

CS4211

Assignment 2

1 Notes

- This assignment is due before 9:59 PM, Monday, 19th November, 2018. No late submissions!
- We shall use the SPIN verification tool for this assignment.
- 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 folders/files in this folder (name these files exactly as instructed.):
 - **Weather:** This folder should contain the Promela model and all the LTL properties (i.e. *.pml and *.ltl files) you used to check your model. This folder should also include a short README file to describe the purpose of each LTL property.
 - **report.pdf:** Please include your particulars (name, matriculation number and NUS email address), assumptions you made in system modeling (if any). Clearly, describe the undesirable behaviour in the specification and the LTL property you used to verify your Promela model. Also give a clear interpretation of the counterexample obtained from 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 IVLE Workbin Folder **Lab2**.

2 Problem Description

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.

More details

- You can assume any fixed number of clients.
- Initially, the WCP is enabled for manually weather updating, the CM is at its idle status, and all the clients are disconnected.

3 Questions

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 propagate 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**)