CLAM: Client-Aware Routing in Mix Networks

Mahdi Rahimi

COSIC, KU Leuven, Belgium

mahdi.rahimi@kuleuven.be

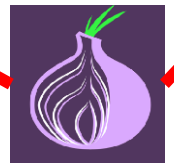
End users on the internet are not anonymized by default.

This creates privacy issues.

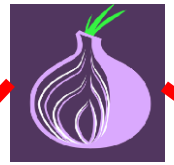
Tor Network

Client

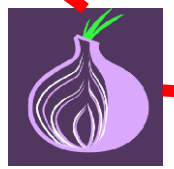
ISP1



Guard Relay



Middle Relay



Exit Relay

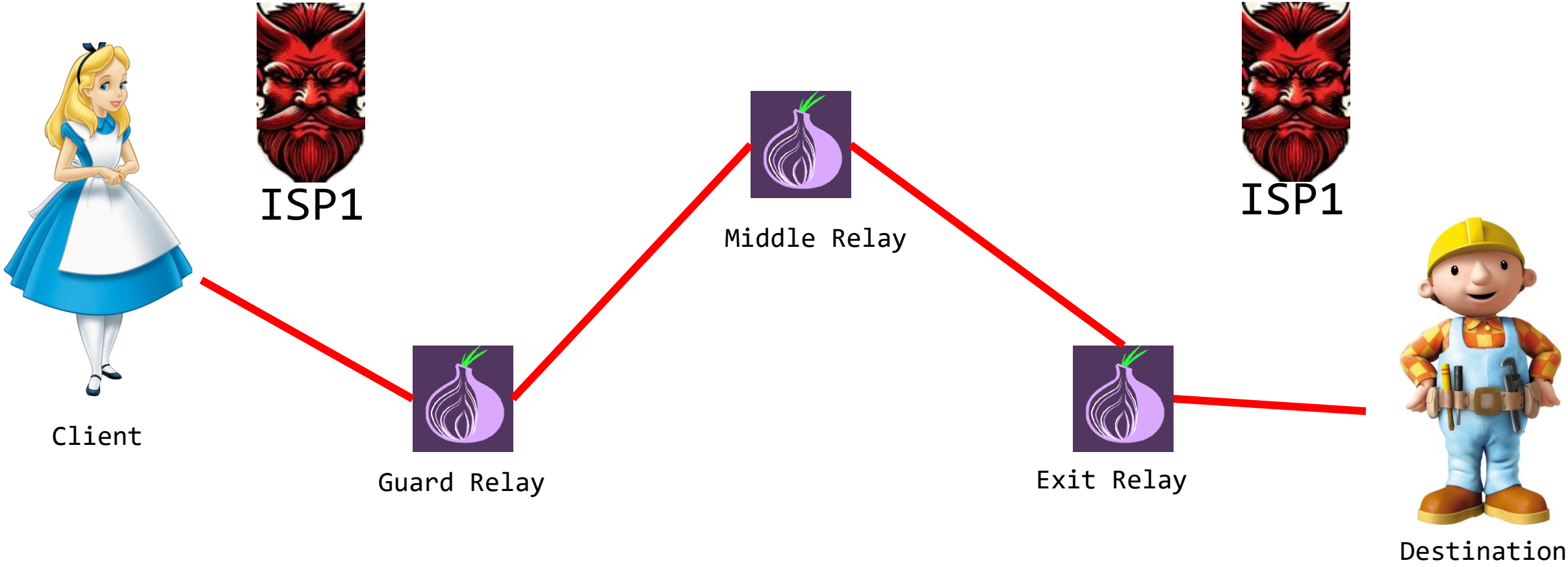
ISP2

Destination

ISP: Internet Service Provider.

ISP1 does not collude with ISP2.

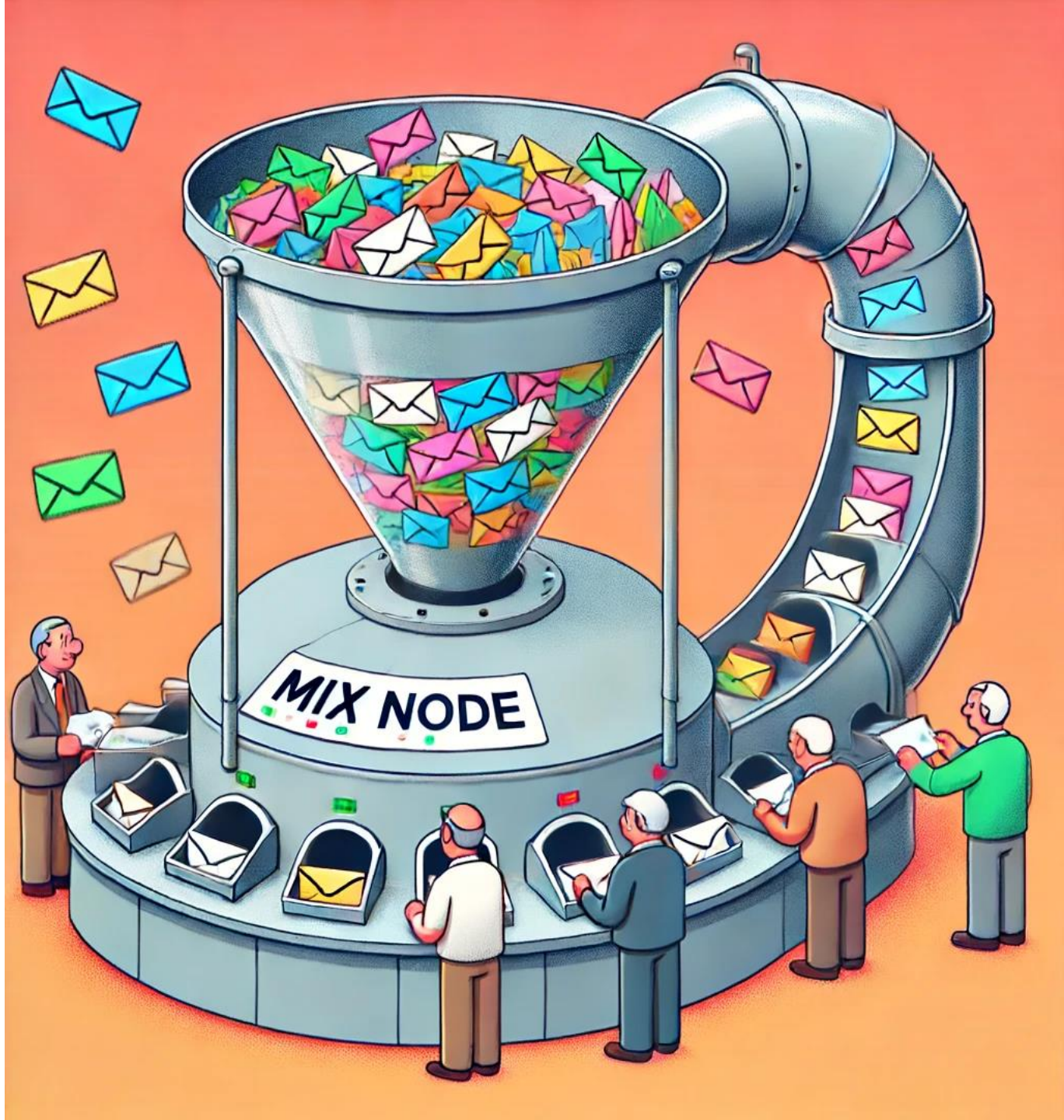
End-to-End Correlation Attacks



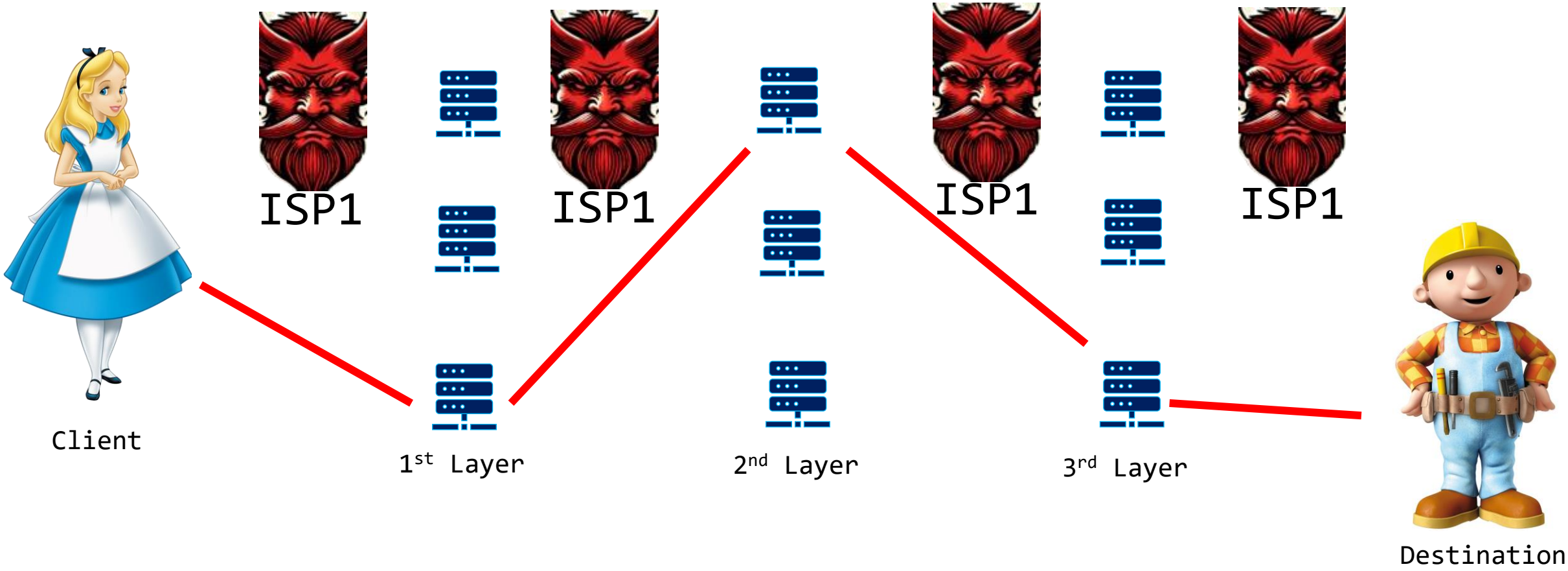
If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

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

Mixnodes make their input and output unlinkable, at the expense of increased latency.

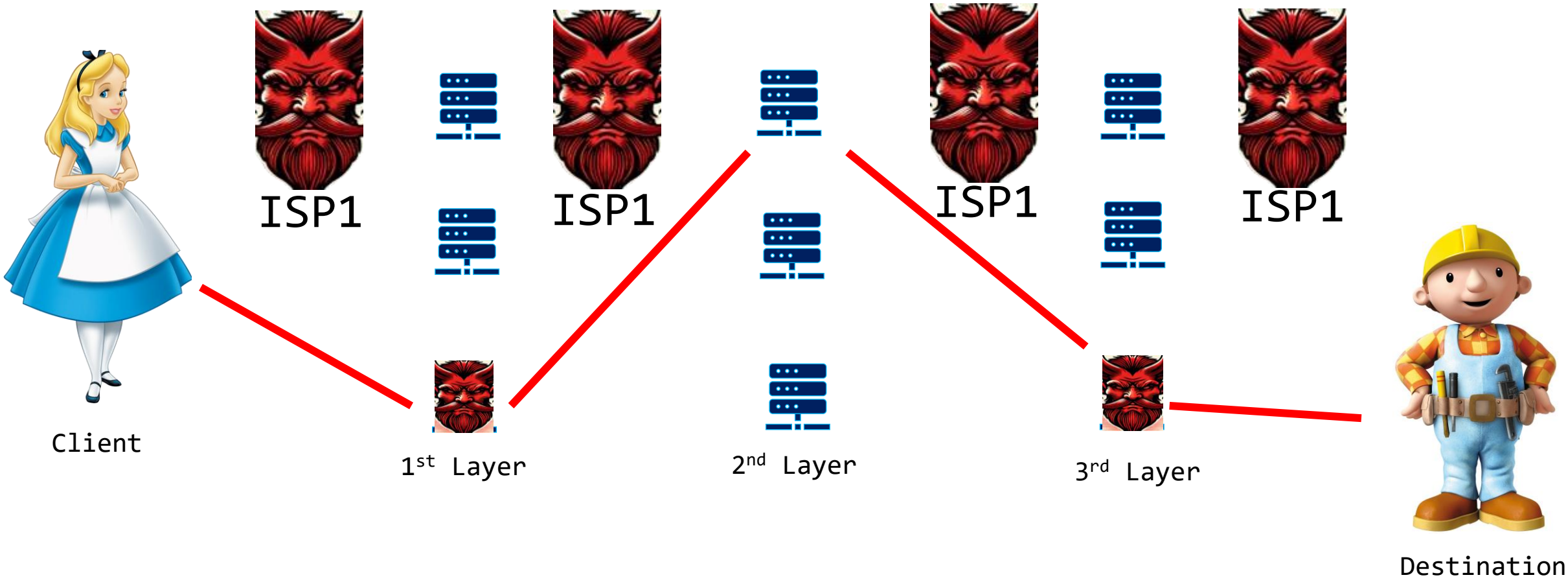


Mix Network(Mixnet)



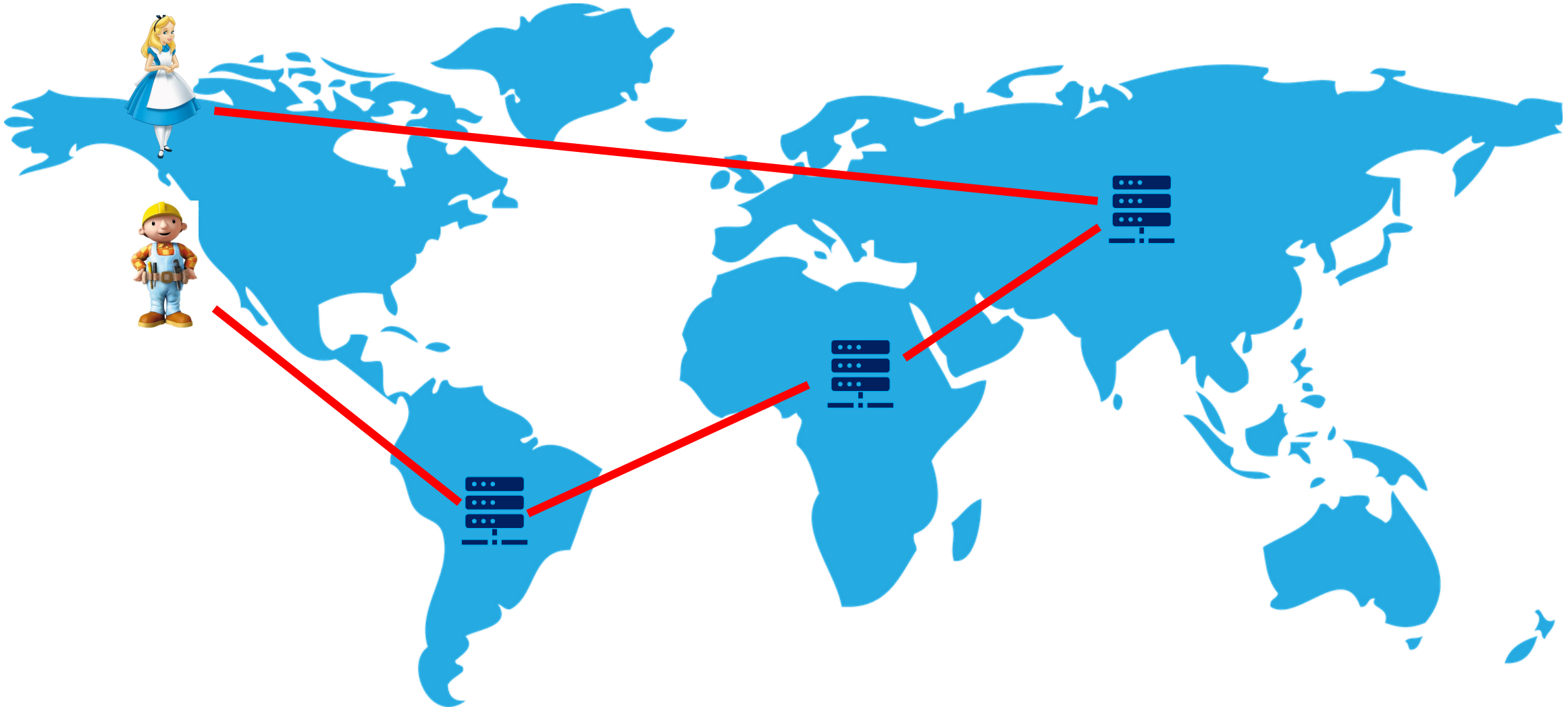
A mixnet is a network consisting of mixnodes, typically arranged in a layered format.

Anonymity Requirement



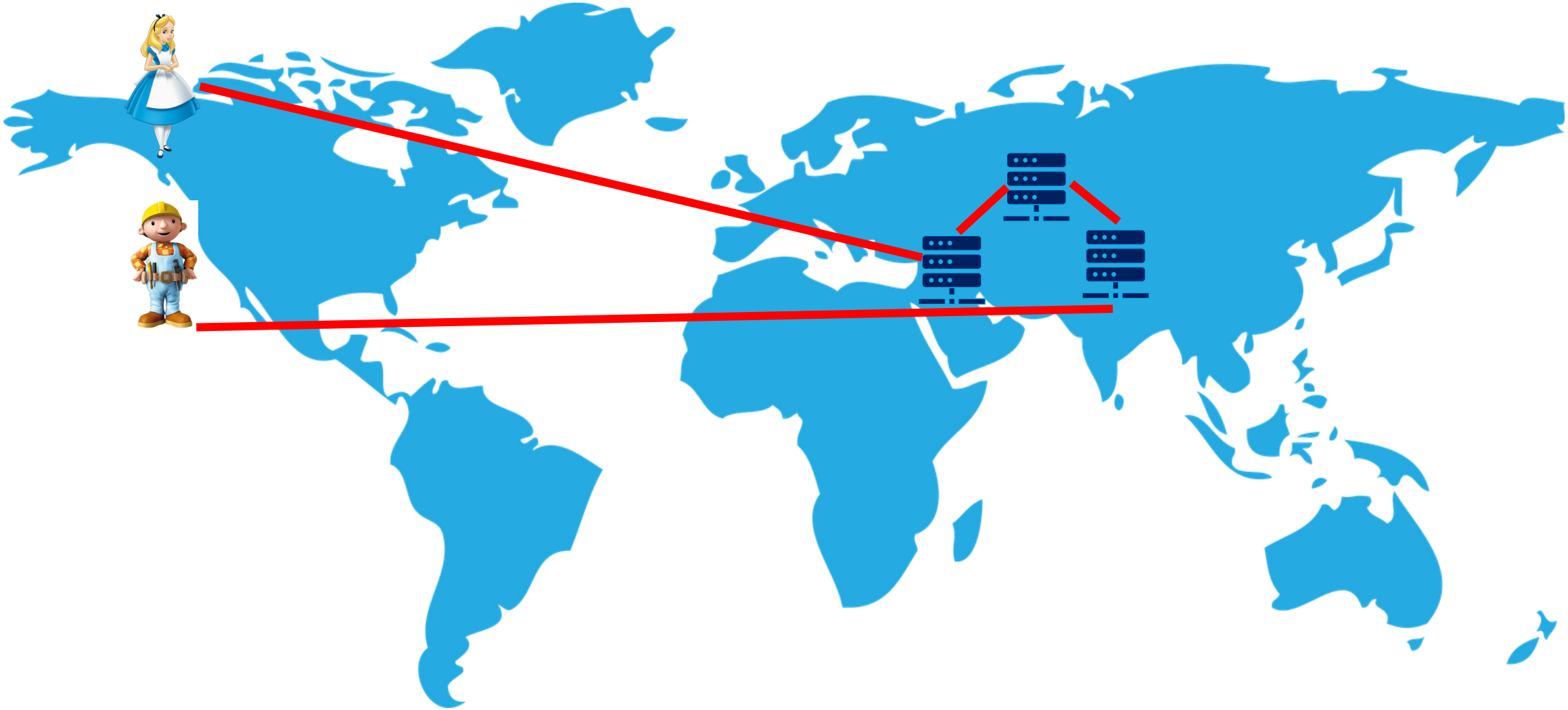
As long as one mixnode in the message route is honest, the client-destination connection will be anonymized.

End-to-End Latency



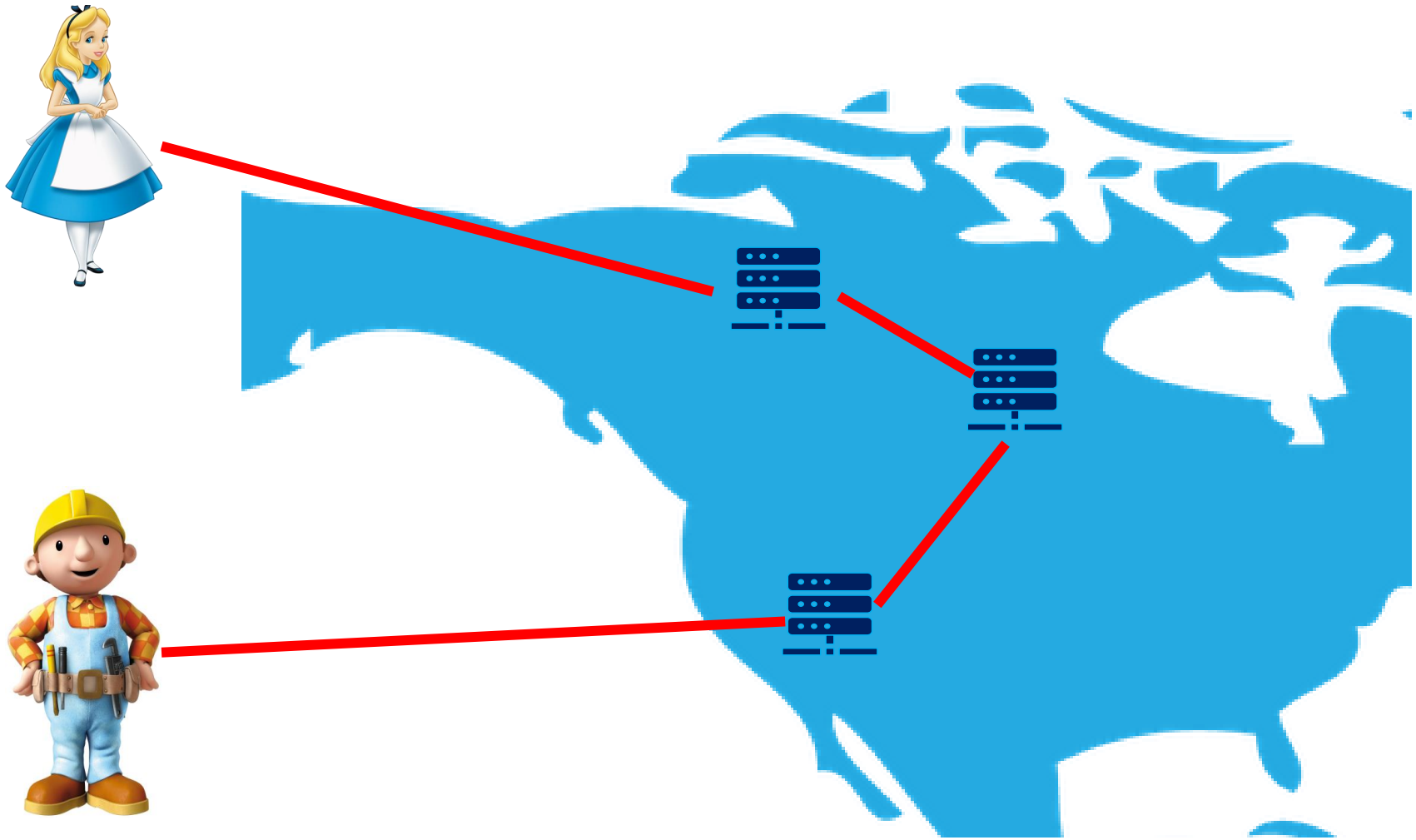
As a result of routing through intermediate mixnodes and intentional delays at each mixnode, the end-to-end latency is very high when using a mixnet.

LARMix



"LARMix" (NDSS, 2024) provides low-latency routing within the mixnet.

CLAM

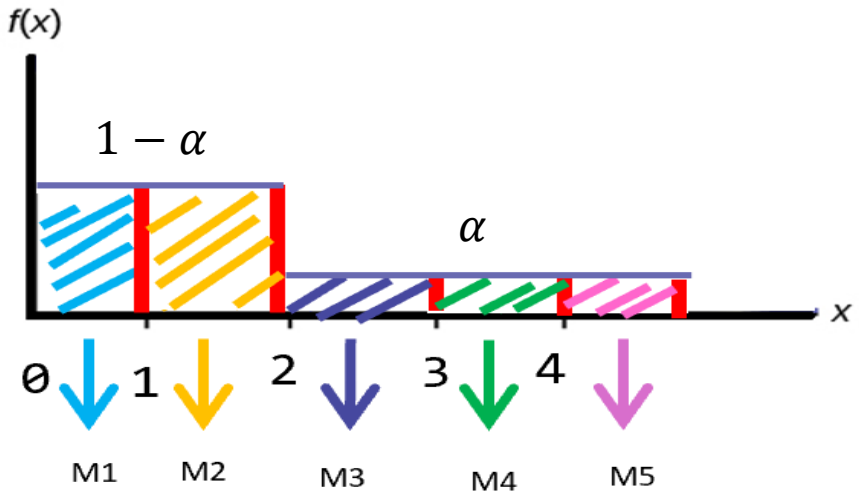


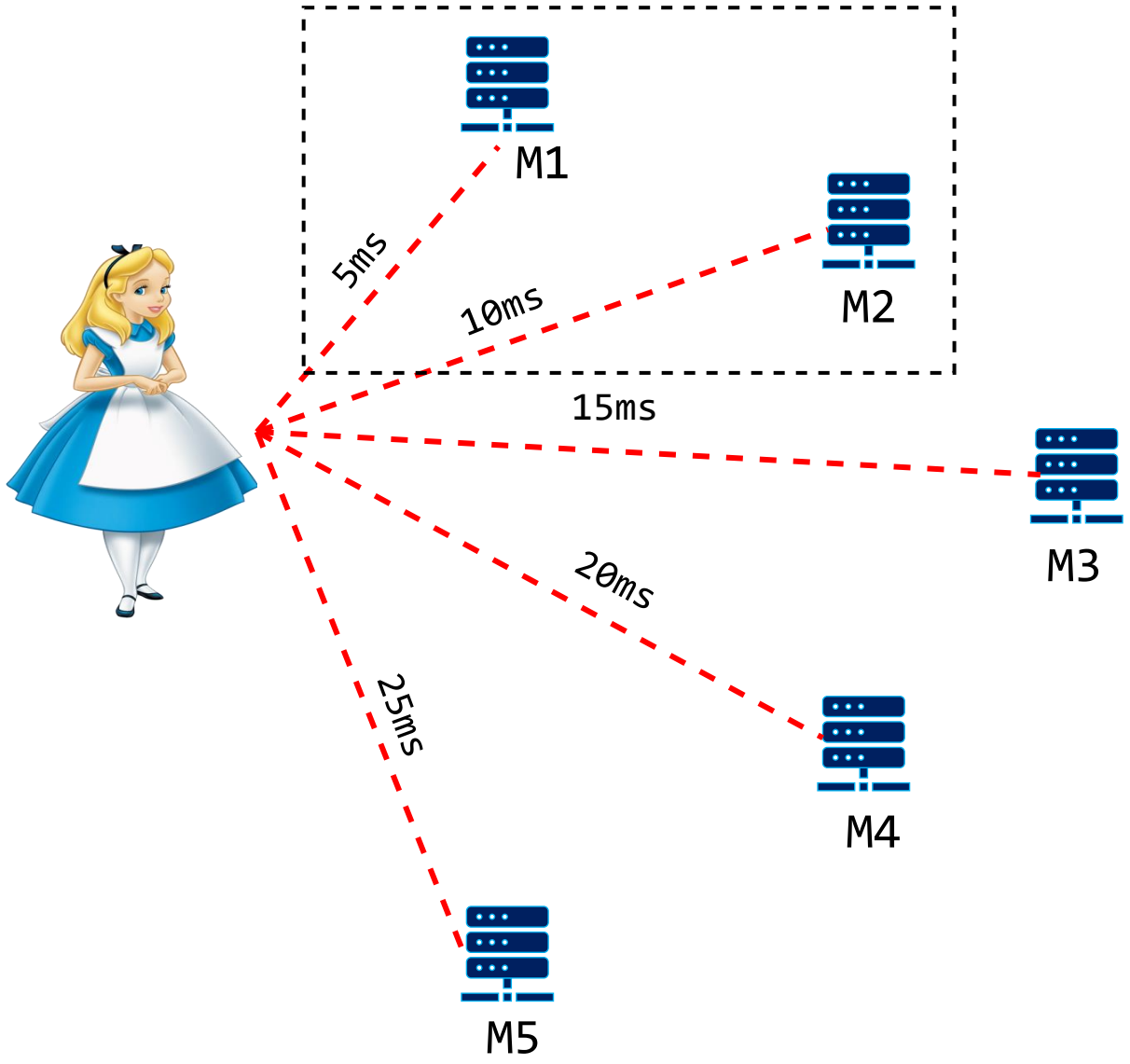
"CLAM " provides low-latency routing from the client to the mix network.

K_αCloseness Routing

Probability of selecting other mixnodes:α

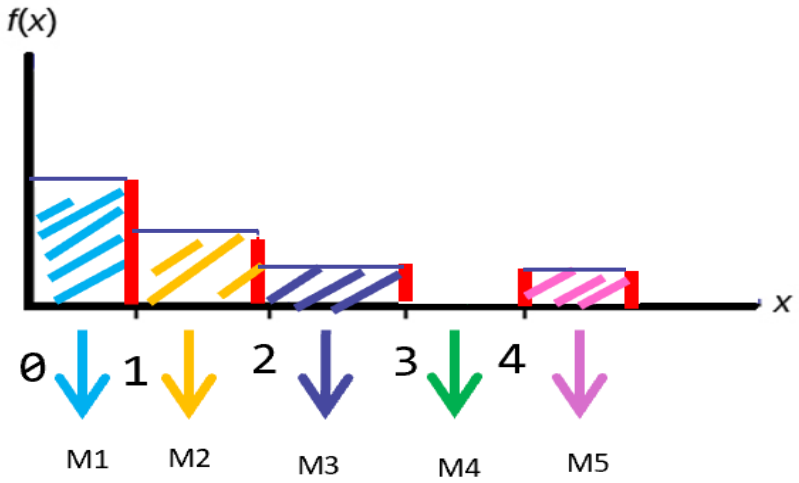
Probability of selecting K closest mixnodes:1-α

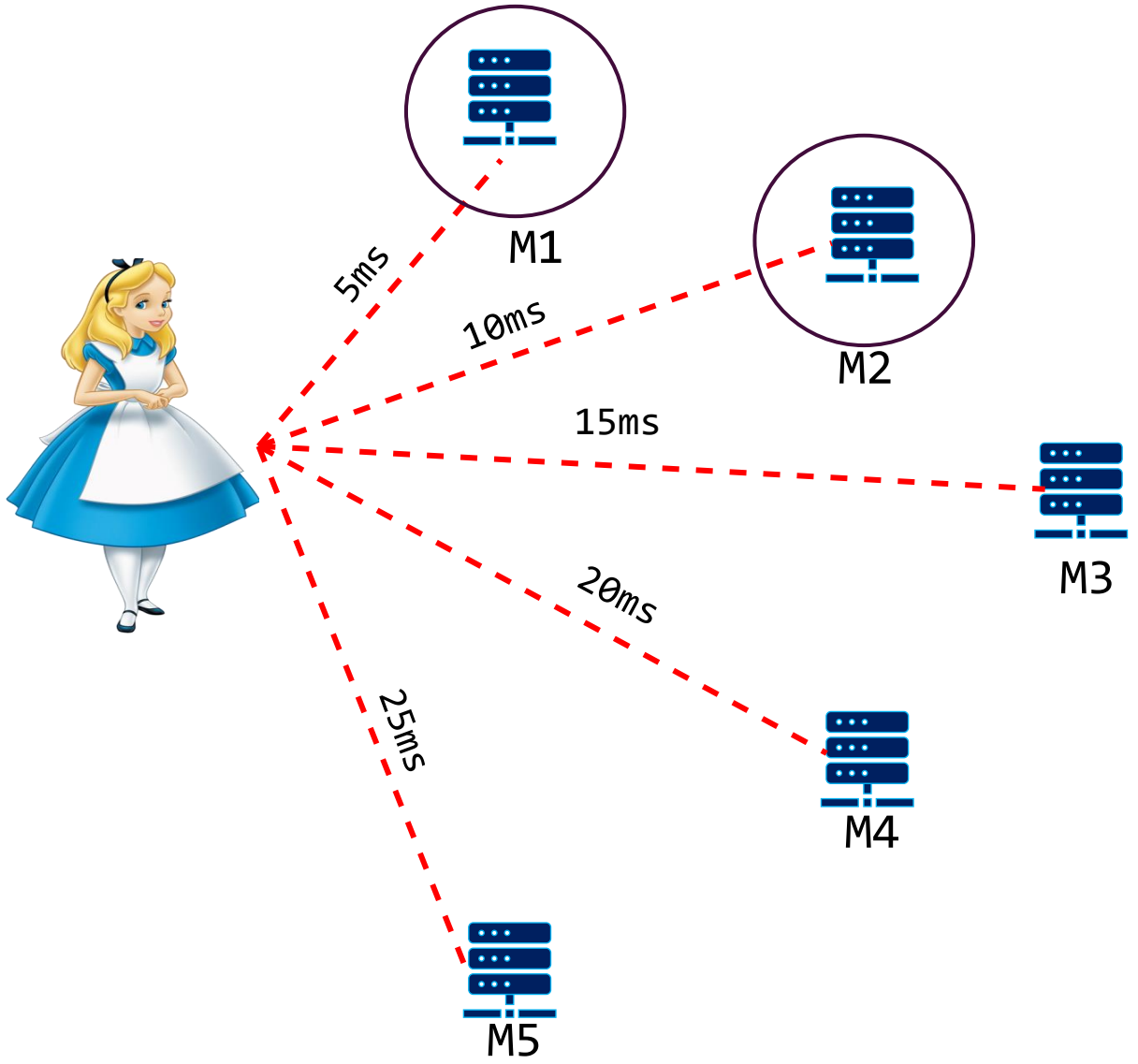




Linear Programming Routing

Minimizing latency while keeping mixnodes load balanced.

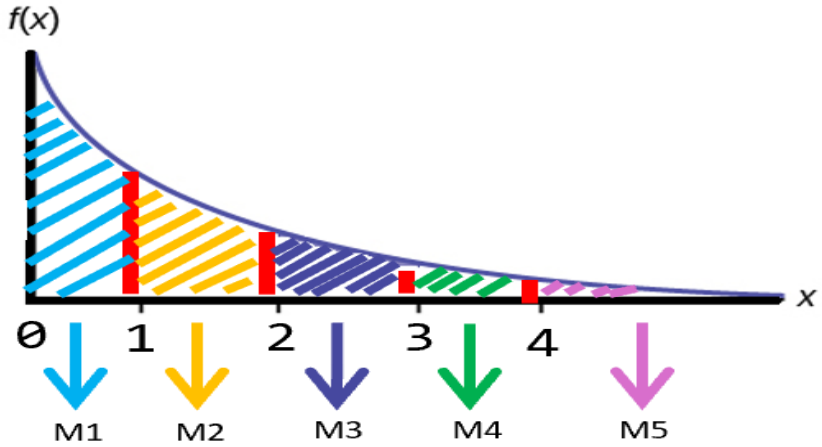


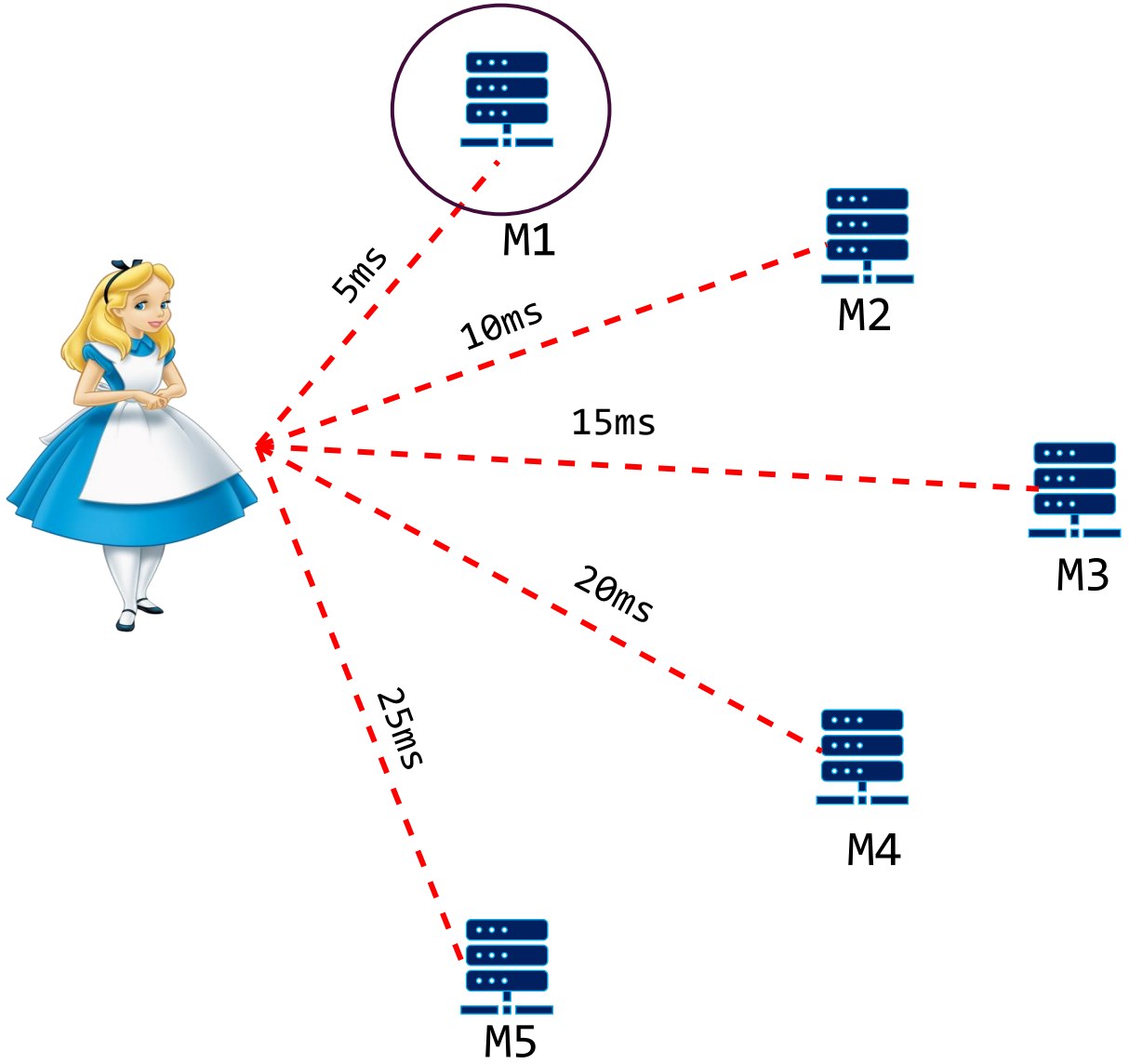


Exponential distribution Routings

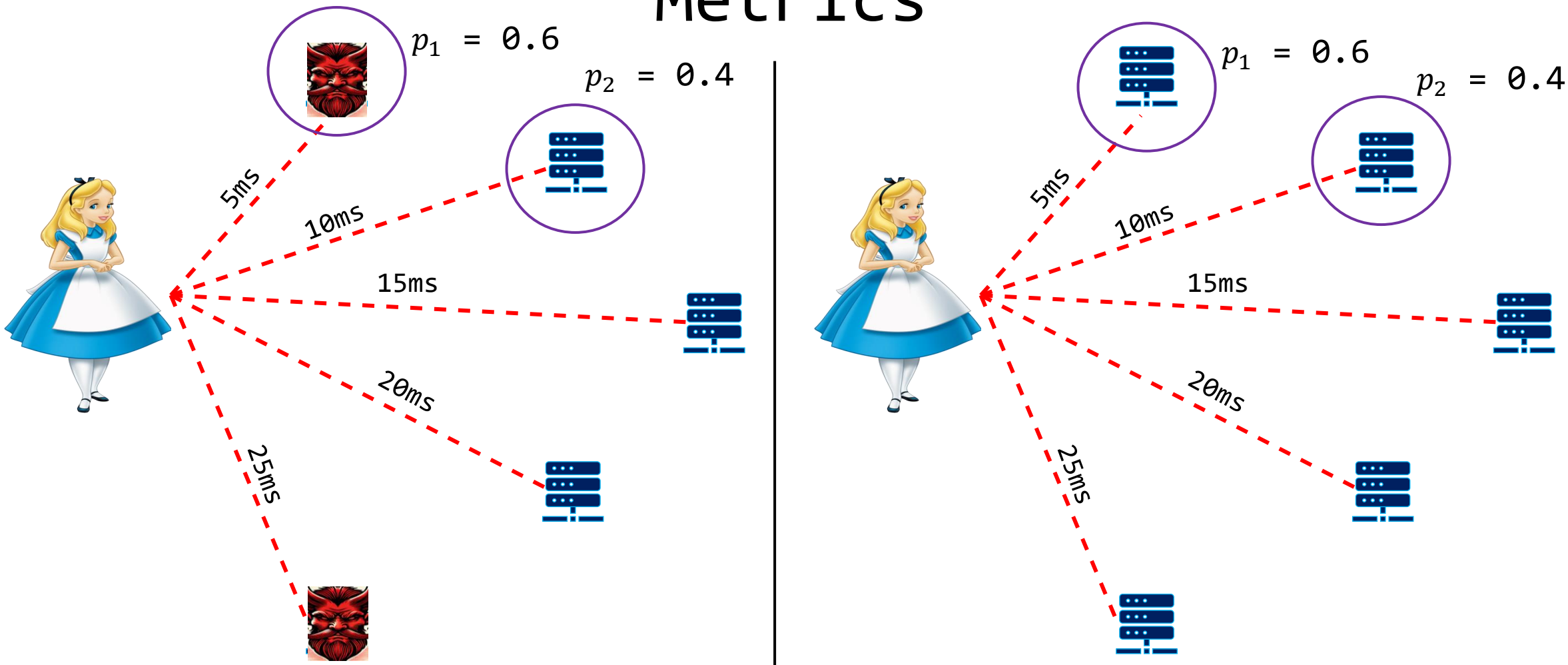
Exponentially prioritizing mixnode selections.

$$f(x) = \mathrm{Exp}(\lambda) = \lambda e^{-\lambda x}$$





Metrics



The Fraction of Corruption (FC) is the percentage of traffic intercepted by the adversary.

Average latency is useful for measuring the latency reduction.

Results

Routings \ Metrics	Latency	FC	Cost
Uniform	61 ms	0.008	Low
KαCloseness	20 ms	0.016	Low
Linear Programming	7 ms	0.018	High
Exponential distribution	7 ms	0.027	Low

"CLAM " 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 together with CLAM which improves the performance of mixnets by up to 70%.

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 distributed cryptography, feel free to connect with me through LinkedIn.