Project 2018/19

Systems Verification Lab

MSc in Computer Science

University of Camerino

Prof. Luca Tesei

Description

Consider a lift system for a 3-floor building composed of different components. The objective of the project is to develop a model for the system and check that the requirements that are given are satisfied. The first model must be untimed and non-deterministic. Later, timing assumptions and probabilistic behaviours will be considered.

Model 1

The following is a first general description of the components and their requisites:

- for each floor there is a *button* to request service, which can be pressed. A pressed button stays pressed until it is reset by the controller. A button that is not pressed can become pressed non-deterministically;

- the *cabin* can be standing at any floor between 1 and 3 or it can have direction up or down;

- the cabin can receive one of the following commands: "stop", in which case it becomes standing, "up", in which case it takes direction up and "down", in which case it takes direction down;

- the cabin can take direction up only if the floor is not 3;

- the cabin can take direction down only if the floor is not 1;

- the cabin is equipped with a *door* that can be either open or closed;

- the door can receive either the "open" or the "close" command from the controller and it responds by opening or by closing;

- the *controller* takes in input (as sensory signals) the floor, the status and the direction of motion of the cabin, the status of the door, and the status of the four buttons. It decides the controls to the cabin, to the door and to the buttons;

- the controller must not reset a button that is not pressed;

- a button must be reset as soon as the cabin stops at the corresponding floor with the door open;

- no pressed button can be reset until the cabin stops at the corresponding floor and opens the door;

- the cabin can move only when the cabin is standing and the door is closed;

- if no button is pressed, the controller must issue no commands, the cabin must be standing and the door must be closed;

- the controller can issue a stop command only if the cabin is going up or down;
- the controller can issue an open command to the door only if the door is closed and the cabin is standing;
- the controller can issue a close command to the door only if the door is open;
- the controller adopts a first-in-first-out policy to serve the requests from the different floors;
- every time the door is open the cabin must be standing;
- a button cannot reach a state where it remains pressed forever;
- the door cannot remain closed forever;

Your tasks are:

1. Model the above scenario in SPIN.
2. Write all the requisites as LTL formulas and model check them with SPIN on the model.

Model 2

Consider all the features of Model 1 and add the following time assumptions:

- to travel from a floor to an adjacent one, in any direction, the elevator can take at least 40 seconds and at most one minute and 20 seconds;
- when the elevator arrives at a certain floor, its door automatically opens. This must not happen until at least 10 seconds from its arrival. However, the door must definitely open within 20 seconds;
- after the door closes, if the cabin is not standing, the elevator waits at least 10 seconds and then travels up or down to the other floor according to its direction;
- if the button at ground floor is pressed, in any situation the cabin will reach the ground floor and the door will be open (*) within at most 8 minutes;

Your tasks are:

1. Translate the Model 1 into an UPPAAL model by adding the timing assumptions.
2. Write all the new timed requisites as UPPAAL formulas and model check them.
3. Calculate the minimum time at which event (*) can happen using the UPPAAL facilities.
4. If the button at the middle floor is pressed, in any situation the cabin will reach the middle floor and the door will be open; calculate the minimum time at which this can happen using the UPPAAL facilities.

Model 3

Consider now only the cabin and focus on an aspect that has not been modelled in Model 1 and Model 2:

- a cabin can accommodate at most 4 passengers;
- when the cabin is at the ground floor, the door is open and no passenger is inside the cabin: with probability 0.3 no passenger enters the cabin and the door remains open, whilst with probability 0.7 one passenger enters the cabin and the door remains open;

- when the cabin is at the ground floor, the door is open and one passenger is inside the cabin: with probability 0.5 no more passengers enter the cabin and the door closes, whilst with probability 0.5 another passenger enters the cabin and the door remains open;
- when the cabin is at the ground floor, the door is open and two passengers are inside the cabin: with probability 0.7 no more passengers enter the cabin and the door closes, whilst with probability 0.3 another passenger enters the cabin and the door remains open;
- when the cabin is at the ground floor, the door is open and three passengers are inside the cabin: with probability 0.9 no more passengers enter the cabin and the door closes, whilst with probability 0.1 another passenger enters the cabin and the door remains open;
- when the cabin is at the ground floor, the door is open and four passengers are inside the cabin: with probability 0.7 no more passengers enter the cabin and the door closes, whilst with probability 0.3 one passenger exits the cabin and the door remains open;

Your tasks are:

1. Model in PRISM the described process of passenger entering (not the whole elevator scenario!) as a Discrete Time Markov Chain.
2. Calculate, using PRISM:
    - the probability or reaching a configuration in which the number of passengers is greater than or equal to 0, 1, 2, 3 and 4;
    - the probability or reaching a configuration in which the door is closed;
    - the probability or reaching a configuration in which the door is closed within 0, 1, 2, ... 12 time steps (hint: make an experiment and plot the results by using the PRISM experiment facilities);
    - the expected number of time steps to reach a configuration in which the door is closed;
    - the expected number of passengers when a configuration in which the door is closed is reached (hint: define a suitable reward structure);
    - the long-run probability of states in which the door is closed and the number of passengers is less than or equal to 2.

Submission

Prepare a written report describing your model of the scenario and how you expressed the properties. You can use screenshots to show some of the results.

Students must create a folder in Google Drive, using the Google account associated to their email name.surname@studenti.unicam.it

The folder must contain all the SPIN, UPPAAL and PRISM files and a pdf report, written in English, which describes all the phases of the developing of the project. The use of screenshots is encouraged to show, within the report, the runs and the results of the project. The folder must be named:

SVL1819-Project-APP-X-Surname-Name

where X is the number of the exam session (Appello) as specified for each date of the written test above.

The folder must be shared (using Google Drive facilities) with luca.tesei@unicam.it and francesco.tiezzi@unicam.it by 11.59pm of the day specified for the Partial Exam SVL1819 Sess. X - Project Deliver relative to Session X. Students should also register for this Partial Exam within the day before on ESSE3.

Exam Results

The exam consists of a written test, containing open-answer questions (exercises), together with this Project. The Written Test and the Project are two independent Partial Exams (see the exam sessions in the ESSE3 career system) and can be passed in different exam sessions. The final grade, which is the average of the grades of the two Partial Exams, can be obtained and registered only if both the Partial Exams have been passed with a grade of at least 18/30.

The results of the evaluation of the Project will be communicated through the course wiki site or by email (depending on the number of students). Contextually to the communication of the results, students will be invited to accept or reject the evaluation.

A positive evaluation ($\geq$18/30) of each Partial Exam (Written Test and Project) remains valid for one year or until the student retries the Partial Exam. If both grades (Written Test and Project) are accepted, the final grade will be registered in ESSE3.