Loopix

The Loopix Anonymity System

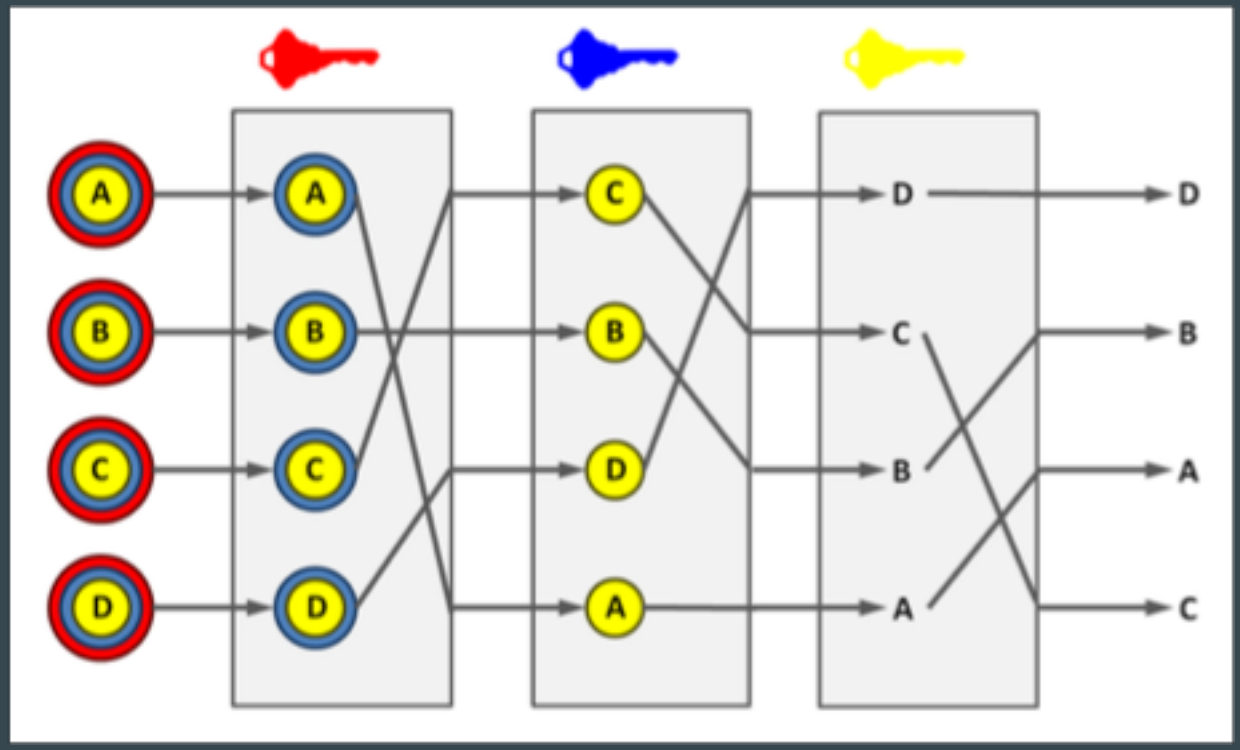
Piotrowska, Ania M., et al. "The loopix anonymity system." *26th USENIX Security Symposium, USENIX Security*. 2017.

Why we need Loopix?

TOR

1. Tor cannot and does not attempt to protect against monitoring of traffic.
2. Per-connection state to be maintained by intermediate nodes.
3. Low Throughput/Scalability.

Mixed Network



Overview Of Loopix

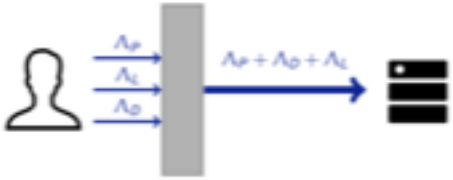
- ➔ It is a type of Mixnet Network
- ➔ No cross-link identification.
- ➔ End to End encryption of all packets
- ➔ Servers prepare a random path for all send messages
- ➔ Uses 3 types of cover traffic

Some Features of Loopix

- Unlinkability of senders and recipients
- Detection of active attacks
- All Relevant information in the headers
- Less latency and for more cover traffic
- Offline Message Service
- Poisson Mixes for traffic

Client - Provider Link

Sending - each stream of traffic follows a Poisson process

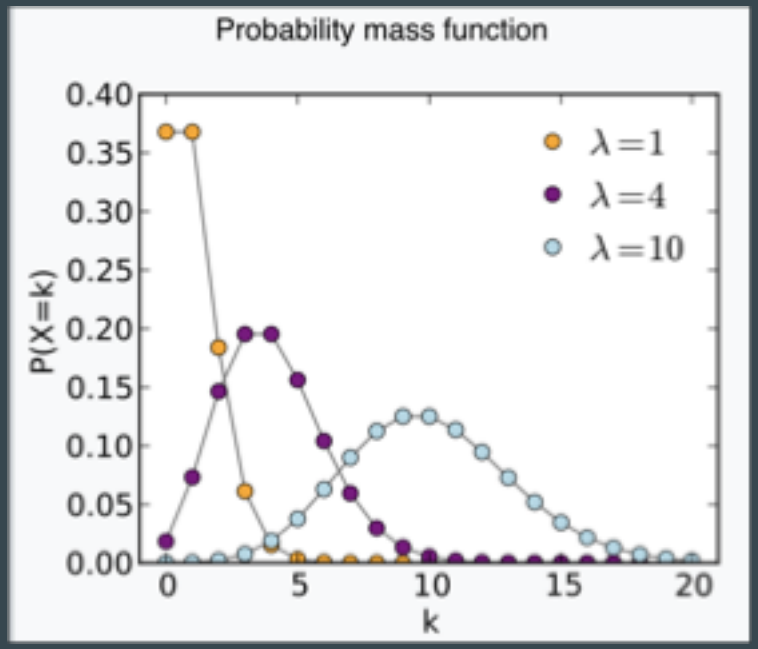


Retrieving - a fixed number of packets from the Provider

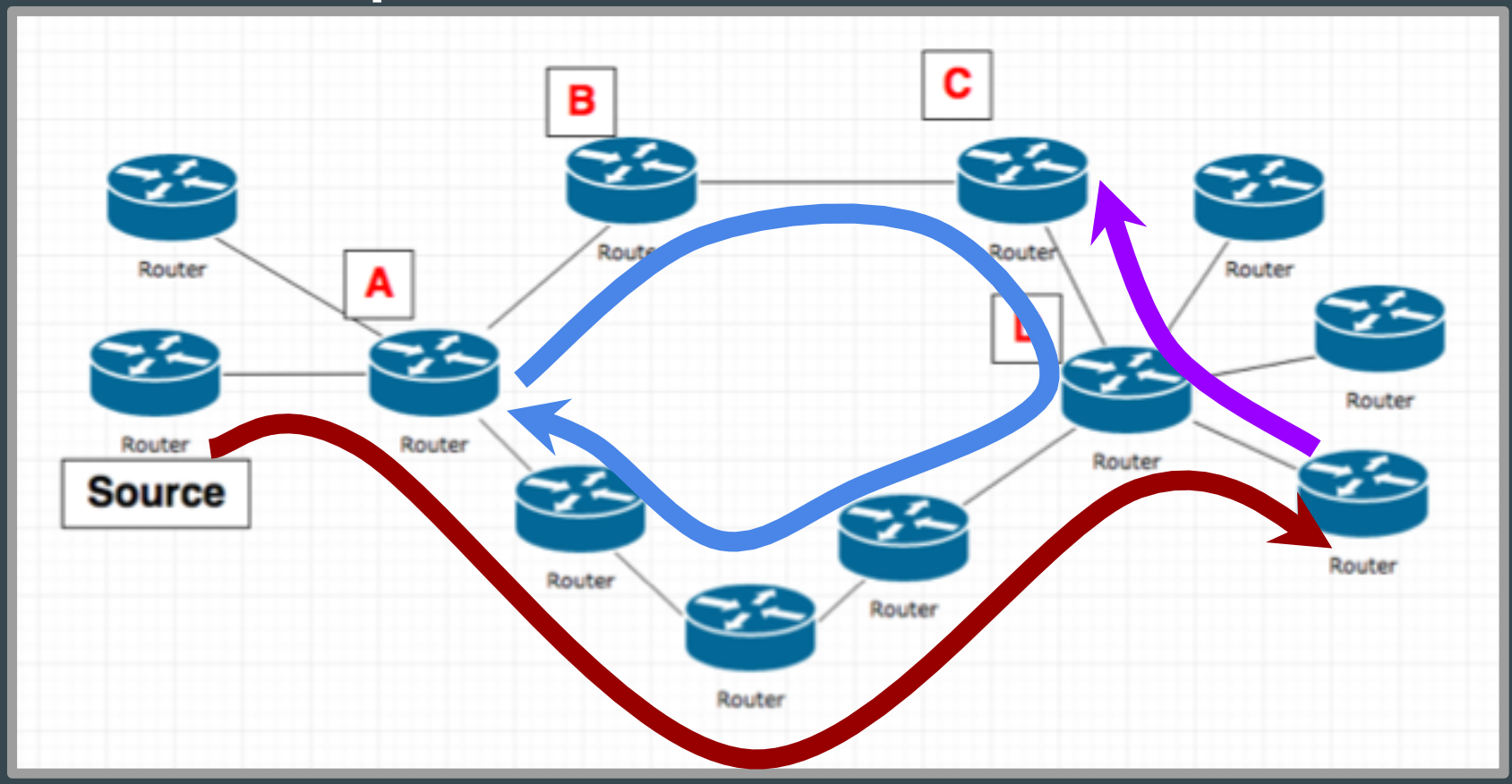
Piotrowska, Ania M., et al. "The loopix anonymity system." *26th USENIX Security Symposium, USENIX Security*. 2017.

Poisson Distribution(Applications)

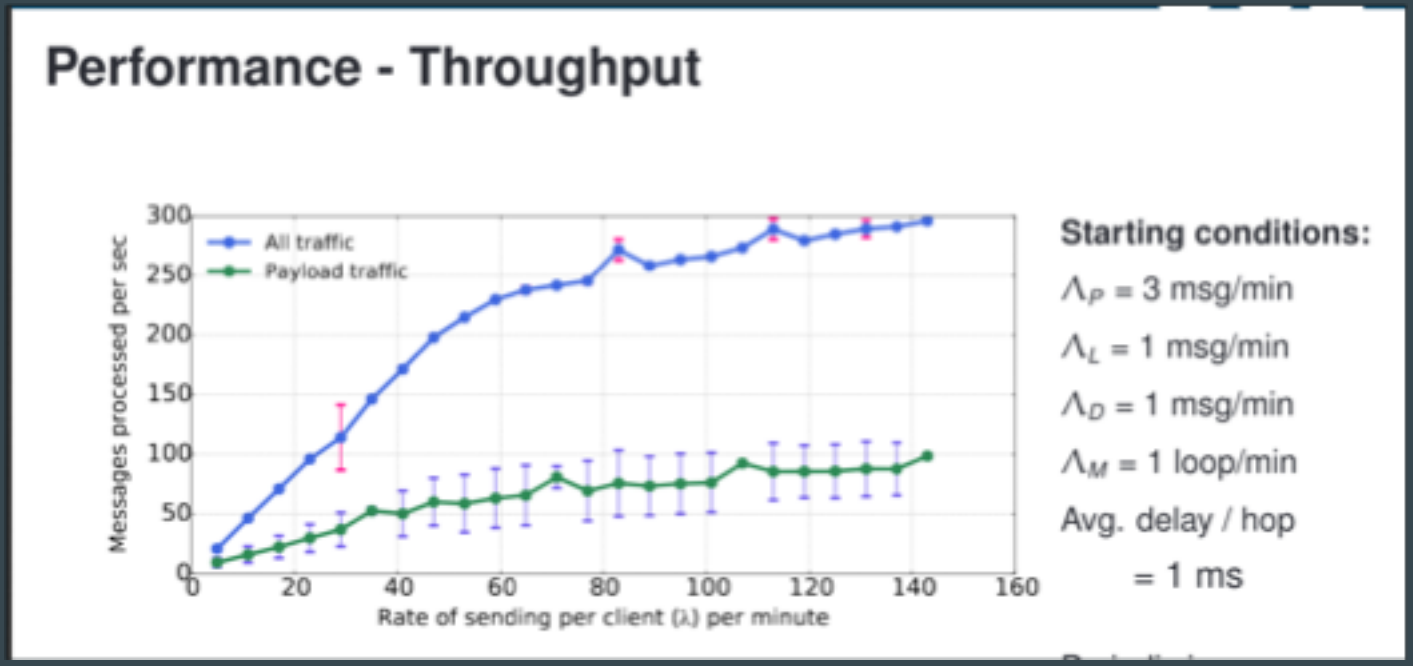
- ➔ The number of mutations on a given strand of DNA per time unit (Wikipedia-Poisson, 2012).
- ➔ The number of bankruptcies that are filed in a month (Jaggia, Kelly, 2012 p.158).
- ➔ The number of network failures per day (Levine, 2010, p. 197).
- ➔ The number of visitors to a Web site per minute (Sharpie, De Veaux, Velleman, 2010, p.654).



Overview Of Loopix

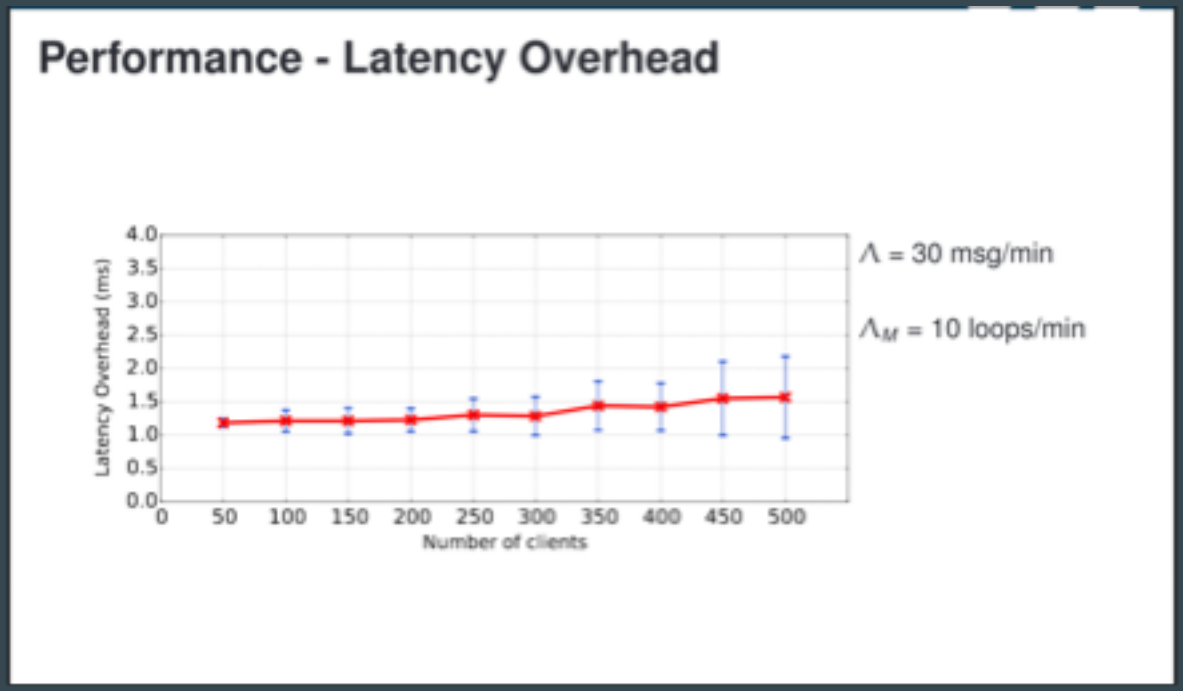


Performance



Piotrowska, Ania M., et al. "The loopix anonymity system." *26th USENIX Security Symposium, USENIX Security*. 2017.

Performance



Piotrowska, Ania M., et al. "The loopix anonymity system." *26th USENIX Security Symposium, USENIX Security*. 2017.

Performance vs Other systems

	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	✓	✓	✓	✓	✗	✗	✗

Piotrowska, Ania M., et al. "The loopix anonymity system." *26th USENIX Security Symposium, USENIX Security*. 2017.

Discussion

1. What are the possible impediments to adoption?
2. What are the disadvantages of Offline Message Service?
3. What are the security metrics used to make comparisons among Protocols?
4. Any disadvantage for using Sphinx?
5. What are the applications that can be built of Loopix?