CS4211 Assignment

September 16, 2019

Notes

- This assignment is due before 9:59 PM, Friday, 1st November, 2019. No late submissions!
- Tool to be used: SPIN model checker `http://spinroot.com/spin/whatispin.html`
- This is an individual assignment. Acts of plagiarism are subjected to disciplinary action by the university. Please refer to `http://www.comp.nus.edu.sg/students/plagiarism/` for details on plagiarism and its associated penalties.
- *Submission Instructions*: (Failure to follow these instructions may result in deduction of marks)
  1. Create a folder named your matriculation number YourMatricNumber, e.g. U123456M. Create the following files in this folder (name these files exactly as instructed.):
     - **assignment1**: Create two folders inside it:
       - **Question 1:** Include your implemented spin source and the LTL property checker file(s) needed for Question 1.
       - **Question 2:** Include your implemented spin source and the LTL property checker file(s) needed for Question 2.
     - **report.pdf:**
       - For Question 1 (Part 2), explain the LTL property used.
       - For Question 1 (Part 3), describe the counter example you get from SPIN and explain how it can violate the property. Include the screenshot of the counter example (*e.g.* message sequence chart) in the report.
       - For Question 1 (Part 4), explain the deadlock free implementation with proof.
       - For Question 2 (Part 2), explain the sequence of events.
     - **readme.txt:** It should contain all information required for me to reproduce any verification runs you have done using SPIN.
  2. Zip (using WinZip) the entire YourMatricNumber folder (including the folder itself and all files in it) into a file YourMatricNumber.zip.
  3. Submit YourMatricNumber.zip to the Luminus Workbin Folder **Lab1**.

Question 1 [12 marks]

Problem Statement

A weather update controller consist of a weather control panel (WCP), a number of weather-aware clients, and a communication manager (CM) which controls the interactions between the WCP and all connected clients. Two standard behaviors of this system are as follows:

- Client Initialization

    1. A disconnected weather-aware client can establish a connection by sending a connecting request to the CM.
    2. If the CMs status is idle when the connecting request is received, it will set both its own status and the connecting clients status to pre-initializing, and disable the weather control panel so that no manual updates can be made by the user during the process of client initialization. Otherwise (CMs status is not idle), the CM will send a message to the client to refuse the connection, and the client remains disconnected.
    3. When the CM is pre-initializing, it will send a message to instruct the newly connected client to get the new weather information, and then set both its own status and the clients status to initializing.
    4. If the client reports success for getting the new weather, the CM will send another message to inform the client to use the weather information, and then set both its own status and the clients status to post-initializing. Otherwise, if getting new weather fails, the CM will disconnect the client and set its own status back to idle.
    5. If the client reports success for using the new weather, this initialization process is completed. the CM will set both its own status and the clients status to idle, and re-enable the WCP so that manual weather update is allowed again. Otherwise, if using new weather fails, the CM will disconnect the client, re-enable the WCP, and set its own status back to idle.

- Weather update
    1. User can manually update new weather information only when the WCP is enabled. By clicking the update button on the WCP, a update message is sent to the CM.
    2. When the CM is idle and receives update request from the WCP, it will set its own status and all the connected weather-aware clients status to pre-updating, and disable the WCP from any further updating requests before the completion of current update.
    3. When CMs status is pre-updating, it will send messages to instruct all connected clients to get the new weather information, and then set its own status and the clients status to updating.
    4. If all the clients report success for getting the new weather, the CM will send messages to inform the clients to use the new weather information, and then set its own status and the clients status to post-updating. Otherwise, if any of the connected clients reports failure for getting the new weather, the CM will send messages to all clients to use their old weather information, and then set its own status and the clients status to post-reverting.
    5. When CMs status is post-updating, if all the clients report success for using the new weather, the updating is completed. The CM will set its own status and the clients status to idle, and re-enable the WCP. Otherwise, if any of the connected clients reports failure for using the new weather, the CM will disconnect all connected clients, re-enable the WCP, and set its own status back to idle.
    6. When CMs status is post-reverting, if all the clients report success for using the old weather, the reverting is completed. The CM will set its own status and the clients status to idle, and re-enable the WCP. Otherwise, if any of the connected clients reports failure for using the old weather, the CM will disconnect all connected clients, re-enable the WCP, and set its own status back to idle.

Questions

Assuming the number of clients is **three** and initially the WCP is enabled for manual weather updating, the CM is at idle state and all the clients are disconnected

1. Write a Promela model for the above controller.
    - Correct implementation of client initialization **(3 marks)**
    - Correct implementation of weather update **(3 marks)**

2. The key property of this system is to be able to propogate the latest weather update to all connected clients via the communication manager. Define the key property in Linear-time temporal logic (LTL) **(1 mark)**
3. Show that there exists a deadlock and provide a clear interpretation of the counter-example obtained from SPIN. Any additional problems you find in the protocol will of course distinguish your answer and earn more credit**(3 marks)**
4. Implement a solution which makes the model deadlock free and provide proof for deadlock free property **(2 marks)**

Question 2 [8 marks]

Problem Description

A railway system consists of interconnected stations. Shuttles running on the railway bid for orders to transport passengers between certain stations. Successful completion of an order results in a cash payment for the shuttle involved. New orders are made known to all shuttles, thus all shuttles can make an offer. The shuttle with the best, i.e. lowest offer will receive the assignment.

- Railway network
  - The railway network consists of stations and tracks. Track can be traveled upon in one direction only (which is fixed). Two stations are connected bidirectionally, while there must only be one track between two stations in each direction. Furthermore, any number of shuttles can be present at a station at the same time.
  - A track can only be occupied by one shuttle at a time. Shuttles willing to travel along the occupied track have to wait until the track is free.
- Orders
  - Orders are made known to all shuttles by the management system. An order defines start and destination stations. Additionally, an order has a certain size, namely the number of people wishing to travel.
  - After all shuttles are informed of the new order, each shuttle must reply with either an offer or refuse message. The offer should include the desired charge the payment it will receive. The shuttle having made the lowest offer will receive the assignment. In the event of two equal offers, the assignment will go to the shuttle that first made the offer.
- Shuttles
  - Order processing is handled by the shuttles. Every shuttle can transport passengers up to its capacity. This means that a shuttle can transport more than one order at the same time, as long as the orders do not exceed the maximum capacity. The number of orders assigned but not necessarily loaded to a shuttle at any given time, is not limited.
  - To complete an order a shuttle has to travel to the start station, load the order and then proceed to the destination station to unload. Loading or unloading at other stations is not permitted.
  - A shuttle traveling on a track can neither change direction nor choose another destination.
  - When an order is received, a shuttle should make an offer only if (a) current loaded size plus the order size does not exceed the capacity, and (b) the start destination of the order is within two stations away from its current position (if it is on a track, its current position is its arriving station). Otherwise the shuttle should refuse to make an offer.

You may assume the following,

- There are six stations labeled from 1 to 6 connected as a ring
- Initially each shuttle should be in a station
- The charge it offers and the capacity can be fixed with respect to a shuttle

Questions

1. Write a Promela model for the above network.
   - Correct implementation of the management system **(3 marks)**
   - Correct implementation of the shuttle **(3 marks)**
2. Produce a sequence of events that leads the system into a state that all shuttle are at stations without load, given the following conditions: **(2 marks)**
   - There are three shuttles;
     - s_1 (capacity: 5 people; charge 2 dollars per person; initially at station 1)
     - s_2 (capacity: 8 people; charge 4 dollars per person; initially at station 1)
     - s_3 (capacity: 10 people; charge 3 dollars per person; initially at station 2)
   - Two orders are available sequentially before any action of shuttles:
     - The first order: 4 people from station 1 to 3
     - The second order: 1 people from station 2 to 3