Privacy-Preserving Network Verification System Scalable for Internet Infrastructures

Melody Yu
Sage Hill School

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

RMP Research Symposium
Aug 2, 2023

UC SANTA BARBARA
Research Mentorship Program

Network Outage

Close

Check your connection

You don't seem to have an active internet connection.
Please check your connection and try again.

Facebook | Error
https://www.facebook.com
Search

Sorry, something went wrong.

We're working on it and we'll get it fixed as soon as we can.

Go Back

Facebook © 2018 · Help Center

ecking the network cables, modem, and router
connecting to Wi-Fi
nning Windows Network Di

E_FINISHED_NO_INTERNET

Error 500 (Server Error)!!1
https://myaccount.google.com
Google

500. That's an error.

There was an error. Please try again later. That's all we know.

503

Service Unavailable

The server is temporarily busy, try again later!

There was a problem loading this website

Try refreshing the page.

If the site still doesn't load, please try again in a few minutes.

Network Outages

$9,000

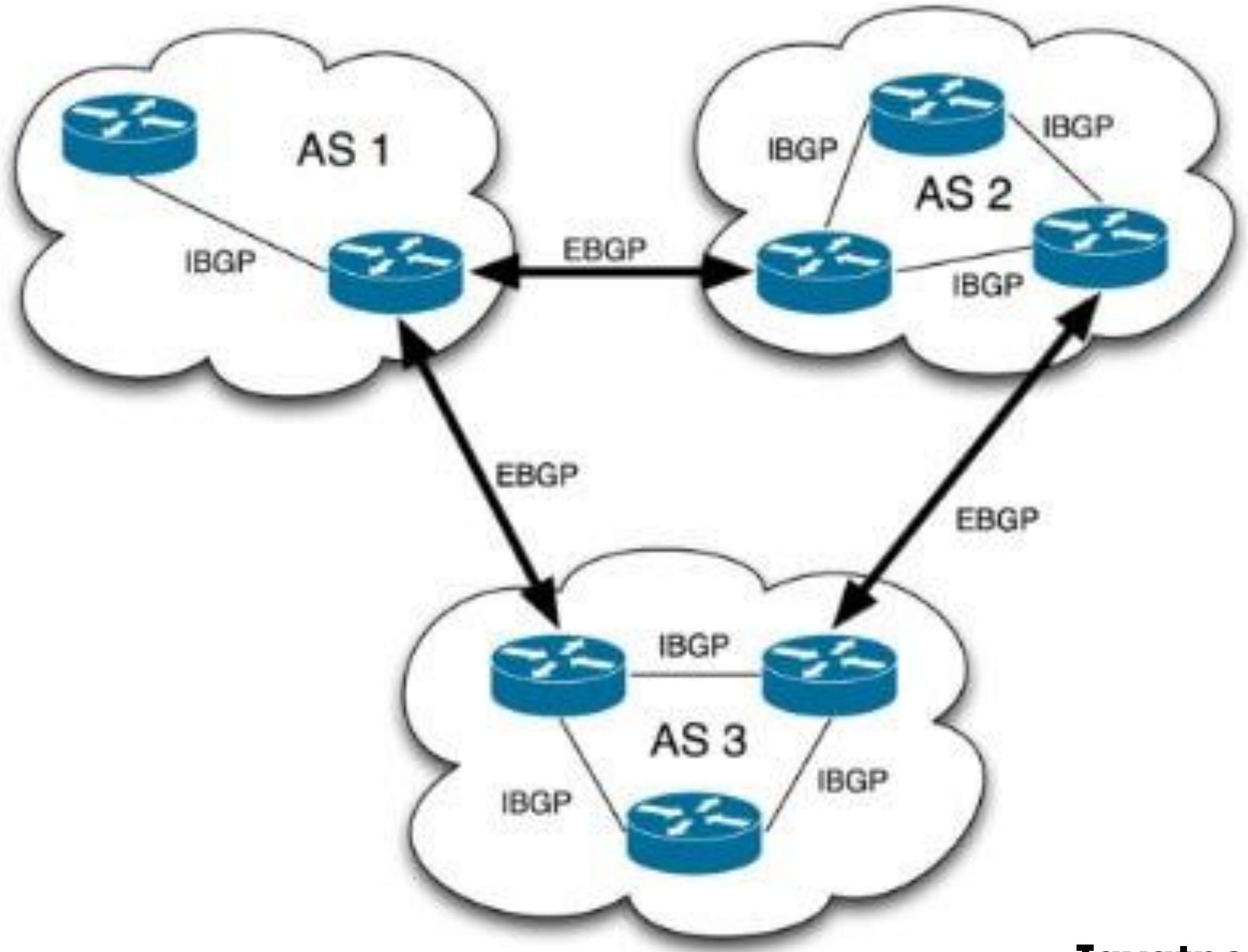
every minute

$100M

Meta’s lost revenue from one outage in 2021

Internet Infrastructure

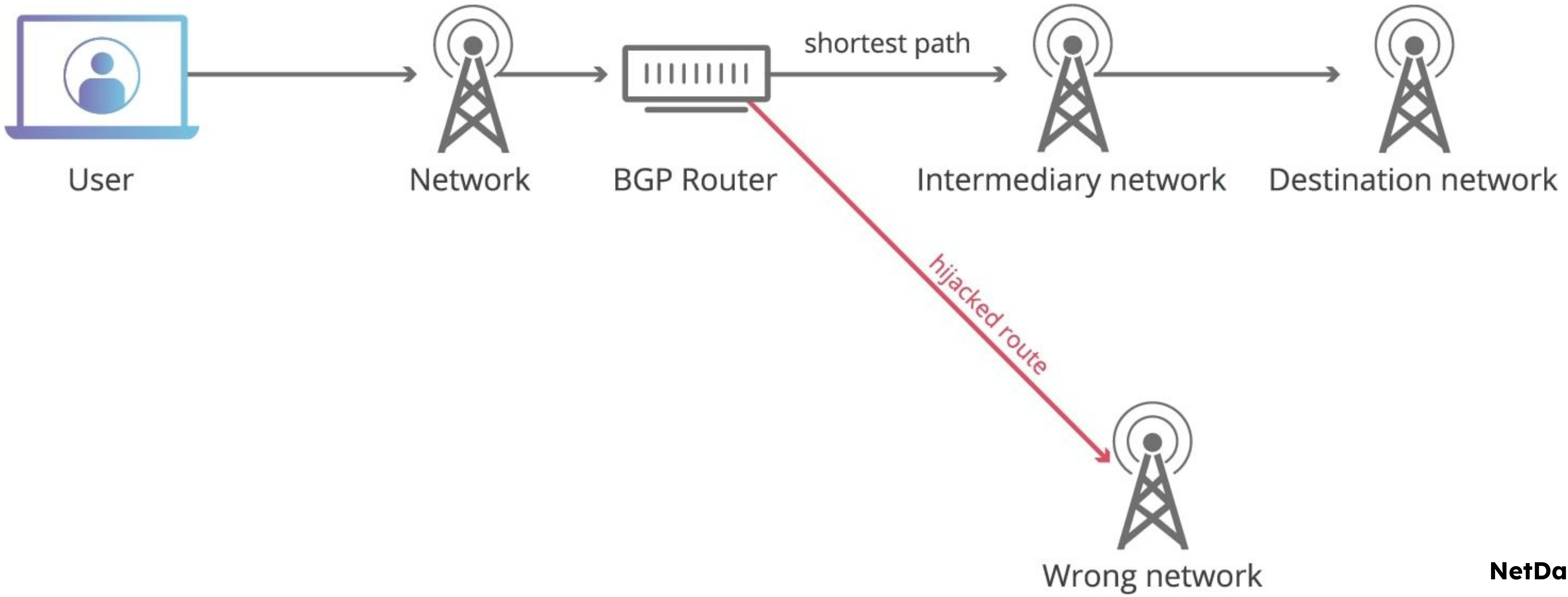
- Graph of **autonomous systems (AS)** connected to each other
  - Each AS contains **routers** which direct the flow of data
  - Communicate by sending data packets to each other



Javatpoint

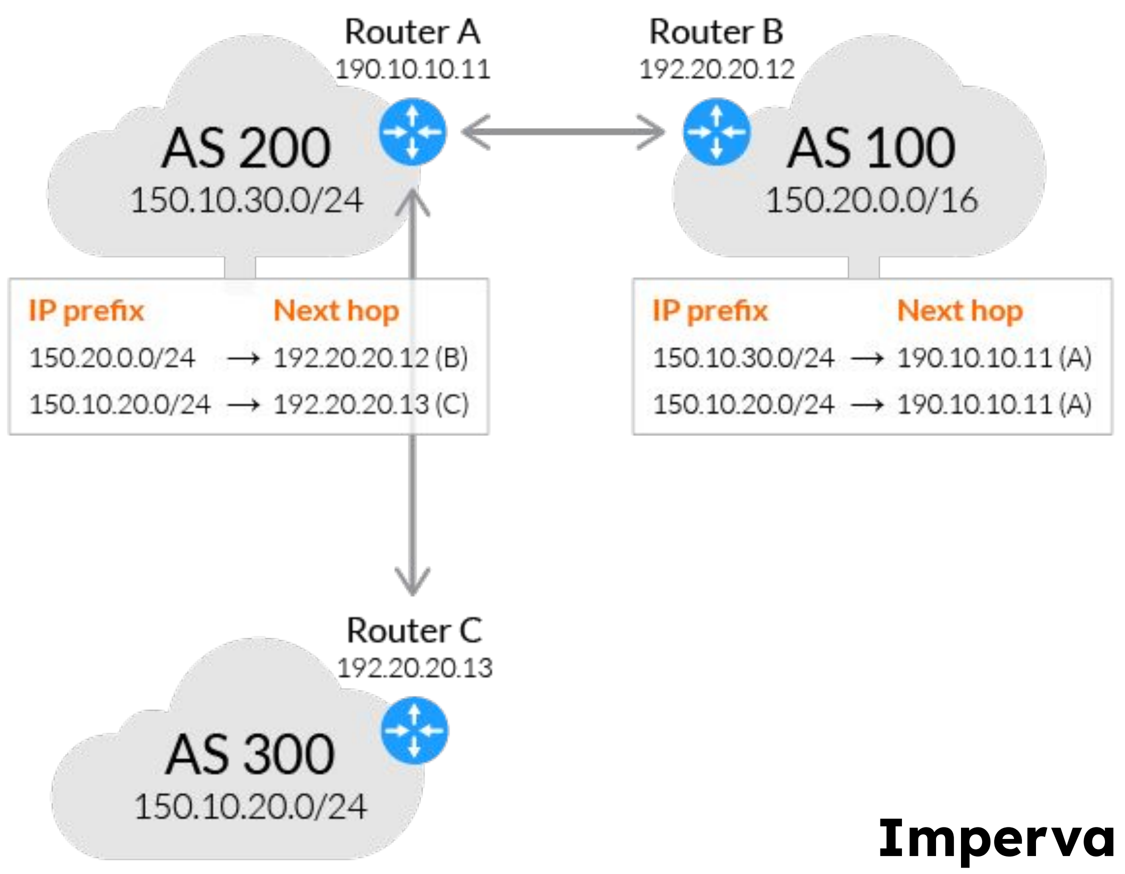
BGP Misconfigurations

- Routers know how and where to transfer information through the **Border Gateway Protocol (BGP) peering** protocol
- AS administrators often need to make changes to BGP peering protocol
- Can lead to **BGP misconfigurations**



NetData

Network Outages



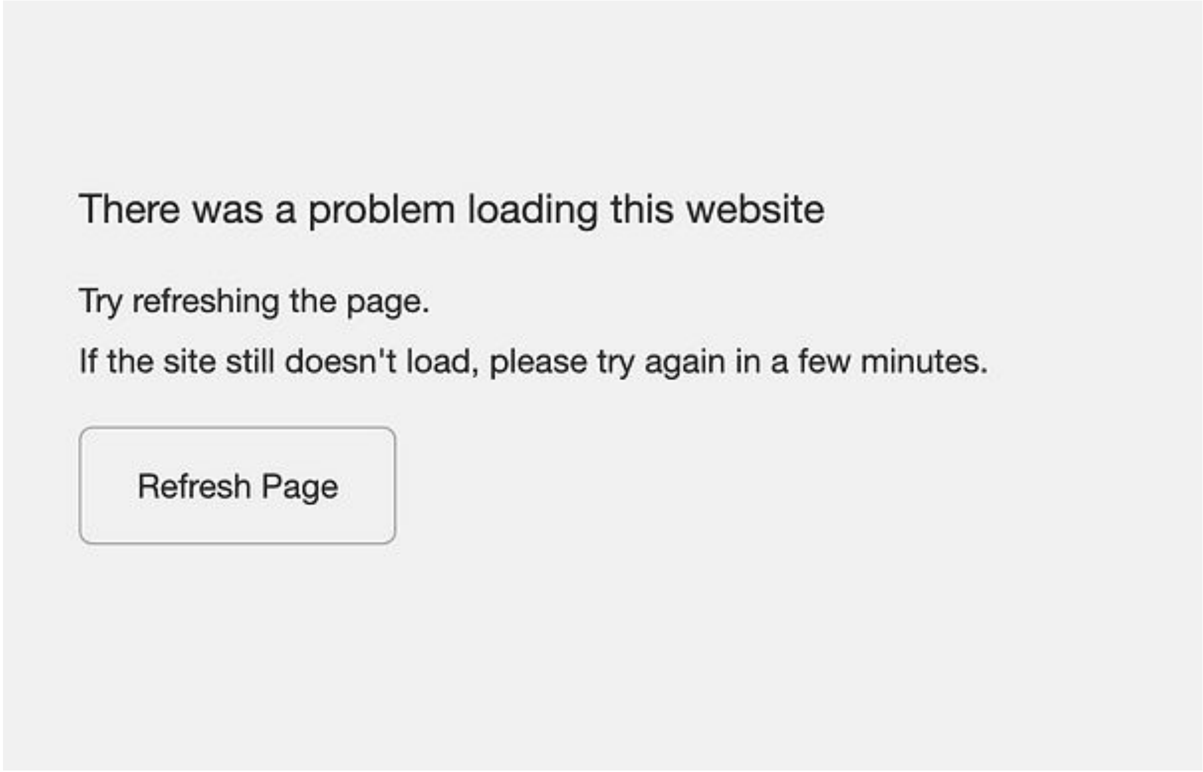
IP prefix		Next hop
150.20.0.0/24	→	192.20.20.12 (B)
150.10.20.0/24	→	192.20.20.13 (C)

IP prefix		Next hop
150.10.30.0/24	→	190.10.10.11 (A)
150.10.20.0/24	→	190.10.10.11 (A)

Imperva

Border Gateway Protocol (BGP) Misconfiguration

Error in the BGP configuration



There was a problem loading this website

Try refreshing the page.

If the site still doesn't load, please try again in a few minutes.

Network Outage

Unexpected downtime and outage of the autonomous system.

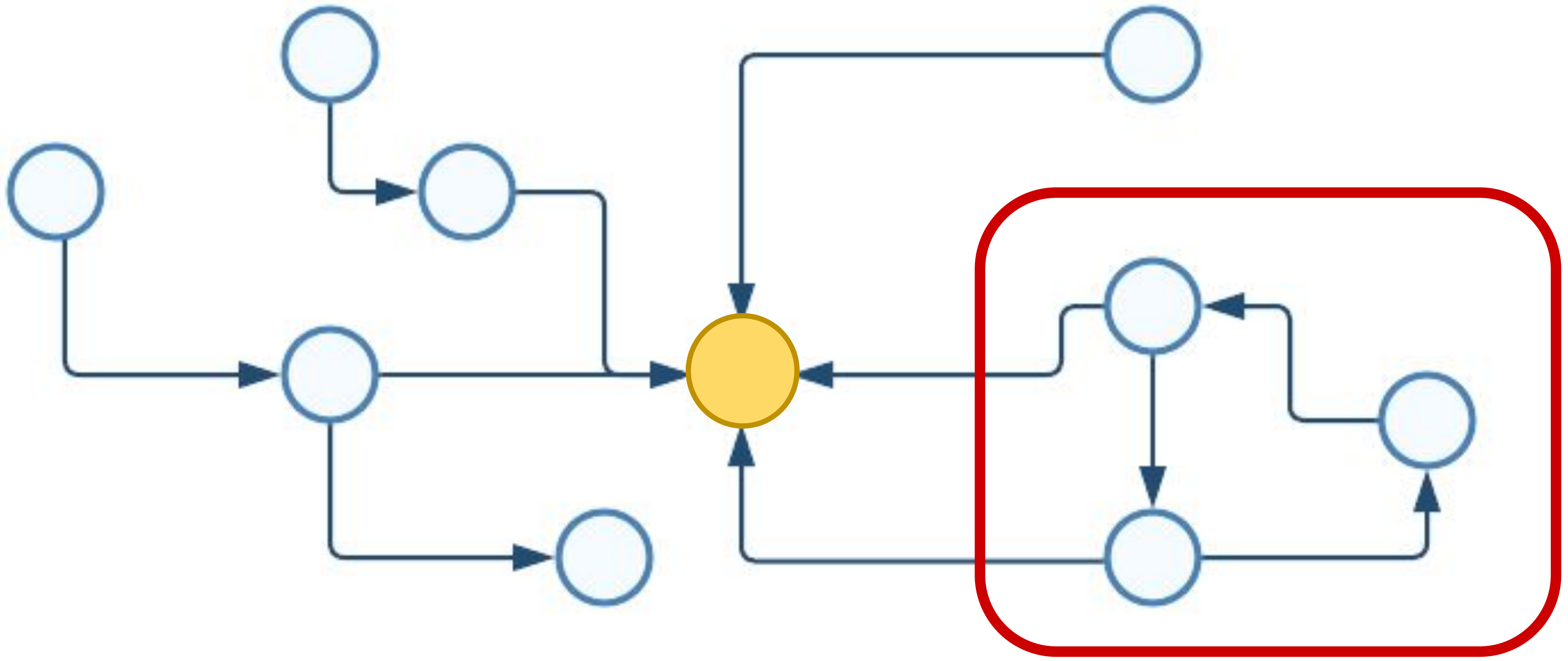
KindPNG

Network Verification

Create a network verification process that checks that the BGP protocol is running correctly, and new protocols are enacted correctly.

Internet Graph Information

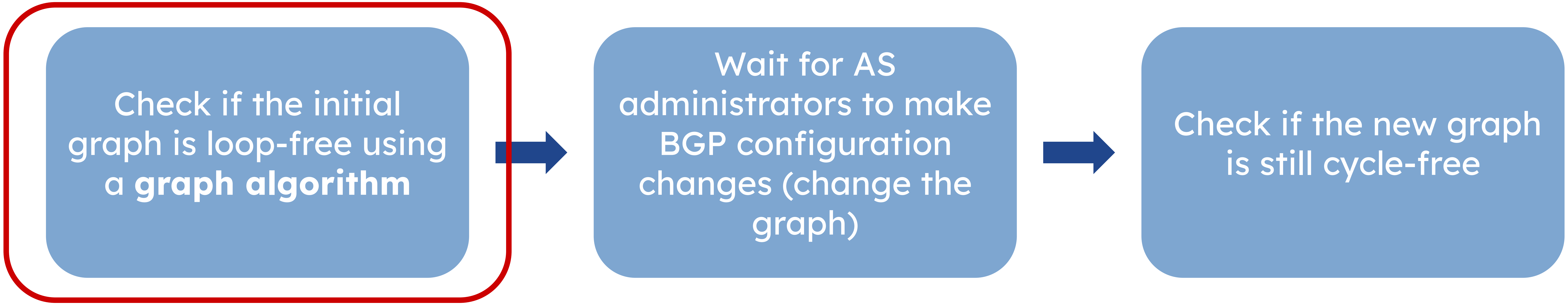
- We operate on **forwarding information base (FIB) table graph** with nodes and edges
  - Each node only points to one other node
  - All nodes should eventually lead to one **destination node**
  - Network should not contain loops



loop in network

Network Verification System Goals

- Create a network verification system that is
  - **efficient:** able to handle real-time processing and live updates
  - **privacy-preserving:** BGP policies and configurations are often private data due to security and commercial reasons
  - **scalable:** Internet networks are large and require scalability



Check if the initial graph is loop-free using a **graph algorithm**

Wait for AS administrators to make BGP configuration changes (change the graph)

Check if the new graph is still cycle-free

Which graph algorithm do we use?

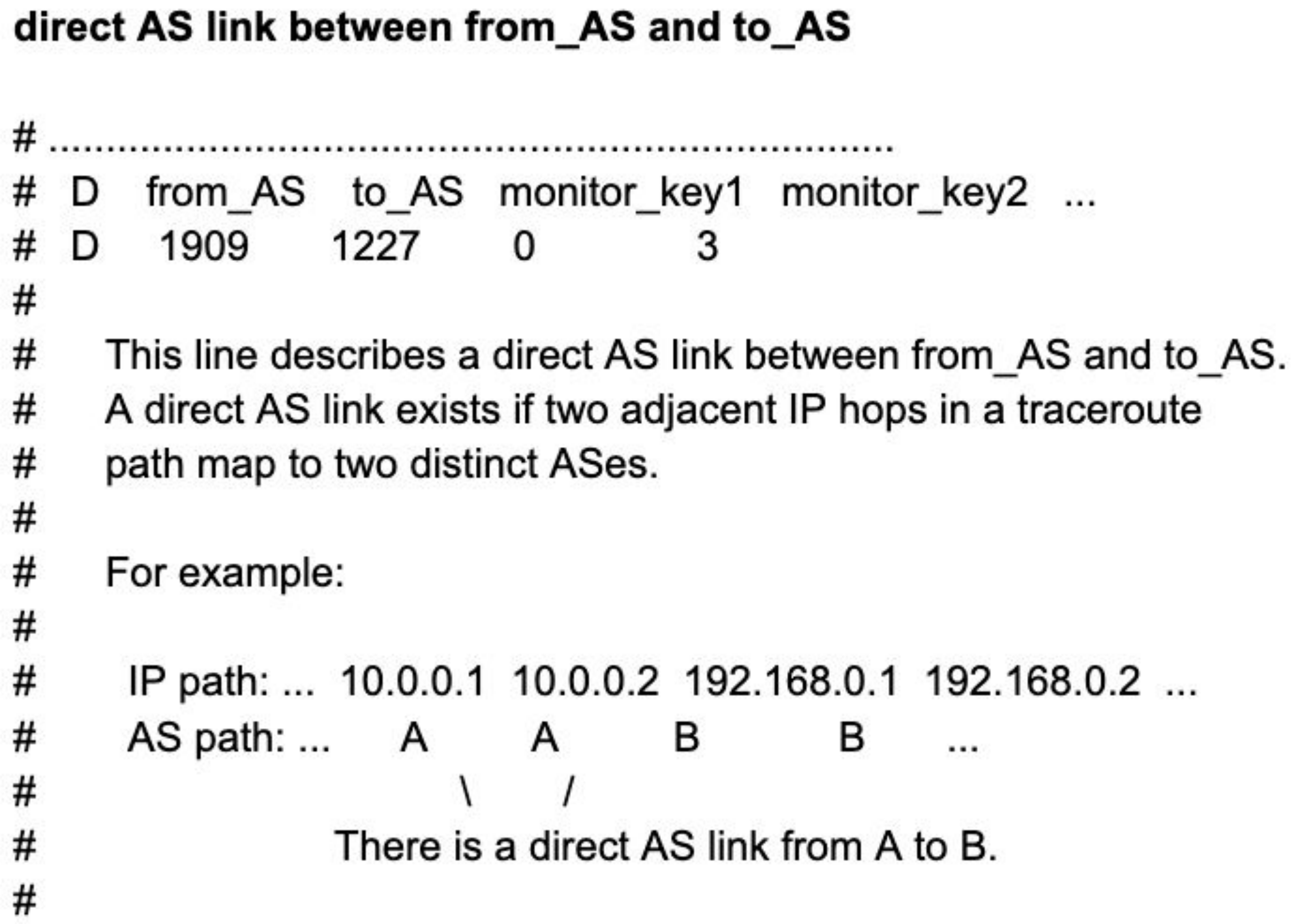
Find Most Efficient Graph Algorithm

- Implement graph algorithms modified to detect cycles
- Benchmark and compare graph algorithm speeds on different graphs
    - Testing for efficiency and scalability
    - Run each algorithm five times and take the average

Graph Algorithm	**Execution Time**
Breadth-First Search	?
Depth-First Search	?
Tarjan’s Algorithm	?
Topological Sort	?
Johnson’s Algorithm	?
Disjoint-Set Union	?

Dataset Pre-Processing

- Pre-process data (CAIDA) and use to create graphs to test algorithms on
- Types of graphs:
  - AS-link graphs (regular graphs) with few nodes and edges to test scalability
  - **forwarding information base (FIB) table graph** as the desired type of graph



direct AS link between from_AS and to_AS

```
# ..........................................................................
#  D    from_AS    to_AS   monitor_key1   monitor_key2   ...
#  D     1909       1227       0              3
#
#     This line describes a direct AS link between from_AS and to_AS.
#     A direct AS link exists if two adjacent IP hops in a traceroute
#     path map to two distinct ASes.
#
#     For example:
#
#       IP path: ...  10.0.0.1  10.0.0.2  192.168.0.1  192.168.0.2  ...
#       AS path: ...      A         A          B            B       ...
#                                    \        /
#                         There is a direct AS link from A to B.
#
```

Dataset from Center for Applied Internet Data Analysis (CAIDA): IPv4 Routed /24 AS Links Dataset

Graph Algorithm Benchmarking

	Nodes	Edges	BFS	DFS	Topology	Tarjan’s	DSU	Johnson
AS Link 1	280	1384	0.0019	0.0011	0.0015	0.0015	0.0572	0.8426
AS Link 2	1421	5500	0.0063	0.0054	0.0067	0.0071	0.0459	0.7315
FIB 1	25061	25066	0.0197	0.0409	0.0686	0.0666	0.0744	22.2109
FIB 2	25061	25089	0.0255	0.0542	0.0637	0.0718	0.0806	21.8804
FIB 3	25061	25071	0.0232	0.0486	0.0588	0.0686	0.1108	22.4681
FIB 4	25061	25067	0.0234	0.0426	0.0619	0.0732	0.0887	22.7568
FIB 5	25061	25079	0.0238	0.0519	0.0664	0.0729	0.0850	22.0689

Graph Algorithm Benchmarking

	Nodes	Edges	BFS	DFS
AS Link 1	280	1384	0.0019	0.0011
AS Link 2	1421	5500	0.0063	0.0054
FIB 1	25061	25066	0.0197	0.0409
FIB 2	25061	25089	0.0255	0.0542
FIB 3	25061	25071	0.0232	0.0486
FIB 4	25061	25067	0.0234	0.0426
FIB 5	25061	25079	0.0238	0.0519

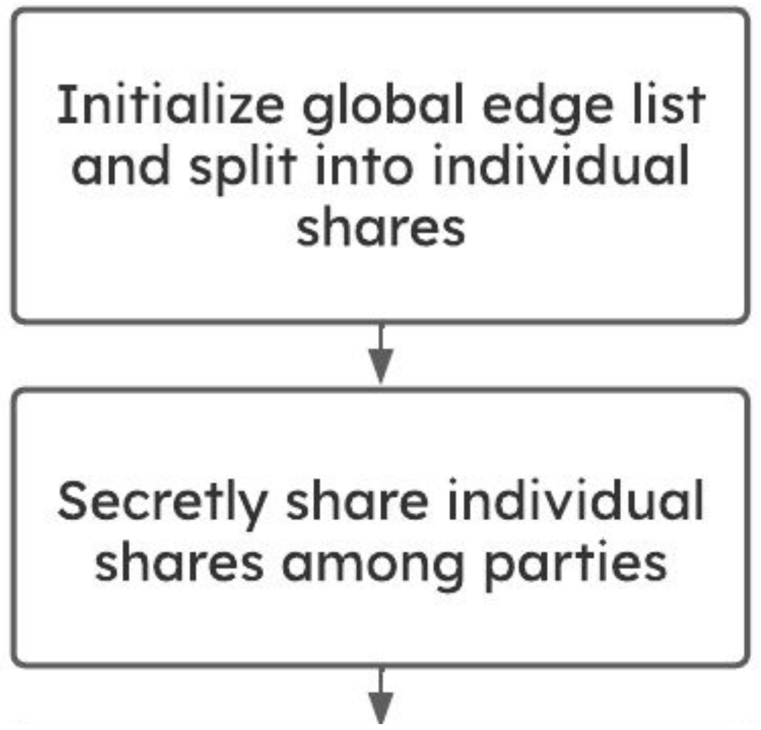
Fastest two algorithms

- Depth-first search is faster in the AS-link graph but breadth-first search is faster on FIB graphs
- FIB graphs are actually used in network verification system
- We choose **breadth-first search** for our network verification system

Proposed Network Verification System

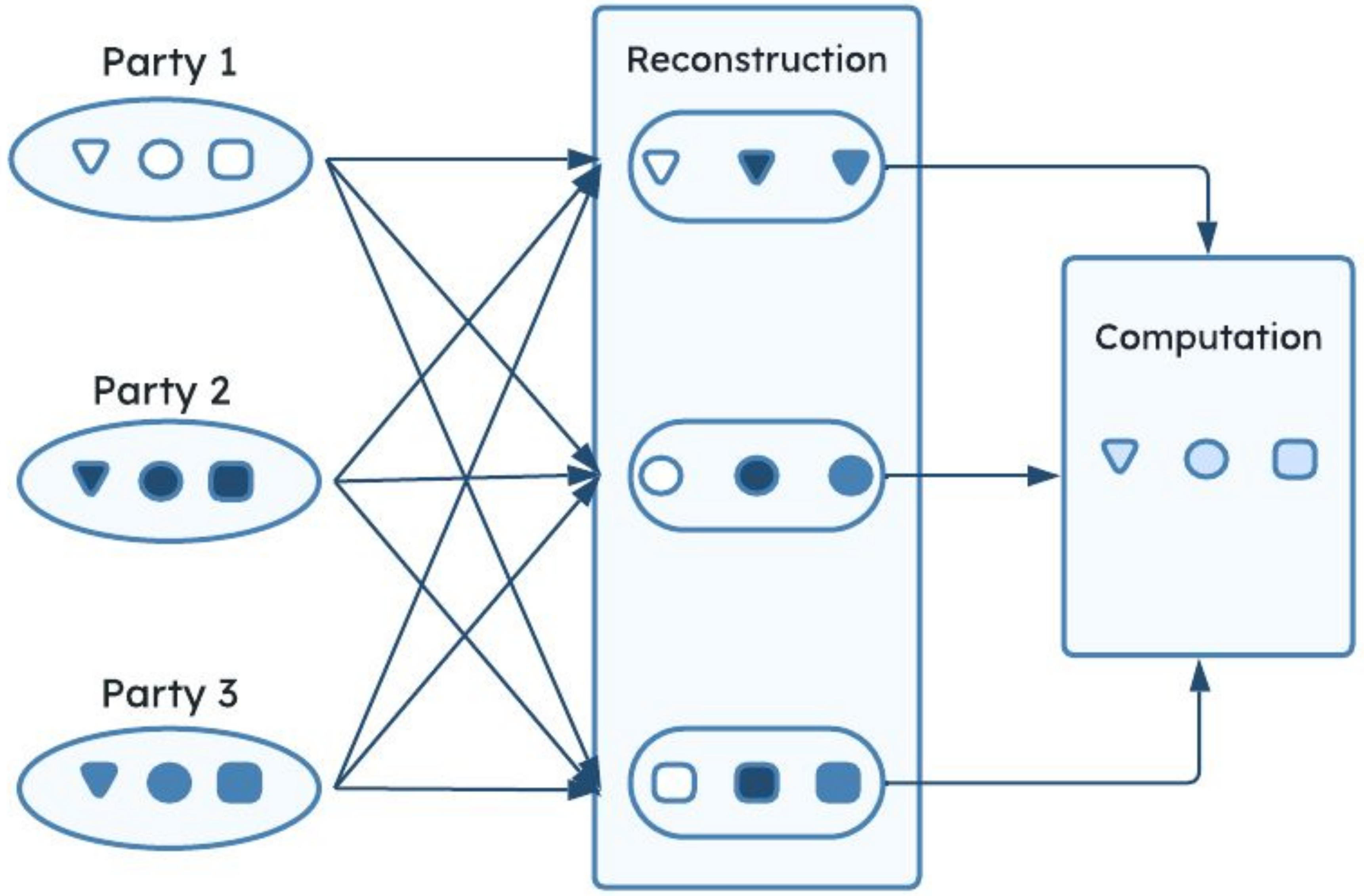
Combine graph algorithm with **multi-party computation**

- Implemented through the SCALE-MAMBA framework
- Allow multiple parties with private inputs to compute together without revealing all graph to one party



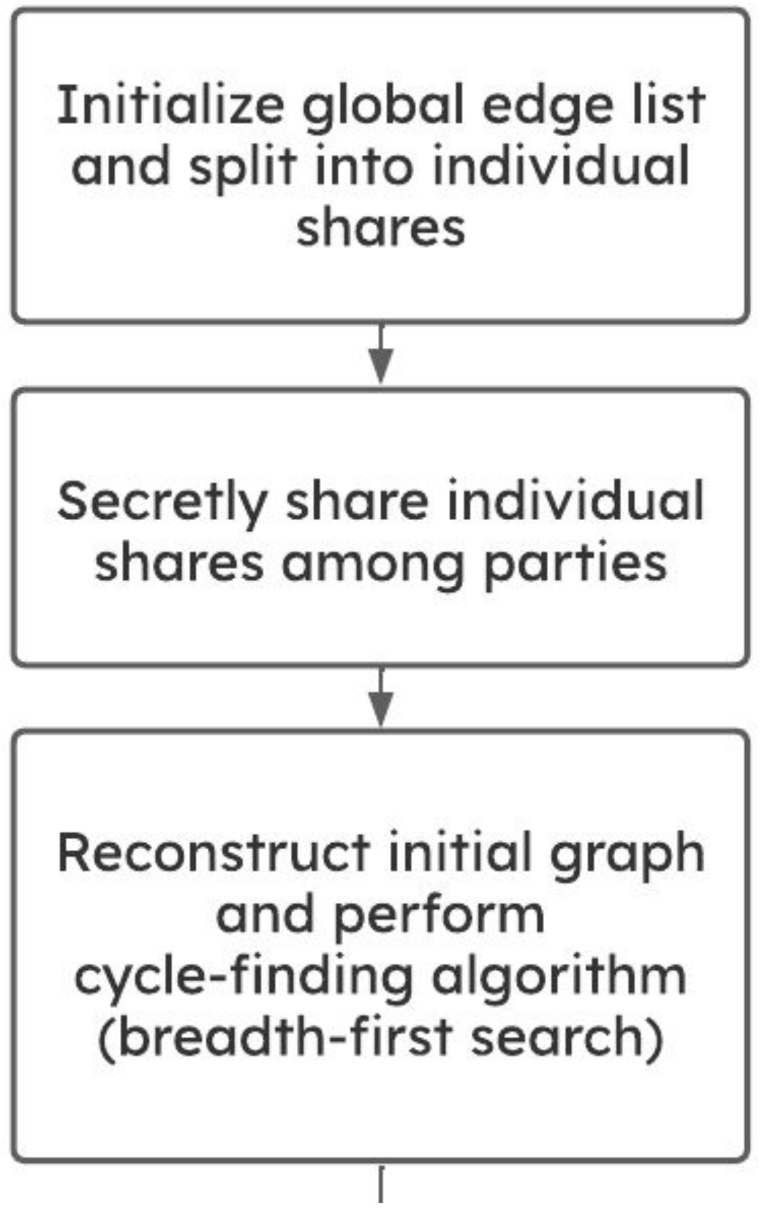
Initialize global edge list and split into individual shares

Secretly share individual shares among parties



Proposed Network Verification System

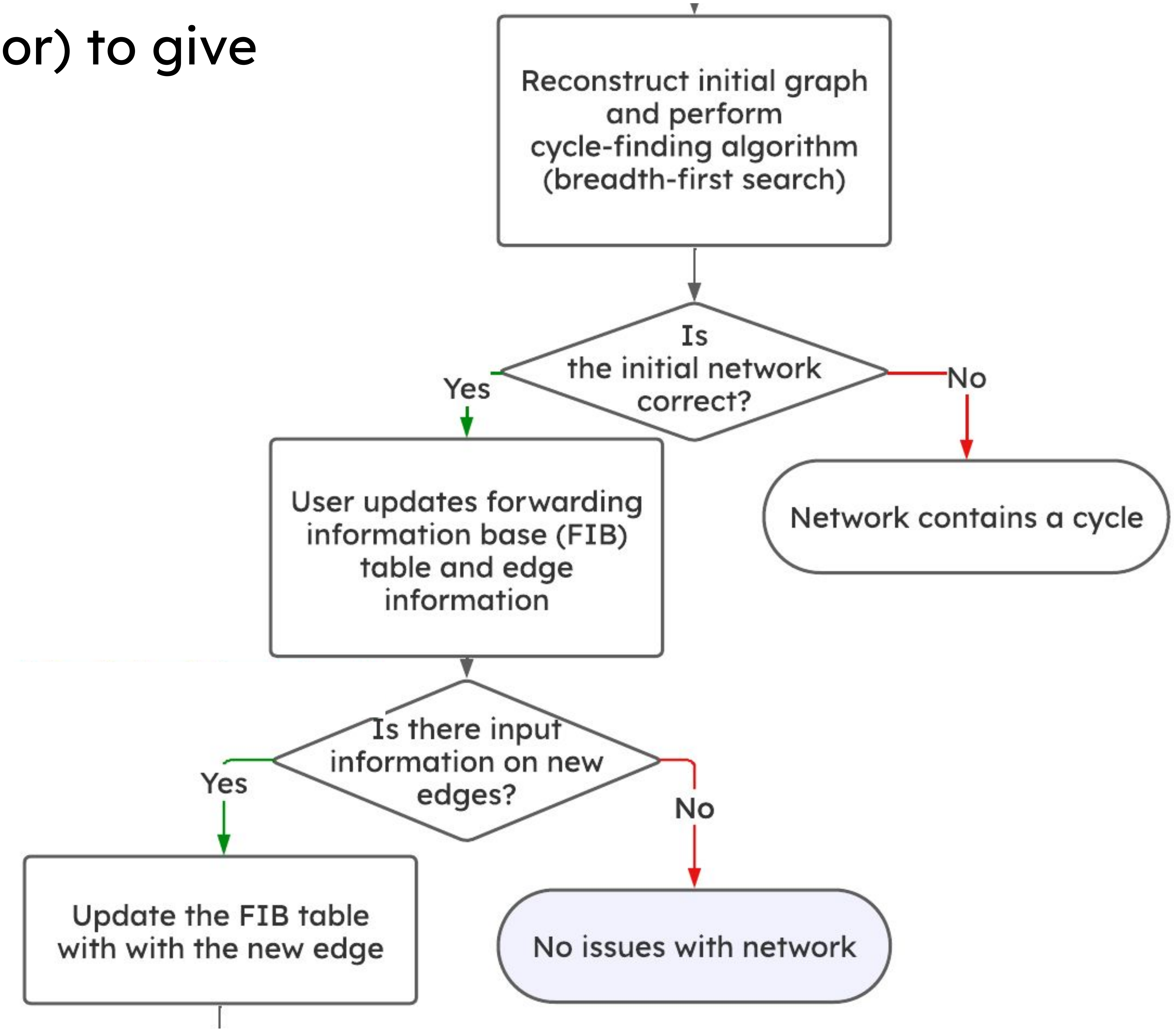
Use loop detection algorithm (**breadth-first search)** to determine if the original graph has errors


Initialize global edge list and split into individual shares
Secretly share individual shares among parties
Reconstruct initial graph and perform cycle-finding algorithm (breadth-first search)

Proposed Network Verification System

If there are no errors, wait for the user (AS administrator) to give potential new information regarding FIB edge:

- In the format *(a, b)* where AS *a* now points to AS *b*
- Changes in the graph can create potential cycles


Reconstruct initial graph and perform cycle-finding algorithm (breadth-first search)
Is the initial network correct?
Yes
No
User updates forwarding information base (FIB) table and edge information
Network contains a cycle
Is there input information on new edges?
Yes
No
Update the FIB table with with the new edge
No issues with network

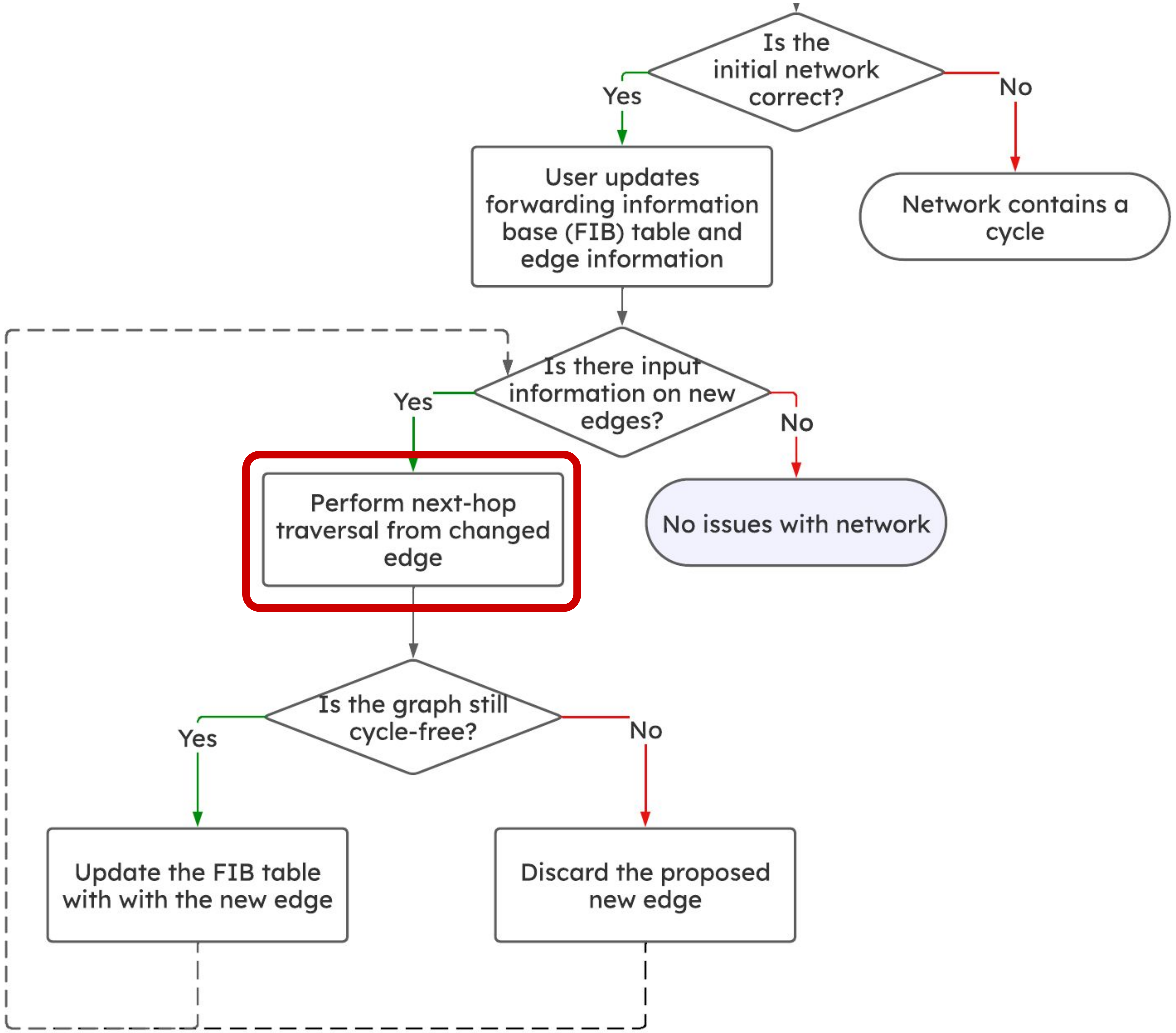
Proposed Network Verification System

Perform next-hop traversal from new edge

- Edge changes only affect nodes directly connected to the edge
- Only reconstruct the edges of nodes directly connected to the changed protocol
- Taken from the individual shares from separate parties and re-aggregate

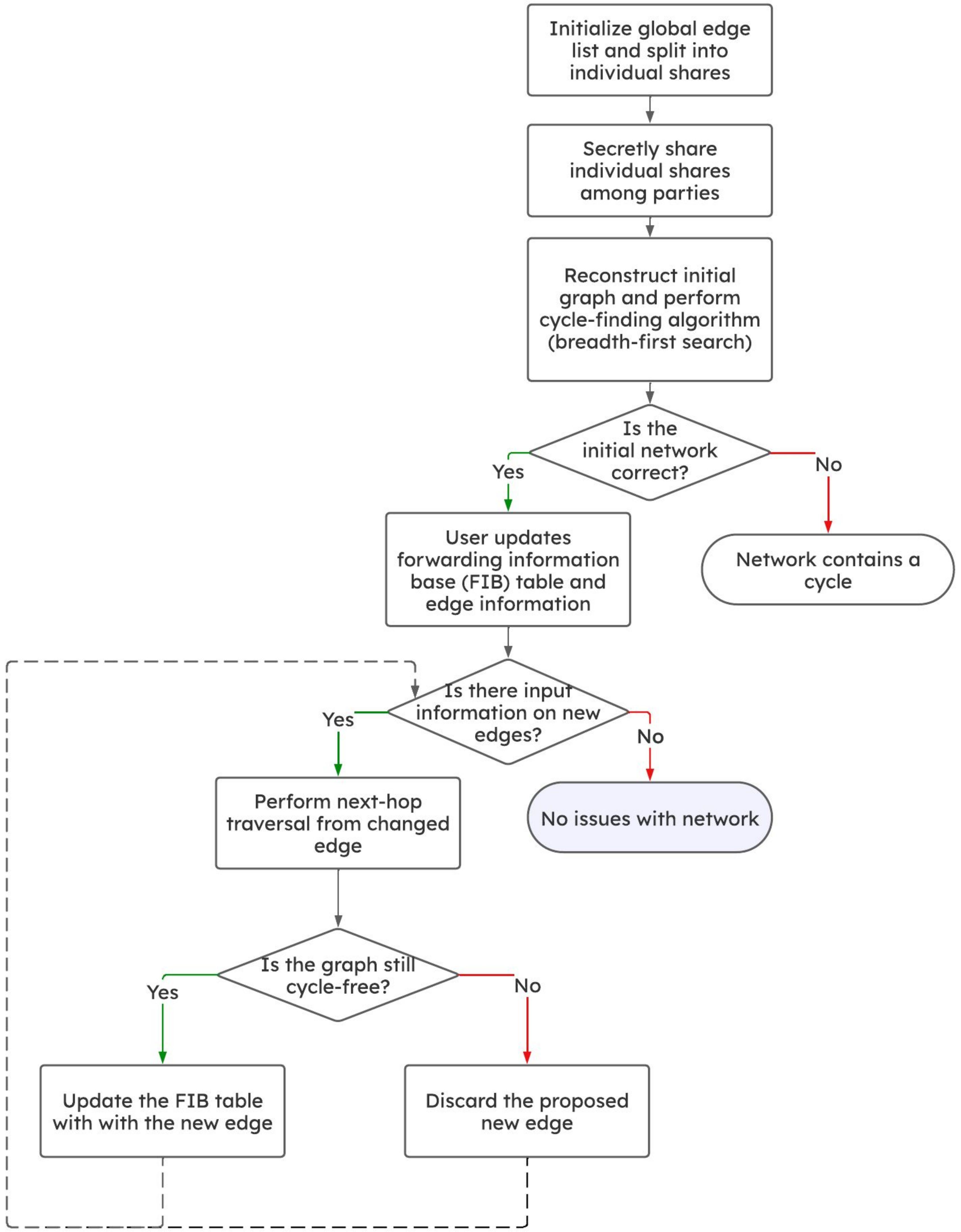
- Follow the next-hop values until

  1. Reach a node we already visited
  2. Reach 15 hops
  3. Reach destination node


Is the initial network correct?
Yes
No
User updates forwarding information base (FIB) table and edge information
Network contains a cycle
Is there input information on new edges?
Yes
No
Perform next-hop traversal from changed edge
No issues with network
Is the graph still cycle-free?
Yes
No
Update the FIB table with with the new edge
Discard the proposed new edge

Conclusion

- As Internet infrastructures grow in scale and complexity, network verification is more important
- We create a network verification system that is efficient, privacy-preserving, and scalable
    - Utilizing **breadth-first search** as our initial cycle-finding algorithm
    - Checking for cycles after an AS administrator changes an edge
- Future direction: find more privacy-preserving techniques i.e. using different multi-party computation framework


Initialize global edge list and split into individual shares
Secretly share individual shares among parties
Reconstruct initial graph and perform cycle-finding algorithm (breadth-first search)
Is the initial network correct?
Yes
No
User updates forwarding information base (FIB) table and edge information
Network contains a cycle
Is there input information on new edges?
Yes
No
Perform next-hop traversal from changed edge
No issues with network
Is the graph still cycle-free?
Yes
No
Update the FIB table with with the new edge
Discard the proposed new edge

Acknowledgements

- Jaber Daneshamooz
- Dr. Lina Kim
- Zheng Ke
- Sucheer Maddury

References

[1] Rekhter, Y., Li, T., & Hares, S. (2006). A Border Gateway Protocol 4 (BGP-4). RFC 4271.

[2] Griffin, T. G., & Wilfong, G. T. (1999). An Analysis of BGP Convergence Properties. IEEE/ACM Transactions on Networking, 7(6), 841-853. doi:10.1109/90.811436

[3] Morris, "Facebook's outage cost the company nearly $100 million in revenue," Fortune, October 4, 2021. [Online]. Available: https://fortune.com/2021/10/04/facebook-outage-cost-revenue-instagram-whatsapp-not-working-stock/.

[4]Ponemon Institute. (2016). Cost of Data Center Outages. [Online]. Available: https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf. Accessed: July 15 2023.

[5] M. Blanton, A. Steele, and M. Alisagari, "Data-oblivious graph algorithms for secure computation and outsourcing," in Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (ASIA CCS '13), May 2013, pp. 207-218.

[6] Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," Journal of Privacy and Confidentiality, vol. 1, no. 1, pp. 59-98, 2009.

[7] Moreno-Sanchez, Pedro & Kate, Aniket & Maffei, Matteo & Pecina, Kim. (2015). Privacy Preserving Payments in Credit Networks. 10.14722/ndss.2015.23284.

[8] The IPv4 Routed /24 AS Links Dataset - <June 24, 2023 - August 5, 2023>, https://www.caida.org/catalog/datasets/ipv4_routed_topology_aslinks_dataset/

[9] D. B. Johnson, "Efficient algorithms for shortest paths in sparse networks," Journal of the ACM, vol. 24, no. 1, pp. 1-13, 1977

[10] Robert W. Floyd. 1962. Algorithm 97: Shortest path. Commun. ACM 5, 6 (1962), 345. https://dl.acm.org/doi/10.1145/367766.368168

[11] R. E. Tarjan, "Depth-first search and linear graph algorithms," SIAM Journal on Computing, vol. 1, no. 2, pp. 146-160, 1972. doi: 10.1137/0201010

[12] Aly, A., Cong, K., Keller, M., Orsini, E., Rotaru, D., Scherer, O., Scholl, P., Smart, N.P., Tanguy, T., Wood, T.: SCALE and MAMBA v1.14: Documentation (2021) https://homes.esat.kuleuven.be/~nsmart/SCALE/.

[13] SCALE–MAMBA v1.14 : Documentation, https://homes.esat.kuleuven.be/~nsmart/SCALE/Documentation.pdf.