LARMix: Latency Aware Routing in Mix Networks

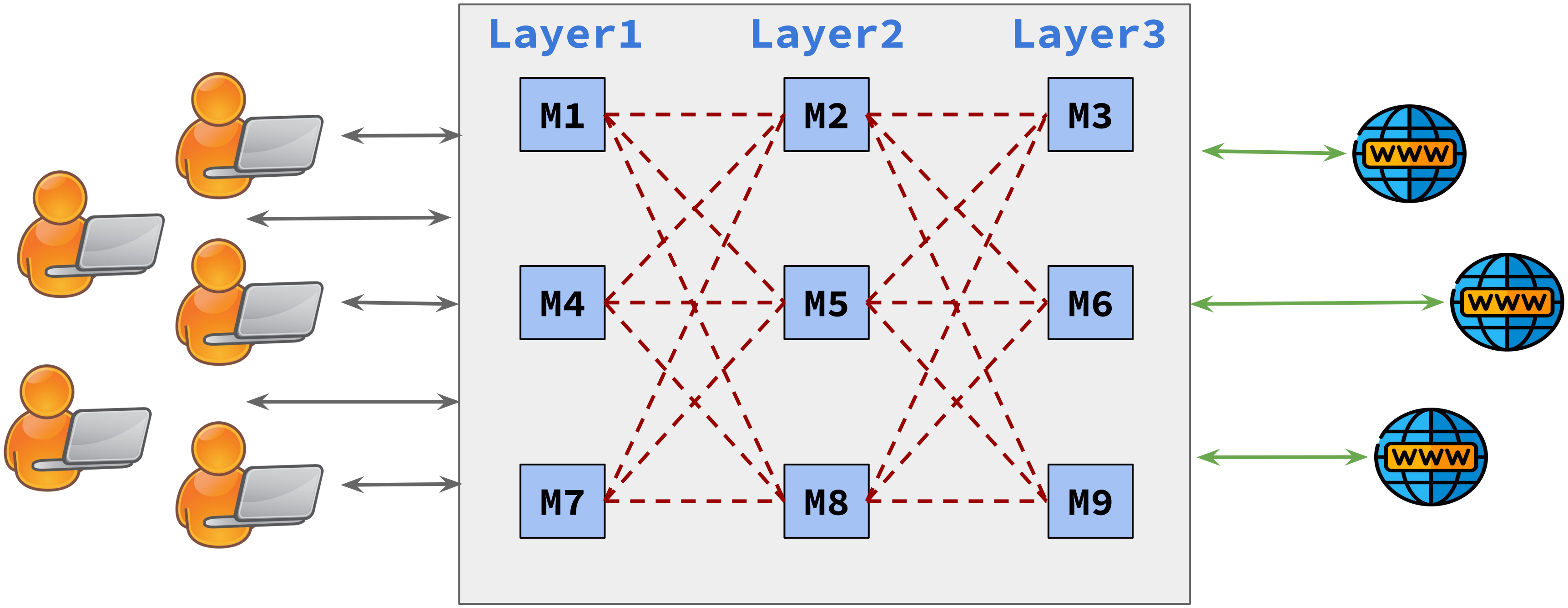
Mahdi Rahimi
Piyush Kumar Sharma
Claudia Diaz

KU LEUVEN

Mixnets

- A type of anonymous communication network
- Routes traffic through multiple hops
  - Providing anonymity from a local traffic observer
- Introduces delay
  - Providing anonymity from the global traffic observer
- Multiple types
  - Cascade mixes, continuous mixes, threshold mixnets, etc.
- Recent deployments
  - Nym network: Layered topology with poisson mixing

MIXNET



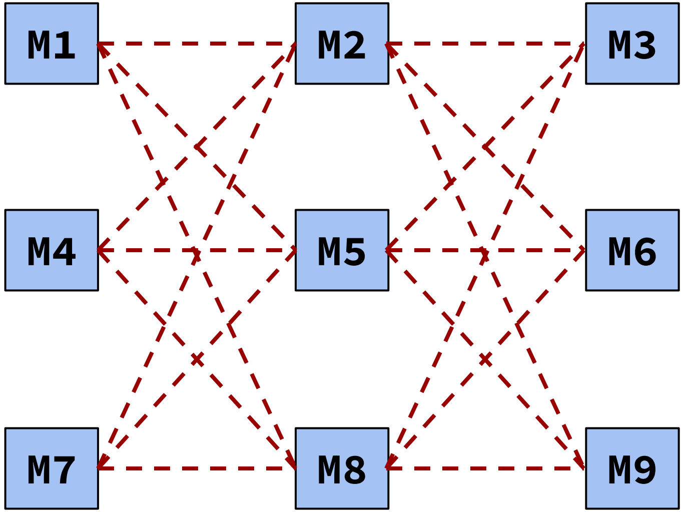
Latency in Mixnets!

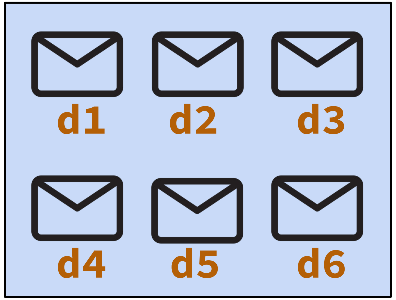
- High latency limits the type of applications supported by mixnets
  - Can support latency tolerant applications: email, bitcoin transaction
  - Suffers in supporting: instant messaging, web browsing

- Q: Can we reduce the latency in mixnets to facilitate support for wider range of applications?
  - What impact will it have on anonymity?

Types of latency

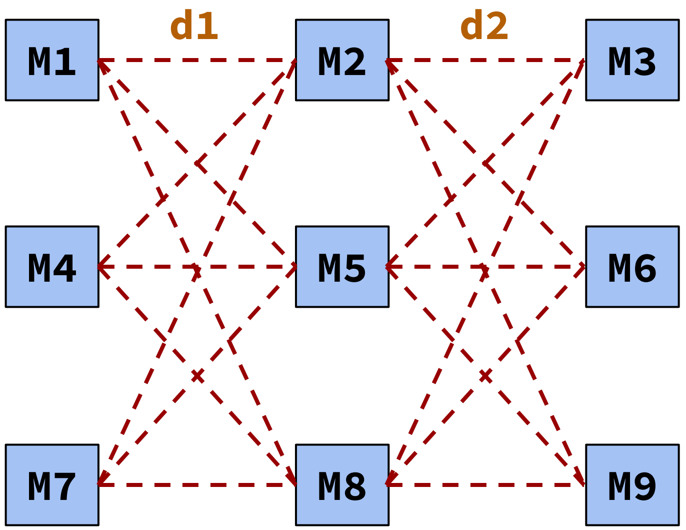
- Mixing latency at each mixnode
  - Direct impact on anonymity





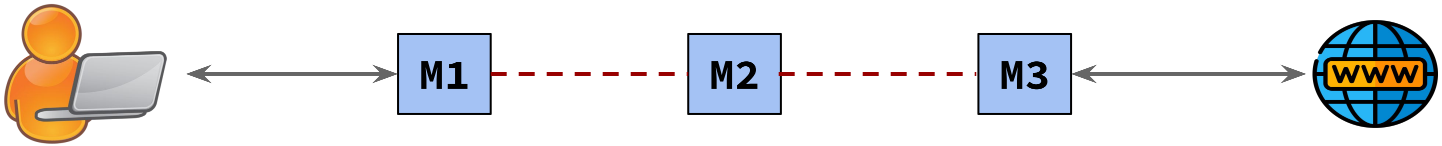
Types of latency

- Propagation latency
    - Indirectly impacts anonymity



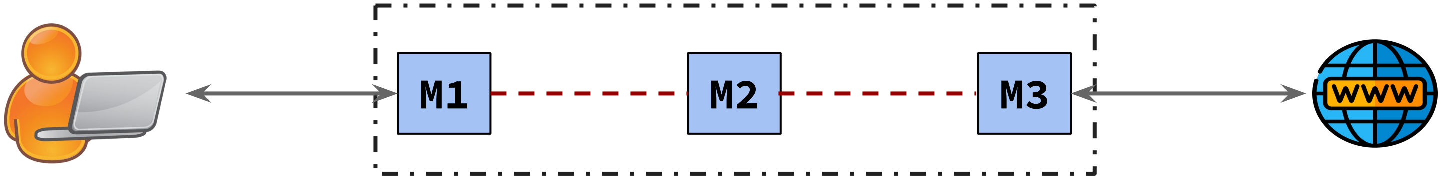
Which latency can we minimize?

- Interested in minimizing propagation latency



Which latency can we minimize?

- Interested in minimizing propagation latency



LARMix goals and threat model

- Develop methods to minimize propagation latency while minimizing impact on anonymity

- Provide a tunable parameter to control latency-anonymity tradeoff
  - Value 0 -> completely deterministic routing
  - Value 1 -> uniform random routing

- Ensure balancing traffic load in the network

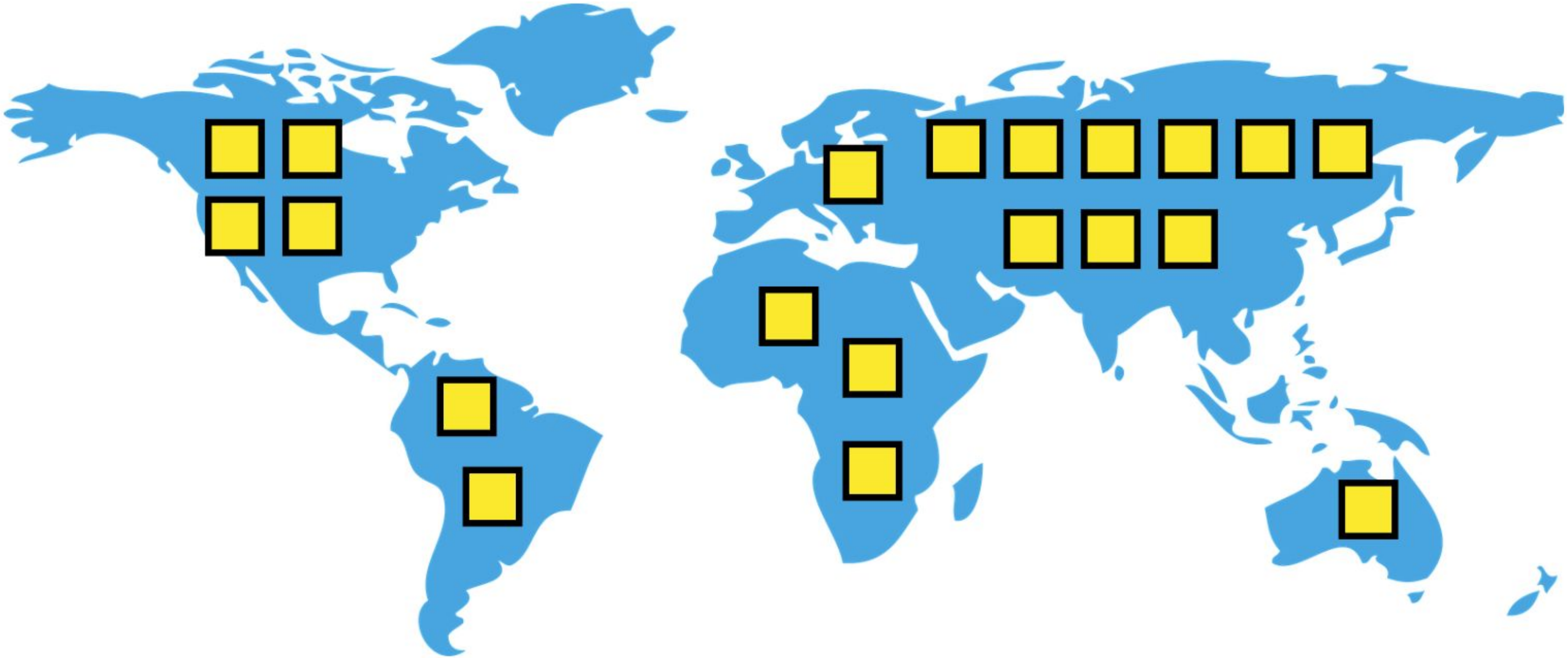
LARMix overview

- Developed approaches for a network designer:
  - To be used at different stages of the mixnet
  - Could be used independently or in conjunction
- Step 1: Arranging mixnodes to support the routing policy
- Step 2: Novel routing policy to enable faster routes
- Step 3: Balance the network load

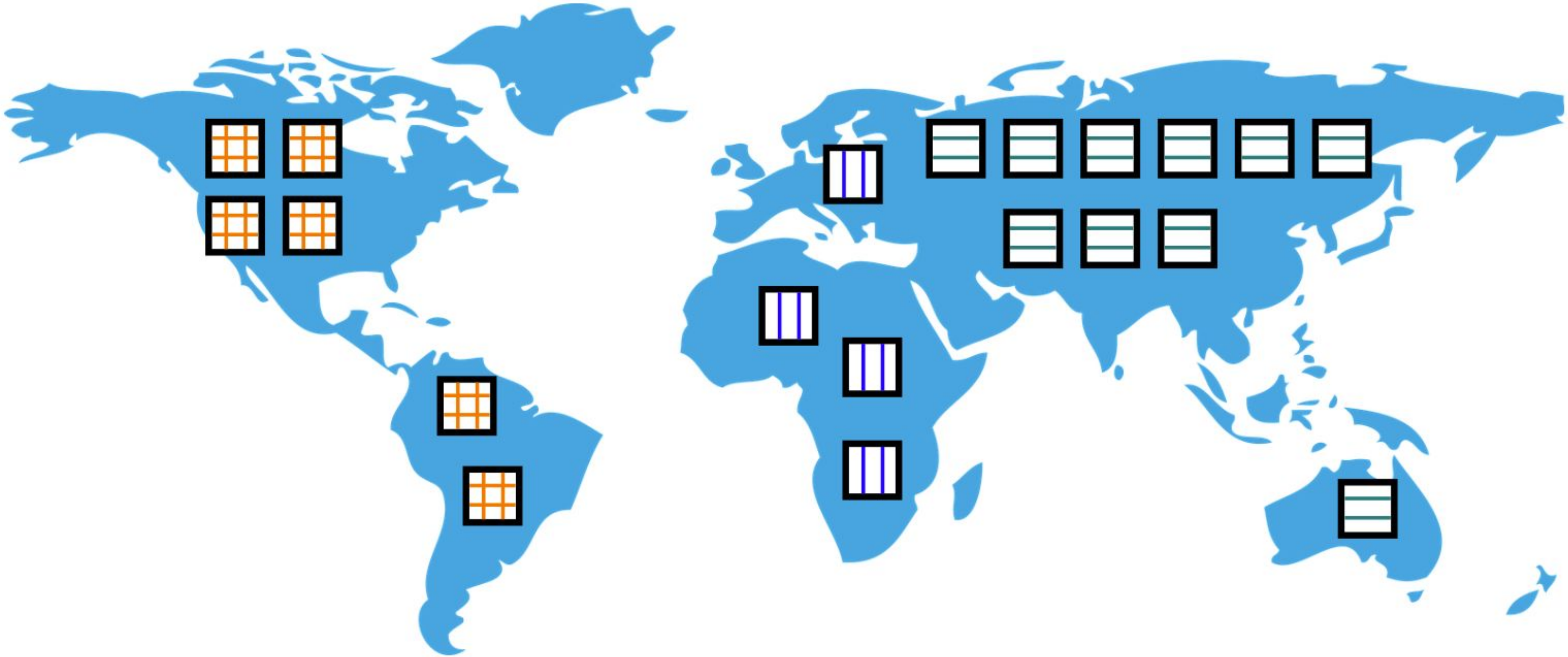
LARMix: Mixnet Arrangement

- Step1: Cluster mixnodes based on location
- Step2: Arrange them in layers via a diversification algorithm
    - The algo facilitates geographical diversity of nodes in each layer that could be exploited by the routing policy

LARMix: Mixnet Arrangement

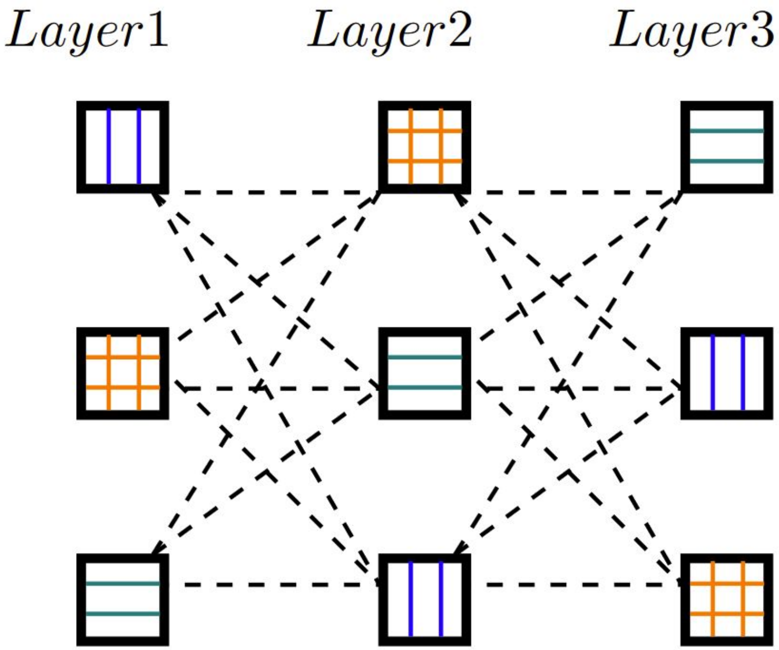


LARMix: Mixnet Arrangement



Cluster1 Cluster2 Cluster3

LARMix: Mixnet Arrangement



Routing policy

- We define a routing formula for selecting next hop
  - The formula returns probability distribution

$$\mathbb{P}[M^2 = m_j^2 | M^1 = m_i^1] = \frac{\left(\frac{1}{e}\right)^{R_i(j)\frac{(1-\tau)}{\tau}} \left(\frac{1}{l_{ij}}\right)^{(1-\tau)}}{\Sigma_k \left(\frac{1}{e}\right)^{R_i(k)\frac{(1-\tau)}{\tau}} \left(\frac{1}{l_{ik}}\right)^{(1-\tau)}}$$

- Tau = 0 results in deterministic next hop
- Tau = 1 results in uniformly selecting next hop

Load balancing

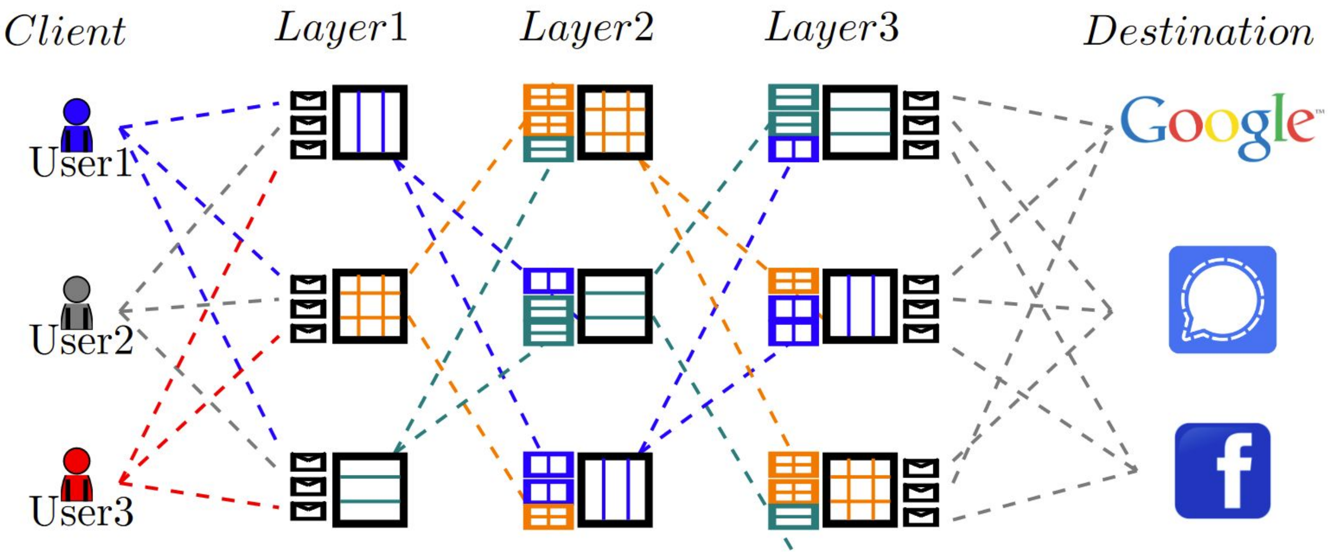
- Routing policy may create imbalanced load
- Need to ensure equal load on all mixnodes
- Identify the overloaded and underloaded nodes and rebalance the probability distribution.

Load balancing

- Greedy balancing:
  - Keep bias towards faster routes while balancing
  - Iterative

- Naive balancing:
  - Naively balance based on node capacity
  - One shot

Larmix: Routing + Balancing



Packets originating from cluster1 (green), cluster2 (blue) and cluster3 (orange) mixnodes

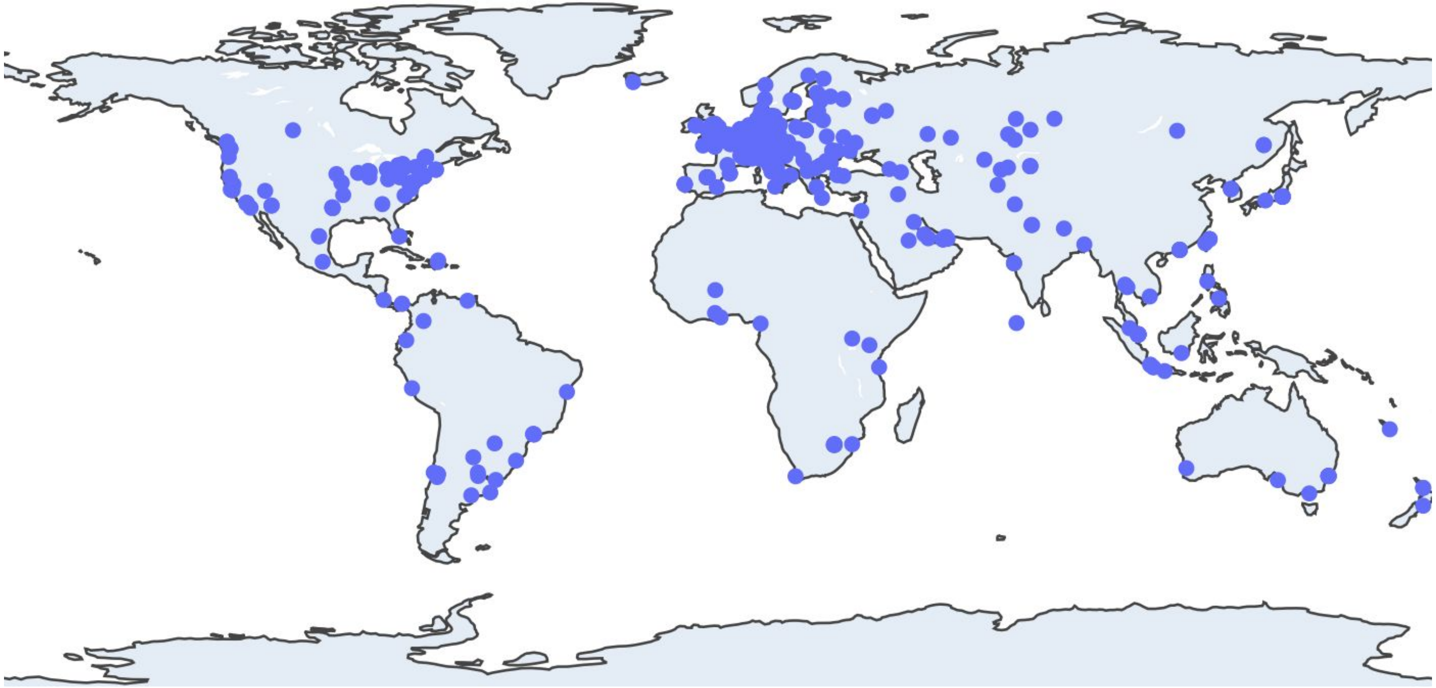
Evaluation overview

- Latency dataset used: RIPE anchor nodes delay measurement

- Performed two types of evaluation:
  - Analytical: A **novel approach** exclusively for routing evaluation
  - Simulations: For overall evaluation (routing + mixing)

- Metrics: latency (seconds) and anonymity (entropy)

RIPE Anchor Latency Dataset



Evaluation setup and 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

Experiments

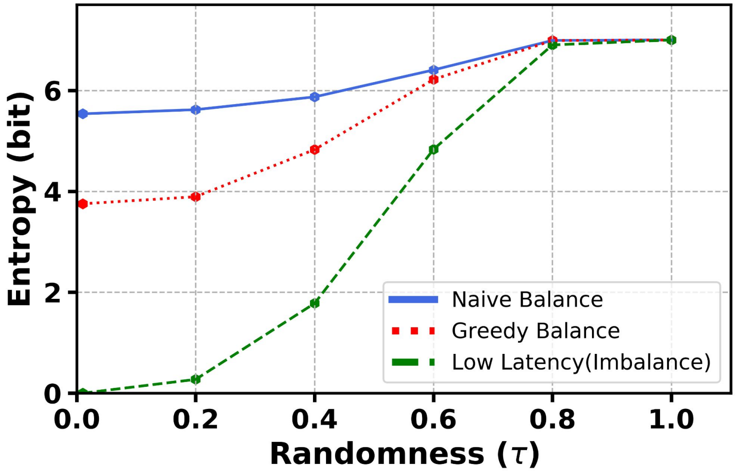
Experiment	Variables	Results
Latency aware routing	Arrangement + Routing + Balancing	Entropy + Latency
Meeting end-to-end delay constraints	Network & Mix latency + Routing	Value of τ with max entropy
Varying network size	Network size + Routing + Balancing	Entropy + Latency

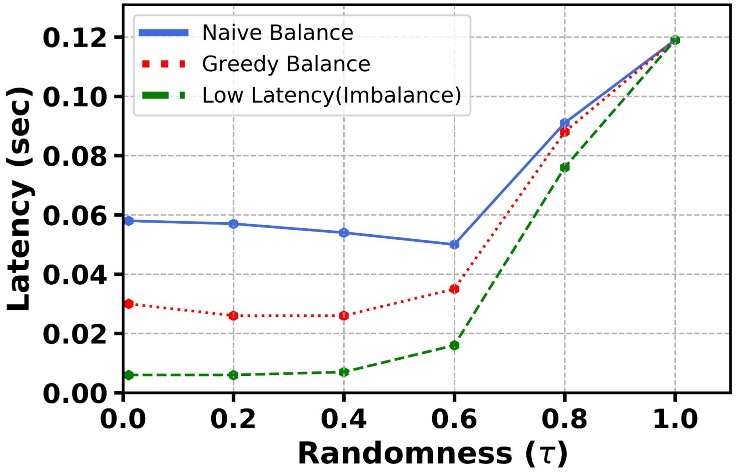
```
Arrangement = random, diversified, worst-case

Routing     = Tau ranging from 0 to 1

Balancing   = Imbalance, Greedy, Naive
```

Results: Analytical





3.5x reduction in latency for 0.8 bit loss in entropy.

Results: Delay constraints

- Given a latency constraint:
  - What should be the division between mixing and propagation delay for maximizing anonymity?
  - 200ms constraint

τ	0	.1	.2	.3	.4	.5	.6	**.7**	.8	.9	1
Propagation Latency	68.0	68.0	68.0	68.0	69.0	71.0	75.99	95.0	121.0	139.0	150.0
Mixing Latency	44.0	44.0	44.0	44.0	43.6	43.0	41.3	**35.0**	26.3	20.3	16.6
Entropy	6.48	6.63	6.75	7.0	7.28	7.62	7.98	**8.14**	7.68	7.0	6.4

Results: Delay constraints

- Given a latency constraint:
  - What should be the division between mixing and propagation delay for maximizing anonymity?
  - 200ms constraint

For a given latency constraint, maximizing anonymity requires a sweet-spot between mixing and routing latency

τ	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
Propagation Latency	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	121.0	139.0	150.0
Mixing Latency	44.0	44.0	44.0	44.0	43.6	43.0	41.3	**35.0**	26.3	20.3	16.6
Entropy	6.48	6.63	6.75	7.0	7.28	7.62	7.98	**8.14**	7.68	7.0	6.4

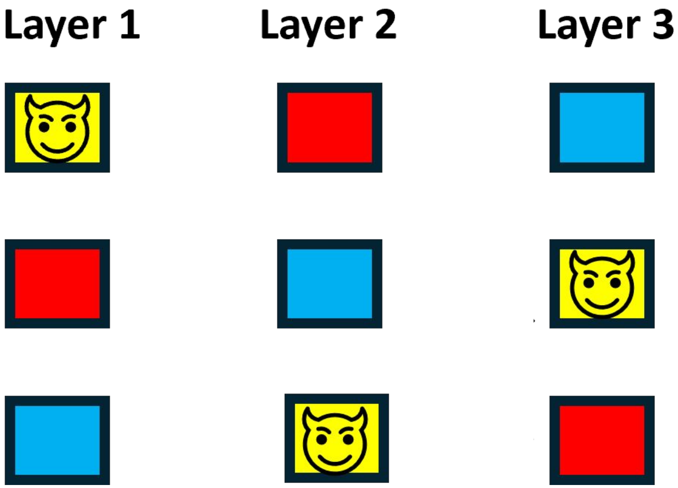
Security analysis

- Adversary
  - Global
  - Subset of mixnodes
  - Global + subset of mixnodes

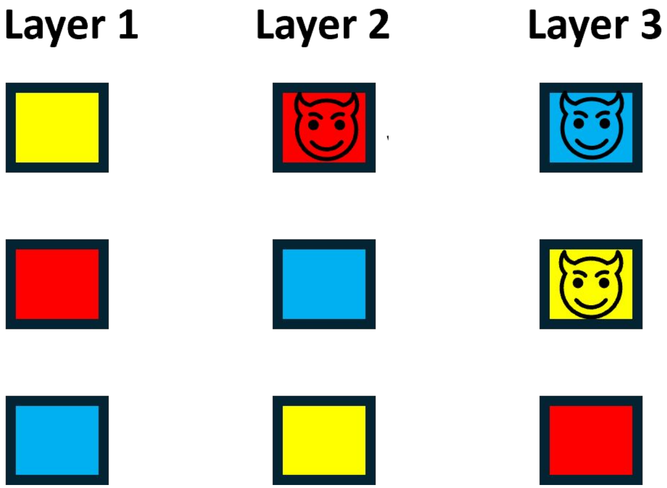
- Metrics
  - Fraction of Corrupted Paths (FCP)
  - Entropy

- Experiments
  - FCP vs Tau
  - FCP vs fraction of corrupted mixnodes
  - Entropy vs Tau

Security analysis: Types of mixnet adversary

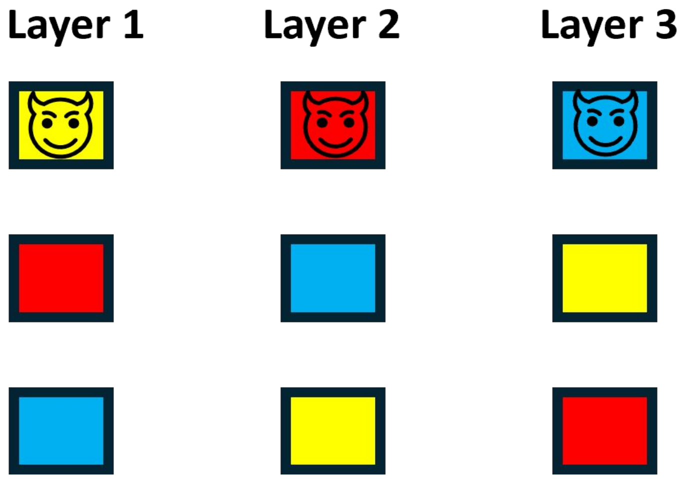


Single Location

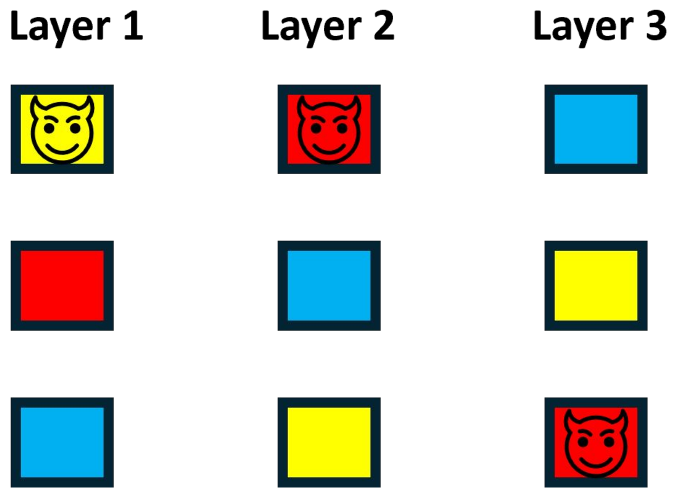


Multiple Location

Security analysis: Types of mixnet adversary

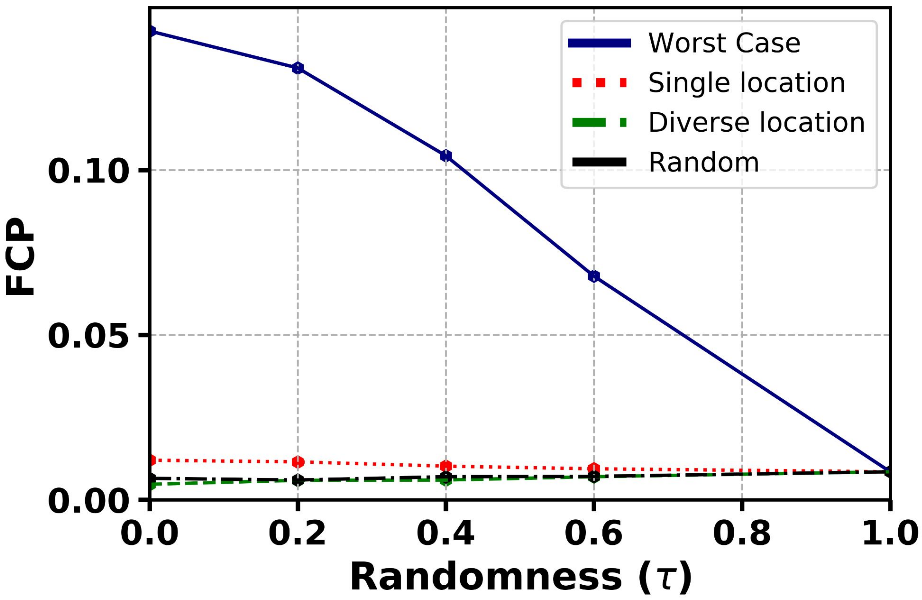


Worst Case



Random

Security Analysis: FCP vs Tau



- Corruption: 20%
- Worst case = high FCP
  - practically impossible
- Single location adversary doesn't provide unprecedented advantage

Comparison with simpler approach

Parameter	2-layer random routing	3-layer LARMix
Analytical Latency	46.9 ms	34.5 ms
Simulation Latency	170.2 ms	150.3 ms
Simulation Anonymity	7.7 bits	8.8 bits

CONCLUSION

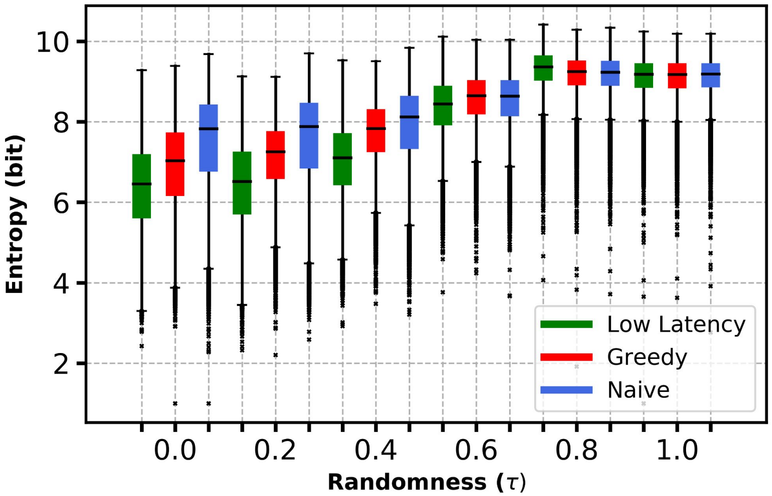
- Latency incurred by mixnets limits usage
- Developed LARMix, a latency-aware routing algorithm for mixnets
- Minimizes latency with limited anonymity impact all while ensuring load balancing
- Extensive evaluation demonstrates practicality
- Implementation code: public for reusability

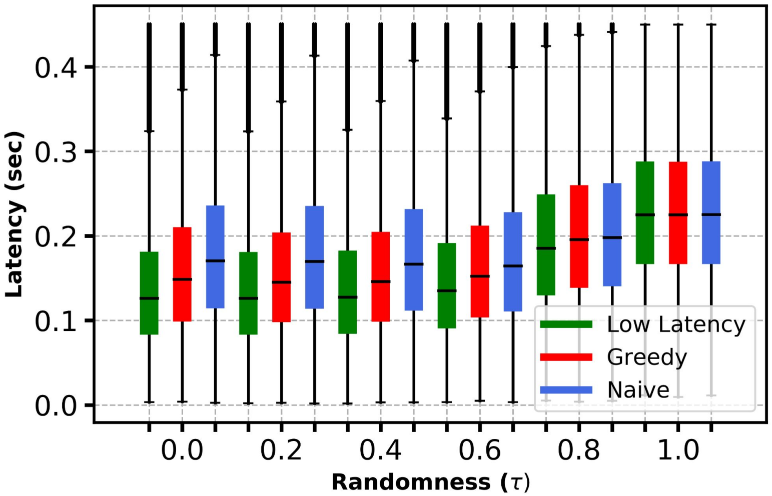
Appendix

METRICS

- Analytical
  - Latency: Average link delay across all possible paths
    Multiplied by the probability of selecting those paths
  - Anonymity: Entropy of mapping output mixnode to the input mixnode
- Simulation
  - Latency: Average link delay + mixing delay of sampled messages
  - Anonymity: Entropy of mapping output messages to the input messages

Results: Simulation





60% reduction in latency for 0.3 bits loss in entropy.

Comparison with state-of-the-art in tor (CLAPS)