Internship offer

Synthesis of Parameters for the Analysis of Opacity Properties

Supervisor Dylan Marinho

Laboratory LIP6, CNRS UMR 7606, Sorbonne Université

Team MoVe (Modeling and Verification)

Keywords formal methods · parametric systems · model checking · temporal logics · timed automata

1. Context

Real-time systems are used in a wide range of applications, such as transport, telecommunications, and industry. These systems must follow restrictive specifications, and formal verification that is as exhaustive as possible is highly desired.

We are interested in the verification of security properties, demonstrating that the system will be resistant to certain attacks. More precisely, we focus on timing leaks, which occur when an attacker is able to infer private behavior based on timing information.

2. Subject

To detect such leaks, we focus on a specific security property, called opacity.

In previous works, we consider that the attacker has access (only) to the system execution time and wonder if they can deduce some secret information from it. We therefore define execution-time opacity (ET-opacity) in [1] and some extensions in [2] and [3] ([4] presents a more recent overview of these works).

These properties are defined over parametric timed automata (PTAs) [5], which are an extension of timed automata (TAs) [6] with parameters. Parameters are unknown constants that can be used in guards and invariants of a TA. We can then synthesize the values of these parameters for which the system verifies a certain property (*e.g.* the ET-opacity synthesis problem asks to synthesize the parameters that ensure ET-opacity).

The goal of this internship is to study the synthesis of parameters for ET-opacity problems and their extensions. Some decidability results are already known, but not for all variants of the problem, and we do not yet have implemented algorithms for the synthesis of parameters.

The two main objectives of the internship are:

- Study the decidability of remaining open problems (*e.g.* the synthesis of expiration dates in the setting of [3]);
- Implement algorithms for the synthesis of parameters ensuring (variants of) ET-opacity.

3. Skills

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

- model checking
- temporal logics
- (parametric) timed automata
- programming (Java, for example; OCaml is welcome)

4. Conditions

The internship will take place at LIP6, within Sorbonne Université in Paris. The LIP6 is a joint research unit (UMR 7606) of Sorbonne University (SU) and the National Centre for Scientific Research (CNRS). It is a computer science research laboratory with approximately 450 members, including over 170 permanent researchers.

The internship can start at any time from now and includes the standard internship stipend. The duration can be discussed.

Application: by email first.

References

[1] É. André, D. Lime, D. Marinho, and S. Jun, "Guaranteeing timed opacity using parametric timed model checking," *ACM Transactions on Software Engineering and Methodology*, vol. 31, no. 4, pp. 1–36, 2022, doi: 10.1145/3502851.

[2] É. André, S. Bolat, E. Lefaucheux, and D. Marinho, "strategFTO: Untimed control for timed opacity," in *FTSCS 2022*, C. Artho and P. C. Ölveczky, Eds., Auckland, New Zealand: ACM, 2022, pp. 27–33. doi: 10.1145/3563822.3568013.

[3] É. André, E. Lefaucheux, and D. Marinho, "Expiring opacity problems in parametric timed automata," in *ICECCS 2023*, Y. Ait-Ameur and F. Khendek, Eds., Toulouse, France: Springer, 2023, pp. 451–469. doi: 10.1109/ICECCS59891.2023.00020.

[4] É. André, E. Lefaucheux, D. Lime, D. Marinho, and S. Jun, "Configuring Timing Parameters to Ensure Execution-Time Opacity in Timed Automata," in *TiCSA@ETAPS 2023*, M. H. ter Beek and C. Dubslaff, Eds., in EPTCS. Paris, France, 2023, pp. 1–26. doi: 10.4204/EPTCS.392.1.

[5] R. Alur, T. A. Henzinger, and M. Y. Vardi, "Parametric real-time reasoning," in *STOC*, S. R. Kosaraju, D. S. Johnson, and A. Aggarwal, Eds., San Diego, California, United States: ACM, 1993, pp. 592–601. doi: 10.1145/167088.167242.

[6] R. Alur and D. L. Dill, "A theory of timed automata," *TCS*, vol. 126, no. 2, pp. 183–235, Apr. 1994, doi: 10.1016/0304-3975(94)90010-8.

Sorbonne Université
CNRS · LIP6
4 place Jussieu · 75005 Paris
Dylan.Marinho@sorbonne-universite.fr
perso.lip6.fr/Dylan-Marinho