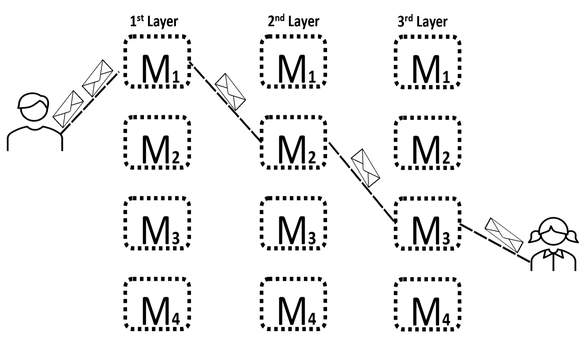
This poster is based on a paper titled "CLAM: Client-Aware Routing in Mix Networks" accepted and presented at IHMMSec 2024. The paper is accessible through the QR code.

Mahdi Rahimi
COSIC, KU Leuven, Leuven, Belgium
PoPETs 2024, Bristol, UK
17 July 2024

CLAM: Client-Aware Routing in Mix Networks

Backgrounds and Motivations

Mix Networks



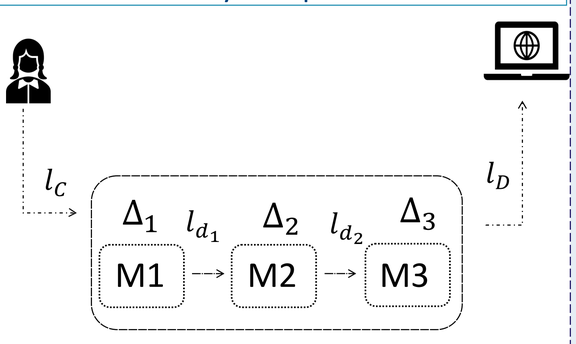
High degree of anonymity

Decentralized (like NYM)

Scalable

High end-to-end latency

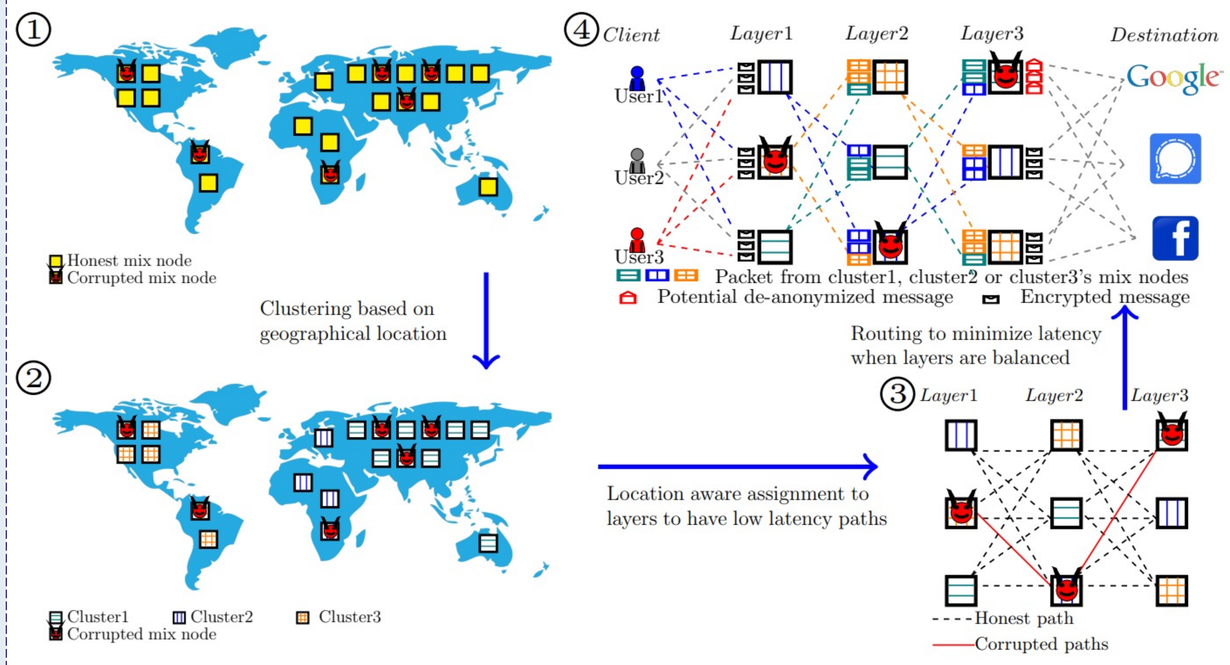
Latency Components



Propagation delay: $l_C + l_{d_1} + l_{d_2} + l_D$.
Mixing delay: $\Delta_1 + \Delta_2 + \Delta_3$.
Processing delay: negligible.

Propagation delay + Mixing delay → End-to-end latency

Related Work (LARMix, NDSS 2024)



LARMix proposes node assignment and selection to ensure within mixnet link delays (l_{d_1} + $l_{d_2)}$ are not very high. However, they don't propose a method to reduce the client-mix link delay (l_C).

CLAM Goals

Latency Reductions

Minimizing average latency for forwarding client packets to the mixnet.

Load Balancing

Keeping the mixnodes somewhat balanced in terms of received loads.

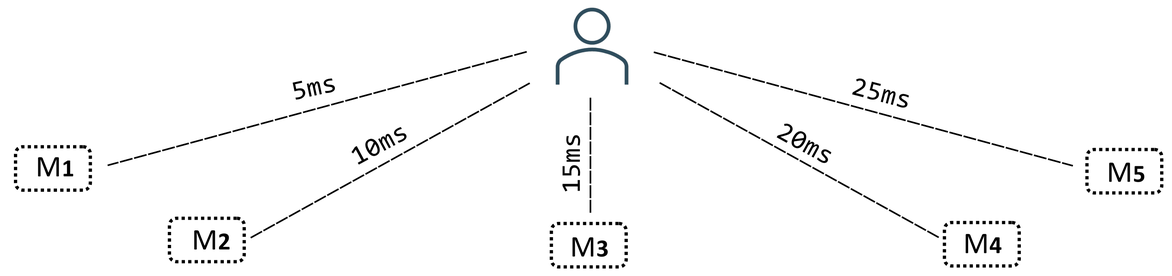
Adversary Advantages

Global Passive Adversary:
A complete view of communications on internet.

Mixnode Adversary:
Linking input to output of the corrupted mixnodes.

CLAM minimizes the advantages of the mentioned adversaries.

Toy Example



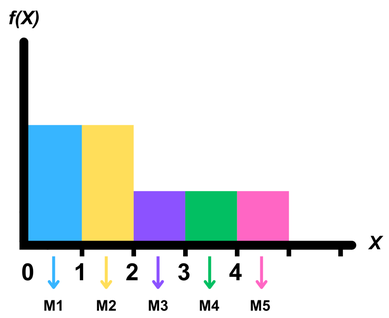
CLAM Routings Strategies

KαCloseness

$$f(C_i, M_j) = \begin{cases} \frac{\alpha}{W}, & \text{if } V_K[j] = 0, \\ \frac{1-\alpha}{K} + \frac{\alpha}{W}, & \text{otherwise.} \end{cases}$$

Probability of selecting K closest mixnodes: 1- α

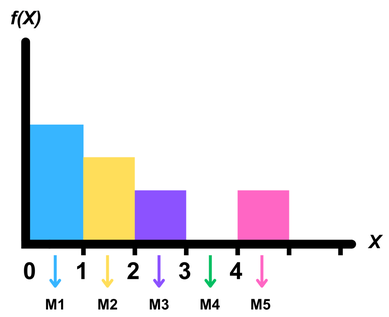
Probability of selecting other mixnodes: α



Linear Programming

$$\begin{aligned} \text{Minimize} \quad & \frac{1}{MW} \sum_{i=1}^{M} \sum_{j=1}^{W} r_{ij} L_{ij}, \\ \text{subject to} \quad & \forall i, j, \quad 0 \le r_{ij} \le 1, \\ & \forall i, \quad \sum_{j=1}^{W} r_{ij} = 1, \\ & \forall j, \quad \frac{\alpha}{W} \le \frac{\sum_{i=1}^{M} r_{ij}}{M} \le \frac{W + \alpha(1-W)}{W} \end{aligned}$$

Minimizing latency while keeping mixnodes load balanced.

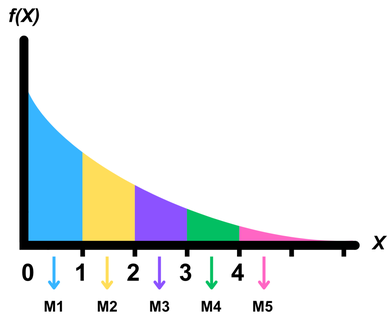


Exponential Distribution

$$f(C_i, M_j) = \frac{e^{-\lambda R(C_i, M_j)}(1 - e^{-\lambda})}{1 - e^{-\lambda W}}$$

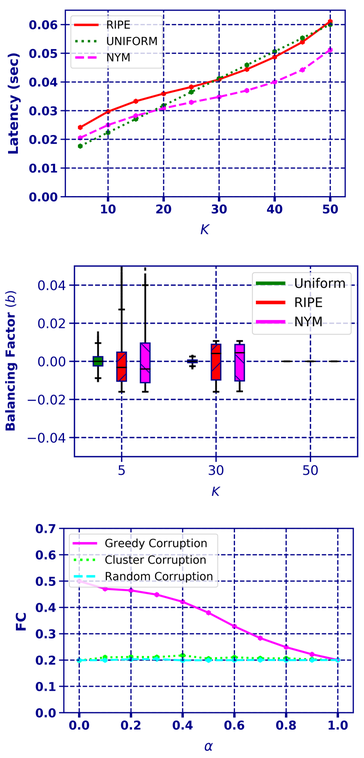
f(x) = Exp(λ) = $\lambda e^{-\lambda x}$

Exponentially prioritizing mixnode selections.

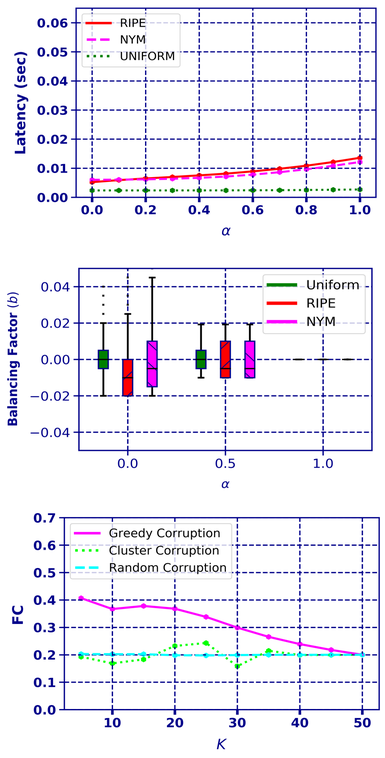


Results

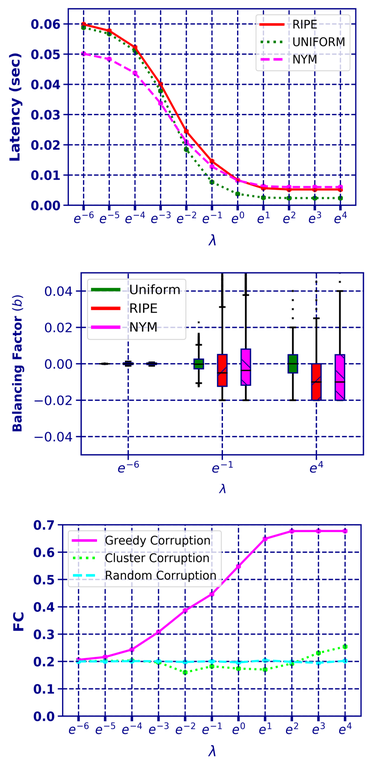
KαCloseness



Linear Programming



Exponential distribution



General Results

Routings \ Metrics	Latency	Entropy	FCP	Cost
Uniform + LARMix	98 ms	5.6 bits	0.008	Low
KαCloseness + LARMix	62 ms	5.3 bits	0.016	Low
Linear Programming + LARMix	47 ms	4.9 bits	0.018	High
Exponential distribution + LARMix	48 ms	4.9 bits	0.027	Low

Conclusions

High latency caused by routing through a mixnet can be detrimental for low-latency tolerant applications like web browsing.

LARMix provides latency reduction within mixnet link delays, ultimately lowering the end-to-end latency in the mixnet.

CLAM, on the other hand, introduces new routing strategies for clients to forward their traffic to the mixnet.

LARMix and CLAM can be used together to reduce end-to-end latency to 70% of default routing in the mixnet.

Acknowledgments
I would like to thank Prof. Claudia Diaz for her constructive feedback on the initial version of the poster.
This work is partially supported by CyberSecurity Research Flanders.

COSIC

Title: *CLAM: Client-Aware Routing in Mix Networks (Poster Version)*

Author: Mahdi Rahimi, COSIC, KU Leuven

Abstract:

Mix networks (mixnets) provide strong anonymity by routing traffic through a network of relays. However, this comes at the cost of increased end-to-end latency, which discourages adoption in latency-sensitive applications like web browsing and instant messaging. Consequently, users may opt for faster but less secure alternatives. LARMix [2] improves latency by optimizing routing *within* the mixnet, but does not address delays between clients and the entry relays.

To address this gap, **CLAM** introduces **client-aware routing strategies** that reduce the latency from clients to the mixnet. Our evaluation shows that CLAM reduces client-to-mixnet link latency by **up to 90%**, with minimal impact on network load. Importantly, CLAM maintains robust anonymity: even when **20% of mix nodes are compromised**, the risk of deanonymization remains negligible. These results position CLAM as a practical enhancement for latency-aware anonymous communication systems.

References.

[1] Rahimi, M. (2024). *CLAM: Client-Aware Routing in Mix Networks*. In *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security* (pp. 199–209).

[2] Rahimi, M., Sharma, P. K., & Diaz, C. (2024). *LARMix: Latency-Aware Routing in Mix Networks*. In *The Network and Distributed System Security Symposium (NDSS)*. Internet Society.