Laboratoire des Sciences du Numérique de Nantes

Internship Proposal

Bounded model checking for energy-aware real-time systems

Supervisors: Gaëtan Staquet
Étienne André
Email: first.last(at)ls2n(dot)fr
Laboratory: LS2N, Nantes Université, France
Team: STR (systèmes temps-réel)

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 thus necessary to use formal methods such as model checking [BK08] so as to prove formally the correctness of such a system.

Formal verification provides mathematically rigorous guarantees that system behaviors satisfy desired safety and correctness properties, which is crucial for detecting subtle errors that testing alone may miss. Often, critical systems feature key continuous variables, such as time, but also energy. Timed automata [AD94] extend classical automata with clocks, enabling precise modeling of real-time constraints, while weighted or energy timed automata [Bac+21] further incorporate quantitative resources such as energy consumption or production, making them well-suited for analyzing energy-critical systems.

Subject

In the context of verification of timed systems, **bounded model checking** [Sor02; KJN12; WZZ17] is valuable because it efficiently explores behaviors within a finite horizon, allowing rapid detection of counterexamples and scalable analysis of complex, resource-constrained models. Even better, bounded model checking can be applied to classes of systems where infinite-horizon analyses are usually undecidable [KP12].

The objective of this internship is to **design algorithms for bounded model checking of timed automata extended with energy variables**, allowing answer to questions such as "given an autonomous vehicle equipped with both a chargeable battery and a solar panel, what is the minimal energy needed to perform a certain itinerary in less than k steps?" Or to answer security-related questions such as: "by looking at the final percentage of charge of the battery of an autonomous

Gaëtan Staquet and Étienne André
CNRS • LS2N • École Centrale Nantes, bâtiment S
1 rue de la Noë, 44 300 Nantes, France

Nantes Université · Centrale Nantes · cnrs

vehicle, can an attacker infer secret information (such as the maximum speed, or geographic information) over the vehicle in the past k steps?"

The analyses will be carried for both well-established timed automata [AD94] and the recent formalism of automata with timers [Bru+23]. Depending on the time and interest of the applicant, an implementation may be carried out using solvers.

Keywords

Formal methods, model checking, real-time systems, energy-aware systems

Skills

The following skills are not compulsory, but would be welcome:

- formal methods;
- timed automata;
- SMT/SAT solvers.

Application

In case of application (or questions), please send us a CV by email, together with an explanation of your motivation, and the adequacy between your curriculum and the proposed subject.

Location and environment

Highly motivated applicants are being sought. The internship will take place at **École Centrale Nantes**, within Nantes Université. LS2N is an internationally recognized research laboratory comprising over 450 scientists.

Nantes combines a lively, student-friendly atmosphere with a rich scientific and cultural scene, making it a great place to learn, research, and enjoy everyday life.

References

[AD94] Rajeev Alur and David L. Dill. "A theory of timed automata". In: *Theoretical Computer Science* 126.2 (Apr. 1994), pp. 183–235. DOI: 10.1016/0304-3975(94)90010-8.

Gaëtan Staquet and Étienne André
CNRS • LS2N • École Centrale Nantes, bâtiment S
1 rue de la Noë, 44 300 Nantes, France

[Bac+21] Giovanni Bacci, Patricia Bouyer, Uli Fahrenberg, Kim Guldstrand Larsen, Nicolas Markey, and Pierre-Alain Reynier. "Optimal and robust controller synthesis using energy timed automata with uncertainty". In: *Formal Aspects of Computing* 33.1 (2021), pp. 3–25. DOI: 10.1007/s00165-020-00521-4.

[BK08] Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking*. MIT Press, 2008. ISBN: 978-0-262-02649-9.

[Bru+23] Véronique Bruyère, Guillermo A. Pérez, Gaëtan Staquet, and Frits W. Vaandrager. "Automata with Timers". In: *FORMATS* (Sept. 19–21, 2023). Ed. by Laure Petrucci and Jeremy Sproston. Vol. 14138. Lecture Notes in Computer Science. Antwerp, Belgium: Springer, 2023, pp. 33–49. DOI: 10.1007/978-3-031-42626-1_3.

[KJN12] Roland Kindermann, Tommi A. Junttila, and Ilkka Niemelä. "Beyond Lassos: Complete SMT-Based Bounded Model Checking for Timed Automata". In: *FMOODS-FORTE* (June 13–16, 2012). Ed. by Holger Giese and Grigore Rosu. Vol. 7273. Lecture Notes in Computer Science. Stockholm, Sweden: Springer, 2012, pp. 84–100. DOI: 10.1007/978-3-642-30793-5_6.

[KP12] Michał Knapik and Wojciech Penczek. "Bounded Model Checking for Parametric Timed Automata". In: *Transactions on Petri Nets and Other Models of Concurrency*. Lecture Notes in Computer Science 6900 (2012). Ed. by Kurt Jensen, Susanna Donatelli, and Jetty Kleijn, pp. 141–159. DOI: 10.1007/978-3-642-29072-5_6.

[Sor02] Maria Sorea. "Bounded Model Checking for Timed Automata". In: *MTCS* (Aug. 24, 2002). Ed. by Walter Vogler and Kim Larsen. Vol. 68. Electronic Notes in Theoretical Computer Science 5. Brno, Czech Republic: Elsevier, 2002, pp. 116–134. DOI: 10.1016/S1571-0661(04)80523-1.

[WZZ17] Bozena Wozna-Szczesniak, Agnieszka M. Zbrzezny, and Andrzej Zbrzezny. "SMT-based Searching for k-quasi-optimal Runs in Weighted Timed Automata". In: *Fundamenta Informaticae* 152.4 (2017), pp. 411–433. DOI: 10.3233/FI-2017-1527.

Gaëtan Staquet and Étienne André
CNRS • LS2N • École Centrale Nantes, bâtiment S
1 rue de la Noë, 44 300 Nantes, France