The Private Peer Sampling Service

The Ground for your Secret Society

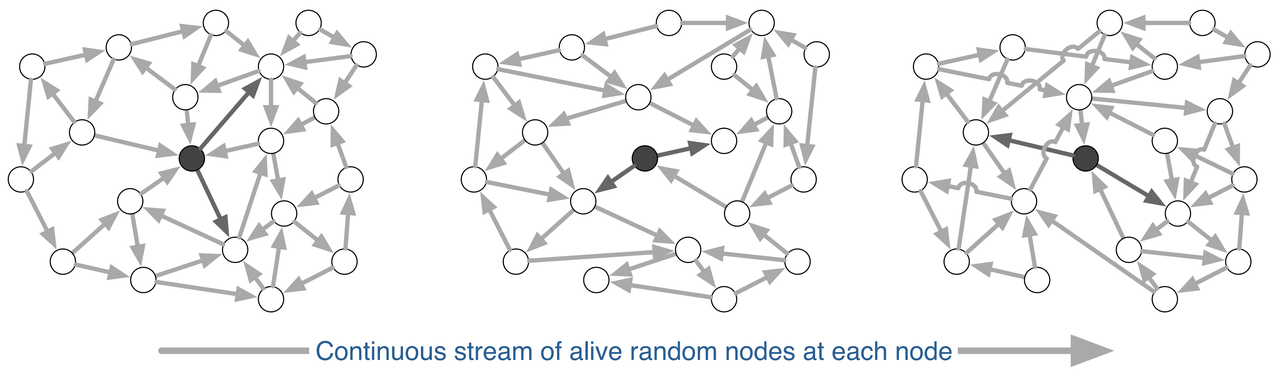
Valerio Schiavoni, Étienne Rivière, Pascal Felber

University of Neuchâtel, Switzerland

Context and Problem

- Large-scale network, no PKS or trusted parties
- Secured communications and confidential membership among members of private groups

Peer Sampling Service: a Building Block for Large-Scale Applications



- Group membership
- Randomness
- Keeps network connected

Challenges

- Serverless confidential communication
- Private and secret group membership
  - Protect groups from targeted attacks

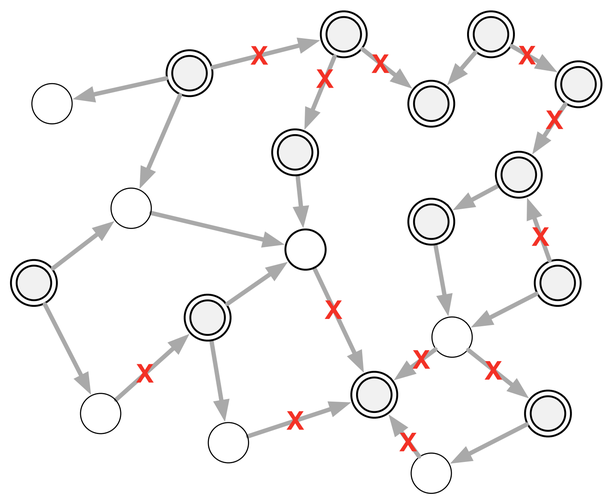
Objectives

- Build a Private PSS for each secret group:
  - stream of secure channels to alive nodes from the group
  - secret membership protects group members identities and prevents group mapping

... based on a system-wide PSS

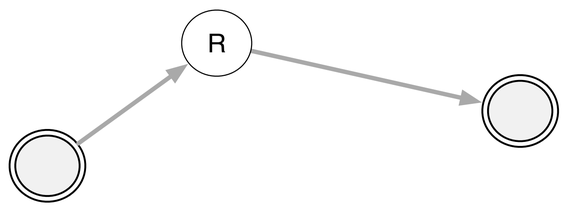
Real World Setting

- NATs
- Firewall
- Relays



Relay nodes

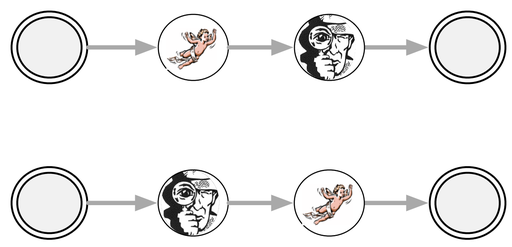
- Help with NATs
- Threat to privacy



- How to use relays but hide source/destination/content ?

benevolent relays

malicious relays



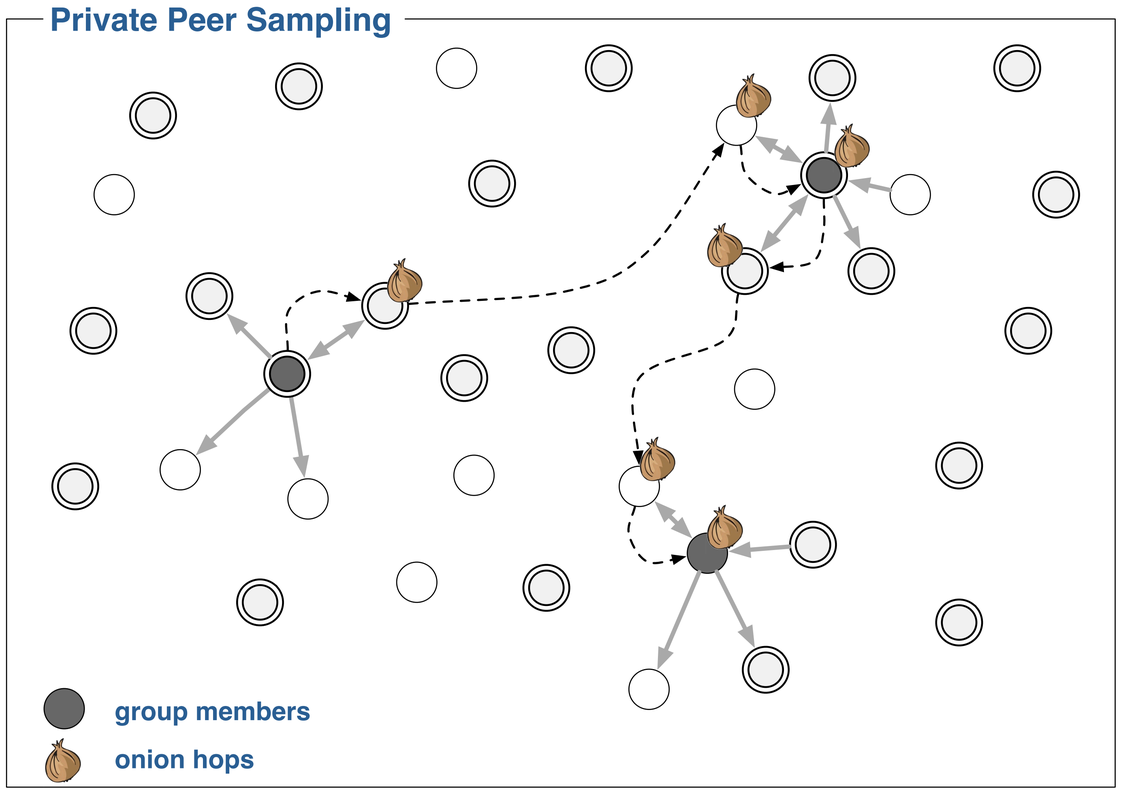
Group Management

- Creation and admission via signed group keys, passports
- Access via explicit invites (IM, emails, ..)

Private Membership Management

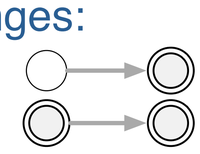
- Gossip-based views exchange
- No direct communications
- PSS over Secure Anonymizing Channels

Private Peer Sampling

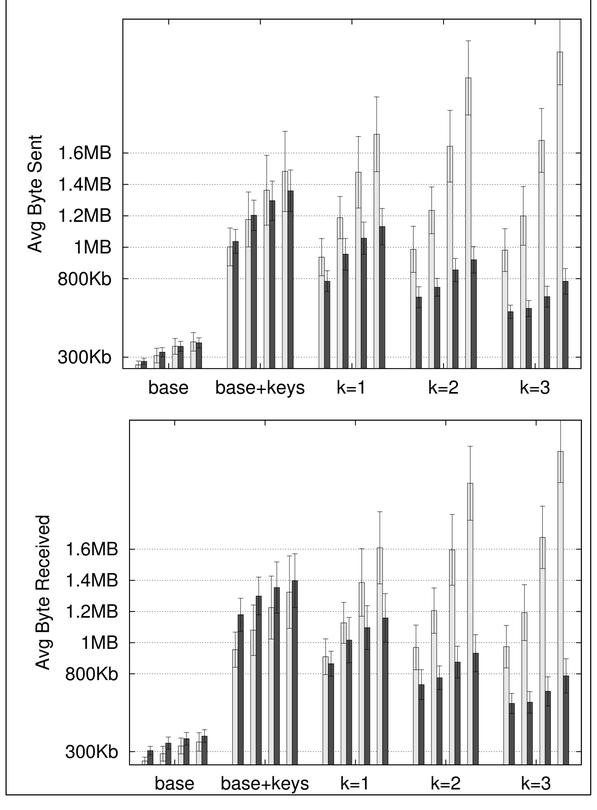


Onion Views

- Messages exchanged via onion routes
- Decentralized PKI
- Routing challenges:
  - Pub-to-NAT
  - NAT-to-NAT



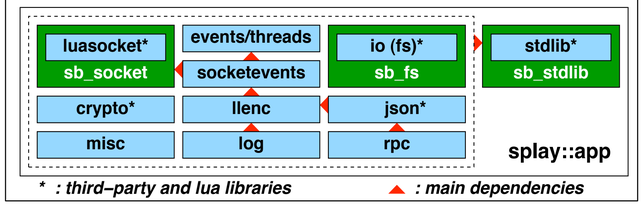
- Bandwidth cost to maintain onion-friendly views:



Implementation

- Tested and implemented using SPLAY (NSDI'09)
- Lua-based DSL and libraries

`www.splay-project.org`



Ongoing Evalution

- Detection/recovery from faulty onion-routes under continuous churn conditions
- Impact of onion-friendly views on clustering
- Computing cost breakdown at relay nodes
- Deployment over PlanetLab and home devices

Institut d'informatique
Université de Neuchâtel

SPLAY

UNIVERSITÉ DE NEUCHÂTEL