Exercise 4

Exercises Peer-to-Peer-Systems and Security (SS2011)

Monday 20.6 2011
Hand-in: Monday 4.7. 2010 in lecture or per mail
Exercise: 7.7. 2010

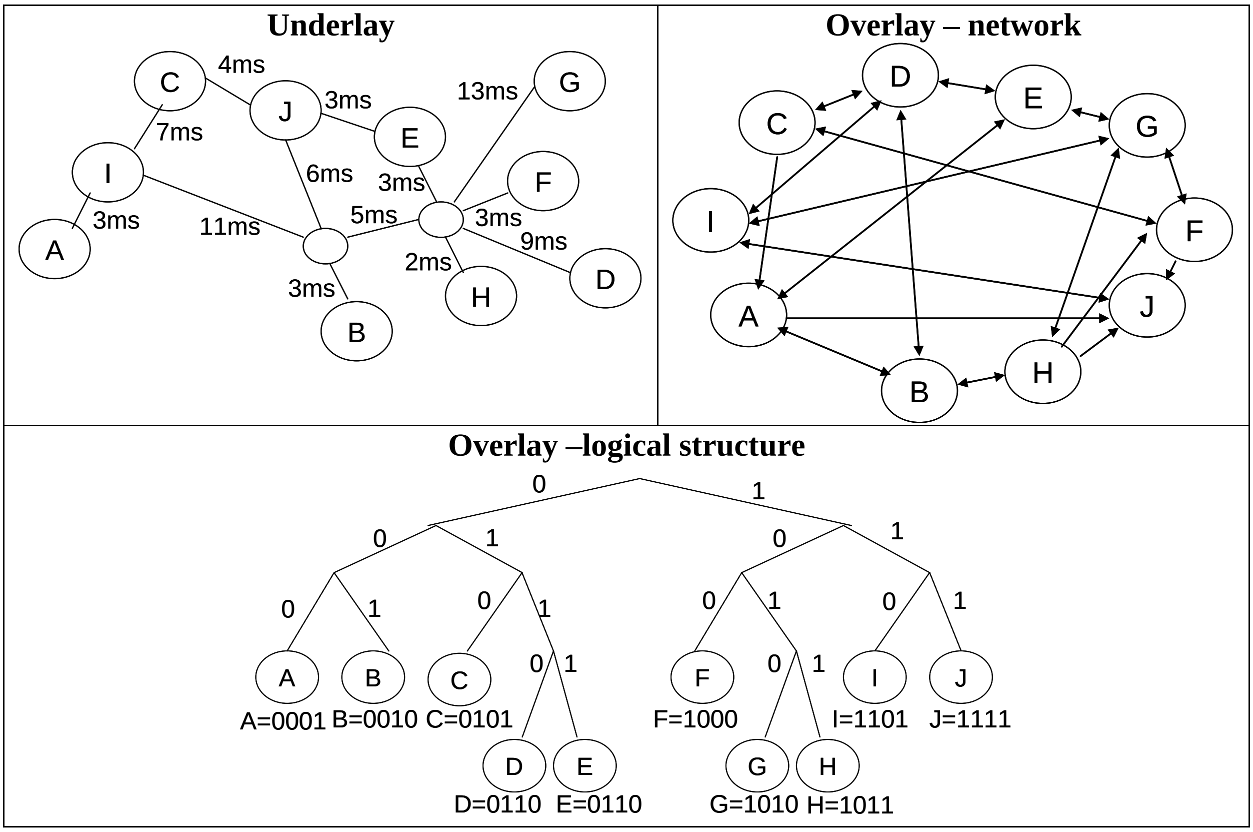
Dr. Heiko Niedermayer
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München

<u>Rules:</u> There will be five exercise sheets. You have to hand-in 70 % of the assignments, attend atleast 3 exercise courses and present a solution in the exercise course to get the 0.3 bonus.

Task 1 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.



a) What is the stretch (with respect to latency) for queries from F to A and from B to E?
b) 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 2 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 for Task 2:

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
```

Task 3 Authentication

Do the same as in task 2, yet with a different protocol. Hint: Use information from previous runs to attack the protocol. Sig_X stands for encryption with private key.

Protocol for Task 3:

Prerequisites: S is TTP and for each participant X S knows the corresponding public key PK_X. All participants know the public key PK_S of S.

Let kab = hash(Na,Nb).

Protocol:

```
A -> S: A, Enc_PK_S(Na, B)
S -> A: PK_B, Enc_PK_A(Sig_S(Na, A))
A -> B: Enc_PK_B(Na, A, B, Sig_S(Na, A))
B -> A: Nb, {Na}kab
A -> B: {Nb}kab
```

Task 4 Some questions

Answer the questions with knowledge from the lecture.

a) Cryptographic identities seem to make authentication a lot easier. Let assume, we use cryptographic identities. Do we still need a Certificate Authority? If yes, for what? If no, why not?

b) Why is trust important for key distribution?

c) Why does Zfone or SSH in the Baby Duck model not simply use a conventional authentication protocol like in SSL to authenticate the communication partners? What problem do they try to resolve?

Task 5 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.