Internship Proposal (M2): Sensitivity Analysis in Timed Automata

Place: Inria - Irisa, Rennes – SUMO team (http://www.irisa.fr/sumo/)

Timed systems refer to computer systems in which timing information plays a crucial role. The correctness of such system rely not only on functional correctness (i.e. computing the right value), but also on extra-functional properties such as response time and worst-case execution time. Embedded systems, such as controllers found in cars, are examples of timed systems. Several methods exist for modeling and verifying different aspects of such systems [1].

One difficulty that arises with timed systems is that they can lack predictability; for instance, task execution times can vary due to different factors including imprecise clocks and unexpected resource usage. *Sensitivity analysis* addresses this issue [3]: given a *nominal* model that captures the behaviors of the system in an idealistic setting, one analyzes the behaviors of the system when its parameters are subject to perturbations. In this internship, we concentrate on perturbations on timing constraints in systems modeled by timed automata [2]. Given a timed automaton that models the nominal behaviors, we consider the executions of the model where each duration is subject to random noise. Given a specification expressed in a timed logic [5] or using timed automata [2], we would like to quantify the sensitivity of the system. Some starting questions for which we will seek answers are the following.

1. Given n and $\epsilon > 0$, what is the probability of the perturbed executions to have a distance of more than ϵ to the nominal behaviors, in n steps?
2. Given a specification satisfied by the nominal model, what is the probability of still satisfying the specification under perturbations, after n steps? How does this probability evolve asymptotically?

As a continuation to the above questions, we will also be interested in the controller synthesis problem with the additional objective of minimizing sensitivity. Assuming that an objective is given, say, in temporal logic, what is the sequence of actions to be taken by a controller so as to 1) satisfy the objective, and 2) minimize the sensitivity? The general goal is to develop quantitative extensions of robustness algorithms studied *e.g.* in [6, 4].

If time permits, and depending on the intern's interests, a simple example application can be developed to test the above ideas. We suggest studying simple communication protocols on infrared remote controllers which are often imprecise in their timings, and checking whether the protocol can be accelerated given a fixed finite set of messages to be sent, while still ensuring that the messages are decoded correctly thanks to the computed guarantees against perturbations.

Keywords: timed automata, sensitivity analysis, model checking, probabilistic systems
Related courses (Rennes): Parcours 1, Techniques de Vérification Avancées

Contact: Ocan Sankur (osankur@ulb.ac.be) – `http://www.ulb.ac.be/di/verif/sankur`

References

[1] R. Alur, K.-E. Arzen, J. Baillieul, T. Henzinger, D. Hristu-Varsakelis, and W. S. Levine. *Handbook of networked and embedded control systems*. Springer Science & Business Media, 2007.

[2] R. Alur and D. L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183 – 235, 1994.

[3] C. G. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[4] Y. Oualhadj, P.-A. Reynier, and O. Sankur. Probabilistic robust timed games. In *CONCUR'14*, volume 8704 of *LNCS*, pages 203–217. Springer, 2014.

[5] J.-F. Raskin and P.-Y. Schobbens. The logic of event clocks: Decidability, complexity and expressiveness. *Automatica*, 34(3):247–282, Mar. 1998.

[6] O. Sankur. Symbolic quantitative robustness analysis of timed automata. In C. Baier and C. Tinelli, editors, *TACAS'15*, volume 9035 of *LNCS*, pages 484–498. Springer, 2015.