
IN PARTNERSHIP WITH:
**CNRS**

**Université Rennes 1**

Activity Report 2015

# Project-Team SUMO

## SUpervision of large MOdular and distributed systems

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:**

1.3. - Distributed Systems
2.3.2. - Cyber-physical systems
2.4.2. - Verification
4.5. - Formal methods for security
6.4. - Automatic control
7.1. - Parallel and distributed algorithms
7.3. - Operations research, optimization, game theory
7.4. - Logic in Computer Science
7.8. - Information theory

**Other Research Topics and Application Domains:**

1.1.9. - Bioinformatics
5.2.2. - Railway
6.2. - Network technologies

# 1. Members

**Research Scientists**

Éric Fabre [Team leader, Inria, Senior Researcher, HdR]
Éric Badouel [Inria, Researcher, HdR]
Nathalie Bertrand [Inria, Researcher, HdR]
Blaise Genest [CNRS, Researcher]
Loïc Hélouët [Inria, Researcher, HdR]
Thierry Jéron [Inria, Senior Researcher, HdR]
Hervé Marchand [Inria, Researcher]
Ocan Sankur [CNRS, Researcher, from Nov 2015]

**Engineer**

Nicolas Berthier [Inria, until Nov 2015, granted by ANR CTRL-GREEN project]

**PhD Students**

Paulin Fournier [Univ. Rennes I]
Karim Kecir [Univ. Rennes I, granted by CIFRE]
Engel Lefaucheux [Univ. Rennes I]
Matthieu Pichené [Inria, granted by ANR STOCH-MC and ARED Région Bretagne]
Srinivas Pinisetty [Inria, until Feb 2015, granted by ANR VACSIM project]

**Post-Doctoral Fellow**

Sucheendra Palaniappan [Inria]

**Visiting Scientists**

Samy Abbes [Associate Professor, on leave from Univ. Paris VII, from Mar 2015 until Aug 2015]
Christophe Morvan [External collaborator, Associate Professor at Univ. Paris Est]
Robert Nsaibirni [PhD student, University of Yaoundé I, from March to May 2015]
Shauna Laurene Ricker [Professor, on leave from Mount Allison University, until May 2015]

**Administrative Assistant**
Laurence Dinh [Inria]

**Others**
Achille Aknin [ENS Ulm, Intern, from Jun 2015 until Jul 2015]
Alexandre Blanche [ENS Rennes, Intern, from May 2015 until Jul 2015]
Miheer Dewaskar [Inria, Intern, from May 2015 until Jul 2015]
André Gueney [CNAM, Intern, from Apr 2015 until Sep 2015]

# 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 of 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 become 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. Discrete event systems approaches follow the same trend towards quantitative models. For diagnosis aspects, one is interested in the most likely explanations to observed failures, in the identification of the most informative tests to perform, in the optimal placement of sensors, and 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 build online a part of their model, on demand 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. Model expressivity and quantitative verification

The overall objective of this axis is to combine the quantitative aspects of models with a distributed/modular setting, while maintaining the tractability of verification and management objectives.

There is first an issue of modeling, to nicely weave time, costs and probabilities with concurrency and/or asynchronism. Several approaches are quite natural, as time(d) Petri nets, networks of timed automata, communicating synchronously or through FIFO, etc. But numerous bottlenecks remain. For example, so far, no probabilistic model nicely fits the notion of concurrency: there is no clean way to express that two components are stochastically independent between two rendez-vous.

Second, the models we want to manipulate should allow for quantitative verification. This covers two aspects: either the verification question is itself quantitative (compute an optimal scheduling policy) or boolean (decide whether the probability is greater than a threshold). 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 work around that we will explore.

In more details, our research program on this axis covers the following topics:

- the verification of distributed timed systems,
- the verification of large scale probabilistic (dynamic) systems, with a focus on approximation techniques for such systems,
- the evaluation of the opacity/diagnosability degree of stochastic systems,
- the design of modular testing methods for large scale modular systems.

## 3.2. Management of large distributed systems

The generic terms of "supervision" or "management" of distributed systems cover problems like control (and controller synthesis), diagnosis, sensor placement, planning, optimization, (state) estimation, parameter identification, testing, etc. These questions have both an offline and an online facet. The literature is abundant for discrete event systems (DES), even in the distributed case, and for some quantitative aspects of DES in the centralized case (for example partially observed Markov decision processes (POMDP), probabilistic diagnosis/diagnosers, (max,+) approaches to timed automata). And there is a strong trend driving formal methods approaches towards quantitative models and questions like the most likely diagnosis, control for best average reward or for best QoS, optimal sensor placement, computing the probability of failure (un)detection, estimating the average impact of some failure or of a decision, etc. This second research axis focuses on these issues, and aims at developing new concepts and tools to master some already existing large scale systems, as telecommunication networks, cloud infrastructures, web-services, etc. (see the Application Domains section).

The objective being to address large systems, our work will be driven by two considerations: how to take advantage of the modularity of systems, and how to best approximate/abstract too complex systems by more tractable ones. We mention below main topics we will focus on:

- Approximate management methods. We will explore the extension of ideas developed for Bayesian inference in large scale stochastic systems (such as turbo-algorithms for example) 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.
- Self-modeling, which consists in managing large scale systems that are known by their building rules, but which specific managed instance is only discovered at runtime, and on the fly. 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.

## 3.3. Data driven systems

The term data-driven systems refers to systems the behavior of which 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 (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 implemented systems designed in low-level languages (for instance BPEL (Business Process Execution Language)). These models should be able to encompass modularity, distribution, in a context where workflows and data aspects are tightly connected.
- provide tractable solutions for validation of models. Important questions that are frequently addressed (for instance safety properties or coverability) should not only remain decidable on our models, but also with a decent complexity.
- 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. Such declarative models are well accepted in business processes (Companies such

as IBM use their own model of business rules [55] to interact with their clients). Our approach is to design collaborative activities in terms of distributed structured documents, that can be seen as communicating rewriting systems. This modeling paradigm also includes models such as distributed Active XML [50], [53]. We think that distributed rewriting rules or attributed grammars can provide a practical but yet formal framework for maintenance, by providing a solution to update mandatory documentation during the lifetime of an artifact.

- address QoS management in large reconfigurable systems:

Data driven distributed systems such as web services often have constraints in terms of QoS. This calls for an analysis of quantitative features, and for reconfiguration techniques to meet QoS contracts. We will build from our experience on QoS contracts composition [56] and planning [49], [51] to propose optimization and reconfiguration schemes.

# 4. Application Domains

## 4.1. Telecommunication network management

The domain of autonomic network management, will remain an important playground for SUMO. It covers a wide variety of problems, ranging from distributed (optimal) control to distributed diagnosis, optimization, reconfiguration, provisioning, etc. We have a long experience in model-based diagnosis, in particular distributed (active) diagnosis, and have recently proposed promising techniques for self-modeling. It consists in building the model of the managed network on the fly, guided by the needs of the diagnosis algorithm. This approach allows one to deal with potentially huge models, that are only described by their construction grammar, and discovered at runtime. Another important research direction concerns the management of "multi-resolution" models, that can be considered at different granularity levels. This feature is central to network design, but has no appropriate modeling formalism nor management approaches. This is a typical investigation field for abstraction techniques. Technology is ahead of theory in this domain since networks are already driven or programmed through management policies, that assign high level objectives to an abstract view of the network, leaving open the question of their optimal implementation. As a last topic of investigation, today management issues are no longer isolated within one operator, but range accross several of them, up to the supported services, which brings game theory aspects into the picture.

## 4.2. Control of data centers

Data centers are another example of a large scale reconfigurable and distributed system: they are composed of thousands of servers on which Virtual Machines (VM) can be (de)activated, migrated, etc. depending on the requests of the customers, on the load of the servers and on the power consumption. Autonomic management functionalities already exist to deploy and configure applications in such a distributed environment. They can also monitor the environment and react to events such as failures or overloads and reconfigure applications and/or infrastructures accordingly and autonomously. To supervise these systems, Autonomic Managers (AM) can be deployed in order to apply administration policies of specific aspects to the different entities of a data center (servers, VM, web services, power supply, etc). These AMs may be implemented in different layers: the hardware level, the operating system level or the middleware level. Therefore several control loops may coexists, and they have to take globally consistent decisions to manage the trade-off between availability, performance, scalability, security and energy consumption. This leads to multi-criteria optimization and control problems in order to automatically derive controllers in charge of the coordination of the different AMs. We are relatively new on this topic, that will require more technical investment. But we are driven to it by both the convergence of IT and networking, by virtualization techniques that reach networks (see the growing research effort about network operating systems), and by the call for more automation in the management of clouds. We believe our experience in network management can help. Some members of the SUMO team are already involved in the ANR Ctrl-Green, which addresses the controller coordination problem. We are also in contact with the Myriads team, which research interests moved from OS for grids/clouds to autonomic methods. This is supported as well by the activities of b<>com, the local IRT, where some projects in cloud management and in networking may start joint activities.

## 4.3. Web services and distributed active documents

Data centric systems are already deployed, and our goal is not to design new languages, architectures, or standards for them, but rather to propose techniques for the verification and monitoring of existing systems. A bottleneck is the complexity and heterogeneity of web-based systems, that make them difficult to model and analyze. However, one can still hope for some lightweight verification or monitoring techniques for some specific aspects, for example to check the absence of conflict of interest in a transaction system, to verify (off line) and maintain (on line) the QoS, to prevent security breaches, etc. Safety aspects of Web Services have received little attention; any progress in that area would be useful. Besides, modeling issues are central for some applications of data centric systems. Collaborative work environments with shared active documents can be found in many domains ranging from banking, maintenance of critical systems, webstores... We think that models for data driven systems can find applications in most of these areas. Our approach will be to favor purely declarative approaches for the specification of such collaborative environments. We have contacts with Centre Pasteur in Yaoundé on the design of diseases monitoring systems in developing countries. Diseases monitoring systems can be seen as a collaborative edition work, where each actor in the system reports and aggregates information about cases he or she is aware of. This collaboration is an opportunity to confront our models to real situations and real users needs. Formally modeling such a large distributed system can be seen as a way to ensure its correctness. We also envision to promote this approach as a support for maintenance operations in complex environments (train transportation, aeronautics,...). We believe this framework can be useful both for the specification of distributed maintenance procedures, for circulating information and sharing processes across teams, but also for the analysis of the correctness of procedures, possibly for their optimization or redesign, and finally to automatically elaborate logs of maintenance operations. We are in contact with several major companies on these topics, for the maintenance application side. Other industrial contacts need to be built: we have preliminary contact with IBM (leader in business artifacts), and would like to establish relations with SAP (leader in service architectures).

# 5. Highlights of the Year

## 5.1. Highlights of the Year

The book on "Petri Net Synthesis" [44] co-authored by Eric Badouel, Luca Bernardinello, and Philippe Darondeau was published in October 2015 by Springer-Verlag in the EATCS Series "Texts in Theoretical Computer Science". This book is a comprehensive, systematic survey of the synthesis problem, and of region theory which underlies its solution, covering the related theory, algorithms, and applications. It is also a tribute to Philippe who passed away two years ago and could not see the final result of this project.

The SUMO team also welcomes the arrival of Ocan Sankur as a CNRS researcher. After a PhD at LSV (ENS Cachan) in 2013 supervised by Patricia Bouyer and Nicolas Markey, Ocan Sankur did a post-doc at Université Libre de Bruxelles in the group of Jean-François Raskin. His research work focuses on the robustness of quantitative systems, for their verification and synthesis.

# 6. New Software and Platforms

## 6.1. SIMSTORS

SIMSTORS is a simulator for regulated stochastic timed Petri nets. These Petri nets are a variant of stochastic and timed nets, which execution is controlled by a regulation policy an a predetermined theoretical schedule. The role of the regulation policy is to control the system to realize the schedule with the best possible precision. This software allows not only for step by step simulation, but also for performance analysis of systems such as production cells or train systems.

SIMSTORS was used successfully during a collaboration with Alstom transport to model existing urban railway systems and their regulation schemes. Alstom transport is willing to transfer this software and use it during early design phase of regulation algorithms in their metro lines.

Future extensions of the software will deal with verification of several new properties such as the robustness of proposed schedules.

- Participants: Loïc Hélouët and Abd El Karim Kecir
- Contact: Loïc Hélouët

## 6.2. Sigali

FUNCTIONAL DESCRIPTION

Sigali is a model-checker 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

## 6.3. Tipex

TImed Properties Enforcement during eXecution
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).

- Contact: Thierry Jéron, Hervé Marchand
- URL: http://srinivaspinisetty.github.io/Timed-Enforcement-Tools/

## 6.4. ReaX

ReaX is a tool developed by Nicolas Berthier that investigates the control of safety properties for infnite reactive synchronous systems modeled by arithmetic symbolic transition systems. It provides effective algorithms allowing to solve the safety control problem (including the dead-lock free case), and report some experiments. Its aim is to replace Sigali, which is limited to finite state systems described by boolean variables.

- Contact : Nicolas Berthier, Hervé Marchand
- URL : http://reatk.gforge.inria.fr/

## 6.5. Open Agora Core

Christophe Morvan participates to the implementation of a sophisticated voting system: Open Agora Core. It currently implements several voting methods among which *Condorcet* (Schulze method) or *instant runoff*. It is integrated into a Slack [1] polling plugin. This development serves as a basic building block in the process of elaborating Open Agora, a startup that should be created during 2016.

- Contact : Christophe Morvan
- URL : http://www.open-agora.com

# 7. New Results

## 7.1. Model expressivity and quantitative verification

### *7.1.1. Diagnosability of stochastic systems*

**Participants:** Nathalie Bertrand, Engel Lefaucheux.

Diagnosis of partially observable stochastic systems prone to faults was introduced in the late nineties. Diagnosability, i.e. the existence of a diagnoser, may be specified in different ways: (1) exact diagnosability (called A-diagnosability) requires that almost surely a fault is detected and that no fault is erroneously claimed while (2) approximate diagnosability (called $\epsilon$-diagnosability) allows a small probability of error when claiming a fault and (3) accurate approximate diagnosability (called AA-diagnosability) requires that this error threshold may be chosen arbitrarily small. In [32] we mainly focus on approximate diagnoses. We first refine the almost sure requirement about finite delay introducing a uniform version and showing that while it does not discriminate between the two versions of exact diagnosability this is no more the case in approximate diagnosis. Then we establish a complete picture for the decidability status of the diagnosability problems: (uniform) $\epsilon$-diagnosability and uniform AA-diagnosability are undecidable while AA-diagnosability is decidable in PTIME, answering a longstanding open question.

### *7.1.2. Probabilistic model checking*

**Participants:** Blaise Genest, Ocan Sankur.

In [16], we considered the verification of Markov chains against properties talking about distributions of probabilities. Even though a Markov chain is a very simple formalism, by discretizing in a finite number of classes the space of distributions through some symbols, we proved that the language of trajectories of distributions (one for each initial distribution) is not regular in general, even with 3 states. We then proposed a parametrized algorithm which approximates what happens to infinity, such that each symbolic block in the approximate language is at most $\epsilon$ away from the concrete distribution. We proved in [26] that if the eigenvalues of the Markov chain are distinct positive real numbers, then the trajectory is effectively regular. This is however not the case anymore if the eigenvalues can be distinct roots of real numbers.

Markov decision processes (MDPs) with multi-dimensional weights are useful to analyze systems with multiple objectives that may be conflicting and require the analysis of trade-offs. In [40], we study the complexity of percentile queries in such MDPs and give algorithms to synthesize strategies that enforce such constraints. Given a multi-dimensional weighted MDP and a quantitative payoff function $f$, thresholds $v_i$ (one per dimension), and probability thresholds $\alpha_i$, we show how to compute a single strategy to enforce that for all dimensions $i$, the probability of outcomes $\rho$ satisfying $f_i(\rho) \geq v_i$ is at least $\alpha_i$. We consider classical quantitative payoffs from the literature (sup, inf, lim sup, lim inf, mean-payoff, truncated sum, discounted sum). Our work extends to the quantitative case the multi-objective model checking problem studied by Etessami et al. [48] in unweighted MDPs.

[1] Slack, http://slack.com, is an industrial team communication tool.

In the invited contribution [25], we revisit the stochastic shortest path problem, and show how recent results allow one to improve over the classical solutions: we present algorithms to synthesize strategies with multiple guarantees on the distribution of the length of paths reaching a given target, rather than simply minimizing its expected value. The concepts and algorithms that we propose here are applications of more general results that have been obtained recently for Markov decision processes and that are described in a series of recent papers, including [40].

### *7.1.3. Stochastic modeling of biological systems*

**Participants:** Blaise Genest, Éric Fabre, Sucheendra Palaniappan, Matthieu Pichené.

In [47], we model a population of Hela cells with non deterministic behavior, subject to the drug TRAIL. TRAIL kills a large fraction of cancerous Hela cells by triggering the apoptosis pathway. Modelling this survival is important to perform *in silico* computations helping designing treatments killing the largest fraction of cancerous cells. We model this system using the stochastic class of Dynamic Bayesian Networks. We maintain large conditional probability tables which are represented by sparse datastructure, and perform simulations by looking ahead one time step and factoring this information to avoid empty probability entries. This considerably improves the simulation based inference of DBNs, getting a 100 times improvement in its efficiency.

### *7.1.4. Robustness of timed models*

**Participants:** Ocan Sankur, Loïc Hélouët.

Robustness of timed systems aims at studying whether infinitesimal perturbations in clock values can result in new discrete behaviors. A model is robust if the set of discrete behaviors is preserved under arbitrarily small (but positive) perturbations. This year we tackled this problem both for Timed Automata and time Petri Nets.

Timed automata are an extension of finite automata with clock variables that can conveniently model real-time systems. In [42], we study the robustness analysis problem for timed automata under guard imprecisions which consists in computing a timing imprecision bound under which a given specification holds. This is a particular kind of parameter synthesis problems specialized for analyzing robustness. We give a symbolic semi-algorithm for the problem based on a parametric data structure, and evaluate its performance in comparison with a recently published one, and with a binary search on the imprecision bound. We show that a safe bound on imprecision can be computed efficiently, and a performance close to that of exact model checking can be obtained thanks to the use of the parametric data structure and cycle acceleration techniques.

Another related problem is that of robust controller synthesis for timed automata where the goal is to choose actions and their timings so as to ensure a given state is reached when the chosen time delays are adversarially perturbed within a bound. In [21], we are interested in synthesizing "robust" strategies for ensuring reachability of a location in timed automata. We model this problem as a game between the controller and its environment, and solve the parameterized robust reachability problem: we show that the existence of an upper bound on the perturbations under which there is a strategy reaching a target location is EXPTIME-complete. We also extend our algorithm, with the same complexity, to turn-based timed games, where the successor state is entirely determined by the environment in some locations.

We also tackled the robustness problem for time Petri nets (TPNs, for short) in [17] by considering the model of parametric guard enlargement which allows time-intervals constraining the firing of transitions in TPNs to be enlarged by a (positive) parameter. We show that TPNs are not robust in general and checking if they are robust with respect to standard properties (such as boundedness, safety) is undecidable. We then extend the marking class timed automaton construction for TPNs to a parametric setting, and prove that it is compatible with guard enlargements. We apply this result to the (undecidable) class of TPNs which are robustly bounded (i.e., whose finite set of reachable markings remains finite under infinitesimal perturbations): we provide two decidable robustly bounded subclasses, and show that one can effectively build a timed automaton which is timed bisimilar even in presence of perturbations. This allows us to apply existing results for timed automata to these TPNs and show further robustness properties.

### 7.1.5. Verification for classes of Petri Nets with time

**Participants:** Blaise Genest, Loïc Hélouët.

We have considered verification problems for classes of Petri Nets with time. We have introduced the first, up to our knowledge, decidability result on reachability and boundedness for Petri Net variants that combine unbounded places, time, and urgency (the ability to enforce actions to happen within some delay). For this, we introduce the class of Timed-Arc Petri Nets with Urgency, which extends Timed-Arc Petri Nets [58] to allow urgency constraints, a feature from Timed-transition Petri Nets (TPNs) [54]. In order to avoid (straightforward) undecidability, we have considered restricted urgency: urgency can be used only on transitions consuming tokens from bounded places. For Timed-Arc Petri Nets with restricted urgency, we extend decidability results from Timed-Arc Petri Nets: control-state reachability and boundedness are decidable. Our main result concerns (marking) reachability, which is undecidable for both TPNs (because of unrestricted urgency) [52] and Timed-Arc Petri Nets (because of infinite number of clocks) [57]. We have obtained decidability of reachability for (unbounded) TPNs with restricted urgency under a new, yet natural, timed-arc semantics presenting them as Timed-Arc Petri Nets with restricted urgency. Decidability of reachability under the original semantics of TPNs was also obtained for a restricted subclass of unbounded nets. This work is under submission.

### 7.1.6. Non-interference in partial order models

**Participant:** Loïc Hélouët.

In [36] we have proposed a new definition of interference for partial order models. Non-interference (NI) is a property of systems stating that confidential actions should not cause effects observable by unauthorized users. Several variants of NI have been studied for many types of models, but rarely for true concurrency or unbounded models. In [36] we have investigated NI for High-level Message Sequence Charts (HMSC), a scenario language for the description of distributed systems, based on composition of partial orders. We firstly have proposed a general definition of security properties in terms of equivalence among observations, and shown that these properties, and in particular NI are undecidable for HMSCs. We hence have considered weaker local properties, describing situations where a system is attacked by a single agent, and show that local NI is decidable in this context. We then have proposed a refinement of local NI to obtain a finer notion of causal NI that emphasizes causal dependencies between confidential actions and observations. This causal NI has then been extended to causal NI with (selective) declassification of confidential events. Finally, we have shown that checking whether a system satisfies local and causal NI and their declassified variants are PSPACE-complete problems. Decidability seems to extend to other classes of partial order models which partially ordered observations can be represented by partial order models that exhibit some forms of regularity such as graph grammars or partial order automata. This conjecture will be explored next year.

### 7.1.7. Synthesis and games

**Participants:** Ocan Sankur, Engel Lefaucheux.

In [33], we investigate compositional algorithms to solve safety games described succinctly by synchronous circuits (given by AND and inverter gates). We show how the safety specification can be decomposed, in most cases, into a set of simpler specifications, each defining a safety game depending on less inputs and state variables. We give several algorithms which consist in solving the subgames, and aggregating them in order to find strategies for the global game. We present results of extensive experiments done on around five hundred benchmarks used in the synthesis competition SYNTCOMP 2014 and show that the compositional approach improves the performence on several classes of benchmarks.

In [35] we investigate priced timed games. Priced timed games are two-player zero-sum games played on priced timed automata (whose locations and transitions are labeled by weights modeling the costs of spending time in a state and executing an action, respectively). The goals of the players are to minimise and maximise the cost to reach a target location, respectively. We consider priced timed games with one clock and arbitrary (positive and negative) weights and show that, for an important subclass (the so-called simple priced timed games), one can compute, in exponential time, the optimal values that the players can achieve, with their

associated optimal strategies. As side results, we also show that one-clock priced timed games are determined and that we can use our result on simple priced timed games to solve the more general class of so-called reset-acyclic priced timed games (with arbitrary weights and one-clock).

In [34], we introduce a novel rule for synthesis of reactive systems, applicable to systems made of $n$ components which have each their own objectives. This rule is based on the notion of admissible strategies. Intuitively, a strategy $\sigma$ is dominated by $\sigma'$ if against all strategies of other players, $\sigma'$ is as good as $\sigma$, and against at least one strategy $\sigma'$ is strictly better than $\sigma$. Admissible strategies are those that are not dominated by any other strategy. The assume-admissible synthesis consists in restricting the space of strategies to admissible ones, and to look for strategy profiles which satisfy given specifications. We compare this rule with previous rules defined in the literature, and show that contrary to the previous proposals, it defines sets of solutions which are rectangular. This property leads to solutions which are robust and resilient, and allows one to synthesize strategies separately for each agent. We provide algorithms with optimal complexity and also an abstraction framework compatible with the new rule.

## 7.2. Management of large distributed systems

### *7.2.1. Parameterized verification in parameterized networks*

**Participants:** Nathalie Bertrand, Paulin Fournier.

We study the problems of reaching a specific control state, or converging to a set of target states, in networks with a parameterized number of identical processes communicating via broadcast. To reflect the distributed aspect of such networks, we restrict our attention to executions in which all the processes must follow the same local strategy that, given their past performed actions and received messages, provides the next action to be performed. We show that the reachability and target problem under such local strategies are NP-complete, assuming that the set of receivers is chosen non-deterministically at each step. On the other hand, these problems become undecidable when the communication topology is a clique. However, decidability can be regained with the additional assumption that all processes are bound to receive the broadcast messages. This is a joint work with Arnaud Sangnier [31].

### *7.2.2. Runtime enforcement of untimed and timed properties*

**Participants:** Thierry Jéron, Hervé Marchand, Srinivas Pinisetty.

Runtime enforcement is a powerful technique to ensure that a running system satisfies some desired properties. Using an enforcement monitor, an (untrustworthy) input execution (in the form of a sequence of events) is modified into an output sequence that complies with a property. Over the last decade, runtime enforcement has been mainly studied in the context of untimed properties. For several years, and in particular in the context of the PhD thesis of Srinivas Pinisetty [15] we elaborated the theory of runtime enforcement of timed properties. This year we also continued our work on the subject in several directions.

In [38] we describe the TiPEX tool that implements the enforcement monitoring algorithms for timed properties proposed in our previous papers . Enforcement monitors are generated from timed automata specifying timed properties. Such monitors correct input sequences by adding extra delays between events. Moreover, TiPEX also provides modules to generate timed automata from patterns, compose them, and check the class of properties they belong to in order to optimize the monitors. This paper also presents the performance evaluation of TiPEX within some experimental setup.

With coleagues from LaBRI (M. Renard, A. Rollet) and LIG (Y. Falcone) we investigate runtime enforcement of (timed and untimes) properties with uncontrollable events. In [41], we introduce a framework that takes as input any regular (timed) property 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 satisfy important properties, namely soundness and compliance, meaning that enforcement mechanisms output correct executions that are close to the input execution. We discuss the conditions for a property to be enforceable with uncontrollable events, and we define enforcement mechanisms that modify executions to obtain a correct output, as soon as possible. Moreover, we synthesize sound and compliant

descriptions of runtime enforcement mechanisms at two levels of abstraction to facilitate their design and implementation.

With colleagues from the Aalto University (S. Pinisetty, S. Tripakis and V. Preoteasa) and LIG (Y. Falcone) we investigate predictive runtime enforcement. In [39] we introduce 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 a classical non-predictive RE framework. All our results are formalized and proved in the Isabelle theorem prover. We are also currently extending this work to the timed setting.

### *7.2.3. Discrete controller synthesis*

**Participants:** Nicolas Berthier, Hervé Marchand.

In [29] we investigate the opportunities given by recent developments in the context of Discrete Controller Synthesis algorithms for infinite, logico-numerical systems. To this end, we focus on models employed in previous work for the management of dynamically partially reconfigurable hardware architectures. We extend these models with logico-numerical features to illustrate new modeling possibilities, and carry out some benchmarks to evaluate the feasibility of the approach on such models.

In [30] we elaborate on our former work for the safety control of infinite reactive synchronous systems modeled by arithmetic symbolic transition systems. By using abstract interpretation techniques involving disjunctive polyhedral overapproximations, we provide effective symbolic algorithms allowing to solve the deadlock-free safety control problem while overcoming previous limitations regarding the non-convexity of the set of states violating the invariant to enforce.

The ever growing complexity of software systems has led to the emergence of automated solutions for their management. The software assigned to this work is usually called an Autonomic Management System (AMS). It is ordinarily designed as a composition of several managers, which are pieces of software evaluating the dynamics of the system under management through measurements (e.g., workload, memory usage), taking decisions, and acting upon it so that it stays in a set of acceptable operating states. However, careless combination of managers may lead to inconsistencies in the taken decisions, and classical approaches dealing with these coordination problems often rely on intricate and ad hoc solutions. To tackle this problem, we take a global view and underscore that AMSs are intrinsically reactive, as they react to flows of monitoring data by emitting flows of reconfiguration actions. Therefore in [19] we propose a new approach for the design of AMSs, based on synchronous programming and discrete controller synthesis techniques. They provide us with high-level languages for modeling the system to manage, as well as means for statically guaranteeing the absence of logical coordination problems. Hence, they suit our main contribution, which is to obtain guarantees at design time about the absence of logical inconsistencies in the taken decisions. We detail our approach, illustrate it by designing an AMS for a realistic multi-tier application, and evaluate its practicality with an implementation.

In the invited paper [24] we make an overview of our works addressing discrete control-based design of adaptive and reconfigurable computing systems, also called autonomic computing. They are characterized by their ability to switch between different execution modes w.r.t. application and functionality, mapping and deployment, or execution architecture. The control of such reconfigurations or adaptations is a new application domain for control theory, called feedback computing. We approach the problem with a programming language supported approach, based on synchronous languages and discrete control synthesis. We concretely use this approach in FPGA-based reconfigurable architectures, and in the coordination of administration loops.

### *7.2.4. Computing knowledge at runtime*

**Participant:** Blaise Genest.

In [37] we compare three notions of knowledge in concurrent system: memoryless knowledge, knowledge of perfect recall, and causal knowledge. Memoryless knowledge is based only on the current state of a process, knowledge of perfect recall can take into account the local history of a process, and causal knowledge depends on the causal past of a process, which comprises the information a process can obtain when all processes exchange the information they have when performing joint transitions. We compare these notions in terms of knowledge strength, number of bits required to store this information, and the complexity of checking if a given process has a given knowledge. We show that all three notions of knowledge can be implemented using finite memory. Causal knowledge proves to be strictly more powerful than knowledge with perfect recall, which in turn proves to be strictly more powerful than memoryless knowledge. We show that keeping track of causal knowledge is cheaper than keeping track of knowledge of perfect recall.

### *7.2.5. Distributed optimal planning*

**Participant:** Éric Fabre.

Planning problems consist in organizing actions in a system in order to reach one of some target states. The actions consume and produce resources, can of course take place concurrently, and may have costs. We have a collection of results addressing this problem in the setting of distributed systems. This takes the shape of a network of components, each one holding private actions operating over its own resources, and shared/synchronized actions that can only occur in agreement with its neighbors. The goal is to design in a distributed manner a tuple of local plans, one per component, such that their combination forms a consistent global plan of minimal cost.

Our previous solutions to this problem modeled components as weighted automata [22]. In collaboration with Loig Jezequel (TU Munich) and Victor Khomenko (Univ. of Newcastle), we have extended this approach to the case of components modeled as safe Petri nets[23]. This allows one to benefit from the internal concurrency of actions within a component. Benchmarks have shown that this method can lead to significant time reductions to find feasible plans, in good cases. In the least favorable cases, performances are comparable to those obtained with components modeled as automata. The method does not apply to all situations however, as computations require to perform $\epsilon$-reductions on Petri-nets (our work also contains a contribution to this difficult question).

### *7.2.6. Regulation of urban train systems*

**Participants:** Éric Fabre, Loïc Hélouët, Karim Kecir, Hervé Marchand, Christophe Morvan.

A part of the SUMO team is involved in a collaboration with Alstom transports on regulation techniques. The role of regulation algorithms is to observe train trajectories and delays with respect to an expected ideal schedule, and then compute commands that are sent to trains to meet some quality of service (punctuality, regularity, ...) The objective of this collaboration is to study regulation techniques that are currently in use in urban train systems and compare their performances, and in the future to be able to compute optimal regulation strategies.

This year, we have proposed models inspired from stochastic Petri nets and from closed loop controllers to simulate regulated railways systems. The Petri net model led to the design of a tool called SIMSTORS, that was sucessfully used to model a real case study (line 1 of Santiago's subway). The simulator relies on event-based symbolic techniques: the time elapsed between two steps of the simulation is the time between two event occurrences (arrival, departure of a train, incident,...). This simulation scheme relying on an abstract model allowed a dramatic speed up of simulation with respect to existing solutions in use at Alstom Transport.

A second line of work has also been explored, in order to design and evaluate new regulation strategies for subway lines. The underlying model is inspired from event-based control theory, in a stochastic and timed setting. It abstracts away several significant topological features of a subway line, and focuses on the optimal command of train speeds in order to achieve high-level objectives such as the equal spacing of trains, or the efficient insertion/extraction of trains. This approach has allowed us to design new distributed regulation policies, which are remarquably stable and efficiently mitigate known instabilities of subway lines, like the bunching phenomenon. We are currently working on an extension of this approach for the management of time-tables and of forks and joins in the topology of subway lines.

## 7.3. Data driven systems

### *7.3.1. A model of large-scale distributed collaborative system*

**Participants:** Éric Badouel, Loïc Hélouët, Christophe Morvan, Robert Nsaibirni.

We have presented in [27] and [18] a purely declarative approach to artifact-centric collaborative systems, a model which we introduced in two stages. First, we assume that the workspace of a user is given by a mindmap, shortened to a map, which is a tree used to visualize and organize tasks in which he or she is involved, together with the information used for the resolution of these tasks. We introduce a model of guarded attribute grammar, or GAG, to help the automation of updating such a map. A GAG consists of an underlying grammar, that specifies the logical structure of the map, with semantic rules which are used both to govern the evolution of the tree structure (how an open node may be refined to a subtree) and to compute the value of some of the attributes (which derives from con-textual information). The map enriched with this extra information is termed an active workspace. Second, we define collaborative systems by making the various user's active workspaces communicate with each other. The communication uses message passing without shared memory thus enabling convenient distribution on an asynchronous architecture. A case study on a disease surveillance system is under development in the PhD thesis of Robert Nsaibirni and a first prototype of the model of active workspaces was written by Eric Badouel.

### *7.3.2. Petri Nets with semi-structured data*

**Participants:** Éric Badouel, Loïc Hélouët, Christophe Morvan.

In [28], we have proposed an extension of Petri nets with data called Structured Data Nets (StDN). This extension allows for the description of transactional systems with data. In StDNs, tokens are structured documents. Each transition is attached to a query, guarded by patterns, (logical assertions on the contents of its preset) and transforms tokens. In [28], we have proposed a semantics for StDNs, and then considered their formal properties: coverability of a marking, termination and soundness of transactions. Unrestricted StDNs are Turing complete, so these properties are undecidable. However, we have proposed an order on structured documents, and shown that under reasonable restrictions on documents and on the ex- pressiveness of patterns and queries, StDNs are well-structured transition systems, for which coverability, termination and soundness are decidable. This work has then been extended to consider properties of sets of configurations described as upward closed sets satisfying patterns, and should appear in a journal paper in 2016.

# 8. Bilateral Contracts and Grants with Industry

## 8.1. Bilateral Contracts with Industry

**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. Alstom agreed to start a second phase of the project 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*

**ANR VACSIM**: Validation of critical control-command systems by coupling simulation and formal analysis, 2011-2015, web site

Partners: EDF R&D, Dassault Systèmes, LURPA, I3S, LaBRI, and Inria SUMO.
The project aims at developing both methodological and formal contributions for the simulation and validation of control-command systems. SUMO contributes to quantitative analysis and its application to testing, monitoring of timed systems, and verification of communicating timed automata.

**ANR Ctrl-Green**: Autonomic management of green data centers, 2011-2014, web site
Partners: UJF/LIG, INPT/IRIT, Inria SUMO, EOLAS, Scalagent.
This project aims at developing techniques for the automatic optimal management of reconfigurable systems in the context of data centers using discrete controller synthesis methodology applied in the synchronous paradigm.

**ANR STOCH-MC**: Model-Checking of Stochastic Systems using approximated algorithms, 2014-2018, web site.
Led by SUMO.
Partners: Inria Project Team CONTRAINTES (Rocquencourt), LaBRI (Bordeaux), and LIAFA (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. National informal collaborations*

We collaborate with Yliès Falcone (VaSCO - LIG) and Antoine Rollet (Labri) on the enforcement of timed properties.

We collaborate with Arnaud Sangnier (LIAFA) on the parameterized verification of probabilistic systems.

We collaborate with B.Bérard (LIP6) on problems related to security.

We collaborate with Eric Rutten and Gwenael delaval on the control of reconfigurable systems as well as making the ling between Reax and Heptagon / BZR (http://bzr.inria.fr/)

## 9.2. International Initiatives

### *9.2.1. Inria International Labs*

Éric Badouel is member of the team Aloco (Architecture logicielle à composants) of LIRIMA, the Inria International Lab in Africa. This collaboration is on the development of artifact-centric business process models.

### *9.2.2. Inria Associate Teams not involved in an Inria International Labs*

#### *9.2.2.1. DISTOL*

Title: Distributed systems, stochastic models and logics

International Partner (Institution - Laboratory - Researcher):

CMI (India) - Madhavan Mukund

Start year: 2013

See also: http://www.irisa.fr/sumo/DISTOL/

The context of this project is formal modeling, and analysis of behaviors of distributed systems. We want to address verification and supervision of distributed systems through formal modeling and automated reasoning on models. By distributed systems, we mean software architectures made of several independent communicating entities. In the 90?s the kind of system addressed was mainly telecommunication protocols. Nowadays, distributed systems are frequently web-based systems such as Web Services, but several aspects of distributed systems can be found in biological applications. Within this context, a challenge is to propose formal tools with potential applications to real systems. We want to address this challenge along three main axes: The first one is realism of models. Models are often an abstraction of real systems. We want to build and study properties of models that are close enough from their implementations, and with robust properties. By robustness, we mean that properties checked on a model (for instance safety properties) should still hold for implementations of this model. The second one is quantitative analysis of systems. Rather that considering boolean answers to formal properties, one can consider the probability that such property holds on a run of the system, and return answers of probabilistic form ("almost surely, a call to a service is successful") or quantitative ("the average failure rate is lower than 0.01"). One possibility to obtain a probability is to compute its exact value. Such questions have answers for markovian models and some quantitative logics (PCTL). However, such computations are expensive, and one can divide the problem into sub-components at the cost of some approximation. We plan to develop efficient algorithms for quantitative analysis of systems. The third one is unification of control theories. There are many proposals for supervisory control, including distributed control with communications. However, none of them seems fully satisfactory. We want to consider connections between control theory, epistemic reasoning (which seems to solve some problems raised by communications between local supervisors), and game theory (which emphasizes the notion of goal to be achieved in a problem), and give a unified framework for supervision of distributed systems.

### *9.2.3. Inria International Partners*

#### *9.2.3.1. Informal International Partners*

The team collaborates on runtime enforcement with the group of Prof. Stavros Tripakis (http://users.ics.aalto.fi/stavros/) at Aalto University (Finland), where our former PhD student Srinivas Pinisetty is doing a Post-doc.

In the context of LIRIMA, the Inria International Lab in Africa, we have strong collaborations with University of Yaoundé I on an artifact-centric model of workflow system based on guarded attribute grammars. In particular with the co-supervision of the PhD thesis of Robert Nsaibirni.

We collaborate with Laurie Ricker (Mount Allison University, Canada) on the control of distributed systems and the enforcement of opacity

### *9.2.4. Participation In other International Programs*

AVeRTS is an Indo-French project on the algorithmic verification of real-time systems. The project is funded by CNRS on the french side, and by DST on the Indian side, under the CEFIPRA - Indo-French Program in ICST 2014-2016. From SUMO, Nathalie Bertrand and Blaise Genest are involved and contribute on stochastic games. In the context of this project, Miheer Dewaskar, a CMI (Chennai Mathematical Institute) master student did an internship in our team on the control of a population of Markov decision processes.

## 9.3. International Research Visitors

### *9.3.1. Visits of International Scientists*

S. Akshay visited the SUMO team for three weeks in May 2015.

Robert Nsaibirni (University of Yaoundé) visited SUMO from March to May 2015 on the use of the Guarded Attribute Grammar formalism for the description of the workspaces of actors of a disease surveillance system.

*9.3.1.1. Internships*

Achille Aknin

Date: May 2015 - July 2015

Institution: ENS Ulm (France)

Alexandre Blanche

Date: May 2015 - July 2015

Institution: ENS Rennes (France)

Miheer Dewaskar

Date: May 2015 - July 2015

Institution: Chennai Mathematical Institute (India)

André Gueney

Date: April 2015 - September 2015

Institution: CNAM (France)

### *9.3.2. Visits to International Teams*

*9.3.2.1. Research stays abroad*

Eric Fabre visited Michele Pinna during 2 weeks (Univ. of Cagliari, Italy). This collaboration focuses on the design of compact unfoldings for Petri nets.

# 10. Dissemination

## 10.1. Promoting Scientific Activities

### *10.1.1. Scientific events organisation*

*10.1.1.1. Member of the organizing committees*

Nathalie Bertrand is an elected steering committee member for the international conference QEST (Quantitative Evaluation of Systems).

Thierry Jéron is member of the steering committee of the european summer school MOVEP (Modélisation et Vérification des Systèmes Parallèles). The next edition will take place in Genova in July 2016.

Hervé Marchand is member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. He is member of the steering committee of MSR (Modélisation de systèmes réactifs).

### *10.1.2. Scientific events selection*

*10.1.2.1. Chair of conference program committees*

Éric Badouel was Scientific President of CRI 2015 (Yaoundé)

Nathalie Bertrand was co-chair of the international workshop QAPL'15 with Mirco Tribastone.

*10.1.2.2. Member of the conference program committees*

Éric Badouel was PC member of ATAED 2016 (Brussel).

Nathalie Bertrand was PC member of the following international conferences: Formats'15, ICLA'15, QEST'15, TACAS'15.

Loïc Hélouët was member of the program committee of ACSD 2015 (Approaches of Concurrency for Systems Design, Brussels june 2015) and SDL 2015 (System Design Languages, Berlin, 2015).

Thierry Jéron was PC member of the following international conferences: ICTSS'15, TAP'15, USE'15, RV'16.

Hervé Marchand was PC member of the DCDS 2015 and MSR 2015 conferences.

*10.1.2.3. Reviewer*

The members of the team reviewed numerous papers for numerous international conferences.

### *10.1.3. Journal*

*10.1.3.1. Member of the editorial boards*

Éric Badouel is Editor in Chief of ARIMA Journal.

*10.1.3.2. Reviewer - Reviewing activities*

Éric Badouel was a reviewer for Science of Computer Programming, Fundamenta Informaticae and Mathematical Review.

Nathalie Bertrand acted as a reviewer for Journal of the ACM, Formal Methods in System Design, Information and Computation.

Éric Fabre reviewed sumissions to IEEE TAC, Automatica, J. of Discrete Event Dynamic Systems, IEEE Trans. on Automation Sciences and Engineering.

Loïc Hélouët was a reviewer for Formal aspects of computing and Theoretical Computer Science.

Hervé Marchand was reviewer for JDEDS and for the Annual Reviews in Control.

Christophe Morvan was a reviewer for Journal of Computer and System Sciences and for IEEE Transactions on Automatic Control.

Ocan Sankur was a reviewer for Theoretical Computer Science, Logical Methods in Computer Science, Science of Computer Programming and Formal Methods in System Design

### *10.1.4. Invited talks*

Nathalie Bertrand gave an invited talk at Gandalf 2015, and at MSR 2015. She gave a lecture on Controlling probabilistic systems under partial information at the EJCIM (École jeunes chercheurs Informatique Mathématiques) in april 2015. See the lecture notes [45].

Thierry Jéron and Ocan Sankur both gave lectures at ETR'15 (Ecole temps réel) in Septembre 2015, respectively on "Model-based conformance test generation for timed systems", and "Control of timed systems".

### *10.1.5. Scientific expertise*

Éric Fabre serves as expert for the Minsitry of Research, for the Credit Impot Recherche, a tax-reduction programme for research activities performed by private companies. He was solicited for 4 companies in 2015.

Loïc Hélouët acted as reviewer for the ANR.

Thierry Jéron was reviewer for the CHIST-ERA consortium and for a NSERC Discovery Grant proposal (Canada).

### *10.1.6. Research administration*

Éric Badouel is secretary of the Permanent Committee of CARI, co-Director of LIRIMA, and the Scientific Manager for Africa and Middle-East region at Inria DPEI.

Nathalie Bertrand is secretary and committee member of Gilles Kahn PhD prize.

Éric Fabre is the co-director, with Olivier Audouin, of the joint research lab of Alcatel-Lucent Bell Labs and Inria.

Loïc Hélouët and Éric Fabre are members of the Scientific Board of the joint lab of Alstom Transport and Inria.

Loïc Hélouët was *référent chercheur* for the Inria Rennes research center.

Thierry Jéron was Vice Scientific Delegate of the Inria Rennes research center and member of the Inria Evaluation Committee until 09/2015. This year he was member of the following Inria hiring committees: junior scientists (CR2) at Lillle, starting and advanced senior research positions (ARP, SRP), and senior scientists (DR2). He is also member of the IFIP Working Group 10.2 on Embedded Systems and member of the Management Committee (substitute) of the COST IC1402 (ARVI: Runtime Verification beyond Monitoring). He is member of the COS Prospective of Irisa Rennes.

## 10.2. Teaching - Supervision - Juries

### *10.2.1. Teaching*

**Nathalie Bertrand**

Agreg: Responsible of computer science organization, 16h (eq. TD), M2, Ecole Normale Supérieure de Rennes, France.

L3: Lecture on Algorithms, 18h (eq. TD), L3, University Rennes 1, France.

**Éric Fabre**

Master : "ASR: introduction to distributed systems and algorithms," 12h, M2, Univ. Rennes 1, France.

Master : "Information theory," 15h, M1, Ecole Normale Superieure de Bretagne, France.

Master : Preparation of Aggregation, 6h, M1, Ecole Normale Superieure de Bretagne, France.

**Blaise Genest**

Master: Advanced verification techniques, M2 in Compuer Science, Université Rennes I, 10h.

**Loïc Hélouët**

Licence: JAVA and algorithmics at INSA de Rennes for students in the second year of engineer cycle. He also supervises practical studies (development of a small project by students under the supervision of two teachers).

Agreg: algorithmics at ENS Rennes (8 hours / year).

**Éric Fabre, Loïc Hélouët, Hervé Marchand**

Master: supervised 3 students from ENS Rennes at the M1 level during 6 month. (2 hours/ week during 6 months)

**Christophe Morvan**

Licence: Compilation, System, Advanced Algorithmics Université de Paris-Est, Marne-la-Vallée, France.

### *10.2.2. Supervision*

HdR: Nathalie Bertrand, “Contributions to the verification and control of timed and probabilistic models”, University Rennes I, November 16, 2015.

PhD:

Paulin Fournier, “Parameterized verification of networks of many identical processes”, Université Rennes I, December 17, 2015, Supervisors: Nathalie Bertrand, Thierry Jéron, Arnaud Sangnier (LIAFA).

Srinivas Pinisetty, “Runtime Enforcement of Timed Properties”, Université Rennes I, January 23, 2015, Supervisors: Thierry Jéron, Hervé Marchand, Yliès Falcone (LIG).

PhD in progress:

Karim Kecir (2015-2018, CIFRE thesis): "Régulation et robustesse des systèmes ferroviaires urbains", Université Rennes I, Supervisor: Loïc Hélouët.

Matthieu Pichené (2014-2017): “Stochastic models for the modelling of apoptosis”, Université Rennes I, Supervisor: Blaise Genest.

Engel Lefaucheux (2015-2018): “Information control in probabilistic systems”, Université Rennes I, Supervisors: Nathalie Bertrand, Serge Haddad (LSV, ENS Cachan).

### *10.2.3. Juries*

Éric Badouel was opponent of the Doctoral Thesis of Abel Armas-Cervantès, "Diagnosing Behavioural Differences Between Business Process Models", University of Tartu, Estonia, August 2015.

Nathalie Bertrand was member of the PhD defense committee of Nathanaël Fijalkow, *Counting and Randomising in Automata Theory*, Université Paris VII, 15/10/2015.

Éric Fabre was in the mid-term jury of 4 PhD students of Telecom Bretagne.

Thierry Jéron was member of the Habilitation defense committee of Nathalie Bertrand, University Rennes I, November 16, 2015 (see above), and president of the PhD defense committee of Abderahman Kriouile, Université de Grenoble, September 17, 2015. He was also in the mid-term PhD jury of Mouna Hkimi (Supélec Rennes).

Hervé Marchand was Member of the PhD Defense of Johan Girault « Conception formelle du pilotage d’une flotte de robots mobiles », Ecole centrale de Nantes, November 2015.

# 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] 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

[4] N. BERTRAND, B. GENEST, H. GIMBERT. *Qualitative Determinacy and Decidability of Stochastic Games with Signals*, in "Proceedings of LICS’09", Los Angeles, États-Unis, August 2009, http://hal.archives-ouvertes.fr/hal-00356566

[5] 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

[6] 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]

[7] 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

[8] 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

[9] E. FABRE, L. JEZEQUEL. *Distributed optimal planning: an approach by weighted automata calculus*, in "CDC", 2009, pp. 211-216

[10] 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

[11] 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

[12] C. JARD, T. JÉRON. *TGV: theory, principles and algorithms*, in "STTT", 2005, vol. 7, n$^{o}$ 4, pp. 297-315

[13] B. JEANNET, T. JÉRON, V. RUSU, E. ZINOVIEVA. *Symbolic Test Selection Based on Approximate Analysis*, in "TACAS", Edinburgh, Royaume-Uni, 2005, http://hal.inria.fr/inria-00564617

## Publications of the year

### Doctoral Dissertations and Habilitation Theses

[14] N. BERTRAND. *Contributions to the verification and control of timed and probabilistic models*, Rennes 1, November 2015, Habilitation à diriger des recherches, https://hal.inria.fr/tel-01243612

[15] S. PINISETTY. *Runtime enforcement of timed properties*, Université Rennes 1, January 2015, https://tel.archives-ouvertes.fr/tel-01185842

### Articles in International Peer-Reviewed Journals

[16] M. AGRAWAL, S. AKSHAY, B. GENEST, P. THIAGARAJAN. *Approximate Verification of the Symbolic Dynamics of Markov Chains*, in "Journal of the ACM (JACM)", 2015, vol. 62, n$^{o}$ 1, pp. 34-65, https://hal.inria.fr/hal-00920793

[17] S. AKSHAY, L. HÉLOUËT, C. JARD, P.-A. REYNIER. *Robustness of Time Petri Nets under Guard Enlargement*, in "Fundamenta Informaticae", 2016, vol. 143, https://hal.inria.fr/hal-01237124

[18] E. BADOUEL, L. HÉLOUËT, G.-E. KOUAMOU, C. MORVAN, R. F. J. NSAIBIRNI. *Active Workspaces: Distributed Collaborative Systems based on Guarded Attribute Grammars*, in "ACM SIGAPP Applied Computing Review (ACM Digital Library)", September 2015, vol. 15, n$^{o}$ 3, 28 p. , https://hal.inria.fr/hal-01237131

[19] N. BERTHIER, É. RUTTEN, N. DE PALMA, S. M.-K. GUEYE. *Designing Autonomic Management Systems by using Reactive Control Techniques*, in "IEEE Transactions on Software Engineering", December 2015, 18 p. , https://hal.inria.fr/hal-01242853

[20] N. BERTRAND, A. STAINER, T. JÉRON, M. KRICHEN. *A game approach to determinize timed automata*, in "Formal Methods in System Design", February 2015, 39 p. [*DOI :* 10.1007/s10703-014-0220-1], https://hal.inria.fr/hal-01102472

[21] P. BOUYER, N. MARKEY, O. SANKUR. *Robust Reachability in Timed Automata: A Game-Based Approach*, in "Journal of Theoretical Computer Science (TCS)", 2015, vol. 563, pp. 43-74 [*DOI :* 10.1016/J.TCS.2014.08.014], https://hal.archives-ouvertes.fr/hal-01105077

[22] L. JEZEQUEL, E. FABRE. *Factored Cost-Optimal Planning Using Message Passing Algorithms*, in "Fundamenta Informaticae", July 2015, vol. 139, n° 4 [*DOI :* 10.3233/FI-2015-1239], https://hal.inria.fr/hal-01247346

[23] L. JEZEQUEL, E. FABRE, V. KHOMENKO. *Factored Planning: From Automata to Petri Nets*, in "ACM Transactions in Embedded Computing Systems", March 2015, vol. 14, n° 2 [*DOI :* 10.1145/2656215], https://hal.inria.fr/hal-01247347

### Invited Conferences

[24] X. AN, G. DELAVAL, J.-P. DIGUET, A. GAMATIE, S. M.-K. GUEYE, H. MARCHAND, N. DE PALMA, E. RUTTEN. *Discrete Control-Based Design of Adaptive and Autonomic Computing Systems*, in "ICDCIT: International Conference on Distributed Computing and Internet Technology", Bhubaneswar, India, 11th International Conference on Distributed Computing and Internet Technology, ICDCIT 2015, Springer, February 2015, vol. LNCS, n° 8956 [*DOI :* 10.1007/978-3-319-14977-6_6], https://hal.archives-ouvertes.fr/hal-01116015

[25] M. RANDOUR, R. JEAN-FRANÇOIS, O. SANKUR. *Variations on the Stochastic Shortest Path Problem*, in "Verification, Model Checking, and Abstract Interpretation", Mumbai, India, January 2015 [*DOI :* 10.1007/978-3-662-46081-8_1], https://hal.archives-ouvertes.fr/hal-01248766

### International Conferences with Proceedings

[26] S. AKSHAY, B. GENEST, B. KARELOVIC, N. VYAS. *On Regularity of unary Probabilistic Automata*, in "STACS 2016", Orléans, France, STACS 2016, 2016, https://hal.archives-ouvertes.fr/hal-01245037

[27] E. BADOUEL, L. HÉLOUËT, G.-E. KOUAMOU, C. MORVAN. *A Grammatical Approach to Data-centric Case Management in a Distributed Collaborative Environment*, in "The 30th ACM/SIGAPP Symposium On Applied Computing", Salamanca, Spain, The 30th ACM/SIGAPP Symposium On Applied Computing, ACM, April 2015 [*DOI :* 10.1145/2695664.2695698], https://hal.inria.fr/hal-01193222

[28] E. BADOUEL, L. HÉLOUËT, C. MORVAN. *Petri nets with semi-structured data*, in "36th International Conference on Application and Theory of Petri Nets and Concurrency", Bruxelles, Belgium, 36th International Conference on Application and Theory of Petri Nets and Concurrency, June 2015, https://hal.inria.fr/hal-01193279

[29] N. BERTHIER, X. AN, H. MARCHAND. *Towards Applying Logico-numerical Control to Dynamically Partially Reconfigurable Architectures*, in "5th IFAC International Workshop On Dependable Control of Discrete Systems - DCDS'15", Cancun, Mexico, May 2015, vol. 48, n° 7, pp. 132-138, https://hal.archives-ouvertes.fr/hal-01187745

[30] N. BERTHIER, H. MARCHAND. *Deadlock-free Discrete Controller Synthesis for Infinite State Systems*, in "54th IEEE Conference on Decision and Control", Osaka, Japan, December 2015, https://hal.inria.fr/hal-01200976

[31] N. BERTRAND, P. FOURNIER, A. SANGNIER. *Distributed local strategies in broadcast networks*, in "26th International Conference on Concurrency Theory (CONCUR 2015)", Madrid, Spain, September 2015 [*DOI :* 10.4230/LIPICS.CONCUR.2015.44], https://hal.inria.fr/hal-01243595

[32] N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Accurate approximate diagnosability of stochastic systems*, in "10th International Conference on Language and Automata Theory and Applications", Prague, Czech Republic, Springer, March 2016, https://hal.inria.fr/hal-01220954

[33] R. BRENGUIER, G. A. PÉREZ, J.-F. RASKIN, O. SANKUR. *Compositional Algorithms for Succinct Safety Games*, in "4th Workshop on Synthesis", San Francisco, United States, July 2015, https://hal.archives-ouvertes.fr/hal-01248767

[34] R. BRENGUIER, J.-F. RASKIN, O. SANKUR. *Assume-Admissible Synthesis*, in "26th International Conference on Concurrency Theory (CONCUR 2015)", Madrid, Spain, Leibniz International Proceedings in Informatics (LIPIcs), September 2015, vol. 42, pp. 100–113 [*DOI :* 10.4230/LIPICS.CONCUR.2015.100], https://hal.archives-ouvertes.fr/hal-01245193

[35] T. BRIHAYE, G. GEERAERTS, A. HADDAD, E. LEFAUCHEUX, B. MONMEGE. *Simple Priced Timed Games Are Not That Simple*, in "35th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'15)", Banaglore, India, Leibniz-Zentrum für Informatik, 2015, https://hal.archives-ouvertes.fr/hal-01242902

[36] B. BÉRARD, L. HÉLOUËT, J. MULLINS. *Non-interference in partial order models*, in "ACSD 2015", Brussels, Belgium, ACSD 2015, IEEE, June 2015, https://hal.inria.fr/hal-01138787

[37] B. GENEST, D. PELED, S. SCHEWE. *Knowledge = Observation + Memory + Computation*, in "FoSSaCS 2015", London, United Kingdom, FoSSaCS 2015, Springer, 2015, vol. LNCS, n$^{o}$ 9034, pp. 215-229 [*DOI :* 10.1007/978-3-662-46678-0_14], https://hal.archives-ouvertes.fr/hal-01245016

[38] S. PINISETTY, Y. FALCONE, T. JÉRON, H. MARCHAND. *TiPEX: A Tool Chain for Timed Property Enforcement During eXecution*, in "RV'2015, 6th International Conference on Runtime Verification", Vienne, Austria, E. BARTOCCI, R. MAJUMDAR (editors), Lecture Notes in Computer Science, Springer, September 2015, vol. 9333, 12 p. [*DOI :* 10.1007/978-3-319-23820-3_22], https://hal.inria.fr/hal-01244446

[39] S. PINISETTY, V. PREOTEASA, S. TRIPAKIS, T. JÉRON, Y. FALCONE, H. MARCHAND. *Predictive Runtime Enforcement* *, in "SAC 2016 31st ACM Symposium on Applied Computing", Pisa, Italy, ACM, April 2016, 6 p. [*DOI :* 10.1145/2851613.2851827], https://hal.inria.fr/hal-01244369

[40] M. RANDOUR, J.-F. RASKIN, O. SANKUR. *Percentile Queries in Multi-dimensional Markov Decision Processes*, in "27th International Conference on Computer Aided Verification (CAV 2015)", San Francisco, United States, Lecture Notes in Computer Science, July 2015, vol. 9206 [*DOI :* 10.1007/978-3-319-21690-4_8], https://hal.archives-ouvertes.fr/hal-01245196

[41] M. RENARD, Y. FALCONE, A. ROLLET, S. PINISETTY, T. JÉRON, H. MARCHAND. *Enforcement of (Timed) Properties with Uncontrollable Events*, in "12th International Colloquium on Theoretical Aspects of Computing (ICTAC 2015)", Cali, Colombia, Theoretical Aspects of Computing - ICTAC 2015, Springer, October 2015, vol. LNCS, n$^{o}$ 9399, 22 p. [*DOI :* 10.1007/978-3-319-25150-9_31], https://hal.inria.fr/hal-01185238

[42] O. SANKUR. *Symbolic Quantitative Robustness Analysis of Timed Automata*, in "Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015)", London, United Kingdom, Lecture Notes in Computer Science, Springer, April 2015, vol. 9035 [*DOI :* 10.1007/978-3-662-46681-0_48], https://hal.archives-ouvertes.fr/hal-01244766

### Scientific Books (or Scientific Book chapters)

[43] *Proceedings of the Thirteenth Workshop on Quantitative Aspects of Programming Languages and Systems (QAPL'15)*, 2015 [*DOI :* 10.4204/EPTCS.194], https://hal.inria.fr/hal-01243625

[44] E. BADOUEL, L. BERNARDINELLO, P. DARONDEAU. *Petri Net Synthesis*, Text in Theoretical Computer Science, an EATCS Series, Springer, November 2015, 339 p. [*DOI :* 10.1007/978-3-662-47967-4], https://hal.inria.fr/hal-01237142

[45] N. BERTRAND, S. HADDAD. *Contrôle, probabilités et observation partielle*, in "Informatique Mathématique. Une photographie en 2015", CNRS Édition, 2015, pp. 177-227, https://hal.archives-ouvertes.fr/hal-01242962

### Research Reports

[46] N. BERTRAND, P. FOURNIER, A. SANGNIER. *Distributed local strategies in broadcast networks*, Inria Rennes, July 2015, https://hal.inria.fr/hal-01170796

### Other Publications

[47] S. K. PALANIAPPAN, F. BERTAUX, M. PICHENE, E. FABRE, G. BATT, B. GENEST. *Approximating the dynamics of the Hybrid Stochastic-Deterministic Apoptosis pathway*, CMSB 2015, 2015, CMSB 2015, Poster, https://hal.archives-ouvertes.fr/hal-01245034

## References in notes

[48] K. ETESSAMI, M. KWIATKOWSKA, M. Y. VARDI, M. YANNAKAKIS. *Multi-objective model checking of Markov decision processes*, in "Log. Methods Comput. Sci.", 2008, vol. 4, n$^{o}$ 4, 4:8, 21 p. , http://dx.doi.org/10.2168/LMCS-4(4:8)2008

[49] E. FABRE, L. JEZEQUEL. *Distributed optimal planning: an approach by weighted automata calculus*, in "CDC", 2009, pp. 211-216

[50] L. HÉLOUËT, A. BENVENISTE. *Document Based Modeling of Web Services Choreographies Using Active XML*, in "IEEE International Conference on Web Services, ICWS 2010", IEEE Computer Society, 2010, pp. 291-298

[51] L. JEZEQUEL, E. FABRE. *A#: A distributed version of A* for factored planning*, in "CDC", 2012, pp. 7377-7382

[52] N. D. JONES, L. H. LANDWEBER, Y. E. LIEN. *Complexity of Some Problems in Petri Nets*, in "Theor. Comput. Sci.", 1977, vol. 4, n$^{o}$ 3, pp. 277–299

[53] B. MASSON, L. HÉLOUËT, A. BENVENISTE. *Compatibility of Data-Centric Web Services*, in "WS-FM", Lecture Notes in Computer Science, Springer, 2011, vol. 7176, pp. 32-47

[54] P. M. MERLIN. *A Study of the Recoverability of Computing Systems*, University of California, Irvine, CA, USA, 1974

[55] A. NIGAM, N. S. CASWELL. *Business artifacts: An approach to operational specification*, in "IBM Systems Journal", 2003, vol. 42, n$^{o}$ 3, pp. 428-445, http://dx.doi.org/10.1147/sj.423.0428

[56] S. ROSARIO. *Quality of Service issues in compositions of Web services*, Université de Rennes 1, 2009

[57] V. V. RUIZ, F. C. GOMEZ, D. D. FRUTOS-ESCRIG. *On Non-Decidability of Reachability for Timed-Arc Petri Nets*, in "PNPM", IEEE Computer Society, 1999, pp. 188–

[58] B. WALTER. *Timed Petri-Nets for Modelling and Analysing Protocols with Real-Time Characteristics*, in "Proc. of PSTV", 1983, pp. 149-159