LAMP: Lightweight Approaches for Latency Minimization in Mixnets with Practical Deployment Considerations

Mahdi Rahimi, **Piyush Kumar Sharma** and Claudia Diaz

Metadata Security

Diffie & Landau – ‘Privacy on the line’:

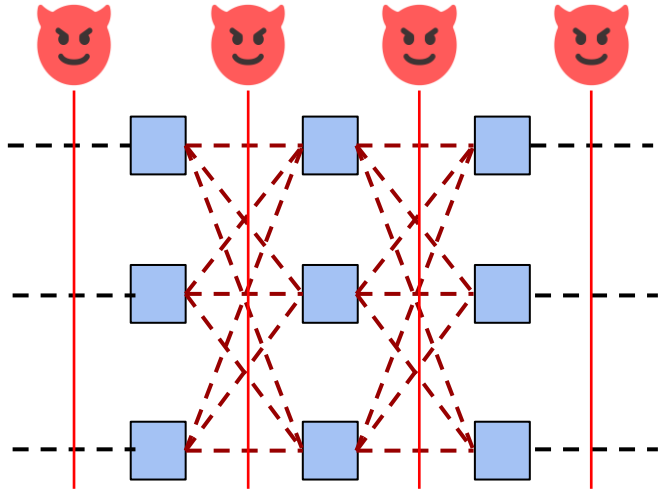
“Traffic analysis, not cryptanalysis, is the backbone of communications intelligence.”

NSA General Counsel Stewart Baker:

“Metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

Mixnets

- Perturb traffic by mixing and shuffling packets
  - Stronger protection
- Threat Model: Global Adversary
- Problem: High latency
  - Limits the kind of applications that could be supported

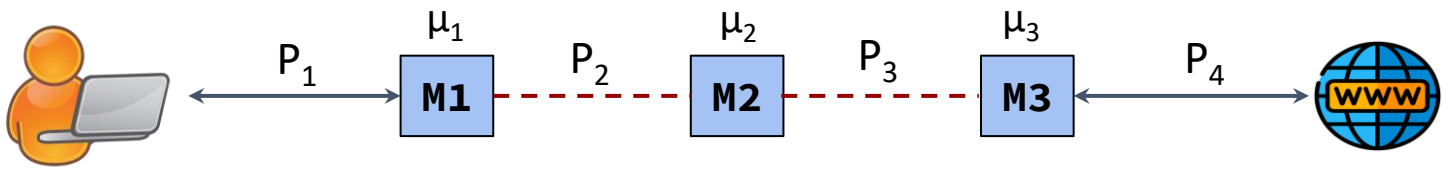


Latency Minimization

- Reducing latency facilitates wider application usage
  - Better privacy protection for end users

- **Mixing latency:** fundamental trade-off

- **Propagation Latency:** indirectly affects anonymity

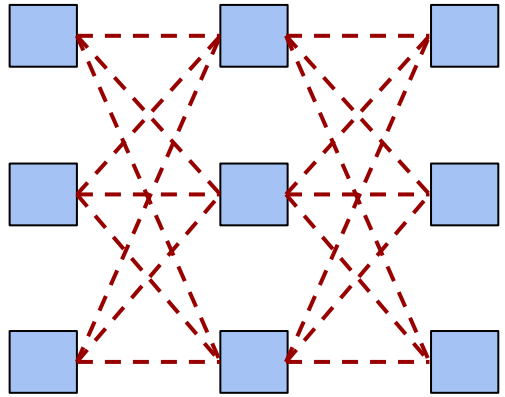


$$D = \{P_1 + P_2 + P_3 + P_4\} + \{\mu_1 + \mu_2 + \mu_3\}$$

Previous Work

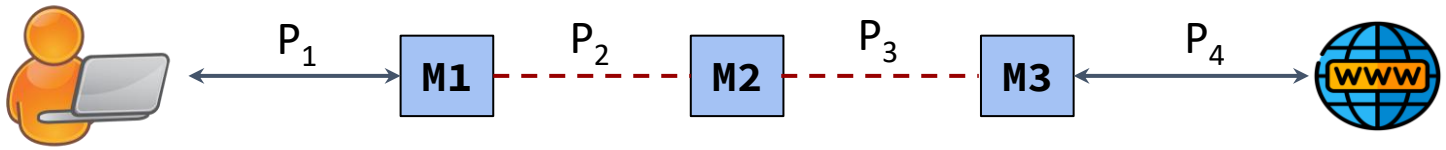
- LARMix (Rahimi et. al. NDSS'24)
  - Reduces **propagation latency**

- Provided a set of approaches for different stages of a mixnet
  - Arrangement (diversification algorithm)
  - Routing
  - Balancing



LARMix Challenges

1. LARMix's computation grows exponentially with the size of the network
2. Does not minimize latency from the client to the mixnet
3. Requires considerable changes to the original mixnet design



Practical Deployment Considerations

- Nym: the largest realistic deployment of a mixnet

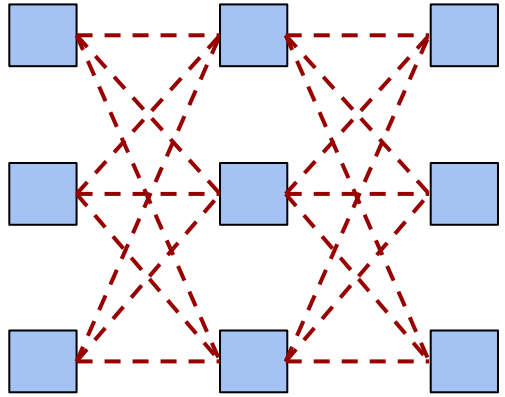
- For deploying latency minimization approaches
  - Lightweight
  - Easy to implement and integrate
    - Minimum codebase changes

LAMP Problem Statement

How to minimize latency in continuous mixnets while not significantly impacting anonymity

Lightweight & easy to integrate in existing deployments

Key ideas



- Random arrangement of nodes to layers
  - Saves computation
  - Minimizes codebase changes
- Create routing approaches with simpler designs
  - Require only a subset of the global network for routing policy computation
- Consider minimizing latency from the client to the last layer
  - Initially done from first to last layer
  - Balancing not possible

Key ideas

- Random arrangement of nodes to layers
  - Saves computation
  - Minimizes codebase changes

- Create routing approaches with simpler designs
  - Require only a subset of the global network for routing policy computation

- Consider minimizing latency from the client to the last layer
  - Initially done from first to last layer
  - Balancing not possible

LAMP Routing

1. Single Circle

2. Multiple Circles

3. Regional

Single Circle

Step1: Client measures latency to all mixnodes

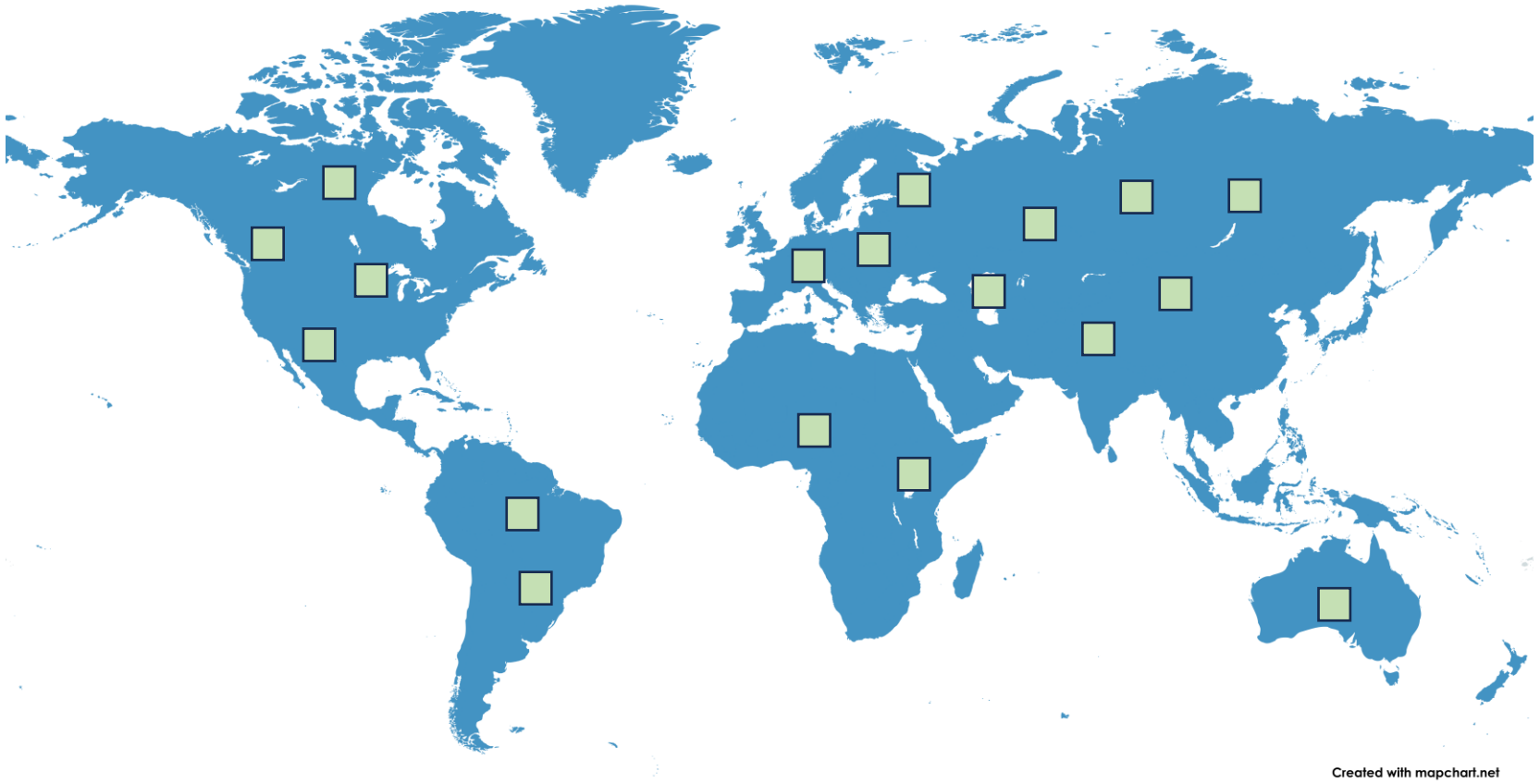
Step2: Forms a circle of radius ‘r’ with ‘r’ being the latency bound

Step3: Client creates a path among nodes within the latency bounded circle

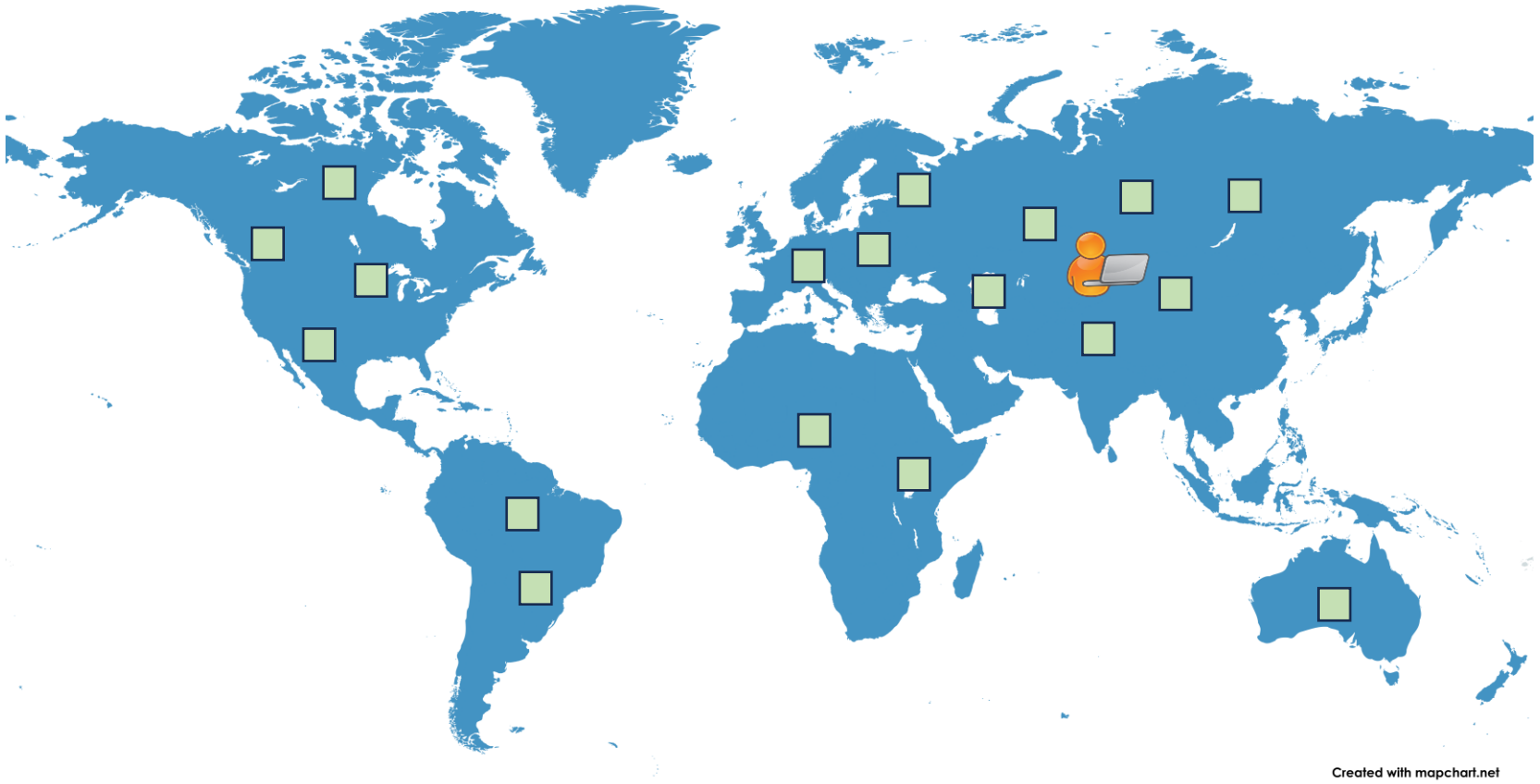
Multiple ways of creating a path

Constraint: Minimum ‘α’ % of mixnodes have to be part of the circle

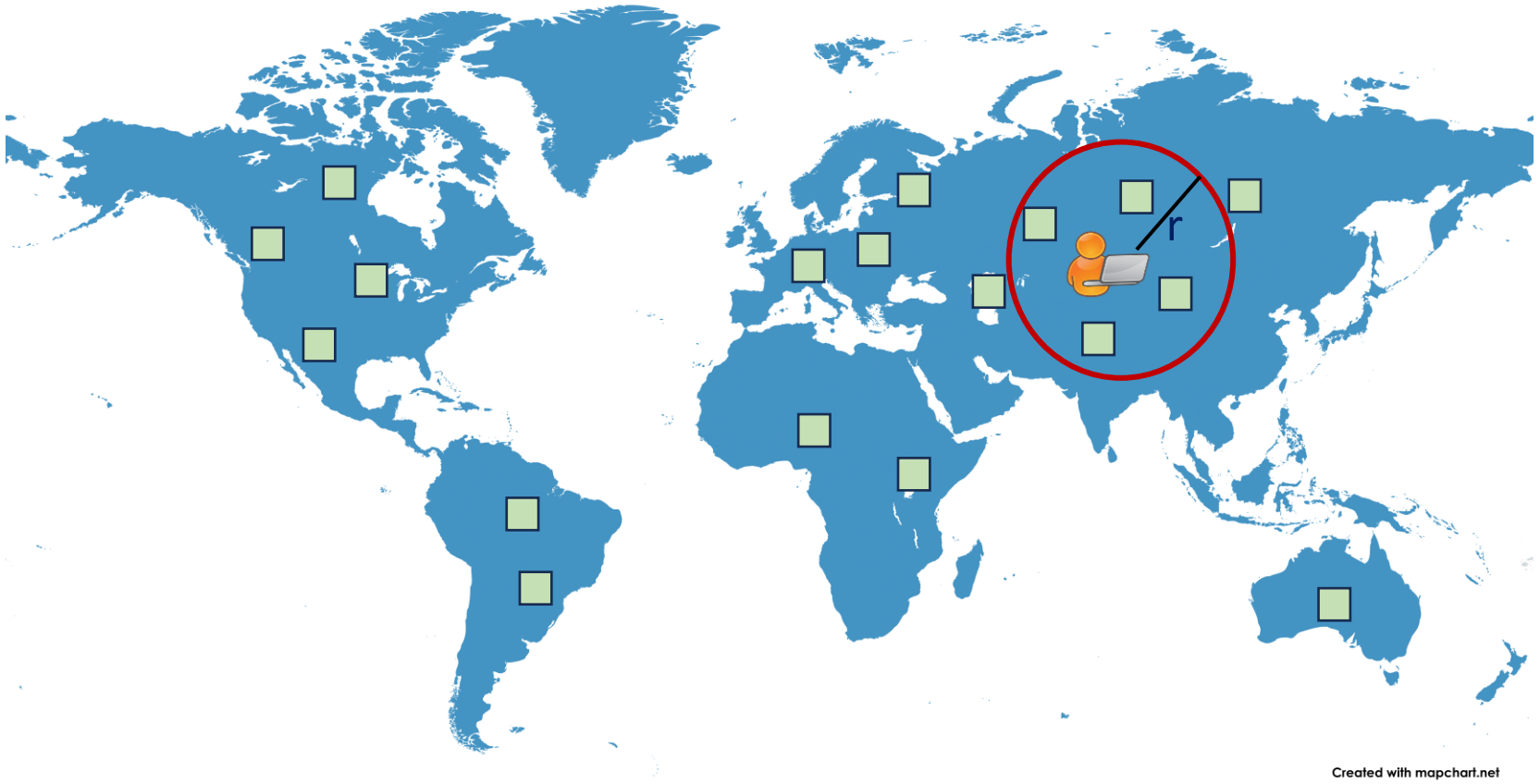
Single Circle



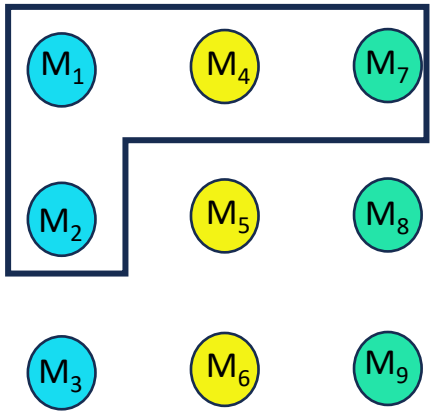
Single Circle

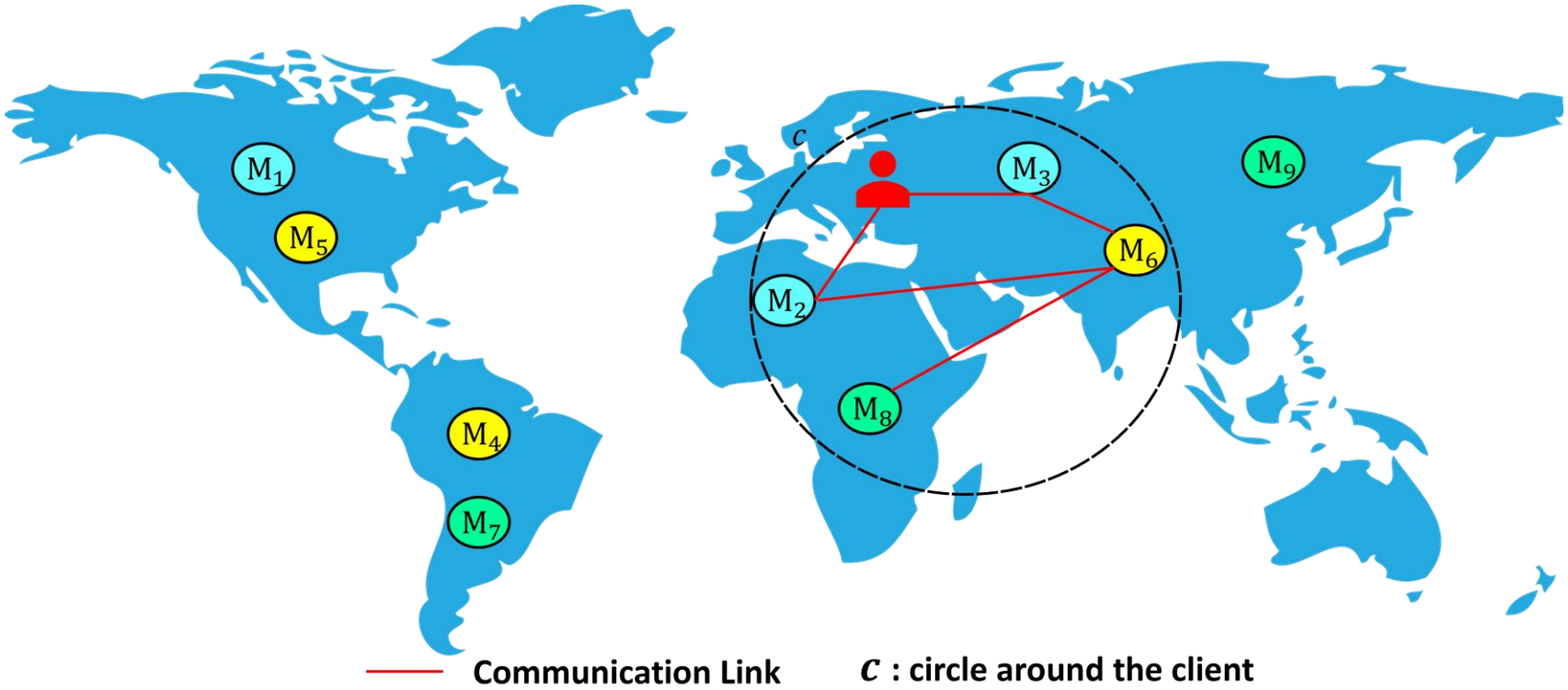


Single Circle



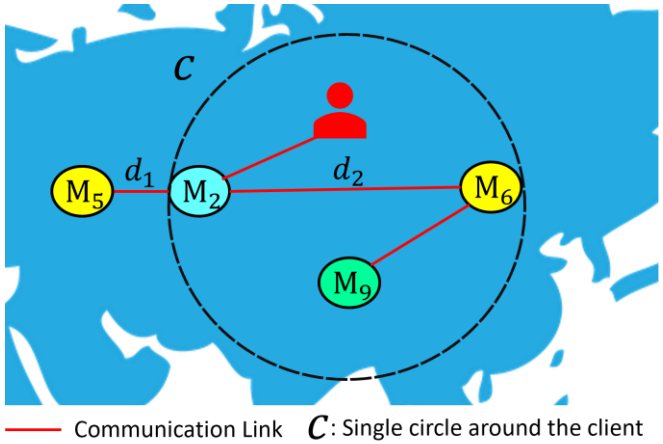
Single Circle



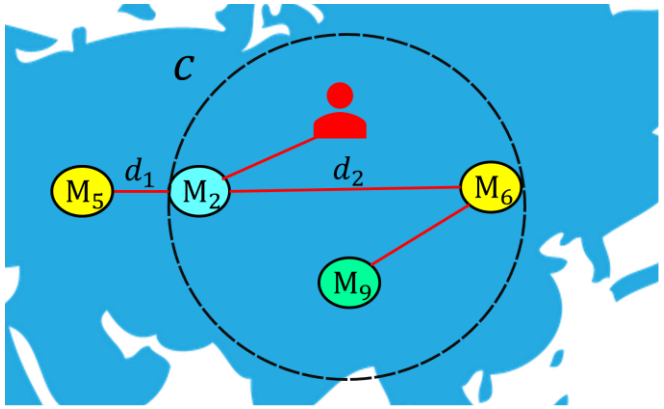


Colors represent different layers: Layer 1 (blue), Layer 2 (yellow), Layer 3 (green)

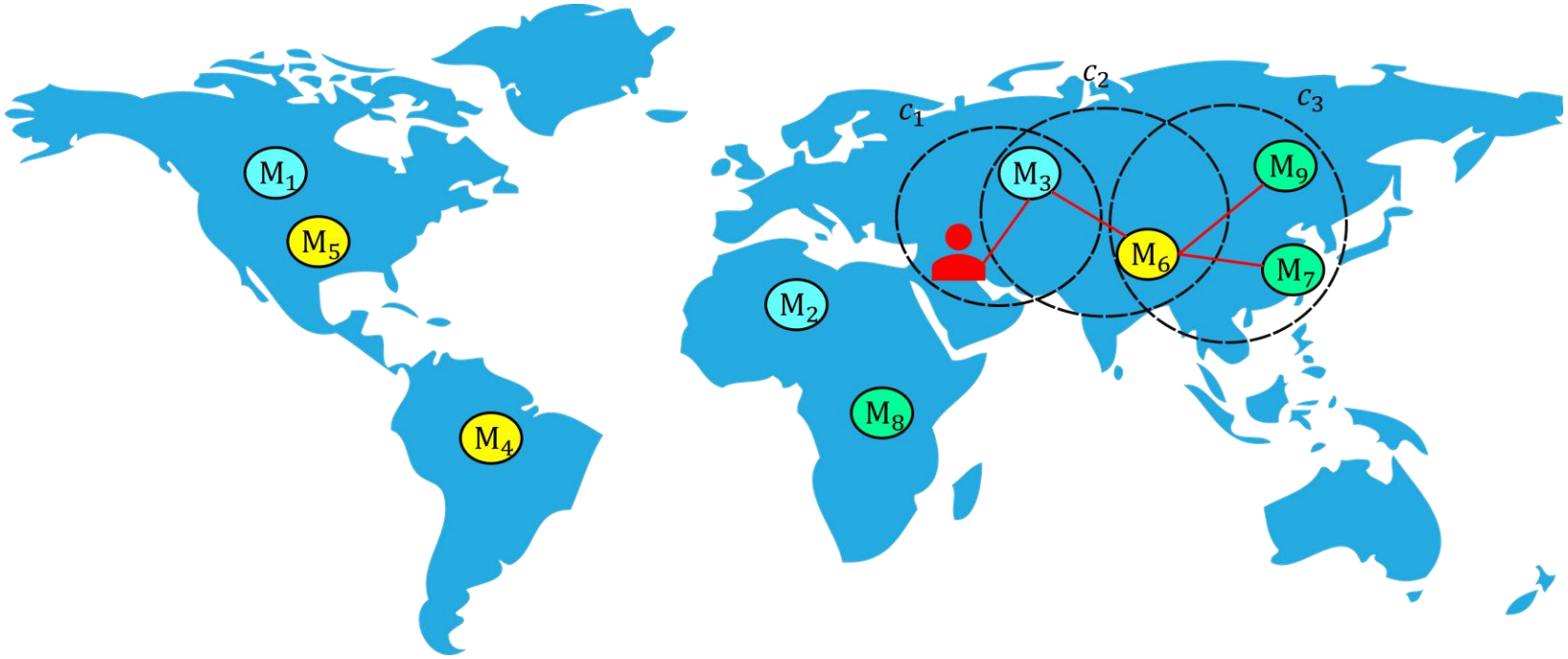
Multiple Circle



Multiple Circle

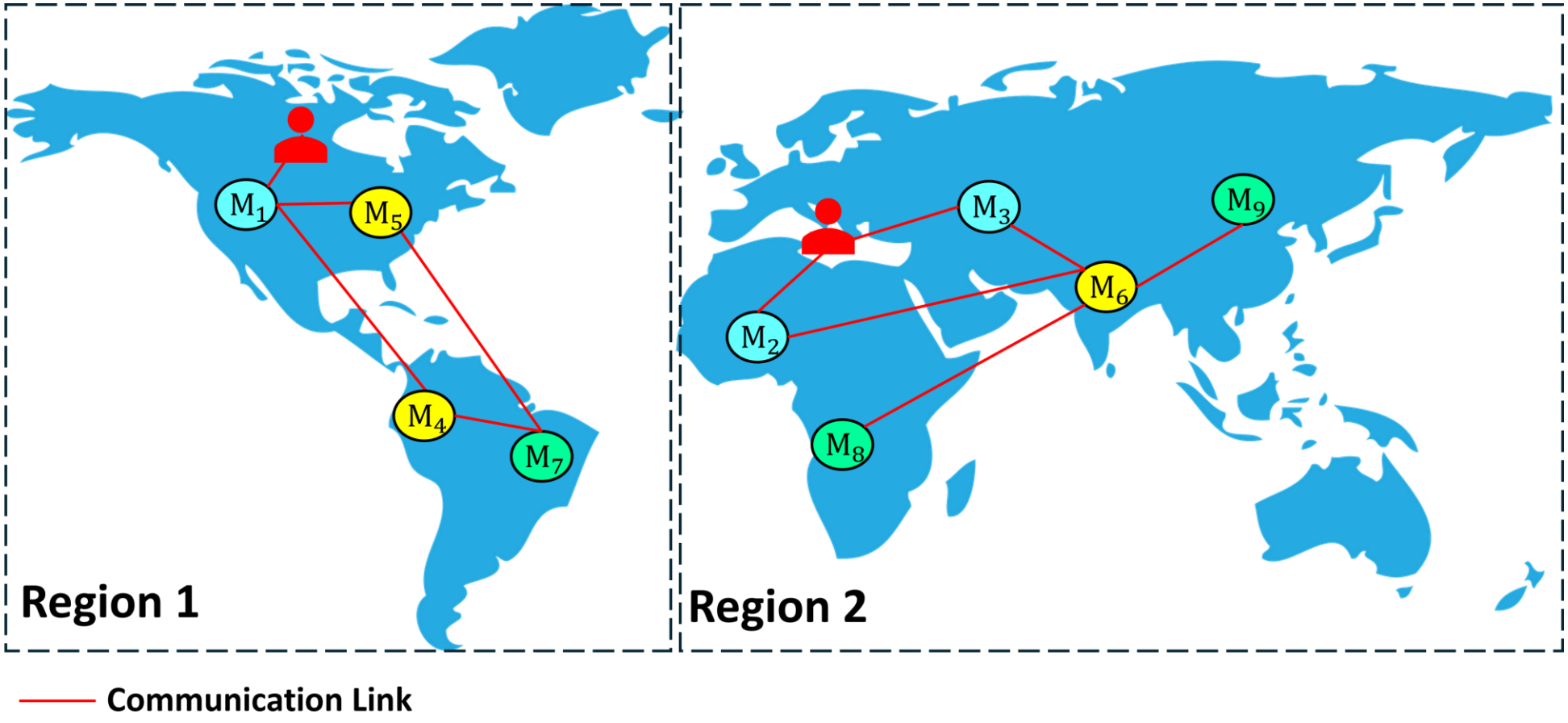


Communication Link C: Single circle around the client



Communication Link $c_1 c_2 c_3$: Multiple Circles

Regional Mixnets



Evaluation

- Metrics
  - Latency
  - Anonymity (Entropy): High entropy → High anonymity
  - Tradeoff: latency/anonymity
- Variables (For SC & MC)
  - Routing within the circle (random, proportional, larmix), α
- Experiments
  - Latency vs r
  - Entropy vs r
  - Effect of α
  - Effect of network size
  - Effect of client traffic rate

Evaluation

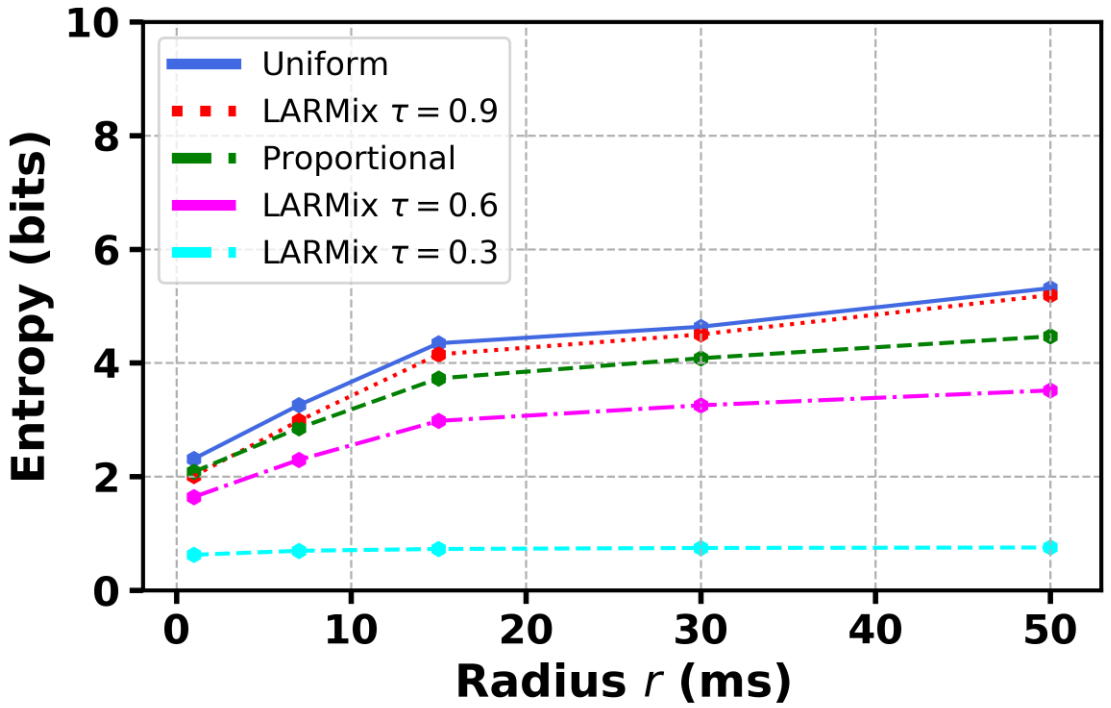
- Metrics
  - Latency
  - Anonymity (Entropy): High entropy → High anonymity
  - Tradeoff: latency/anonymity
- Variables (For SC & MC)
  - Routing within the circle (random, proportional, larmix), α
- Experiments
  - Latency vs r
  - Entropy vs r
  - Effect of α
  - Effect of network size
  - Effect of client traffic rate

Dataset

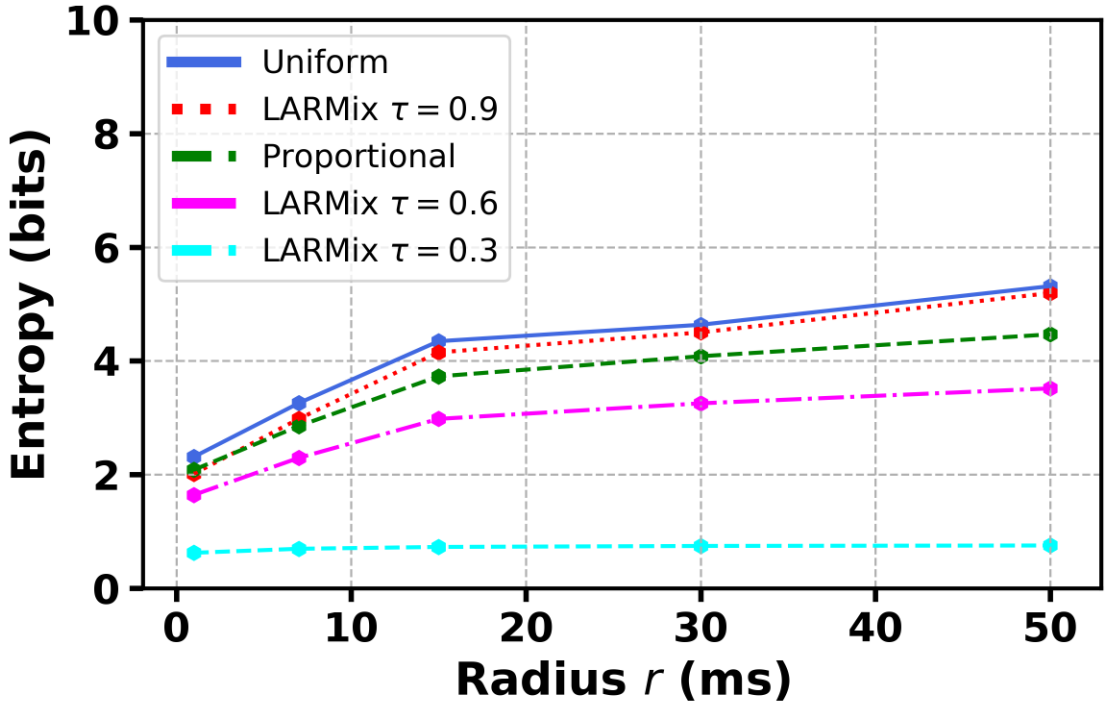
- Use real mixnode latency dataset from deployed Nym network

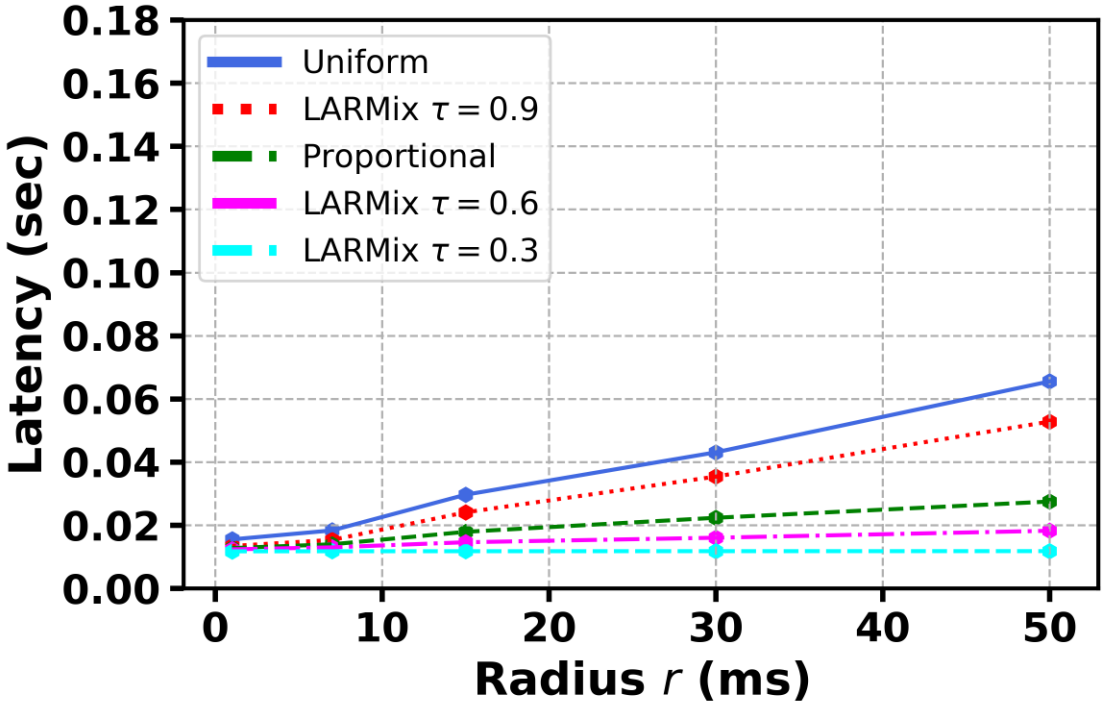
- VERLOC (USENIX Sec'21) protocol used for consistent latency measurement

Results: MC

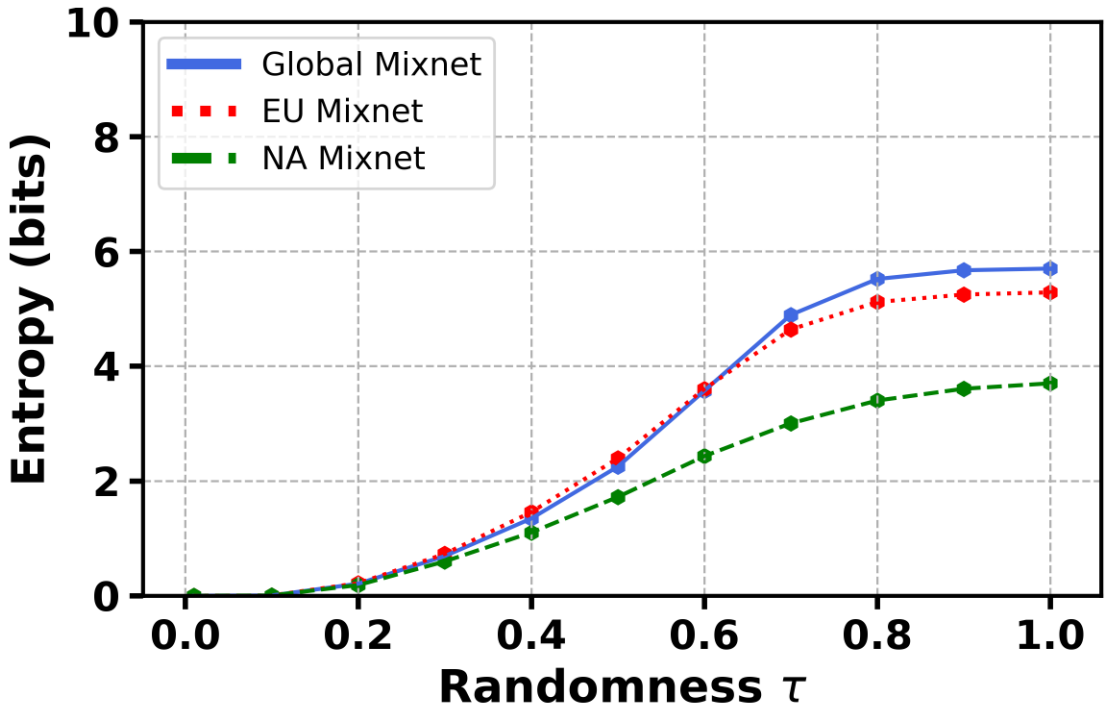

Uniform
LARMix $\tau = 0.9$
Proportional
LARMix $\tau = 0.6$
LARMix $\tau = 0.3$
Entropy (bits)
Radius r (ms)
0
2
4
6
8
10
0
10
20
30
40
50

Results: MC

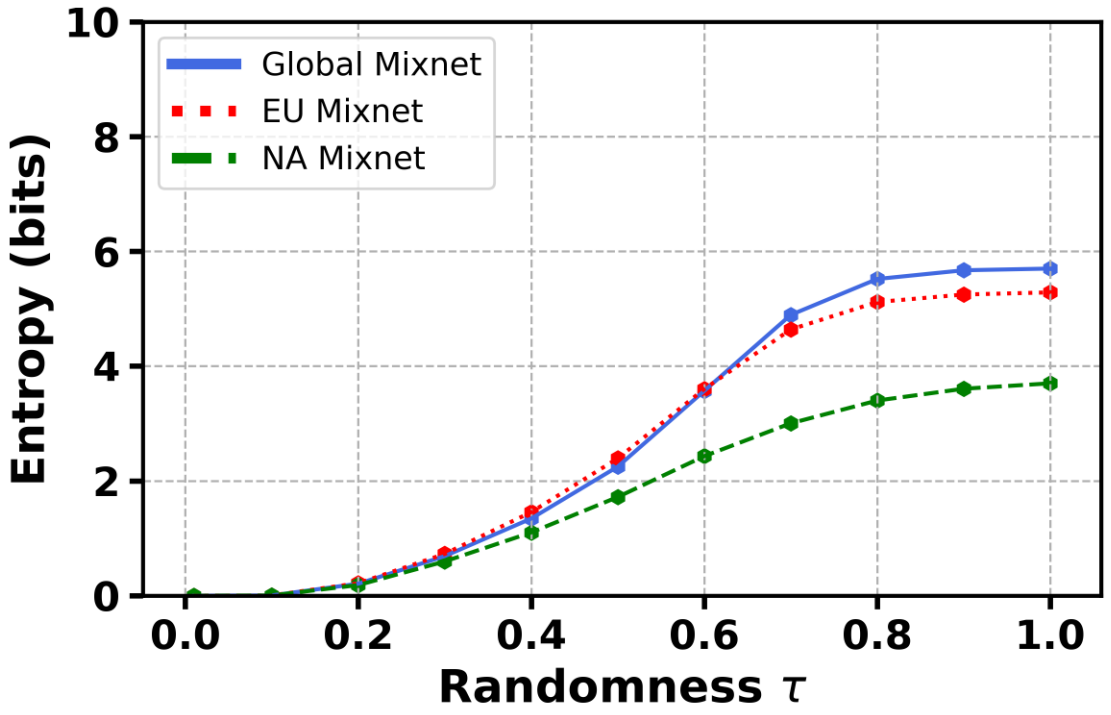

Uniform
LARMix $\tau = 0.9$
Proportional
LARMix $\tau = 0.6$
LARMix $\tau = 0.3$
Entropy (bits)
Radius r (ms)
0
2
4
6
8
10
0
10
20
30
40
50

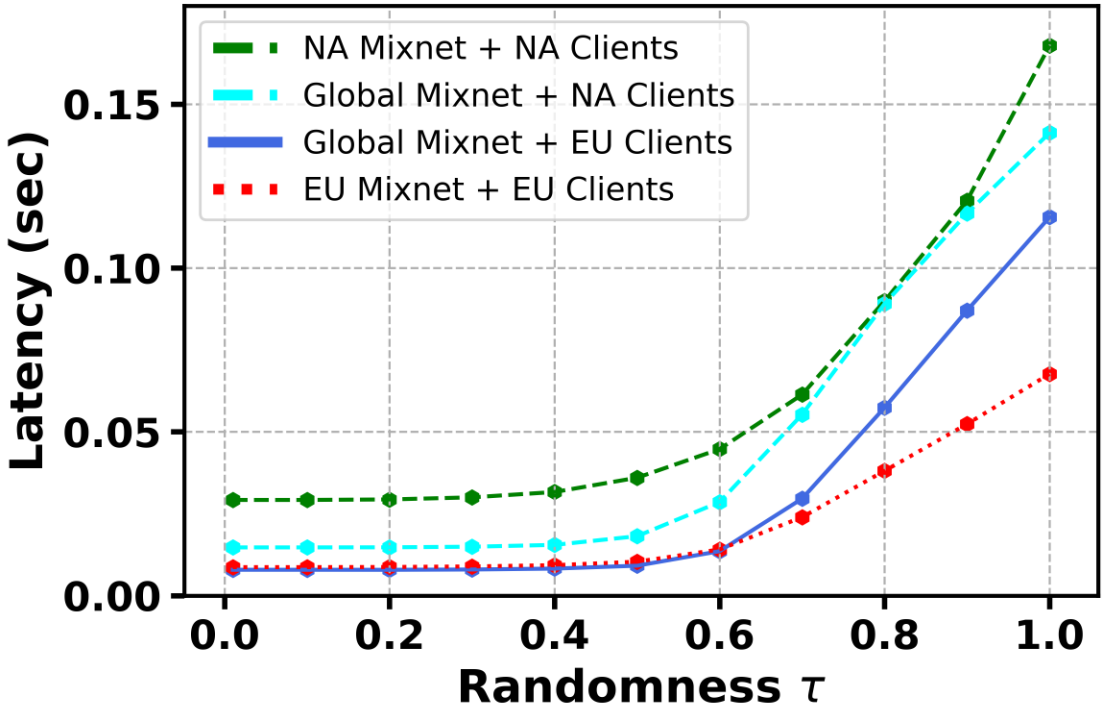

Uniform
LARMix $\tau = 0.9$
Proportional
LARMix $\tau = 0.6$
LARMix $\tau = 0.3$
Latency (sec)
Radius r (ms)
0.00
0.02
0.04
0.06
0.08
0.10
0.12
0.14
0.16
0.18
0
10
20
30
40
50

Results: Regional



Results: Regional





Overall Comparison

Approach \ Metrics	Latency	Entropy	Tradeoff	Runtime
Vanilla	153.4 ms	5.9 bits	38.5	t
LARMix	68 ms	3.9 bits	57.35	13958t
Single Circle	52 ms	4.2 bits	80.77	t
Multiple Circles	20 ms	3.8 bits	190	56t
Regional Mixnet (EU)	18 ms	3.75 bits	208.3	8t
Regional Mixnet (NA)	46 ms	2.4 bits	52.2	t

Summary

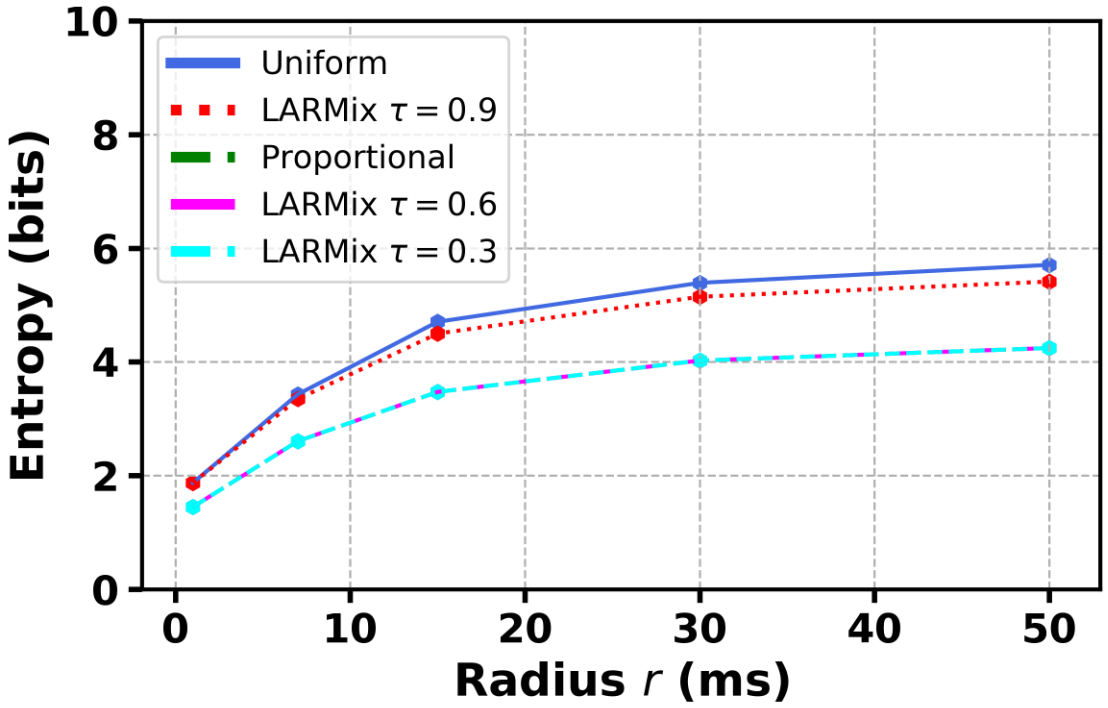
- Present LAMP, an approach to minimize latency in mixnets
  - With practical deployment considerations
- Develop three novel routing approaches
  - Single circle, Multiple circles, Regional mixnets
- Perform realistic evaluation on the deployed mixnet: Nym
  - Obtain superior tradeoffs than the state-of-the-art
  - 3x better Anonymity-Latency tradeoff
  - Supported by theoretical analysis for larger scale
- Conducted a thorough security analysis
  - Corrupt a subset of mixnodes (randomly, single location, worst case)
  - Measure fraction of corrupted paths (FCP)
  - LAMP does not give away significant advantage

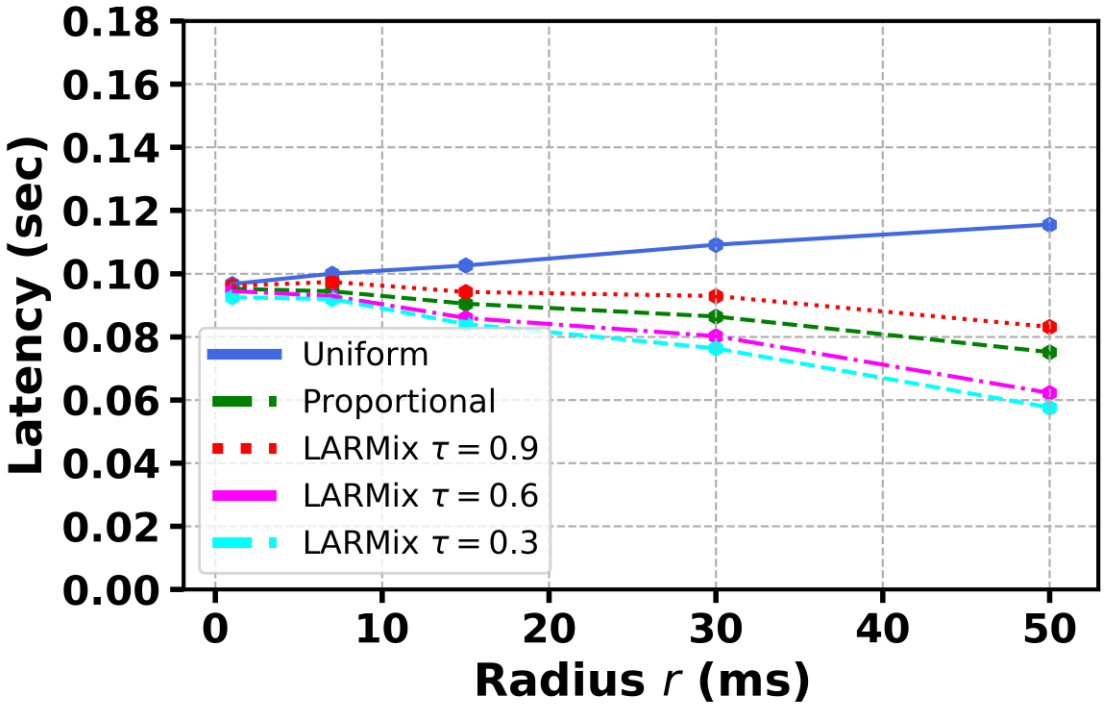
Appendix Slides

Security Analysis

- Adversary
  - Corrupt a subset of mixnodes (randomly, single location, worst case)
- Metrics
  - Fraction of Corrupted Paths
- Variables
  - Corruption rate
  - Value of r
  - Value of α

Evaluation: Results





Security Analysis: Results