Title: Bounded model checker for threshold automata with delays

Topic: Computer science – formal verification
City: Nancy, France
Team: Veridis, Inria Nancy – Grand Est

Advisors: Igor Konnov (igor.konnov@inria.fr), Stephan Merz (stephan.merz@inria.fr)

Context of the topic

The internship topic concerns the parameterized verification of fault-tolerant distributed algorithms such as distributed consensus, agreement, and fault-tolerant clock synchronization. In such algorithms, the participants communicate by exchanging messages, in order to arrive at a common decision. The problem is aggravated by the presence of faults: some participants may crash and some may exhibit Byzantine behaviors such as lie about their state. As fault-tolerant algorithms are notoriously difficult to design right, one needs verification tools that check whether a fault-tolerant distributed algorithm is indeed robust to faults.

Objectives of the internship

The authors of [1, 2] modelled fault-tolerant distributed algorithms with threshold automata. They have shown that one can verify safety of parameterized systems of threshold automata by constructing queries to an SMT solver. This result was achieved under the assumption of asynchronous reliable communication, that is, every message is guaranteed to be delivered, although there is no upper bound on the delivery time. This model is known to be too permissive: It is impossible to solve consensus under the assumptions of pure asynchrony [3]. To circumvent this problem, many fault-tolerant distributed algorithms work under timing assumptions: every message is delivered in a time interval [min_delta, max_delta], where min_delta and max_delta are predefined constants. One can model such algorithms by using threshold automata with delays.

Recently, it was found that accelerated systems of threshold automata with time constraints have bounded diameters [4], similar to the accelerated systems of ordinary (non-timed) threshold automata. Hence, in this internship work, we propose to extend the verification approach of [2] to threshold automata with delays. This work requires: (1) fundamental contributions on how to extend the SMT schemas to schemas with delays, (2) an extension of the existing Byzantine model checker to support verification of threshold automata with delays.

References

[1] Igor Konnov, Helmut Veith, Josef Widder. SMT and POR Beat Counter Abstraction: Parameterized Model Checking of Threshold-Based Distributed Algorithms. CAV (1) 2015: 85-102

[2] Igor Konnov, Marijana Lazic, Helmut Veith, Josef Widder. Para2: parameterized path reduction, acceleration, and SMT for reachability in threshold-guarded distributed algorithms. Formal Methods in System Design 51(2): 270-307 (2017)

[3] Michael J. Fischer, Nancy A. Lynch, Mike Paterson. Impossibility of Distributed Consensus with One Faulty Process. J. ACM 32(2): 374-382 (1985)

[4] Axel Palaude. Short counterexample property for threshold automata with time constraints. Internship report. ENS Rennes, 2018.

[5] Igor Konnov, Josef Widder. ByMC: Byzantine Model Checker. Accepted to ISoLA 2018.

Prerequisites

Candidates should be interested in formal techniques for modeling and verifying (distributed) algorithms. Knowledge of timed automata and SMT solving is a plus, but is not required. The Byzantine model checker [2] is written in OCaml, and basic knowledge of OCaml is necessary.