IN PARTNERSHIP WITH:
CNRS

Université Rennes 1

Activity Report 2017

Project-Team SUMO

SUpervision of large MOdular and distributed systems

IN COLLABORATION WITH: Institut de recherche en informatique et systèmes aléatoires (IRISA)

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Proofs and Verification

Table of contents

Project-Team SUMO

Creation of the Team: 2013 January 01, updated into Project-Team: 2015 January 01

Keywords:

Computer Science and Digital Science:

A1.2.2. - Supervision
A1.3. - Distributed Systems
A2.3.2. - Cyber-physical systems
A2.4.2. - Model-checking
A4.5. - Formal methods for security
A6.4. - Automatic control
A7.1. - Algorithms
A7.2. - Logic in Computer Science
A8.2. - Optimization
A8.6. - Information theory
A8.11. - Game Theory

Other Research Topics and Application Domains:

B1.1.3. - Cellular biology
B1.1.9. - Bioinformatics
B5.2.2. - Railway
B6.2. - Network technologies
B6.3.3. - Network Management

1. Personnel

Research Scientists

Éric Fabre [Team leader, Inria, Senior Researcher, HDR]
Éric Badouel [Inria, Researcher, HDR]
Nathalie Bertrand [Inria, Researcher, HDR]
Blaise Genest [CNRS, Researcher, HDR]
Loïc Hélouët [Inria, Researcher, HDR]
Thierry Jéron [Inria, Senior Researcher, HDR]
Hervé Marchand [Inria, Researcher, HDR]
Nicolas Markey [CNRS, Senior Researcher, HDR]
Ocan Sankur [CNRS, Researcher]

PhD Students

Hugo Bazille [Inria]
Sihem Cherrared [Orange Labs]
Arij Elmajed [Nokia, from Feb 2017]
Bruno Karelovic [Univ. Paris VII]
Abd El Karim Kecir [ALSTOM Transport]
Engel Lefaucheux [Univ de Rennes I]
The Anh Pham [Univ de Rennes I, from Sep 2017]
Matthieu Pichené [Inria]
Victor Roussanaly [Univ de Rennes I, from Sep 2017]

Interns

Balasubramanian Ayikudi Ramachandrakumar [Inria, from May 2017 until Jul 2017]
Romain Boitard [Inria, from Apr 2017 until Jul 2017]
Thomas Mari [Inria, from May 2017 until Jul 2017]
Aina Rasoamanana [Inria, from Feb 2017 until Jul 2017]
Victor Roussanaly [École normale supérieure de Rennes, from Feb 2017 until Jun 2017]

Administrative Assistant

Laurence Dinh [Inria]

Visiting Scientists

Robert Nsaibirni [University of Yaounde, until Jun 2017]
Shauna Laurene Ricker [Mount Allison Univ., Canada, from May 2017 until Jul 2017]

2. Overall Objectives

2.1. Overall objectives

Most software-driven systems we commonly use in our daily life are huge hierarchical assemblings of components. This observation runs from the micro-scale (multi-core chips) to the macro-scale (data centers), and from hardware systems (telecommunication networks) to software systems (choreographies of web services). The main characteristics of these pervasive applications are size, complexity, heterogeneity, and modularity (or concurrency). Besides, several such systems are actively used before they are fully mastered, or they have grown so much that they now raise new problems that are hardly manageable by human operators. While these systems and applications are becoming more essential, or even critical, the need for their *reliability*, *efficiency* and *manageability* becomes a central concern in computer science. The main objective of SUMO is to develop theoretical tools to address such challenges, according to the following axes.

2.1.1. Necessity of quantitative models.

Several disciplines in computer science have of course addressed some of the issues raised by large systems. For example, formal methods (essentially for verification purposes), discrete-event systems (diagnosis, control, planning, and their distributed versions), but also concurrency theory (modelling and analysis of large concurrent systems). Practical needs have oriented these methods towards the introduction of quantitative aspects, such as time, probabilities, costs, and their combinations. This approach drastically changes the nature of questions that are raised. For example, verification questions become the reachability of a state in a limited time, the average sojourn duration in a state, the probability that a run of the system satisfies some property, the existence of control strategies with a given winning probability, etc. In this setting, exact computations are not always appropriate as they may end up with unaffordable complexities, or even with undecidability. Approximation strategies then offer a promising way around, and are certainly also a key to handling large systems. Approaches based on discrete-event systems follow the same trend towards quantitative models. For diagnosis aspects, one is interested in the most likely explanations to observed malfunctions, in the identification of the most informative tests to perform, or in the optimal placement of sensors. For control problems, one is of course interested in optimal control, in minimizing communications, in the robustness of the proposed controllers, in the online optimization of QoS (Quality of Service) indicators, etc.

2.1.2. Specificities of distributed systems.

While the above questions have already received partial answers, they remain largely unexplored in a distributed setting. We focus on structured systems, typically a network of dynamic systems with known interaction topology, the latter being either static or dynamic. Interactions can be synchronous or asynchronous. The state-space explosion raised by such systems has been addressed through two techniques. The first one consists in adopting true-concurrency models, which take advantage of the parallelism to reduce the size of the trajectory sets. The second one looks for modular or distributed “supervision" methods, taking the shape

of a network of local supervisors, one per component. While these approaches are relatively well understood, their mixing with quantitative models remains a challenge (as an example, there exists no proper setting assembling concurrency theory with stochastic systems). This field is largely open both for modeling, analysis and verification purposes, and for distributed supervision techniques. The difficulties combine with the emergence of data-driven distributed systems (as web services or data centric systems), where the data exchanged by the various components influence both the behaviors of these components and the quantitative aspects of their reactions (e.g. QoS). Such systems call for symbolic or parametric approaches for which a theory is still missing.

2.1.3. New issues raised by large systems.

Some existing distributed systems like telecommunication networks, data centers, or large-scale web applications have reached sizes and complexities that reveal new management problems. One can no longer assume that the model of the managed systems is static and fully known at any time and any scale. To scale up the management methods to such applications, one needs to be able to design reliable abstractions of parts of the systems, or to dynamically build a part of their model, following the needs of the management functions to realize. Besides, one does not wish to define management objectives at the scale of each single component, but rather to pilot these systems through high-level policies (maximizing throughput, minimizing energy consumption, etc.) These distributed systems and management problems have connections with other approaches for the management of large structured stochastic systems, such as Bayesian networks (BN) and their variants. The similarity can actually be made more formal: inference techniques for BN rely on the concept of conditional independence, which has a counterpart for networks of *dynamic* systems and is at the core of techniques like distributed diagnosis, distributed optimal planning, or the synthesis of distributed controllers. The potential of this connection is largely unexplored, but it suggests that one could derive from it good approximate management methods for large distributed dynamic systems.

3. Research Program

3.1. Analysis and verification of quantitative systems

The overall objective of this axis is to develop the quantitative aspects of formal methods while maintaining the tractability of verification objectives and progressing toward the management of large systems. This covers the development of relevant modeling formalims, to nicely weave time, costs and probabilities with existing models for concurrency. We plan to further study time(d) Petri nets, networks of timed automata (with synchronous or asynchronous communications), stochastic automata, partially-observed Markov decision processes, etc. A second objective is to develop verification methods for such quantitative systems. This covers several aspects: quantitative verification questions (e.g. computing an optimal scheduling policy), Boolean questions on quantitative features (deciding whether some probability is greater than a threshold), robustness issues (will a system have the same behaviors if some parameter is slightly altered?), etc. Our goal is to explore the frontier between decidable and undecidable problems, or more pragmatically tractable and untractable problems. Of course, there is a tradeoff between the expressivity and the tractability of a model. Models that incorporate distributed aspects, probabilities, time, etc., are typically untractable. In such a case, abstraction or approximation techniques are a workaround that we will explore.

Here are some precise topics that we place in our agenda:

- analysis of diagnosability and opacity properties for stochastic systems;
- verification of time(d) Petri nets;
- robustness analysis for timed and/or stochastic systems;
- abstraction techniques for quantitative systems.

3.2. Control of quantitative systems

The main objective of this research axis is to explore the quantitative and/or distributed extensions of classical control problems. We envision control in its widest meaning of driving a system in order to guarantee or enforce some extra property (i.e. not guaranteed by the system alone), in a partially- or totally-observed setting. This property can either be logical (e.g. reachability or safety) or quantitative (e.g. reach some performance level). These problems have of course an offline facet (e.g. controller design, existence of a policy/strategy) and an online facet (e.g. algorithm to select some optimal action at runtime).

Our objectives comprise classical controler synthesis for discrete-event systems, with extensions to temporal/stochastic/reward settings. They also cover maintaining or maximizing extra properties such as diagnosability or opacity, for example in stochastic systems. We also target further analysis of POMDPs (partially-observed Markov decision processes), and multi-agent versions of policy synthesis relying on tools from game theory. We aim at adressing some control problems motivated by industrial applications, that raise issues like the optimal control of timed and stochastic discrete-event systems, with concerns like robustness to perturbations and multicriteria optimization. Finally, we also plan to work on modular testing, and on runtime enforcement techniques, in order to garantee extra logical and temporal properties to event flows.

3.3. Management of large or distributed systems

The generic terms of “supervision” or “management” of distributed systems cover problems like control, diagnosis, sensor placement, planning, optimization, (state) estimation, parameter identification, testing, etc. This research axis examines how classical settings for such problems can scale up to large or distributed systems. Our work will be driven by considerations like: how to take advantage of modularity, how to design approximate management algorithms, how to design relevant abstractions to make large systems more tractable, how to deal with models of unknown size, how to design mechanisms to obtain relevant models, etc.

As more specific objectives, let us mention:

- Parametric-size systems: how to verify properties of distributed systems with an unknown number of components;
- Approximate management methods: we will explore the extension of ideas developed for Bayesian inference in large-scale stochastic systems (such as turbo-algorithms) to the field of modular dynamic systems. When component interactions are sparse, even if exact management methods are unaccessible (for diagnosis, planning, control, etc.), good approximations based on local computations may be accessible;
- Model abstraction: we will explore techniques to design more tractable abstractions of stochastic dynamic systems defined on large sets of variables;
- Self-modelling, which consists in managing large-scale systems that are known by their building rules, but where the specific instance is only discovered on-the-fly at runtime. The model of the managed system is built on-line, following the needs of the management algorithms;
- Distributed control: we will tackle issues related to asynchronous communications between local controllers, and to abstraction techniques allowing to address large systems;
- Test and enforcement: we will tackle coverage issues for the test of large systems, and the test and enforcement of properties for timed models, or for systems handling data.

3.4. Data driven systems

Data-driven systems are systems whose behaviour depends both on explicit workflows (scheduling and durations of tasks, calls to possibly distant services, ...) and on the data processed by the system (stored data, parameters of a request, results of a request, ...). This family of systems covers workflows that convey data (business processes or information systems), transactional systems (web stores), large databases managed with rules (banking systems), collaborative environments (crowds, health systems), etc. These systems are distributed, modular, and open: they integrate components and sub-services distributed over the web, and

accept requests from clients. Our objective is to provide validation and supervision tools for such systems. To achieve this goal, we have to solve several challenging tasks:

- provide realistic models, and sound automated abstraction techniques, to reason on models that are reasonable abstractions of real systems. These models should be able to encompass modularity, distribution, in a context where workflows and data aspects are tightly connected;
- address design of data driven systems in a declarative way: declarative models are another way to handle data-driven systems. Rather than defining the explicit workflows and their effects on data, rule-based models state how actions are enacted in terms of the shape (pattern matching) or value of the current data. We think that distributed rewriting rules or attributed grammars can provide a practical yet formal framework for maintenance, by providing a solution to update mandatory documentation during the lifetime of an artifact.
- provide tractable solutions for validation of models: frequent issues are safety questions (can a system reach some bad configuration?), but also liveness (workflows progess), ... These questions should not only remain decidable on our models, but also with efficient computational methods.
- address QoS management in large reconfigurable systems: data-driven distributed systems often have constraints in terms of QoS. This QoS questions adress performance issues, but also data quality. This calls for an analysis of quantitative features and for reconfiguration techniques to meet desired QoS.

4. Application Domains

4.1. Smart transportation systems

The smart-city trend aims at optimizing all functions of future cities with the help of digital technologies. We focus on the segment of urban trains, which will evolve from static and scheduled offers to reactive and eventually on-demand transportation offers. We address two challenges in this field. The first one concerns the optimal design of robust subway lines. The idea is to be able to evaluate, at design time, the performance of time tables and of different regulations policies. In particular, we focus on robustness issues: how can small perturbations and incidents be accommodated by the system, how fast will return to normality occur, when does the system become unstable? The second challenge concerns the design of new robust regulation strategies to optimize delays, recovery times, and energy consumption at the scale of a full subway line. These problems involve large-scale discrete-event systems, with temporal and stochastic features, and translate into robustness assessment, stability analysis and joint numerical/combinatorial optimization problems on the trajectories of these systems.

4.2. Management of telecommunication networks and of data centers

Telecommunication-network management is a rich provider of research topics for the team, and some members of SUMO have a long background of contacts and transfer with industry in this domain. Networks are typical examples of large distributed dynamic systems, and their management raises numerous problems ranging from diagnosis (or root-cause analysis), to optimization, reconfiguration, provisioning, planning, verification, etc. They also bring new challenges to the community, for example on the modeling side: building or learning a network model is a complex task, specifically because these models should reflect features like the layering, the multi-resolution view of components, the description of both functions, protocols and configuration, and they should also reflect dynamically-changing architectures. Besides modeling, management algorithms are also challenged by features like the size of systems, the need to work on abstractions, on partial models, on open systems, etc. The networking technology is now evolving toward software-defined networks, virtualized-network functions, multi-tenant systems, etc., which reinforces the need for more automation in the management of such systems.

Data centers are another example of large-scale modular dynamic and reconfigurable systems: they are composed of thousands of servers, on which virtual machines are activated, migrated, resized, etc. Their management covers issues like troubleshooting, reconfiguration, optimal control, in a setting where failures are frequent and mitigated by the performance of the management plane. We have a solid background in the coordination of the various autonomic managers that supervise the different functions/layers of such systems (hardware, middleware, web services, ...) Virtualization technologies now reach the domain of networking, and telecommunication operators/vendors evolve towards providers of distributed open clouds. This convergence of IT and networking strongly calls for new management paradigms, which is an opportunity for the team.

This application domain will be revived in the team by a collaboration with Orange Labs (1 Cifre PhD in the common lab Orange/Inria) and a collaboration with Nokia Bell Labs (1 Cifre PhD, and participation to the joint research team “Softwarization of Everything” of the common lab Nokia Bell Labs/Inria).

4.3. Collaborative workflows

A current trend is to involve end-users in collection and analysis of data. Exemples of this trend are contributive science, crisis-management systems, and crowds. All these applications are data-centric and user-driven. They often are distributed and involve complex, and sometimes dynamic workflows. In many cases, there are strong interactions between data and control flows: indeed, decisons taken regarding the next tasks to be launched highly depend on collected data. For instance, in an epidemic-surveillance system, the aggregation of various reported disease cases may trigger alerts. Another example is crowds where user skills are used to complete tasks that are better performed by humans than computers. In return, this requires addressing imprecise and sometimes unreliable answers. We address several issues related to complex workflows and data. We study declarative and dynamic models that can handle workflows, data, uncertainty, and competence management.

Once these models are mature enough, we plan to experiment them on real use cases from contributive science, health-management systems, and crowd platforms using prototypes. We also plan to define abstaction schemes allowing formal reasonning on these systems.

4.4. Systems Biology

Systems Biology is a recent topic in SUMO. In systems biology, many continuous variables interact together. Biological systems are thus good representatives for large complex quantitative systems, for which we are developing analysis and management methods. For instance, the biological pathway of apoptosis explains how many molecules interact inside a cell, triggered by some outside signal (drug, etc.), eventually leading to the death of the cell by apoptosis. While intrinsically quantitative in nature and in problems, data are usually noisy and problems need not be answered with ultimate precision. It thus seems reasonable to resort to approximations in order to handle the state-space explosion resulting from the high dimensionality of biological systems.

We are developing models and abstraction tools for systems biology. Studying these models suggests new reduction methods, such as considering populations instead of explicitly representing every single element into play (be it cells, molecules, etc): we thus develop algorithm handling population symbolically, either in a continuous (distributions) or a discrete (parametric) way. An intermediate goal is to speed-up analysis of such systems using abstractions, and a long term goal is to develop top-down model-checking methods that can be run on these abstractions.

5. Highlights of the Year

5.1. Highlights of the Year

5.1.1. New partnership

Several members of the team are involved in the joint research team “Softwarization of Everything”, part of the joint research lab of Nokia Bell Labs France and Inria. This activity will finance two PhDs in the team, related to the management and control of software-defined networks.

5.1.2. Awards

- Engel Lefaucheux received the best young-researcher-paper award (“Prix Jeune Chercheur”) at MSR 2017 for his paper titled *Diagnostic et contrôle de la dégradation des systèmes probabilistes* .
- Nicolas Markey was awarded an *Allocation d’Installation Scientifique* (at senior-researcher level) from Rennes Métropole.

BEST PAPER AWARD:

[42]
N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Diagnostic et contrôle de la dégradation des systèmes probabilistes*, in "MSR 2017 - Modélisation des Systèmes Réactifs", Marseille, France, November 2017, https://hal.inria.fr/hal-01618922

6. New Software and Platforms

6.1. Active Workspaces

KEYWORDS: Active workspace - Collaborative systems - Artifact centric workflow system
SCIENTIFIC DESCRIPTION: Tool for computer supported cooperative work where a user’s workspace is given by an active structured repository containing the pending tasks together with information needed to perform the tasks. Communication between active workspaces is asynchronous using message passing. The tool is based on the model of guarded attribute grammars.

- Authors: Éric Badouel and Robert Nsaibirni
- Contact: Éric Badouel
- URL: http://people.rennes.inria.fr/Eric.Badouel/Research/ActiveWorkspaces.html

6.2. DAXML

KEYWORDS: XML - Web Services - Distributed Software - Active documents
SCIENTIFIC DESCRIPTION: DAXML is an interpreter and implementation of Distributed Active Documents, a formalism for data centric design of Web Services. This implementation is based on a REST framework, and can run on a network of machines connected to internet and equiped with JAVA.
FUNCTIONAL DESCRIPTION: This prototype interprets distributed Active XML documents. It can be used to deploy services defined as active documents over the web.

- Participants: Benoît Masson and Loïc Hélouët
- Contact: Loïc Hélouët
- URL: http://www.irisa.fr/sumo/Software/DAXML/

6.3. Sigali

FUNCTIONAL DESCRIPTION: Sigali is a model-checking tool that operates on ILTS (Implicit Labeled Transition Systems, an equational representation of an automaton), an intermediate model for discrete event systems. It offers functionalities for verification of reactive systems and discrete controller synthesis. The techniques used consist in manipulating the system of equations instead of the set of solutions, which avoids the enumeration of the state space. Each set of states is uniquely characterized by a predicate and the operations on sets can be equivalently performed on the associated predicates. Therefore, a wide spectrum of properties, such as liveness, invariance, reachability and attractivity, can be checked. Algorithms for the computation of predicates on states are also available. Sigali is connected with the Polychrony environment (Tea project-team) as well as the Matou environment (VERIMAG), thus allowing the modeling of reactive systems by means of Signal Specification or Mode Automata and the visualization of the synthesized controller by an interactive simulation of the controlled system.

- Contact: Hervé Marchand

6.4. SIMSTORS

Simulator for stochastic regulated systems
KEYWORDS: Simulation - Public transport - Stochastic models - Distributed systems
FUNCTIONAL DESCRIPTION: SIMSTORS is a software for the simulation of stochastic concurrent timed systems. The heart of the software is a variant of stochastic and timed Petri nets, whose execution is controlled by a regulation policy (a controller), or a predetermined theoretical schedule. The role of the regulation policy is to control the system to realize obbjectives or a schedule when it exists with the best possible precision. SIMSTORS is well adapted to represent systems with randomness, parallelism, tasks scheduling, and resources. It is currently in use within collaboration P22 with Asltom Transport, where it is used to model metro traffic and evaluate performance of regulation solutions. This software allows for step by step simulation, but also for efficient performance analysis of systems such as production cells or train systems. The initial implementation was released in 2015, and the software is protected by the APP.

In 2017, SIMSTORS has been extended along two main axes: on one hand, SIMSTORS models were extended to handle situations where shared resources can be occupied by more than one object (this is of paramount importance to represent conveyors, roads occupied by cars, or train tracks with smoothed scheduling allowing shared sections among trains) with priorities, constraint on their ordering and individual characteristics. This allows for instance to model vehicles with different speeds on a road, while handling safety distance constraints. On the other hand, SIMSTORS models were extended to allow control of stochastic nets based on decision rules that follow optimization schemes.

- Participants: Abd El Karim Kecir and Loïc Hélouët
- Contact: Loïc Hélouët
- URL: http://www.irisa.fr/sumo/Software/SIMSTORS/

6.5. Tipex

TImed Properties Enforcement during eXecution
KEYWORDS: Monitoring - Controller synthesis - Formal methods

FUNCTIONAL DESCRIPTION: We are implementing a prototype tool named Tipex (TImed Properties Enforcement during eXecution) for the enforcement of timed properties. Tipex is based on the theory and algorithms that we develop for the synthesis of enforcement monitors for properties specified by timed automata (TA). The prototype is developped in python, and uses the PyUPPAAL and DBMpyuppaal libraries of the UPPAAL tool . It is currently restricted to safety and co-safety timed property. The property provided as input to the tool is a TA that can be specified using the UPPAAL tool, and is stored in XML format. The tool synthesizes an enforcement monitor from this TA, which can then be used to enforce a sequence of timed events to satisfy the property. Experiments have been conducted on a set of case studies. This allowed to validate the architecture and feasibility of enforcement monitoring in a timed setting and to have a first assessment of performance (and to what extent the overhead induced by monitoring is negligible).

- Participants: Thierry Jéron, Srinivas Pinisetty and Hervé Marchand
- Contact: Thierry Jéron

7. New Results

7.1. Analysis and Verification of Quantitative Systems

7.1.1. Diagnosability

Participants : Hugo Bazille, Éric Fabre, Blaise Genest, Loïc Hélouët, Hervé Marchand, Engel Lefaucheux

7.1.1.1. Diagnosability of repairable faults.

Diagnosability (i.e., the existence of a diagnoser detecting faults in partially-observable systems) can be decided in polynomial time, relying on the so-called twin-machine construction. We have examined the case of repairable faults, and a notion of diagnosability that requires the detection of the fault before it is repaired. We have extended a contribution of 2016 to show that diagnosability of faults and of their repair could help counting the number of occurred faults. It was proved [51] that diagnosability with repair is a *PSPACE*-complete problem. We have completed this result, showing that the close notion of P-diagnosability (diagnosability of a fault even after it is repaired) is also *PSPACE*-complete [20].

7.1.1.2. Diagnosability degree of stochastic systems.

For stochastic systems, several diagnosability properties have been defined. The simplest one, also called A-diagnosability, characterizes the fact that after each fault, detection will almost surely occur. We have considered quantitative versions of the problem, to determine how much a system is diagnosable (when it is not diagnosable for sure). This amounts to characterizing the probability that a faulty run will lead to detection. We have proposed several notions of dignosability degree. Their derivation is generally *NP*-hard, but we have identified situations where complexity becomes polynomial. Besides, we have developed techniques to compute the different moments of the detection delay (mean, variance and upper moments). This allows one to compare systems with similar detection degrees, but that can react faster to faults. In some cases, one may be able to tune a system and trade diagnosability degree againts a faster detection. This approach also yields the distribution of fault location (in time) once detection takes place. Given the first moments of the detection delay, one is also able to compute (sometimes tight) bounds on the response time, for example to lower bound the probability that detection takes place at most T seconds/events after the fault [31].

7.1.1.3. The cost of diagnosis.

We addressed diagnosability and its cost for safe Petri nets. In [37] we have defined an energy-like cost model for Petri nets: transitions can consume or restore energy of the system. We then have defined a partial-order representation for state estimation, and extend the cost model and the capacities of diagnosers. Diagnosers are allowed to use additional energy to refine their estimations. Diagnosability is then seen as an energy game: checking whether disambiguation mechanisms are sufficient to allow diagnosability is in *2EXPTIME*, and one can also decide in *2EXPTIME* whether diagnosability under budget constraint holds.

7.1.2. Analysis of timed systems

Participants : Nicolas Markey, Loïc Hélouët

7.1.2.1. Determinizing timed automata.

In [35], we introduce a new formalism called *automata over a timed domain*, which generalizes timed automata; this formalism provides an adequate framework for determinization. In our formalism, determinization w.r.t. timed language is always possible at the cost of changing the timed domain. We give a condition for determinizability of automata over a timed domain *without changing the timed domain*, which allows us to recover several known determinizable classes of timed systems, such as strongly-non-zeno timed automata, integer-reset timed automata, perturbed timed automata, etc. Moreover, in the case of timed automata, this condition encompasses most determinizability conditions from the literature. Our aim now is to extend this work towards more efficient algorithms for monitoring timed systems.

7.1.2.2. Concurrent Timed Systems.

Time Petri nets (TPNs) are a classical extension of Petri nets with timing constraints attached to transitions, for which most verification problems are undecidable. We consider TPNs under a strong semantics with multiple enablings of transitions. This year, we have extened a work started in 2016, focusing on a structural subclass of unbounded TPNs, where the underlying untimed net is free choice, and showed that it enjoys nice properties in the timed setting under a multi-server semantics [46], [25]. In particular, we have showed that the questions of firability (whether a chosen transition can fire), and termination (whether the net has a non-terminating run) are decidable for this class. Next, we have considered the problem of robustness under guard enlargement and guard shrinking, i.e., whether a given property is preserved even if the system is implemented on an architecture with imprecise time measurement. For unbounded free choice TPNs with a multi-server semantics, we have show decidability of robustness of firability and of termination under both guard enlargement and shrinking.

7.2. Control of Quantitative Systems

7.2.1. Expressing and verifying properties of multi-agent systems

Participants : Ocan Sankur, Nicolas Markey

7.2.1.1. Admissible strategies in controller synthesis.

In game theory, a strategy is dominated by another one if the latter systematically yields a payoff as good as the former, while also yielding a better payoff in some cases. A strategy is admissible if it is not dominated. This notion is well-studied in game theory and is useful to describe the set of strategies that are "reasonable" (i.e., whose choice can be justified; here, no players would play a dominated strategy, since better strategies exist). Recent works studied this notion in graph games with omega-regular objectives and investigated its applications in controller synthesis. For multi-agent controller synthesis, admissibility can be used as a hypothesis on the behaviors of each agent, thus enabling a compositional reasoning framework for controller synthesis.

We continue the study of admissibility in controller synthesis with three developments detailed as follows:

- In [29], we study the characterization and computation of admissible strategies in multiplayer concurrent games. We study both deterministic strategies and randomized ones with almost-sure winning criteria. We prove that admissible strategies always exist in concurrent games, and we characterise them precisely. Then, when the objectives of the players are omega-regular, we show how to perform assume-admissible synthesis, i.e., how to compute admissible strategies that win (almost surely) under the hypothesis that the other players play admissible strategies only.

- In [30], we study timed games, which are multiplayer games played on arena defined by timed automata, which are a particular case of concurrent games. First, we show that admissible strategies may not exist in timed games with a continuous semantics of time, even for safety objectives. Second, we show that the discrete time semantics of timed games is better behaved w.r.t. admissibility: the existence of admissible strategies is guaranteed in that semantics. Third, we provide symbolic algorithms to solve the model-checking problem under admissibility and the assume-admissible synthesis problem for real-time non-zero sum n-player games for safety objectives.
- In [26], we study admissible strategies in games with imperfect information. We show that in stark contrast with the perfect information variant, admissible strategies are only guaranteed to exist when players have objectives that are closed sets. As a consequence, we also study decision problems related to the existence of admissible strategies for regular games as well as finite duration games.

7.2.1.2. Strategy dependences in Strategy Logic.

Strategy Logic (SL) is a very expressive logic for specifying and verifying properties of multi-agent systems: in SL, one can quantify over strategies, assign them to agents, and express properties of the resulting plays (using linear-time temporal logic). This defines a very expressive framework, encompassing e.g. (pure) Nash equilibria, or admissibility. Such a powerful framework has two drawbacks: first, SL model checking has non-elementary complexity; second, the exact semantics of SL is rather intricate, and may not correspond to what is expected.

In [49], we focus on *strategy dependences* in SL, by tracking how existentially-quantified strategies in a formula may (or may not) depend on other strategies selected in the formula. We study different kinds of dependences, refining a previous approach [52], and prove that they give rise to different satisfaction relations. In the setting where strategies may only depend on what they have observed, we identify a large fragment of SL for which we prove model checking can be performed in *2EXPTIME*.

7.2.2. Active diagnosis

Participants : Nathalie Bertrand, Blaise Genest, Engel Lefaucheux

7.2.2.1. Diagnosis and control of the degradation of probabilistic systems.

Active diagnosis is performed by a controler so that a system becomes diagnosable. In order to avoid the controler to degrade the funtionning of the system too much, one often provides it with an additional objective specifying the desired quality of service.

In the context of probabilistic systems, a possible specification consists in requiring a positive probability of infinite correct runs, referred to as the safe active diagnosis. In [42], we introduced two alternative specifications. First (γ, v)-correction of a system associates with an execution a correction value which depends on a discount factor γ, and the controler must ensure an expected correction value greater than a threshold v. Second, α-persistence requires that asymptotically, at each time unit, a proportion at least α of runs that were correct so far remain correct.

Our contributions are twofold. On the one hand, from a semantical viewpoint, we make explicit the equivalences and (non-)implications between the various notions, for finite-state systems as well as infinite-state ones. On the other hand, algorithmically, we establish the decidability frontier of the corresponding decision problems, and for decidable problems characterize their precise complexity, together with algorithms to design controlers.

7.2.2.2. Probabilistic Disclosure: Maximisation vs. Minimisation.

We consider opacity questions where an observation function provides to an external attacker a view of the states along executions and secret executions are those visiting some secret state from a fixed subset. Disclosure occurs when the observer can deduce from a finite observation that the execution is secret. In a probabilistic and non deterministic setting, where an internal agent can choose between actions, there are two points of view, depending on the status of this agent: the successive choices can either help the attacker trying to disclose the secret, if the system has been corrupted, or they can prevent disclosure as

much as possible if these choices are part of the system design. In the former situation, corresponding to a worst case, the disclosure value is the supremum over the strategies of the probability to disclose the secret (maximisation), whereas in the latter case, the disclosure is the infimum (minimisation). We address quantitative problems (relation between the optimal value and a threshold) and qualitative ones (when the threshold is zero or one) related to both forms of disclosure for a fixed or finite horizon. For all problems, we characterise their decidability status and their complexity. Surprisingly, while in maximisation problems optimal strategies may be chosen among deterministic ones, it is not the case for minimisation problems, but more minimisation problems than maximisation ones are decidable. These results appeared in [36].

7.2.3. Control and enforcement for quantitative systems

Participants : Nathalie Bertrand, Blaise Genest, Thierry Jéron, Hervé Marchand, Nicolas Markey

7.2.3.1. Qualitative determinacy and Decidability of Stochastic Games with Signals.

In [17], we consider two-person zero-sum stochastic games with signals, a standard model of stochastic games with imperfect information. The only source of information for the players consists of the signals they receive; they cannot directly observe the state of the game, nor the actions played by their opponent, nor their own actions.

We are interested in the existence of almost-surely winning or positively winning strategies, under reachability, safety, Büchi, or co-Büchi winning objectives, and the computation of these strategies when the game has finitely many states and actions. We prove two qualitative determinacy results. First, in a reachability game, either player 1 can achieve almost surely the reachability objective, or player 2 can achieve surely the dual safety objective, or both players have positively winning strategies. Second, in a Büchi game, if player 1 cannot achieve almost surely the Büchi objective, then player 2 can ensure positively the dual co-Büchi objective. We prove that players only need strategies with finite memory. The number of memory states needed to win with finite-memory strategies ranges from one (corresponding to memoryless strategies) to doubly exponential, with matching upper and lower bounds. Together with the qualitative determinacy results, we also provide fix-point algorithms for deciding which player has an almost-surely winning or a positively winning strategy and for computing an associated finite-memory strategy. Complexity ranges from *EXPTIME* to *2EXPTIME*, with matching lower bounds. Our fix-point algorithms also enjoy a better complexity in the cases where one of the players is better informed than their opponent.

Our results hold even when players do not necessarily observe their own actions. The adequate class of strategies, in this case, is mixed or general strategies (they are equivalent). Behavioral strategies are too restrictive to guarantee determinacy: it may happen that one of the players has a winning general strategy but none of them has a winning behavioral strategy. On the other hand, if a player can observe their actions, then general, mixed, and behavioral strategies are equivalent. Finite-memory strategies are sufficient for determinacy to hold, provided that randomized memory updates are allowed.

7.2.3.2. Average-energy games.

In [34], we consider average-energy games, where the goal is to minimize the long-run average of the accumulated weight (seen as an *energy level*) in a two-player game on a finite-state weighted automaton. Decidability of average-energy games with a lower-bound constraint on the energy level (but no upper bound) is an open problem; in particular, there is no known upper bound on the memory that is required for winning strategies.

By reducing average-energy games with lower-bounded energy to infinite-state mean-payoff games and analyzing the frequency of low-energy configurations, we show an almost tight doubly-exponential upper bound on the necessary memory, and that the winner of average-energy games with lower-bounded energy can be determined in doubly-exponential time. We also prove *EXPSPACE*-hardness of this problem.

Finally, we consider multi-dimensional extensions of all types of average-energy games: without bounds, with only a lower bound, and with both a lower and an upper bound on the energy. We show that the fully-bounded version is the only case to remain decidable in multiple dimensions.

7.2.3.3. Runtime enforcement.

The journal paper [23] details our work about predictive runtime enforcement, done in collaboration with University Aalto (Finland) and Inria CORSE/LIG Grenoble.

Runtime enforcement (RE) is a technique to ensure that the (untrustworthy) output of a black-box system satisfies some desired properties. In RE, the output of the running system, modeled as a sequence of events, is fed into an enforcer. The enforcer ensures that the sequence complies with a certain property, by delaying or modifying events if necessary. This paper deals with predictive runtime enforcement, where the system is not entirely black-box, but we know something about its behavior. This a priori knowledge about the system allows to output some events immediately, instead of delaying them until more events are observed, or even blocking them permanently. This in turn results in better enforcement policies. We also show that if we have no knowledge about the system, then the proposed enforcement mechanism reduces to standard (non-predictive) runtime enforcement. All our results related to predictive RE of untimed properties are also formalized and proved in the Isabelle theorem prover. We also discuss how our predictive runtime enforcement framework can be extended to enforce timed properties.

The journal paper [24], done in collaboration with LaBRI Bordeaux and Inria Corse/LIG Grenoble, deals with runtime enforcement of untimed and timed properties with uncontrollable events. Runtime enforcement consists in defining and using mechanisms that modify the executions of a running system to ensure their correctness with respect to a desired property. We introduce a framework that takes as input any regular (timed) property described by a deterministic automaton over an alphabet of events, with some of these events being uncontrollable. An uncontrollable event cannot be delayed nor intercepted by an enforcement mechanism. Enforcement mechanisms should satisfy important properties, namely soundness, compliance, and optimality—meaning that enforcement mechanisms should output as soon as possible correct executions that are as close as possible to the input execution. We define the conditions for a property to be enforceable with uncontrollable events. Moreover, we synthesise sound, compliant, and optimal descriptions of runtime enforcement mechanisms at two levels of abstraction to facilitate their design and implementation.

7.2.3.4. Control of logico-numerical systems.

In paper [32], we have targeted the problem of the safe control of reconfigurations in component-based software systems, where strategies of adaptation to variations in both their environment and internal resource demands need to be enforced. In this context, the computing system involves software components that are subject to control decisions. We have approached this problem under the angle of discrete-event systems (DES), involving properties on events observed during the execution (e.g., requests of computing tasks, work overload), and a state space representing different configurations such as activity or assemblies of components. We have considered in particular the potential of applying novel logico-numerical control techniques to extend the expressivity of control models and objectives, thereby extending the application of DES in component-based software systems. We elaborate methodological guidelines for the application of logico-numerical control based on a case-study, and validate the result experimentally.

7.2.4. Smart regulation for urban trains

Participants : Éric Fabre, Loïc Hélouët, Hervé Marchand, Karim Kecir

The regulation of subway lines consists in accomodating small random perturbations in transit times as well as more impacting incidents, by playing on continuous commands (transit times and dwell times) and by making more complex decisions (insertions or extractions of trains, changes of missions, overpassing, shorter returns, etc.) The objectives are multiple: ensuring the regularity and punctuality of trains, adapting to transportation demand, minimizing energy consumption, etc. We have developed an event-based control strategy that aims at equalizing headways on a line. This distributed control strategy is remarquably robust to perturbations and reactive enough to accomodate train insertions/extractions. We have integrated this control startegy to our SIMSTORS software. We have also developed another approach based on event graphs in order to optimally interleave trains at a junction. We started investigating new predictive control policies based of optimisation of criteria in forecast schedules [43].

In [47], we have extended a work started in 2016, that considers realizability of schedules by metro systems. Schedules are defined as high-level views of desired executions of systems, and represented as partial orders decorated with timing constraints. Train networks are modeled as stochastic time Petri nets (STPN) with an elementary (1-bounded) semantics. We have proposed a notion of time processes to give a partial-order semantics to STPNs. We then have considered Boolean realizability: a schedule S is realizable by a net N if S embeds in a time process of N that satisfies all its constraints. However, with continuous time domains, the probability of a time process with exact dates is null. We thus consider probabilistic realizability up to α time units, that holds if the probability that N realizes S with constraints enlarged by α is strictly positive. Upon a sensible restriction guaranteeing time progress, Boolean and probabilistic realizability of a schedule can be checked on the finite set of symbolic prefixes extracted from a bounded unfolding of the net. We give a construction technique for these prefixes and show that they represent all time processes of a net occurring up to a given maximal date. We then show how to verify existence of an embedding and compute the probability of its realization. The technique has then been illustrated by a concrete example, namely deciding wheter a simple flip-flop shunting mechanism suffices to route trains in appropriate direction when delays can occur in trips or during stops at stations. We have also conducted a series of experiment [28] with the SIMSTORS tool to obtain statistics, and show feasibiliy of Key Performance Indicators (KPIs) evaluation with this formal model.

A second line of research relates to the development of new regulation strategies. New techniques were derived to equalize headways of trains along a line, and thus improve regularity and resilience to perturbations. A distributed control strategy was developed, easily implementable in existing rule engines. Simulations have proved the efficiency of this technique on orbital lines. We have also developed a global regulation approach based on timed event graphs. In this setting, control is event-based: a command is issued each time a train crosses a control point, but it takes into account information along the whole line and for a finite time horizon. This amounts to adapting the whole time-table for any new event in the system. This approach has been proved to perform well at junctions (on computer simulations), where randomly spaced trains arriving from two branches must be correctly interleaved at the junction of the two lines, while at the same time train intervals must be equalized in all branches. We are now working on the combinatorial aspects of the question, in order to reduce energy consumption (by synchronizing arrivals and departures of trains), and in order to allow for insertions/extractions and reorderings of trains.

Several patents are in preparation for this activity.

7.3. Management of Large Distributed Systems

7.3.1. Analysis and synthesis of distributed systems

Participants : Éric Badouel, Thierry Jéron, Hervé Marchand, The Anh Pham

7.3.1.1. Control of Distributed Systems.

In [40], we have extended our examination of decentralized discrete-event-system architectures that use exclusive or (XOR) as the fusion rule to reach control decisions. A characterization of XOR inference-observable languages has been provided. Additionally, XOR observability is defined for languages that are not inference-observable but are distributed-observable.

7.3.1.2. Verification of distributed applications

In the context of IPL HAC-SPECIS, in collaboation with Martin Quinson (Myriads Inria project team) we are interested in the verification of real distributed applications.

In the conference paper [38] we explain the current status of the tool SimGridMC used for the verification of MPI applications. SimGridMC (also dubbed Mc SimGrid) is a stateful Model Checker for MPI applications. It is integrated to SimGrid, a framework mostly dedicated to predicting the performance of distributed applications. We describe the architecture of McSimGrid, and show how it copes with the state space explosion problem using Dynamic Partial Order Reduction and State Equality algorithms. As case studies we show how SimGrid can enforce safety and liveness properties for MPI applications, as well as global invariants over communication patterns.

7.3.2. Analysis of parameterized systems

Participants : Nathalie Bertrand, Éric Fabre, Blaise Genest, Matthieu Pichené, Ocan Sankur

7.3.2.1. Parameterized Verification of a time-synchronization protocol.

In [41], we consider distributed timed systems that implement leader-election protocols, which are at the heart of clock-synchronization protocols. We develop abstraction techniques for parameterized model checking of such protocols under arbitrary network topologies, where nodes have independently-evolving clocks. We apply our technique for model checking the root election part of the flooding time-synchronisation protocol (FTSP), and obtain improved results compared to previous work. We model-check the protocol for all topologies in which the distance to the node to be elected leader is bounded by a given parameter.

7.3.2.2. Controlling population models.

In [33], we introduce a new setting where a population of agents, each modelled by a finite-state system, are controlled uniformly: the controller applies the same action to every agent. The framework is largely inspired by the control of a biological system, namely a population of yeasts, where the controller may only change the environment common to all cells. We study a synchronisation problem for such populations: no matter how individual agents react to the actions of the controller, the controller aims at driving all agents synchronously to a target state. The agents are naturally represented by a non-deterministic finite state automaton (NFA), the same for every agent, and the whole system is encoded as a 2-player game. The first player (Controller) chooses actions, and the second player (Agents) resolves non-determinism for each agent. The game with m agents is called the m-population game. This gives rise to a parameterized control problem (where control refers to 2-player games), namely the population control problem: can Controller control the m-population game for all $m \in \mathbb{N}$, whatever Agents does?

In this work, we prove that the population control problem is decidable, and it is an *EXPTIME*-complete problem. As far as we know, this is one of the first results on parameterized control. Our algorithm, not based on cut-off techniques, produces winning strategies which are symbolic, that is, they do not need to count precisely how the population is spread between states. We also show that if there is no winning strategy, then there is a population size M such that Controller wins the m-population game if, and only if, $m \leq M$. Surprisingly, M can be doubly-exponential in the number of states of the NFA, with tight upper and lower bounds.

7.3.2.3. Handling large biological systems.

This year, we propose to use approximated probabilistic distribution to handle large homogeneous populations of cells [39]. Beyond classical approximations, we propose to use the Chow-Liu tree representation, based on *non-disjoint* clusters of two variables. Our experiments show that our proposed approximation scheme is more accurate than existing ones to model probability distributions deriving from biopathways, while requiring a minimal complexity overhead.

To handle *dynamics* of a population of cells governed by biopathways, we develop *coarse-grained* abstractions of the biological pathways [21], and more precisely *Dynamic Bayesian Networks* (DBNs). We show that simulating a DBN is much faster than simulating the fine-grained model it abstracts, for comparable prediction performances.

We also explore the approximate inference problem of DBNs, that is, *computing* the probability distributions at every time point given the initial distribution at time 0. We evaluate several classical approximate inference algorithms for DBNs, and compare with a new method we propose, which consists in using the Chow-Liu tree approximation to represent distributions at each time step. It is very accurate, yet efficient according to experiments we report. We finally provide an error analysis of this approximate inference algorithm [39].

7.4. Data-Driven Systems

7.4.1. Incremental process discovery using Petri-net synthesis.

Participants : Éric Badouel

In [16], we present an incremental process discovery using Petri-net synthesis. Process discovery aims at constructing a model from a set of observations given by execution traces (a log). Petri nets are a preferred target model in that they produce a compact description of the system by exhibiting its concurrency. This article presents a process-discovery algorithm using Petri-net synthesis, based on the notion of region introduced by A. Ehrenfeucht and G. Rozenberg, and using techniques from linear algebra. The algorithm proceeds in three successive phases which make it possible to find a compromise between the ability to infer behaviours of the system from the set of observations while ensuring a parsimonious model, in terms of fitness, precision and simplicity. All used algorithms are incremental which means that one can modify the produced model when new observations are reported without reconstructing the model from scratch.

7.4.2. An artifact model with imprecision and uncertainty

Participants : Éric Badouel, Loïc Hélouët

In the context of the HeadWork ANR project, we started investigating how complex workflows can be defined to handle uncertainty, and use joint knowledge of pools of user to build correct information. The solution proposed so far is a variant of business artifact managing fuzzy datasets. As there are several ways to reach an acceptable final and sufficiently precise dataset, we started investigating equivalence of complex workflows with partial information to allow refinement, enhance performance of data collection, with mastered precision loss.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. ADR Softwarization of Everything

Joint Nokia-Inria research lab: Several researchers of SUMO are involved in the joint research lab of Nokia Bell Labs France and Inria, in a common research team called "Softwarization of Everything". The objective of this joint team is to design programming and management methods for software defined networks. Several other Inria teams take part to this group: Convecs, Diverse, Spades. Within this team, SUMO focuses on the management of reconfigurable systems, both at the edge (IoT based applications) and in the core (e.g. virtualized IMS systems). In particular, we focus on control and diagnosis issues for such systems.

8.1.2. Alstom P22

Joint Alstom-Inria research lab: Several researchers of SUMO are involved in the joint research lab of Alstom and Inria, in a common research team called P22. On Alstom side, this joint research team involves researchers of the ATS division (Automatic Train Supervision). The objective of this joint team is to evaluate regulation policies of urban train systems, to assess their robustness to perturbations and failures, to design more efficient regulation policies and finally to provide decision support for human regulators. The project started in march 2014. A second phase of the project started in 2016, for a duration of three years. This covers in particular the CIFRE PhD of Karim Kecir.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR STOCH-MC: Model-Checking of Stochastic Systems using approximated algorithms (2014-2018)

- web site at http://perso.crans.org/~genest/stoch.html.
- Led by Blaise Genest (SUMO);

- Participants: Nathalie Bertrand, Blaise Genest, Éric Fabre, Matthieu Pichené;
- Partners: Inria Project Team CONTRAINTES (Rocquencourt), LaBRI (Bordeaux), and IRIF (Paris).

The aim of STOCH-MC is to perform model-checking of large stochastic systems, using controlled approximations. Two formalisms will be considered: Dynamic Bayesian Networks, which represent compactly large Markov Chains; and Markov Decision Processes, allowing non deterministic choices on top of probabilities.

9.1.2. ANR HeadWork: Human-Centric Data-oriented WORKflows (2016-2020)

- web site at http://headwork.gforge.inria.fr/
- Led by David Gross-Amblard (Université Rennes 1);
- Participants : Loïc Hélouët, Éric Badouel;
- Partners: Inria Project-Teams Valda (Paris), DRUID (Rennes) SUMO (Rennes), LINKs (Lille), MNHN, Foule Factory.

The objective of this project is to develop techniques to facilite development, deployment, and monitoring of crowd-based participative applications. This requires handling complex workflows with multiple participants, incertainty in data collections, incentives, skills of contributors, ... To overcome these challenges, Headwork will define rich workflows with multiple participants, data and knowledge models to capture various kind of crowd applications with complex data acquisition tasks and human specificities. We will also address methods for deploying, verifying, optimizing, but also monitoring and adapting crowd-based workflow executions at run time.

9.1.3. IPL HAC-SPECIS: High-performance Application and Computers, Studying PErformance and Correctness In Simulation (2016-2020)

- web site at http://hacspecis.gforge.inria.fr/
- Led by Arnaud Legrand (Inria Rhône-Alpes)
- Participants: Thierry Jéron, The Anh Pham.
- Partners: Inria project-teams Avalon (Lyon), POLARIS (Grenoble), HiePACS, STORM (Bordeaux), MExICo (Saclay), MYRIADS, SUMO (Rennes), VeriDis (Nancy).

The Inria Project Lab HAC-SPECIS (High-performance Application and Computers, Studying PErformance and Correctness In Simulation, 2016-2020: http://hacspecis.gforge.inria.fr/) is a transversal project internal to Inria. The goal of the HAC SPECIS project is to answer the methodological needs raised by the recent evolution of HPC architectures by allowing application and runtime developers to study such systems both from the correctness and performance point of view. Inside this project, we collaborate with Martin Quinson (Myriads team) on the dynamic formal verification of high performance runtimes and applications. The PhD of The Anh Pham is granted by this project.

This year we have been mainly intrested in dynamic partial-order-reduction methods that allow to reduce the explored state space, and a first prototype implementation of an existing method that combines DPOR with true-concurrency models.

9.1.4. CNRS INS2I JCJC SensAs (2017)

- Led by Ocan Sankur (SUMO).
- Participants: Ocan Sankur
- Partners: Benjamin Monmege, Pierre-Alain Reynier (Université Aix-Marseille).

Model-checking allows one to analyse the reliability of critical systems. There is currently an ongoing effort to extend formal verification and synthesis techniques to check non-functional properties such as performance, energy consumption or robustness, that are particularly important for real-time systems. SensAS is a project whose objective is to develop techniques to analyse the sensitivity of such systems with formal tools. In this context, a nominal behaviour, described with a deterministic timed automaton, is submitted to nondeterministic or stochastic perturbations. We seek then to quantify the variability of perturbed behaviours, giving formal guarantees on the computed result.

9.1.5. National informal collaborations

The team collaborates with the following researchers:

- Arnaud Sangnier (IRIF, UP7-Diderot) on the parameterized verification of probabilistic systems;
- François Laroussinie (IRIF, UP7-Diderot) on logics for multi-agent systems;
- Béatrice Bérard (LIP6) on problems of opacity and diagnosis, and on problems related to logics and partial orders for security;
- Serge Haddad (Inria team MExICo, LSV, ENS Paris-Saclay) on opacity and diagnosis;
- Patricia Bouyer (LSV, ENS Paris-Saclay) on the analysis of probabilistic timed systems and quantitative aspects of verification;
- Stefan Haar and Thomas Chatain (Inria team MExICo, LSV, ENS Paris-Saclay) on topics related to concurrency and time, and to modeling and verification of metro networks, multimodal systems and passenger flows;
- Éric Rutten and Gwenaël Delaval (Inria team Ctrl-A, LIG, Université Grenoble-Alpes) on the control of reconfigurable systems as well as making the link between Reax and Heptagon/BZR (http://bzr.inria.fr/);
- Didier Lime, Olivier H. Roux (LS2N Nantes) on topics related to stochastic and timed nets;
- Loïg Jezequel (LS2N Nantes) on topics related to stochastic and timed nets, and on distributed optimal planning;
- Yliès Falcone (CORSE LIG/Inria Grenoble) and Antoine Rollet (LaBRI Bordeaux) on the enforcement of timed properties;

9.2. International Initiatives

9.2.1. Inria Associate Teams Not Involved in an Inria International Labs

9.2.1.1. QuantProb

- Title: Quantitative analysis of non-standard properties in probabilistic models
- International Partner (Institution - Laboratory - Researcher):

  Technical University of Dresde (Germany) - Faculty of Computer Science - Christel Baier
- Start year: 2016
- See also: http://www.irisa.fr/sumo/QuantProb/
- Quantitative information flow and fault diagnosis share two important characteristics: quantities (in the description of the system as well as in the properties of interest), and users partial knowledge. Yet, in spite of their similar nature, different formalisms have been proposed. Beyond these two motivating examples, defining a unified framework can be addressed by formal methods. Formal methods have proved to be effective to verify, diagnose, optimize and control qualitative properties of dynamic systems. However, they fall short of modelling and mastering quantitative features such as costs, energy, time, probabilities, and robustness, in a partial observation setting. This project proposal aims at developing theoretical foundations of formal methods for the quantitative analysis of partially observable systems.

9.2.2. Inria International Partners

9.2.2.1. Informal International Partners

The team collaborates with the following researchers:

- Jean-François Raskin, Gilles Geeraerts (Université Libre de Bruxelles, Belgium) on multiplayer game theory and synthesis;
- Thomas Brihaye (UMons, Belgium) on the verification of stochastic timed systems;

- Mickael Randour (UMons, Belgium) on quantitative games for synthesis;
- Kim G. Larsen (Aalborg University, Denmark) on quantitative timed games, and on topics related to urban train systems modeling;
- Josef Widder, Igor Konnov and Marijana Laźic (TU Wien, Austria) on the automated verification of randomized distributed algorithms.
- John Mullin (Polytechnique Montréal, Canada), on topics related to security and opacity;
- S. Akshay (IIT Bombay, India) on topics related to timed concurrent models;
- Andrea D'ariano (University Roma Tre, Italy), on topics related to train regulation;
- Stavros Tripakis, Srinivas Pinisetty (Aalto University, Finland) on runtime verification and enforcement.

9.3. International Research Visitors

9.3.1. Visits of International Scientists

- Laurie Ricker visited the SUMO team for 2 months in May-June 2017.

9.3.1.1. Internships

- M2 Internship of Aina Toky Rasoamanana, Feb-July 2017, Nathalie Bertrand and Nicolas Markey
- L3 Internship of Balasubramanian A.R., May-July 2017, Nathalie Bertrand and Nicolas Markey

9.3.2. Visits to International Teams

9.3.2.1. Research Stays Abroad

- Éric Badouel made in September 2017 a one-month visit to Luca Bernardinello and Lucia Pomello from Milan University, and Carlo Ferigato from EJCR at Ispra. A work has been initiated on computer tools for the coordination of debates (from open citizen debates to parliamentary debates) and for managing the related documents (minutes, syntheses, ...) in an open data perspective.
- Engel Lefaucheux spent 6 weeks (May-June 2017) in Cagliari, working with Alessandro Giua and Carla Seatzu on the diagnosis of stochastic Petri nets.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Éric Badouel was the scientific chair of CRI 2017.
- Hervé Marchand is member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. Hervé Marchand is member of the steering committee of MSR (modélisation de systèmes réactifs) since 2012 and became president of this steering in November 2017;
- Nathalie Bertrand and Nicolas Markey are members of the steering committee of the Summer School MOVEP ("*Modelisation et Vérification des Processus Parallèles*").

10.1.1.2. Member of the Organizing Committees

- Thierry Jéron is member of the steering committee of FMF 2017 (Formal Methods Forum), a forum gathering people from academia and industry and dedicated to the use of formal methods. It is held in Toulouse and, since this year, retransmitted in Grenoble, Saclay and Rennes. Two sessions took place in 2017, in January on the theme "Formal methods and cybersecurity" and in October about "Autonomous vehicles and formal methods".

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

- Nathalie Bertrand was PC co-chair with Luca Bortolussi of QEST'2017, the 14th International Conference on Quantitative Evaluation of Systems, held in Berlin in September 2017 [45].

10.1.2.2. Member of the Conference Program Committees

- Éric Badouel was member of the program committees of VECOS 2017, ATAED 2017 and CRI 2017.
- Nathalie Bertrand was member of the PC of the following conferences: LICS 2017, FCT 2017, MSR 2017.
- Blaise Genest was a PC member of ATVA 2017;
- Thierry Jéron served on the Program Committees of the following international conferences: SAC-SVT 2017 and SAC-SVT 2018.
- Hervé Marchand served on the Program Committees of MSR 2017, Wodes 2018, CDC 2017, CCTA 2017.
- Nicolas Markey was a PC member of ATVA 2017, FORMATS 2017, SR 2017.
- Ocan Sankur was a PC member of SR 2017 and SYNT 2017.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

- Éric Badouel is co-editor-in-Chief of ARIMA Journal.

10.1.4. Invited Talks

- Nathalie Bertrand was invited to give a talk at the workshop organized for the 20 years of LSV (ENS Cachan) in May 2017. She was also invited to talk at the workshop OPCT (Open Problems in Concurrency) in June 2017 at IST Vienna (Austria).
- Hervé Marchand gave an invited talk during the conference of MSR (November 2017) titled *Contribution to the Analysis of Discrete Event Systems* as well as during the workshop "30 years of the Ramadge-Wonham Theory of Supervisory Control: A Retrospective and Future Perspectives" at the CDC conference in December 2017 titled *Opacity and Supervisory Control*.
- Nicolas Markey gave an invited talk about *Temporal logics for multi-agent systems* at MFCS 2017, Aalborg (Denmark), in August 2017 [27].

10.1.5. Leadership within the Scientific Community

- Since September 2017, Nathalie Bertrand is, together with Pierre-Alain Reynier, co-head of the *Groupe de Travail Verif* belonging to the *GDR Informatique Mathématique* (GDR-IM).

10.1.6. Research Administration

- Éric Badouel is the co-director (with Moussa Lo, UGB, Saint-Louis du Sénégal) of LIRIMA, the Inria International Lab for Africa. He is scientific officer for the African and Middle-East region at Inria European and International Partnership Department and member of the executive board of GIS SARIMA.
- Nathalie Bertrand is elected member of the *Conseil National des Universités*, section 27 (computer science).
- Nathalie Bertrand, Loïc Hélouët and Ocan Sankur organize the weekly seminar 68NQRT at IRISA (40 talks each year).

- Éric Fabre is the co-director (with Olivier Audouin, Nokia) of the joint lab of Nokia Bell Labs France and Inria. The lab has been running for 9 years and started in Nov. 2017 its 3rd phase of joint research teams. A series of 6 new teams just started, for a duration of 4 years. They cover topics like network virtualization, network management, information theory, (distributed) machine learning, network security. SUMO is involved in the joint team "Softwarization of Everything".
- Loïc Hélouët is a representative of rank-B researchers in the *Comité de Centre* of Inria Rennes. He is also part of the bureau of the Comité de Centre. He leads the P22 projects with Alstom transports and is responsible for Workpackage 2 of the Headwork ANR project.
- Thierry Jéron is Member Committee Substitute for COST IC1402 ARVI (Runtime Verification beyond Monitoring). He is member of the IFIP Working Group 10.2 on Embedded Systems. He is member of the COS Prospective of Irisa Rennes and member of the *Comité de Centre* of Inria Rennes. Since 2016 he is *référent chercheur* for the Inria-Rennes research center.
- Hervé Marchand is chairman of the CUMI in Rennes and member of the ADT commission in Rennes.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

- Licence: Nathalie Bertrand, Advanced Algorithms (ALGO2), 20h, L3, Univ Rennes 1, France;
- Licence: Loïc Hélouët, JAVA and algorithmics, L2, 40h, INSA de Rennes, France.
- Licence: Loïc Hélouët, practical studies (development of a small project), 8h, INSA de Rennes, France.
- Master : Nathalie Bertrand, Language Theory; Algorithms, 15h, Agrégation, ENS Rennes, France;
- Master: Éric Fabre, Models and Algorithms for Distributed Systems (MADS), 10h, M2, Univ Rennes 1, France;
- Master: Éric Fabre, Information Theory, 15h, M1, ENS Rennes, France.
- Master: Blaise Genest, Verification of Complex Systems (CSV), 10h, M2, Univ. Rennes 1, France;
- Master: Loïc Hélouët, Algorithms; complexity, 8h, Agrégation, ENS Rennes, France;
- Master: Loïc Hélouët, Nathalie Bertrand, Ocan Sankur, supervision of 3 students in M1 SIF (2017-2018).
- Master: Nicolas Markey, Verification of Complex Systems (CSV), 10h, M2, Univ Rennes 1, France;
- Master: Nicolas Markey, Algorithms for graphs, 3h, Agrégation, ENS Rennes, France;
- Master: Ocan Sankur, Lab sessions for the course on Foraml Analysis and Design (ACF), 22h, M1, Univ. Rennes 1, France.

10.2.2. Supervision

10.2.2.1. Defences

- HdR: Hervé Marchand, *Contribution to the Analysis of Discrete Event Systems* [15], Univ. Rennes 1. The defence took place on 6 June 2017.
- PhD: Bruno Karelovic, *Analyse quantitative des systèmes stochastiques – Jeux de priorité et population de chaînes de Markov*, Univ. Paris 7. The defence took place on 7 July 2017. Co-directed by Blaise Genest.

10.2.2.2. PhD in progress

- Robert Nsaibirni, *A Guarded Attribute Grammar Model for User centered Distibuted Collaborative Case Management: Case of the Disease Surveillance Process*, co-advised by Éric Badouel and Maurice Tchuenté (University of Yaoundé).

- Engel Lefaucheux, *Controlling information in probabilistic systems*, started September 2015, Nathalie Bertrand and Serge Haddad
- The Anh Pham, *Dynamic Formal Verification of High Performance Runtimes and Applications*, started Nov. 2016, Thierry Jéron and Martin Quinson (Myriads, Inria Rennes).
- Karim Kecir, *Régulation et robustesse des systèmes ferroviaires urbains*, planned May 2018, Loïc Hélouët and Pierre Dersin (Alstom).
- Hugo Bazille, *Information flows in quantitative dynamic systems*, started oct. 2016, Blaise Genest and Éric Fabre.
- Erij Elmajed, *Diagnosis of reconfigurable systems*, started March 2017, Éric Fabre and Armen Aghasaryan (Nokia).
- Sihem Cherrared, *Diagnosis of multi-tenant programmable networks*, started Dec. 2016, Éric Fabre, Gregor Goessler (Inria, Spades) and Sofiane Imadali (Orange).
- Victor Roussanaly, *Efficient verification of timed systems*, started Sep. 2017, Nicolas Markey and Ocan Sankur.

10.2.2.3. Master2 internship supervision

- Internship Aina Toky Rasoamanana, Feb-July 2017, Nathalie Bertrand and Nicolas Markey
- Internship Victor Roussanaly, Feb-June 2017, Nicolas Markey and Ocan Sankur

10.2.2.4. Other internship supervision

- L3 Internship of Balasubramanian A.R., May-July 2017, Nathalie Bertrand and Nicolas Markey
- L3 Internship of Thomas Mari, *Observation-based unfolding of Petri nets*, (May-July 2017)
- L3 Internship of Romain Boitard, *Design of interfaces for railway systems*, (April-June 2017)

10.2.3. Juries

10.2.3.1. Juries of PhD defences:

- Nicolas David, École Centrale Nantes, october 2017 : Nathalie Bertrand examiner;
- Thomas Geffroy, Univ. Bordeaux, december 2017: Nathalie Bertrand examiner;
- Ludovic Hofer, Univ. Bordeaux, november 2017: Blaise Genest examiner;
- Daniel Stan, École Normale Supérieure Paris-Saclay, march 2017: Nathalie Bertrand reviewer;
- Serge Tembo, Telecom Bretagne, January 2017: Éric Fabre examiner.

10.2.3.2. Other juries

- Ocan Sankur was in the computer science entrance exam jury of École Normale Supérieures and École Polytechnique.

10.3. Popularization

- Éric Badouel gave a talk at TEDx Lorient on digital democracy (coordination of citizen debates).

11. Bibliography

Major publications by the team in recent years

[1] S. AKSHAY, B. GENEST, L. HÉLOUËT, S. YANG. *Regular Set of Representatives for Time-Constrained MSC Graphs*, in "Information Processing Letters", 2012, vol. 112, n^{o} 14-15, pp. 592-598, http://hal.inria.fr/hal-00879825

[2] E. BADOUEL, M. A. BEDNARCZYK, A. M. BORZYSZKOWSKI, B. CAILLAUD, P. DARONDEAU. *Concurrent Secrets*, in "Discrete Event Dynamic Systems", 2007, vol. 17, n^{o} 4, pp. 425-446

[3] E. BADOUEL, L. BERNARDINELLO, P. DARONDEAU. *Petri Net Synthesis*, Springer, 2015, http://dx.doi.org/10.1007/978-3-662-47967-4

[4] A. BENVENISTE, E. FABRE, S. HAAR, C. JARD. *Diagnosis of Asynchronous Discrete Event Systems: A Net Unfolding Approach*, in "IEEE Transactions on Automatic Control", November 2003, vol. 48, n^{o} 5, pp. 714-727, RNRT project MAGDA [*DOI :* 10.1109/TAC.2003.811249], http://hal.inria.fr/inria-00638224

[5] N. BERTRAND, B. GENEST, H. GIMBERT. *Qualitative Determinacy and Decidability of Stochastic Games with Signals*, in "Proceedings of the 24th Annual IEEE Symposium on Logic in Computer Science (LICS'09)", Los Angeles, USA, August 2009, http://hal.archives-ouvertes.fr/hal-00356566

[6] N. BERTRAND, T. JÉRON, A. STAINER, M. KRICHEN. *Off-line Test Selection with Test Purposes for Non-Deterministic Timed Automata*, in "Logical Methods in Computer Science", October 2012, vol. 8, n^{o} 4:8, pp. 1-33, http://hal.inria.fr/hal-00744074

[7] J. DUBREIL, P. DARONDEAU, H. MARCHAND. *Supervisory Control for Opacity*, in "IEEE Transactions on Automatic Control", May 2010, vol. 55, n^{o} 5, pp. 1089-1100 [*DOI :* 10.1109/TAC.2010.2042008]

[8] E. FABRE, A. BENVENISTE. *Partial Order Techniques for Distributed Discrete Event Systems: why you can't avoid using them*, in "Journal of Discrete Events Dynamical Systems", 2007, vol. 17, n^{o} 3, pp. 357-403

[9] E. FABRE. *Trellis Processes: A Compact Representation for Runs of Concurrent Systems*, in "Journal of Discrete Event Dynamical Systems", 2007, vol. 17, n^{o} 3, pp. 267-306

[10] E. FABRE, L. JEZEQUEL. *Distributed optimal planning: an approach by weighted automata calculus*, in "Proceedings of the 48th IEEE Conference on Decision and Control (CDC'09)", 2009, pp. 211-216

[11] B. GAUDIN, H. MARCHAND. *An Efficient Modular Method for the Control of Concurrent Discrete Event Systems: A Language-Based Approach*, in "Discrete Event Dynamic System", 2007, vol. 17, n^{o} 2, pp. 179-209

[12] T. GAZAGNAIRE, B. GENEST, L. HÉLOUËT, P. THIAGARAJAN, S. YANG. *Causal Message Sequence Charts*, in "Theoretical Computer Science", 2009, 38 p. , EA DST, http://hal.inria.fr/inria-00429538

[13] C. JARD, T. JÉRON. *TGV: theory, principles and algorithms*, in "International Journal on Software Tools for Technology Transfer", 2005, vol. 7, n^{o} 4, pp. 297-315

[14] B. JEANNET, T. JÉRON, V. RUSU, E. ZINOVIEVA. *Symbolic Test Selection Based on Approximate Analysis*, in "Proceedings of the 11th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'05)", Edinburgh, UK, 2005, http://hal.inria.fr/inria-00564617

Publications of the year

Doctoral Dissertations and Habilitation Theses

[15] H. MARCHAND. *Contribution to the Analysis of Discrete Event Systems*, Université de Rennes 1, June 2017, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01589972

Articles in International Peer-Reviewed Journals

[16] E. BADOUEL, U. SCHLACHTER. *Incremental Process Discovery using Petri Net Synthesis*, in "Fundamenta Informaticae", June 2017, vol. 154, n° 1-4, pp. 1-13 [*DOI :* 10.3233/FI-2017-1548], https://hal.inria.fr/hal-01599760

[17] N. BERTRAND, B. GENEST, H. GIMBERT. *Qualitative Determinacy and Decidability of Stochastic Games with Signals*, in "Journal of the ACM (JACM)", October 2017, vol. 64, n° 5, pp. 1 - 48 [*DOI :* 10.1145/3107926], https://hal.inria.fr/hal-01635127

[18] A. BOHY, V. BRUYÈRE, J.-F. RASKIN, N. BERTRAND. *Symblicit algorithms for mean-payoff and shortest path in monotonic Markov decision processes*, in "Acta Informatica", September 2017, vol. 54, n° 6, pp. 545 - 587 [*DOI :* 10.1007/s00236-016-0255-4], https://hal.inria.fr/hal-01635132

[19] B. BÉRARD, L. HÉLOUËT, J. MULLINS. *Non-interference in partial order models*, in "ACM Transactions on Embedded Computing Systems (TECS)", 2017, vol. 16, n° 2, 34 p. [*DOI :* 10.1145/2984639], https://hal.inria.fr/hal-01379451

[20] E. FABRE, L. HÉLOUËT, E. LEFAUCHEUX, H. MARCHAND. *Diagnosability of Repairable Faults*, in "Discrete Event Dynamic Systems", June 2017, https://hal.inria.fr/hal-01646911

[21] S. K. PALANIAPPAN, F. BERTAUX, M. PICHENÉ, E. FABRE, G. BATT, B. GENEST. *Abstracting the dynamics of biological pathways using information theory: a case study of apoptosis pathway*, in "Bioinformatics", February 2017, vol. 33, n° 13, pp. 1980 - 1986, free access to online article: https://academic.oup.com/bioinformatics/article/33/13/1980/2996220/Abstracting-the-dynamics-of-biological-pathways?guestAccessKey=7083a393-ea30-4113-b5f9-816fb9b56287 [*DOI :* 10.1093/BIOINFORMATICS/BTX095], https://hal.inria.fr/hal-01547618

[22] S. PINISETTY, T. JÉRON, S. TRIPAKIS, Y. FALCONE, H. MARCHAND, V. PREOTEASA. *Predictive Runtime Verification of Timed Properties*, in "Journal of Systems and Software", October 2017, vol. 132, pp. 353 - 365 [*DOI :* 10.1016/J.JSS.2017.06.060], https://hal.inria.fr/hal-01666995

[23] S. PINISETTY, V. PREOTEASA, S. TRIPAKIS, T. JÉRON, Y. FALCONE, H. MARCHAND. *Predictive runtime enforcement*, in "Formal Methods in System Design", August 2017, vol. 51, n° 1, pp. 154 - 199 [*DOI :* 10.1007/s10703-017-0271-1], https://hal.inria.fr/hal-01647787

[24] M. RENARD, Y. FALCONE, A. ROLLET, T. JÉRON, H. MARCHAND. *Optimal Enforcement of (Timed) Properties with Uncontrollable Events*, in "Mathematical Structures in Computer Science", May 2017 [*DOI :* 10.1017/S0960129517000123], https://hal.archives-ouvertes.fr/hal-01262444

Invited Conferences

[25] S. AKSHAY, L. HÉLOUËT, R. PHAWADE. *Combining Free choice and Time in Petri Nets*, in "6th IFIP Working group on trends in Concurrency", Berlin, Germany, September 2017, Présentation dans un working group sans actes, https://hal.inria.fr/hal-01650751

[26] R. BRENGUIER, A. PAULY, J.-F. RASKIN, O. SANKUR. *Admissibility in Games with Imperfect Information*, in "CONCUR 2017 - 28th International Conference on Concurrency Theory", Berlin, Germany, LIPICs, September 2017, vol. 85 [*DOI :* 10.4230/LIPICS], https://hal.archives-ouvertes.fr/hal-01598152

[27] N. MARKEY. *Temporal Logics for Multi-Agent Systems*, in "MFCS 2017 - 42nd International Symposium on Mathematical Foundations of Computer Science", Aalborg, Denmark, August 2017 [*DOI :* 10.4230/LIPICS.MFCS.2017.84], https://hal.inria.fr/hal-01653855

International Conferences with Proceedings

[28] B. ADELINE, P. DERSIN, E. FABRE, L. HÉLOUËT, K. KECIR. *An efficient evaluation scheme for KPIs in regulated urban train systems*, in "RSSRail 2017 - International Conference on reliability, safety, and security of railway systems", Pistoia, Italy, A. FANTECHI, T. LECOMTE, A. ROMANOVSKY (editors), Lecture Notes in Computer Science, Springer, November 2017, n^{o} 10598, https://hal.inria.fr/hal-01646919

[29] N. BASSET, G. GEERAERTS, J.-F. RASKIN, O. SANKUR. *Admissiblity in Concurrent Games*, in "ICALP 2017 - 44th International Colloquium on Automata, Languages, and Programming", Warsaw, Poland, LIPICs, July 2017, vol. 80 [*DOI :* 10.4230/LIPICS.ICALP.2017.123], https://hal.archives-ouvertes.fr/hal-01598148

[30] N. BASSET, J.-F. RASKIN, O. SANKUR. *Admissible Strategies in Timed Games*, in "Models, Algorithms, Logics and Tools", aalborg, Denmark, Lecture Notes in Computer Science, July 2017, vol. 10460, https://hal.archives-ouvertes.fr/hal-01515874

[31] H. BAZILLE, E. FABRE, B. GENEST. *Diagnosability Degree of Stochastic Discrete Event Systems*, in "CDC 2017 - 56th IEEE Conference on Decision and Control", Melbourne, Australia, December 2017, pp. 1-6, https://hal.inria.fr/hal-01651232

[32] N. BERTHIER, F. ALVARES, H. MARCHAND, G. DELAVAL, E. RUTTEN. *Logico-numerical Control for Software Components Reconfiguration*, in "CCTA 2017 - IEEE Conference on Control Technology and Applications", Mauna Lani, HI, United States, IEEE, August 2017, pp. 1599 - 1606 [*DOI :* 10.1109/CCTA.2017.8062685], https://hal.inria.fr/hal-01644754

[33] N. BERTRAND, M. DEWASKAR, B. GENEST, H. GIMBERT. *Controlling a Population*, in "CONCUR 2017 - 28th International Conference on Concurrency Theory", Berlin, Germany, September 2017, pp. 1-23, https://hal.archives-ouvertes.fr/hal-01625661

[34] P. BOUYER, P. HOFMAN, N. MARKEY, M. RANDOUR, M. ZIMMERMANN. *Bounding Average-Energy Games*, in "FoSSaCS'17", Uppsala, Sweden, Proceedings of the 20th International Conference on Foundations of Software Science and Computation Structure (FoSSaCS'17), Springer, April 2017, vol. 10203, pp. 179-195 [*DOI :* 10.1007/978-3-662-54458-7_11], https://hal.archives-ouvertes.fr/hal-01566431

[35] P. BOUYER, S. JAZIRI, N. MARKEY. *On the determinization of timed systems*, in "FORMATS'17", Berlin, Germany, Proceedings of the 15th International Conferences on Formal Modelling and Analysis of Timed Systems (FORMATS'17), September 2017, vol. 10419, pp. 25-41 [*DOI :* 10.1007/978-3-319-65765-3 2], https://hal.archives-ouvertes.fr/hal-01566436

[36] B. BÉRARD, S. HADDAD, E. LEFAUCHEUX. *Probabilistic Disclosure: Maximisation vs. Minimisation* , in "FSTTCS 2017", Kanpur, India, December 2017 [*DOI :* 10.4230/LIPICS.FSTTXS.2017], https://hal.inria.fr/hal-01618955

[37] L. HÉLOUËT, H. MARCHAND. *On the cost of diagnosis with disambiguation*, in "QEST 2017", Berlin, France, 14th International Conference on Quantitative Evaluation of SysTems (QEST 2017), September 2017, https://hal.inria.fr/hal-01537796

[38] T. A. PHAM, T. JÉRON, M. QUINSON. *Verifying MPI Applications with SimGridMC*, in "Correctness 2017 - First International Workshop on Software Correctness for HPC Applications", Denver, United States, November 2017 [*DOI :* 10.1145/3145344.3145345], https://hal.inria.fr/hal-01632421

[39] M. PICHENÉ, S. K. PALANIAPPAN, E. FABRE, B. GENEST. *Non-Disjoint Clustered Representation for Distributions over a Population of Cells (poster)*, in "CMSB 2017", Darmstadt, Germany, CMSB 2017 - 15th International Conference on Computational Methods in Systems Biology, Springer, 2017, vol. LNCS/LNBI, n^{o} 10545, pp. 324-326, https://hal.archives-ouvertes.fr/hal-01625665

[40] L. RICKER, T. F. LIDBETTER, H. MARCHAND. *Inferencing and beyond: further adventures with parity-based architectures for decentralized discrete-event systems*, in "20th World Congress The International Federation of Automatic Control", Toulouse, France, July 2017, 6 p. , https://hal.inria.fr/hal-01590438

[41] O. SANKUR, J.-P. TALPIN. *An Abstraction Technique For Parameterized Model Checking of Leader Election Protocols: Application to FTSP*, in "23rd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)", Uppsala, Sweden, Lecture Notes in Computer Science, April 2017, vol. 10206, https://hal.archives-ouvertes.fr/hal-01431472

National Conferences with Proceedings

[42] *Best Paper*
N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Diagnostic et contrôle de la dégradation des systèmes probabilistes*, in "MSR 2017 - Modélisation des Systèmes Réactifs", Marseille, France, November 2017, https://hal.inria.fr/hal-01618922.

Conferences without Proceedings

[43] K. KECIR, L. HELOUET, P. DERSIN, B. ADELINE, A. D'ARIANO. *From Reactive to Predictive Regulation in Metros*, in "ECSO 2017 : 2nd European Conference on Stochastic Optimization", Rome, Italy, September 2017, https://hal.inria.fr/hal-01646916

Scientific Books (or Scientific Book chapters)

[44] P. BOUYER, F. LAROUSSINIE, N. MARKEY, J. OUAKNINE, J. WORRELL. *Timed temporal logics*, in "Models, Algorithms, Logics and Tools: Essays Dedicated to Kim Guldstrand Larsen on the Occasion of His 60th Birthday", Lecture Notes in Computer Science, Springer, August 2017, vol. 10460, pp. 211-230 [*DOI :* 10.1007/978-3-319-65764-6_11], https://hal.archives-ouvertes.fr/hal-01566439

Books or Proceedings Editing

[45] N. BERTRAND, L. BORTOLUSSI (editors). *Proceedings of the 14th International Conference on Quantitative Evaluation of Systems (QEST 2017), Berlin, Germany, September 5-7, 2017*, 2017, https://hal.inria.fr/hal-01635134

Research Reports

[46] S. AKSHAY, L. HÉLOUËT, R. PHAWADE. *Combining Free choice and Time in Petri Nets*, Inria Rennes - Bretagne Atlantique, July 2017, https://hal.inria.fr/hal-01646913

[47] L. HÉLOUËT, K. KECIR. *Realizability of Schedules by Stochastic Time Petri Nets with Blocking Semantics: (Extended Version)*, Inria Rennes - Bretagne Atlantique, October 2017, https://hal.inria.fr/hal-01646920

Other Publications

[48] N. BERTRAND, M. DEWASKAR, B. GENEST, H. GIMBERT. *Controlling a Population*, July 2017, https://arxiv.org/abs/1707.02058 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01558029

[49] P. GARDY, P. BOUYER, N. MARKEY. *Dependences in Strategy Logic*, October 2017, https://arxiv.org/abs/1708.05849 - working paper or preprint, https://hal.archives-ouvertes.fr/hal-01609523

[50] V. JUGÉ, P. BOUYER-DECITRE, N. MARKEY. *Courcelle's Theorem Made Dynamic*, October 2017, https://arxiv.org/abs/1702.05183 - 14 pages, 4 figures. arXiv admin note: text overlap with arXiv:1610.00571, https://hal.archives-ouvertes.fr/hal-01615275

References in notes

[51] E. FABRE, L. HÉLOUËT, E. LEFAUCHEUX, H. MARCHAND. *Diagnosability of Repairable Faults*, in "13th International Workshop on Discrete Event Systems (WODES'16)", Xi'an, China, 2016, pp. 256–262

[52] F. MOGAVERO, A. MURANO, G. PERELLI, M. Y. VARDI. *Reasoning About Strategies: On the Model-Checking Problem*, in "ACM Transactions on Computational Logic", August 2014, vol. 15, n^{o} 4, pp. 34:1-34:47, http://dx.doi.org/10.1145/2631917