Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Parameter synthesis for probabilistic timed automata using stochastic game abstractions

Aleksandra Jovanović, Marta Kwiatkowska *

Department of Computer Science, University of Oxford, Oxford, UK

ARTICLE INFO

Article history:
Received 31 January 2016
Received in revised form 20 April 2017
Accepted 5 May 2017
Available online xxxx

Keywords:
Model checking
Parameter synthesis
Probabilistic reachability
Probabilistic timed automata
Markov decision processes
Stochastic games

ABSTRACT

We propose a symbolic method to synthesise optimal values of timing parameters for probabilistic timed automata, in the sense that the probability of reaching some set of states is either maximised or minimised. Our first algorithm, based on forward exploration of the symbolic states, can only guarantee parameter values that correspond to upper (resp. lower) bounds on maximum (resp. minimum) reachability probability. To ensure precise reachability probabilities, we adapt the game-based abstraction refinement method. In the parametric setting, our method is able to determine all the possible maximum or minimum reachability probabilities that arise for different values of timing parameters, and yields optimal valuations represented as a set of symbolic constraints between parameters. We report on a prototype implementation of the algorithm in the PRISM model checker and its evaluation on a case study.

1. Introduction

Stochastic aspects are very important for modelling numerous classes of systems, including communication, network and security protocols, due to component failures, unreliable channels or randomisation. The correctness of such systems can be guaranteed only with some probability. Many of them also operate under certain timing constraints. In such cases, the probability of a property being true depends on the timing aspects in the system: for example, increasing a certain delay might increase the maximum or minimum probability of reaching an error state.

Automatic synthesis of timing constraints to ensure the satisfaction of a given property has received a lot of attention lately. Its aim is to overcome the disadvantage of model checking, which requires complete knowledge of the system. This is often difficult to obtain, especially in the early design stages, when the whole environment is not yet known. The use of parameters instead of concrete values gives more freedom to the designers. A parametric timed model can specify that a transition is enabled for a time units, or that a system can stay in a location for b time units, where a and b are parameters. The goal is then to automatically synthesise the values of model's parameters such that its behaviour is guaranteed to satisfy the specification. Parameterisation, however, makes verification more difficult, as most problems become undecidable.

In this paper, we consider the synthesis of timing parameters for probabilistic real-time systems modelled as probabilistic timed automata (PTA) [1]. PTA have been introduced as an extension of timed automata (TA) [2] for modelling and analysing systems which exhibit real-time, nondeterminism and probabilistic behaviour. They are finite-state automata extended with clocks, real-valued variables which increase at the same, constant rate. The edge relation of a PTA differs from that of a TA, in

* Corresponding author.
E-mail address: marta.kwiatkowska@cs.ox.ac.uk (M. Kwiatkowska).

http://dx.doi.org/10.1016/j.tcs.2017.05.005
0304-3975/

the sense that purely nondeterministic choice over the set of edges is replaced by a set of discrete probability distributions, each of which is defined over a finite set of edges. A fundamental property of PTA is the maximum/minimum probability of reaching a certain set of states in the model (i.e. the reachability probabilities). These probabilities allow one to express a broad range of properties, from quality of service to reliability, for example, the deadline properties: "the maximum probability of an airbag failing to deploy within 0.02 seconds" or "the minimum probability that a packet is correctly delivered within 1 s". As shown in [1], model checking of more complex properties can be reduced to probabilistic reachability.

PTA arise naturally in distributed coordination and wireless communication protocols, and have been successfully used to analyse several protocols, including IEEE 1394 FireWire, Bluetooth and IEEE 802.11 WiFi, that rely on the use of randomisation and timing delays. The analyses were performed using the probabilistic model checker Prism, which provides native support for PTA through a variety of techniques, including symbolic zone-based methods. Since these protocols are embedded in a networked environment, their properties are almost always expressed parametrically, as concrete values make sense only when the network environment is known. Further, the choice of values of timing parameters may affect the probability of certain properties to be satisfied, as has been demonstrated for IEEE 1394 FireWire in [3] using Prism. The process of enumerating all the possible values of parameters, assuming a restriction to bounded integers/rationals, and performing verification for each instantiation is time consuming and error-prone. It is thus desirable to be able to automatically derive the constraints on parameters for probabilistic real-time systems, so that their correctness is ensured with optimal probability.

Contributions. We propose an algorithm for parameter synthesis for PTA based on the symbolic zone-based exploration of the underlying probabilistic reachability graph. As the forward approach gives only upper (resp. lower) bounds on maximum (resp. minimum) reachability probability, we adapt the game-based abstraction refinement method. This method has been introduced in [4] for Markov decision processes, and extended in [5] for PTA, for the computation of exact maximum/minimum reachability probabilities. As we consider parametric models, these probabilities are not unique and depend on particular parameter valuations. In the case of a *negative* specification, such as "the maximum probability of a message being lost", we are typically interested in the maximum probabilities, which we want to minimise, while in the case of a *positive* specification, such as "the minimum probability of message being received", we are interested in the minimum probabilities, which we want to maximise. Our algorithm derives a finite set of symbolic constraints on parameters for which the probability is either maximised or minimised, thus allowing us to choose optimal parameter valuations. We implement the algorithm as an extension of the Prism model checker [6], where a PTA can be input as a parametric model and the analysis proceeds through exploration of the underlying parametric zone graph. To the best of our knowledge, this is the first paper dealing with optimal timing parameter synthesis for probabilistic timed automata.

A preliminary version of this paper appeared as [7]. This paper extends [7] with full proofs, as well as an implementation and integration of the algorithm within Prism, and its evaluation on a case study.

Related work. Parameter synthesis for untimed probabilistic models includes [8], now implemented in Prism [9], where transition probabilities are considered as parameters for Markov chains. Given a property specified in some probabilistic logic, the goal is to find the values of parameters such that the formula holds in the model. Our work is orthogonal to this framework. We consider fixed probabilities and aim to synthesise timing constraints which maximise or minimise some reachability probability in the system.

Concerning non-probabilistic timed systems, parametric timed automata have been introduced in [10] as a means to specify parametric timing constraints. The *reachability-emptiness* problem, which asks whether there exists a parameter valuation such that the automaton has an accepting run, is undecidable. In [11], the undecidability proof is extended for parametric timed automata that use only strict inequalities. Subsequent research has thus concentrated on finding subclasses for which certain problems are decidable by restricting the use of parameters [12,13] or by restricting the parameter domain [14]. In [15], the authors deal with deterministic networks of timed automata with priorities and parametric guards and develop an algorithm based on constraint solving and Monte Carlo sampling to synthesise timing delays for MTL extended with counting formulas. In [16], optimal synthesis of timing parameters is considered for systems modelled as (deterministic) networks of timed I/O automata and quantitative objectives, such as energy consumption, formulated as a bilevel optimisation problem. An approach for the verification of Parametric TCTL (PTCTL) formulae has been developed in [17], where the problem has been proved decidable. A more general problem is studied in [18], where parameters are allowed both in the model and the desired PTCTL property. The authors show that the model checking problem is decidable and the parameter synthesis problem is solvable, in discrete time, over a PTA with one parametric clock, if equality is not allowed in the formulae. In [19], it is shown how bounded model checking can be applied to parameter synthesis for timed automata to synthesise part of the set of all the parameter valuations under which the given property holds in a model. A construction that enables the synthesis of an implementation of a specification for real-timed systems based on timed I/O automata, which is robust under a given timed perturbation, is presented in [20].

There is little work, however, on timing parameter synthesis for probabilistic real-time systems. In [21] the authors presented an approach based on the decomposition of the parametric space into behavioural tiles, i.e., sets of parameter valuations for which the behaviour of the system is uniform. The method is also extended for probabilistic systems. In [22], a technique is proposed to approximate parametric rate values for continuous-time Markov chains for bounded reachability probabilities, implemented in a GPU-based tool Prism-Psy [23]. In [24], the authors apply their *Inverse* method for parameter

Please cite this article in press as: A. Jovanović, M. Kwiatkowska, Parameter synthesis for probabilistic timed automata using stochastic game abstractions, Theoret. Comput. Sci. (2017), http://dx.doi.org/10.1016/j.tcs.2017.05.005