Robustness in Quantitative Systems: Verification and Synthesis

Ocan Sankur (Candidate 73198)

December 13, 2017

1 Introduction

Formal methods are an important part of the development of critical software and hardware systems. Among available techniques, model-checking plays an important role, and is being used in more and more industries developing complex systems, such as hardware, aerospatial, and transportation industries. The first model-checking algorithms were developed to verify finite-state systems against properties expressed in temporal logic [40]; so complex systems were handled at a very high-level, abstracting away many important properties of the system at hand. While this approach allowed significantly improving the development process of critical systems, only a limited set of properties on abstract designs could be handled. Today, several extensions of the finite automata formalism are considered including features such as timing constraints, probabilities, and cost, giving rise to the extensions of the verification techniques for quantitative systems. However, functional requirements (*e.g.* can a state be reached?) for these complex systems are not sufficient to describe complete specifications. One rather needs a complex set of constraints such as combinations of guarantees on execution time, cost, performance under several scenarios, say, both in normal conditions and in case of a failure. Moreover such systems are often subject to a stochastic model of the environment against which performance guarantees must be met. The object of this research is the verification and synthesis of systems with timed and probabilistic aspects against such complex properties.

Quantitative Verification With the introduction of quantities in formal models, researchers concentrated in extending existing verification techniques to take into account these quantities. In this context, considered problems include verification under *average* resource consumption [29], computing *optimal* controllers [69, 17], determining *time-bounds* on termination [38], and *measuring* the similarity of two systems [68]. While these results are important extensions of the known framework, they lack of generality and there is currently an important research effort that aims at systematically generalizing the theory of verification and synthesis from the Boolean case (which classifies as correct or incorrect) to the quantitative case (which measures the correctness) [41].

However there exist correctness criteria proper to quantitative systems which cannot be seen as extensions or refinements of existing notions in the classical theory of verification. Among these, I will also consider *robustness* issues in this project, which is recognized as an important notion (*e.g.* [42, 41]) but has attracted less attention.

Robustness In classical theories in formal verification no guarantee is given, even partial, when the system or its environment slightly deviates from the assumptions. Such deviations can be observed due to several reasons, such as, hardware failures, unintended use (say, a component being used in a different platform than for which it was designed), and an environment model that is too simplistic. Robustness of a system means that the behaviors do not change drastically under a slight change in environmental conditions. In control theory, it is often expressed as the continuity of the output as a function of the input. It follows that assumptions on the system and environment could be relaxed, perhaps upto some amount, while preserving at least partial correctness. However, existing theories do not apply to computer systems; the definition of an appropriate notion of robustness and the development of techniques for ensuring robustness are challenging problems, and were identified as an important challenge for the field by Henzinger and Sifakis [42].

Research Objectives More precisely, I will concentrate on two well-established formalisms for the design of systems with real-time and probabilistic aspects: timed automata and games [7, 10, 9], and Markov decision processes [57]. In timed systems, I will concentrate on robustness issues against an imprecise measure of time, and focus on (i) developing efficient algorithms for analyzing and quantifying the robustness of systems, and synthesizing robust controllers, (ii) extending the theory of robustness to the full controller synthesis setting, with distributed and stochastic aspects. On probabilistic systems, I will study robustness (iii) by simultaneously considering multiple models for the environment (say, one for normal conditions and one for failure) with the aim of combining formal guarantees and optimal average behaviors in the design of such systems. Furthermore, I suggest (iv) studying robustness against imprecisions in the probabilities of a given model, and developing robust controller synthesis algorithms in this setting.

In the long run, mainly two advantages will follow from the research on robustness in timed and probabilistic systems. First, the reach of formal methods will be extended in the design process of real-time systems; in fact, while the classical theory only allows checking abstract properties on formal models, some robustness questions related to timing imprecisions, imprecise probabilities, and unknown environments will also be answered by formal methods. This means more confidence in the model since a richer set of properties can be ensured formally, and the results depend less on assumptions on the environment. Second, these algorithms can help detect behaviors that appear in an idealistic formal model, but which are not realizable by a real system. On timed systems,

robustness analysis algorithms can help to detect timing anomalies such as controllers that are theoretically correct but fail in finite-precision hardware; on probabilistic systems, similar phenomena can occur when the environment (*e.g.* the probabilities) is assumed to be known precisely. Hence, the suggested research direction will have the aspiration of making future formal verification and synthesis algorithms more meaningful.

2 State of the Art

Finite-state formalisms The study of robustness in classical finite-state formalisms such as finite automata and games is a relatively new topic. In [18], robustness is expressed for finite-state reactive systems by bounding the (measure of the) output error as a function of input error, and a similar notion was considered for sequential circuits in [36], where it is required that the behavior of a robust circuit should recover in bounded time after an anomaly in input. In [16], the authors investigate synthesis problems under a robustness notion that requires guarantees on subsets of properties even if some liveness assumptions are violated. For control software, test generation and symbolic execution were employed for sensitivity analysis in [49].

Timed automata In timed formalisms such as timed and hybrid automata [7, 6], robustness has attracted more attention since in these formalisms time is modeled using perfectly continuous and precise clocks. In fact, it was observed that the semantics of some timed automata change qualitatively (i.e. w.r.t. location reachability) under the slightest drift or enlargement for the clocks [56]. The guard enlargement approach was later studied extensively; it consists in relaxing any guard of the form $x \in [a, b]$ into $x \in [a - \delta, b + \delta]$, where δ is an unknown parameter. The *robust model-checking* problem consists in deciding whether there exists a positive value for δ (and computing one), such that a given timed automaton satisfies a property. The problem was investigated for several properties such as safety [34], ω-regular properties [20, 22], timed temporal logics [21], untimed languages [60]. Some similar results about bounded clock drifts were also obtained [35, 67].

In [61], I studied and extended the guard enlargement approach in timed automata, with new perturbation models, and several analysis and synthesis algorithms. I contributed to the robust model-checking setting [22, 60], and considered the dual notion of the enlargement which is investigated in [64], where one checks the robustness of timed automata against restricting the guards. Such a notion is interesting both for checking the preservation of liveness properties, and for deriving implementations; tool support is also available for this setting [62]. The data structure called *shrunk difference-bound matrices* introduced in [64] was then used to study synthesis problems: I considered in [23, 65] semantics where perturbations on timings are controlled by an adversarial environment, and obtained algorithms to solve the synthesis problem in the resulting game

semantics while the bound on imprecisions is still parameterized. Extensions of the work include weighted timed automata and games [24], and timed games [52].

Most of the work in this framework consisted in reasoning with infinitesimal perturbations, while little attention was given to the computation of witnessing parameters. One exception is [43] where the largest tolerated imprecision parameter is computed symbolically in a restricted class of timed automata (without nested loops). Furthermore, the semi-algorithm of iteratively testing decreasing values of the parameter is investigated in [47] to estimate the tolerated perturbations.

Probabilistic systems Markov decision processes were also studied under multiple objectives. In [37] algorithms are given to synthesize a single strategy satisfying a conjunction of ω-regular properties where the probability of each property satisfies a given lower bound. One can thus chose an appropriate Pareto-optimal strategy that ensures good satisfaction probabilities on each property. In MDPs with multi-dimensional rewards, Pareto-optimal strategies were studied in [30, 25]. Some of these results were extended to stochastic games, and value iteration algorithms were given to approximate the Pareto curve [31].

Markov chains have been considered under imprecise probabilities, in the so-called interval-valued Markov chains (or MDPs) [46, 44] where probabilities are only known to belong to given intervals. The model may either be interpreted as a family of Markov chains, or as an MDP where at each step a distribution that conforms to given intervals is chosen by an adversary [66]. Recently, efficient algorithms were obtained for the PCTL model-checking problem, and for the adversarial semantics [55, 32].

3 Work Plan

3.1 Overview

This research proposal concerns the definition of appropriate notions of robustness in timed and probabilistic systems, and the development of efficient algorithms for verification and synthesis under such complex objectives. I will mainly consider these problems for timed automata [7], and Markov decision processes (MDP) [57].

Timed systems The first part of the project is on the development of robustness analysis and synthesis algorithms for timed systems modeled as timed automata and games, as well as the development of efficient tools:

- On timed systems, the first goal is to obtain efficient algorithms for robustness analysis, by concentrating first on *infinitesimal* analysis (that is, concentrating on small values of the parameter), and then extending the techniques to *maximal perturbation* analysis. Second, distributed timed systems will also be investigated for corresponding robustness problems.

Last, in order to support a shift from verification (analysis) to synthesis of systems, robust controller synthesis problems will be investigated on timed game models.

- In parallel to these developments, I will develop efficient algorithms and tools to solve robustness problems in timed automata, but also symbolic synthesis tools for succinctly represented systems. I also suggest specific applications for these tools. The long-term objective is to obtain robustness analysis algorithms of comparable efficiency with model-checking algorithms in timed automata so that robustness can become a standard feature in model-checking and synthesis tools such as Uppaal and Synthia [48, 53].

These directions are developed next, in Section 3.2.

Probabilistic systems The second part of the project concerns the study of robustness problems in probabilistic systems with rewards. I suggest enriching the set of properties that can be ensured in controller synthesis via several approaches.

- The transition probabilities in a probabilistic system correspond to a stochastic model of the behaviors of the system to be controlled. These probabilities are often assumed to be known and fixed. As a short to mid-term objective, I will develop algorithms for *multiple-environment synthesis*, that is synthesizing strategies against a set of known transition probabilities, each describing a different scenario, such as, normal conditions, minor failure, and major failure. The resulting setting allows one to combine formal guarantees (on several scenarios) with optimal average behaviors for each of the specific scenarios.

- As a long-term objective, I will consider probabilistic systems whose probabilities contain uncertainties: they are only known to belong to given intervals. Strategy synthesis in this context is a challenging problem for which some progress was made recently [55, 32].

These objectives have the common goal of considering robustness constraints in synthesis, while extending the classical average-case optimization setting to complex objectives. This direction is developed in Section 3.3.

3.2 Timed Systems

From Infinitesimal to Maximal Perturbation Analysis [short to mid term] Previous works on robustness in timed automata concentrated on the computation of *some* safe bound on perturbations tolerated by a given timed automaton. This is called *infinitesimal analysis* since one does not require the computation of the maximal bound. No efficient symbolic algorithm is currently known for infinitesimal perturbation analysis in timed automata (see [43] for a restricted class of timed automata), other than a binary search on possible values for the perturbation. Very recently, in [63], I obtained an efficient semi-algorithm for this problem whose performance is close to that of exact model checking in several benchmarks. My first short-term goal is to investigate complete algorithms for this problem. This will require studying cycle acceleration techniques on parametric data structures already used in [63].

One of the main objectives in this direction is to develop maximal perturbation analysis techniques for timed automata so as to quantify the sensitivity of a given system modeled by timed automata. As a mid-term goal I will consider *integer* parameter synthesis algorithms for timed automata [45], which were recently proposed. Known techniques for exact model checking could be lifted to this setting, yielding efficient algorithms in restricted cases. By exploiting the particular structure of the perturbation parameters in our setting, it may be possible to extend these techniques to handle a larger class of models and parameter types and solve robustness problems. More general parametric data structures can also be used, as in [43] for timed automata without nested cycles, to obtain semi-algorithms for general timed automata.

Robust Controller Synthesis [mid-term] In controller synthesis, the model contains *controllable* and *uncontrollable* transitions, and one is interested in synthesizing a control strategy so as to ensure a given property. Thus, rather than analyzing a given system, controller synthesis aims at synthesizing one from given constraints. I will investigate *robust* controller synthesis problems by requiring the strategies to be valid even if the suggested timings are perturbed by an adversary by a bounded amount.

I obtained preliminary results on this problem in [65, 52] by limiting the adversary's role to perturbing delays, and resolving non-determinism. However most controller synthesis problems require more expressive formalisms involving uncontrollable delays and actions. As a short-term goal, I will thus study *concurrent timed games* to model these problems and investigate strategy synthesis algorithms that tolerate timing perturbations chosen by the adversary. For general LTL objectives, perturbations can sometimes force the system into a deadlock; these behaviors were characterized as *unstable cycles* in [65, 52]. Algorithms for general timed games will require extending the notion of *stable cycles* from paths to execution trees. Developing symbolic (*e.g.* zone-based) algorithms to detect such cycles will also be a challenge.

In mid-term, I will consider a setting where the perturbations is due to random noise which is independent at each step. Such systems can be modeled as $2\frac{1}{2}$-

player timed games, where the adversary is still present but the perturbations are random. I obtained preliminary results in [52] on almost-sure and limit-sure satisfaction cases. I will investigate algorithms to compute bounds on the probability of the distance of the current behavior from the nominal behaviors to go above a threshold, as a function of the perturbation magnitude, execution length, and the threshold. This will allow one to *quantify* the effect of the noise on the behaviors of the system. In some restricted classes of models, it may be possible to compute (bounds on) *mean-time-to-failure*, that is, the expected number of steps before a safety specification can be violated.

Distributed Timed Systems [long-term] Issues related to imprecisions in time are crucial in distributed systems, e.g. due to communication delays. Furthermore, handling by formal methods the drifts of clocks that are local to different processes is a challenging problem open for many years. So far, only the robustness of clocks without drift has been tackled for distributed systems, and only for systems equivalent with regular sequential systems [4]. My first objective will be to extend recent techniques [**?**] to tackle non regular systems.

There is a strong connection between timed automata under clock drifts and clock imprecisions we consider; some robustness analysis algorithms are identical in both settings [34]. There are in fact precise simulation relations that show that one semantics can over-approximate the other one [5]. Although some related problems quickly become undecidable [2], this approach of approximating by guard enlargements might allow obtaining sufficient practical conditions for analyzing distributed timed systems.

3.3 Probabilistic Systems

In this section, I describe some directions I will explore in topics related to the robustness of probabilistic systems.

Multiple-Environment Synthesis [short to mid-term] The classical setting in probabilistic systems considers a single set of given transition probabilities, and the goal is often to maximize some given objective such as reachability probability or average reward. This modeling approach aims at optimizing the average behavior, but may not be sufficient when it comes to ensuring robustness, or when one requires multiple guarantees from the system.

To improve the guarantees given in such synthesized systems, I will consider the problem of synthesizing strategies in MDPs with guarantees against several *environments*, in the following sense. Rather than considering one transition probability matrix, we consider a finite set of them, each corresponding to a different scenario that may occur. In addition, we also consider the *environment* scenario, where the probabilistic transitions are replaced with an adversarial agent's choices. We consider the problem of synthesizing a *single* strategy with guarantees against each of these environments without any prior knowledge. Such strategies are *robust* since they give guarantees, say, in normal conditions,

under a minor failure, and against a major arbitrary failure, without the need of detecting the current one. The resulting setting allows one to mix *formal guarantees* with *optimal average behaviors*.

I obtained preliminary results in this direction in [58] for the case of two probabilistic environments; and [28] studies the case of one probabilistic and one worst-case environments. As a short term goal, I will pursue this direction in order to obtain algorithms for combinations of a worst-case and several probabilistic environments, and identify the precise computational complexity of the resulting problems. An important question that remains open is whether one can efficiently solve the multi-objective optimization problem which consists in optimizing the probability of success against each environment. To answer this question, I will investigate algorithms based on value iteration in the style of [39], which might yield an efficient solution for these problems. This requires operations on polyhedra and the challenge will be to bound the size of these sets along the iterations. These directions should help one understand at which extent known techniques for probabilistic systems can be lifted to the case of multiple environments. As a mid-term goal, if these techniques work on MDPs, I will investigate extensions to stochastic games; note that multi-dimensional value iteration has been used in this setting; see *e.g.* [31]. I will also consider *dynamic* variants of this model where the environment can regularly change non-deterministically. Strategies then must regularly update their believes and switch to different modes.

Interval-Valued Markov Chains and Decision Processes [long term] Verification and synthesis algorithms on MDPs usually assume that a precise model of the system is given, which means that probabilities are known exactly. In some cases this assumption is not appropriate since probabilities may result from estimations and known up to an error bound. Markov chains in which probabilities are only known to belong to given intervals have been considered in several works [32, 55, 51]. Several semantics have been considered to tackle the problem, and efficient algorithms for verifying Markov chains were given for some of them. Most works consider the case where the exact probabilities are *uncorrelated*: it is assumed that the exact probabilities of different transitions are independent and can dynamically change. Some efficient algorithms are developed thanks to this simplification, but this assumption can be overly conservative. I will study the precise complexity of the verification problems on so-called *uncertain* Markov chains (where the probabilities do not change dynamically), and explore the cases where this model is equivalent to the uncorrelated case, in particular, for quantitative objectives. The generalization of these problems to MDPs is also open. I will investigate whether the multiple environments setting presented above can approximate these problems, and whether one can obtain approximate solutions efficiently.

3.4 Efficient Algorithms and Tools

Symbolic Synthesis Algorithms for Synchronous Circuits [short to mid-term] In [26], I explored the problem of solving finite two-player games whose arenas are succinctly encoded as synchronous circuits, with controllable and uncontrollable inputs. The goal is to compute efficiently a small circuit implementing a strategy so as to ensure a safety specification. Our tool `AbsSynthe` was awarded the first prize in the synthesis competition organized during FLoC'14.

Our tool is based on binary decision diagrams (BDDs), several heuristics to shorten the search space, and on abstraction refinement techniques. I will pursue this work in the following directions. First, I will investigate heuristics to choose the way in which the abstraction are refined when a spurious counter-example is found. In fact, although several techniques are known for model checking, their extensions to synthesis is often too costly. Moreover, predicate abstraction is often used on systems given in a particular syntax (such as programs), but their application in circuit-like low-level descriptions is difficult.

Second, I will apply game theoretical notions in order to derive compositional algorithms. Models can often be decomposed into smaller systems with simpler specifications. Seeing each component as an agent with a possibly different -but not necessarily conflicting- objective, it is possible to make assumptions on surrounding components. Sufficient criteria to synthesize profiles of *dominant* strategies have been investigated in [33]. I will develop techniques that use weaker notions such as *admissibility* [27] to derive *necessary and sufficient* conditions on the components, and apply them to decompositions of circuits.

The last direction I will pursue concerns a discrete-time semantics for timed games with several cost functions. While the corresponding problems in the classical setting of continuous-time semantics are undecidable, they are decidable in the discrete-time setting which can be encoded by circuits. Particular BDD variable orderings and encodings for clocks have been suggested for timed automata verification, but not for timed games or weighted timed games. As a mid-term objective, I will investigate encodings for clock variables, and cost variables by exploiting assumptions on their structure *e.g.* assuming only positive weights. In a similar spirit, I will explore bounded model checking techniques in the context of robustness in timed automata; in fact, the results of [65] suggest that robustly controllable timed automata are discretizable, so incremental bounded model-checking techniques based on discretization and SAT-solving (e.g. [50]) can be made complete. Here, the difficulty will be in obtaining bounds on the length of such lassos, and in their discretization factors.

Robustness Tools for Timed Automata [mid-term] I will consider algorithms based on infinitesimal analysis to solve the maximal perturbation problem in two ways. First, infinitesimal analysis can be run iteratively, to improve the safe bound at each step. In this case, the convergence of this procedure needs to be investigated. Second, infinitesimal analysis can efficiently detect some problematic cycles where perturbations accumulate; this information can be incorporated in a fully parametric analysis.

I will develop robust controller synthesis algorithms in restricted cases based on theoretical results from previous work [65, 52]. For objectives not involving liveness properties, such as reachability objectives, it should be possible to derive symbolic *backwards* algorithms for the infinitesimal case. However, *forward* algorithms are more efficient in practice, especially if the models contain bounded data variables (like in Uppaal models). Such algorithms might be obtained for the parametric case, which might require extending operations on parametric data structures used in infinitesimal analysis.

The analysis of large systems are often handled by modularity, that is, by dividing the task into smaller ones on separate components, and then recombining the results. Accordingly, a long-term direction for obtaining efficient solutions for robustness analysis in timed automata will be based on this approach. The idea is to define appropriate parallel composition operators that yield a robust system whenever the components are themselves robust, while allowing computing (an upper bound on) the tolerated imprecisions. The resulting approach will be applicable to distributed timed systems since components to be considered appear naturally. To achieve this goal, some restriction of the specification or that of composed systems may be required. The challenge with this direction is to obtain restrictions on synchronization and specification that are not excessive, and it may be computationally difficult to exploit local information in subsystems.

Applications **[mid-term]** I believe it is crucial to apply the ideas developed in theoretical works in applications in order to obtain a feedback on the accuracy of the models and the problems formalized on them. Accordingly, I have already worked on several verification and synthesis tools; in this paragraph, I present some directions for application areas where these tools, and the algorithms I will develop in the future will be applied.

I will pursue the collaboration I started with F. Jacquemard (Inria & Ircam) on an application of robustness analysis in timed automata models to measure the robustness of scores in the music recognition and accompaniment system developed at Ircam. This is a complex system which consists of several components that detect the tempo played by the musician and follows the scores to play the accompaniment. The scores contain not only music but also events involving switching on and off the light, and the events have timings and dependencies between them. Robustness problems occur during performances due to unexpected delays, or errors in tempo: *e.g.* if the ordering of some events change, the lights may not be switched on back until the end of the concert. In a preliminary work, general parameter synthesis tools for timed automata were used to find tolerated imprecisions in some parts of the scores. The tools I will develop both for infinitesimal and maximal perturbation analysis can be immediately applied to these models. Furthermore, I will investigate the use of robust controller synthesis algorithms can be used to compute robust schedulers.

In a broader setting, robustness analysis and robust control synthesis algorithms will be of interest for sensitivity analysis of scheduling systems. In fact, timed automata have been used for solving scheduling problems, see e.g. [1],

and tool support is available [8]. In the long term, I will use obustness analysis algorithms to quantify the sensitivity of a given scheduler on given instances on particular settings. Moreover, robust controller synthesis can also allow one to synthesize a scheduling policy with guaranteed robustness.

Members of the SUMO team in Irisa work with the industrial partner Alstom to study automatic train regulation problems. A problem of interest is the design of train schedules which must be robust to incidents in the network such as shorter or longer delays, removal of a train etc. The computation of strategies to guide the management of the schedule, or the computation of robust schedules are difficult problems of interest due to the size of the schedules and to the stochastic nature of incidents. Astom is interested by a large number of questions on this topic. In case of my integration to Irisa, I will join ongoing works on the topic and also investigate the use of parameter synthesis algorithms, and robustness analysis tools in particular to approach this problem.

4 Integration

I describe in this section my possible integration in three laboratories: IRISA in Rennes (UMR 6074), IRCCyN (UMR 6597) and LINA (UMR 6241) in Nantes.

4.1 IRISA, Rennes

I wish to join the team SUMO in IRISA, founded recently with the main objectives of developing algorithms for the modeling, analysis, and supervision of large modular systems with real-time and quantitative aspects.

Research interests One of the objectives of the team is to develop algorithms for the analysis of distributed timed systems, for instance with unreliable communication and clock drifts; some results on infinite-state systems were obtained in [4, 3], and the team has experience in timed formalisms such as timed automata, time Petri nets, and timed MSC graphs [15, 4, 3]. Another line of work in IRISA is on testing and enforcement of timed systems, where one seeks to monitor and control the timings of input to a system so as to satisfy a given specification [54]. These objectives are closely related to my research project, and given my experience in similar problems on imprecise timings in timed automata, I could join ongoing work by Thierry Jéron, Blaise Genest, Loïc Hélouët, and Hervé Marchand and bring my experience on the subject. Furthermore, my proposal on compositional techniques for the robustness of timed automata could integrate naturally the team's research goal on building on modular techniques to tackle large systems.

Probabilistic semantics for timed automata have been investigated in the team by Nathalie Bertrand [11, 12, 13]. In this setting, a major difficulty is the computation of probabilities along cycles. Some techniques used in the study of robustness in timed automata, such as the notion of *stable cycles* [14, 65] might be employed to obtain abstractions allowing one to tackle the general problem.

Another problem of common interest in the team is opacity and diagnosability. The team seeks to develop techniques for quantitative extensions of these notions, for instance formalized on partial-observation MDPs, with an emphasis on parametric models, component-based approach, and multi-player aspects. Involved researchers are Nathalie Bertrand, Loïc Hélouët, Eric Fabre, Hervé Marchand, Eric Badouel, Thierry Jéron, and Christophe Morvan. Although I have little background on diagnosis, I am interested in related problems on MDPs and POMDPs, and I could join ongoing works and find collaborations of common interest.

The team is involved in the development of tools for discrete-event systems: Hervé Marchand works on the tool Sigali, a controller synthesis tool using symbolic data structures (such as binary decision diagrams or other algebraic data structures). Recent works concentrate extending these techniques to models with data (that is, program variables). I can collaborate on this topic given my recent work in this area.

Projects I have been involved in the ANR ImpRo project (2011-2014) between IRISA, IRCCyN (Nantes), LIP6 (Paris), and LSV (Cachan), in which the robustness and implementability of real-time systems are investigated. I regularly attended meetings, discussions of the project along with several researchers from IRISA (Nathalie Bertrand, Loïc Hélouët). The project has ended but a new project between the same partners is in preparation with an emphasis on quantitative, stochastic, parameterized aspects.

The project ANR Vacsim (2011-2015) between EDF R&D, Dassault Systemes, LURPA (Cachan), I3S (Nice), LABRI (Bordeaux), and IRISA aims at contributions for the simulation and validation of control-command systems. The team has been contributing in quantitative analysis, monitoring in timed systems, and verification of communicating timed systems. These topics are related to my experience and research project, and I could join ongoing efforts.

Another new project is ANR StochMC (2014-2017), lead by Blaise Genest, on stochastic models for biological systems, in which approximation techniques for Markov chains will be investigated. Although I have little experience on this area, my research project includes long-term goals on similar topics, such as robust MDPs, and I would be interested in participating in the project.

Other collaborations in IRISA On suggested applications of robustness in timed automata to scheduling systems, I could collaborate with the ALF team in IRISA which is specialized in multicore embedded systems. On compositional aspects of robustness analysis in timed automata, some related work on interface theories has been done by Axel Legay and collaborators from the Triskell team [47]. Some of the directions I describe concerns the applications of game theory to controller synthesis. On this direction, I could collaborate with Sophie Pinchinat from the Logica team who has ongoing works on imperfect information games.

4.2 IRCCyN and LINA, Nantes

I wish to join the *real-time systems* team of IRCCyN (UMR 6597) or the AELOS team (*Architectures et Logiciels Sûrs*) of LINA (UMR 6241). The two laboratories are being merged, which is expected to be done in 2017. In this section, I present my possible integration with both teams.

The two teams form the regional transversal team *AFSEC (approches formelles des systèmes embarqués communicants)* on formal methods for embedded communicating systems. Members from both teams (Olivier H. Roux, Didier Lime from Irccyn, Claude Jard, Benoît Delahaye from Lina) jointly participate to the ANR project PACS (2014-2018) involving as other members LIPN (U. Paris Nord), and LIAFA (U. Paris Diderot). The goal of the project is to develop parameter synthesis techniques in formal models (automata and Petri nets) where the parameters can appear in timing constraints, cost, or probabilities. Given my research background and interests I can naturally join this project.

IRCCyN, Nantes The real-time team of IRCCyN gathers reseachers with expertises in formal methods, scheduling, and real-time operating systems. I have been in contact with several members of both teams through regular meetings of the project ANR ImpRo (2011-2014).

The development of verification and synthesis algorithms for timed models have been an active research area of the group. Olivier H. Roux and Didier Lime work on the verification of timed automata and time Petri nets and maintain the time Petri net verification tool Romeo. Recent works include efficient algorithms for integer parameter synthesis in such models. I could join ongoing works on this topic, and investigate, with the team members, formulations of robustness problems as parameter synthesis problems. The group has also experience on controller synthesis problems based on timed games, and contributed to the development of Uppaal-Tiga, the extension of Uppaal that solves timed games.

Recent works of the group by Jean-Luc Béchennec, Olivier H. Roux, Mikaël Briday and their students include device driver synthesis using formal methods. The current project on the topic SeeForSys (2011-2014) is ending, but the contributors will pursue their work. Synthesis algorithms as I am investigating on synchronous circuits have been used to automatically synthesize real device drivers by other teams, see *e.g.* [59]. I would be interested in joining ongoing efforts in this topic, compare and combine different approaches to improve existing techniques.

On applications of formal methods to schedulability and sensitivity analysis of schedulers suggested in my research project, I could collaborate with Maryline Chetto, Anne-Marie Déplanche, and Sebastien Faucou who have works on real-time multiprocessor scheduling.

LINA, Nantes The research interests of the team AELOS in LINA include design, verification and monitoring of distributed, timed, and stochastic systems, and validation of software architectures in software engineering, but also proof and test, and concurrent semantics. The team concentrates on developing

techniques based on components in order to design and analyze systems, and ensure their quality of service.

One line of work by Claude Jard consists in the verification of distributed timed systems; although I have less experience on techniques for distributed systems, *e.g.* on unfoldings, I do have background on similar topics and could naturally join these works. Other works include diagnostic and monitoring techniques for distributed systems. I am also interested in compositional techniques for synthesis and verification of systems. Some abstraction techniques used to handle components can be applied to distributed systems as well.

The team has also works on compositional analysis for probabilistic systems. Benoît Delahaye has recent works on constraint Markov chains, a model similar to interval Markov chain I suggest studying in my project. Several composition operators are studied on this model, which allows one to refine, and analyze systems compositionally. I could collaborate with the team on these topics, and in the case of my integration to the team, will give more priority to the development of algorithms for interval Markov chains and MDPs.

4.3 External Collaborations

On problems related to robustness in timed automata, I am currently collaborating with Pierre-Alain Reynier (LIF, Marseille) (see [65, 52]) and plan to continue the work. During the ANR project ImpRo (2011-2014), I started a collaboration with S. Akshay (IIT Bombay, India) who was with the IRISA, Rennes by the time, and I plan to pursue the work on distributed timed automata. This collaboration will be natural in case of my integration to IRISA, since he has ongoing works with researchers from IRISA. I am also starting a collaboration with Ashutosh Trivedi and S. Narayanan Krishna from IIT Bombay on decidability of weighted timed games. On applications of robustness in music accompaniment, I started a collaboration with Florent Jacquemard (INRIA - IRCAM, Paris). I collaborated with Kim G. Larsen (Aalborg, Denmark) in [19], and am in contact with his team on problems related to timed automata. Last, I plan to continue to work with Jean-François Raskin (Brussels, Belgium) and his team on synthesis of probabilistic systems.

References

[1] Yasmina Adbeddaïm, Eugene Asarin, and Oded Maler. Scheduling with timed automata. *Theoretical Computer Science*, 354(2):272–300, 2006.

[2] S. Akshay, Benedikt Bollig, Paul Gastin, Madhavan Mukund, and K. Narayan Kumar. Distributed timed automata with independently evolving clocks. In *CONCUR'08*, LNCS 5201, p. 82–97. Springer, August 2008.

[3] S. Akshay, B. Genest, L. Hélouet, and S. Yang. Regular set of representatives for time-constrained msc graphs. *Inf. Process. Lett*, 112(14):592–598, 2012.

[4] S. Akshay, Loïc Hélouët, Claude Jard, and Pierre-Alain Reynier. Robustness of time petri nets under guard enlargement. In *Reachability Problems*, LNCS 7550, p. 92–106. Springer Berlin Heidelberg, 2012.

[5] S. Akshay and Pierre-Alain Reynier. Personal communication. 2013.

[6] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.

[7] Rajeev Alur and David L. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[8] Tobias Amnell, Elena Fersman, Leonid Mokrushin, Paul Pettersson, and Wang Yi. Times: Atool for schedulability analysis and code generation of real-time systems. In *Formal Modeling and Analysis of Timed Systems*, LNCS 2791, p. 60–72. Springer Berlin Heidelberg, 2004.

[9] Eugene Asarin, Oded Maler, and Amir Pnueli. Symbolic controller synthesis for discrete and timed systems. In *Hybrid Systems II*, LNCS 999, p. 1–20. Springer, 1995.

[10] Eugene Asarin, Oded Maler, Amir Pnueli, and Joseph Sifakis. Controller synthesis for timed automata. In SSC'98, p. 469–474. Elsevier Science, 1998.

[11] Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Marcus Größer. Probabilistic and topological semantics for timed automata. In FSTTCS'07, LNCS 4855, p. 179–191. Springer, 2007.

[12] Christel Baier, Nathalie Bertrand, Patricia Bouyer, Thomas Brihaye, and Marcus Größer. Almost-sure model checking of infinite paths in one-clock timed automata. In *Proceedings of the 23rd Annual IEEE Symposium on Logic in Computer Science (LICS'08)*, p. 217–226, Pittsburgh, Pennsylvania, USA, June 2008. IEEE Computer Society Press.

[13] P. Ballarini, N. Bertrand, A. Horvath, M. Paolieri, and E. Vicario. Transient analysis of networks of stochastic timed automata using stochastic state classes. In *10th International Conference on Quantitative Evaluation of SysTems (QEST'13)*, LNCS 8054, p. 355–371, Buenos Aires, Argentina, August 2013.

[14] Nicolas Basset and Eugene Asarin. Thin and thick timed regular languages. In *Formal Modeling and Analysis of Timed Systems*, LNCS 6919, p. 113–128. Springer Berlin Heidelberg, 2011.

[15] Nathalie Bertrand, Thierry Jéron, Amélie Stainer, and Moez Krichen. Off-line test selection with test purposes for non-deterministic timed automata. *Logical Methods in Computer Science*, 8(4), 2012.

[16] Roderick Bloem, Krishnendu Chatterjee, Karin Greimel, Thomas A. Henzinger, and Barbara Jobstmann. Robustness in the presence of liveness. In *Computer Aided Verification*, LNCS 6174, p. 410–424. Springer Berlin Heidelberg, 2010.

[17] Roderick Bloem, Krishnendu Chatterjee, Thomas Henzinger, and Barbara Jobstmann. Better quality in synthesis through quantitative objectives. In *Computer Aided Verification (CAV)*, p. 140–156, 2009.

[18] Roderick Bloem, Karin Greimel, Thomas A. Henzinger, and Barbara Jobstmann. Synthesizing robust systems. In *Formal Methods in Computer-Aided Design, 2009. FMCAD 2009*, p. 85–92, 2009.

[19] Patricia Bouyer, Kim G. Larsen, Nicolas Markey, Ocan Sankur, and Claus Thrane. Timed automata can always be made implementable. In CONCUR'11, LNCS 6901, p. 76–91, Aachen, Germany, September 2011. Springer.

[20] Patricia Bouyer, Nicolas Markey, and Pierre-Alain Reynier. Robust model-checking of linear-time properties in timed automata. In LATIN'06, LNCS 3887, p. 238–249. Springer, 2006.

[21] Patricia Bouyer, Nicolas Markey, and Pierre-Alain Reynier. Robust analysis of timed automata via channel machines. In FoSSaCS'08, LNCS 4962, p. 157–171. Springer, 2008.

[22] Patricia Bouyer, Nicolas Markey, and Ocan Sankur. Robust model-checking of timed automata via pumping in channel machines. In FORMATS'11, LNCS 6919, p. 97–112, Aalborg, Denmark, September 2011. Springer.

[23] Patricia Bouyer, Nicolas Markey, and Ocan Sankur. Robust reachability in timed automata: A game-based approach. In ICALP'12, LNCS 7392, p. 128–140. Springer, 2012.

[24] Patricia Bouyer, Nicolas Markey, and Ocan Sankur. Robust weighted timed automata and games. In *Proceedings of the 11th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'13)*, LNCS 8053, p. 31–46, Buenos Aires, Argentina, August 2013. Springer.

[25] Tomáš Brázdil, Václav Brozek, Krishnendu Chatterjee, Vojtech Forejt, and Antonn Kucera. Two views on multiple mean-payoff objectives in markov decision processes. In LICS'11, p. 33–42. IEEE Computer Society Press, June 2011.

[26] Romain Brenguier, Guillermo A. Pérez, Jean-François Raskin, and Ocan Sankur. Abssynthe: abstract synthesis from succinct safety specifications. In Proceedings 3rd Workshop on *Synthesis (SYNT'14)*, Electronic Proceedings in Theoretical Computer Science 157, p. 100–116. Open Publishing Association, 2014.

[27] Romain Brenguier, Jean-François Raskin, and Mathieu Sassolas. The complexity of admissibility in omega-regular games. In *Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS '14, Vienna, Austria, July 14 - 18, 2014*, p. 23, 2014.

[28] Véronique Bruyère, Emmanuel Filiot, Mickael Randour, and Jean-François Raskin. Meet your expectations with guarantees: Beyond worst-case synthesis in quantitative games. In *STACS*, p. 199–213, 2014.

[29] Krishnendu Chatterjee, Laurent Doyen, and Thomas A Henzinger. Quantitative languages. *ACM Transactions on Computational Logic (TOCL)*, 11(4):23, 2010.

[30] Krishnendu Chatterjee, Rupak Majumdar, and Thomas A. Henzinger. Markov decision processes with multiple objectives. In *STACS 2006*, LNCS 3884, p. 325–336. Springer Berlin Heidelberg, 2006.

[31] Taolue Chen, Vojtech Forejt, Marta Z. Kwiatkowska, Aistis Simaitis, and Clemens Wiltsche. On stochastic games with multiple objectives. In *MFCS*, p. 266–277, 2013.

[32] Taolue Chen, Tingting Han, and Marta Kwiatkowska. On the complexity of model checking interval-valued discrete time markov chains. *Information Processing Letters*, 113(7):210 – 216, 2013.

[33] Werner Damm and Bernd Finkbeiner. Automatic compositional synthesis of distributed systems. In *FM 2014: Formal Methods*, LNCS 8442, p. 179–193. Springer International Publishing, 2014.

[34] Martin De Wulf, Laurent Doyen, Nicolas Markey, and Jean-François Raskin. Robust safety of timed automata. *Formal Methods in System Design*, 33(1-3):45–84, 2008.

[35] Catalin Dima. Dynamical properties of timed automata revisited. In FORMATS'07, LNCS 4763, p. 130–146. Springer Berlin / Heidelberg, 2007.

[36] Laurent Doyen, Thomas A. Henzinger, Axel Legay, and Dejan Nickovic. Robustness of sequential circuits. In *Proceedings of the 2010 10th International Conference on Application of Concurrency to System Design*, ACSD '10, ACSD '10, p. 77–84. IEEE Computer Society, 2010.

[37] Kousha Etessami, Marta Z. Kwiatkowska, Moshe Y. Vardi, and Mihalis Yannakakis. Multi-objective model checking of markov decision processes. *Logical Methods in Computer Science*, 4(4), 2008.

[38] Vojtěch Forejt, Marta Kwiatkowska, Gethin Norman, and Ashutosh Trivedi. Expected reachability-time games. In *Formal Modeling and Analysis of Timed Systems*, LNCS 6246, p. 122–136. Springer Berlin Heidelberg, 2010.

[39] Vojtěch Forejt, Marta Kwiatkowska, and David Parker. Pareto curves for probabilistic model checking. In *Automated Technology for Verification and Analysis*, LNCS, Lecture Notes in Computer Science, p. 317–332. Springer Berlin Heidelberg, 2012.

[40] Orna Grumberg and Helmut Veith, editors. *25 Years of Model Checking - History, Achievements, Perspectives*, LNCS 5000. Springer, 2008.

[41] Thomas A. Henzinger. Quantitative reactive modeling and verification. *Computer Science - Research and Development*, 28(4):331–344, 2013.

[42] Thomas A. Henzinger and Joseph Sifakis. The embedded systems design challenge. In FM'06, LNCS 4085, p. 1–15, Hamilton, Canada, 2006. Springer.

[43] Rémi Jaubert and Pierre-Alain Reynier. Quantitative robustness analysis of flat timed automata. In FOSSACS'11, LNCS 6604, p. 229–244. Springer, 2011.

[44] B. Jonsson and K.G. Larsen. Specification and refinement of probabilistic processes. In *Logic in Computer Science, 1991. LICS '91., Proceedings of Sixth Annual IEEE Symposium on*, p. 266–277, 1991.

[45] Aleksandra Jovanović, Didier Lime, and Olivier H. Roux. Integer Parameter Synthesis for Real-Time Systems. *IEEE Transactions on Software Engineering (TSE)*, 2014. To appear.

[46] Igor O. Kozine and Lev V. Utkin. Interval-valued finite markov chains. *Reliable Computing*, 8(2):97–113, 2002.

[47] Kim G. Larsen, Axel Legay, Louis-Marie Traonouez, and Andrzej Wasowski. Robust specification of real time components. In *Formal Modeling and Analysis of Timed Systems*, LNCS 6919, p. 129–144. Springer Berlin Heidelberg, 2011.

[48] Kim Gulstrand Larsen, Paul Pettersson, and Wang Yi. UPPAAL in a nutshell. *International Journal on Software Tools for Technology Transfer*, 1(1-2):134–152, 1997.

[49] Rupak Majumdar and Indranil Saha. Symbolic robustness analysis. In *Proceedings of the 2009 30th IEEE Real-Time Systems Symposium*, RTSS '09, RTSS '09, p. 355–363. IEEE Computer Society, 2009.

[50] Janusz Malinowski and Peter Niebert. Sat based bounded model checking with partial order semantics for timed automata. In TACAS'10, LNCS 6015, p. 405–419. Springer Berlin Heidelberg, 2010.

[51] Arnab Nilim and Laurent El Ghaoui. Robust control of markov decision processes with uncertain transition matrices. *Operations Research*, 53(5):780–798, 2005.

[52] Youssouf Oualhadj, Pierre-Alain Reynier, and Ocan Sankur. Probabilistic robust timed games. In *Proceedings of the 25th International Conference on Concurrency Theory (CONCUR'14)*, LNCS 8704, p. 203–217. Springer, 2014.

[53] Hans-Jörg Peter, Rüdiger Ehlers, and Robert Mattmüller. Synthia: Verification and synthesis for timed automata. In *Proceedings of the 23rd International Conference on Computer Aided Verification (CAV)*, LNCS 6806, p. 649–655. Springer, 2011.

[54] S. Pinisetty, Y. Falcone, T. Jéron, H. Marchand, A. Rollet, and O. Nguena Timo. Runtime enforcement of timed properties. In *Third International Conference on Runtime Verification RV 2012*, LNCS 7687, p. 229–244, Istanbul, Turkey, September 2012.

[55] Alberto Puggelli, Wenchao Li, Alberto L. Sangiovanni-Vincentelli, and Sanjit A. Seshia. Polynomial-time verification of pctl properties of mdps with convex uncertainties. In *Computer Aided Verification*, LNCS 8044, p. 527–542. Springer Berlin Heidelberg, 2013.

[56] Anuj Puri. Dynamical properties of timed automata. *Discrete Event Dynamic Systems*, 10(1-2):87–113, 2000.

[57] Martin L Puterman. *Markov decision processes: discrete stochastic dynamic programming*. Wiley, 2009.

[58] Jean-François Raskin and Ocan Sankur. Multiple-environment markov decision processes. In *Proceedings of the 34st Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'14)*, 2014.

[59] Leonid Ryzhyk, Peter Chubb, Ihor Kuz, Etienne Le Sueur, and Gernot Heiser. Automatic device driver synthesis with termite. In *Proceedings of the ACM SIGOPS 22Nd Symposium on Operating Systems Principles*, SOSP '09, SOSP '09, p. 73–86, New York, NY, USA, 2009. ACM.

[60] Ocan Sankur. Untimed language preservation in timed systems. In MFCS'11, LNCS 6907, p. 556–567. Springer, August 2011.

[61] Ocan Sankur. *Robustness in Timed Automata: Analysis, Synthesis, Implementation*. Thèse de doctorat, Laboratoire Spécification et Vérification, ENS Cachan, France, June 2013.

[62] Ocan Sankur. Shrinktech: A tool for the robustness analysis of timed automata. In CAV'13, LNCS 8044, p. 1006–1012, Saint Petersburg, Russia, 2013. Springer.

[63] Ocan Sankur. Symbolic quantitative robustness analysis of timed automata. To appear in Tools and Algorithms for the Construction and Analysis of Systems (TACAS'15), 2015.

[64] Ocan Sankur, Patricia Bouyer, and Nicolas Markey. Shrinking timed automata. In FSTTCS'11, LIPIcs 13, p. 375–386. Leibniz-Zentrum für Informatik, December 2011.

[65] Ocan Sankur, Patricia Bouyer, Nicolas Markey, and Pierre-Alain Reynier. Robust controller synthesis in timed automata. In CONCUR'13, LNCS 8052, p. 546–560. Springer, 2013.

[66] Koushik Sen, Mahesh Viswanathan, and Gul Agha. Model-checking markov chains in the presence of uncertainties. In *Tools and Algorithms for the Construction and Analysis of Systems*, LNCS 3920, p. 394–410. Springer Berlin Heidelberg, 2006.

[67] Mani Swaminathan, Martin Fränzle, and Joost-Pieter Katoen. The surprising robustness of (closed) timed automata against clock-drift. In *Fifth IFIP International Conference On Theoretical Computer Science TCS 2008*, IFIP International Federation for Information Processing 273, p. 537–553. Springer US, 2008.

[68] Pavol Černý, Thomas A. Henzinger, and Arjun Radhakrishna. Simulation distances. In *CONCUR 2010 - Concurrency Theory*, LNCS 6269, p. 253–268. Springer Berlin Heidelberg, 2010.

[69] Christian von Essen and Barbara Jobstmann. Synthesizing efficient controllers. In *International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)*, p. 428–444, 2012.