LARMix++: Latency-Aware Routing in Mix Networks with Free Routes Topology

Mahdi Rahimi

mahdi.rahimi@kuleuven.be

COSIC, KU Leuven, Belgium

23rd International Conference on Cryptology And Network Security (CANS)24th-27th September 2024

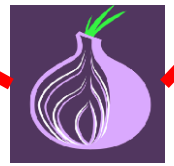
End users on the internet are not anonymized by default.

This creates privacy issues.

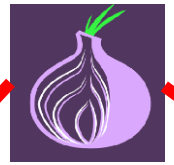
Tor Network

Client

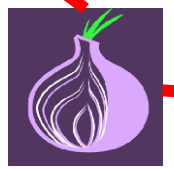
ISP1



Guard Relay



Middle Relay



Exit Relay

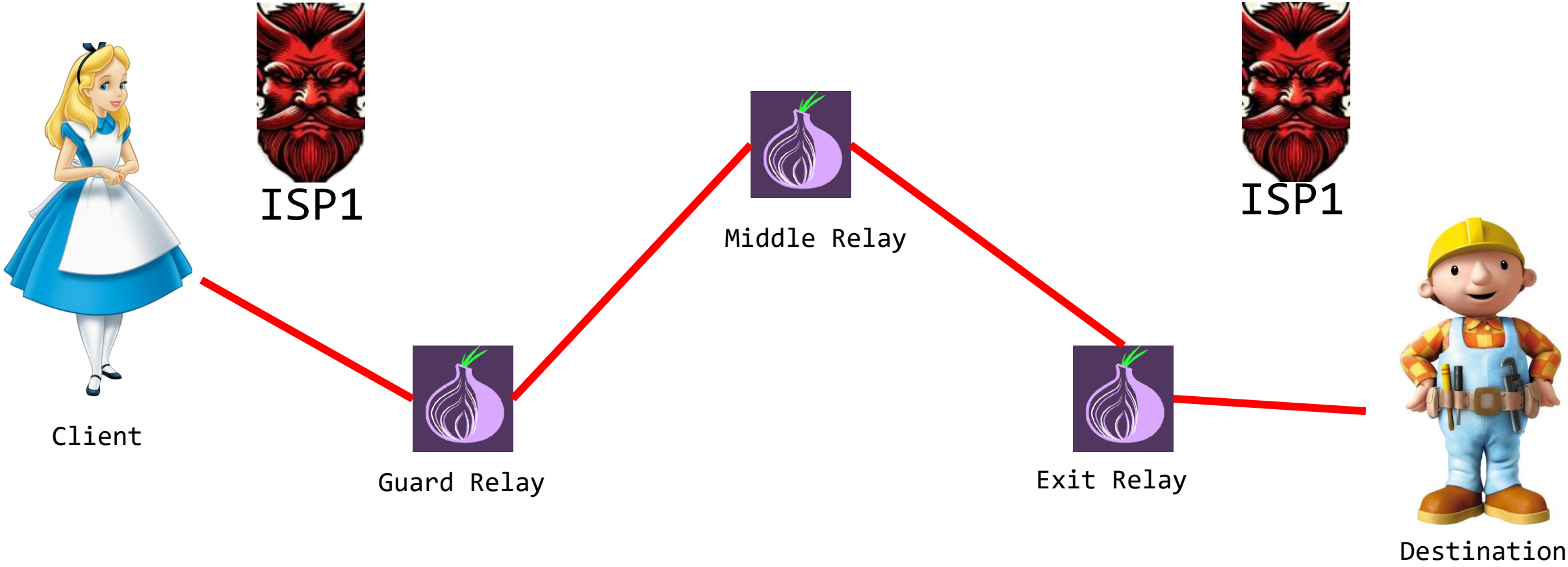
ISP2

Destination

ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

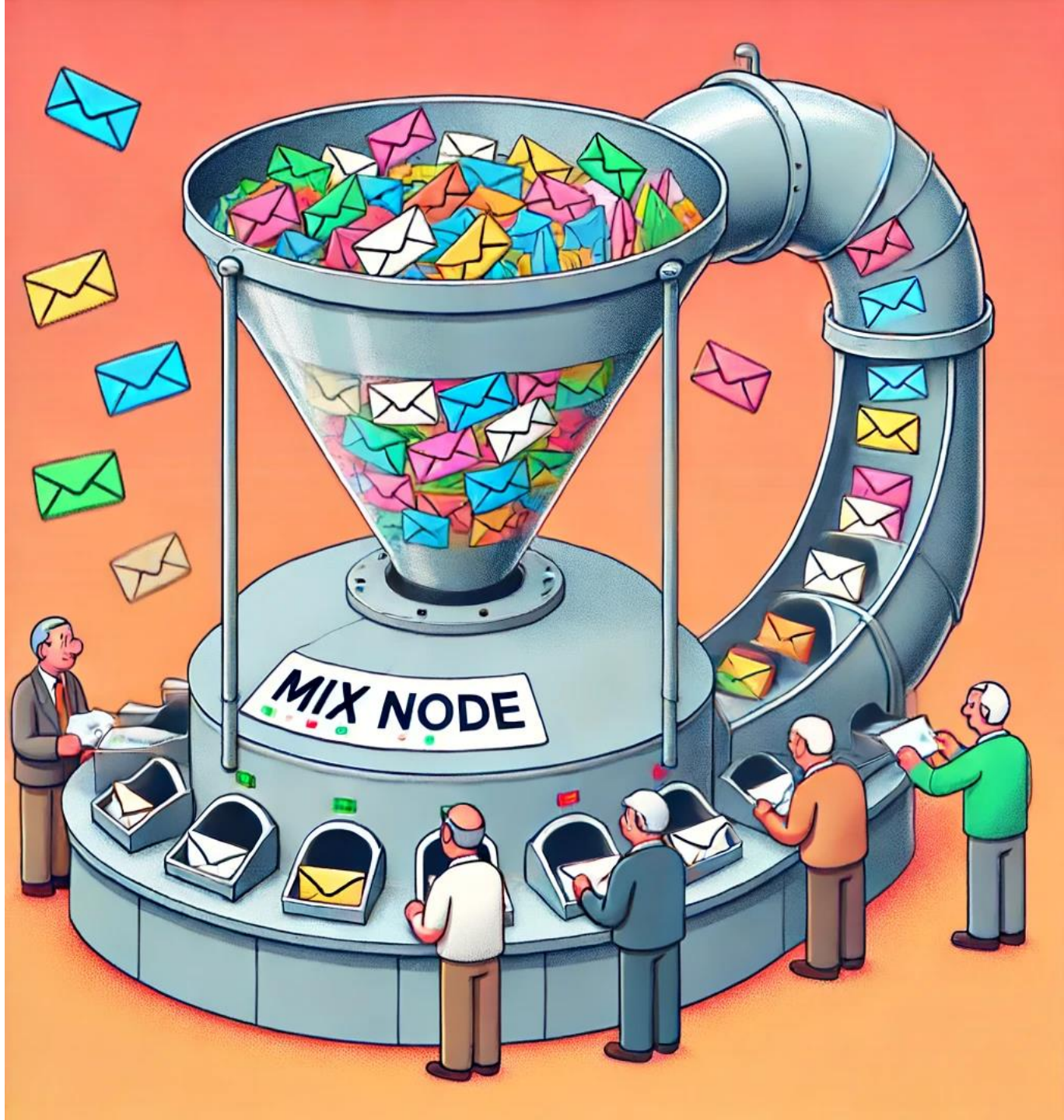
End-to-End Correlation Attacks



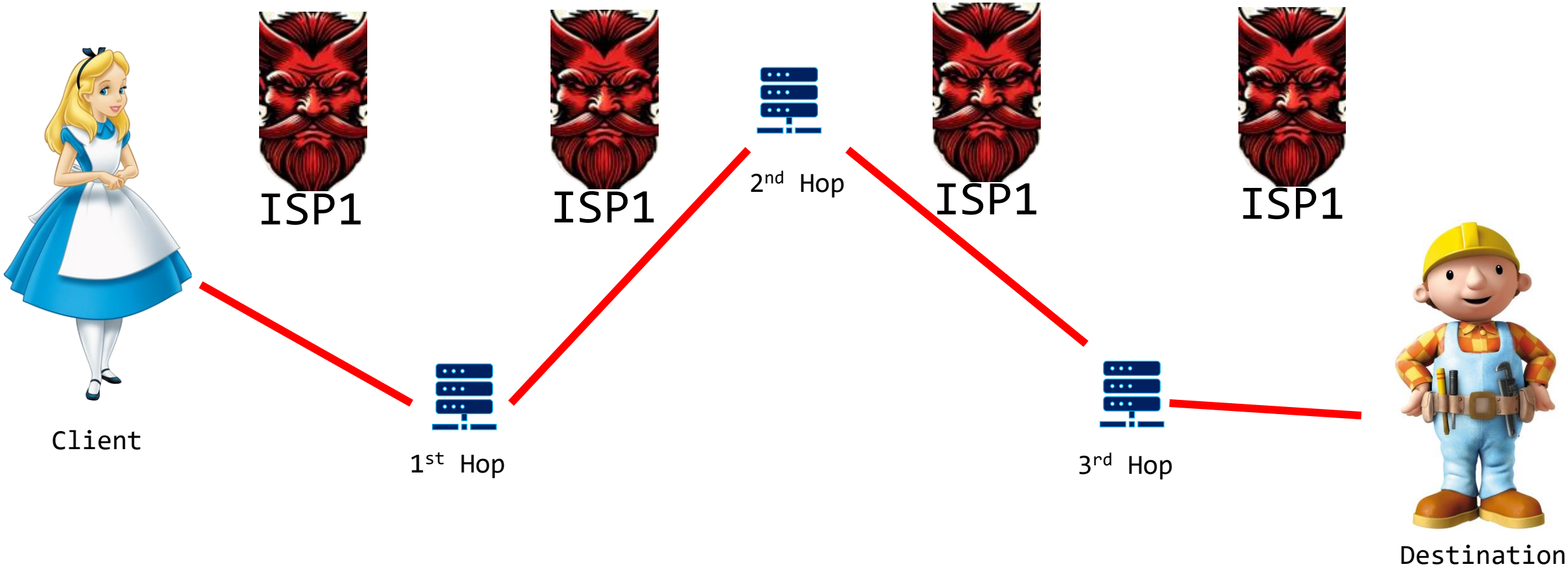
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

To have strong tools to provide anonymity, we can consider using mixnodes.

Mixnodes make their input and output unlinkable.

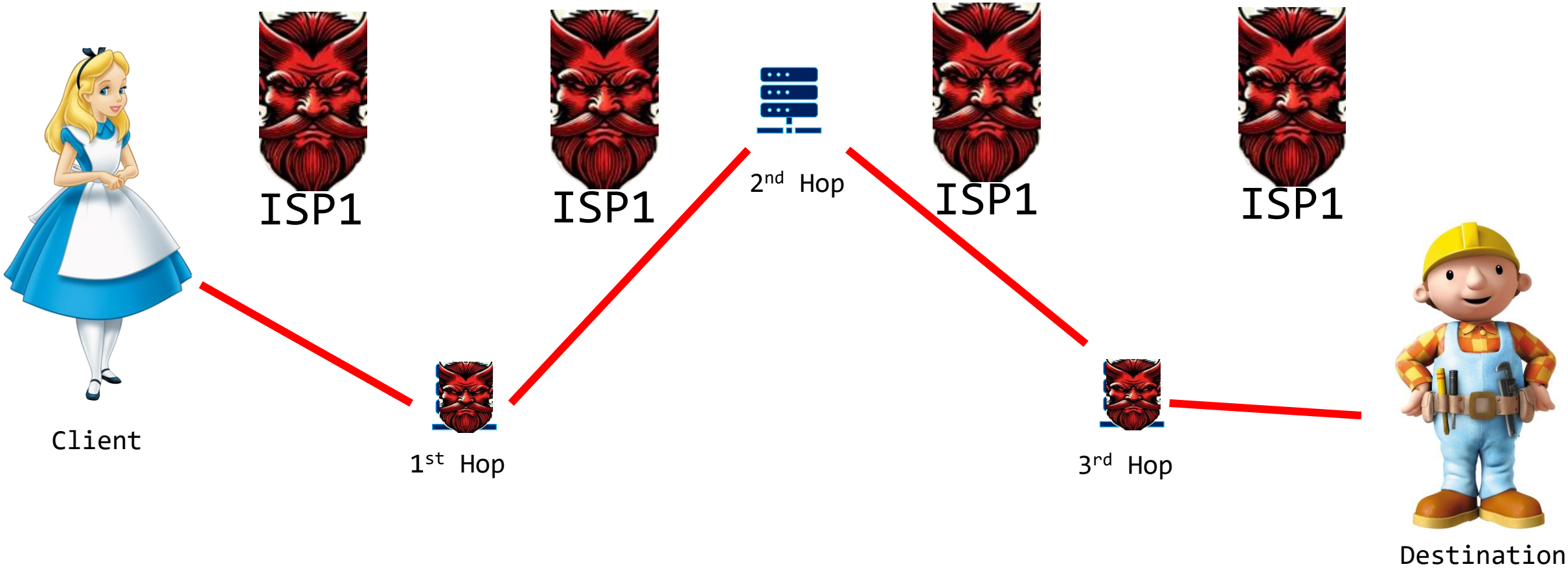


Mix Network(Mixnet)



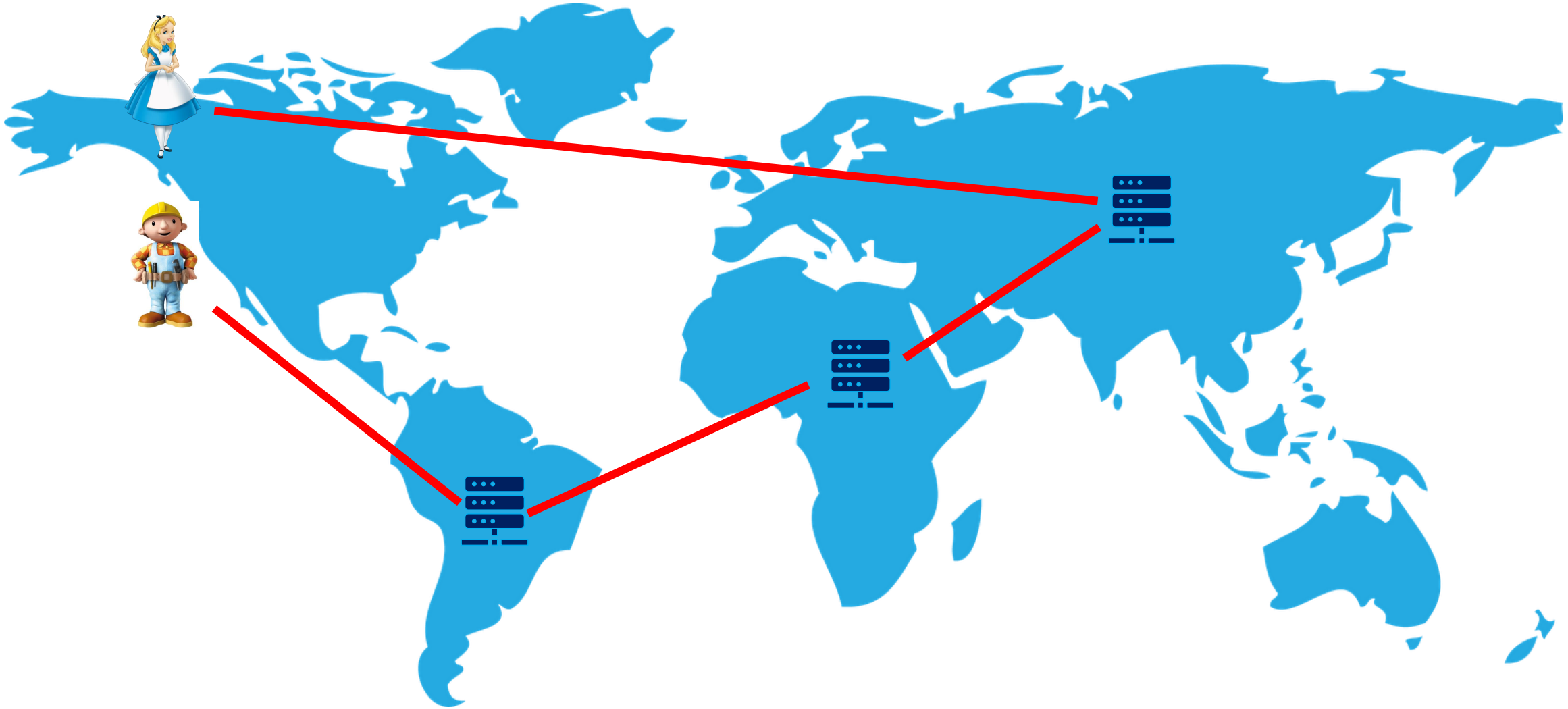
A mixnet is a network consisting of mixnodes, providing shuffling.

Anonymity Requirement



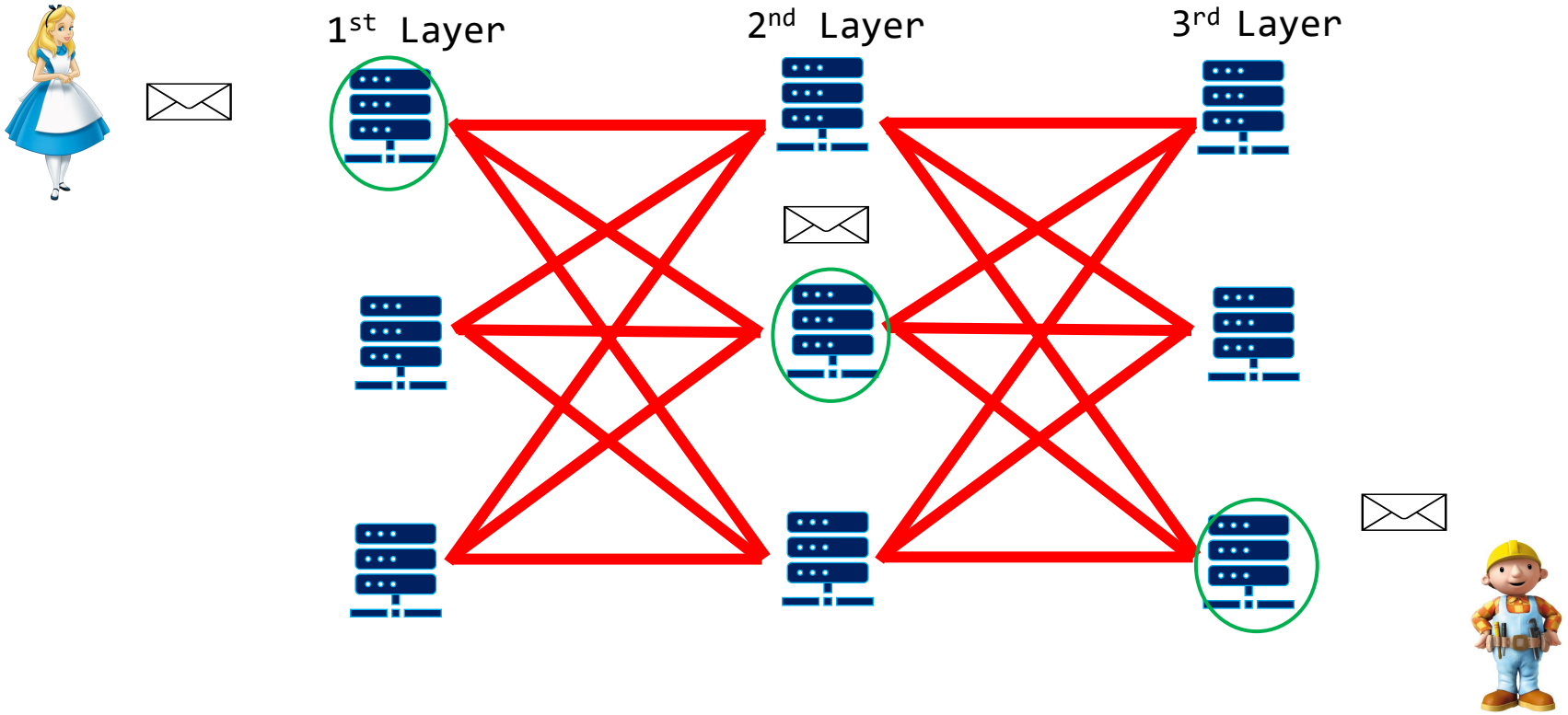
As long as one mixnode in the message route is honest, the client-destination connection will be anonymized.

End-to-End Latency



As a result of routing through intermediate mixnodes and intentional delays at each mixnode, the end-to-end latency is very high when using a mixnet.

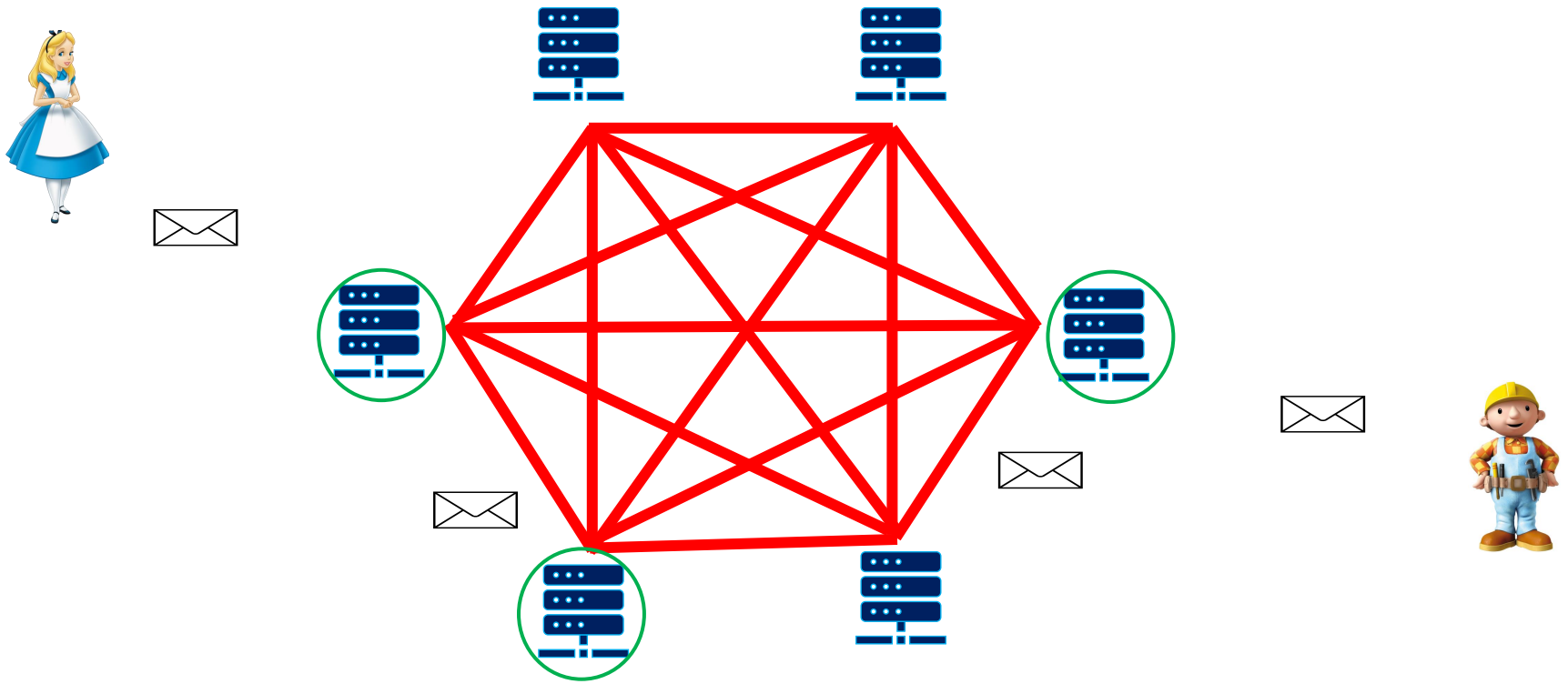
LARMix[1]



LARMix provides low-latency routing for mixnets with layered structures, which require an additional process to arrange nodes in layers.

1: **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

LARMix++

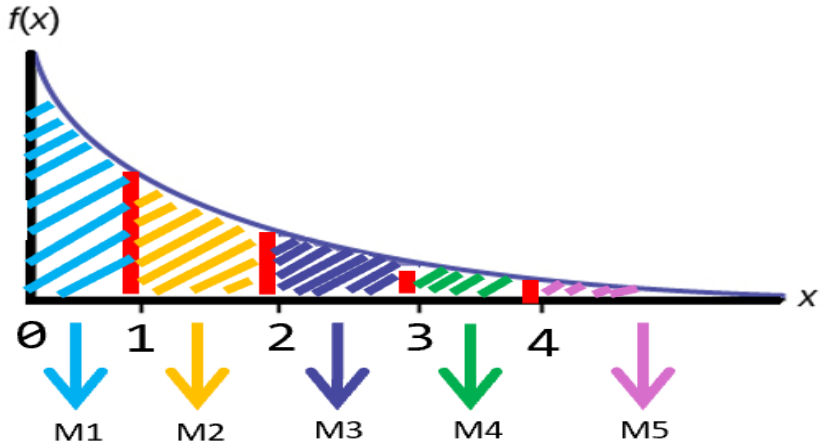


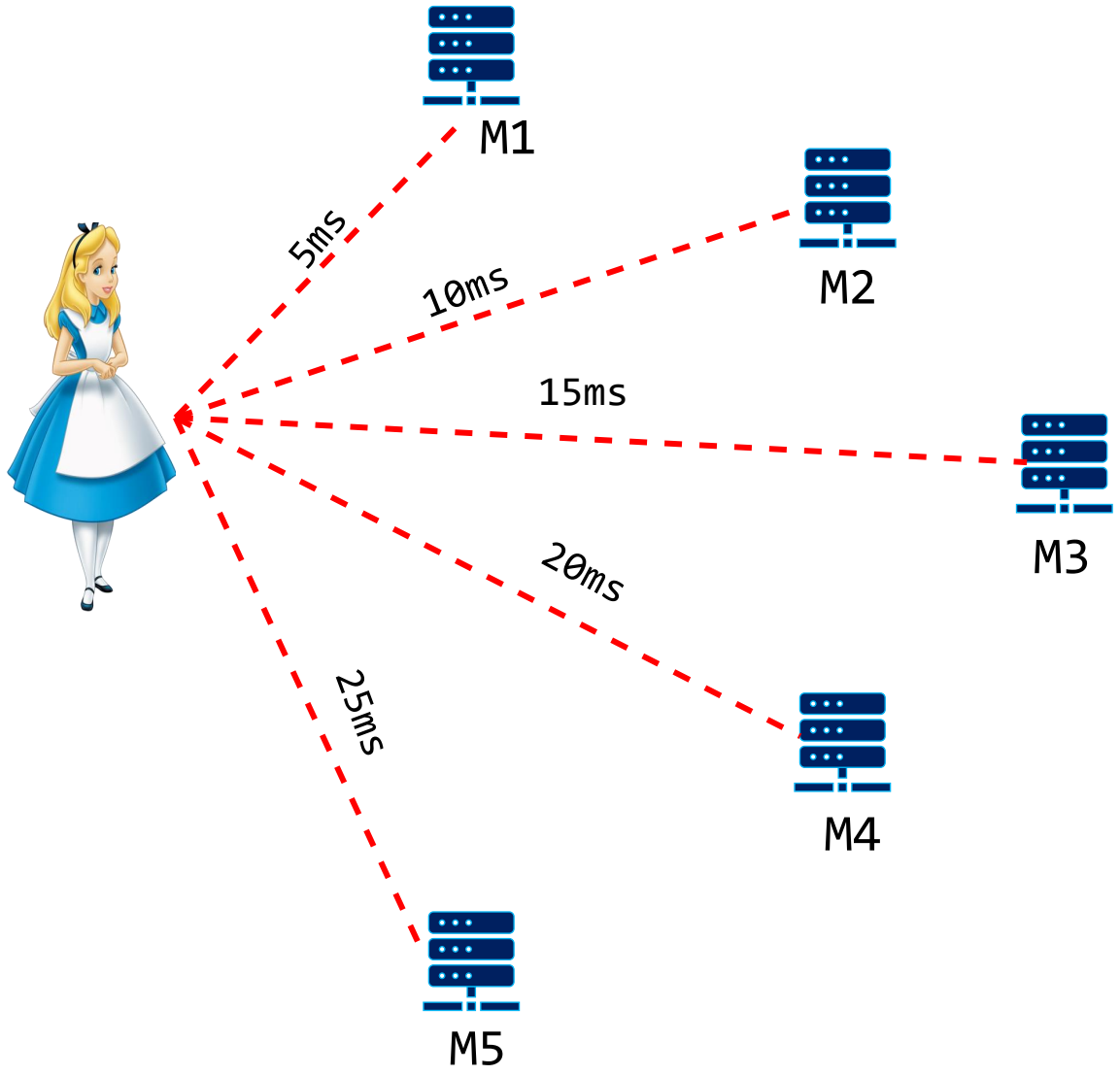
Free Routes topologies, on the other hand, do not impose any restrictions on nodes’ connections.

Routing Strategies

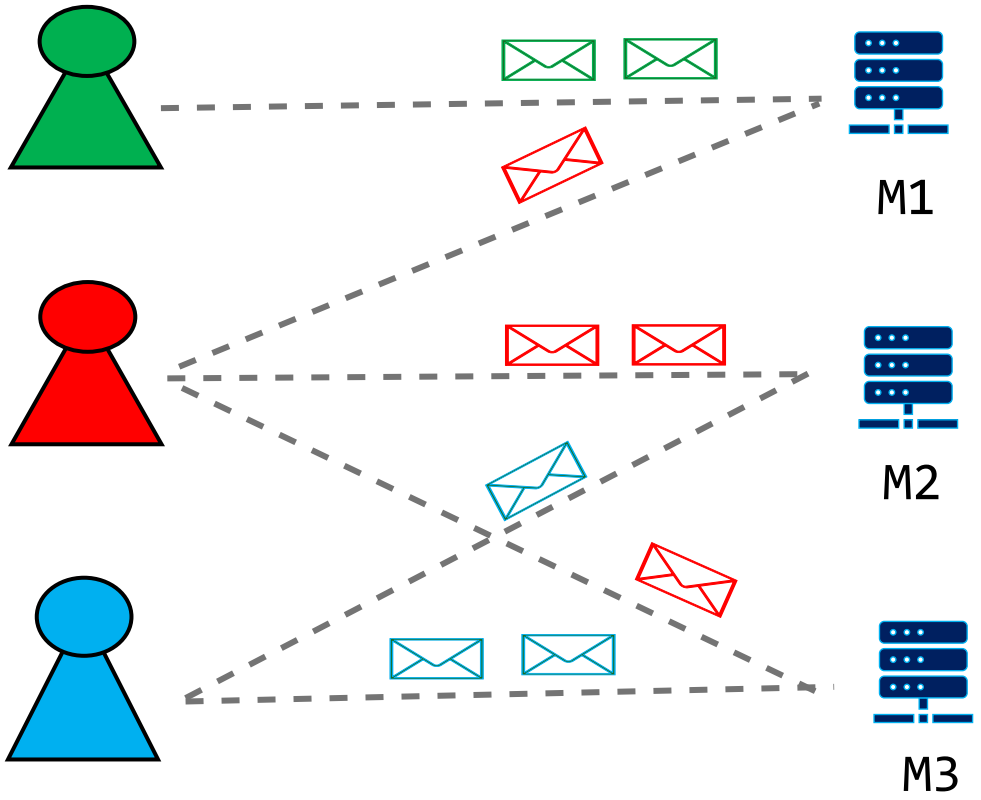
Select low-latency links with high probability.

Select the remaining nodes with low probability.



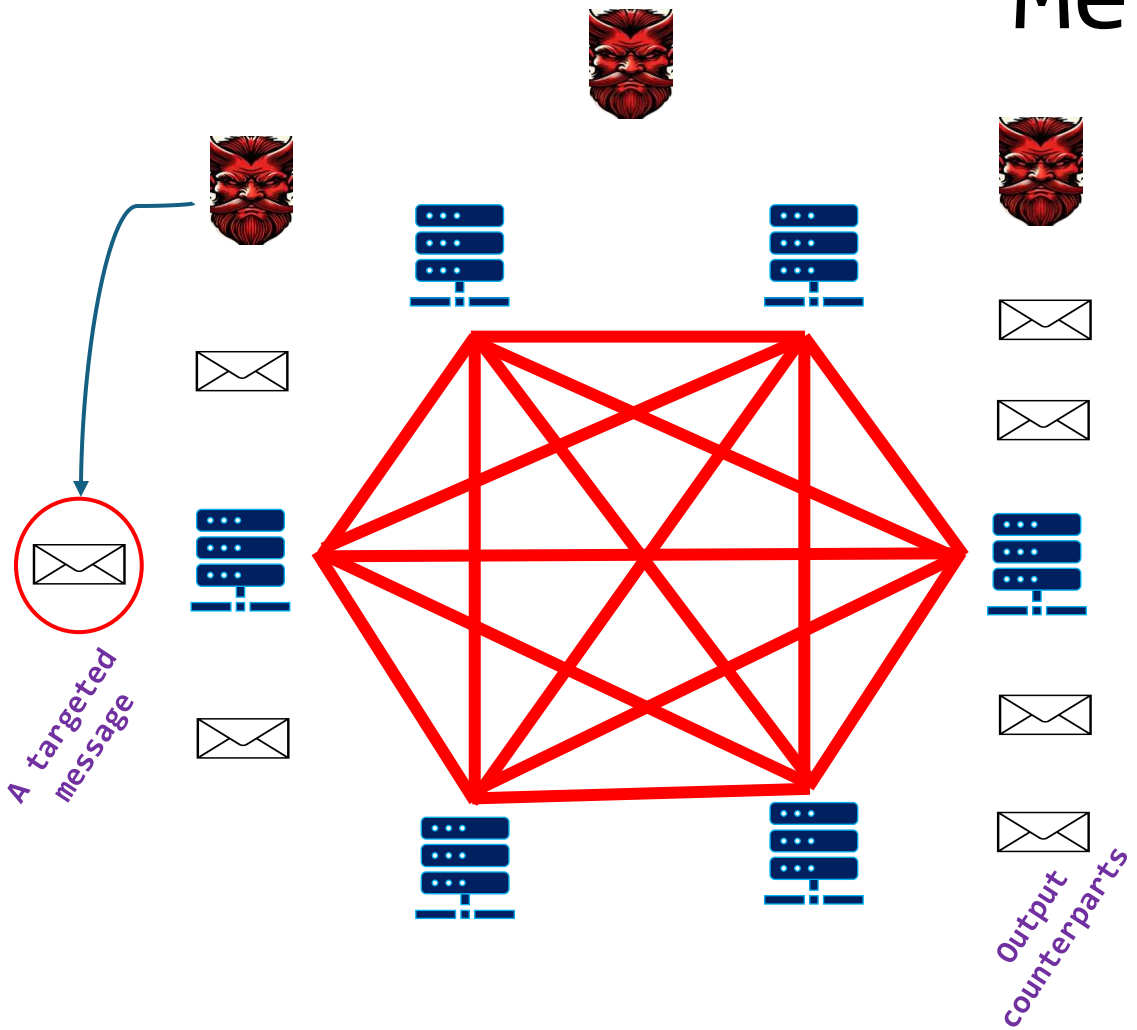


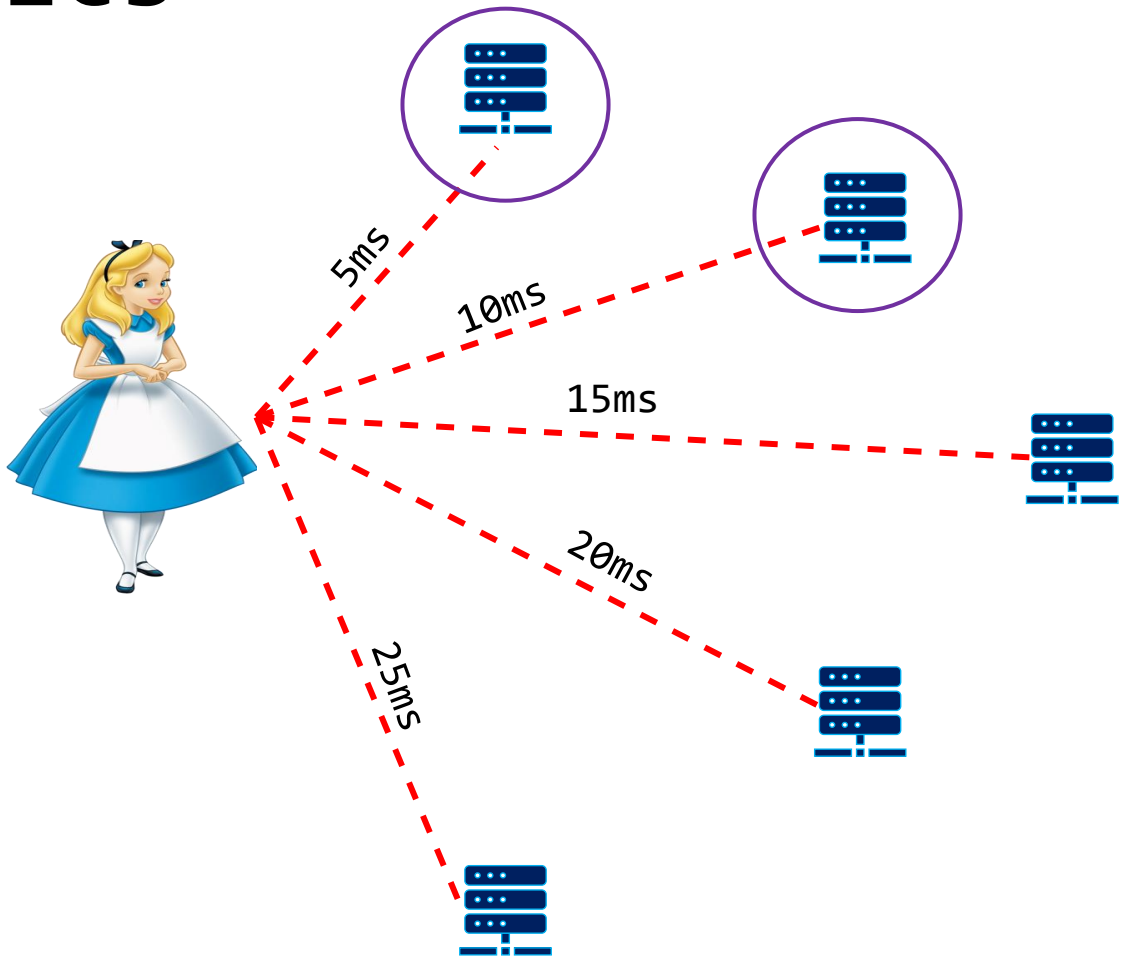
Load balancing the nodes



Load balancing algorithm ensures that mixnodes receive the same portion of traffic.

Metrics





Anonymity is quantified with the entropy of a targeted message distribution over the outgoing messages in the mixnet exit.

Average latency is useful for measuring the latency reduction.

Results

Routings \ Metrics	Latency	Entropy
Uniform	125 ms	12 bits
Strategic routing	50 ms	11.5 bits
Load balancing	75 ms	11.8 bits

LARMix++ gives a free hand to the client to make different trade-offs.

Conclusions

Hiding who communicates with whom is necessary on the Internet.

The Tor Network can reliably provide this anonymity but is vulnerable to traffic correlations.

Mixnet provides high degree of anonymity at the cost of high latency.

To reduce the high latency, we can use LARMix++ which improves the performance of mixnets by up to 60%.

Thank you for listening!

You can find the slides from this talk, along with other related papers and blog posts, on my webpage.

If you'd like to learn more about mix networks or anonymous communications, feel free to connect with me through LinkedIn.