On the Performance of Secure Graph Algorithms in Detecting Routing Loops

Sucheer Maddury
Leland High School, CA

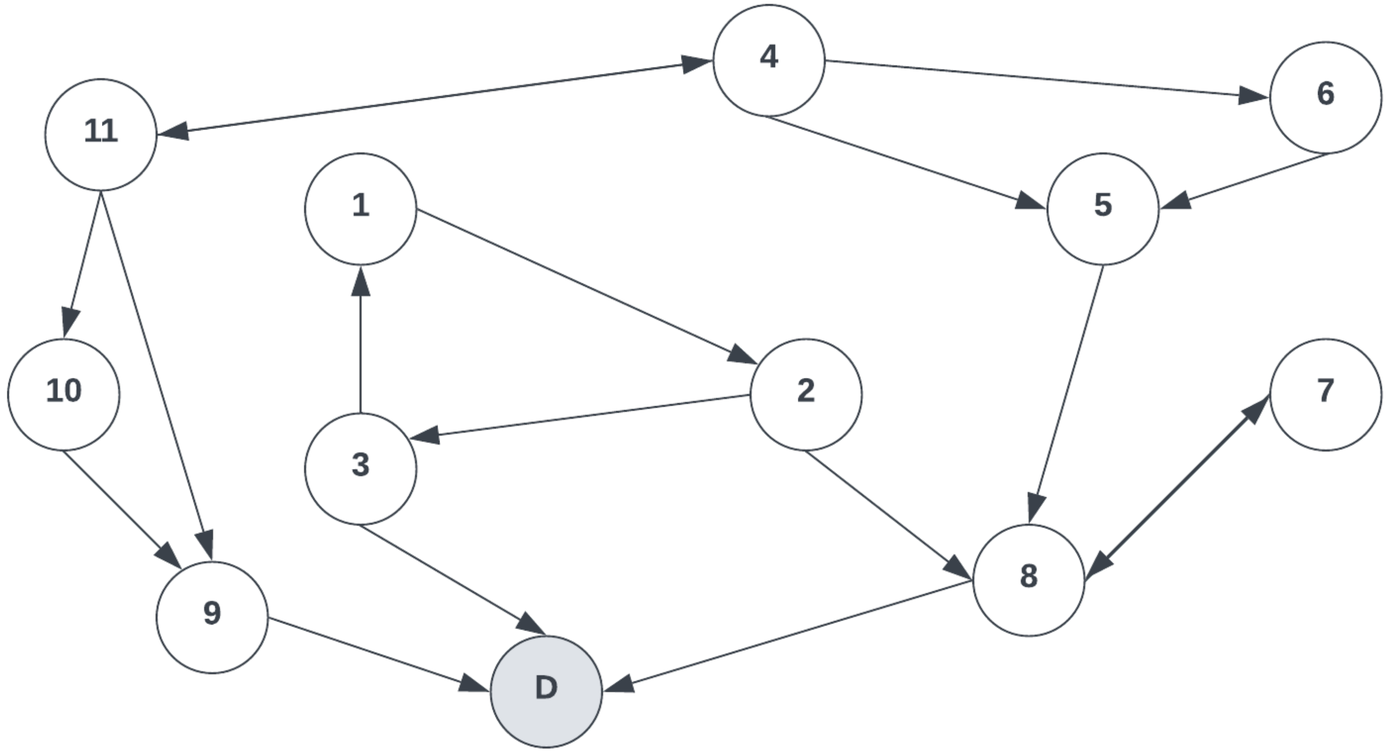
Jaber Daneshamooz
Department of Computer Science
University of California, Santa Barbara, CA 93106

UC SANTA BARBARA
Research Mentorship Program

RMP Research Symposium
August 2, 2023

Network Verification

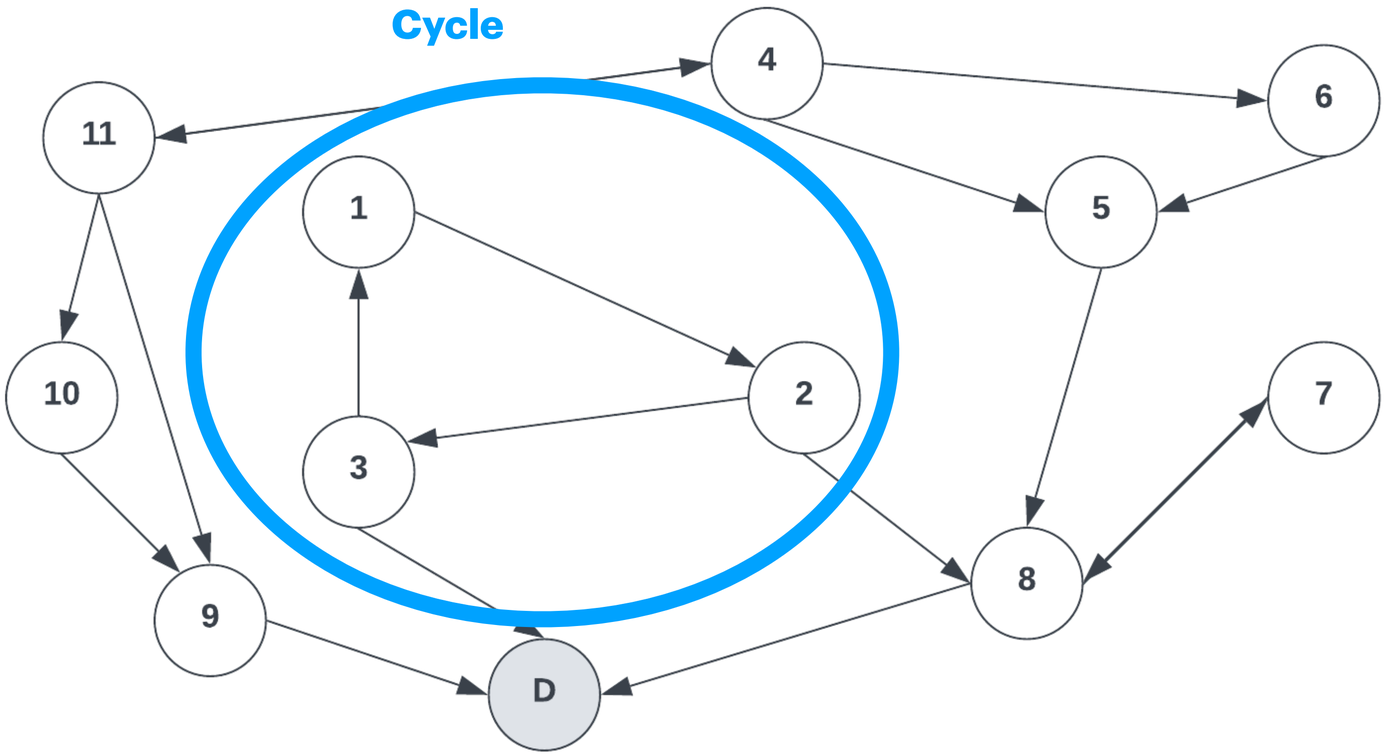
Edge List Representation



SRC	DEST
6	5
5	8
8	D
...	...

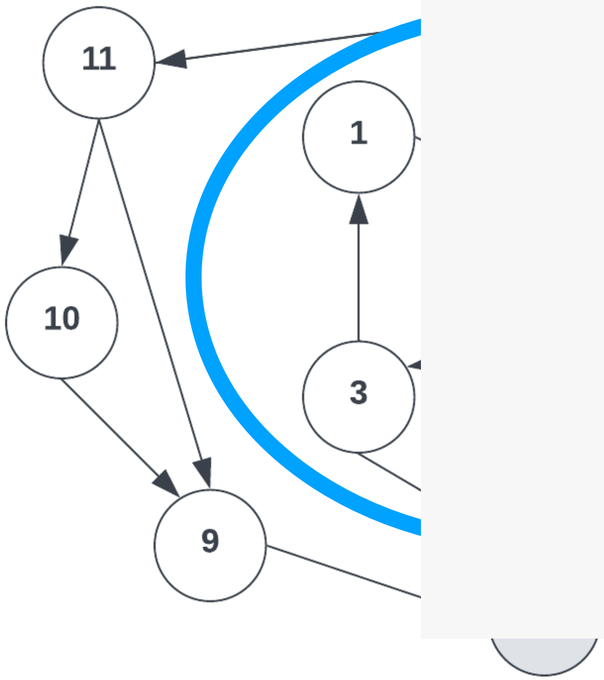
Network Verification

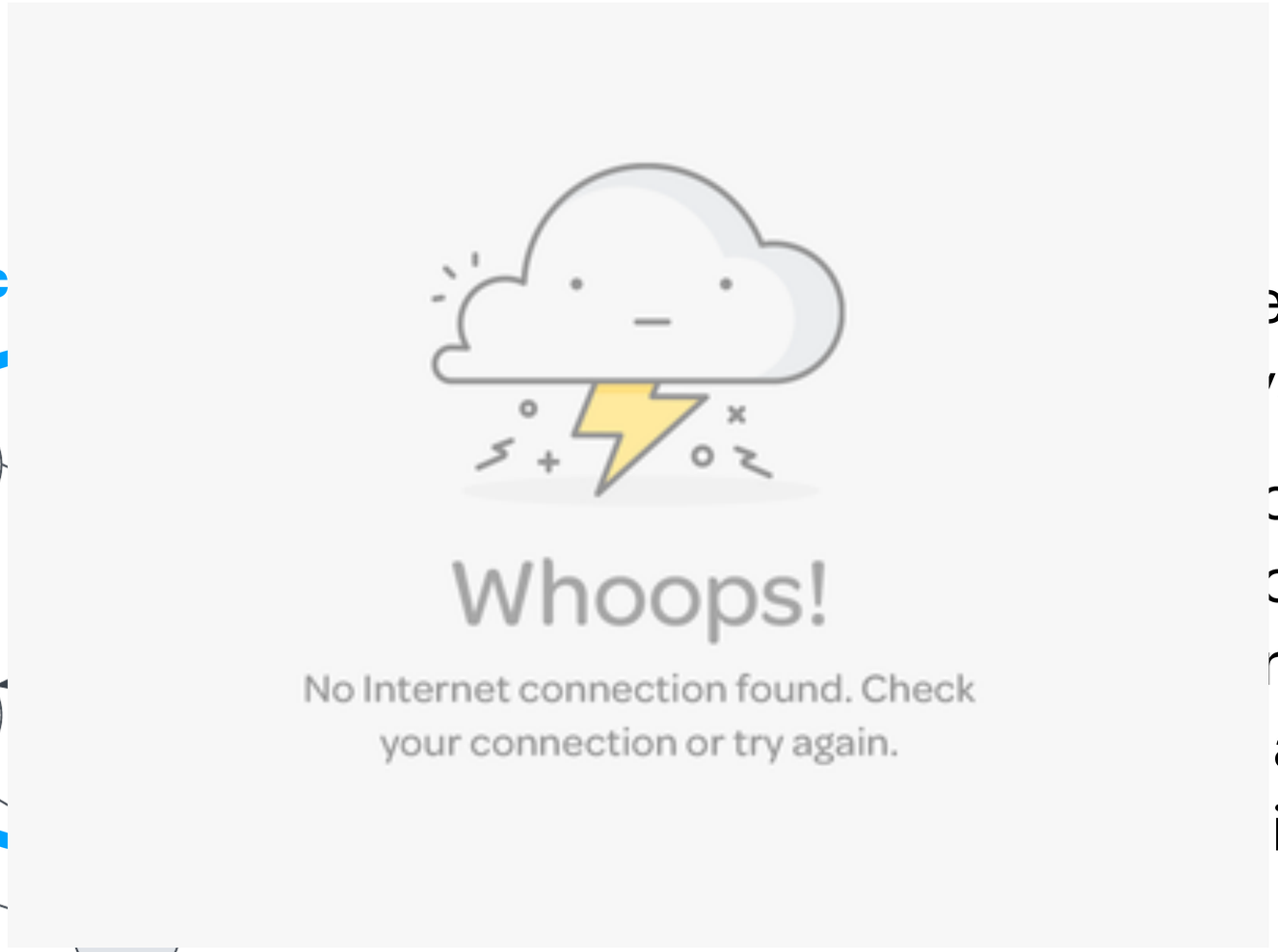
Graph Theory Approach



- Cycles can cause delays and outages
- Detecting misconfigurations securely requires MPC and graph algorithms

Network Verification





es can cause
s and outages

cting
onfigurations
rely requires
and graph
ithms

Challenges and Goals

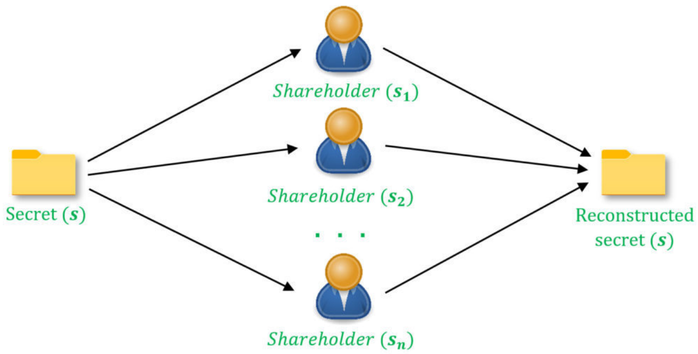
Potential Challenges

- Network administrators are reluctant to expose BGP configuration information
- Algorithms may function on smaller examples, but fail to scale to large networks

Multi-Party Computation - Secret Sharing

Shamir's Secret Sharing

(Additive SS)



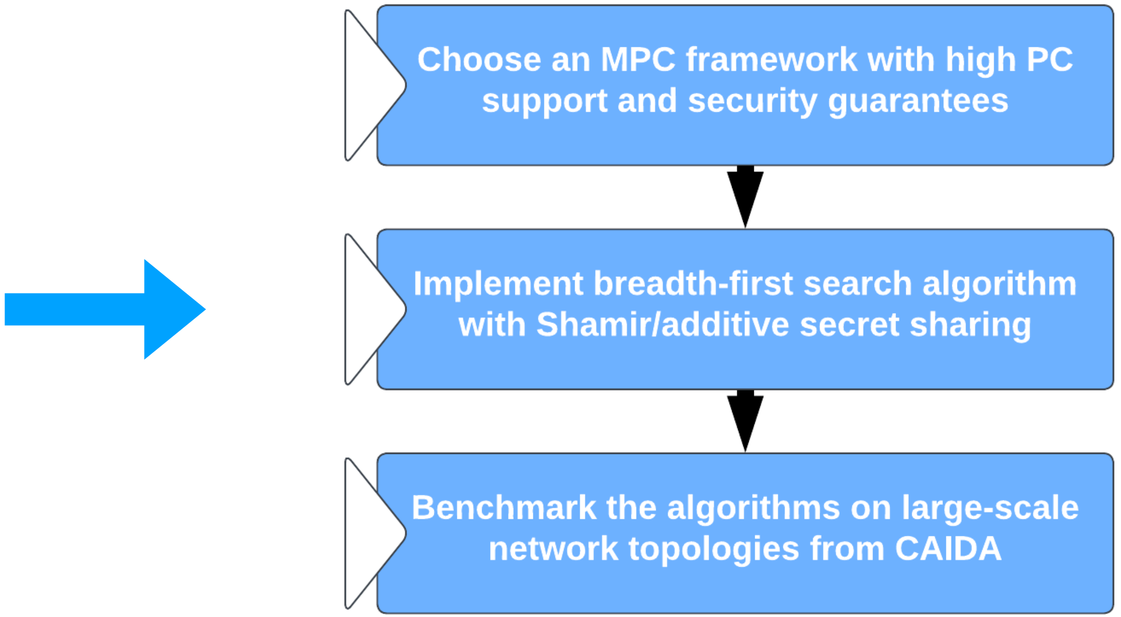
GeeksforGeeks (2021)

Shares scalars with summable pieces

Challenges and Goals

Potential Challenges

- Network administrators are reluctant to expose BGP configuration information
- Algorithms may function on smaller examples, but fail to scale to large networks



Choosing an MPC Framework

- We first reviewed all frameworks in Rotaru's awesome-MPC list
- We filtered out frameworks without documentation and/or <3PC support

NOTE: We also worked with TinySMPC for educational purposes

TNO-MPC

✓ Comprehensive documentation

✓ Wide array of arithmetic operators

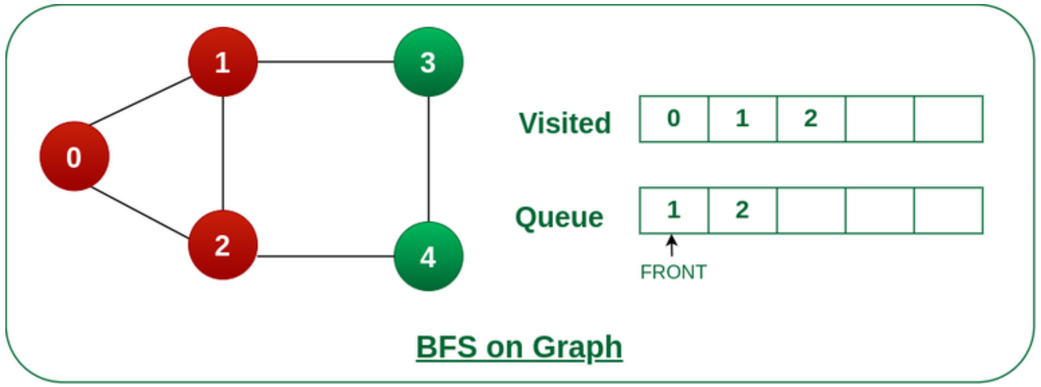
✓ Extensive Shamir SS support

The Algorithm

Breadth-First Search

- Create visited, in-progress, and to-be-visited sets
- Add dest_node to queue and in-progress set
- Continually look at front node in queue and search for a neighboring node that is in-progress **---> Cycle exists**

GeeksforGeeks (2023)

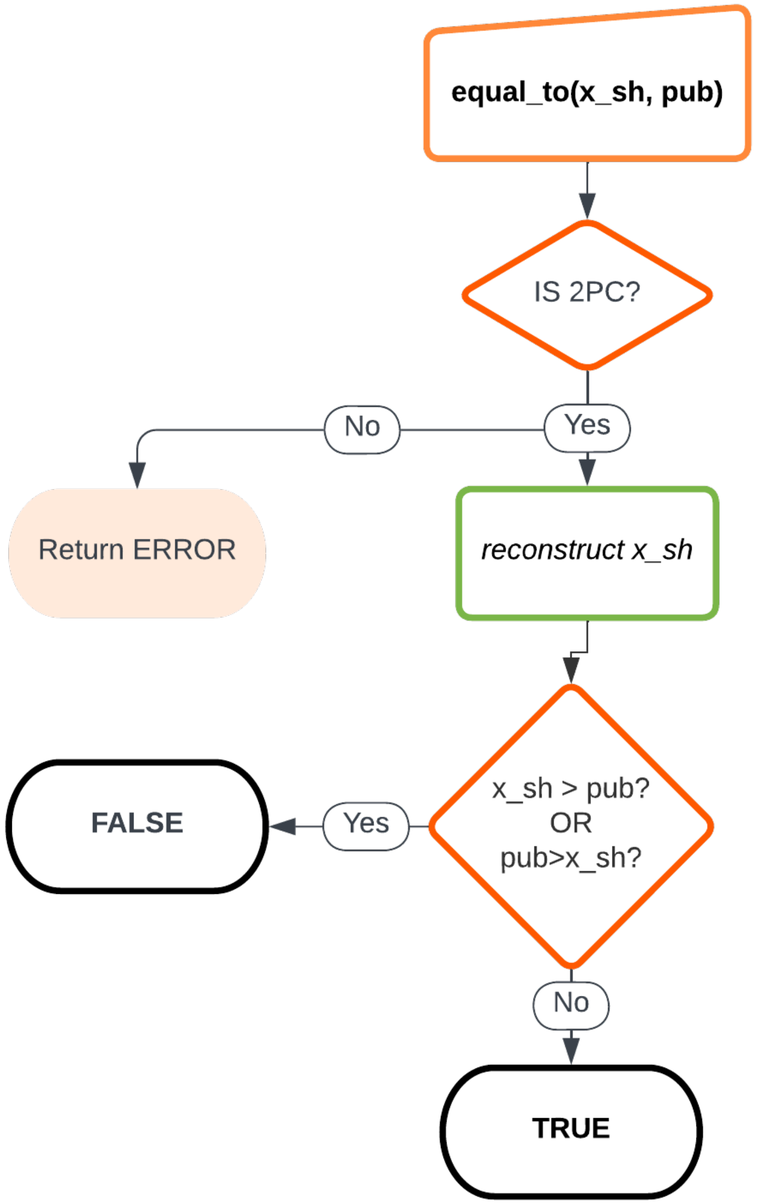


For UNdirected graphs

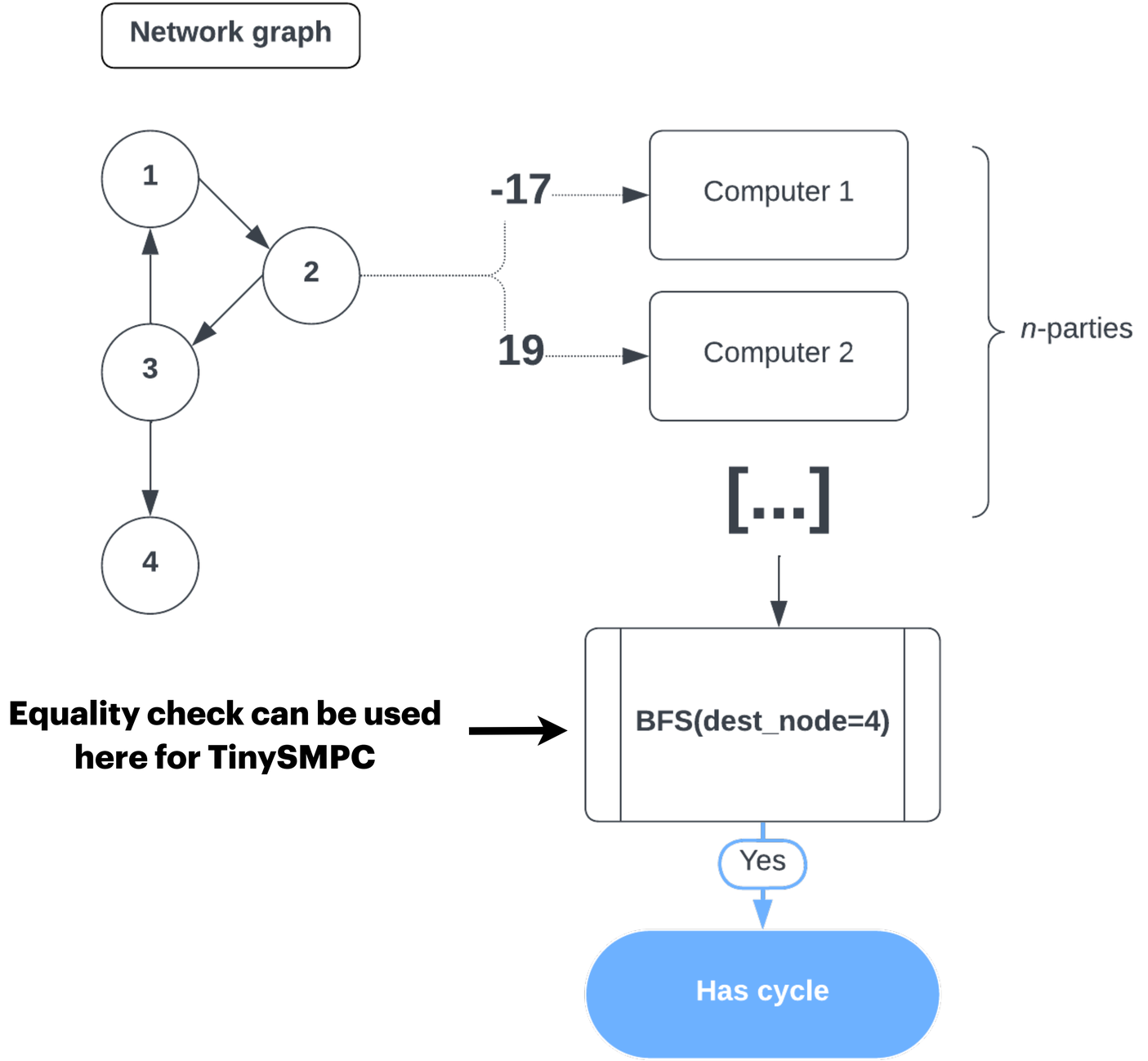
Equality Check

TinySMPC

Allows for node comparison



Basic Scheme



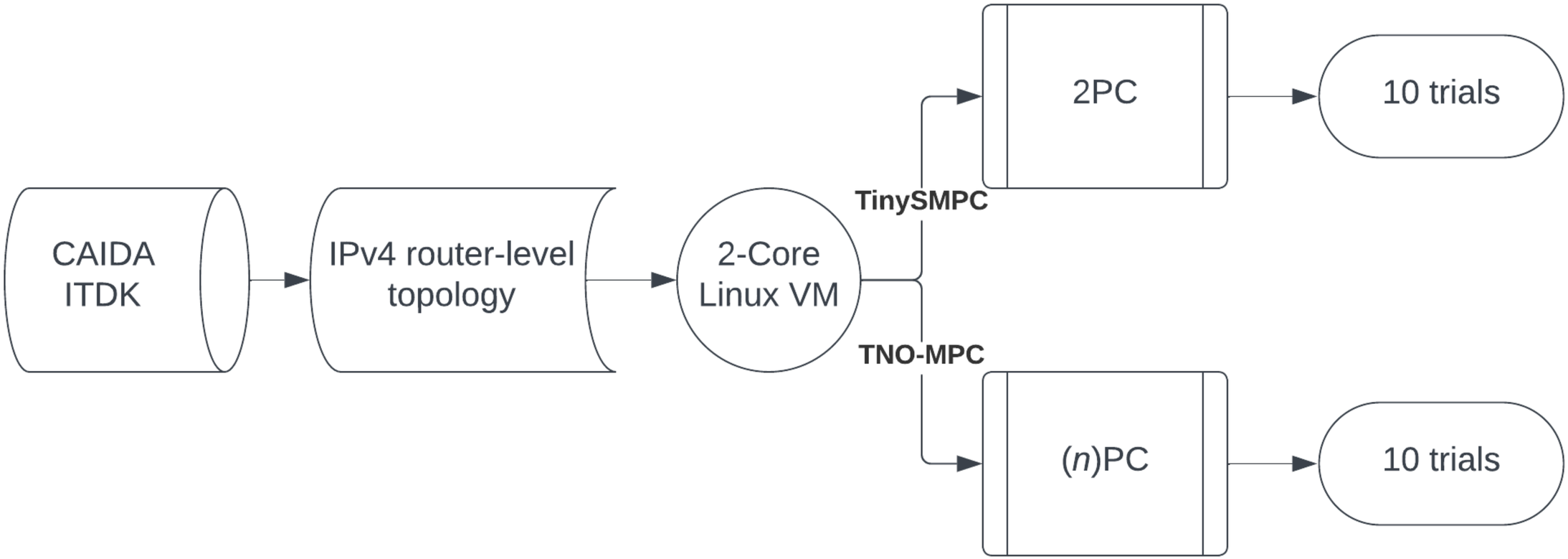
Choosing CAIDA Datasets

- From the CAIDA ITDK, we choose six datasets from various teams
- Each had varying amounts of edges and nodes from different years
- Each contained >= one cycle

Dataset Specifications

ITDK dataset	Node count	Direct edge count
Team 1/20100101	16695	33315
Team 1/20180101	25194	54086
Team 1/20190101	27895	55675
Team 1/20200101	34796	77650
Team 2/20180101	24868	53910
Team 3/20180101	25059	54375

Benchmarking Protocol



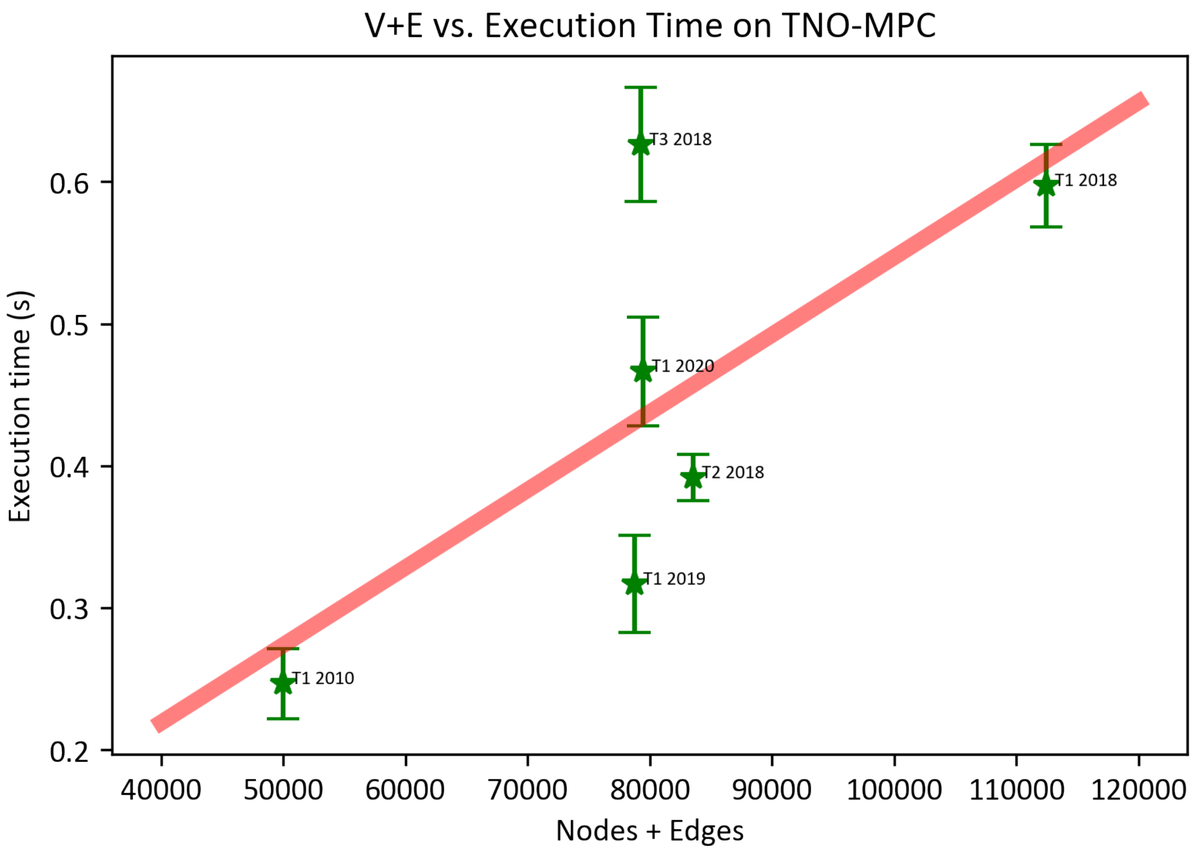
V+E vs. Execution Time

ITDK dataset	Nodes + Edges	TNO-MPC time (s)	TinySMPC time (s)
Team 1/20100101	50010	0.247 ± 0.0249	0.661 ± 0.113
Team 1/20180101	83570	0.392 ± 0.0164	1.213 ± 0.145
Team 1/20190101	112446	0.597 ± 0.0291	1.199 ± 0.0934
Team 1/20200101	79280	☆ 0.626 ± 0.0402	1.711 ± 0.214
Team 2/20180101	78778	0.317 ± 0.0343	☆ 2.868 ± 0.152
Team 3/20180101	79434	0.466 ± 0.0383	0.806 ± 0.120

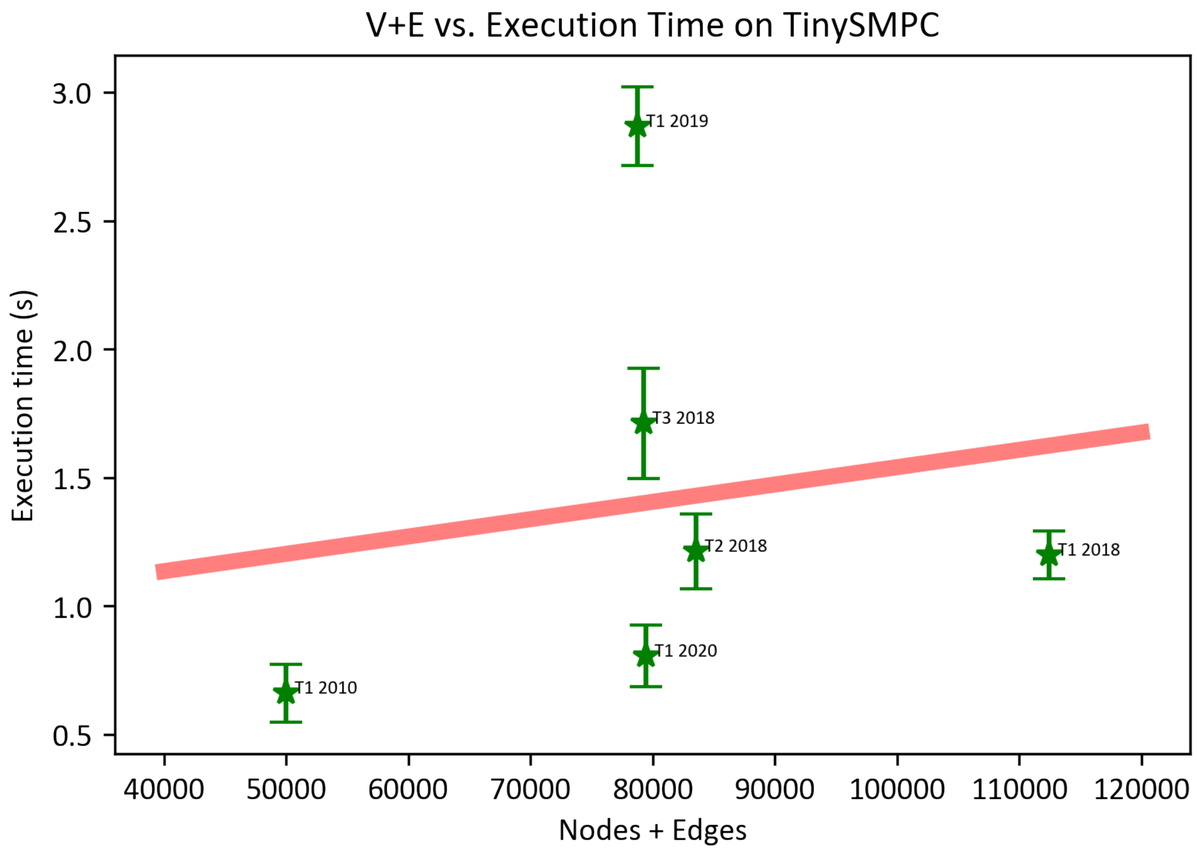
Significantly slower

☆ These points are outliers and likely represent worst-case time complexity

V+E vs. Execution Time



P value **



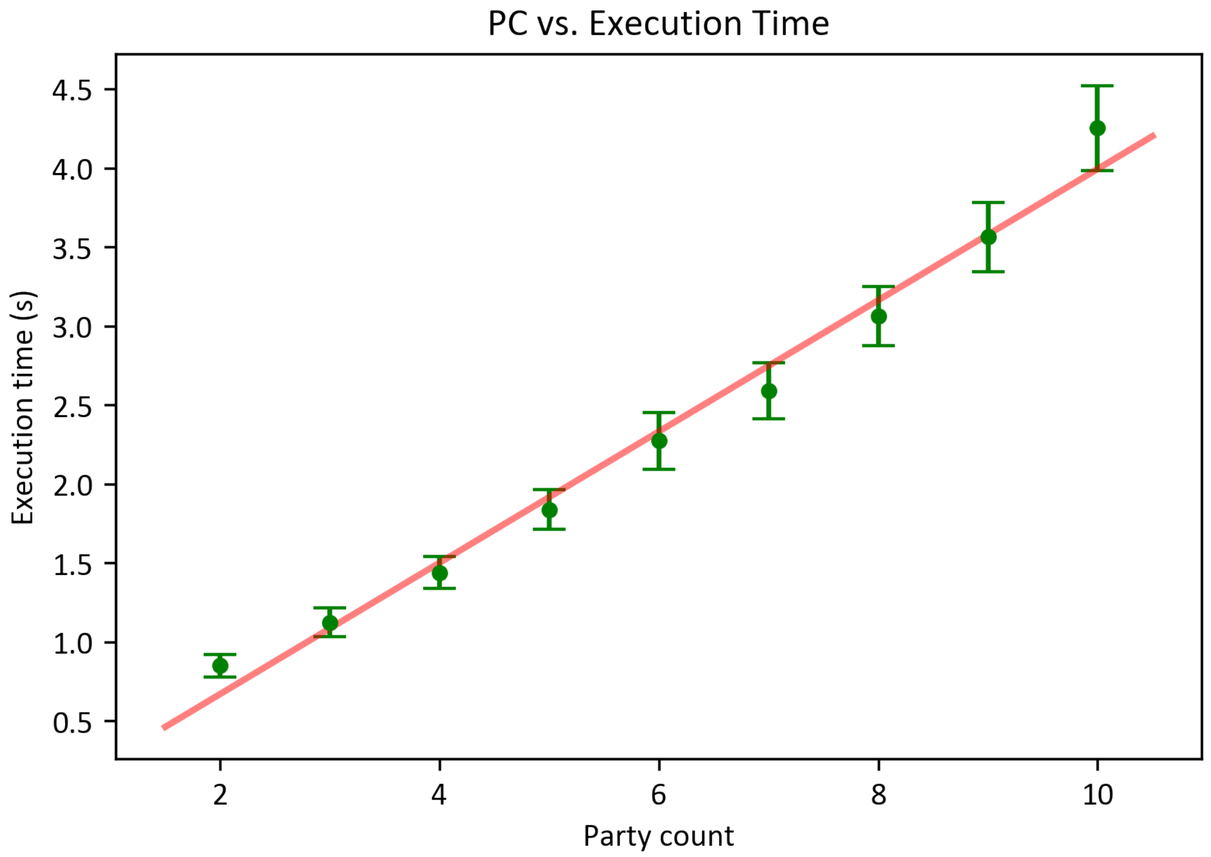
P value **

PC vs. Execution Time on TNO-MPC

Party count	Execution time mean (s)
2	0.849
3	1.124
4	1.439
5	1.837
6	2.273
7	2.589
8	3.0606
9	3.564
10	4.252

minimum security

directly proportional



P value **

Results in Context

Privacy

Securities

- Node addresses will remain private to computing parties
- Node order will remain secure

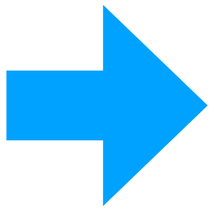
Insecurities

- Corrupted parties can gain information about general network structure
- Vulnerable to malicious actors

Results in Context

Scalability

Secure BFS execution time is relatively fast, but too slow to be run at extremely high rates



Useful for:

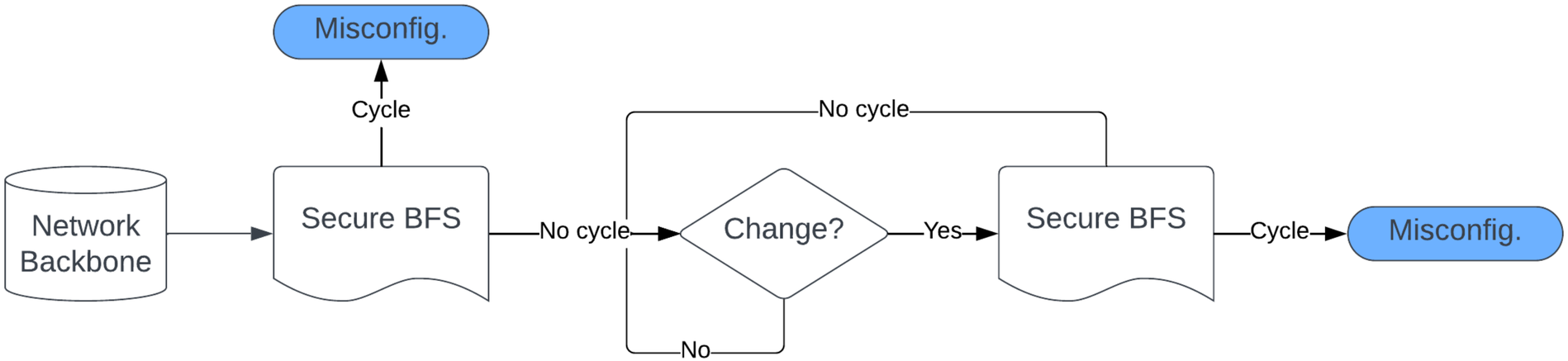
- Large network changes
- New network backbones

Not useful for:

- Rerouting
- Frequent backbone edits

Future Direction

- Higher specificity in location of cycles
- Experimentation with local BFS (next-hop traversal)
- Integration with broader network verification system



Acknowledgements

I would like to acknowledge:

- Jaber Daneshamooz
- Melody Yu
- Zheng Ke
- Dr. Lina Kim and the RMP staff
- Summer Discovery
- Parents