PDS, 15.12.21

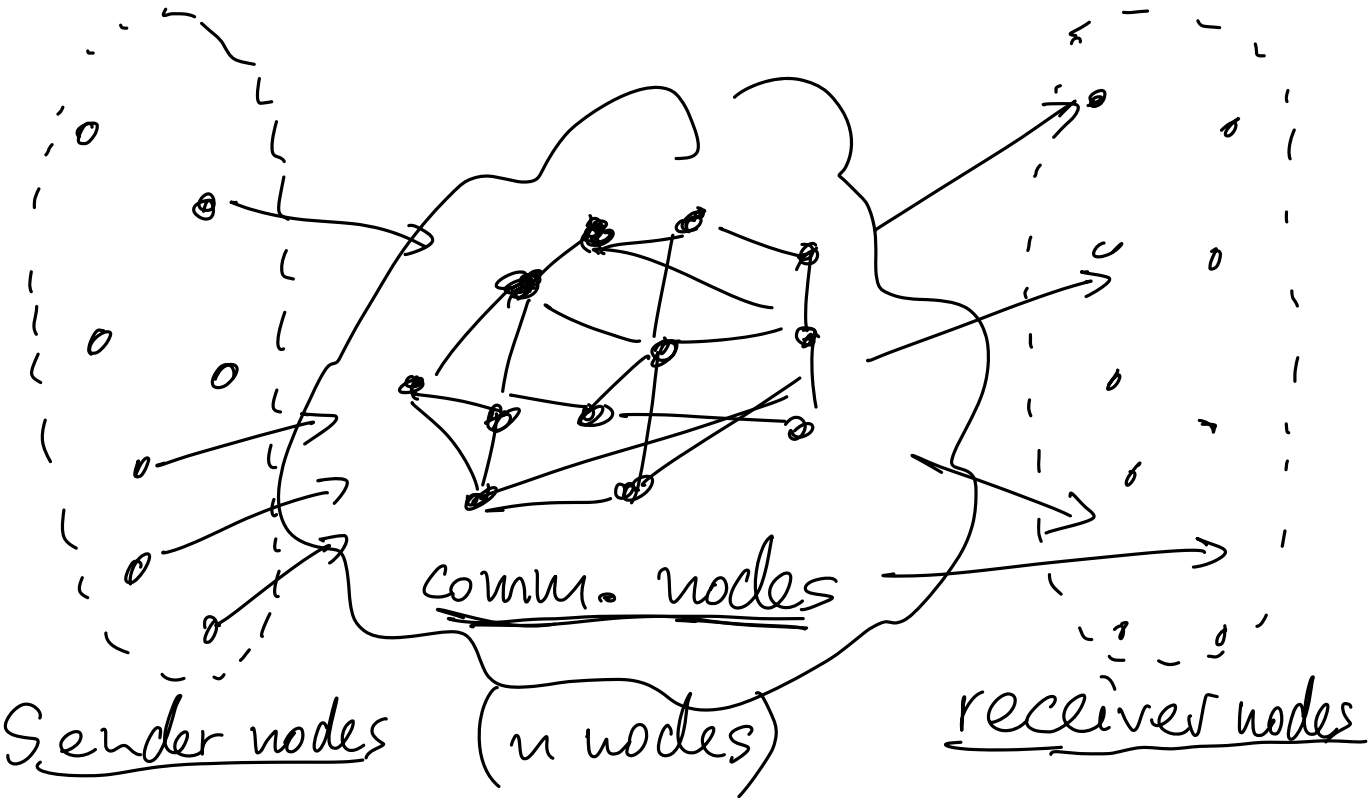
9) Anonymous Communication

Anonymity: hide in a crowd

Network needs addresses, routing, transmission metadata

9.1) Terminology

(Pfitzmann & Hansen)



(initiators) (targets)

- For datagrams (single messages)
- For circuits (connections, bi-directional)

Assumptions

- Each node only sees messages that it receives or sends
- Messages carry source and dest. addrs.

Global observer: sees all msgs. on network

Anonymity means that a node (sender or receiver) is one of many nodes among a anonymity set.

Anonymity of a message (or connection)

Property	... against node(s) ...
Sender anonymity	receiver / some nodes / global obs.
Receiver anonymity	sender / some nodes / global observer
Unlinkability of sender and receiver	- / some nodes / global observer

Ex. VPN or Proxy

- Communication through one node

Properties

- Sender anonymity against receiver, but not against any other node
- Receiver anonymity: against sender,

but not against other nodes

- Unlinkability against global observer (when meta-data is removed)

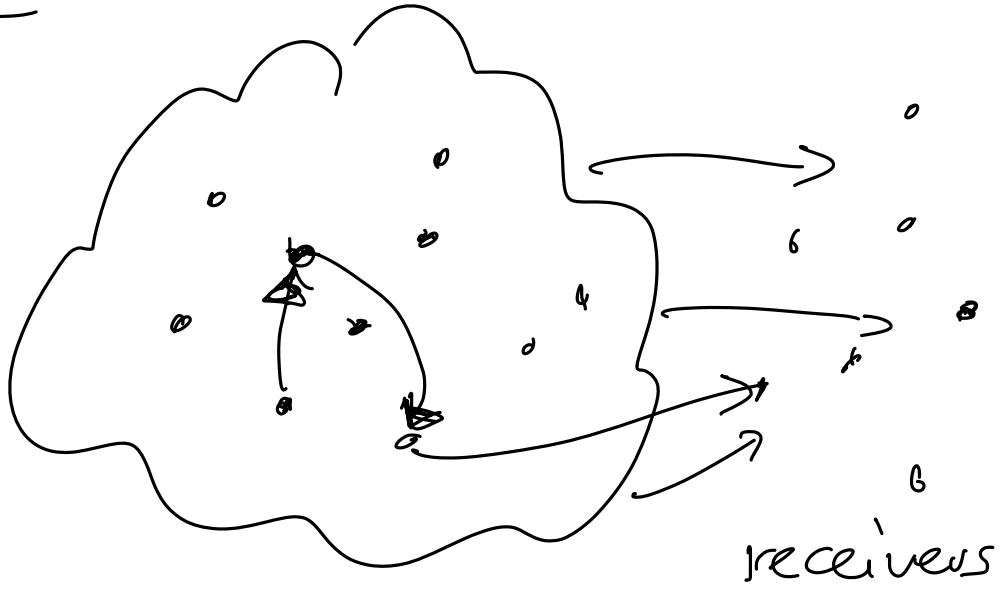
Assumptions

- Ignoring timing, sizes, traffic shape, inter-packet arrival times

9.2) Crowds

- Early research prototype
- Influential
- AT&T Research (ex Bell Labs)

Model



Crowd

- Crowd needs membership service
- Algorithm
  - To send a msg, send msg. to myself
  - Upon receiving some msg.

    Flip a coin b, with prob. p

    If b = 1 then

    select a uniformly random member d of crowd

    send msg. to d

    record route to receiver node via d

    else

    send msg. to receiver node

Properties

- Sender anonymity
  - against receiver : excellent
  - against some node: partially good
  - against all nodes: none
  - against global obs: none

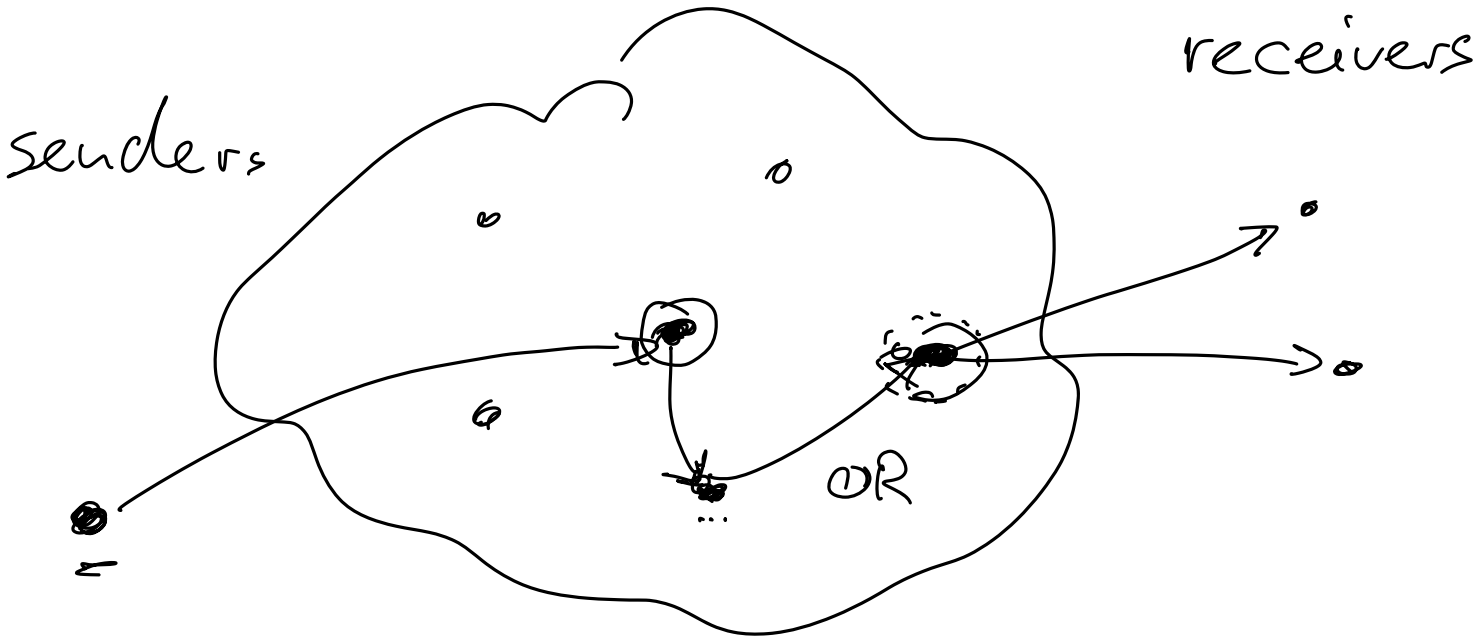
- Receiver anonymity: none

- Unlinkability:
  - against some nodes: partially
  - against all nodes: none
  - against global observer: none

9.3) Onion Routing

- TOR : The Onion Router
- Practical connection-oriented routing protocol
- Low latency

TOR network



- Collection of comm. nodes, acting as onion routers (OR)
- Each OR maintains a encrypted longe

standing connection to every other OR

- Traffic among OR consists only of fixed-size cells (512 bytes)
- Membership (directory) service
- Client (sender) connects via a Onion Proxy (OP)

Onion Routes

- Each OP communicates via one circuit (onion connection)
- Route through the network
- Carries multiple types of traffic (HTTPS, SSH, ...)
- Lifetime of minutes (10)

Onion route setup

- Sender (OP) picks a random route of length ℓ through network ($\ell = 3$)
- Source routing
- for $h = 1, \ldots, \ell$ do

  OP establishes a session key K_h with node h

Onion communication protocol

- Sender (OP) encrypts msg. m as

$$c \leftarrow Enc_{K_1}\Big(Enc_{K_2}\big(\cdots Enc_{K_\ell}(m; Dest); OR_3\big); OR_2\Big)$$

"The onion"

Dest is receiver addr. outside TOR netw.

- Every OR (node h) operates

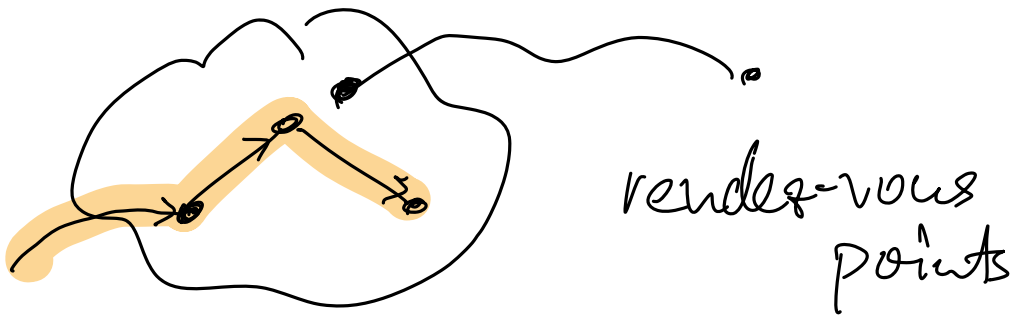
$$o \leftarrow Dec_{K_h}(e)$$
$$(c'; OR_{h+1}) \leftarrow o$$
send c' to OR_{h+1} (via comm.)

- Exit nodes (OR when $h = \ell$)

send m to Dest

- Reverse direction follows inverse ops.

Today ~ 7000 OR nodes
millions of users



Security

- Each OR_n sees encrypted traffic from random OR_{n-1} to OR_{n+1}

- Exit nodes (OR_e) for one circuit see all traffic
  - receiver
  - content
  - correlations

Properties

- Sender anonymity
  - against receiver : excellent
  - against one $(n-1)$ nodes: excellent
  - against all nodes: none
  - against global obs: none

- Receiver anonymity
  - against sender : none
  - against one $(n-1)$ nodes: excellent

- against all nodes: none
- against global obs: none

- Unlinkability
  - against one $(n-1)$ nodes: excellent
  - against global observer: none

Remaining information leaks

- Metadata (timing, traffic shape...)
- DNS ?
- Exit nodes

→ Mix networks