Stopping Silent Sneaks: Defending against Malicious Mixes through Topological Engineering

Xinshu Ma[1], Florentin Rochet[2], Tariq Elahi[1]

[1]University of Edinburgh [2]University of Namur

ACSAC, 7 December 2022

THE UNIVERSITY of EDINBURGH

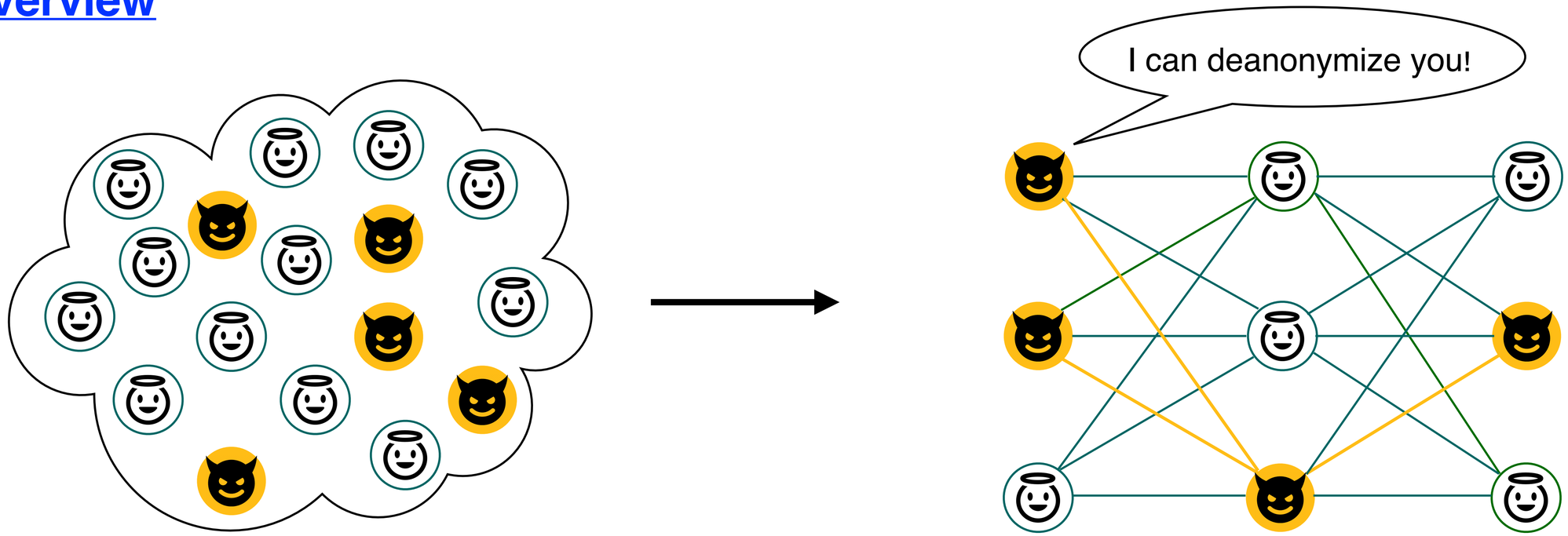
UNIVERSITÉ DE NAMUR

REPHRAIN
Protecting citizens online

Engineering and Physical Sciences Research Council

Problem: Trustworthy Mixnet Construction

Overview

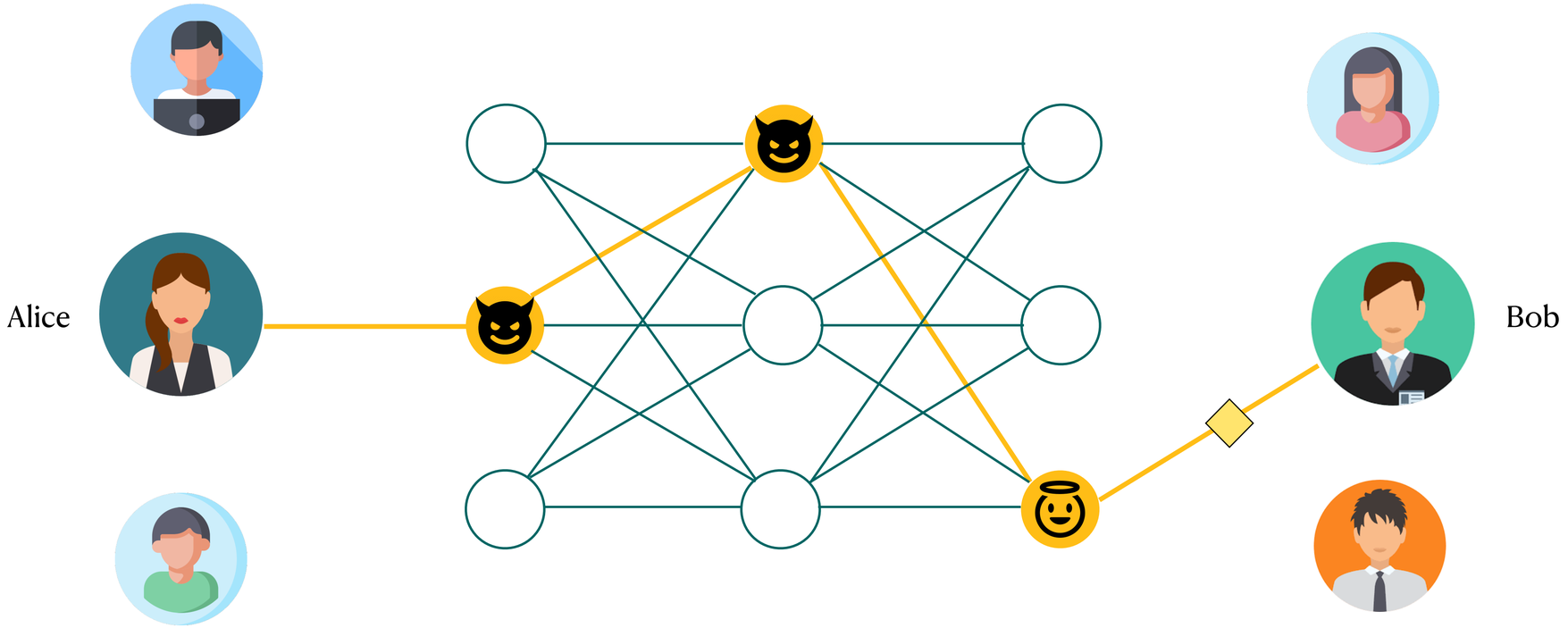


- Untrustworthy network resources
- End-to-end compromise

How to construct the mixnets to mitigate the impacts of malicious mixes.

Problem: Trustworthy Mixnet Construction

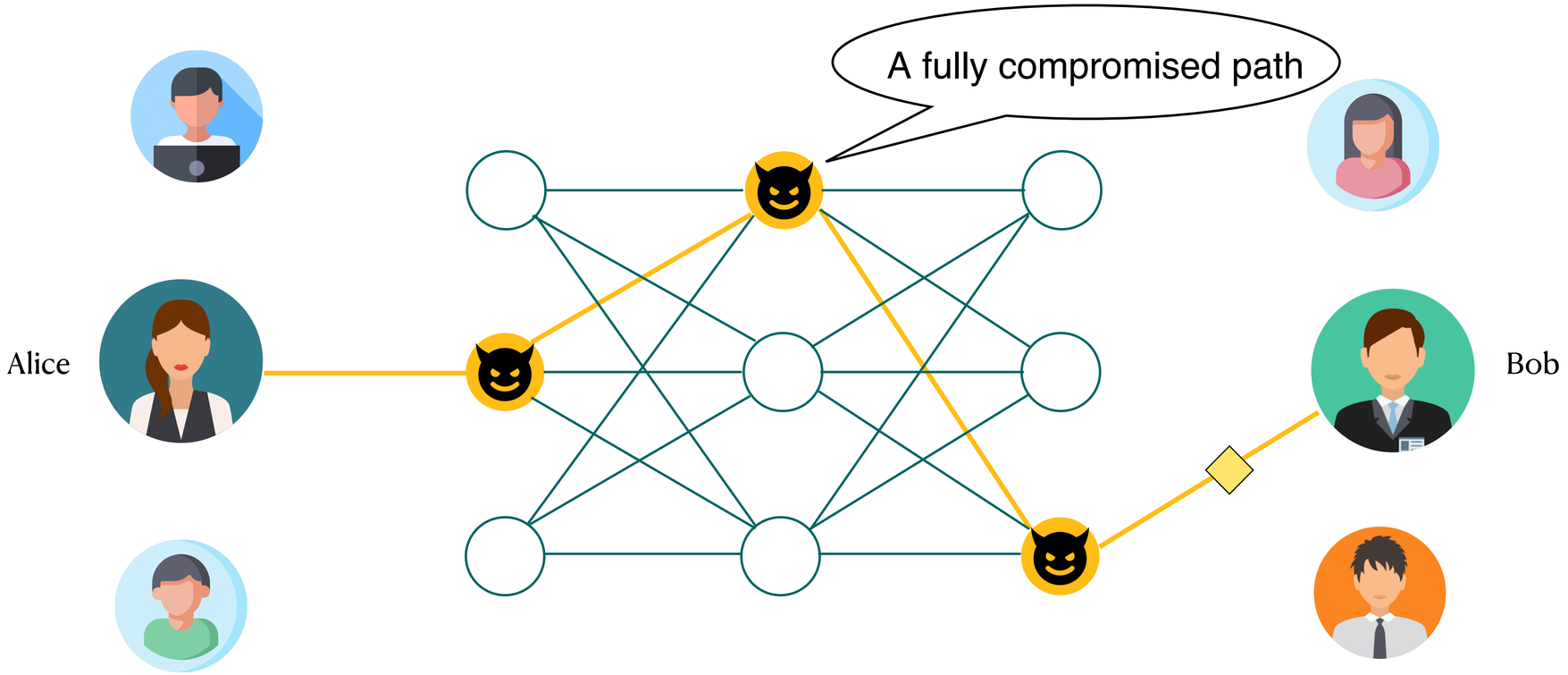
Anytrust assumtion is the security basis.



At least one server in the path must be honest.

Problem: Trustworthy Mixnet Construction

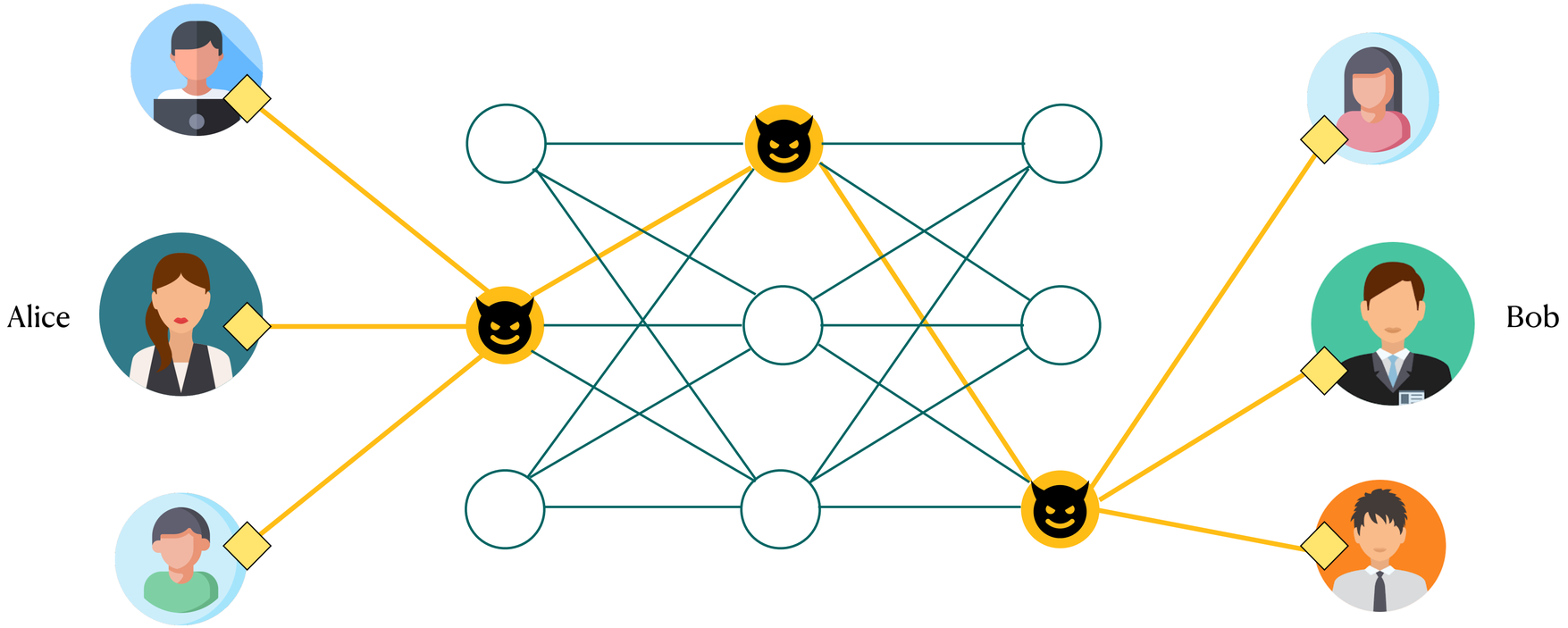
Anytrust assumtion might break in the real world.



- Mixnet literature typically considers active attacks: (n-1) attack and DoS attack.
- **End-to-end deanonymization by passive adversaries.**

Problem: Trustworthy Mixnet Construction

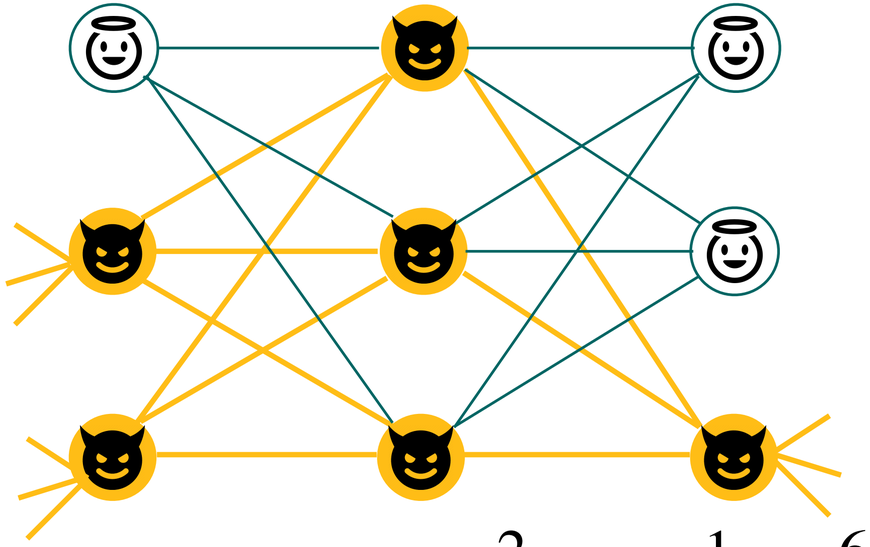
Client enumeration: the number of deanonymized clients matters.



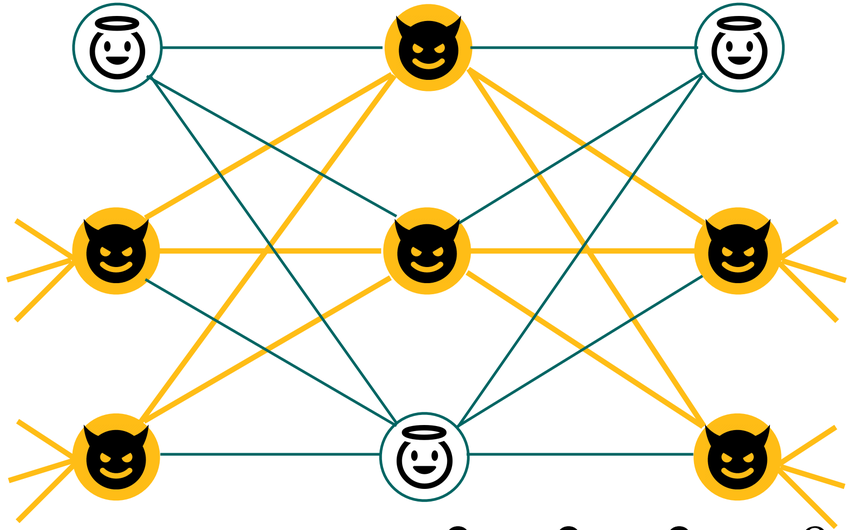
- Eventually, each user has at least one message traverses a fully compromised path.

Problem: Trustworthy Mixnet Construction

Adversary's best resource allocation to maximise the compromise rate



Uneven distribution: $\frac{2}{3} \times 1 \times \frac{1}{3} = \frac{6}{27}$

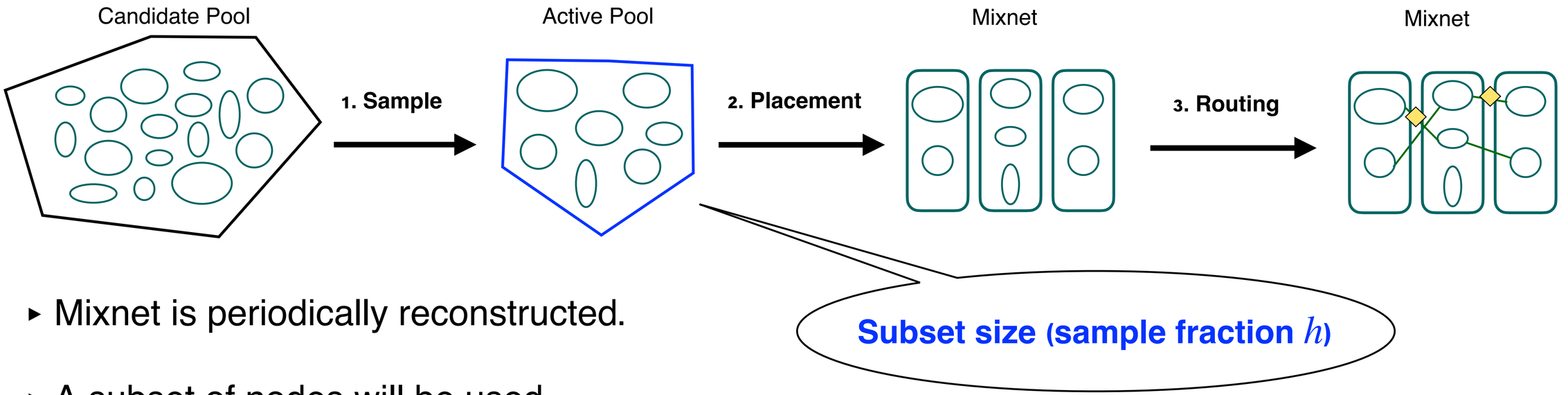


Even distribution: $\frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} = \frac{8}{27}$

End-to-end compromise rate

Problem: Trustworthy Mixnet Construction

Mixnet construction model: 3-stages process



- Mixnet is periodically reconstructed.
- A subset of nodes will be used.
- We consider these heuristic choices:
  1. Sample: bw-weighted, random
  2. Placement: random

Problem: Trustworthy Mixnet Construction

Example: How adversary manipulates the construction process?

Adversary

- The number of nodes and their bw to deploy
- Bandwidth budget: $\alpha = 0.2$

Fig 1. Probability of falling into each layer

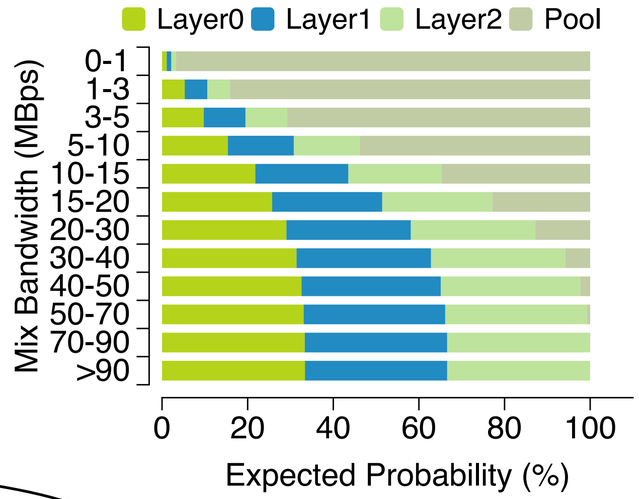
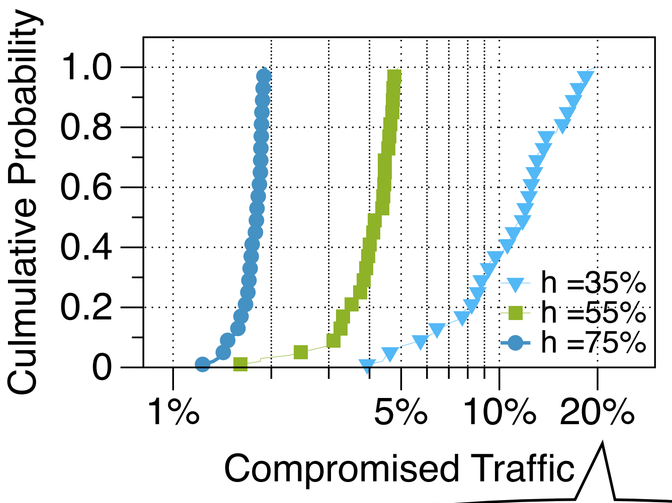
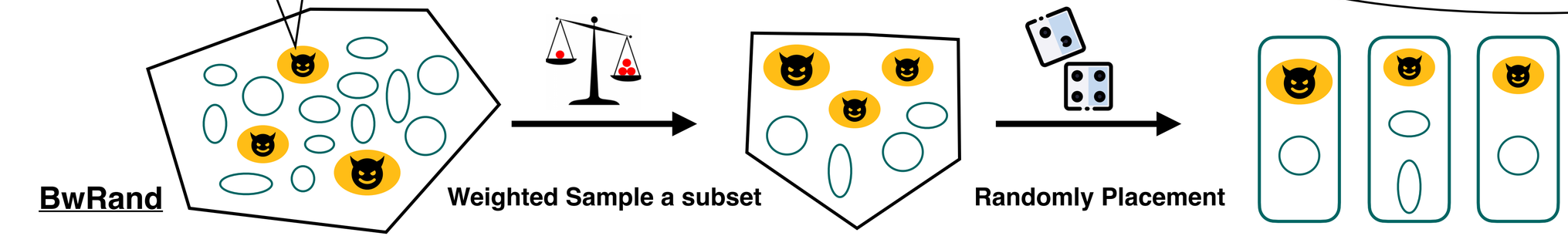


Fig 2. CDF of worst-case compromised fraction



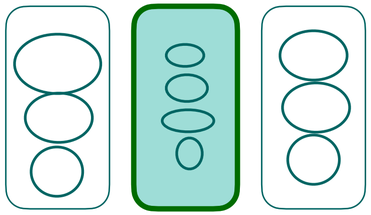
By manipulating the weights (bw)!

Sample fraction h has a big impact.



Challenges

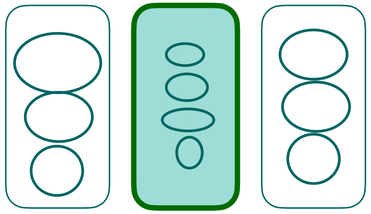
1. The adversary's manipulation is hard to prevent.
2. The adversary can do client enumeration with merely one fully compromised path.
3. The generated network should be performant.
4. Nodes churn in real-world deployments.



Bottleneck

Challenges

1. **The adversary's manipulation is hard to prevent.**
2. **The adversary can do client enumeration with merely one fully compromised path.**
3. **The generated network should be performant.**
4. **Nodes churn in real-world deployments.**



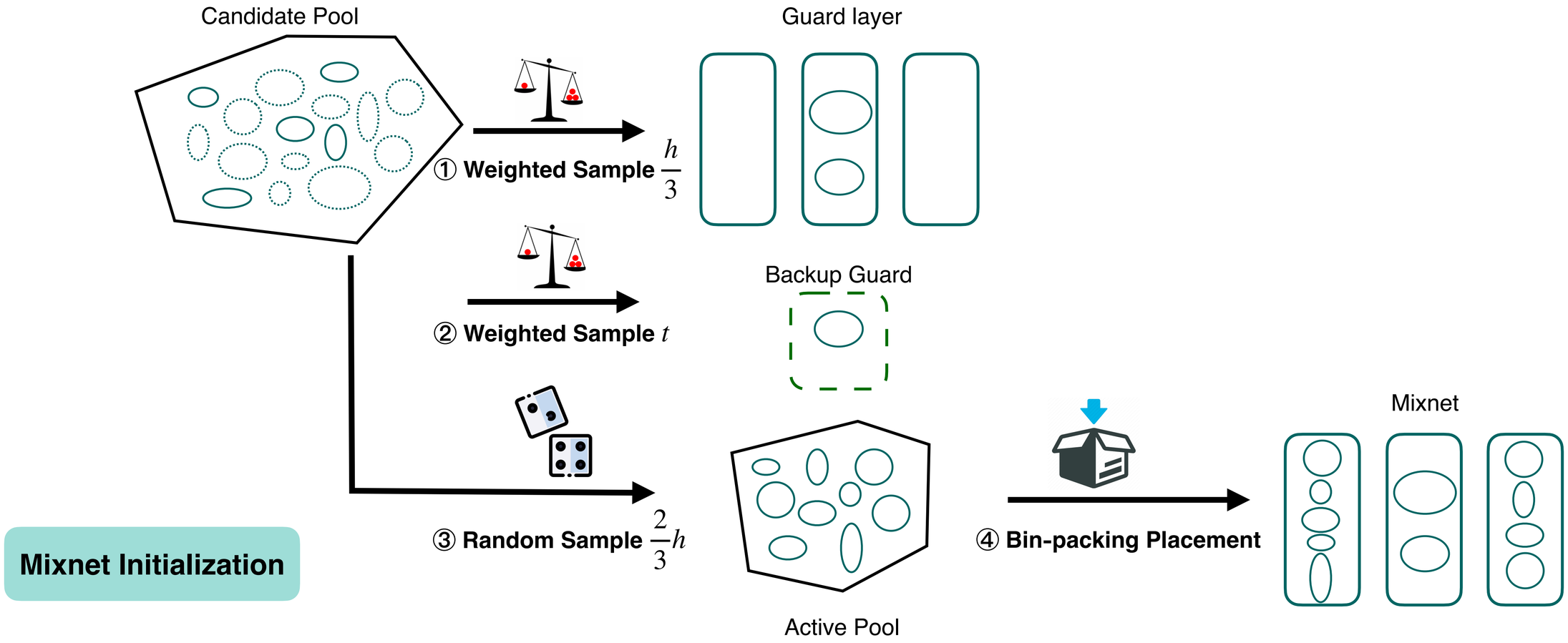
Bottleneck

Solution Intuition

- A constrained guard layer that is populated with stable and high performance relays. This creates a challenge for the adversary to achieve even placement.
- Bin-packing placement to improve the performance.

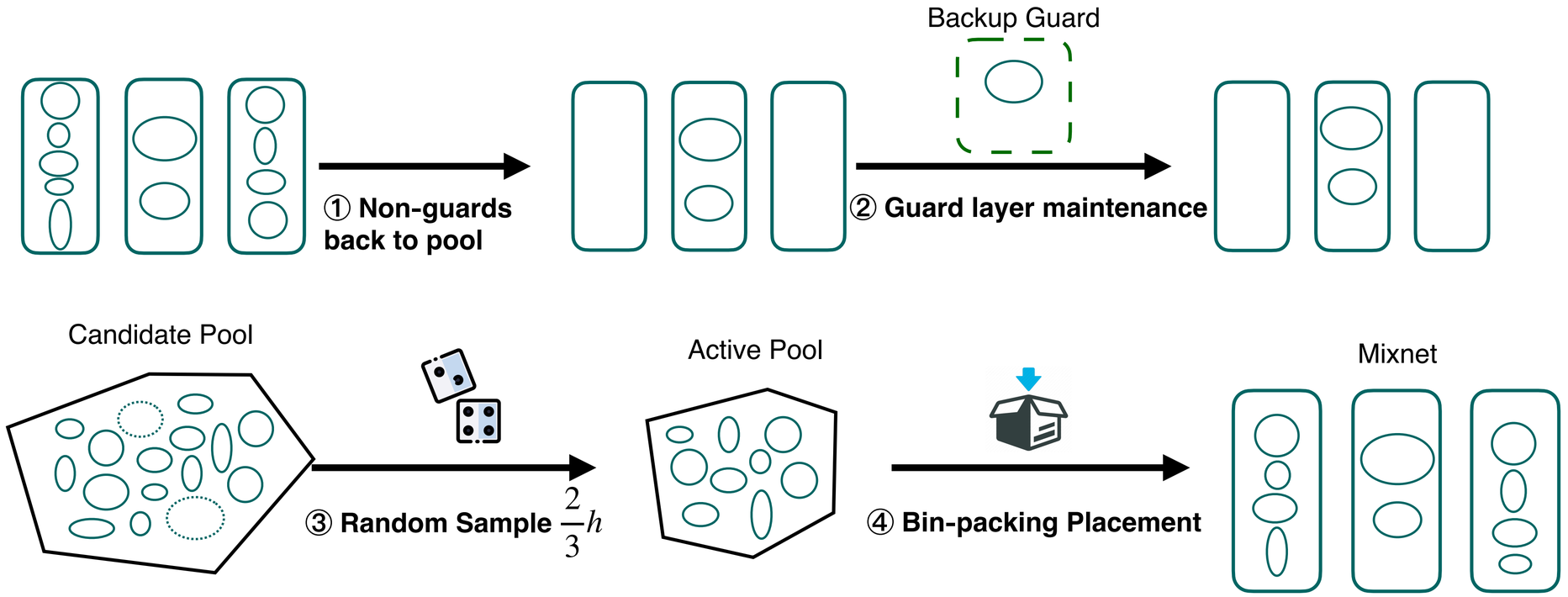
Bow-Tie: High-level Overview

How to shape the network to strengthen anytrust assumption?



Bow-Tie: High-level Overview

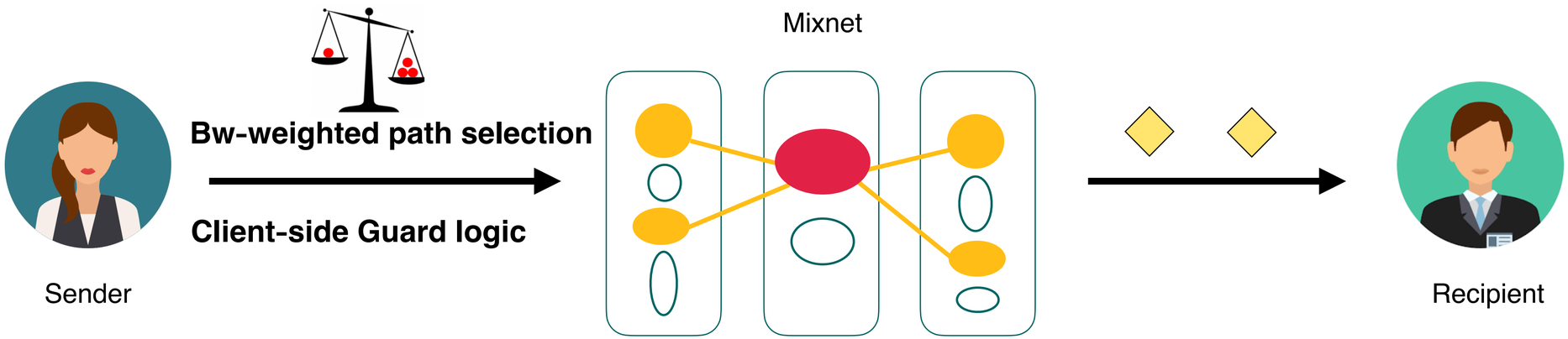
How to shape the network to strengthen anytrust assumption?



Mixnet Maintenance

Bow-Tie: High-level Overview

How to shape the network to strengthen anytrust assumption?



Keep using one guard node in all potential paths.

Mixnet Routing

Results: A Balance between Security and Performance

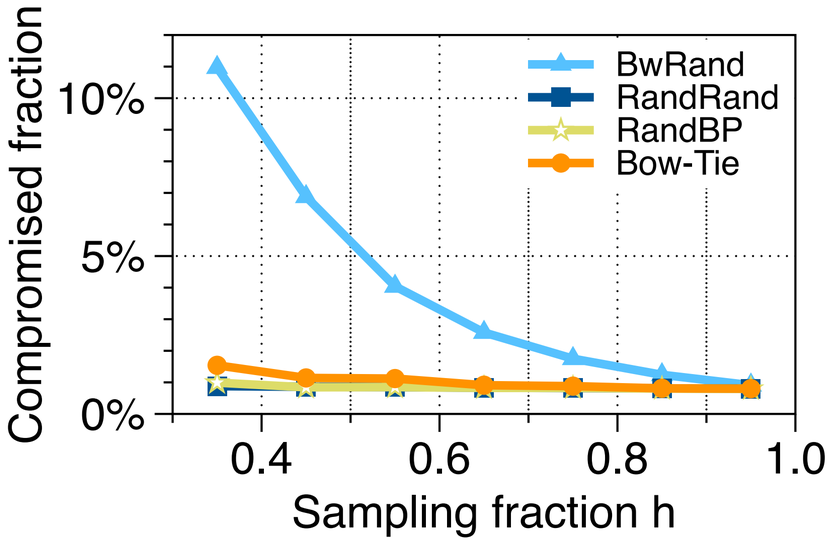


Fig3. End-to-end compromise rate

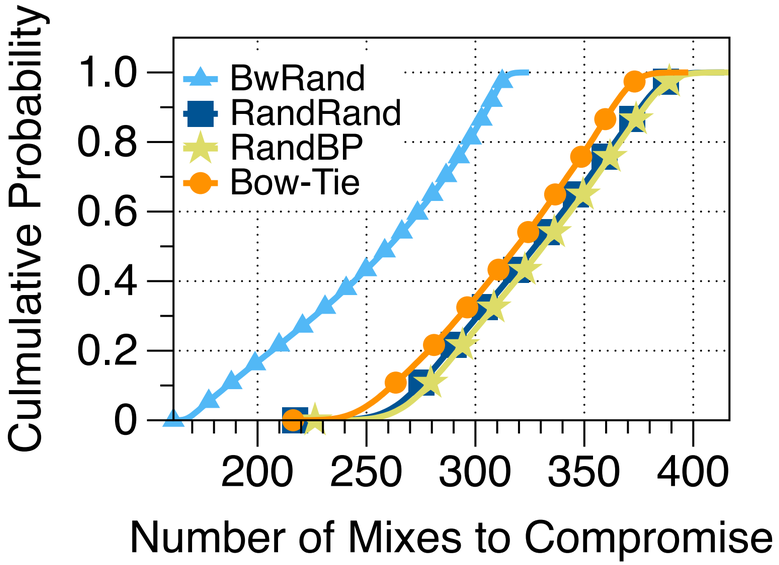


Fig4. Guessing entropy

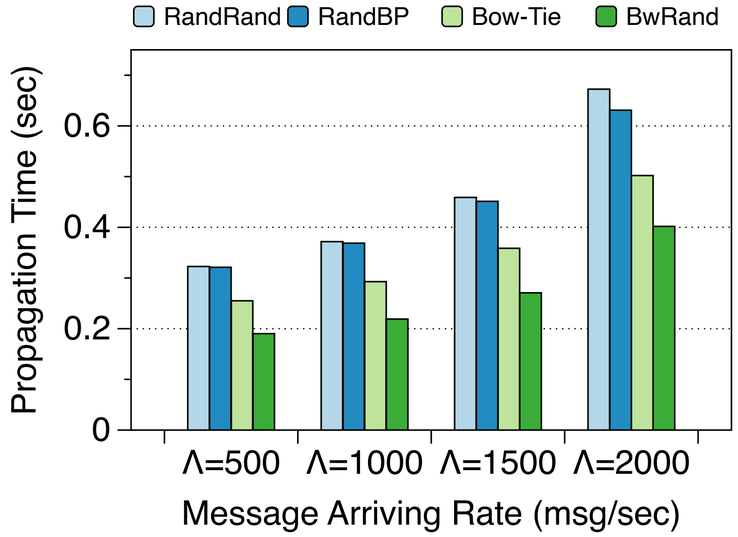


Fig5. Average Queuing delay

Results: Necessity of Guard Design

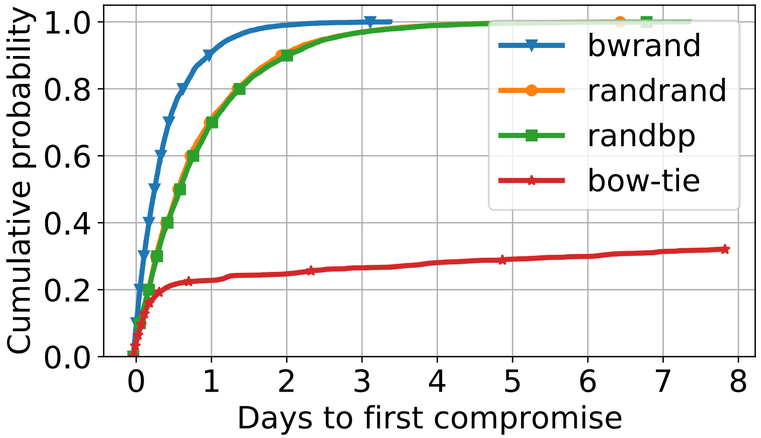


Fig6. Bow-tie vs others

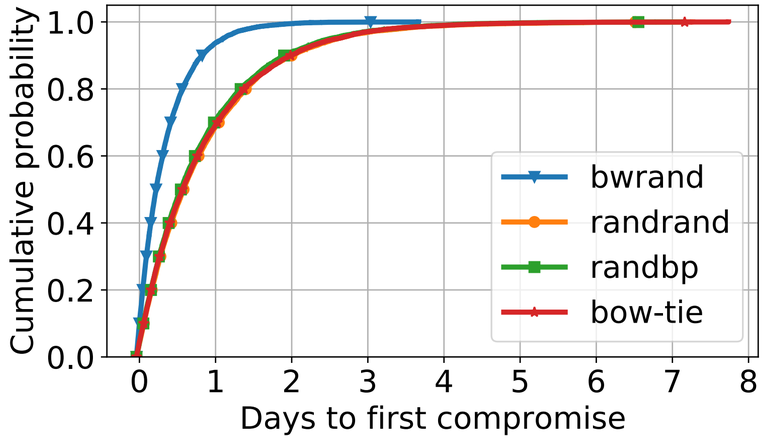


Fig7. Turn off guard logic for Bow-tie

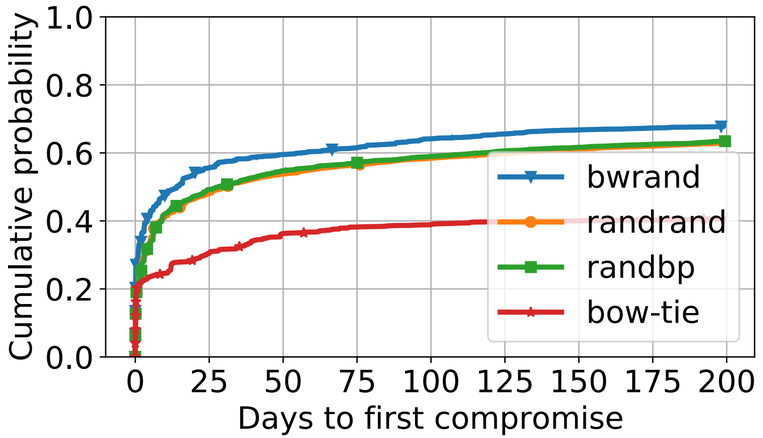


Fig8. Turn on guard logic for others

- The combination of guard layer and client-side guard logic reduces clients' exposure more effectively than they each could alone.

Results: Analysis of Other Aspects

Influence of Protocol designs and User behaviour

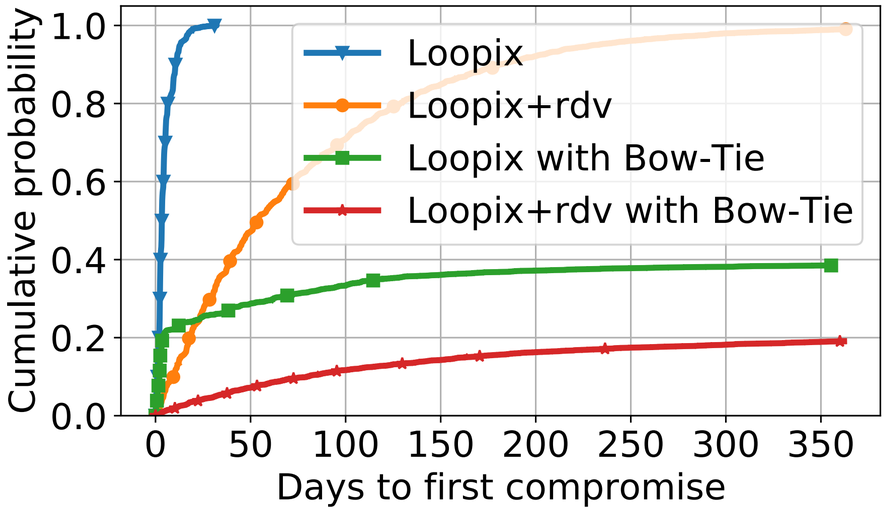


Fig9. Influence of protocol design

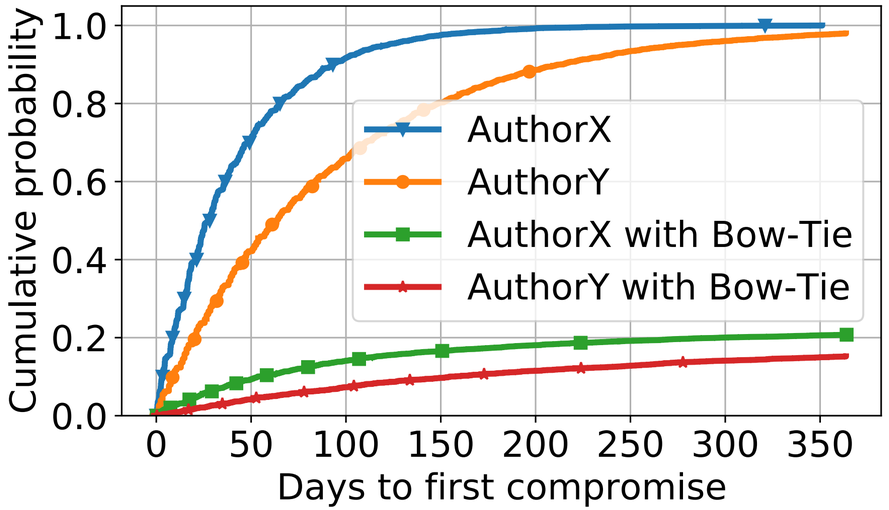


Fig10. Influence of individual behaviours

- User Model-1: dataset of UoE staff members over two months.
- Bow-Tie's effect is compatible to protocol designs.

- User Model-2: years of two authors' own email usage patterns.
- Users can figure out how long they could safely use the network based on their behaviours.

Takeaways

- **Problem:** How to construct a mixnet using untrustworthy resources with high security & performance.
- **Our Design:** A constrained guard layer that is populated with stable and high performance relays. This creates a challenge for the adversary to achieve even placement.
- **Results:** Bow-Tie finds a good balance between security and performance.
- **Simulator&Tools:** https://github.com/susopid/BowTie-Artifacts