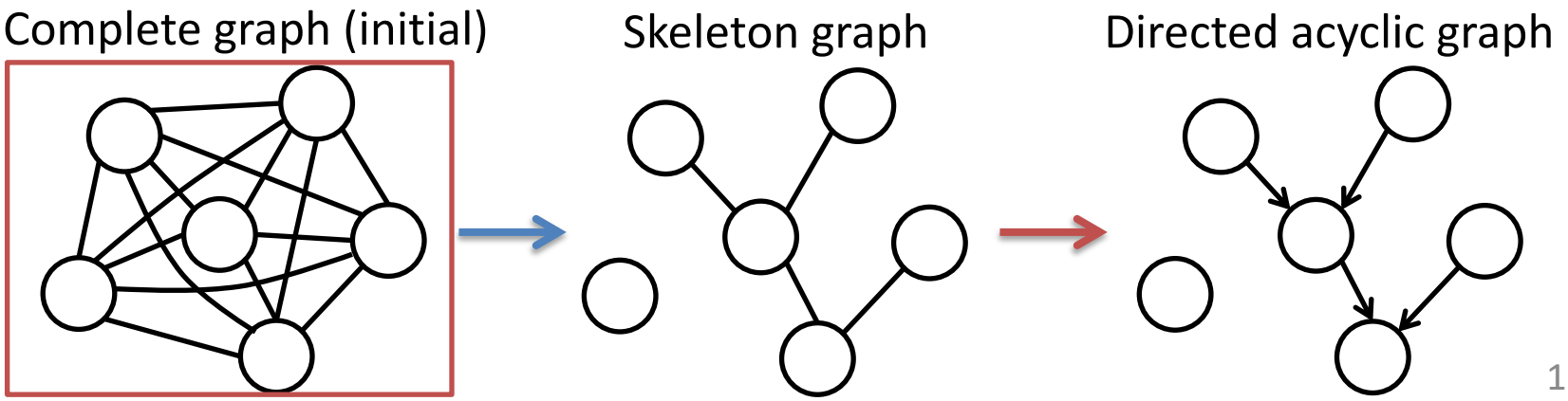


System architecture



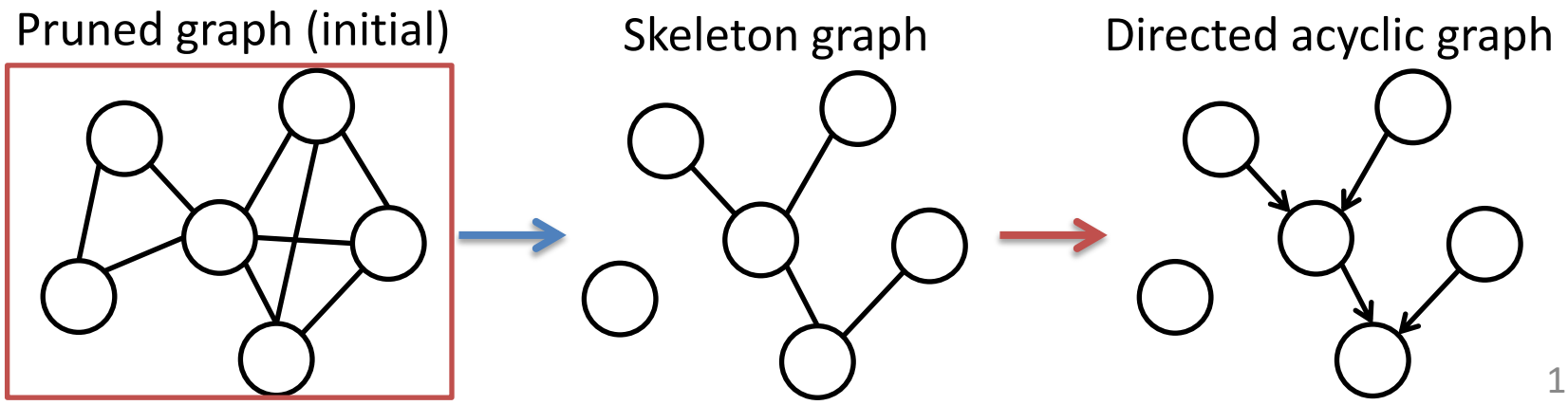
Proposed method

- Preprocessing based on network topology
  - Heuristic: **Only network events of connected devices have causal relations**
- Edit initial graph of PC algorithm
  - Complete graph -> Pruned graph

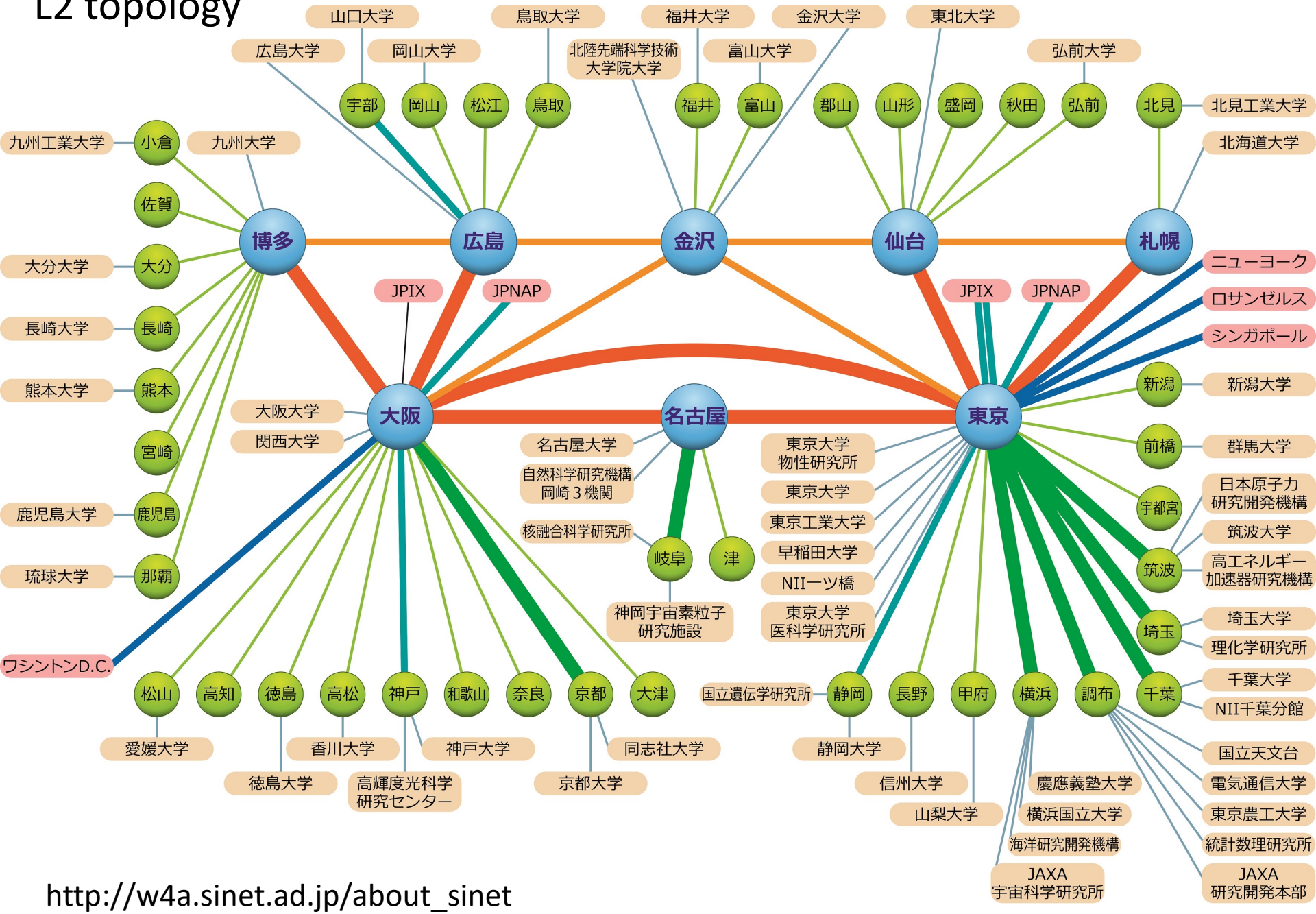


Proposed method

- Preprocessing based on network topology
  - Heuristic: **Only network events of connected devices have causal relations**
- Edit initial graph of PC algorithm
  - Complete graph -> Pruned graph



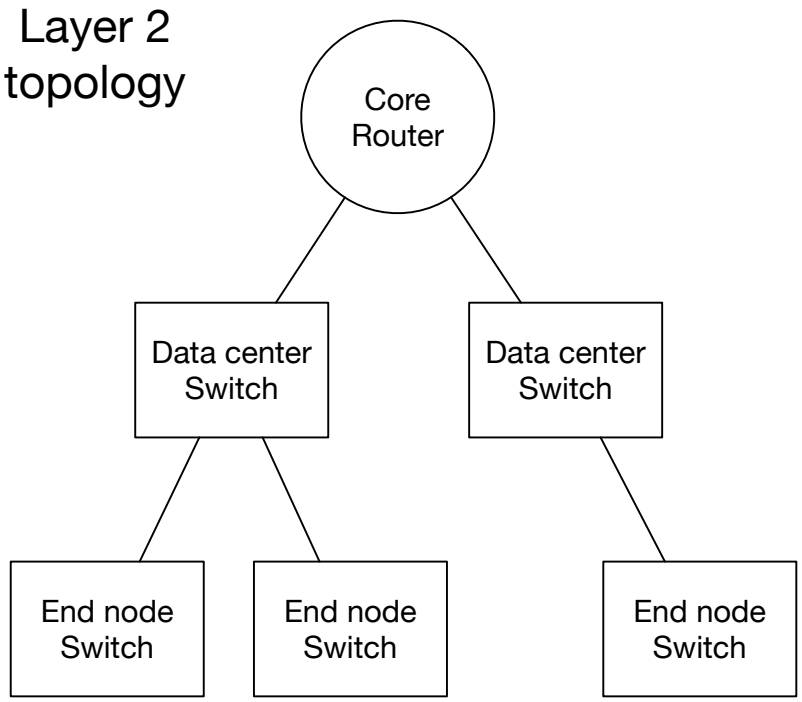
L2 topology

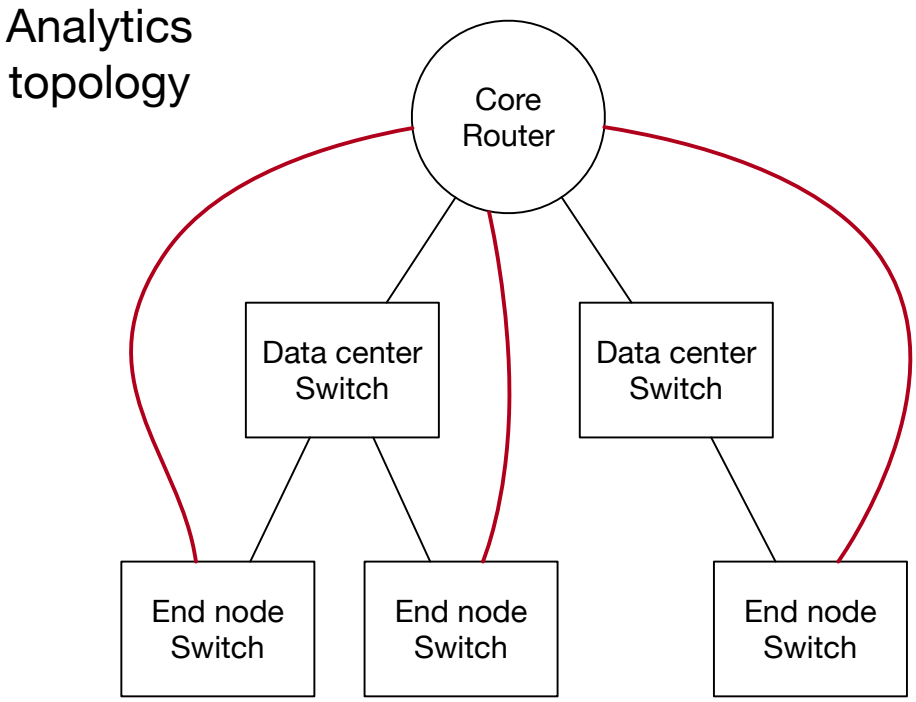


http://w4a.sinet.ad.jp/about_sinet

Generate analytics topology

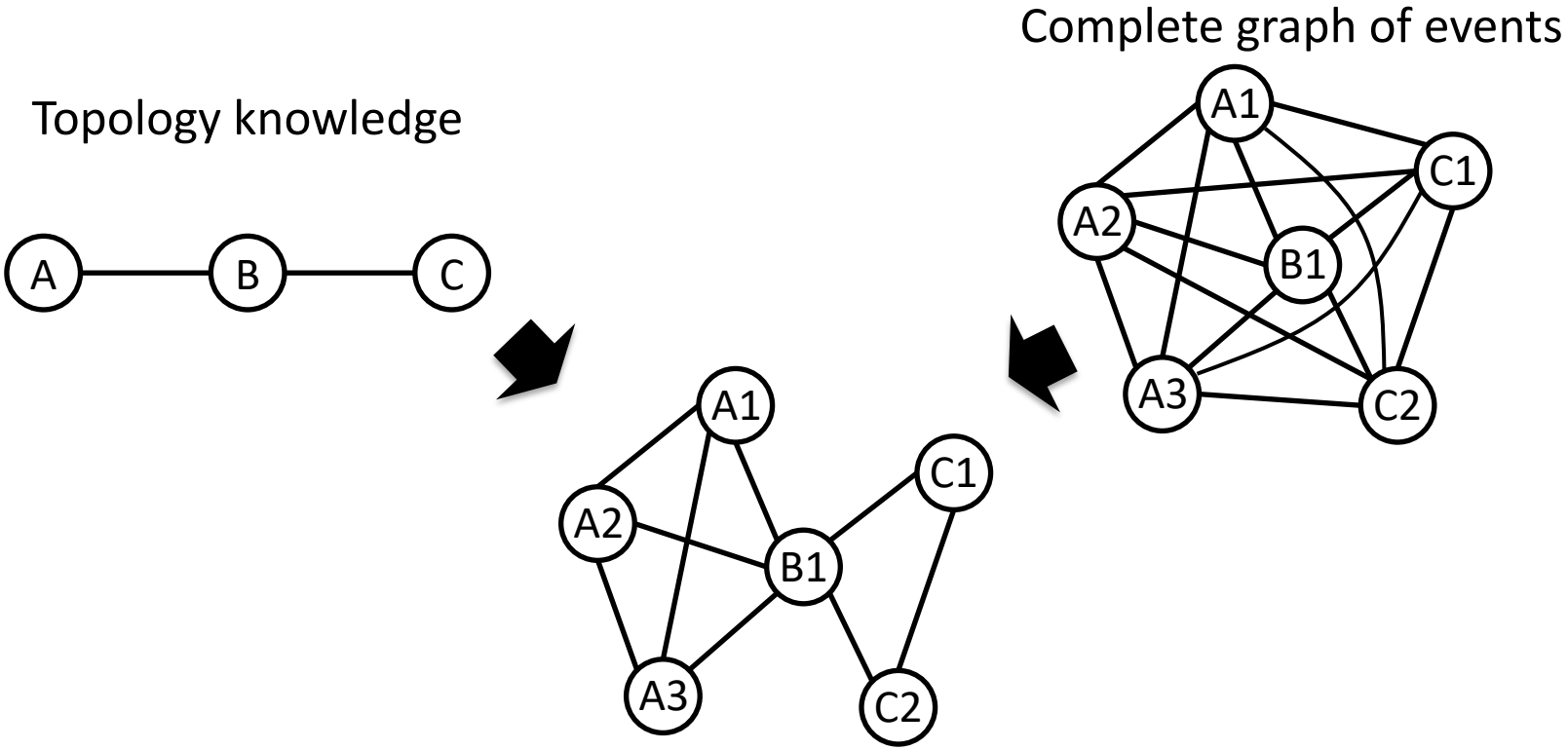
- Consider both L2 and L3 connectivity
  - Add edges of L3 connections





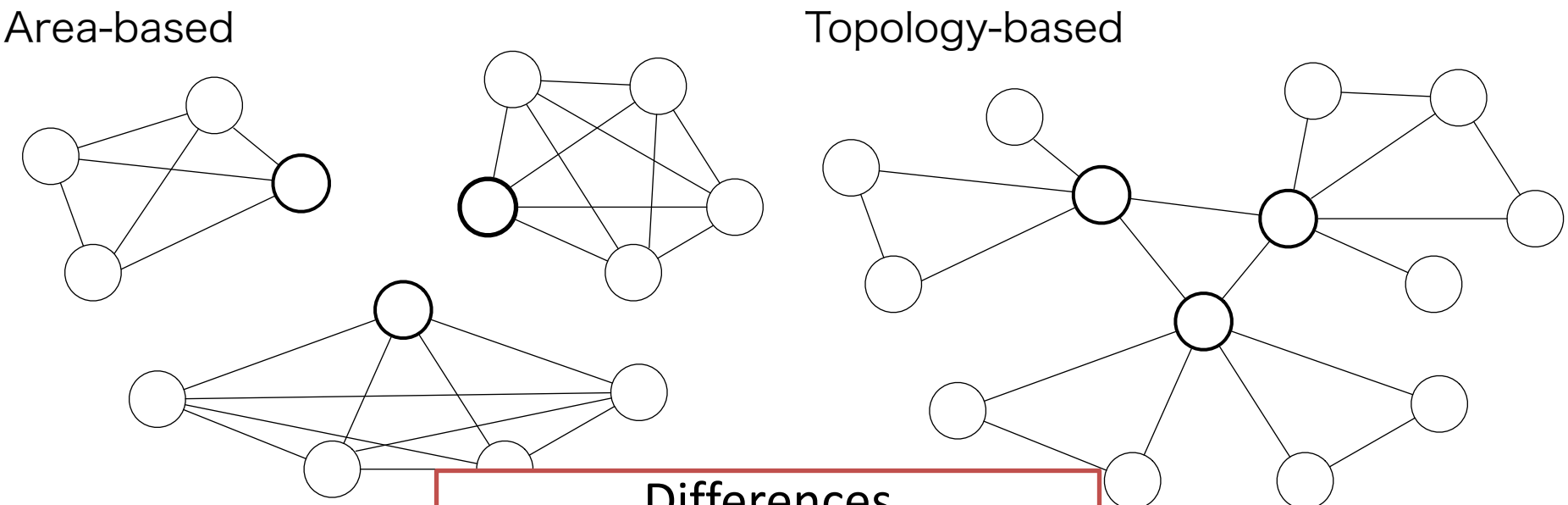
Pruning initial graph

- Prune edges between events of unconnected devices in given analytics topology



Compare with existing method

- Existing method: Area-based separation [9]
  - Multiple smaller complete graphs



Differences
- Edges among core routers
- Sparse edges

[9] S. Kobayashi et al. "Mining cau ... l. 15, no.1, pp. 37–67, 2018.

Evaluation

- Generate causal DAGs for 455-days log data
  - 35 million lines
  - 1789 log templates, 132 devices
- Results

Method	Edges	Time (sec/day)
None	30,174	1,220
Area-based	29,195	870
Topology-based	26,005	940

Both methods decrease 25% processing time

Classification of causal edges

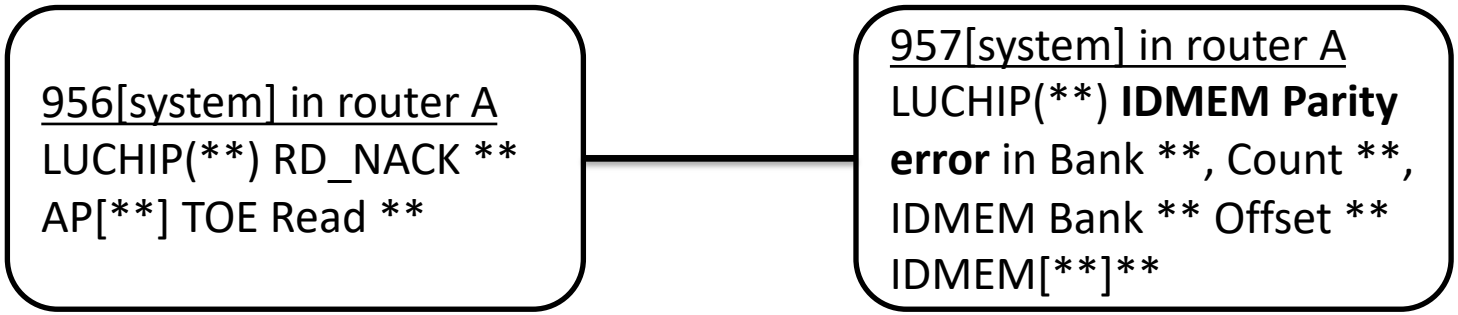
Type	Nodes	Ends of edges		
		None	Area	Topology
System	53,505	[illegible]	[illegible]	[illegible]
Network	12,901			
Interface	13,446			
Service	7,697	742	435	367
Mgmt	75,677	25,183	23,722	17,359
Monitor	2,452	267	305	298
VPN	3,465	50	1,074	106
Rt-EGP	3,831	1,576	1,6[illegible]	1,605
Rt-IGP				
Total				

SSH remote connections from a monitoring server

VPN connections in core routers
-> Conditional independence not effective in area-based method

Case study 1

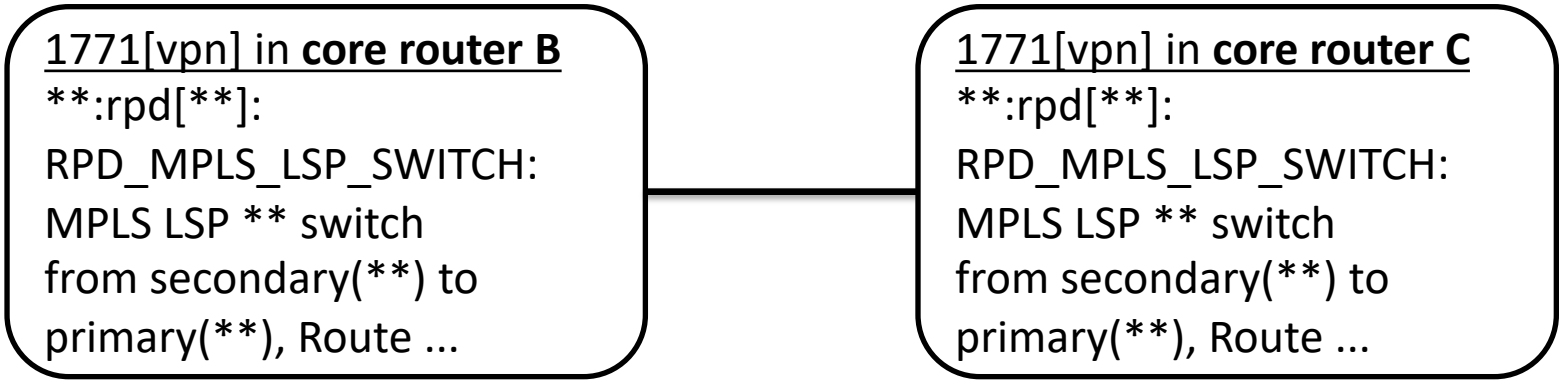
- Found causal edges in topology-based method (and NOT in area-based method)
- Events of system errors



Removed in area-based method
because of conditional independence
of failed (impossible) confounding factor

Case study 2

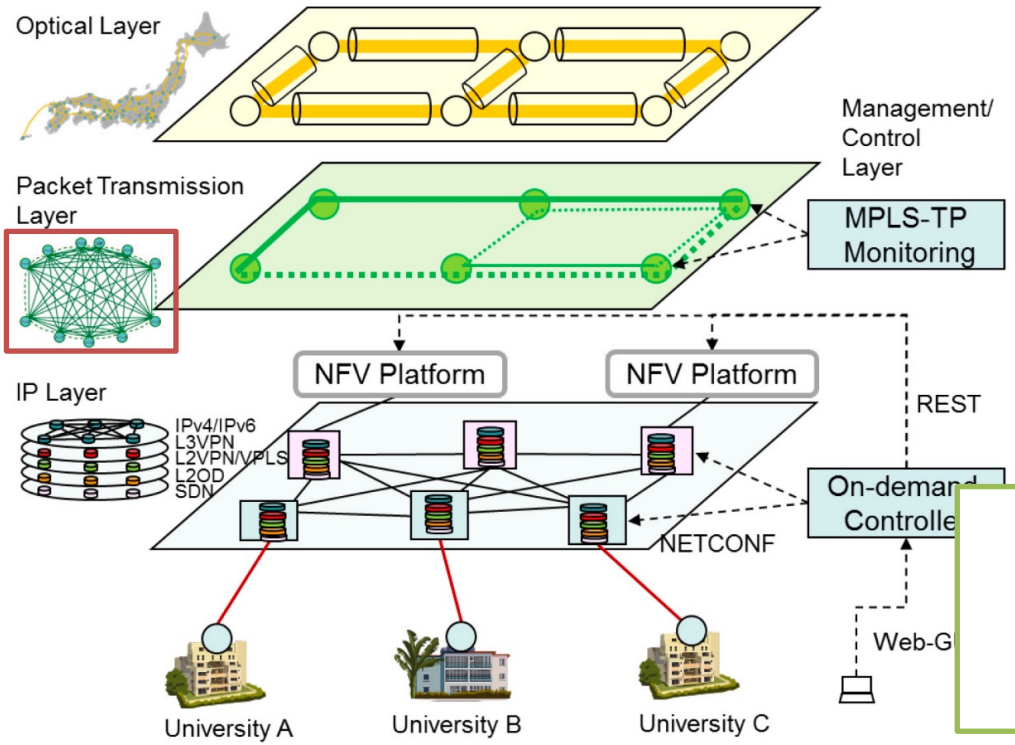
- Found causal edges in topology-based method (and NOT in area-based method)
- Events of VPN among core nodes



Topology-based method can find edges between core-router events (and Area-based method cannot)

Discussion

- Depends on network topology
  - Not effective in SINET5 (Full mesh topology) [13]



Next step:
Layer-based
preprocessing?

[13] T. Kurimoto, *et al.* "SINET5: A low-latency and high-bandwidth backbone network for SDN/NFV Era", in *IEEE International Conference on Communications,* 2017

Concluding remarks

- Estimate causal relations among network events in SINET4 log data
  - Use topology knowledge of network devices to prune initial edges of PC algorithm
  - Decrease 25% processing time
  - More accurate analysis than area-based method
- Future work
  - Co-operative analysis with other data sources
  - Layer-based preprocessing