Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

How Alice and Bob meet if they don’t like onions

Survey of Network Anonymisation Techniques

Erik Sy

34th Chaos Communication Congress, Leipzig

Agenda

1. Introduction to Anonymity Networks
   - Anonymity
   - Strategies Towards Anonymity
   - Adversaries

2. Anonymous Communication Networks
   - I2P
   - Freenet
   - GNUnet
   - JonDonym

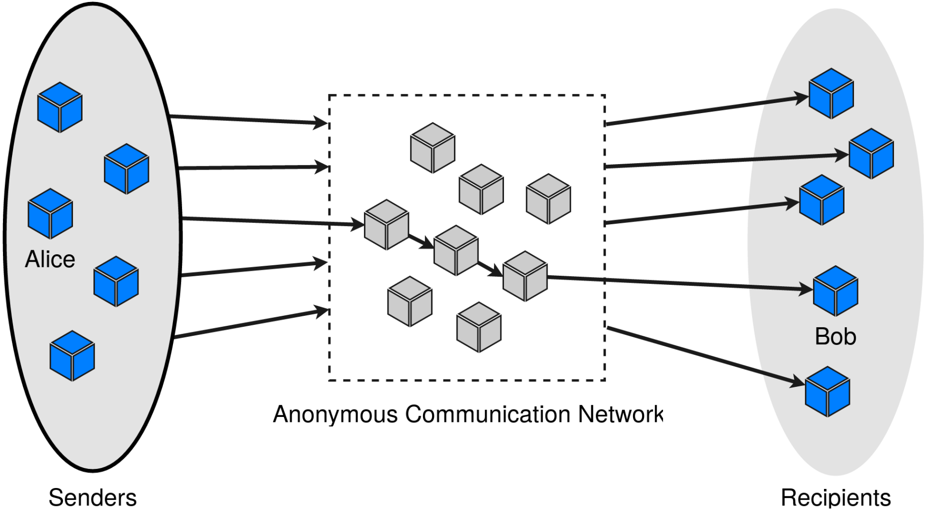
3. Research Work

4. Conclusion

Anonymity

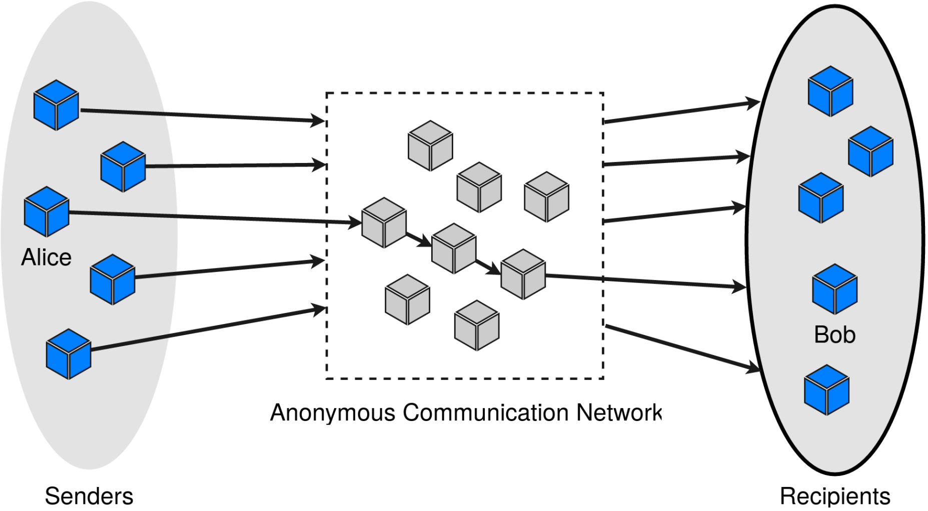
Anonymity is the state of being not identifiable within a set of subjects, the anonymity set. Andreas Pfitzmann

Sender Anonymity



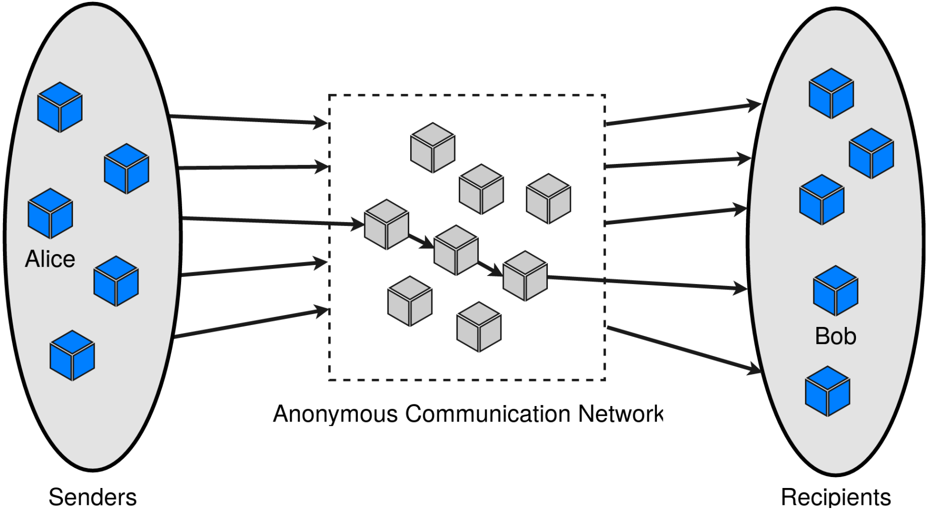
The sender may be anonymous only within a set of potential senders.

Recipient Anonymity



The recipient may be anonymous only within a set of potential recipients.

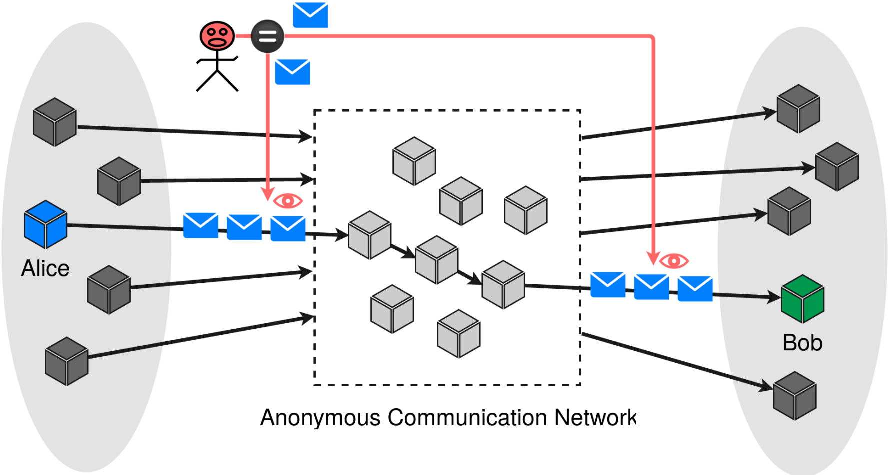
Sender Recipient Anonymity



Unlinkability

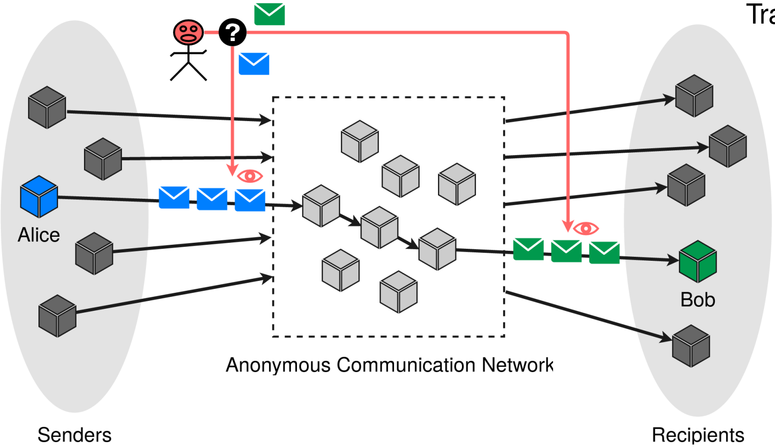
Unlinkability of two or more items of interest from an attacker’s perspective means that within the system, the attacker cannot sufficiently distinguish whether these subjects are related or not. Pfitzmann, Hansen

Relationship Anonymity



Alice can be linked to Bob.

Relationship Anonymity



Traffic analysis

- pattern in size of packets
- pattern in timing of packets
- content of messages
- ...

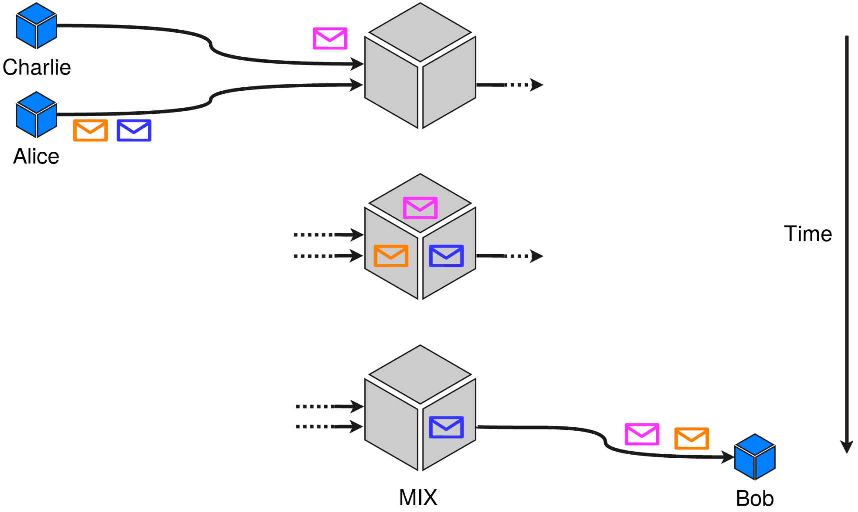
Alice cannot be linked to Bob.

Who do you trust?

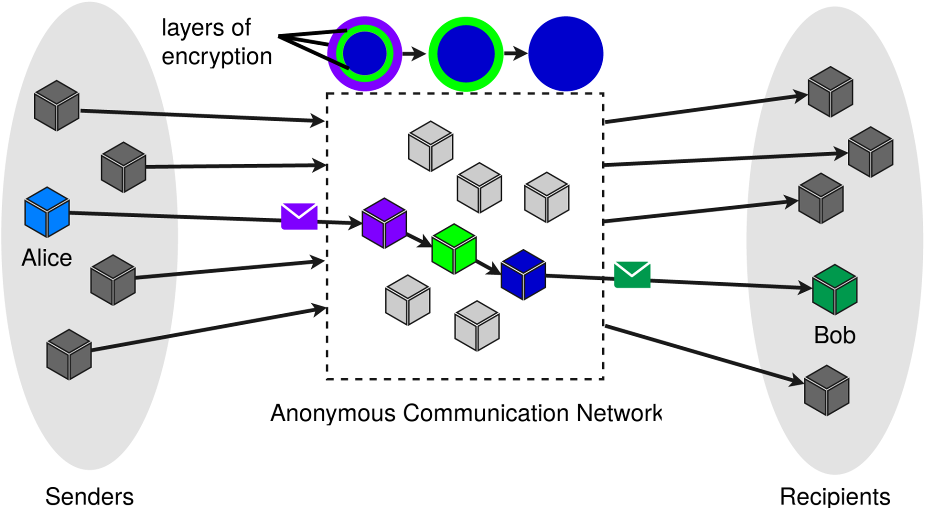
Strategies Towards Anonymity

- Cover traffic
- Broadcasting messages
- Trusted third party (VPN, Proxy)
- Shuffling and delaying of messages (mix, anonymous remailer)
- Anonymity systems that distribute trust
  - Secure multi-party computation (DC-Nets)
  - Cascades of mixes
  - Onion routing
  - Garlic routing
  - ...

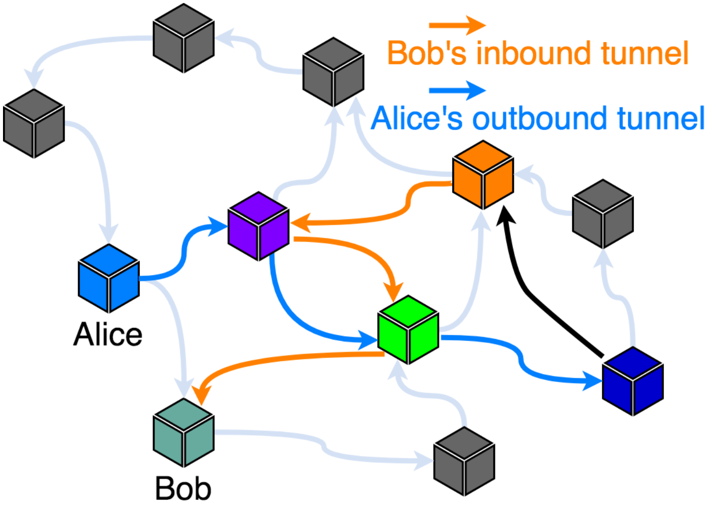
One-hop Mix



Onion Routing



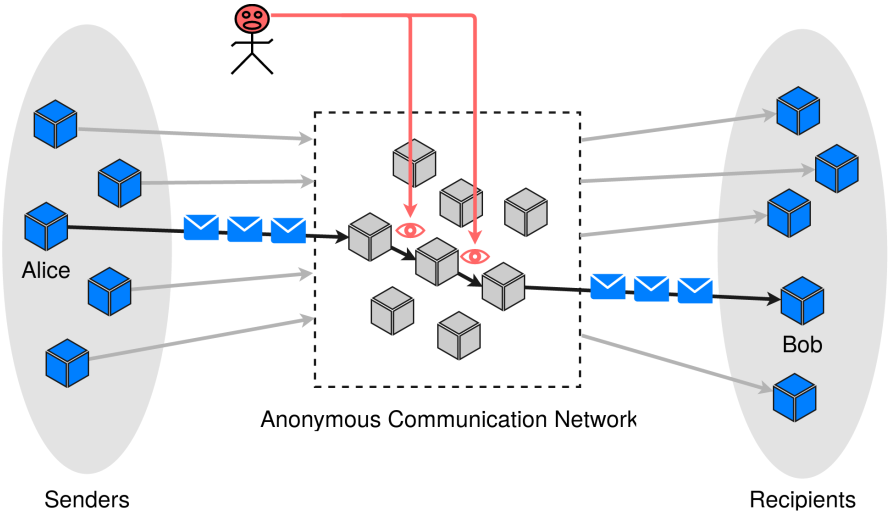
Garlic Routing



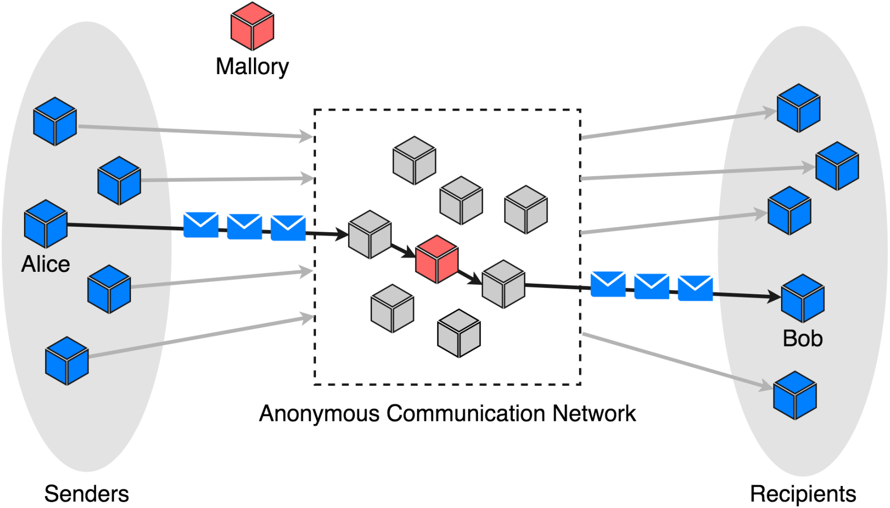
- Peer-to-peer
- Uni-directional channels
- Messages can be bundled
- Uses layers of encryption

Adversaries

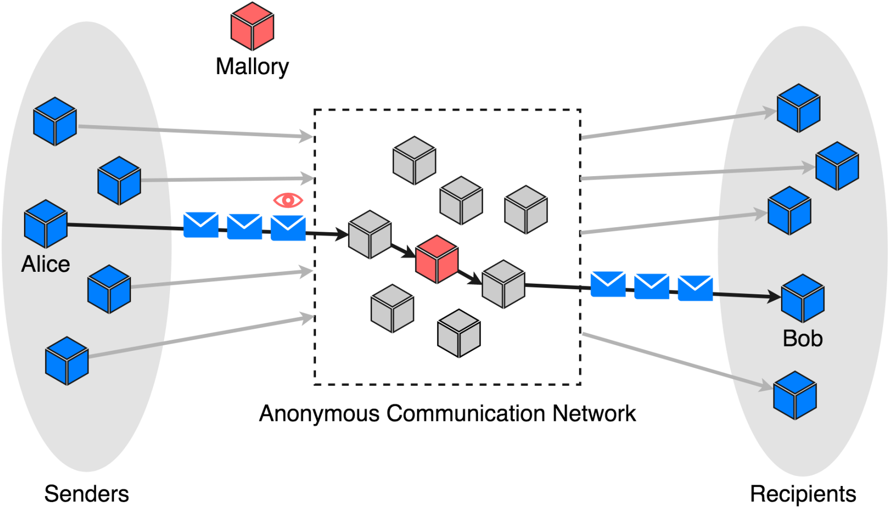
External Adversary



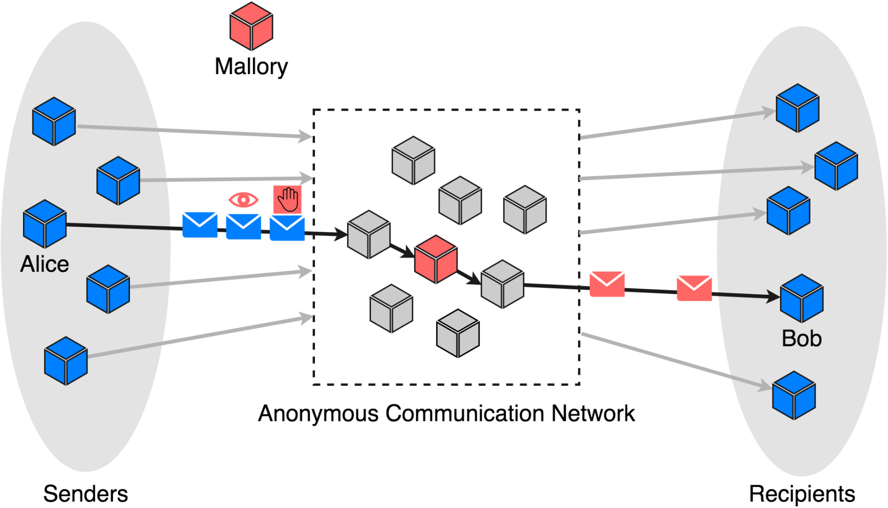
Internal Adversary



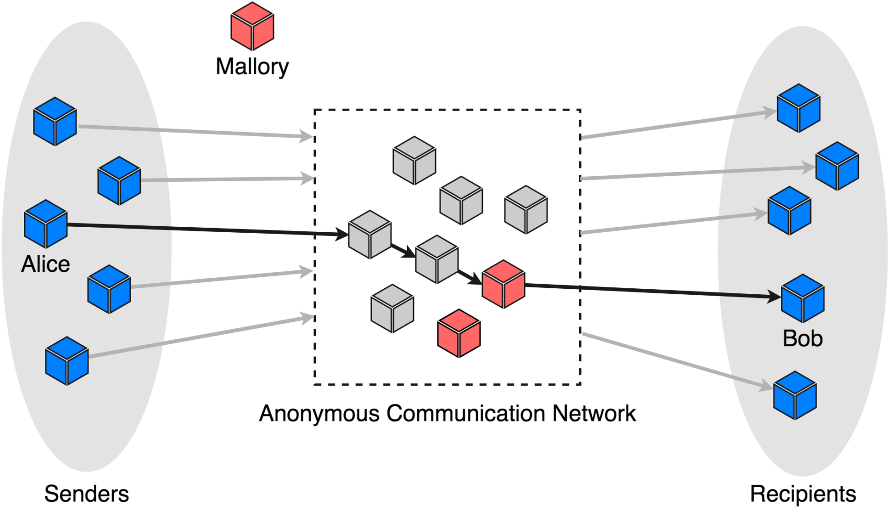
Passive Adversary



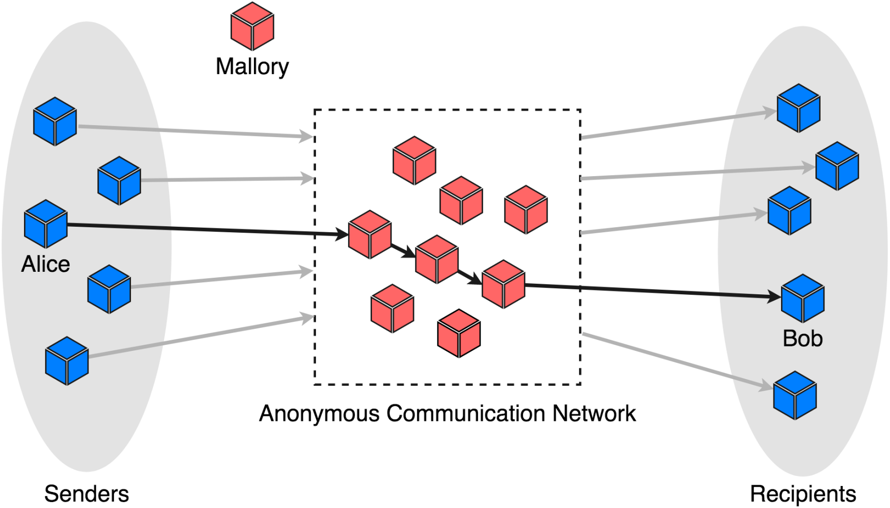
Active Adversary



Local Adversary



Global Adversary



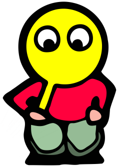
Anonymous Communication Networks

Anonymous Communication Networks (ACNs)

- Many defunct, unimplemented or unavailable networks exist
  - Conflux
  - MorphMix
  - Herbivore
  - . . .
- We selected a few implemented and usable networks:
  - JonDonym
  - Freenet
  - I2P
- Some research projects:
  - Vuvuzela
  - Loopix
  - AN.ON-Next

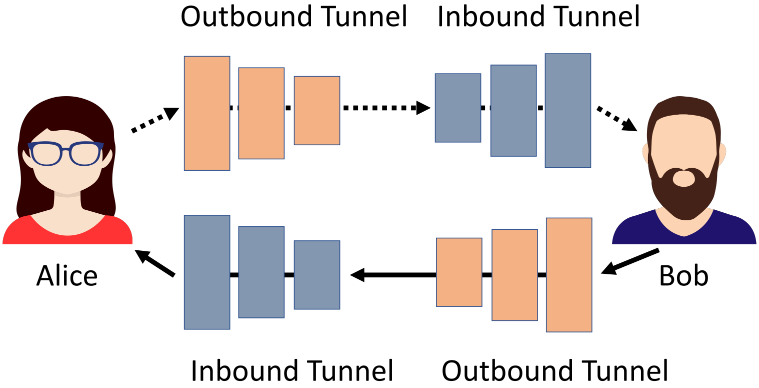
I2P

- Low-latency peer-to-peer network of 70 000 nodes
- Focuses on Hidden Services with few outproxies
- I2P applications
  - P2P applications
  - Web browsing
  - Email, instant messaging, and IRC
  - File storage
- Actively developed with releases every two months



Itoopie

How Alice and Bob meet on I2P with Garlic Routing



- Encryption layers are added/removed along the path
- Alice sends messages towards Bob's entry point of the inbound tunnel
- Lifetime of a tunnel is limited to 10 minutes

I2P – How does Alice build her tunnels?

- Loads an initial set of active peers from public sources (bootstrapping)
- Collects a local statistic about all seen routers
- *Exploratory tunnels* are used to build, manage and destroy other tunnels
- Selects set of well performing seen routers for tunnel establishment
- Sends *tunnel construction request* over *exploratory tunnel* to chosen peers
- If peer accepts request, then symmetric keys and successor address are exchanged

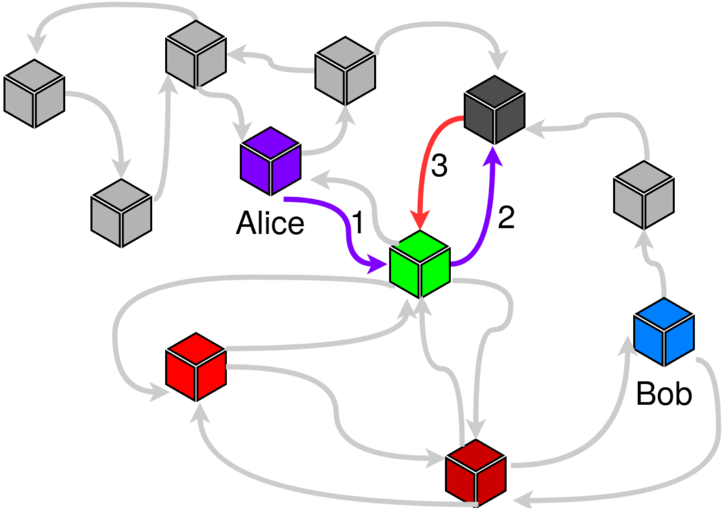
I2P – How does Alice get the contact information of Bob?

- Every peer is uniquely identified by the *routerInfo* data structure containing public key, identifier, and contact information of the peer
- Super-peers store *routerInfo* for every peer in a distributed hash table (*netDB*)
- For offered services the entry points of the inbound tunnels (*leaseSets*) are also stored in *netDB*
- I2P protects the information which peer operates a certain service
- With previous knowledge about Bob, his routerInfo or leaseSet can be retrieved from the netDB

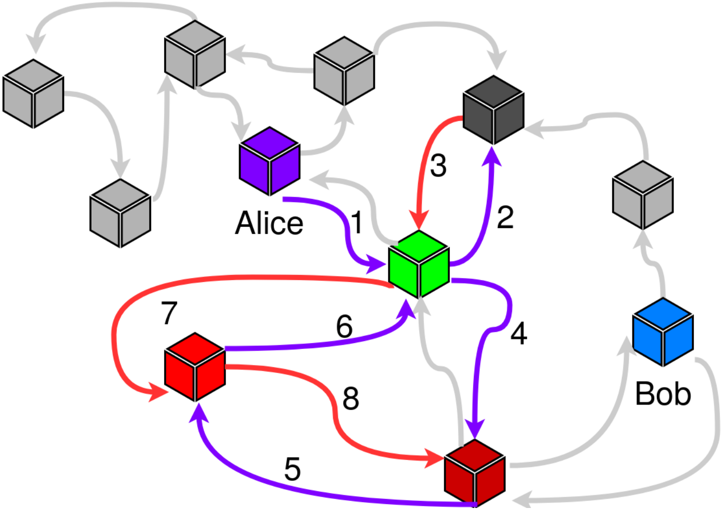
Freenet

- Peer-to-peer network of 10 000 nodes
- Focuses on distributed information storage
- Actively developed since 2001
- Optional friend-to-friend topology
- Applications:
  - File storage
  - Static Web pages
  - Chat, Email, Social

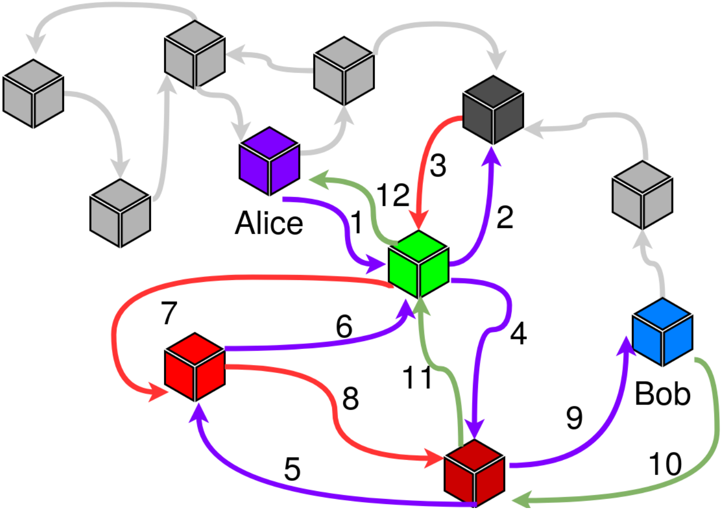
Freenet – How Alice and Bob meet



Freenet – How Alice and Bob meet

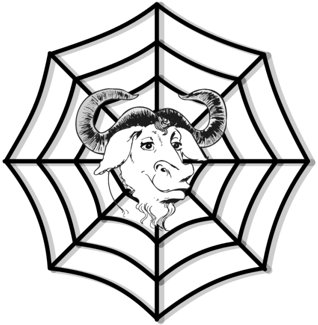


Freenet – How Alice and Bob meet

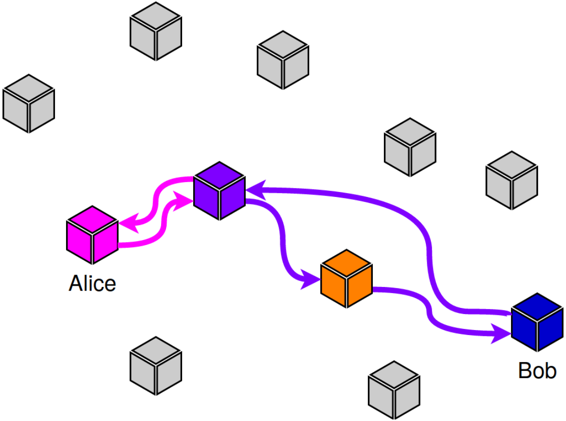


GNUnet

- Foundation for an alternative network stack
- Primary application: file sharing
- Similar to Freenet, but with economically inspired trust model
  - Depending on a relay’s load, messages are forwarded to zero or more nodes
  - Users can trade anonymity for efficiency
- Optional friend-to-friend topology



GNUnet – Trading Anonymity for Efficiency



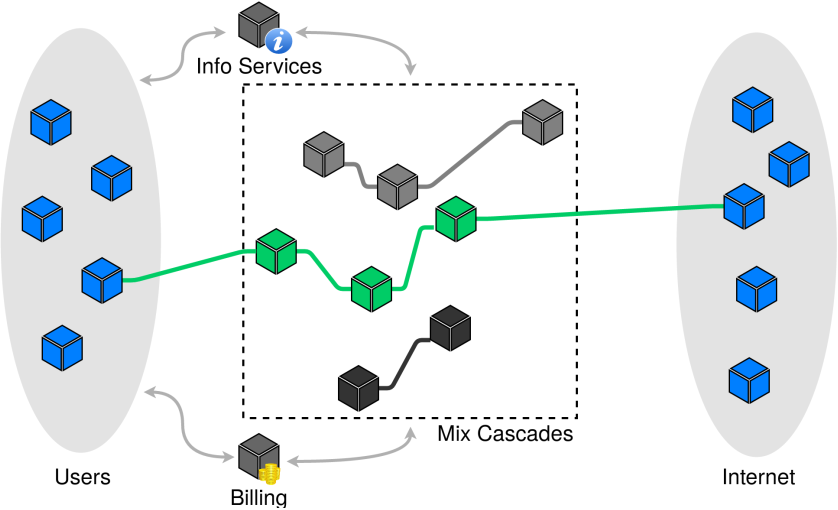
Nodes may indirect traffic by replacing reply addresses (→cover traffic). . .

. . . or forward traffic without rewriting reply addresses (→preserve bandwidth)

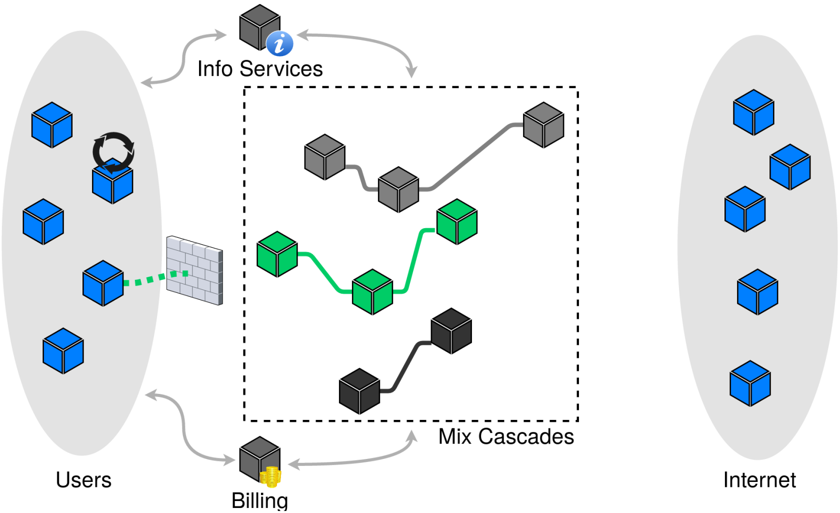
JonDonym – Overview

- Focuses on legacy Internet
- Developed as part of research project AN.ON
  - formely known as **J**ava **A**non **P**roxy
- Mix-based ACN
  - Two (free) or three (premium) hops per cascade
  - Mix operators are known
- 5000 paying users

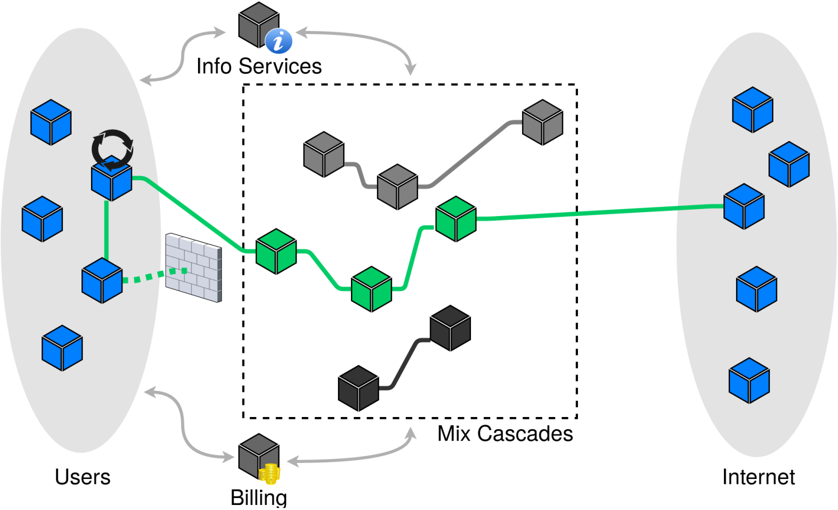
JonDonym – Network Architecture



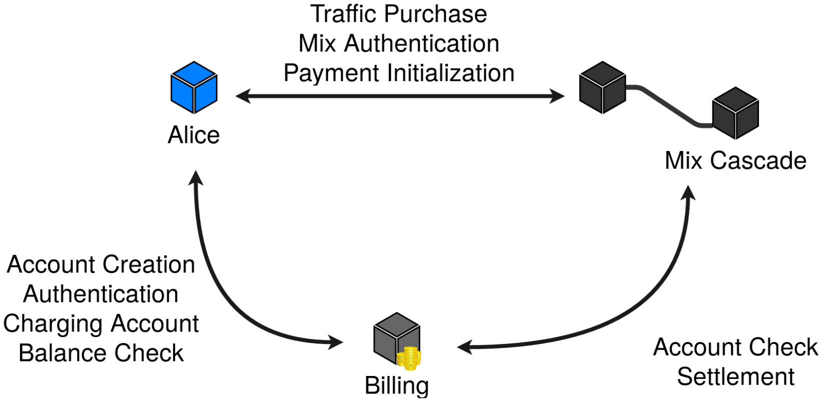
JonDonym – Censorship Circumvention



JonDonym – Censorship Circumvention



JonDonym – Payment



Billing methods paysafecard, Bitcoin, bank transfer, cash by mail, . . .

Comparison of Anonymity Systems

- Threat model
  - None of these ACNs protects against a global, passive observer
  - Each ACN has some tolerance against internal, local and active adversaries
  - GNUnet and Freenet protect hosts in case of identification with plausible deniability
- Use Cases
  - Sender anonymity in legacy Internet with Tor, JonDonym and partially I2P
  - Hidden Services with Tor, I2P, Freenet and GNUnet
  - Files remain online after publisher goes offline with Freenet and GNUnet
  - Anonymous file sharing with I2P, Freenet, GNUnet and partially Tor

Comparison of Anonymity Systems

- Provider model
  - Relays are run by volunteers (Tor)
  - Relay operators are approved by provider (JonDonym)
  - Every peer is a relay for others (I2P, Freenet, GNUnet)
- Usability, size of anonymity set, active community
  - Tor seems to be considerably better in these categories

Research Work

AN.ON-Next

Vuvuzela

Loopix

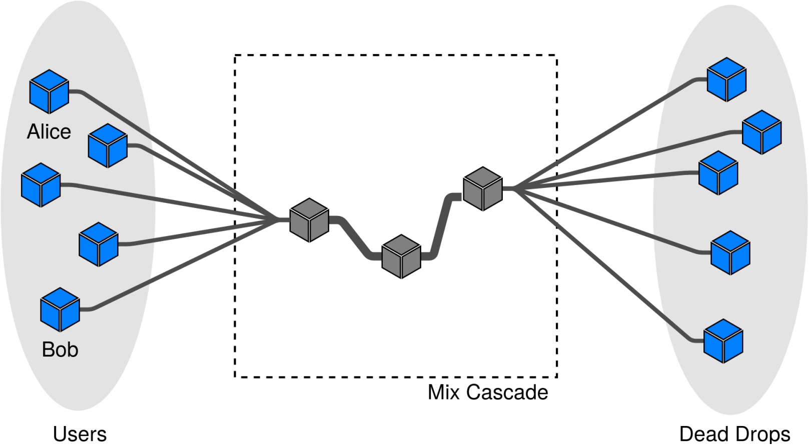
AN.ON-Next

- Ongoing research project
- Zero-effort privacy
  - Relaxed attacker model
  - Trust in ISP
  - Shuffling of IPv6 addresses
- *JonDonym 2.0*
  - Low-latency MIXnet

AN.ON
NEXT GENERATION

Vuvuzela

- MIXnet hides origin of messages
- Noise obscures metadata
- Scales with number of users



Loopix

- Mixnet-based anonymous communication system
- Makes use of cover traffic
- Sender determines a delay for messages in the mixes
- Aims to resist powerful adversaries such as global passive observer and active attacker
- Security goals
  - Sender-receiver third-party unlinkability
  - Sender online unobservability
  - Receiver unobservability

Conclusion

- Tor is good but not alone
- There is no practical anonymity systems that resists a global passive observer
- There is no anonymity without security
  - Test system
  - Report bugs
  - Send patches
- Your participation in these networks protects your privacy and the one of others

How Alice and Bob meet if they don’t like onions

Survey of Network Anonymisation Techniques

Erik Sy

34th Chaos Communication Congress, Leipzig