582615 - Overlay and P2P Networks, Spring 2015

Exercise package 2 (20 points)

The exercises are intended to be done working in pairs. This package contains four exercises and an optional turbo challenge. During the course there will be three sets of exercises. The course book and the lectures contain some answers, but searching for outside sources too is strongly encouraged.

Schedule

There are two types of exercise sessions: Clarification sessions, where you can ask questions about the exercises or other matters about the course; and Answer sessions, where some answers to the returned exercises are presented and discussed.

- Clarification session: Tuesday 3.2. at 14:15
- **Exercise deadline**: Monday 9.2. at 12:00
- Answer session: Tuesday 10.2. at 14:15

Submission

Return your answers by email to juhani.toivonen@cs.helsinki.fi as an attached PDF or TXT document. Use "Overlay Exercise 2" as the subject line. The document should include:

- The title "Overlay exercise package 2"
- The name and student number of both writers
- The answers to the exercises

Assignments

Assignment 1 - Freenet (5 points)

The Freenet Project has created a model and software for an overlay network to enhance online privacy and prevent censorship.

- A user wants to download a file and inserts its CHK (Content Hash Key) to Freenet. Explain how Freenet fetches the file.
- What is the difference between Freenet's Opennet and Darknet operating modes? How are they bootstrapped? Why is Darknet considered more secure?

The basic operation of Freenet is described in the journal article *"Protecting Free Expression Online with Freenet"* by Ian Clarke, Scott G. Miller, Theodore W. Hong, Oskar Sandberg and Brandon Wiley. It was published in *IEEE Internet Computing journal, volume 6, issue 1, year 2002*. https://freenetproject.org/papers/freenet-ieee.pdf

Information on the operating modes can be found in the Freenet project wiki.

Assignment 2 - Network modelling (5 points)

Modelling and simulation are good starting points to find out if an idea, like a routing protocol, should work. They're also valuable in finding the optimum values for parameters in the protocol. Some networks have something called *power law* properties, or the *small world property*.

- What are power laws? Give an example of a power law regarding networks.
- What are small-world networks and scale-free networks?
- Why is a network whose nodes' degree (number of links) follows a power law resilient against random node failures?

Assignment 3 - Consistent hashing (5 points)

Consistent hashing is a technique used for load balancing and minimizing the effort of redistributing keys when changing the amount of nodes in a distributed hash table.

- How does consistent hashing work?
- What happens when you add/remove a node in a cluster-based system that uses consistent hashing?
- Why is it important to use a well balanced hash function?
- How can replication be done with consistent hashing?

Assignment 4 - Bloom filter (5 points)

A Bloom filter (named after its inventor Burton Howard Bloom) is a deliberately non-error-free data-structure that can be used to quickly determine whether an element might be found in a set.

- How are bloom filters different from ordinary hash tables?
- Bloom filters are a probablistic data structure and sometimes return false results. Can they still be useful? Why?
- How does one insert an element to a bloom filter, and how does one query it?
- How to remove an element from a standard bloom filter?

Consider the standard Bloom filter.

For reference: Tarkoma, S., Rothenberg, C. E., & Lagerspetz, E. (2012). *Theory and practice of bloom filters for distributed systems*. Communications Surveys & Tutorials, IEEE, 14(1), 131–155. http://www.dca.fee.unicamp.br/~chesteve/pubs/bloom-filter-ieee-survey-preprint.pdf

Turbo challenge (optional)

The turbo challenge allows you to recover lost points from other assignments, but will not increase the maximum points available. You can get full points from the exercise set without the turbo challenge.

Tor is another overlay system for increasing anonymity and circumventing censorship on the internet. Unlike Freenet, Tor can be used to anonymise browsing of the regular World Wide Web.

- How does Tor anonymise the browsing?
- How does *Onion routing* work? i.e. What happens while a message travels across the Tor network.
- In addition to regular WWW, Tor can be used to access so called *hidden services*. How are they different from browsing regular WWW sites?
- Tor provides anonymity. Does it also mean security? How can anonymity get compromised on Tor?