Online Exam Distributed Algorithms

Vrije Universiteit Amsterdam, 27 May 2020, 8:30-12:00

By participating in this exam, I declare to understand that taking an online exam during this corona crisis is an emergency measure to prevent study delays as much as possible. I know that fraud control will be tightened and realize that a special appeal is being made to trust my integrity. With this statement, I promise to:

- make this exam completely on my own,
- not share my solutions with other students, and
- make myself available for any oral explanation of my answers.

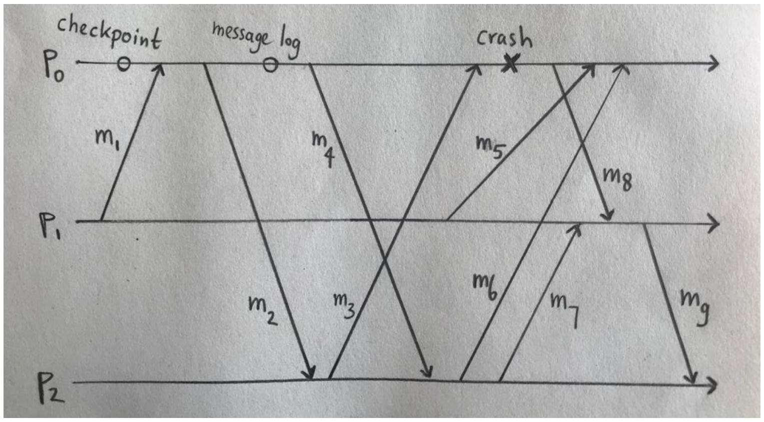
(The 7 exercises in this exam sum up to 90 points; each student gets 10 points bonus.)

1. Compute the vector clock values of the send and receive events and the decide event in an execution of the echo algorithm on an undirected ring of three processes, in which a spanning tree of depth 2 is constructed. (12 pts)

2. Consider the Merlin-Segall algorithm with topology changes. Suppose a new channel pq becomes operational. How can processes p and q together determine whether this channel is part of a shortest path toward the initiator, and how could they act if this is the case? (10 pts)

3. Explain where the proof of Theorem 12.1 in the textbook, that there is no (always correctly terminating) algorithm for 1-crash consensus, breaks down in the presence of an eventually weakly accurate failure detector. (16 pts)

4. The picture below shows the time line of events at three processes p_0, p_1, and p_2 with regard to some basic computation, where real time progresses from left to right.



Explain in detail how the three processes roll back to a consistent configuration in the past using the Peterson-Kearns algorithm. (12 pts)

5. In the time stamp ordering approach for transactions, suppose transaction T_1 wants to perform a write on a variable, but finds that another ongoing transaction T_2 that comes later in the serialization order read this same variable. Explain why it would be a bad idea, instead of aborting T_1 immediately, to let T_1 wait to see whether T_2 will maybe abort, in which case T_1 could still perform the write. (12 pts)

6. Sketch how the AODV protocol can be adopted to allow a peer to look for multiple minimum-hop paths to different destinations with the broadcast of a single RREQ message. (16 pts)

7. Consider the Merkle signature scheme.

   (a) Suppose an attacker manages to store the entire Merkle tree in memory. Explain why this does not seriously jeopardize the corresponding one-time signatures. (7 pts)

   (b) Why is it still not a good idea to publish the entire Merkle tree, relieving Alice from the duty to provide authentication values to Bob in her corresponding signatures? Give two reasons. (5 pts)