LARMix: Latency-Aware Routing in Mix Networks

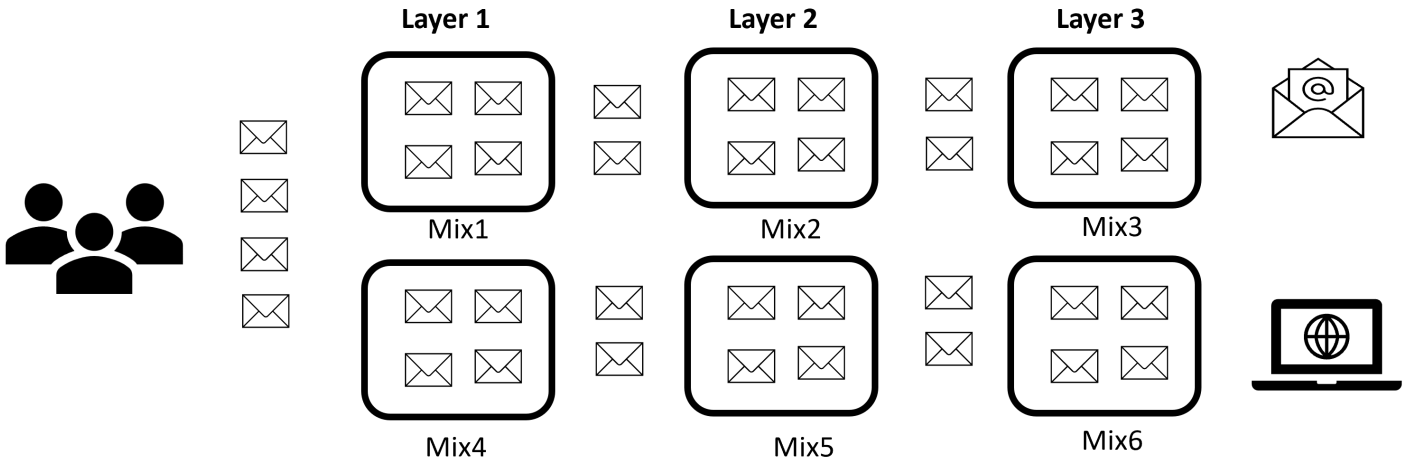
Mahdi Rahimi, Piyush Kumar Sharma and Claudia Diaz

mahdi.rahimi@esat.kuleuven.be

February 22, 2024

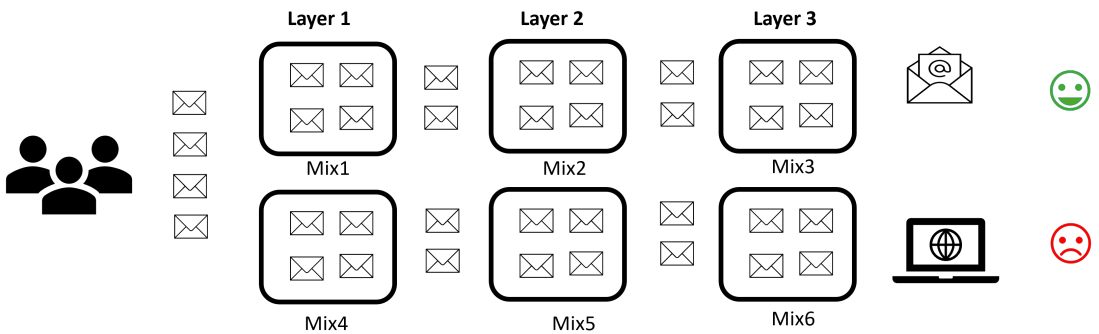
Background: Mixnet

- **Mix network (mixnet) is a layered network that ensures anonymity by relaying messages through multiple hops and reshuffling them at each hop.**
- Clients select intermediary hops and specify the amount of delay each hop should introduce for reshuffling messages based on an exponential distribution.

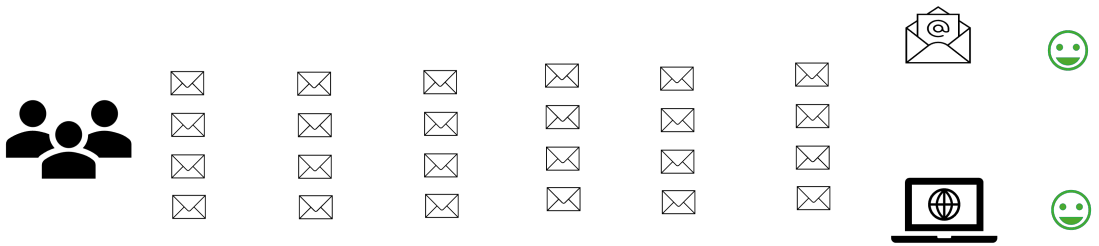


High end to end latency

- When considering a mixnet with L layers, the end-to-end latency for clients includes $L + 1$ link delays and L mixing delays, as opposed to direct transmission which incurs only one link delay.
- **This high latency restricts the application of mixnets for instant messaging or web browsing.**
- Mixnet:



- Direct transmission:



LARMix: Latency-Aware Routing in Mix networks

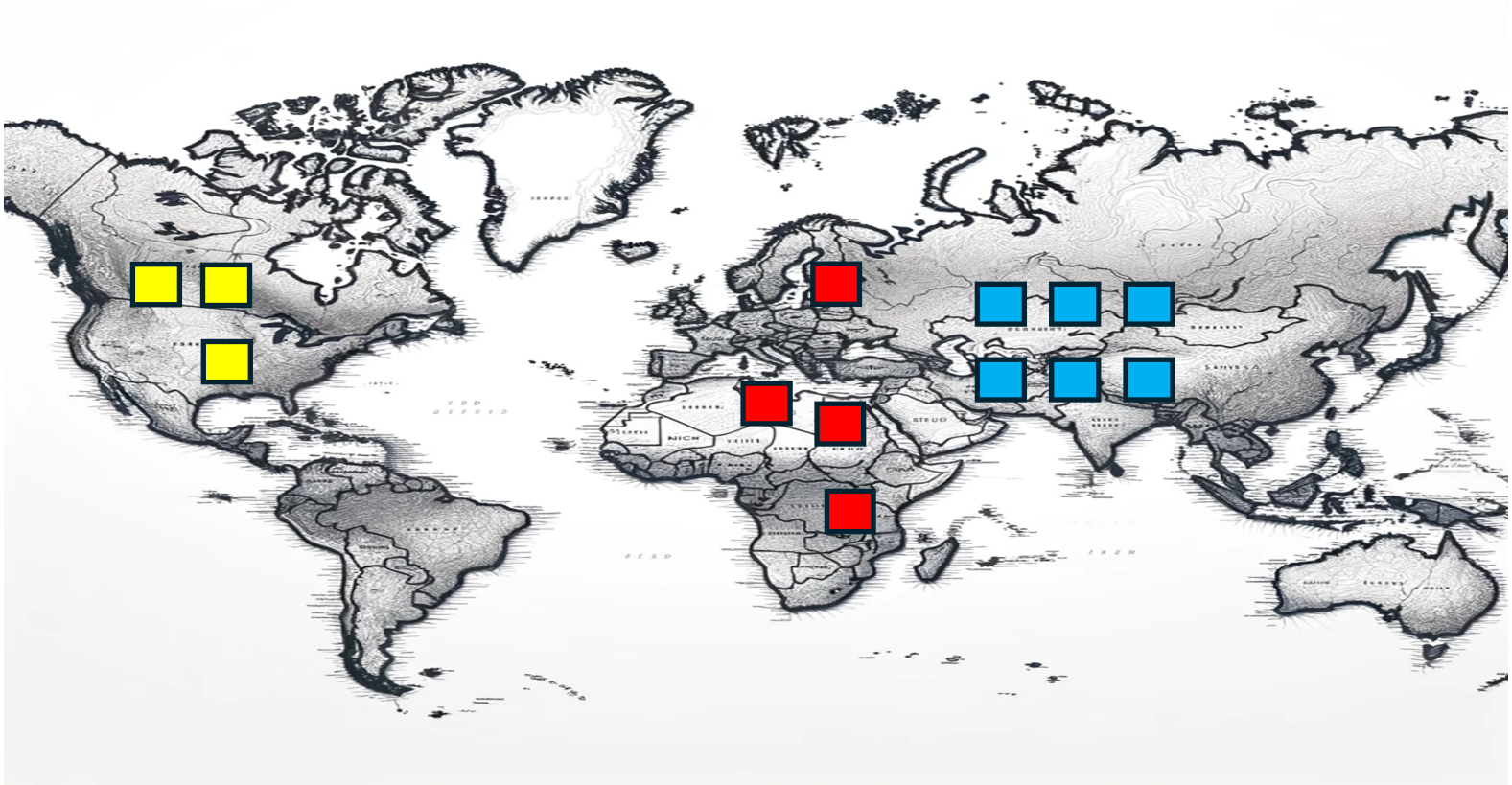
- In LARMix, our goal is to reduce the link delay caused by mixnets, thereby enhancing their usability.
- LARMix achieves this through the following steps:

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.

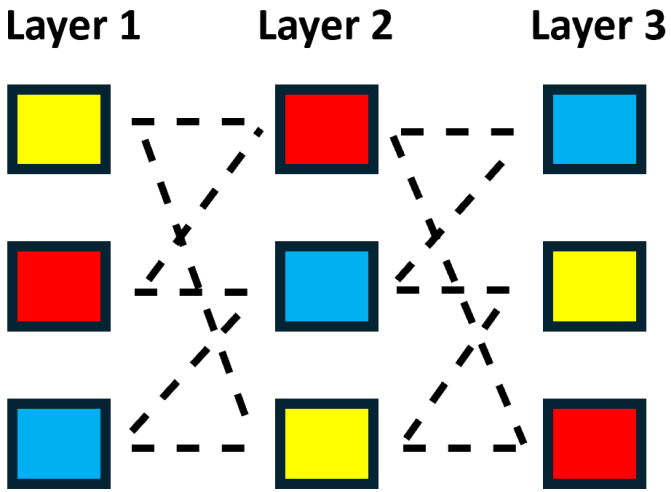


Mixnet Arrangement

- 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.

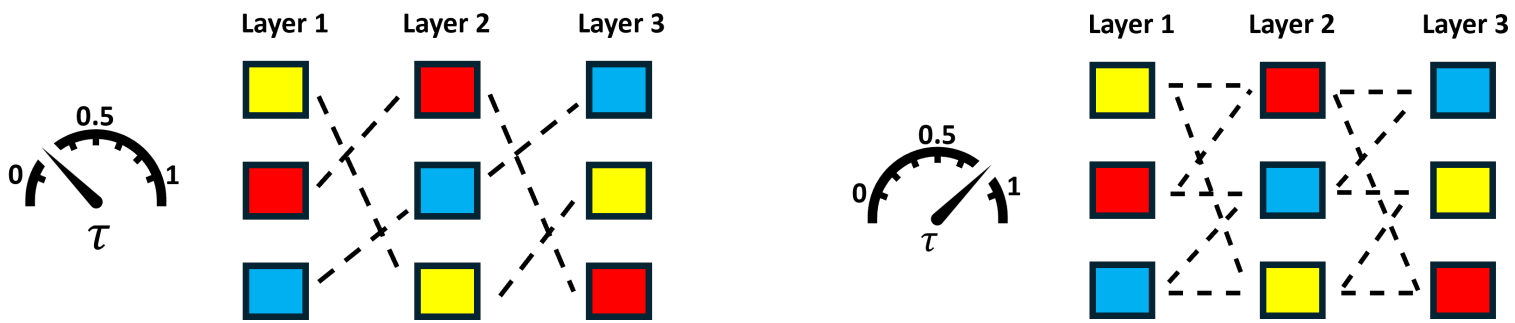
Mixnet Arrangement

- 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.**



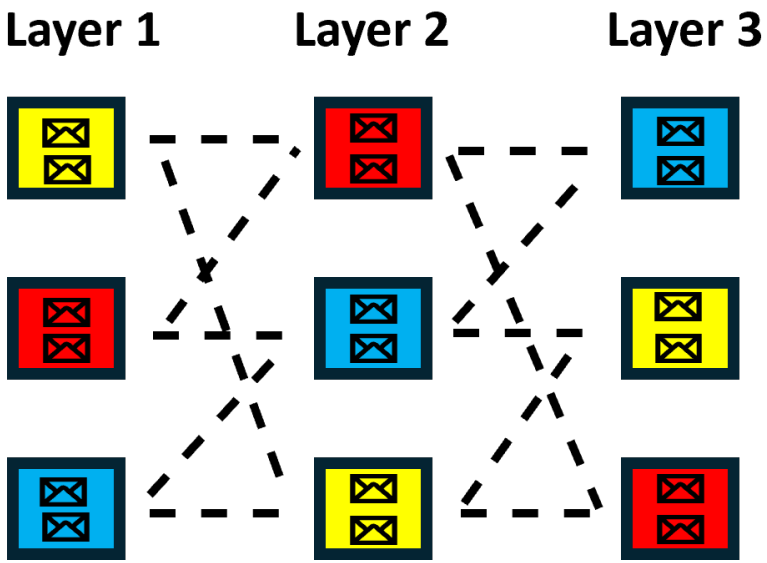
Low-Latency Routing Policy

- 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.

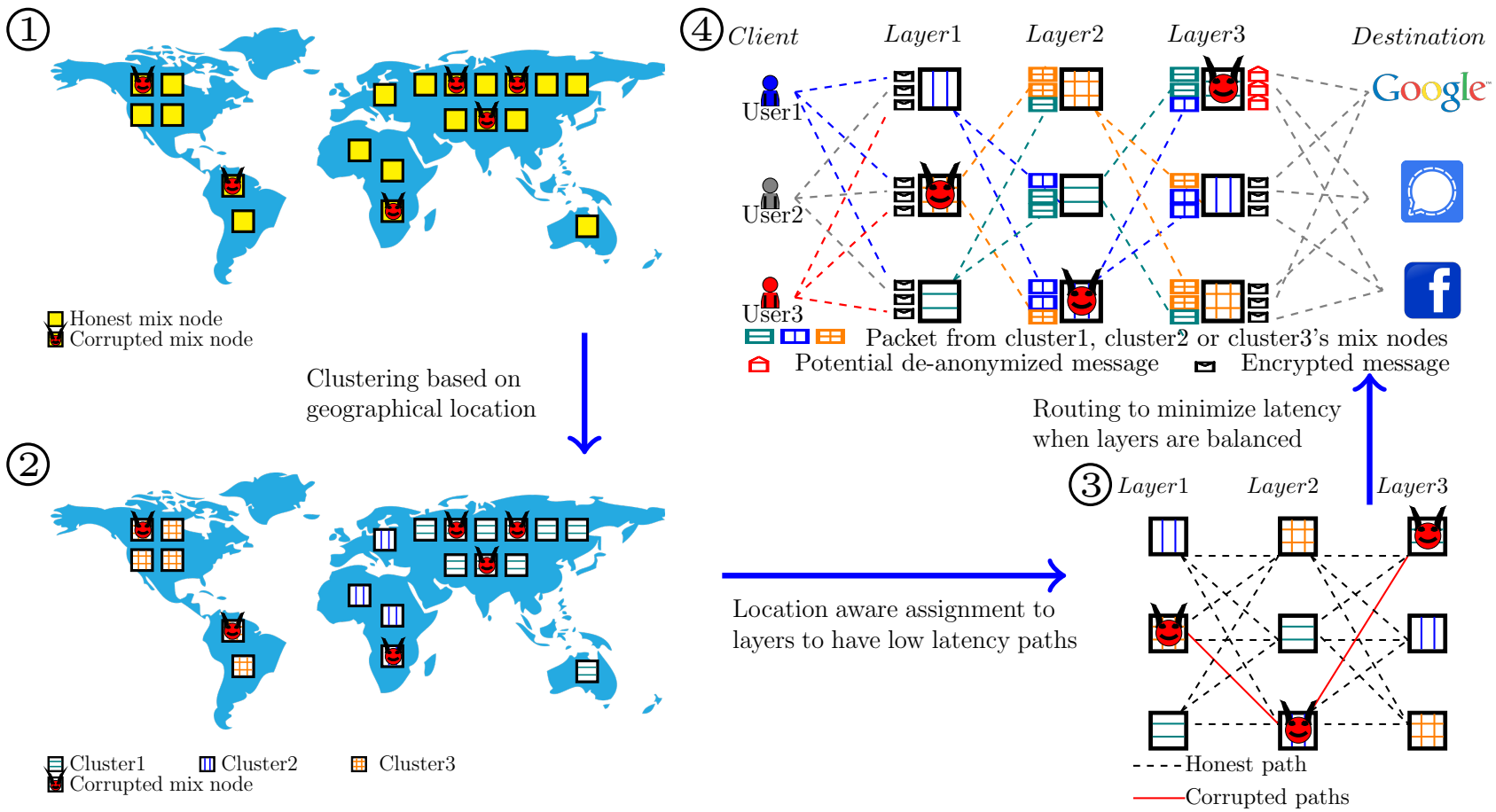


Balancing the mix network

- 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.

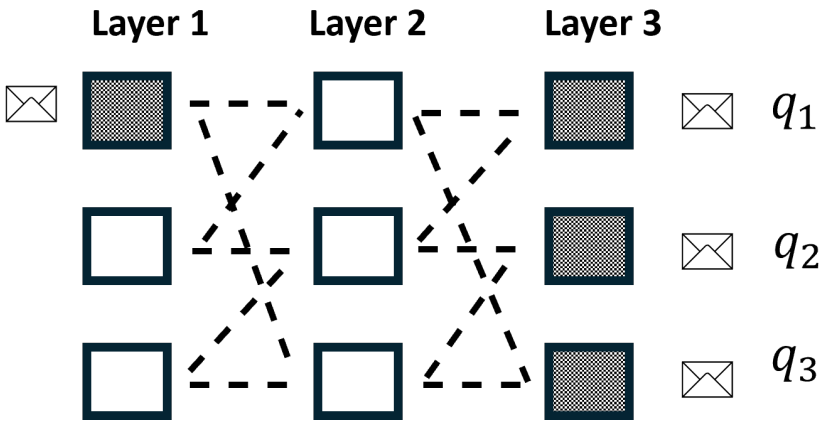


In a nutshell



Metrics for evaluating LARMix

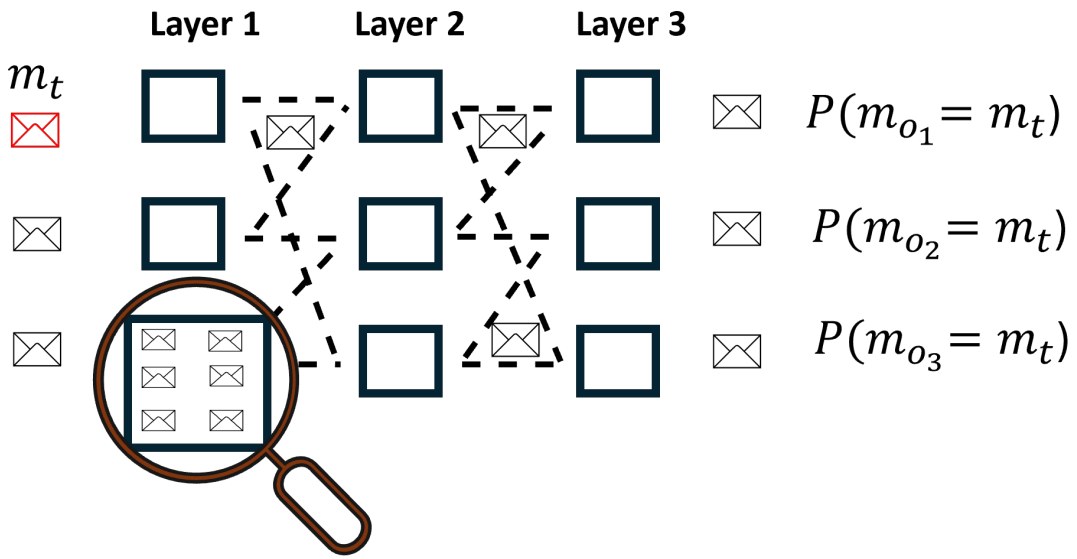
- In analytical approach, LARMix introduces the average link delay in mixnet as the average latency (l_{mix}).
- LARMix introduces the entropy of mapping the initial mixnode to the last in messages route as analytical anonymity.



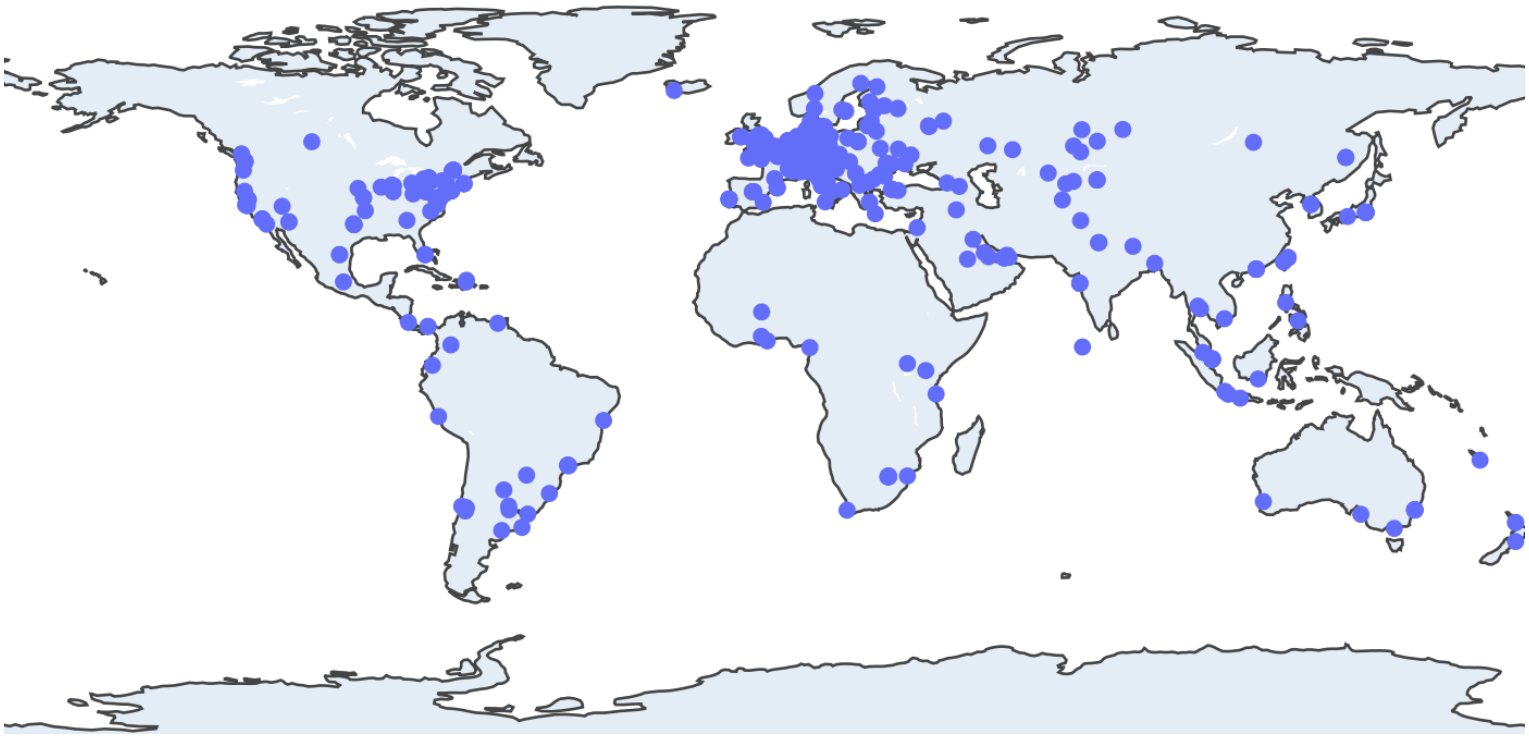
$$H(T) = -\sum_{i=1}^{3} q_i \log q_i$$

Metrics for evaluating LARMix

- In simulations, LARMix introduces the average link delay in mixnet plus the average mixing delay introduced by each mixnode as the average end-to-end delay (l_{e2e}).
- LARMix considers the discrete event simulation to account for both randomness in routing and the amount of mixing caused by each mixnode to measure target messages anonymity.
- $H(m_t) = -\sum_{i=1}^{3} P(m_{o_i} = m_t) \log\left(P(m_{o_i} = m_t)\right).$



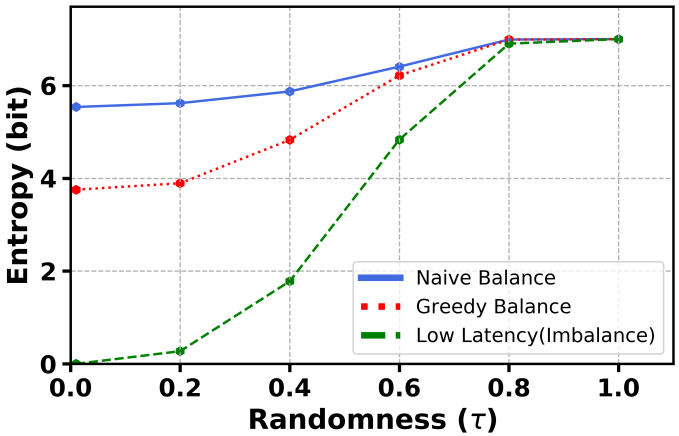
Evaluation Parameters

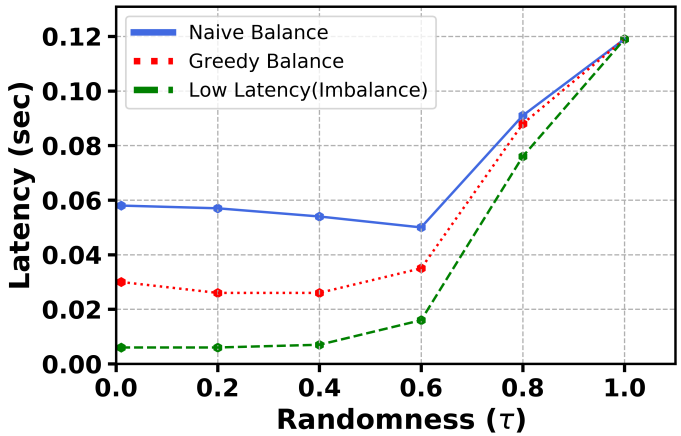


Parameter	Value
Topology	Stratified
Mix layers (L)	3
Size of network (N)	384
Layer size (W)	128
Mix latency (μ)	50 ms

Parameter	Value
Input traffic rate	10000 msgs per sec
Target messages	200
Iterations	400
Number of clusters (K)	5
Clustering method	K-medoids

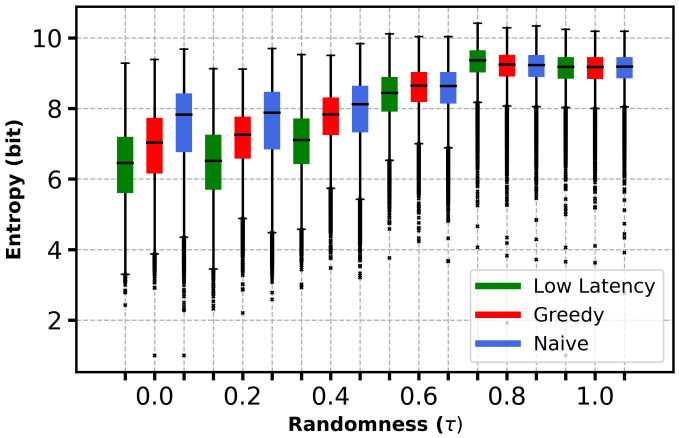
Evaluation: Analytic approaches

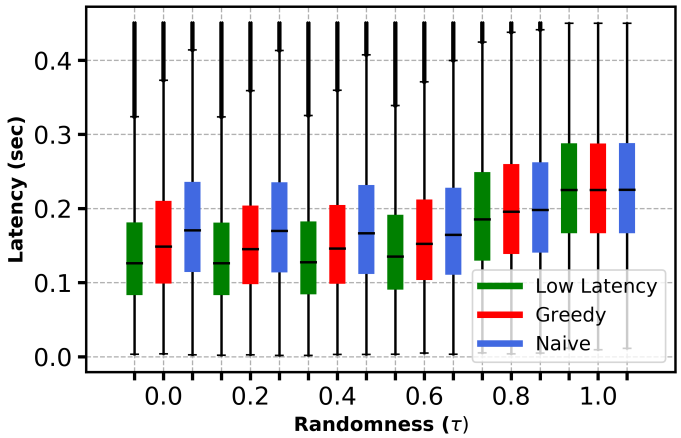




- Low latency approach ($\tau = 0.6$) reduces link delays to $\frac{1}{8}$ of vanilla routing, while reducing entropy by 2 bits.
- Greedy and naive balancing approaches impose higher latency compared to low latency routing but provide a balanced network with higher anonymity.

Evaluation: simulations





- In the simulation, we observed a similar trend, with an increase in latency due to the addition of mixnode delay in the simulation results.

Trade-off between mixing delay and link delay

- How to optimize the anonymity? Increasing τ or mixing delays?
- Imagine a scenario when there is a fixed average end-to-end latency to meet.
- In this case, clients aim to maximize anonymity of its messages.
- Increasing the value of τ or mixing delay both increase end-to-end latency and consequently the anonymity.

Trade-off between mixing delay and link delay

- How to optimize the anonymity? Increasing τ or mixing delays?
- Imagine a scenario when there is a fixed average end-to-end latency to meet.
- In this case, clients aim to maximize anonymity of its messages.
- Increasing the value of τ or mixing delay both increase end-to-end latency and consequently the anonymity.
- Considering an end-to-end delay of 200 ms, we found that $\tau = 0.7$ maximize the anonymity.

τ	0	.1	.2	.3	.4	.5	.6	**.7**	.8	.9	1
$\bar{l}_{mix}$	68.0	68.0	68.0	68.0	69.0	71.0	75.99	95.0	121.0	139.0	150.0
μ	44.0	44.0	44.0	44.0	43.6	43.0	41.3	**35.0**	26.3	20.3	16.6
H(T)	4.27	3.92	4.18	4.61	5.13	5.70	6.35	6.84	6.99	6.99	7.0
H(m)	6.48	6.63	6.75	7.0	7.28	7.62	7.98	**8.14**	7.68	7.0	6.4

Mixnode Adversary

- The adversary's goal is to maximize the fraction of fully corrupted paths (FCP), which will be achieved through different scenarios.

Mixnode Adversary

- The adversary's goal is to maximize the fraction of fully corrupted paths (FCP), which will be achieved through different scenarios.

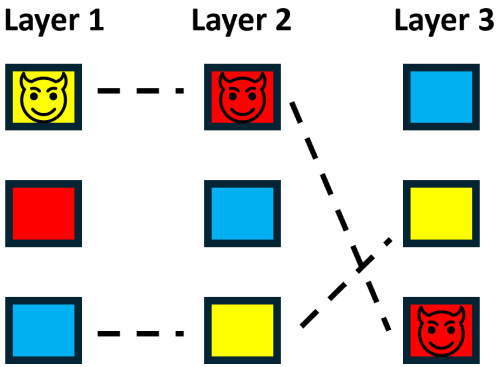


Figure: Worst Case

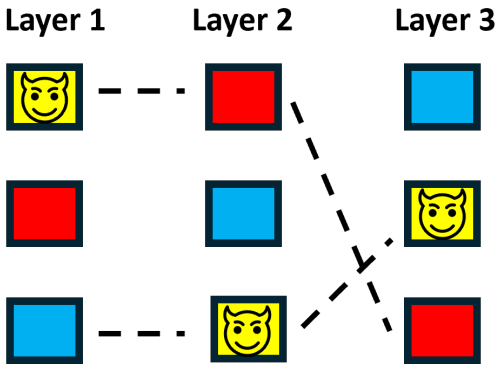


Figure: Single Location

Mixnode Adversary

- The adversary's goal is to maximize the fraction of fully corrupted paths (FCP), which will be achieved through different scenarios.

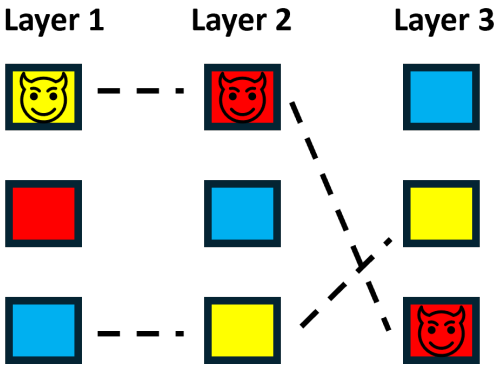


Figure: Worst Case

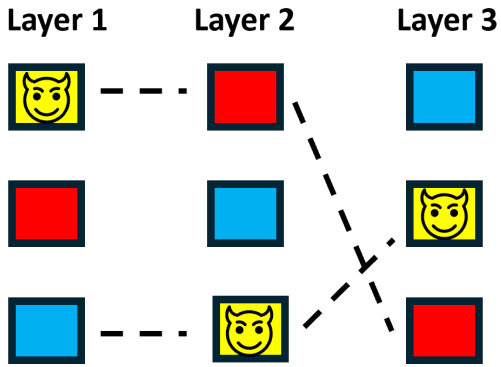


Figure: Single Location

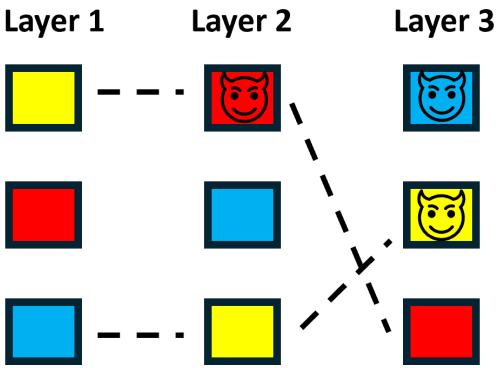


Figure: Diverse Location

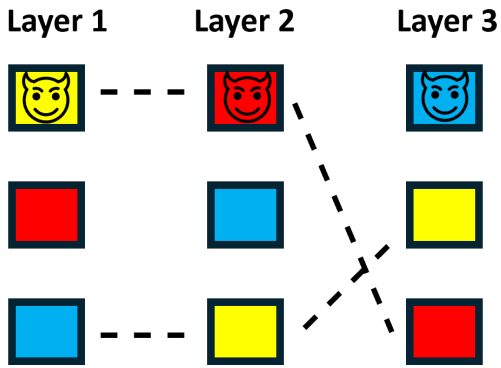
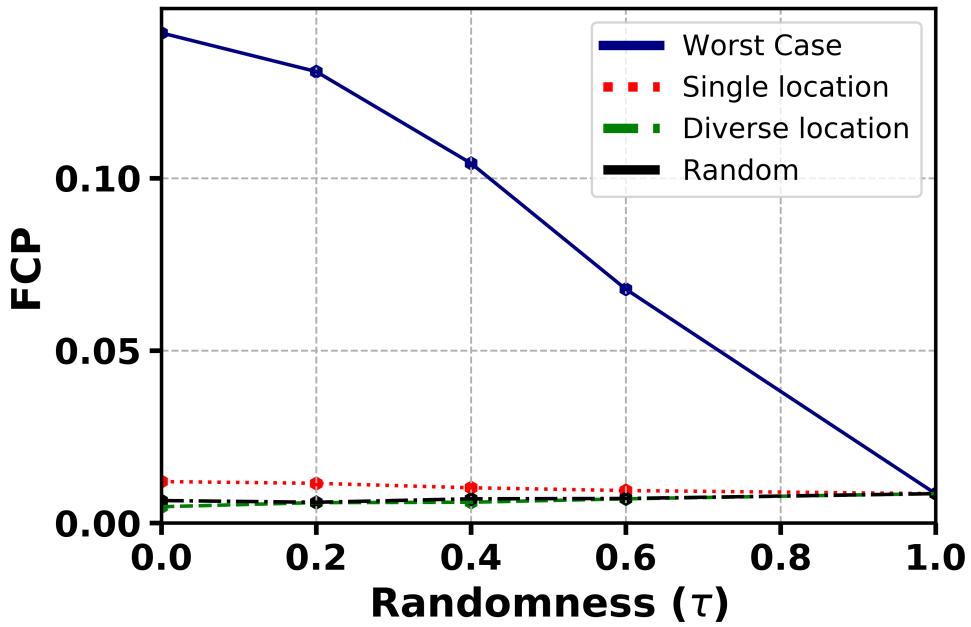


Figure: Random

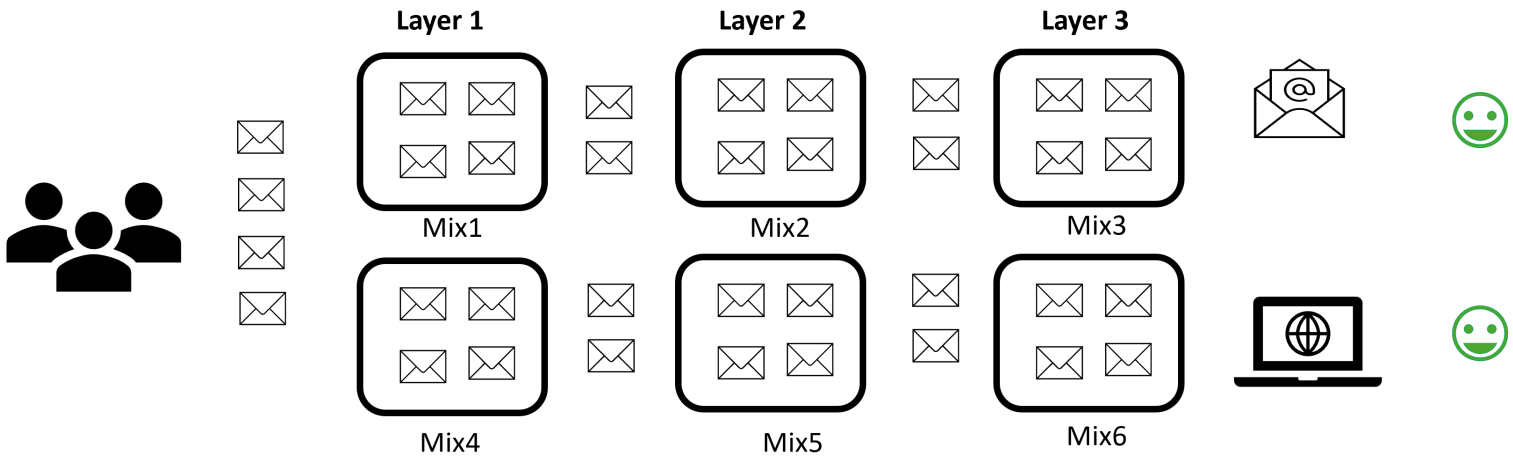
Mixnode Adversary



- The worst-case scenario can result in a dramatically high fraction of corrupted paths, but the chance of this scenario occurring is close to zero.
- An adversary who places all the mix nodes in one location wouldn't gain a significant advantage regarding vanilla approaches.

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.



Thanks for listening to LARMix :)

- 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