Latency-Aware Routing in Mix Networks

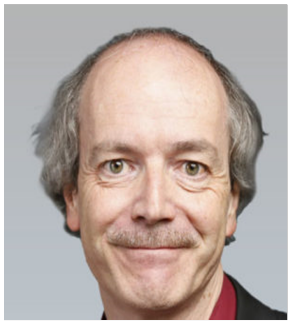
Mahdi Rahimi

mahdi.rahimi@esat.kuleuven.be

September 20, 2024



KU Leuven (COSIC)





COSIC



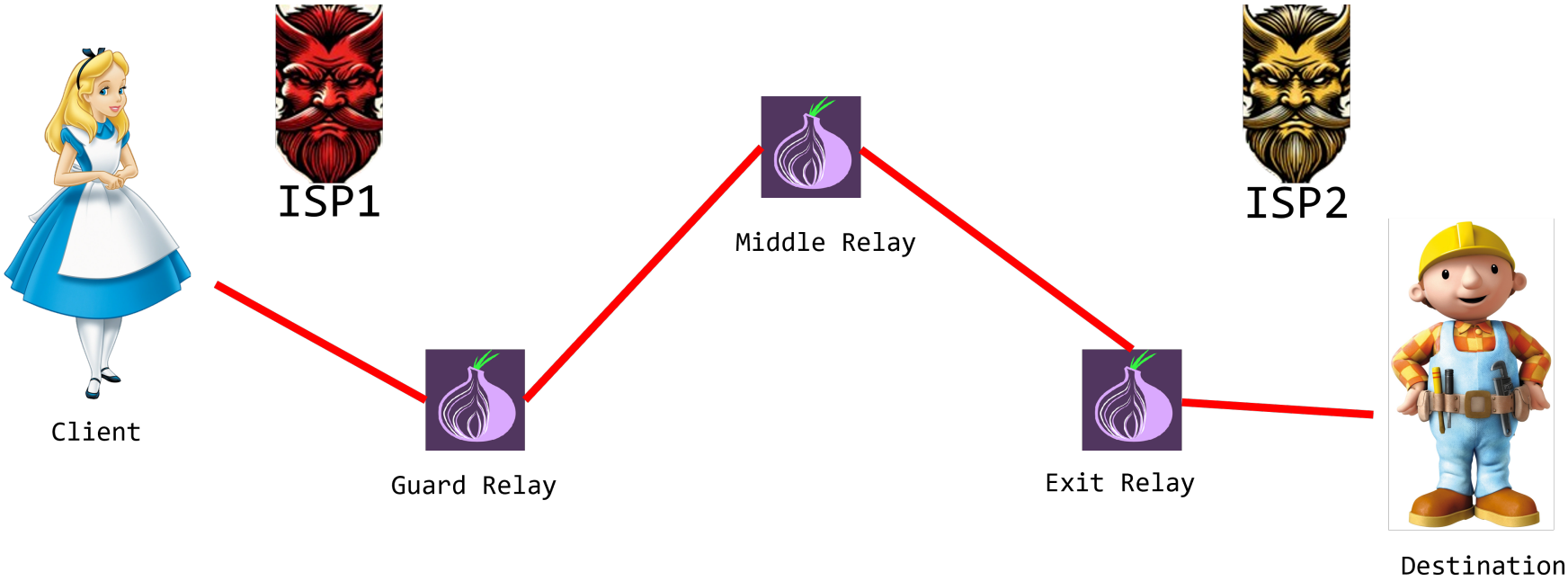






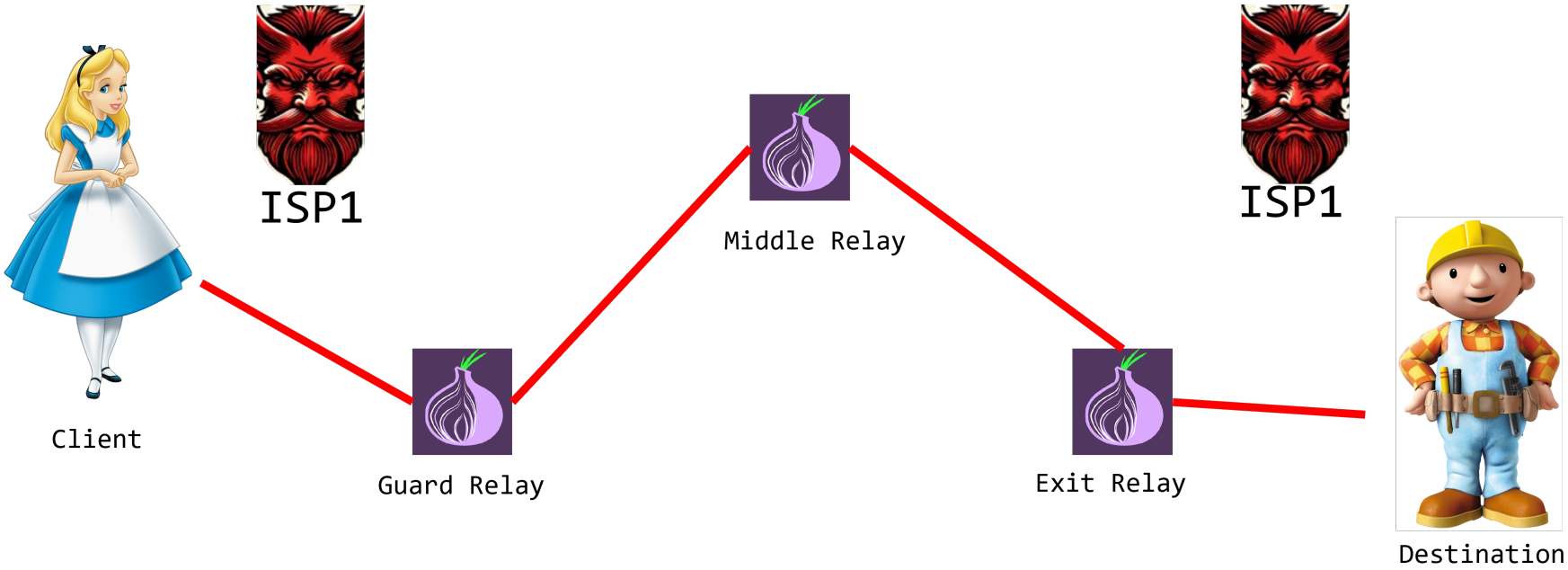


Background: Tor network



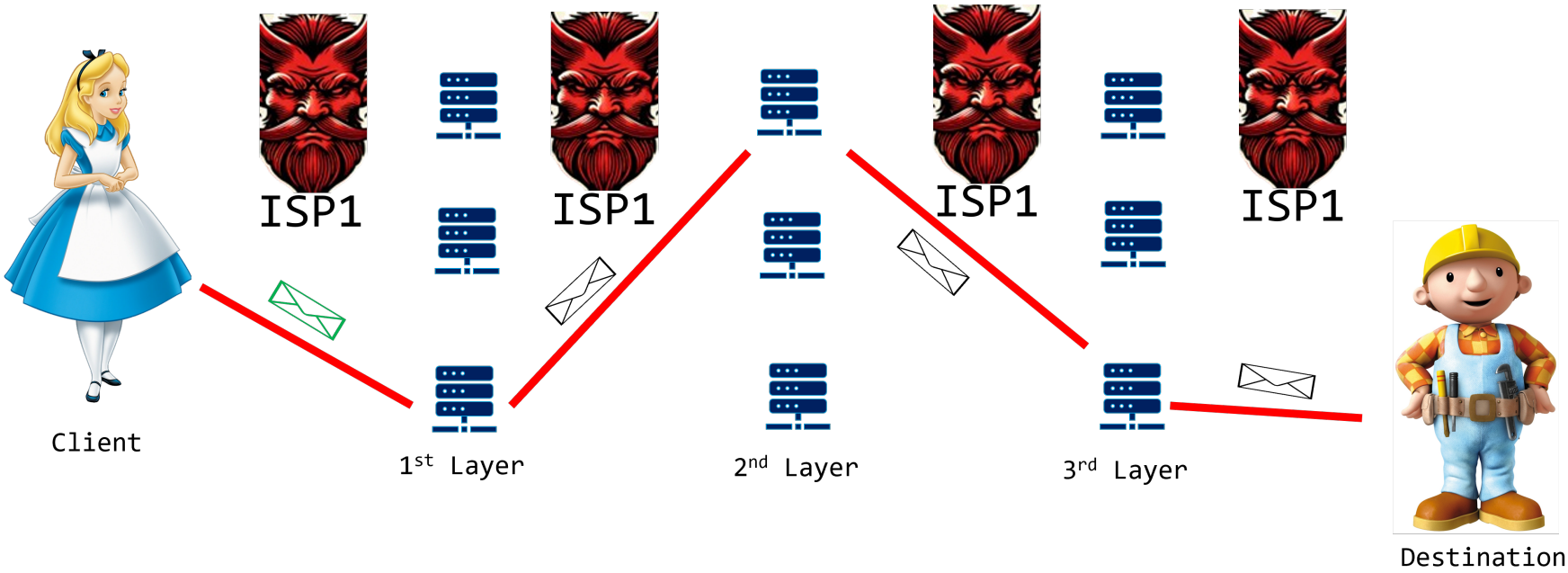
- Threat model: Local adversary (ISP: Internet Service Provider)
- ISP1 does not collude with ISP2.

Background: Tor network



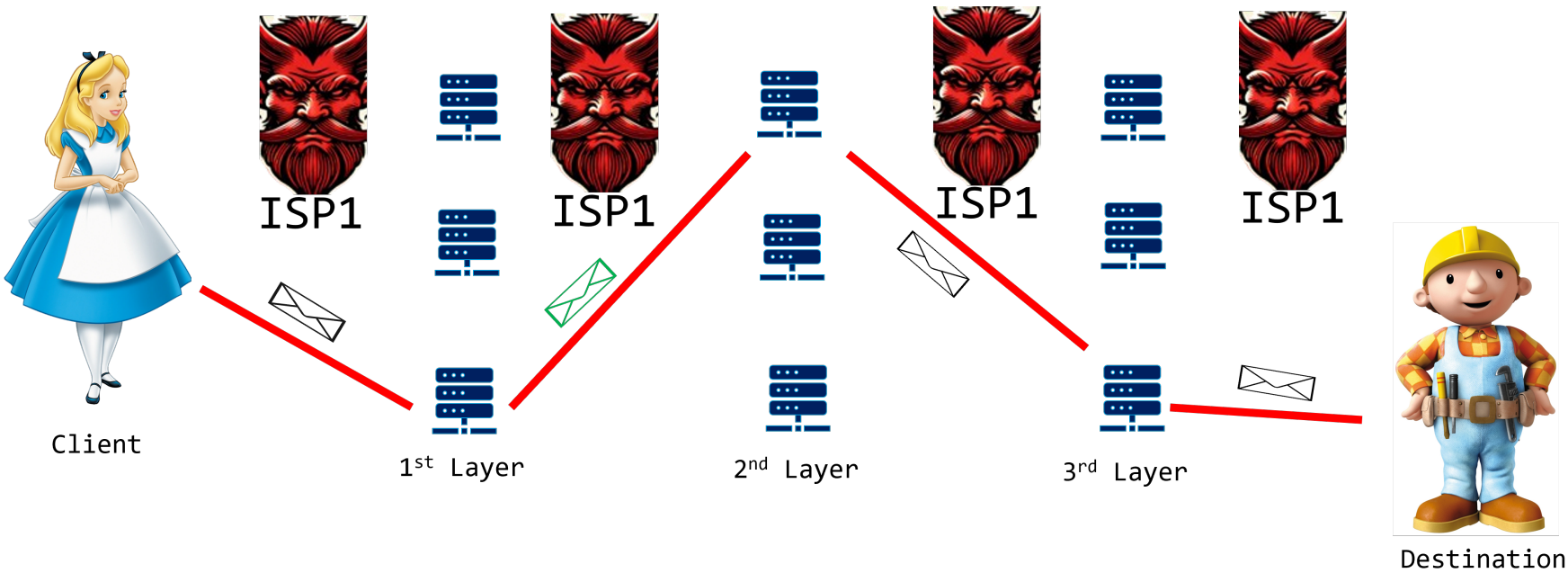
- If ISP1 colludes with ISP2, they can deanonymize the client-destination connection.

Background: Mix network

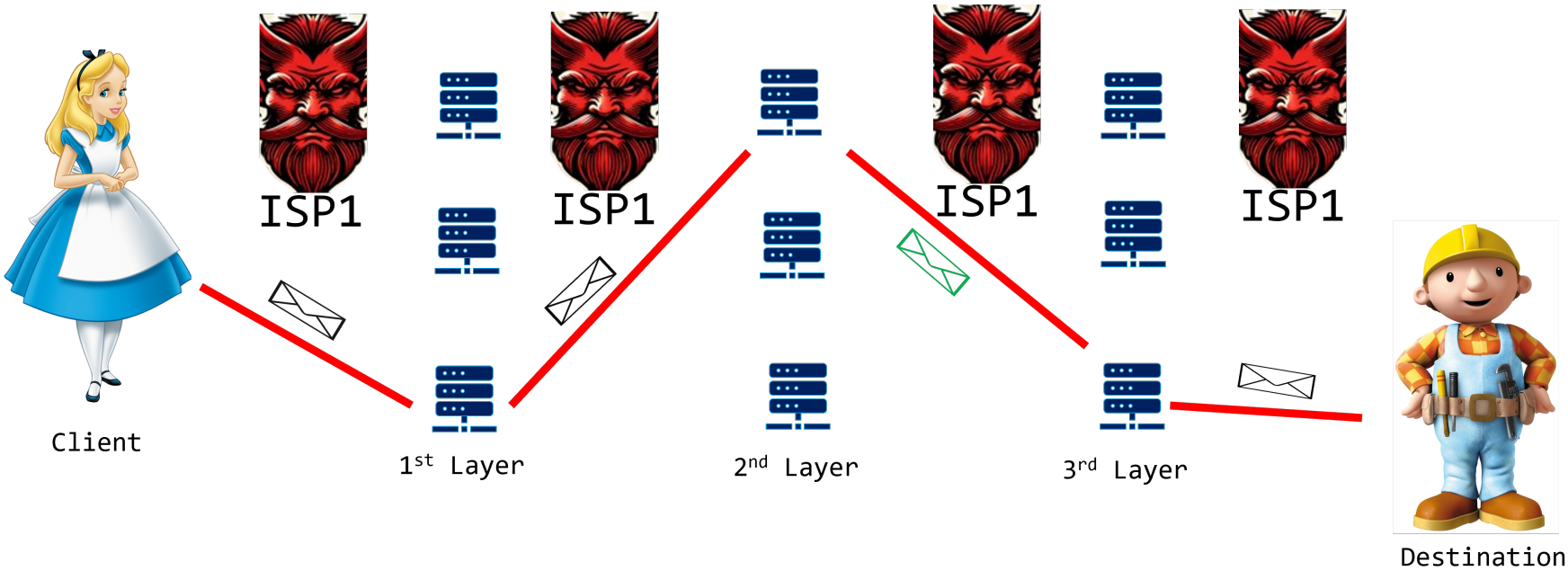


- A mixnet is a network consisting of mixnodes, typically arranged in a layered format.
- Threat model: Global network adversary.

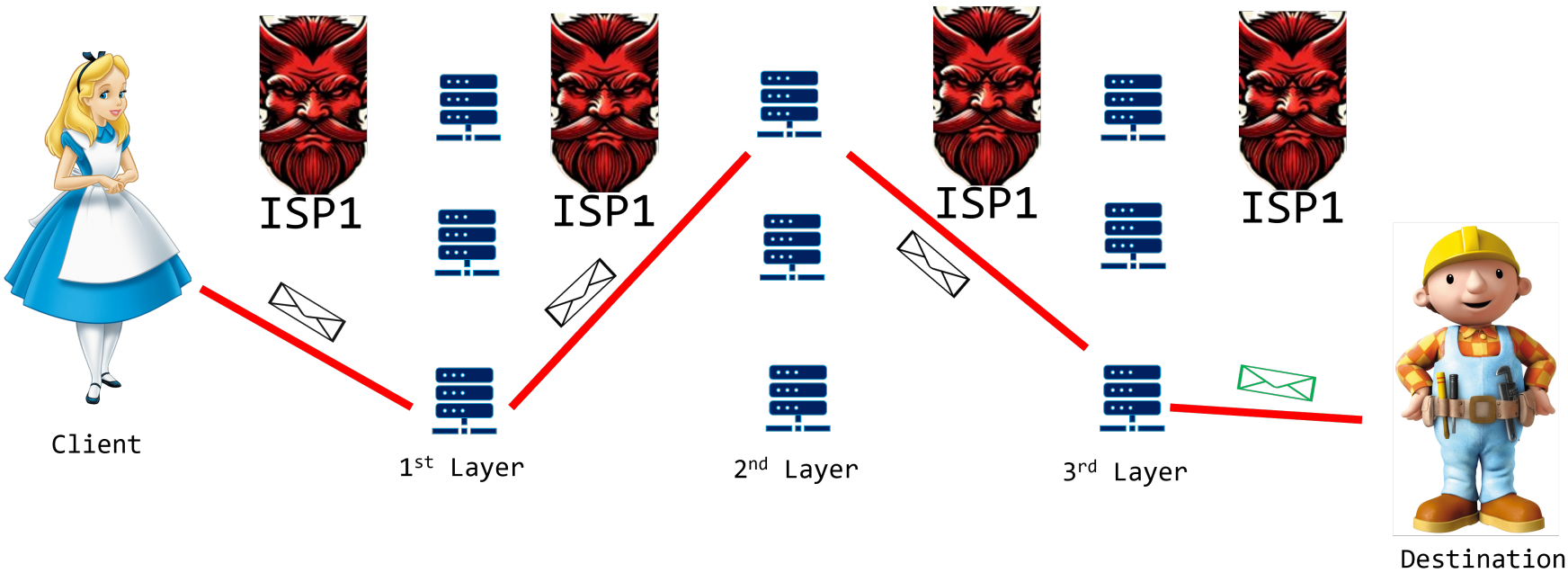
Background: Mix network



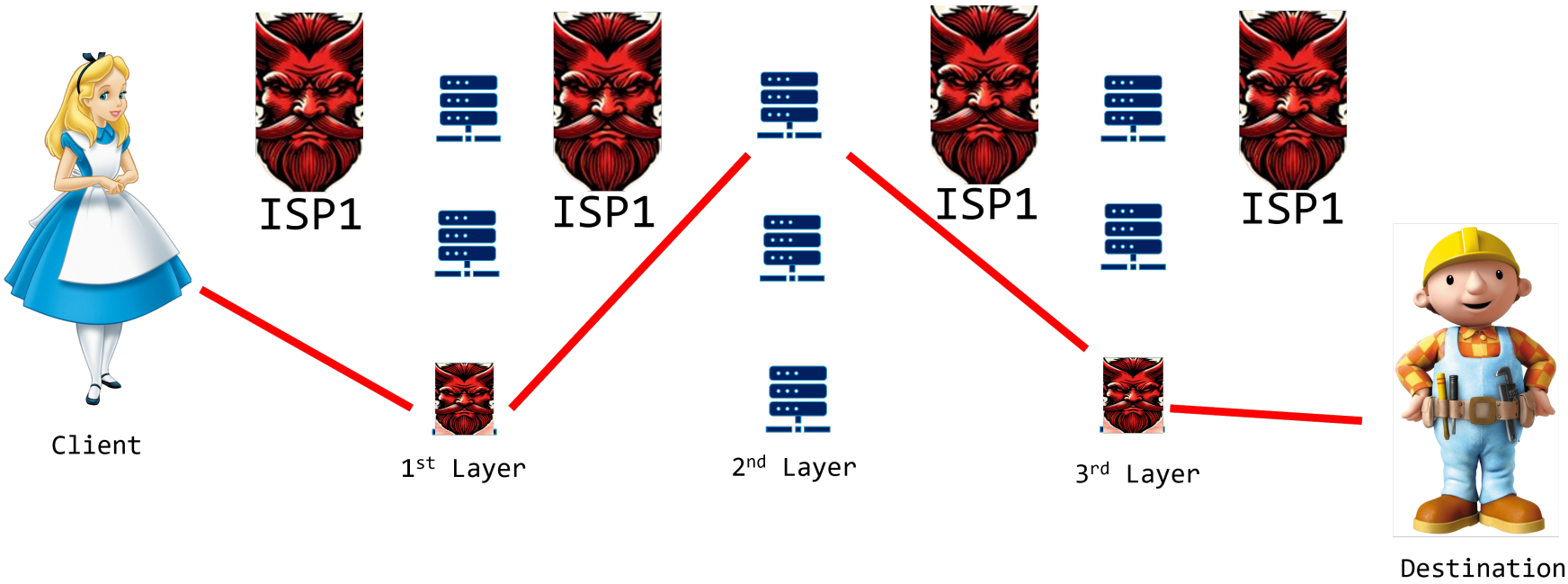
Background: Mix network



Background: Mix network

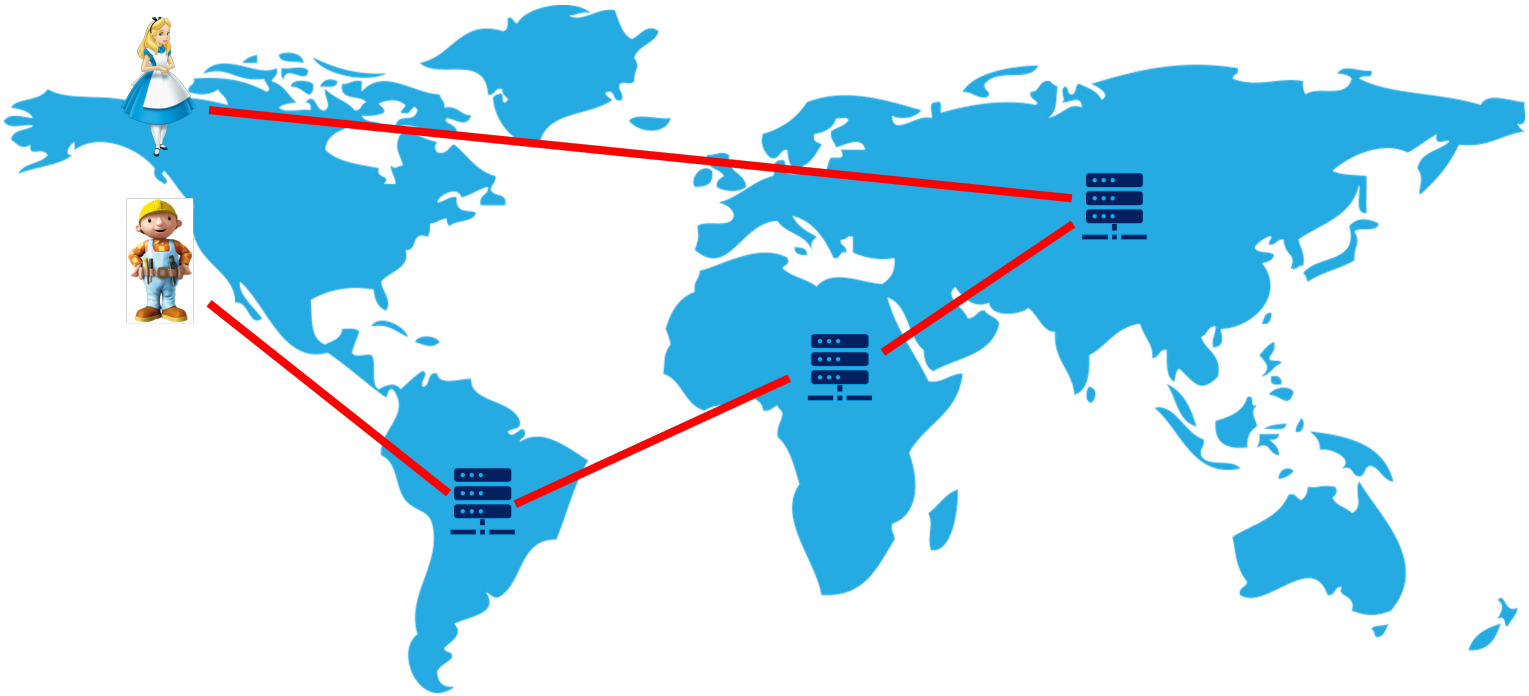


Background: Mix network



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

High 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.

Overview

- Mahdi Rahimi, Piyush Kumar Sharma, and Claudia Diaz. "LARMix: Latency-Aware Routing in Mix Networks." In The Network and Distributed System Security Symposium. Internet Society. 2024.
- Mahdi Rahimi. "CLAM: Client-Aware Routing in Mix Networks." In Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security, pp. 199-209. 2024.
- Mahdi Rahimi. "LARMix++: Latency-Aware Routing in Mix Networks with Free Routes Topology." In International Conference on Cryptology and Network Security.

LARMix: Latency-Aware Routing in Mix networks

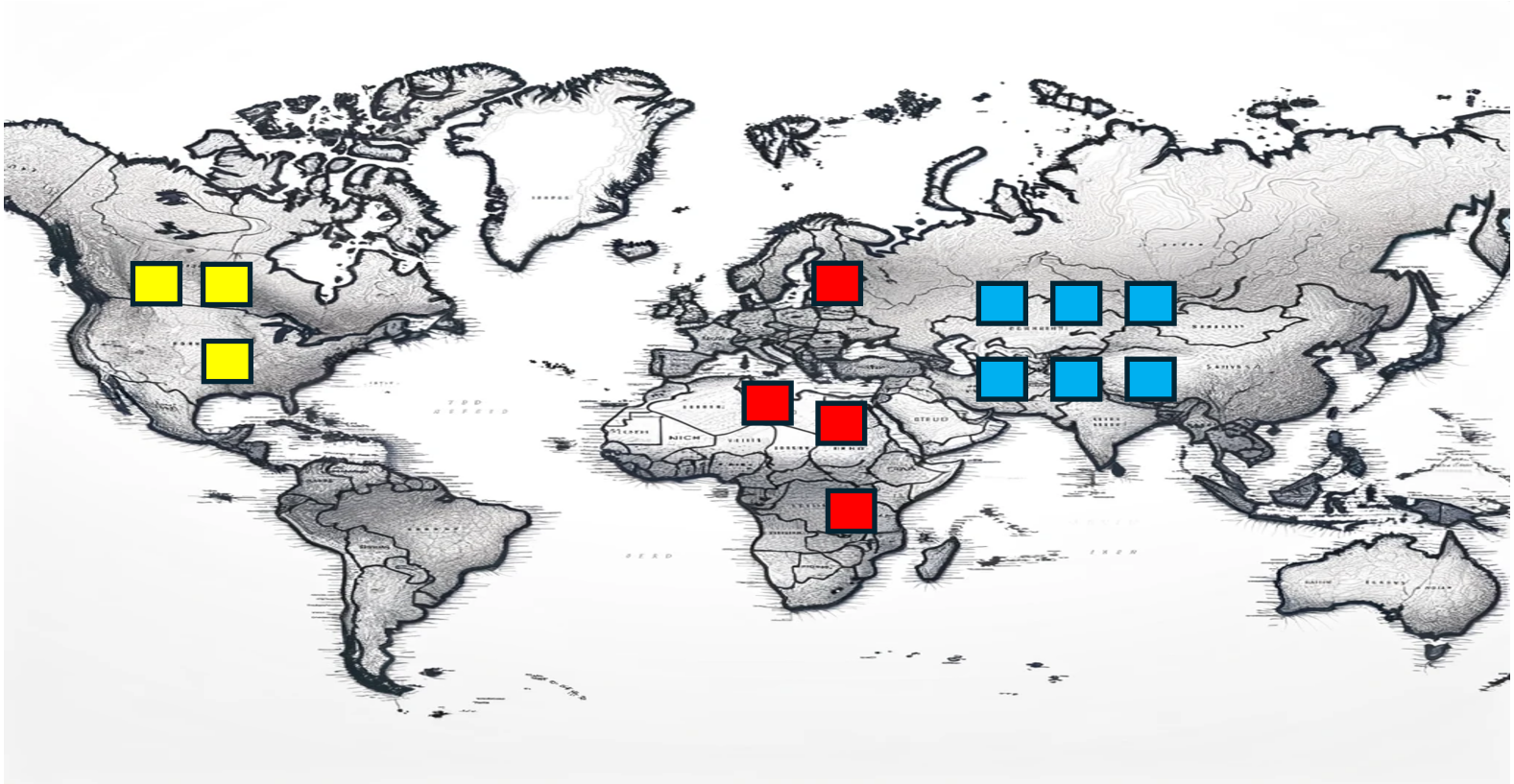
- In LARMix, our goal is to reduce the link delay caused by mixnets, thereby enhancing their usability.
- LARMix achieves this through the following steps:

LARMix: Latency-Aware Routing in Mix networks

- In LARMix, our goal is to reduce the link delay caused by mixnets, thereby enhancing their usability.
- LARMix achieves this through the following steps:
- Step 1) Diversified mixnode arrangement.
- Step 2) Low-latency routing.
- Step 3) Rebalancing the mixnet.

Clustering the mixnodes

- Mixnodes are clustered based on their geographical location features.

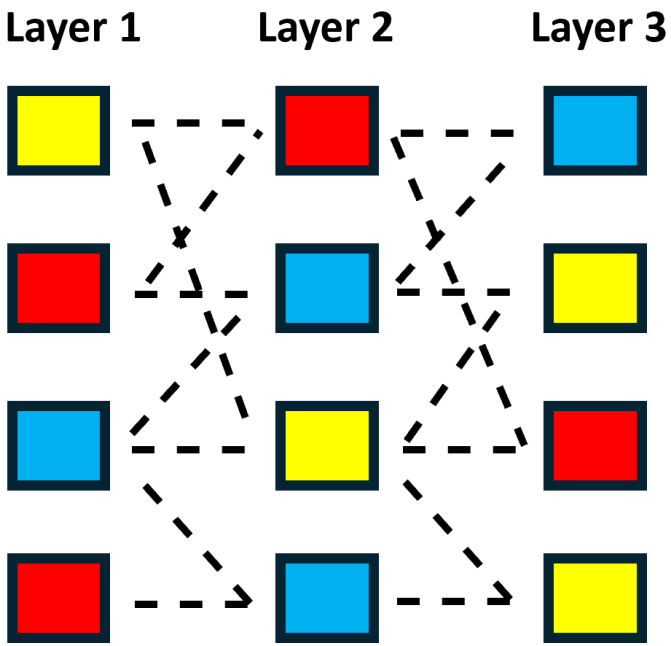


Mixnet Arrangement

- Instead of randomly assigning mixnodes to the mixing layer as in the vanilla approach, we propose using a diverse set of mixnodes for each mixing layer.

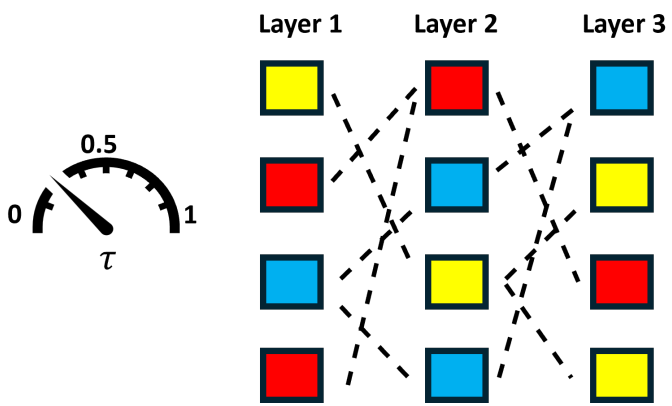
Mixnet Arrangement

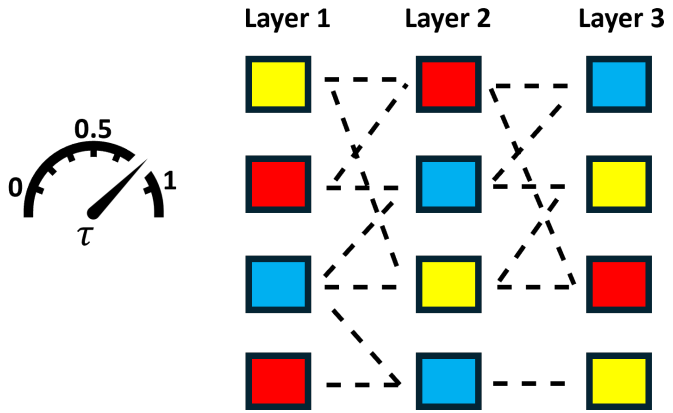
- Instead of randomly assigning mixnodes to the mixing layer as in the vanilla approach, we propose using a diverse set of mixnodes for each mixing layer.
- **Diversification: Ensures that each mixing layer has an adequate number of nodes with diverse geographical locations.**



Low-Latency Routing Policy

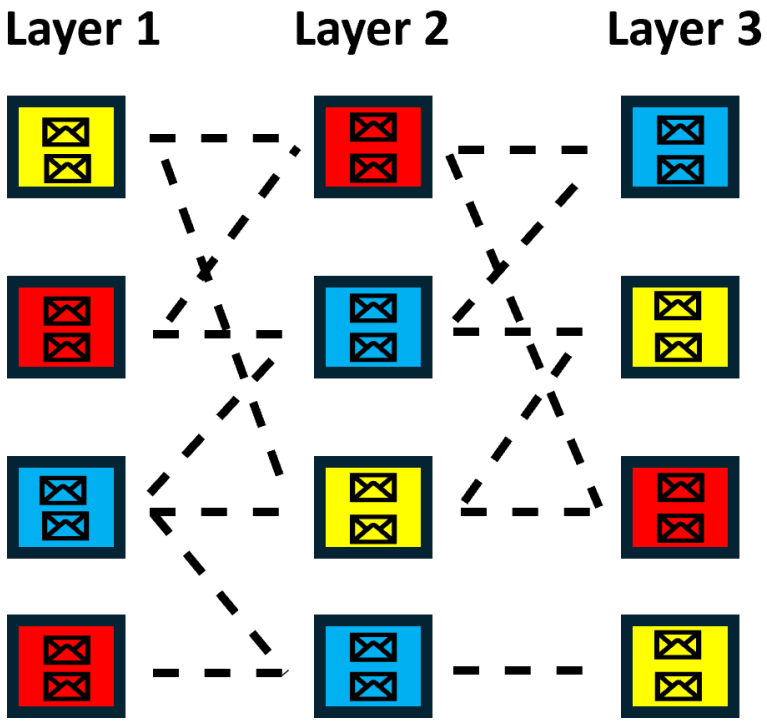
- Routing policies will be defined based on the latency between the mixnodes and the parameter $0 \leq \tau \leq 1$.
- The lower the value of τ, the more deterministic and low-latency the paths are, and vice versa.
- Tuning the variable τ provides clients with the flexibility to adjust routing from the lowest latency to fully uniform distribution.





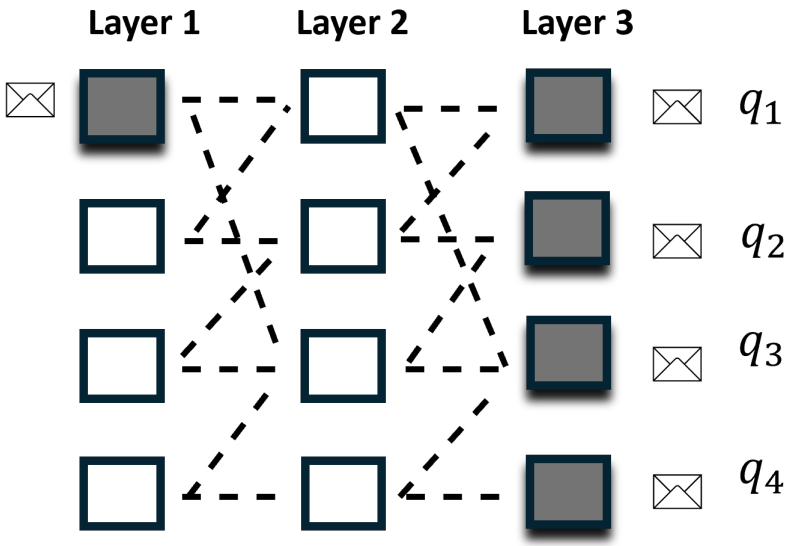
Balancing the mix network

- Introducing bias toward low-latency paths may overload some mixnodes.
- **Naive Algorithm**: Balancing the mixing layers in terms of **mixnode capacity**.
- **Greedy Algorithm**: Taking into account the **proximity of mix nodes** through an iterative approach.



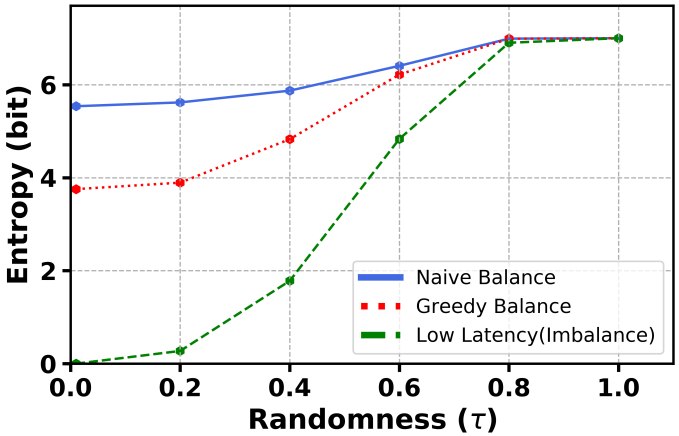
Metrics for evaluating LARMix

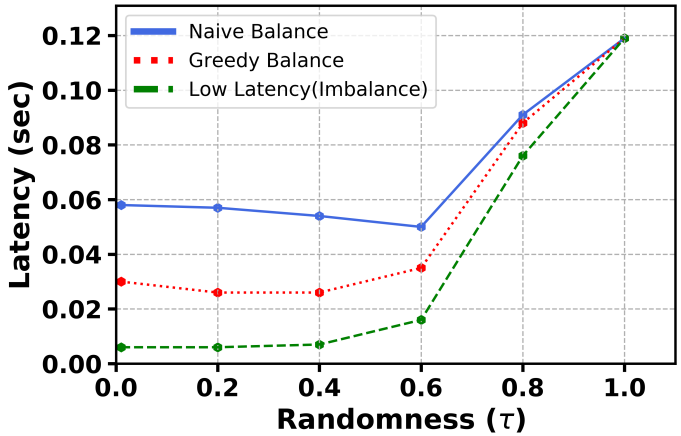
- In analytical approach, LARMix introduces the average link delay in mixnet as the average latency (l_{mix}).
- LARMix introduces the entropy of mapping the initial mixnode to the last in messages route as analytical anonymity.



$$H(T) = -\sum_{i=1}^{4} q_i \log q_i$$

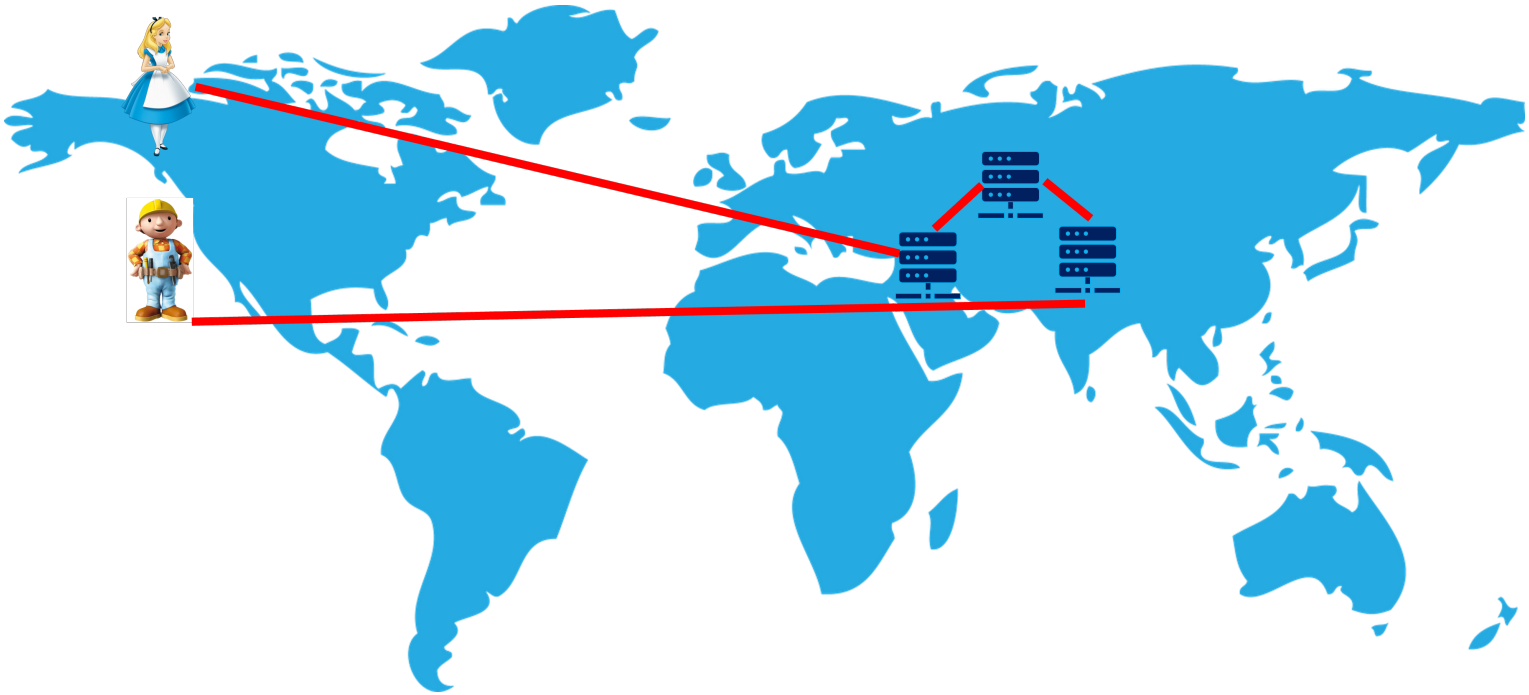
Evaluation: Analytic approaches





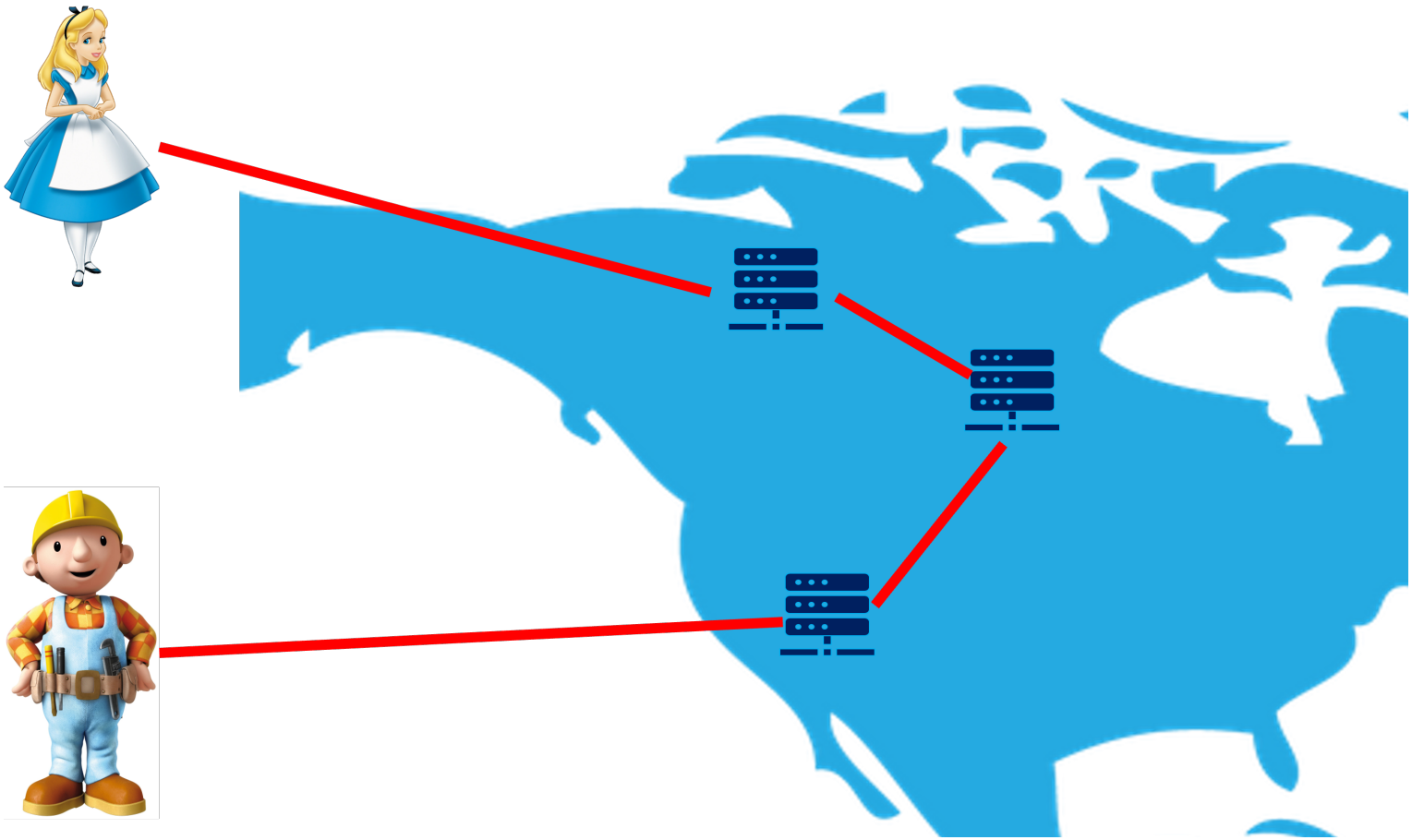
- Low latency approach ($\tau = 0.6$) reduces link delays to $\frac{1}{8}$ of vanilla routing, while preserving $\frac{5}{7}$ of anonymity provided by vanilla routing.
- Greedy and naive balancing approaches impose higher latency compared to low latency routing but provide a balanced network with higher anonymity.

LARMix



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

CLAM

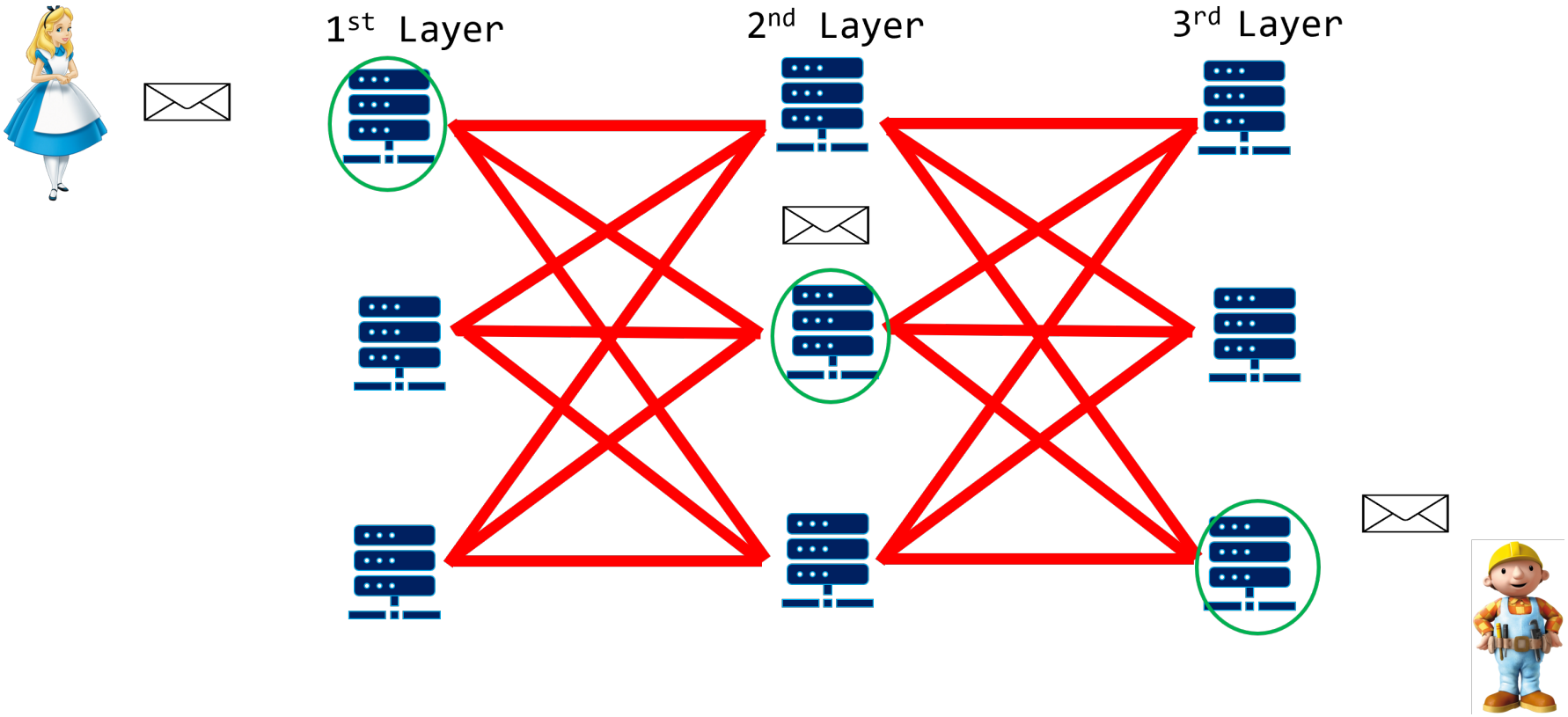


- CLAM provides low-latency routing from the client to the mix network.

CLAM, Results

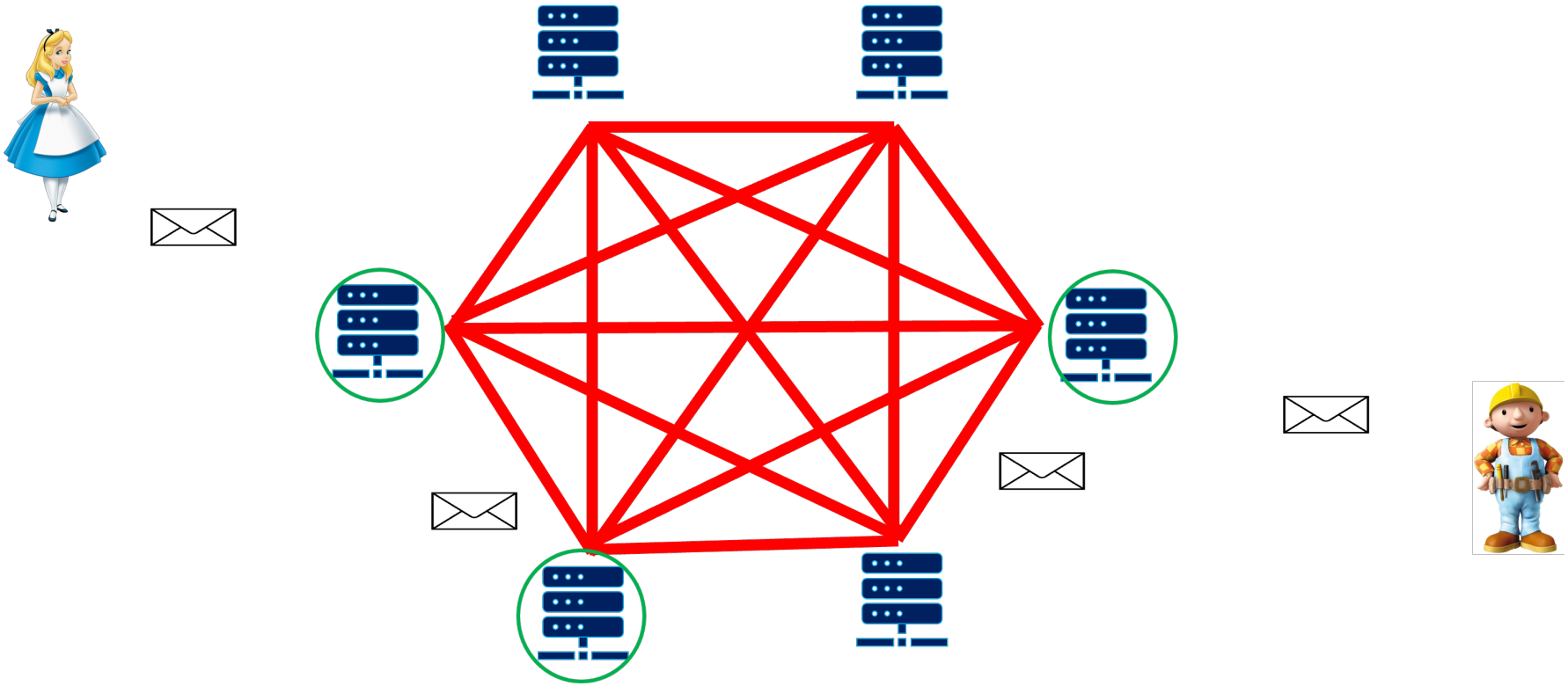
Routings \ Metrics	Latency	FC	Cost
Uniform	61 ms	0.008	Low
KαCloseness	20 ms	0.016	Low
Linear Programming	7 ms	0.018	High
Exponential distribution	7 ms	0.027	Low

LARMix++, Layered Structures



- Layered structures need an additional process to arrange nodes in layers.

LARMix++, Free Routes Topology



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

LARMix++, Results

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

Conclusion

- Mixnets incur high latency for end-to-end communication, which may result in poor user experience, specifically for latency-sensitive applications like web browsing.
- LARMix is the first work which implements strategic mixnet arrangement and low-latency routing, leading to a low latency mixnet, enhancing usability, without compromising a significant amount of message anonymity.
- CLAM can further enhance LARMix's latency reduction by extending it to include the client-mixnet link, while LARMix++ adapt LARMix to the Free Routes topology.

Thanks for listening :)

- Access to the paper, its implementation, this talk slides, and my webpage can be obtained via the following QR codes.



Figure: Paper



Figure: Implementations



Figure: Talk slides



Figure: My webpage