PhD thesis proposal

Efficient lightweight verification of cyberphysical systems

Supervisors: Étienne André[1,2] and Laure Petrucci[1] (both full professor)
Email: `firstname.lastname@univ-paris13.fr`
Laboratory: [1]LIPN, CNRS UMR 7030, Université Sorbonne Paris Nord
[2]Institut Universitaire de France (IUF)
Team: SAFER

Context

Cyber-physical systems are ubiquitous in our society (automated subways, smartphones, medical devices, etc.). These systems must avoid any unforeseen errors (bugs) that could threaten lives, and a formal verification as exhaustive as possible is highly desired.

For cyber-physical systems for which full formal verification is not feasible (due to state space combinatorial explosion, or for black-box systems for which no model is available, e.g., for confidentiality reasons, or for systems based on unreliable AI), applying lightweight verification techniques, such as *monitoring*, is a highly interesting option.

Subject

A key challenge in monitoring is to formalize complex requests involving *quantities* such as "the vehicle always remains at a minimum distance from other vehicles, with energy consumption maintained below a predefined threshold (where this threshold is not necessarily known a priori with full precision), except in the event of exceptional danger at most one minute per hour"; and then to detect possible violations of these requests on huge quantities of data.

Directions of research for the thesis include:

- propose new formalisms to support offline and online monitoring of quantitative logs against quantitative (and potentially parametric) properties;
- design monitoring algorithms, and propose efficient data structures;
- implement these algorithms (potentially reusing the IMITATOR [And21] engine) and evaluate them against benchmarks.

Keywords

Monitoring, formal methods, model checking, timed systems, parametric systems

Conditions

Highly motivated applicants are being sought. The thesis will take place at LIPN (Laboratoire d'Informatique de Paris Nord) within Université Sorbonne Paris Nord. LIPN is an internationally recognized research laboratory comprising over 150 scientists.

References

[And21] Étienne André. "IMITATOR 3: Synthesis of timing parameters beyond decidability". In: *CAV* (July 18–23, 2021). Ed. by Rustan Leino and Alexandra Silva. Vol. 12759. Lecture Notes in Computer Science. virtual: Springer, 2021, pp. 1–14. DOI: 10.1007/978-3-030-81685-8_26.

[Bar+18] Ezio Bartocci, Jyotirmoy V. Deshmukh, Alexandre Donzé, Georgios E. Fainekos, Oded Maler, Dejan Ničković, and Sriram Sankaranarayanan. "Specification-Based Monitoring of Cyber-Physical Systems: A Survey on Theory, Tools and Applications". In: *Lectures on Runtime Verification – Introductory and Advanced Topics*. Ed. by Ezio Bartocci and Yliès Falcone. Vol. 10457. Lecture Notes in Computer Science. Springer, 2018, pp. 135–175. DOI: 10.1007/978-3-319-75632-5_5.

[Fin+19] Bernd Finkbeiner, Christopher Hahn, Marvin Stenger, and Leander Tentrup. "Monitoring hyperproperties". In: *Formal Methods in System Design* 54.3 (2019), pp. 336–363. DOI: 10.1007/S10703-019-00334-Z.

[QD20] Xin Qin and Jyotirmoy V. Deshmukh. "Clairvoyant Monitoring for Signal Temporal Logic". In: *FORMATS* (Sept. 1–3, 2020). Ed. by Nathalie Bertrand and Nils Jansen. Vol. 12288. Lecture Notes in Computer Science. Vienna, Austria: Springer, 2020, pp. 178–195. DOI: 10.1007/978-3-030-57628-8_11.

[WAH19] Masaki Waga, Étienne André, and Ichiro Hasuo. "Symbolic Monitoring against Specifications Parametric in Time and Data". In: *CAV, Part I* (July 15–18, 2019). Ed. by Işil Dillig and Serdar Tasiran. Vol. 11561. Lecture Notes in Computer Science. New York City, USA: Springer, 2019, pp. 520–539. DOI: 10.1007/978-3-030-25540-4_30.

[WAH22] Masaki Waga, Étienne André, and Ichiro Hasuo. "Model-Bounded Monitoring of Hybrid Systems". In: *ACM Transactions on Cyber-Physical Systems* 6.4 (Nov. 2022), 30:1–30:26. DOI: 10.1145/3529095.

Version: December 11, 2024

LIPN • Institut Galilée • Université Sorbonne Paris Nord • 93 430 Villetaneuse, France
Etienne.Andre@univ-paris13.fr
https://lipn.univ-paris13.fr/~andre/