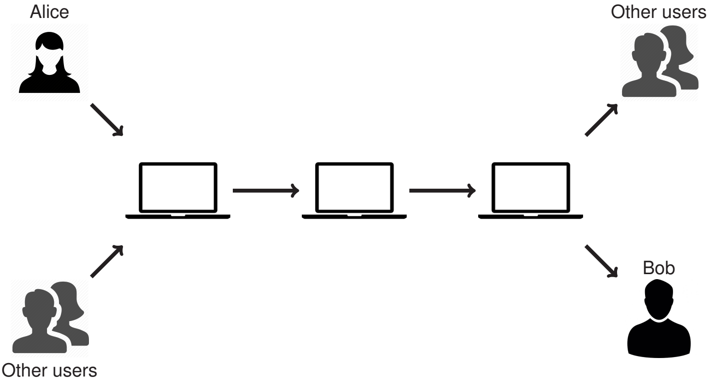
The Loopix Anonymity System

Ania M. Piotrowska[1] Jamie Hayes[1] Tariq Elahi[2] Sebastian Meiser[1] George Danezis[1]

[1]University College London, UK [2]KU Leuven

Mixnets Background

A set of cryptographic relays hiding input and output correspondence, by using layered encryption and secret permutation.



Motivation

Mixnet design shortcomings:

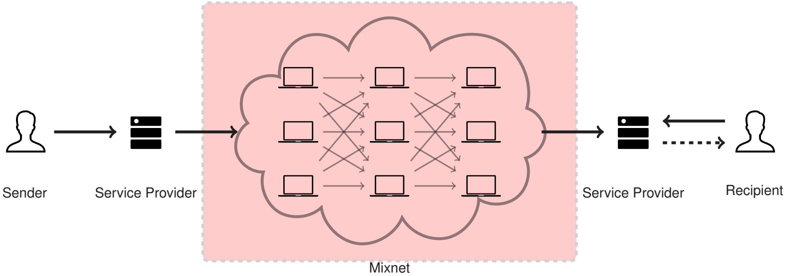
- In order to guarantee anonymity, mixnet requires long delays (**high latency**) and cover traffic (**scalability**).
- Not resistant against active attacks.
- No support for offline delivery.

Onion-routing design shortcomings:

- Not resistant against global passive adversary.

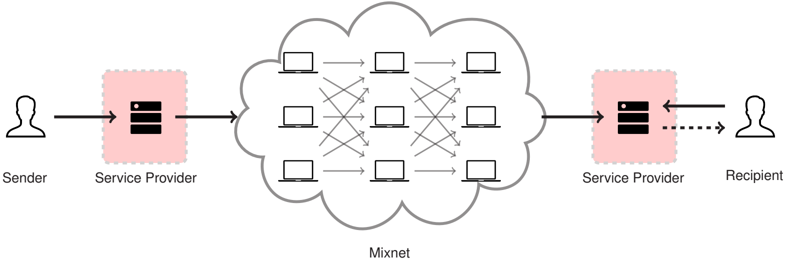
Loopix Overview

A new mixnet-based anonymous communication system, allowing for a tunable trade-off between **latency** and **genuine and cover traffic** volume.

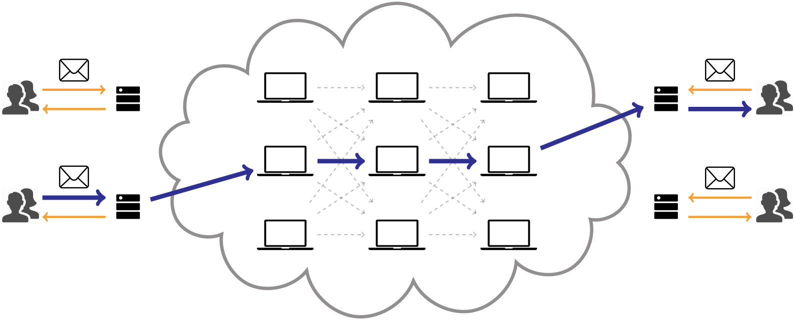


Loopix Overview

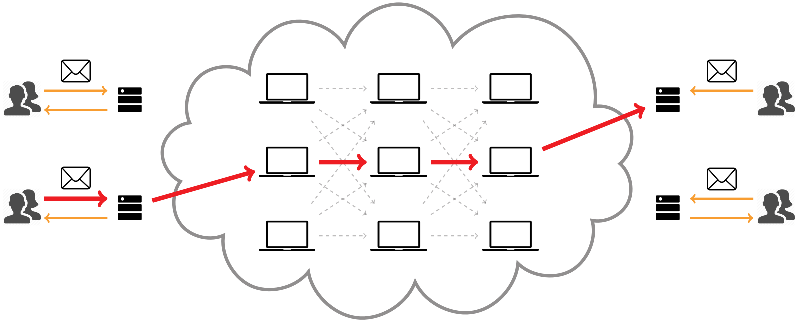
A new mixnet-based anonymous communication system, allowing for a tunable trade-off between **latency** and **genuine and cover traffic** volume.



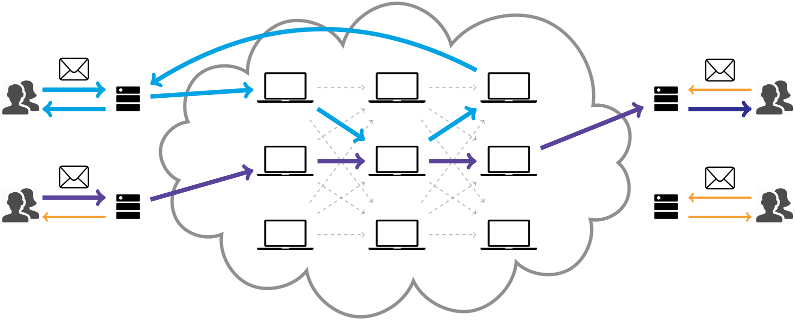
End-to-end messages



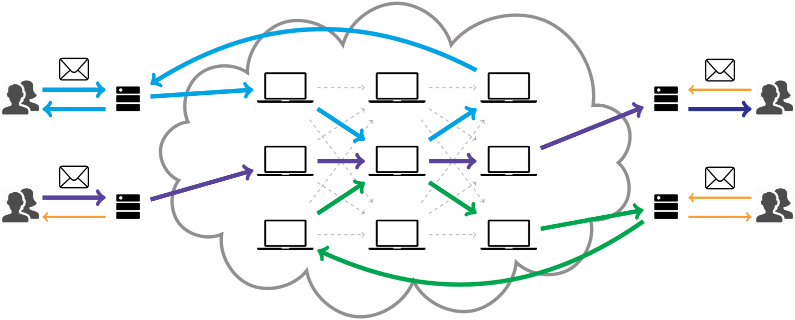
Drop cover traffic



Client's loop cover traffic

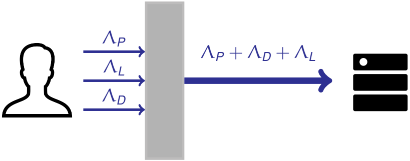


Mix's loop cover traffic



Client - Provider Link

Sending - each stream of traffic follows a Poisson process



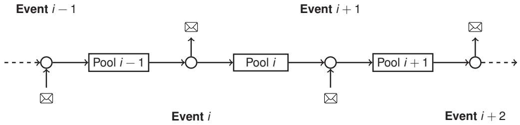
Retrieving - a fixed number of packets from the Provider

Mixing strategy - Poisson mix

Each packet is **delayed** according to a sender determined exponential delay.

Properties:

Poisson mix can be modeled as a pool mix.



Messages in the mix pool are indistinguishable due to the **memoryless property**.

No synchronized rounds required.

Security Properties - Summary

	GPA	Corrupt mixes	Corrupt provider
Sender-Recipient Third-Party Unobservability	✓	✓	✓
Sender online unobservability	✓	✓	✓
Sender anonymity	✓	✓	✓
Receiver unobservability	✓	✓	✗
Receiver anonymity	✓	✓	✗

Anonymity vs Latency vs Rate of traffic

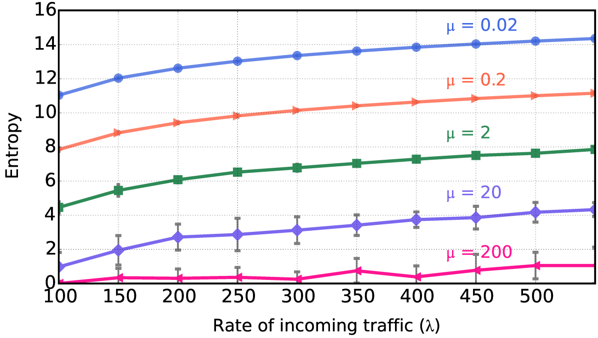


Figure: Entropy versus the changing rate of the incoming traffic for different delays (seconds). Lower μ is a higher delay.

Performance - Throughput

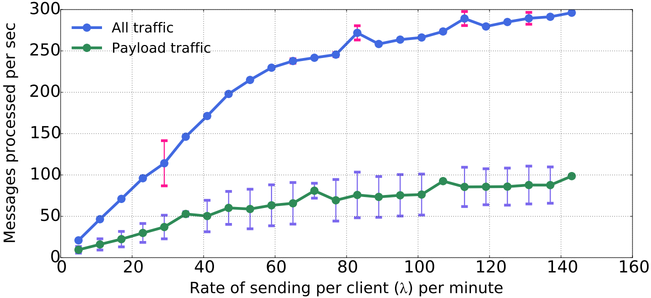


Figure: Overall bandwidth and goodput per second for a single mix node.

Starting conditions:

Λ_P = 3 msg/min

Λ_L = 1 msg/min

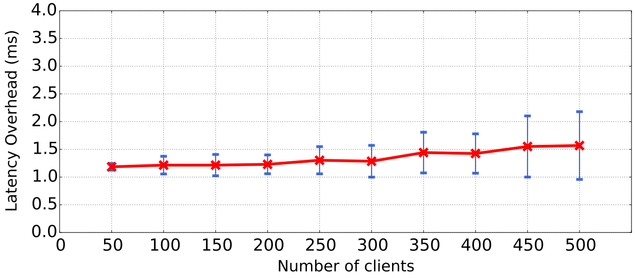
Λ_D = 1 msg/min

Λ_M = 1 loop/min

Avg. delay / hop = 1 ms

Periodic increase by 2 msg/min

Performance - Latency Overhead



Λ = 30 msg/min

Λ_M = 10 loops/min

Performance - End-to-end Message Latency

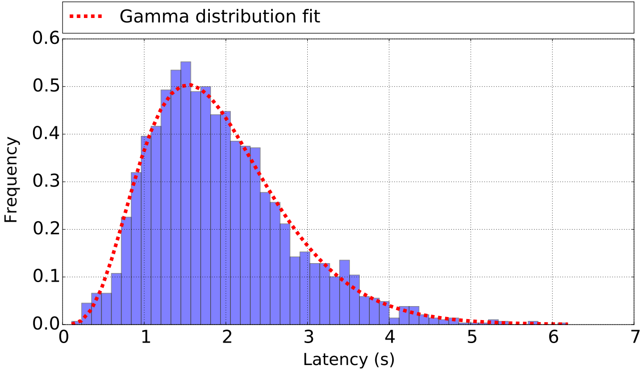


Figure: End-to-end latency histogram.

Λ = 180 msg/min

$\Lambda_M = 60$ loops/min

Avg. delay / hop

= 0.5 sec

Loopix Key takeaways

- Unlinkability of senders and recipients
- Detection of active attacks
- Unobservability of clients actions
- Balanced trade-off between latency and cover traffic
- Supporting off-line storage

Loopix Key takeaways

- Unlinkability of senders and recipients
- Detection of active attacks
- Unobservability of clients actions
- Balanced trade-off between latency and cover traffic
- Supporting off-line storage

Loopix Implementation: `https://github.com/UCL-InfoSec/loopix`

My Website: `http://www0.cs.ucl.ac.uk/staff/A.Piotrowska/`

My E-mail: a.piotrowska@cs.ucl.ac.uk

Thank you!

	Low Latency	Low Communication Overhead	Scalable Deployment	Asynchronous Messaging†	Active Attack Resistant	Offline Storage*	Resistance to GPA
Loopix	✓	✓	✓	✓	✓	✓	✓
Dissent	✗	✗	✗	✗	✓	✗	✓
Vuvuzela	✗	✗	✓	✗	✓	✗	✓
Stadium	✗	✓	✓	✗	✓	✗	✓
Riposte	✗	✗	✓	✗	✓	✗	✓
Atom	✗	✓	✓	✗	✓	✗	✓
Riffle	✓	✓	✗	✗	✓	✗	✓
AnonPoP	✗	✓	✓	✗	✗	✓	✓
Tor	✓	✓	✓	✓	✗	✗	✗

Table: Comparison of popular anonymous communication systems. By *, we mean if the design intentionally incorporates provisions for delivery of messages when a user is offline, perhaps for a long period of time. By †, we mean that the system operates continuously and does not depend on synchronized rounds for its security properties and users do not need to coordinate to communicate together.