Automating Timed Automata Design

Reporting

Project Information

AutoTADes

Grant agreement ID: 798482

Project website

DOI
10.3030/798482

Project closed

EC signature date
11 July 2018

Start date
1 August 2018

End date
31 July 2020

Funded under
EXCELLENT SCIENCE - Marie Skłodowska-Curie Actions

Total cost
€ 157 845,60

EU contribution
€ 157 845,60

Coordinated by
MIDDLE EAST TECHNICAL UNIVERSITY
Türkiye

Periodic Reporting for period 1 - AutoTADes (Automating Timed Automata Design)

Reporting period: 2018-08-01 to 2020-07-31

Summary of the context and overall objectives of the project

Cyber-physical systems (CPSs) are everywhere, from autonomous vehicles to medical devices to smart buildings. Designing such CPSs that achieve complex tasks is a tedious and error prone process. During the design, high-level specifications describing desired functionalities, safety measures, physical properties and restrictions, and optimality criteria have to be considered.

Furthermore, as people's life may depend on CPSs, their correctness is of critical importance. In CPS theory, the system correctness is guaranteed via automated verification of formal models, such as timed automata (TA), a central modelling formalism for cyber-physical systems.

Verification tools allow for verifying correctness of TA from specifications expressed in rich formal languages, and have been proven to be practically applicable on industrial case studies. Unfortunately, designing a complete TA model that can be fed into a verifier for the system under study is a very challenging process. In addition, if the system does not meet its specification, it is again very hard to make the right modifications on the TA to meet the specification.

The overall research objective of this MSCA-IF project is to automate the design of timed automata. This objective is broken down to five research objectives, and the design automation problem is studied from different perspectives: a) the development of a framework to automate construction of template models from descriptions given in natural language, b) the identification of a class of parametric TA and specifications for which a solution to synthesis of controllers and parameters exists, c) the development of an algorithm to solve the synthesis problem for the class identified in (b), d) optimizing the synthesized parameters and strategy and e) the extension of the developed methods for a larger class of systems and specifications.

Work performed from the beginning of the project to the end of the period covered by the report and main results achieved so far

In this project, automating timed automata design process is studied from different perspectives that are aligned with the project objectives.

We developed a new method for construction of TA models and generation of specification formula from descriptions given in structured natural language (WP1). The method is implemented as a tool named ATAC. The tool, its manual, and a white paper explaining the theory behind it are available on the project web-page.

For control synthesis for parametric timed automaton (PTA) problem, we showed that the undecidability results on the parameter synthesis problem applies to this problem (WP2). For this reason, we formulated the synthesis problem for PTA restricted to bounded integer parameters under reachability specifications for deterministic systems (WP2), and developed an efficient synthesis algorithm using iterative feasibility analysis (WP3). We extended the algorithm to synthesize optimal control strategy and parameter valuation pair (WP4). We also extended it for non-deterministic systems under unavoidability specifications (guaranteed reachability for non-determinism) (WP3-4).

We studied the synthesis problem for safety specifications for a special type of timed automata embedding the controller synthesis into the parameter synthesis problem. We designed a parametric TA of this type modelling an adaptive cruise control system (ACC), and presented efficient synthesis methods using the monotonicity properties of this model (WP3-4-5).

The controller and parameter synthesis methods intend to assist the design when a partial model is developed. On the other hand, in general, a designer makes some design choices regarding the uncertainties to produce a complete model. This model needs to be updated if it does not satisfy its specification. At this end, we studied tuning constraints of a TA for reachability, data-driven controller synthesis for safety, and finally, data-driven system repair for safety (WP3-4-5). Each of these problems is closely related to the control of parametric timed automata problem since each of them can be cast as this problem by parametrizing the considered TA. For reachability, we developed a method to find a minimal amount of change in the timing constraints(in collaboration with Prof. Cerna, initiated during the secondment). In data-driven system repair approach, we find the causes of undesired events as a temporal logic formula from system traces, and repair the system in an automated way to avoid the satisfaction of the formula. In data-driven controller synthesis, we synthesize controllable formulas that explain events leading to desired behavior and synthesize controllers from such formulas.

Finally, we developed a novel clock reduction method that reduces the number of clocks while preserving semantics and design choices to reduce the computational complexity.

At the end of the project, 3 conference papers have been published, 2 journal papers are under review, 1 conference paper is under review, another one is written and will be sent in October, 2020. A web-page for the project was established. The key-results, the progress reports and the developed tools (available for download) are shared through the web-page. Two articles are written for the general public.

To communicate the results with different audiences, I had meetings with SMEs from METU TechnoPark, gave informal talks to K-12 students, and had a stand for the project at Science is Wonderful, 2019 (Brussels).

Progress beyond the state of the art and expected potential impact (including the socio-economic impact and the wider societal implications of the project so far)

This MSCA-IF project has studied the timed automata design problem from new aspects. First, it combined the controller synthesis and parameter synthesis problems that have been studied separately. System analysis via synthesis of temporal logic formulas from traces has been studied for different modeling formalisms such as Simulink models. This project developed data-driven analysis and design techniques tuned for timed automata. Our experiments showed that these methods are capable of repairing benchmark TA examples with a high success rate. On the other hand, tuning the constraints of a TA to satisfy a reachability specification has not been studied before. However, it is a practically important problem since a verifier does not give an explanation when a TA does not satisfy such a specification.

Algorithms to find a TA with a minimal number of clocks that is equivalent to the given TA has been developed. However, these algorithms can change the structure of the automaton. The structure

reflects the physical properties and design parameters of the underlying system. This motivated our novel approach on reducing the number of clocks without changing the TA's structural properties.

Finally, ATAC is a novel tool for construction of TA models and generation of specification formula from descriptions given in structured natural language. The tool has two intended uses. The first use is as an educational tool to teach formal methods, and it was successfully used in outreach activities. The second use is to automate initial phases of the design process as detailed system descriptions are commonly derived for safety-critical systems.

As summarized above, throughout the project, the timed automata design problem is studied from new aspects and novel methods are developed. The main underlying goal is to simplify the design process for engineers and students by using formal models, since use of formal models is essential on guaranteeing correctness, and should become more widespread for safety-critical systems.

Last update: 27 November 2020

Permalink: https://cordis.europa.eu/project/id/798482/reporting