Exercise 3

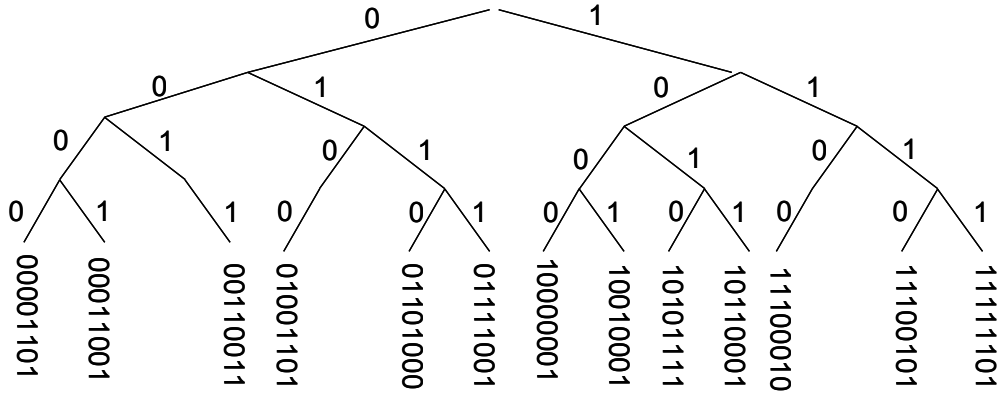
Exercises Peer-to-Peer-Systems and Security (SS2012)

Thursday 21.6 2012
Hand-in: Thursday 28.6. 2012 in lecture or per mail
Exercise: Monday 9.7. 2012

Dr. Heiko Niedermayer
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München

Task 1 Kademlia

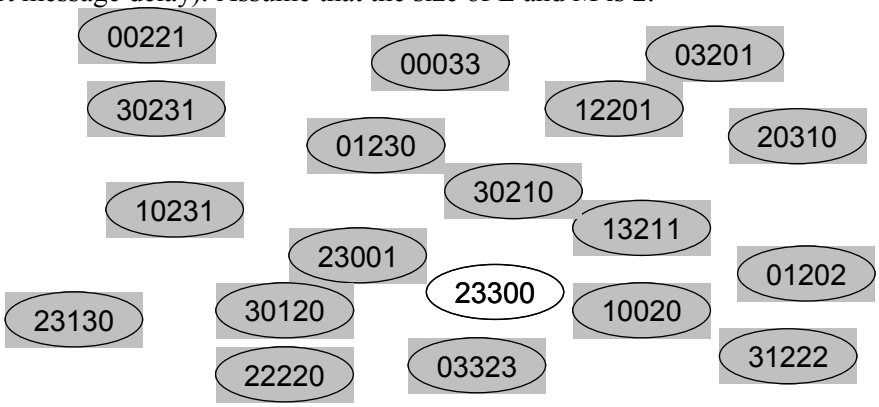
Now, we simulate the operation of Kademlia. Bucket size is k=2. Alpha is 2. The IDs are 8 bit long.



a) You want to store item 01000001. Calculate the distance (in bits and decimal notation) according to the XOR metric to the nodes 00110011, 01001101 and 10101111. Which node is responsible for the item?
b) Node 11010101 joins the network. Node 00110011 is the rendezvous peer that node 11010101 uses to join. Describe the operations of the join operations over time including the filling of the buckets.

Task 2 Pastry

This task is about Pastry. The figure is a snapshot with the current nodes (dark) and the new node (white) and how they are positioned in the underlay. If they are close in the figure they are close in the underlay (short message delay). Assume that the size of L and M is 2.

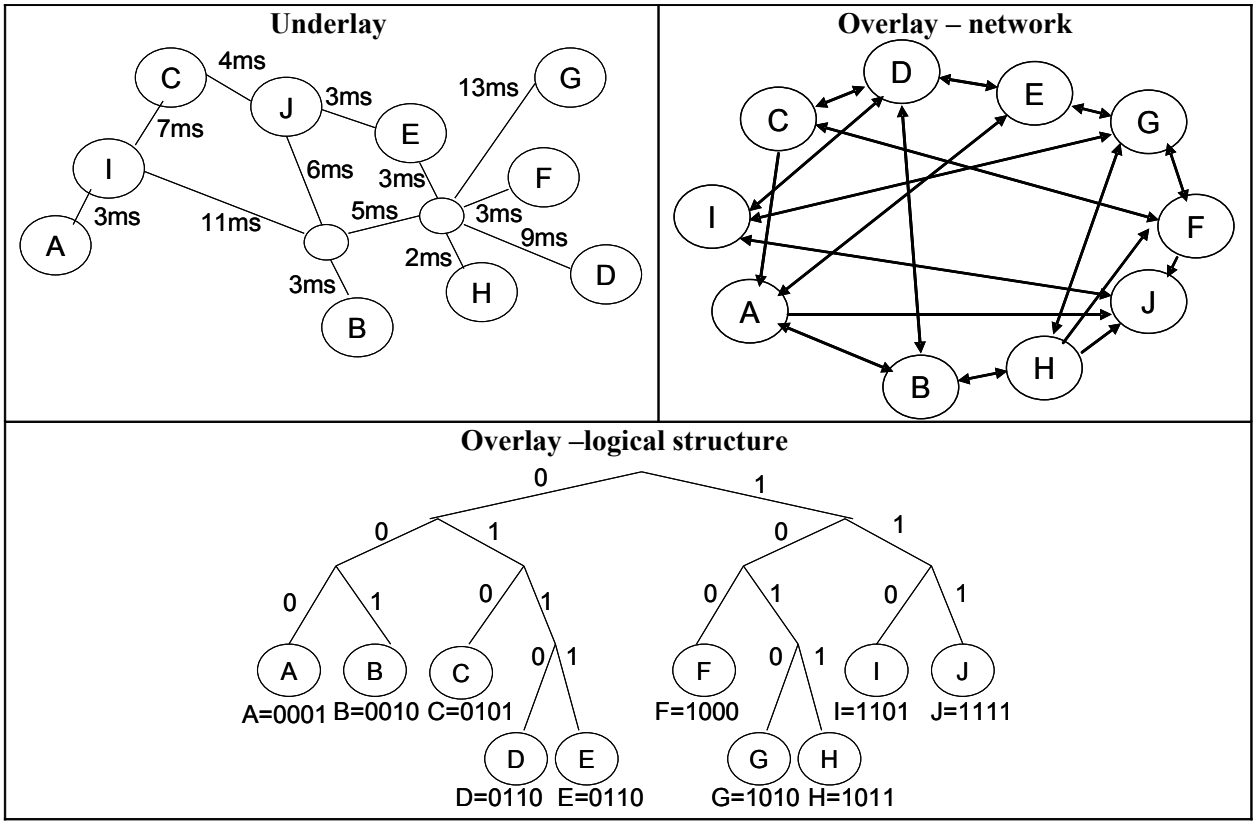


a) The white node 23300 wants to join the network via the node 10020. Describe the join process step-by-step and state the corresponding routing information seen and stored by the white node. What is the routing table of 23300 at the end? (Hint: There is no need to calculate each routing table, but simply make reasonable assumptions.)
b) Now, send a message from 23300 to ID 03023. For the first step use the routing table from a) and then make reasonable assumptions.

Task 3 Stretch and Proximity Neighbor Selection

The Figure below shows the underlay including the latencies along different paths. The second image is the structure of the overlay (nodes that link to each other) and the image on the bottom is the logical structure if we assume that our network uses a routing table like in Pastry, but without neighbor and leaf set.

In this task, stretch always refers to latency. Always state what path is used when you calculate the stretch.



c) What is the stretch (with respect to latency) for queries from F to A and from B to E?

d) Assume that each node on the way now applies PNS for its routing table. This means that it selected the latency-optimal node in each subtree. What is now the stretch for the queries from a)?

Task 4 Fighting Hotspots in Chord

From the lecture you should know two things. First, Chord proposes to replicate items to the k successors of the item ID for resilience. Second, this successor list as replica set cannot be hit by queries for the item. Thus, this does not help to fight hotspots (popular items are served by multiple nodes).

Modify Chord, so that all nodes in the replica set are utilized to answer queries for an item (Please note: This means that instead of using the successor list, do something different). Argue that your solution reaches this goal.

Task 5 Authentication

In this task we specify a cryptographic protocol which is meant to be used for mutual authentication.

a) Specify on what information and when in the protocol do the entities A,B, and S detect a successful authentication run?
b) The protocol is insecure. Find an attack. (The strength of the attacker is that it can read, send, fake, and drop messages in the network, yet it cannot break cryptography. This is a common security model in network security.)

Protocol :

Prerequisites:

S is a TTP.

Each participant X has a shared key with S. This key is called k kXS.

Let kab = Nb.

Protocol:

```
A -> B: Na, A
B -> S: {Na, A, B, Nb}kBS
S -> A: B, {Na, Nb}kAS
A -> B: {Nb}kab
```