P2P user identification: username/password

Rodrigo Fernández
rfernand@inf.utfsm.cl

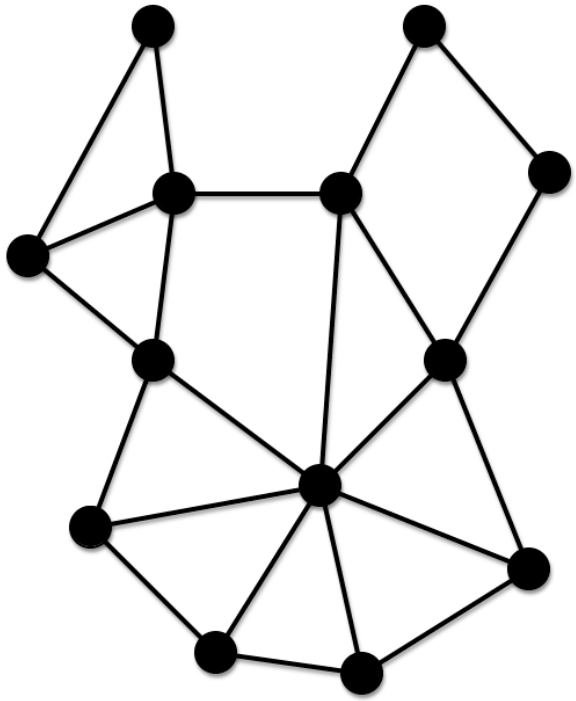
Universidad Técnica Federico Santa María

24 de junio de 2013

P2P Networks

Characteristics

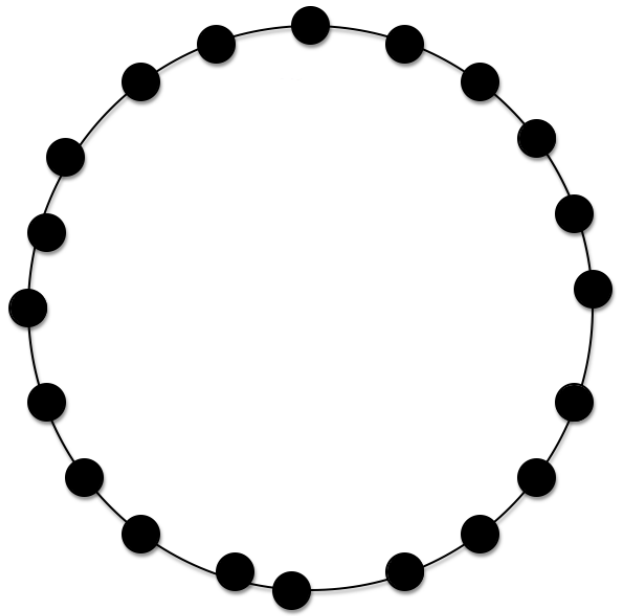
- Scalable
- Decentralized
- Self-maintained
- Robust



P2P Networks

Overlay structure

- Structured networks (CAN, CHORD)
- Unstructured networks (Gnutella, Bittorrent)



P2P Networks

Overlay structure

- Images of structured/unstructures networks
- Differences

Username / password identification

Why?

- Many complex systems require authenticated users to work.
- Most of the users has more than one device, so identification through multiple devices is needed.
- User are accostumed to username/password solutions.

Username / password identification

P2P Identification Schemes

Descentralized schemes distributes the task of public key auth to all participants.

- PGP-like scheme
  Creates web of trust to auth public keys based on their acquaintances opinions.
- Quorum-based scheme
  Multiple independent participants replicate public keys.

Identification schemes

In need of a third party

- PKI
- Username/password pair

Poor scaling, single point of failure, heavy administration overhead.

Trust in P2P networks

Bizantine nodes

Are all nodes that not behave as expected

1. Faulty nodes
2. Malicious nodes
3. Infected nodes

Trust in P2P networks

Bizantine node tolerance

P2P networks can achieve byzantine fault tolerance under 1/3 byzantine peers
A peer is honest only if the peers executes the protocol faithfully; otherwise, the peer is faulty.

Byzantine Generals Problem

Redes P2P

- ...

Identificación de problemáticas actuales

- Vender ideas en cuanto son comercializables.
- Imponerse a propósito más presión sobre sí mismo.

EOF