

Exercise No. 5
Peer-To-Peer Networks
Winter 2012/2013

Exercise 1 *Rumor spreading*

The following description is an algorithm for rumor spreading:

- At the beginning one node is infected.
- In one round, each infected node contacts and thus infects a random neighbor.
- No termination strategy is used.

Answer the following questions for both a line of n nodes, and a balanced binary tree of $n = 2^b - 1$ nodes ($b \in \mathbb{N}$), if the first infected node is the first on the line, or the root of the tree, respectively.

1. What is the expected number of rounds necessary to infect all nodes?
2. With k -times as many as the expected number of rounds ($k > 1$). What probability do you get for infecting all nodes with Chernoff?

Exercise 2 *Onion Routing*

Chaum's Mix Cascades can send a message anonymously from a peer A to a target peer B . Extend the algorithm such that the target peer B can send anonymously an answer to A without revealing A 's identity (i.e. IP address) to B .

Design an Onion Routing algorithm where after sending and replying B does not know A and the send and reply messages cannot be distinguished by all other nodes (except A).