)

# MALARIA: Management of Low-Latency Routing Impact on Mix Network Anonymity

**Mahdi Rahimi**

mahdi.rahimi@kuleuven.be

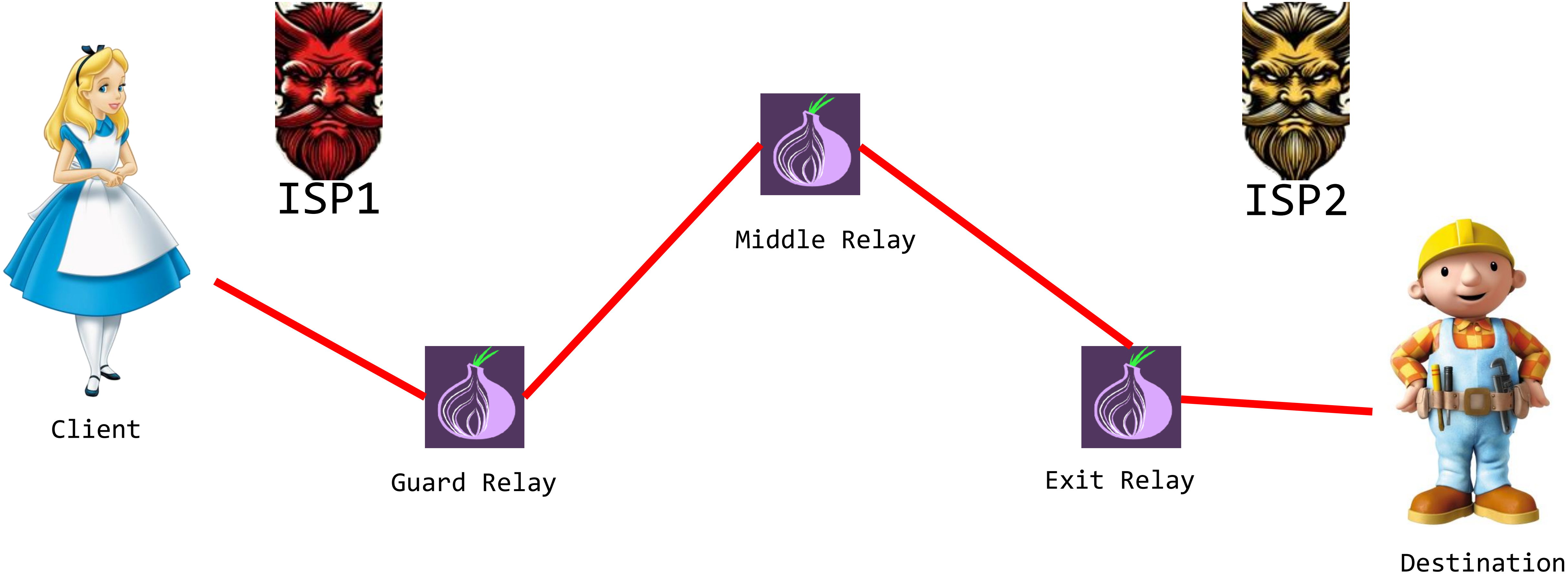
COSIC, KU Leuven, Belgium

The 22nd International Symposium on Network Computing and Applications (NCA 2024) 24th-26th October.

End users on the internet are not anonymized by default.

This creates privacy issues.

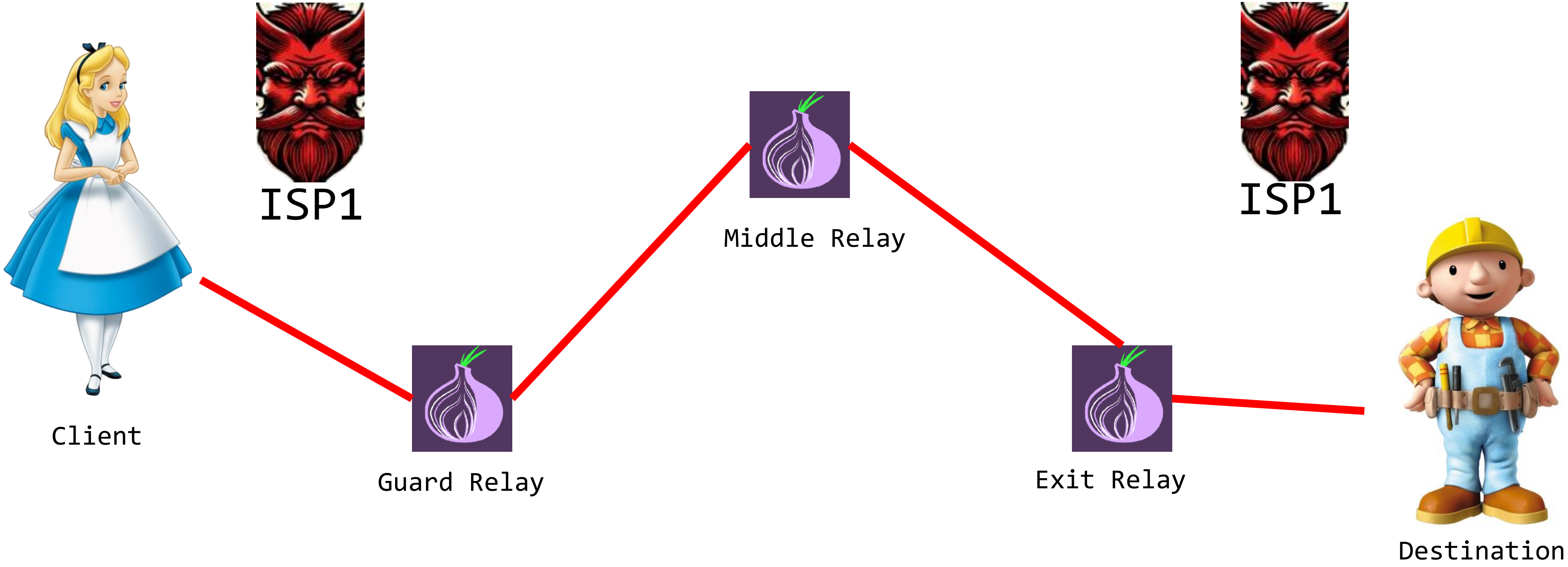
# Tor Network



ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

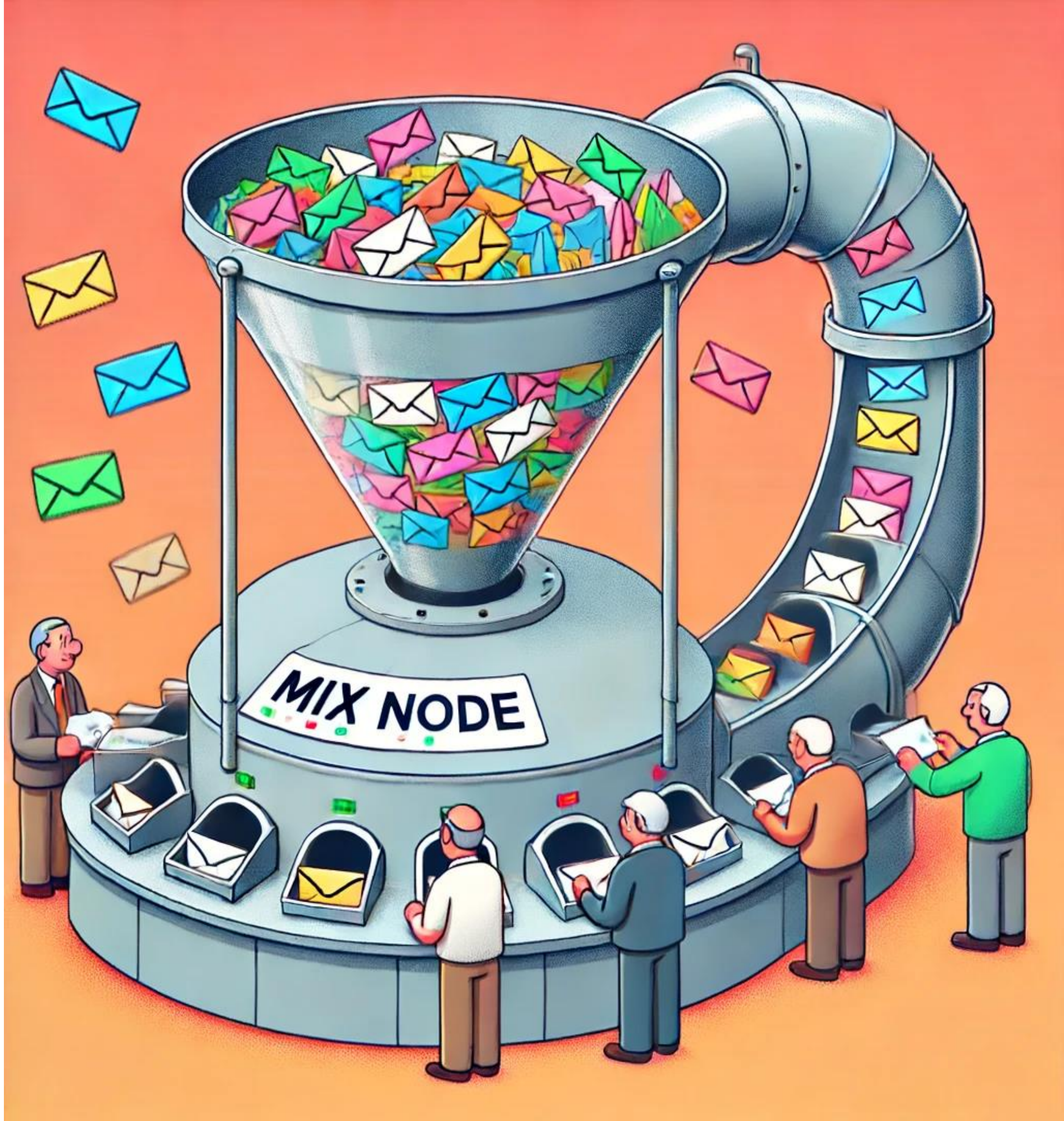
# End-to-End Correlation Attacks



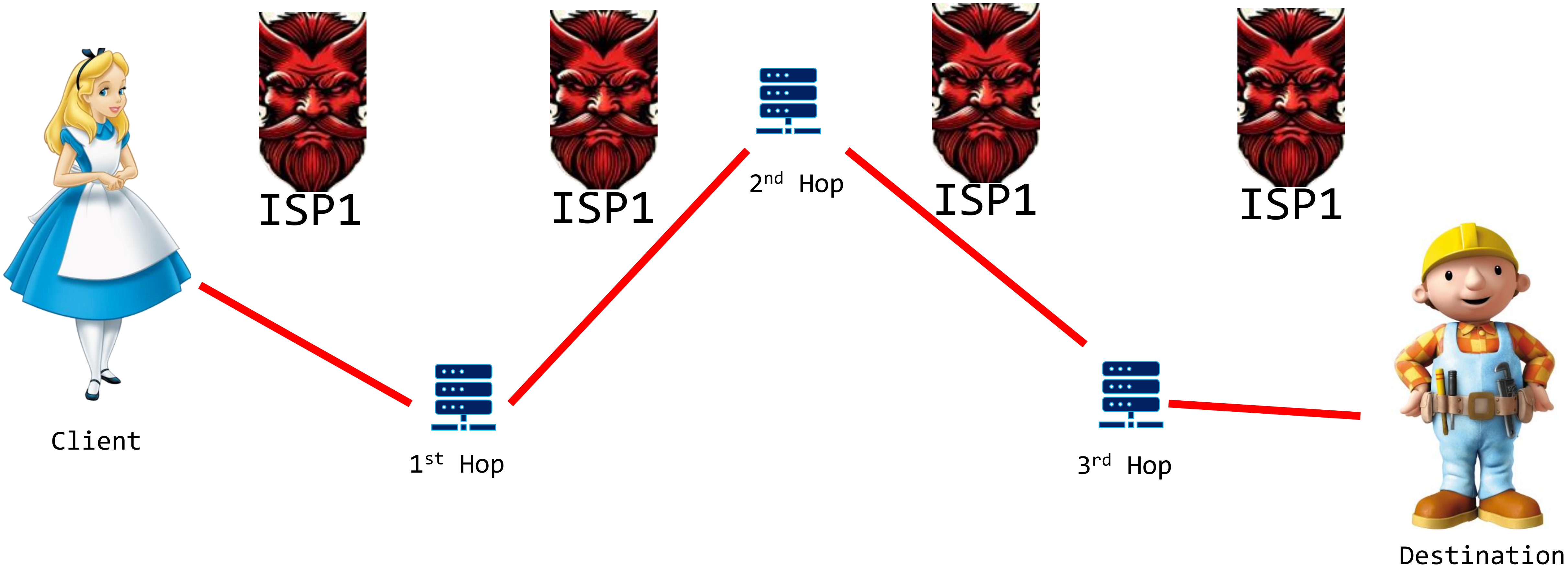
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

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

Mixnodes make their input and output unlinkable.

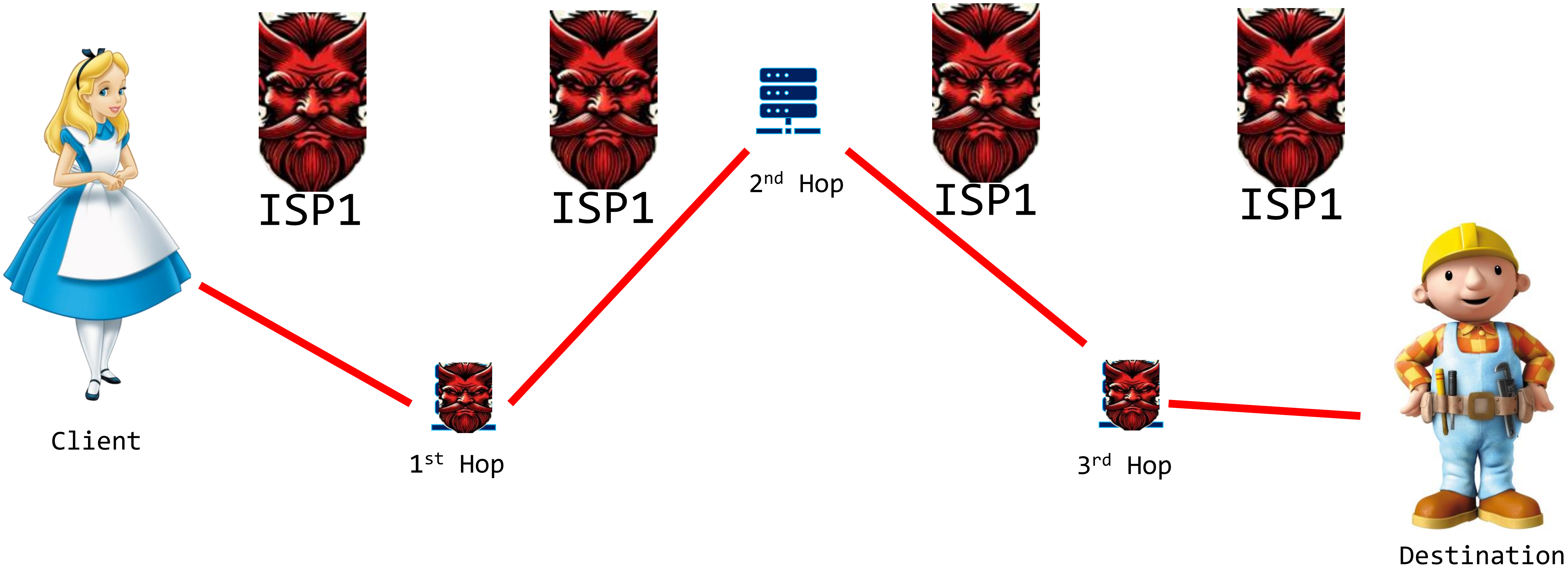


# Mix Network(Mixnet)



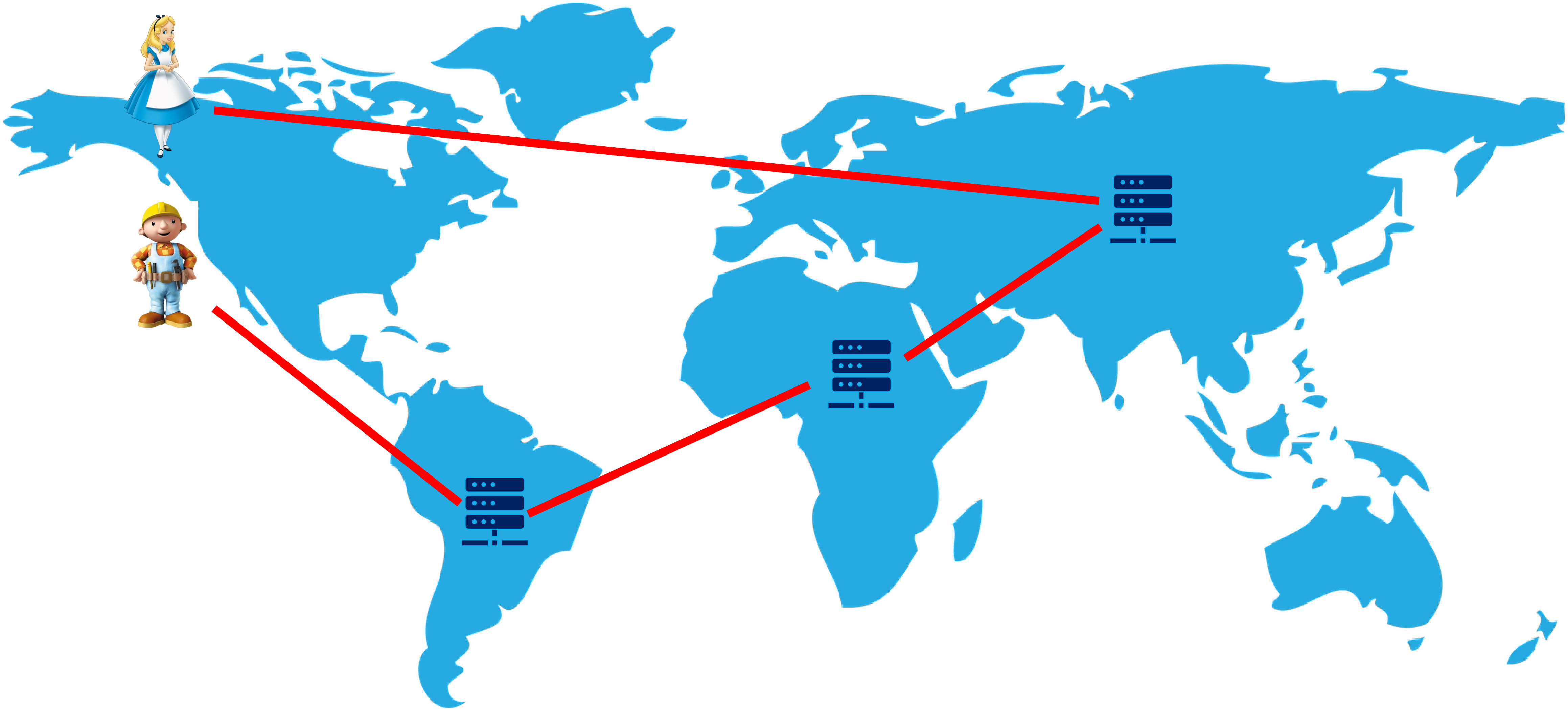
A mixnet is a network consisting of mixnodes, providing shuffling.

# Anonymity Requirement



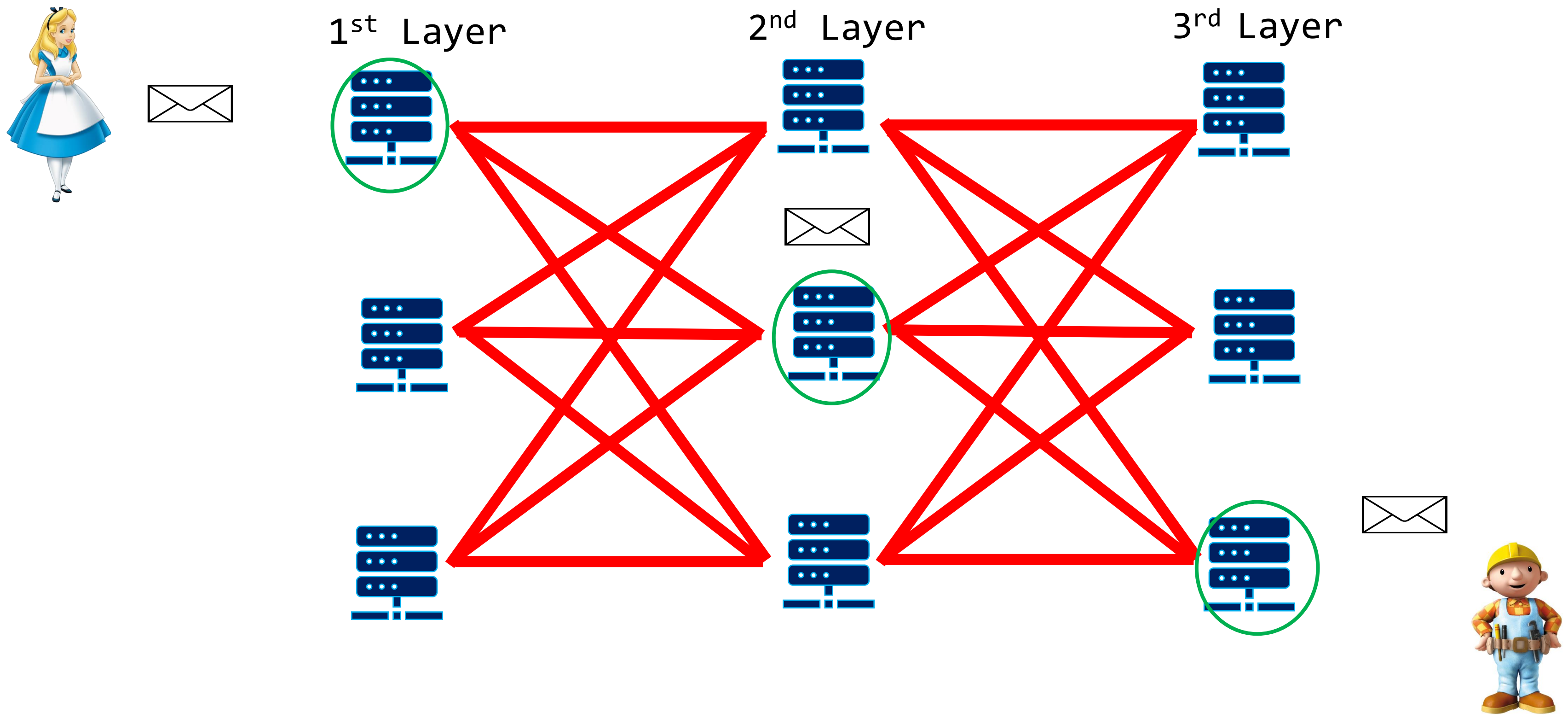
As long as one mixnode in the message route is honest, the client-destination connection will be anonymized.

# 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]

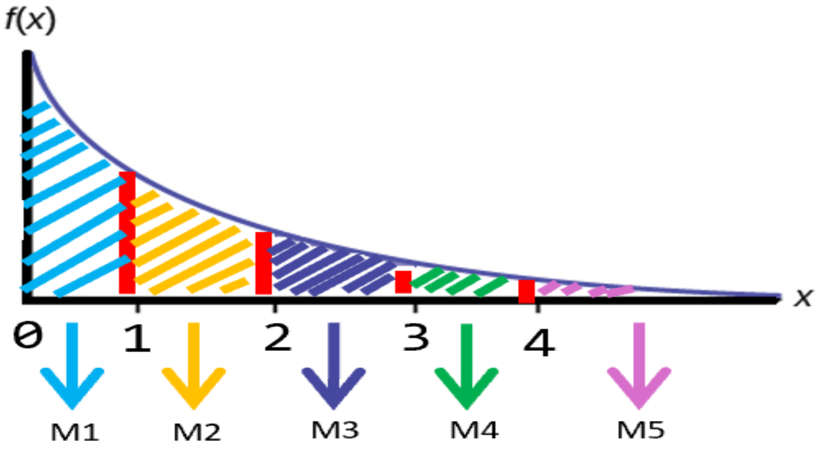


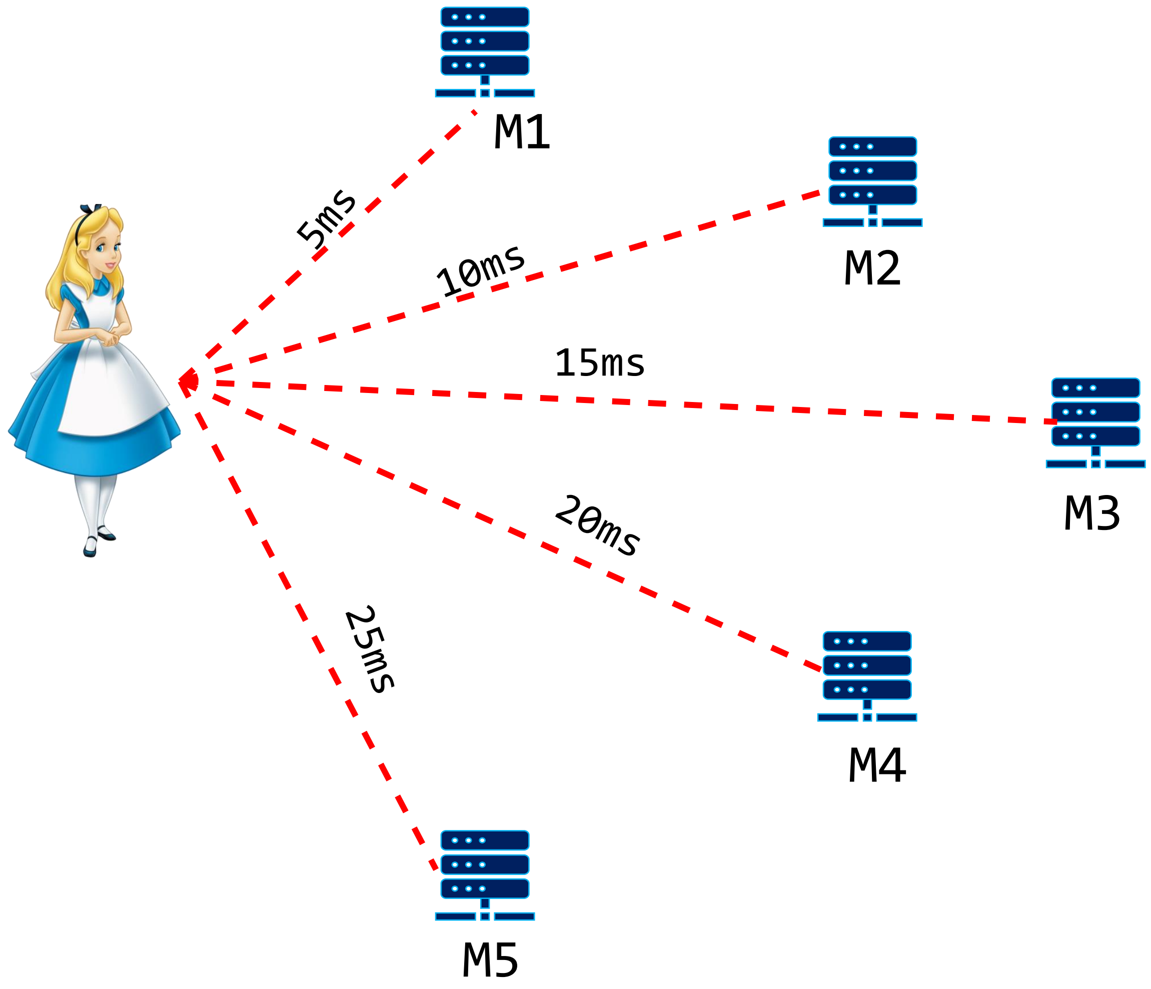
[1] **Mahdi Rahimi**, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." NDSS, 2024.

# LARMix Routing Strategies

Select low-latency links with high probability.

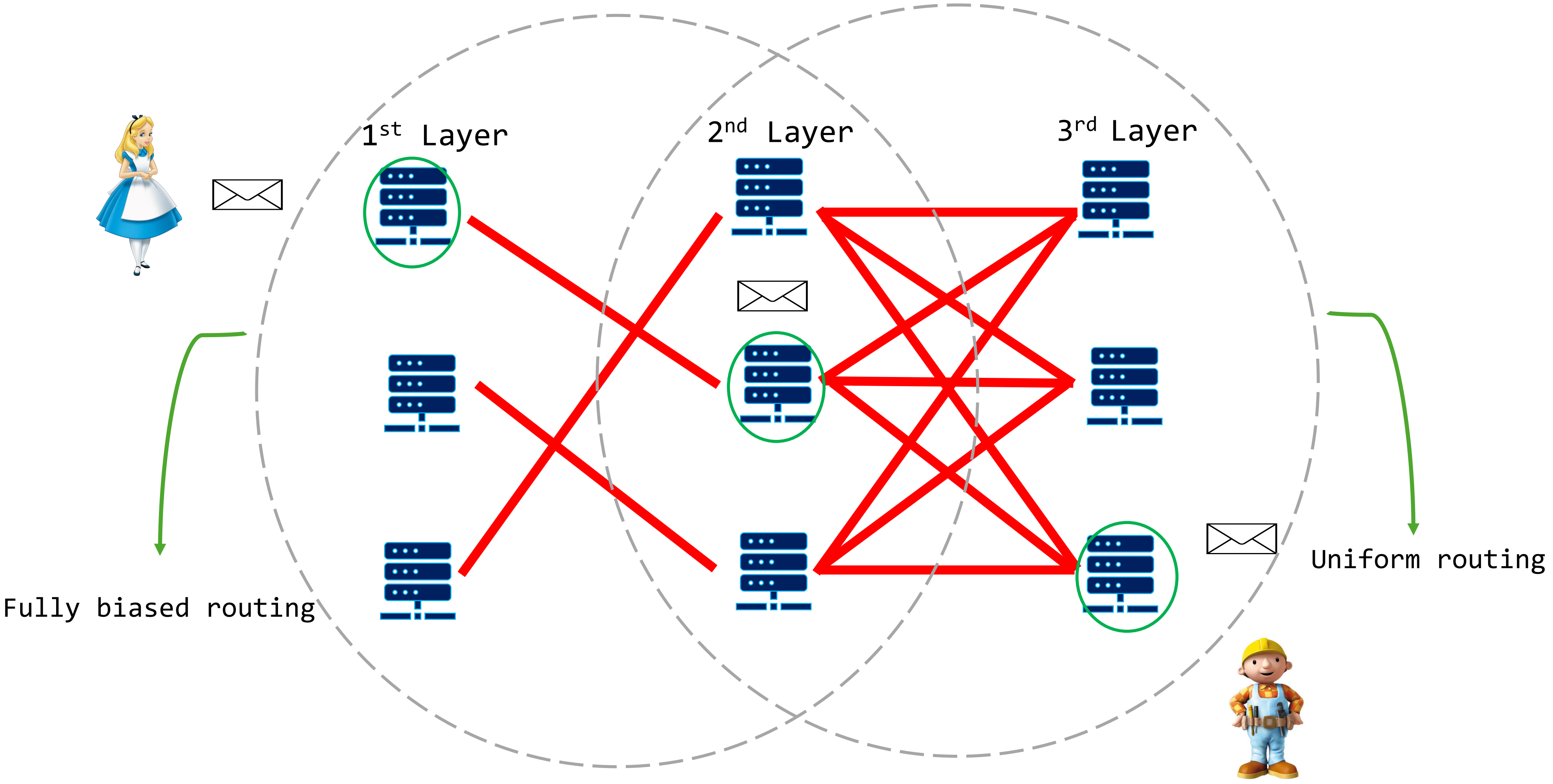
Select the remaining nodes with low probability.





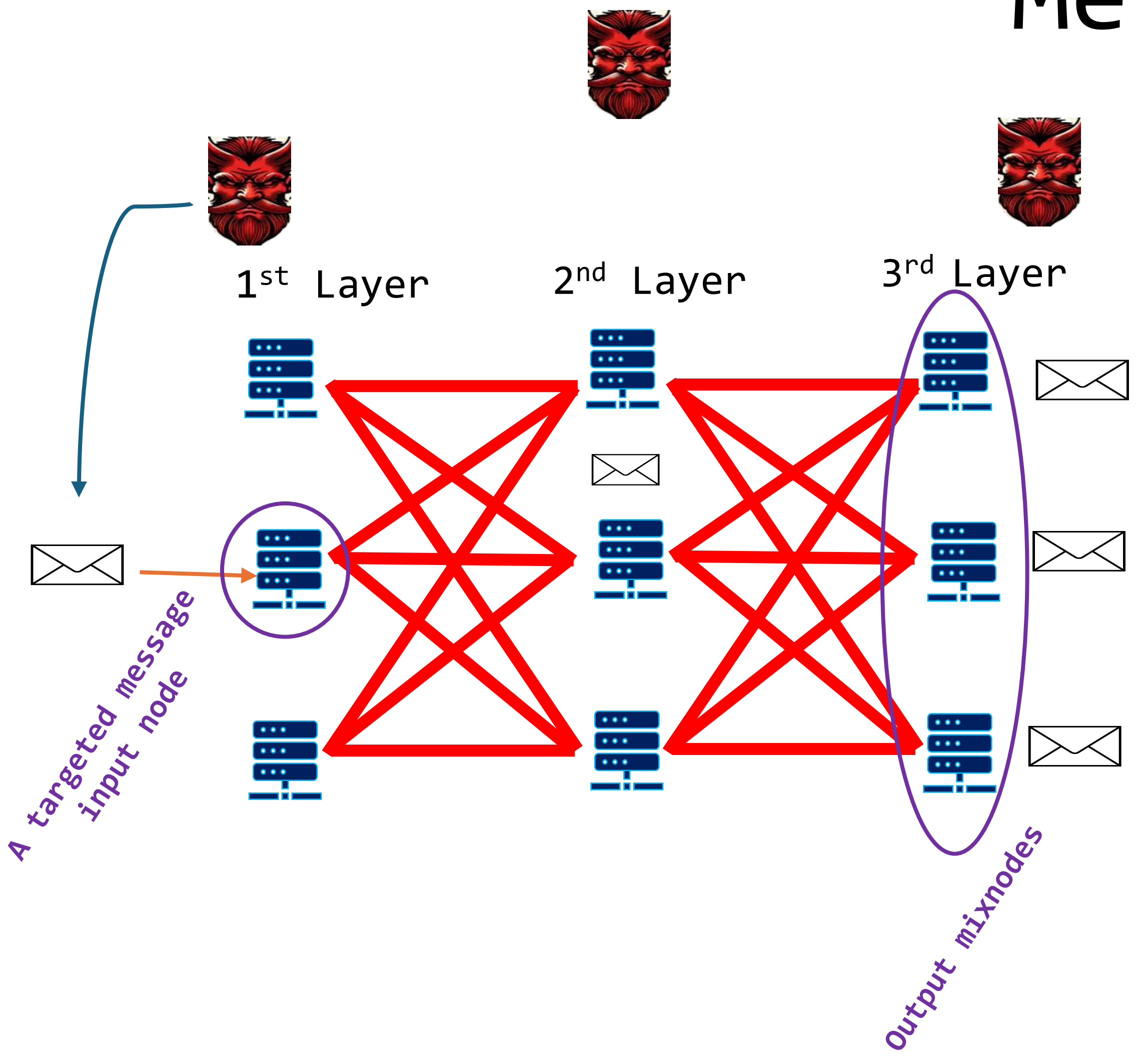
LARMix's biased routing, while effective in reducing latency, compromises anonymity.

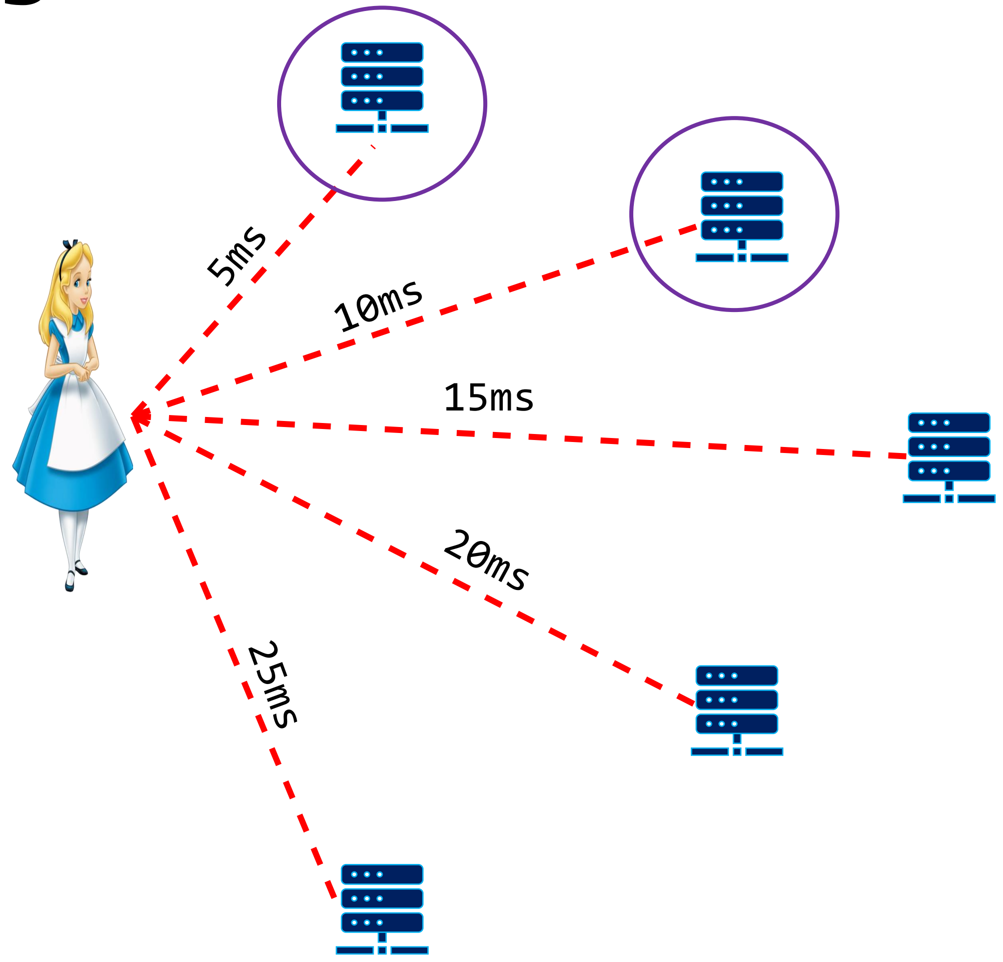
# MALARIA



MALARIA biases the routing for all layers toward the fastest nodes, except for the last layer mixnodes, which are selected uniformly at random.

# Metrics





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

Average latency is useful for measuring the latency reduction.

# Results

| Metrics<br>Routings | Latency | Entropy | Cost |
|---|---|---|---|
| Uniform | 125 ms | 5 bits | Low |
| LARMix | 55 ms | 4 bits | Low |
| Linear Programming | 32 ms | 1 bits | High |
| MALARIA | 28 ms | 5 bits | Low |

MALARIA 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 MALARIA which improves the performance of mixnets by up to 78%.

# 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.