M2 Research Internship

Distributed verification of real-time systems

Supervisors: Étienne ANDRÉ and Laure PETRUCCI
Email: {first.last}@lipn.univ-paris13.fr
Laboratory: LIPN, CNRS UMR 7030, Université Paris 13, Sorbonne Paris Cité

Context

Real-time systems have become ubiquitous in the past few years. Some of them (automated plane and unmanned systems control, banking systems, etc.) are critical in the sense that no error must occur. Testing these systems can possibly detect the presence of bugs, but not guarantee their absence. It is necessary to use formal methods such as model checking [BK08] so as to prove formally the correctness of a system.

Real-time systems are characterized by a set of timing constants, such as the reading period of a sensor on an unmanned aircraft system, the traversal time of a circuit by the electric current, or the delay before retransmitting data in a cellphone. Although numerous techniques to verify a system for *one* set of constants exist, formally verifying the system for numerous values of these constants can require a very long time, or even infinite if one aims at verifying dense sets of values.

It is therefore interesting to reason in a parametric manner, by considering that these constants are unknown, i.e., parameters, and synthesize a constraint on these parameters guaranteeing the system correctness. A method, the *inverse method* [AS13, APP13], has been proposed for both timed automata [AHV93] and time Petri nets [JK09, TLR09], two formalisms widely used. Starting from a reference valuation of the parameters corresponding to a correct behavior, this method synthesizes a constraint on the parameters guaranteeing the same correct behavior. As a consequence, this guarantees that the system will be correct for any parameter valuation satisfying this constraint.

Internship subject

In order to take advantage of the multi-core processors and clusters, the verification algorithm shall be redefined to be adapted to the distributed case. The goal is, for a processor with n cores, that the improved algorithm be (almost) n times faster than on a mono-core processor – and similarly for clusters. It may be interesting to base on a modular approach proposed for timed Petri nets. An implementation will also be performed by the intern, so as to validate the proposed approach.

An implementation will also be performed by the intern, so as to validate the proposed approach. An option is to reuse the IMITATOR software tool [AFKS12].

Keywords

Formal methods, model checking, distributed algorithmic, real-time systems, parameter synthesis

Skills

The following skills are not compulsory, but would be welcome: distributed calculus, timed automata, OCaml.

Conditions

Highly motivated applicants are being sought. The internship will take place at LIPN (Laboratoire d'Informatique de Paris Nord) in the Université de Paris 13, Sorbonne Paris Cité (campus of Villetaneuse).

Standard remuneration.

Depending on the candidate's motivation and wishes, this internship can lead to a PhD thesis.

References

[AFKS12] Étienne André, Laurent Fribourg, Ulrich Kühne, and Romain Soulat. IMITATOR 2.5: A tool for analyzing robustness in scheduling problems. In Dimitra Giannakopoulou and Dominique Méry, editors, *Proceedings of the 18th International Symposium on Formal Methods (FM'12)*, volume 7436 of *Lecture Notes in Computer Science*, pages 33–36. Springer, August 2012.

[AHV93] Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. Parametric real-time reasoning. In *Proceedings of the twenty-fifth annual ACM symposium on Theory of computing*, STOC'93, pages 592–601, New York, NY, USA, 1993. ACM.

[APP13] Étienne André, Laure Petrucci, and Giuseppe Pellegrino. Precise robustness analysis of time Petri nets with inhibitor arcs. In Víctor Braberman and Laurent Fribourg, editors, *11th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'13)*, volume 8053 of *Lecture Notes in Computer Science*, pages 1–15. Springer, August 2013.

[AS13] Étienne André and Romain Soulat. *The Inverse Method*. FOCUS Series in Computer Engineering and Information Technology. ISTE Ltd and John Wiley & Sons Inc., 2013. 176 pages.

[BK08] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT Press, 2008.

[JK09] Kurt Jensen and Lars Michael Kristensen. *Coloured Petri Nets – Modelling and Validation of Concurrent Systems*. Springer, 2009.

[TLR09] Louis-Marie Traonouez, Didier Lime, and Olivier H. Roux. Parametric model-checking of stopwatch Petri nets. *Journal of Universal Computer Science*, 15(17):3273–3304, 2009.