

0. Course Overview

- **I. Introduction**
- **II. Fundamental Concepts of Distributed Systems**
 - Architecture models; network architectures: OSI, Internet and LANs; interprocess communication
- **III. Time and Global States**
 - Clocks and concepts of time; Event ordering; Synchronization; Global states
- **IV. Coordination**
 - Distributed mutual exclusion; Multicast; Group communication, Byzantine problems (consensus)
- **V. Distribution and Operating Systems**
 - Protection mechanisms; Processes and threads; Networked OS; Distributed and Network File Systems (NFSs)
- **VI. Peer to peer systems**
 - Routing in P2P, Bittorrent, OneSwarm, Ants P2P, Tor, Freenet, I2P
- **VII. Security**
 - Security concepts; Cryptographic algorithms; Digital signatures; Authentication; Secure Sockets

Peer to peer systems

- **Fundamental properties**

- No central server
- Redundant data storage
 - Routing is w.r.t. data objects → Overlay routing
 - Objects identified by GUID. Works best for immutable objects
- Dynamic structure. Constantly adding and removing peers
- Highly robust by replication of data/services
- Scalability

- **Examples**

- File sharing: Bittorrent, Gnutella, etc.
- VoIP, e.g., Skype
- Peercasting, e.g., PeerCast, IceShare, FreeCast
- Cloud computing; Grid computing
 - SETI@home (ET search in radio signals)
 - Folding@home (Protein folding)
 - Einstein@home (Search for gravitational waves)

Overlay routing

- **Overlay routing**
 - On application layer, i.e., extra layer on top of network
 - Unlike IP routing which is on network layer
- **Distributed Hash Table (DHT)**
 - Using secure hash, e.g. SHA1
 - Obtain GUID
 - Overlay routing based on distance of GUIDs.
 - Distance logical, not geographic.
 - Overlay routing can be seen as 'data object oriented' routing.
 - Examples:
 - Pastry
 - Tapestry
 - Kademlia
 - Distance measure can be based on, e.g.,
 - Numerical distance
 - Hypercube
 - XOR of two GUIDs

Bittorrent

- **Distributed sharing of data**
 - Simultaneous upload and download
 - Starting with .torrent file containing initial set of peers (and tracker(s))
- **Can use trackers**
 - E.g., <http://openbittorrent.com>
 - E.g., <http://www.publicbt.com>
- **Trackers not needed (e.g., using DHT)**
 - Vuze, µ-torrent, BitComet, Ktorrent support DHT
- **Many clients support additional features**
 - Protocol encryption
 - IP blocklists (e.g., <http://blocklistpro.com>)
- **Anonymity preserving extensions:**
 - OneSwarm
 - Distributed darknet; friend-to-friend sharing
 - I2PSnark (via I2P net)
 - Vuze (via Tor)

Anonymous P2P

- **Freedom of speech**
 - Anonymous blogging
- **Defeating censorship by**
 - Oppressive governments
 - Organizations
 - ISP
- **Exposing wrongdoings of**
 - Governments
 - Organizations
 - Companies
 - Individuals

**Without fear of retribution --> whistleblower protection
(see also www.wikileaks.org)**

- **Preserving privacy: protecting against**
 - Data mining
 - Tracking

Examples of Anonymous P2P Systems

- **Tor**
 - Onion routing
 - Layered encryption
 - Intermediate nodes do not know origin, destination or content of message
 - Does not protect against end-to-end analysis
 - Vuze bittorrent client can use Tor or I2P
- **Freenet**
 - Information sharing network; not proxy
 - Key-based routing (similar to DHT)
 - Distributed storage. Main goal is to defeat censorship.
 - Higher latency
- **I2P**
 - Anonymous P2P communication layer
 - Encrypted UDP (using AES 256 for packets and 2048bit DH key exchange)
 - Intermediate communication layer for all Internet services; → outproxies
 - Supports file sharing (e.g., iMule, i2phex (Gnutella), I2PSnark (bittorrent))
- **Ants P2P**
 - AES encrypted and anonymous traffic; eDonkey link format