Internship: Uniform sampling of timed patterns for cyber-physical systems test generation

Advisors: Nicolas Basset and Thao Dang

CNRS/VERIMAG, Grenoble, France.
{bassetni,thao.dang}@univ-grenoble-alpes.fr

Validation techniques for cyber-physical systems are essential for ensuring correct operations of safety-critical applications. Current validation techniques for these systems are costly if high confidence in the results is expected and can still fail to identify all of the significant system behavioural patterns, which can have a detrimental effect on safety and performance. When no bug is revealed, as the behaviours were not explored exhaustively, this does not mean the absence of bugs. Instead a test coverage measure or a probability of error can be given to the designer to evaluate the confidence that the system is free of bugs.

In cyber-physical system models, input signals can represent either uncontrollable disturbances from the external environment in which the system operates, or some control signals that are fed to the system. In the latter case, the signals controlled often satisfy some properties or preconditions. In the former case, input signals must also belong to a class of functions describing realistic disturbances or meaningful input stimuli. The properties we are interested in this project are expressed using STL (Signal Temporal Logic) or timed automata, formalisms useful for describing real-time constraints or temporal patterns of behaviours. Exhaustive exploration of all possible behaviours is infeasible in practice. The test-based approach we will adopt, will make use of random sampling and will provide statistical guarantees of the results.

The goal of the project is to apply recent results on uniform random generation of behaviours of timed automata [1] to test generation for cyber-physical systems [2]. In particular, we focus on the problem of generating signals satisfying an STL formula with a good coverage. The concrete objective of this internship is to design algorithms to solve this problem and possibly implement them based on the existing tool-chain described in [1] and available online at `http://www.prismmodelchecker.org/files/qest16/`.

Related course at MPRI and suitable skills: It is suitable but not necessary to have followed some of the following courses.

- Course 2.8.2: *Foundations of real time and hybrid systems* (The main related course to the project);
- Course 2.9.2: *Algorithmic verification of programs*;
- Course 1.24: *Probabilistic Aspects of Computer Science*;
- Course 1.22: *Basics of verification*.

Programming skills and knowledge of probability theory are welcome.

References

1. B. Barbot, N. Basset, M. Beunardeau and M. Kwiatkowska. Uniform Sampling for Timed Automata with Application to Language Inclusion Measurement. Proceedings QEST'16.
2. Arvind S. Adimoolam, Thao Dang, Alexandre Donzé, James Kapinski, Xiaoqing Jin. Classification and Coverage-Based Falsification for Embedded Control Systems. CAV 2017, pages 483-503, Springer.