IN PARTNERSHIP WITH:
CNRS

Université Rennes 1

Activity Report 2016

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:

1.2.2. - Supervision
1.3. - Distributed Systems
2.3.2. - Cyber-physical systems
2.4.2. - Model-checking
4.5. - Formal methods for security
6.4. - Automatic control
7.1. - Parallel and distributed algorithms
7.3. - Optimization
7.4. - Logic in Computer Science
7.8. - Information theory
7.14. - Game Theory

Other Research Topics and Application Domains:

1.1.3. - Cellular biology
1.1.9. - Bioinformatics
5.2.2. - Railway
6.2. - Network technologies
6.3.3. - Network Management

1. Members

Research Scientists

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

Engineer

Olivier Bache [Inria, from April to September 2016]

PhD Students

Hugo Bazille [Inria]
Sihem Cherrared [Orange Labs, from Sep 2016, granted by CIFRE]
Paulin Fournier [Univ. Rennes I, until Aug 2016]
Abd El Karim Kecir [Alstom, granted by CIFRE]
Engel Lefaucheux [Univ. Rennes I]
Matthieu Pichené [Inria]

Post-Doctoral Fellow
Sucheendra Palaniappan [Inria, until Sep 2016]

Visiting Scientists
Robert Nsaibirni [University of Yaoundé I, from September 2016]
Shauna Laurene Ricker [Prof. Mount Allison Univ., Canada, until Jul 2016]

Administrative Assistant
Laurence Dinh [Inria]

Others
Vincent Aubry [ENS Paris, from Jun 2016 until Jul 2016]
Christophe Morvan [Ass. Prof., Univ. Paris Est Marne La Vallée]
Arthur Queffelec [Inria, from May 2016 until Jul 2016]
Jérémy Thibault [Inria, from May 2016 until Jul 2016]

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. Discrete event systems approaches 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 build dynamically 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 (compute 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 work around that we will explore.

Here are some more detailed 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 or/and 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 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 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 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.
- Model abstraction. We will explore techniques to design more tractable abstractions of stochastic dynamic systems defined on large sets of variables.
- 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.

3.4. Data driven systems

Data-driven systems are systems whose behavior 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 adresse 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 cities 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 small perturbations and incidents can be accomodated by the system, and how fast return to normality occurs, 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 reflect as well dynamically changing architectures. Besides modeling, management algorithms are also challenged by features like the size of systems, the need to work on abstractions, on partially known models, on open (multi-tenant) systems, on dynamically changing systems, etc. The networking technology is now evolving toward software defined networks, virtualized network functions, 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 trouble shooting, 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 are often distributed and involve complex and sometimes dynamic workflows. In many cases, there are strong interactions between data and control flows: indeed, decisons taken to decide of 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 needs to address 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 competences 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

A quite new topic in SUMO is about Systems Biology. 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 explain how many molecules interact inside a cell, triggered by some outside signal (drug, etc.), eventually leading to the death of the cell through apoptosis. While intrinsically quantitative in nature, 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 system 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

Start-up creation. Christophe Morvan (Ass. Prof. Univ. Paris Est Marne la Vallée) has been hosted by Sumo for several years for his research activities. In 2016, he created Open Agora with two other computer scientists.

The company develops a software suite to help the decision process in large structures. It offers tools to structure discussions, voting mechanisms, and automated argument summaries. The company will maintain connections with the team for the development of GAGs (Guarded Attributed Grammars) that are instrumental in the automated summary tools.

New team member. Nicolas Markey (DR CNRS) recently joined the team, after several years in LSV (*Laboratoire Spécification et Vérification*), Cachan. Nicolas will reinforce the activities of the team in the modeling and analysis of timed systems, abstraction techniques and game theory.

6. New Software and Platforms

6.1. Active Workspaces

KEYWORDS: Guarded attribute grammar - Active workspace - 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 [44]. Late in 2015 Éric Badouel produced in Haskell a software prototype implementing active workspaces based on Guarded Attribute Grammars (GAGs).

Concurrently, Christophe Morvan was beginning a startup project consisting in making on-line collective decision making tools: *Open Agora*. This project included collaboration workspaces for people participating in constructing possible decisions. There was a natural connection between the prototype, and the startup project.

In order to make industrial use of the GAG prototype, Olivier Bache (already involved in the Open agora project) applied to a 6 month InriaHub program (between April and September 2016). During these 6 months he bundeled the prototype into an API (also programmed in Haskell) and developped a web infrastructure, based on the PHP framework, to allow the interaction with Active Workspaces in a browser. This developpement will be licenced to Open Agora SAS after its creation expected in January 2017.
FUNCTIONAL DESCRIPTION

Prototype in Haskell of user's active workspaces based on Guarded Attribute Grammars.

- Author: Eric Badouel
- Contact: Eric Badouel
- URL: http://people.rennes.inria.fr/Eric.Badouel/Research/ActiveWorkspaces.html

6.2. SIMSTORS

SIMSTORS is a simulator for regulated stochastic timed Petri nets. These Petri nets are a variant of stochastic and timed nets, whose 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. This year, the software has been extended to consider headway management.

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

7. New Results

7.1. Analysis and verification of quantitative systems

7.1.1. Quantitative verification of distributions of stochastic models

Participant: Blaise Genest.

In [24], we obtained conditions under which quantitative verification of distributions of stochastic systems is decidable. This is a challenging question as for general Markov Chains, verification of distribution is Skolem-complete, a problem on linear recurrence sequences whose decidability is a long-standing problem open for 40 years. In this paper, we approach this problem by studying the languages generated by Markov Chains, whose regularity would entail the decidability of quantitative verification. Given an initial distribution, we represent the trajectory of Markov Chain over time as an infinite word over a finite alphabet, where the n^{th} letter represents a probability range after n steps. We extend this to a language of trajectories (a set of words), one trajectory for each initial distribution from a (possibly infinite) set. We show that if the eigenvalues of the transition matrix associated with the Markov Chain are all distinct positive real numbers, then the language is *effectively regular*. Further, we show that this result is at the boundary of regularity, as non-regular languages can be generated when the restrictions are even slightly relaxed. The regular representation of the language allows us to reason about more general properties, e.g., robustness of a regular property in a neighbourhood around a given distribution.

7.1.2. Diagnosability of repairable faults

Participants: Éric Fabre, Loïc Hélouët, Hervé Marchand, Engel Lefaucheux.

For (partially observable) discrete event systems, diagnosability characterizes the ability to detect the occurrence of a permanent fault in bounded time after it occurs, given the observations available on that system. Diagnosability 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. It was proved in [35]that diagnosability is a PSpace complete problem.

7.1.3. Diagnosability of stochastic systems

Participants: Éric Fabre, Blaise Genest, Hugo Bazille, Ocan Sankur.

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 ε-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 a recent work [27], we focused on approximate diagnoses. We first refined 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. We then gave a complete picture of relations between the different diagnosability specifications for probabilistic systems and establish characterisations for most of them in the finite-state case. Based on these characterisations, we developped decision procedures, studied their complexity and proved their optimality. We also designed synthesis algorithms to construct diagnosers and we analysed their memory requirements. Finally we established undecidability of the diagnosability problems for which we provided no characterisation. Notably, we proved the AA-diagnosability problem to be undecidable, answering a longstanding open question.

In another work [28], we investigated semantical and computational issues for exact notions of diagnosability in the context of infinite-state probabilistic systems. We first showed established a characterisation of the so-called FF-diagnosability using a $G\delta$ set (instead of an open set for finite-state systems) and also for two other notions, IF- and IA-diagnosability, when models are finitely branching. We also proved that surprisingly the last notion, FA-diagnosability, cannot be characterised in this way even in the finitely branching case. Then we applied our characterisations for a partially observable probabilistic extension of visibly pushdown automata, yielding EXPSPACE procedures for solving diagnosability problems. In addition, we establish some computational lower bounds and show that slight extensions of these probabilistic visibly pushdown automata lead to undecidability.

7.1.4. Analysing decisive stochastic processes

Participant: Nathalie Bertrand.

In 2007, Abdulla et al. introduced the elegant concept of decisive Markov chain. Intuitively, decisiveness allows one to lift the good properties of finite Markov chains to infinite Markov chains. For instance, the approximate quantitative reachability problem can be solved for decisive Markov chains (enjoying reasonable effectiveness assumptions) including probabilistic lossy channel systems and probabilistic vector addition systems with states. In a recent work [26], we extended the concept of decisiveness to more general stochastic processes. This extension is non trivial as we consider stochastic processes with a potentially continuous set of states and uncountable branching (common features of real-time stochastic processes). This allowed us to obtain decidability results for both qualitative and quantitative verification problems on some classes of real-time stochastic processes, including generalized semi-Markov processes and stochastic timed automata.

7.1.5. Concurrent timed systems

Participants: Loïc Hélouët, Blaise Genest.

Adding real time information to Petri net models often leads to undecidability of classical verification problems such as reachability and boundedness. For instance, models such as Timed-Transition Petri nets (TPNs) [47] are intractable except in a bounded setting. On the other hand, the model of Timed-Arc Petri nets [50] enjoys decidability results for boundedness and control-state reachability problems at the cost of disallowing urgency (the ability to enforce actions within a time delay).

We have addressed semantics variants of time and timed Petri nets to obtain concurrent models with interesting expressive power, but yet allowing decidability of verification and robustness questions. 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.

In [25] we have considered time in Petri nets under a strong semantics with multiple enabling of transitions. We focus on a structural subclass of unbounded TPNs, where the underlying untimed net is free-choice, and show that it enjoys nice properties under a multi-server semantics. In particular, we showed that the questions of fireability (whether a chosen transition can fire), and termination (whether the net has a non-terminating run) are decidable for this class. We then consider the problem of robustness under guard enlargement [48], i.e., whether a given property is preserved even if the system is implemented on an architecture with imprecise time measurement. Unlike in [15], where decidability of several problems is obtained for bounded classes of nets, we showed that robustness of fireability is decidable for unbounded free choice TPNs with a multi-server semantics.

The robustness of time Petri nets was addressed in [15] 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.

The goal of [23] is to investigate decidable classes of Petri nets with time that capture some urgency and still allow unbounded behaviors, which go beyond finite state systems. We have shown, up to our knowledge, the first decidability results on reachability and boundedness for Petri net variants that combine unbounded places, time, and urgency. For this, we have introduced the class of Timed-Arc Petri nets with restricted Urgency, where urgency can be used only on transitions consuming tokens from bounded places. We showed that control-state reachability and boundedness are decidable for this new class, by extending results from Timed-Arc Petri nets (without urgency) [43]. Our main result concerns (marking) reachability, which is undecidable for both TPNs (because of unrestricted urgency) [46] and Timed-Arc Petri Nets (because of infinite number of "clocks") [49]. We 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 intermediate marking semantics is also obtained for a restricted subclass.

7.1.6. Petri nets realizability

Participants: Loïc Hélouët, Abd El Karim Kecir.

We considered in [30] the realizability of urban train schedules by stochastic concurrent timed systems. Schedules are high level views of desired timetables that a metro system should implement. They are represented as partial orders decorated with timing constraints. Train systems are represented as elementary stochastic time Petri nets. We have first considered logical realizability: a schedule is realizable by a net $\mathcal{N}$ if it embeds in a time process of $\mathcal{N}$ that satisfies all its constraints. However, with continuous time domains, the probability of a time process that realizes a schedule is null. We have extended the former notion of realizability to consider probabilistic realizability of schedules up to some imprecision α. This probabilistic realizability holds if the probability that $\mathcal{N}$ logically realizes S with constraints enlarged by α time units is strictly positive. We have shown that upon a sensible restriction guaranteeing time progress (systems can not perform an arbitrary number of actions within a single time unit), logical 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 have provided a construction technique for these prefixes and shown that they represent all time processes of a net occurring up to a given maximal date. We have then shown how to verify existence of an embedding and compute the probability of its realization.

7.2. Control of quantitative systems

7.2.1. Smart regulation for urban trains

Participants: Éric Fabre, Loïc Hélouët, Hervé Marchand, Abd El 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 also developed another approach based on event graphs in order to optimally interleave trains at a junction.

7.2.2. Games and reactive synthesis

Participant: Ocan Sankur.

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" whose choice can be justified. 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. In [29], we investigate this framework for quantitative graph games. We characterize admissible strategies, study their existence, and give an effective characterization of the set of paths that are compatible with admissible payoffs. This is then used to derive algorithms for model checking under admissibility, but also assume-admissible synthesis.

In [21], we present the reactive synthesis competition (SYNTCOMP), a long-term effort intended to stimulate and guide advances in the design and application of synthesis procedures for reactive systems. The first iteration of SYNTCOMP is based on the controller synthesis problem for finite-state systems and safety specifications. We provide an overview of this problem and existing approaches to solve it, and report on the design and results of the first SYNTCOMP. This includes the definition of the benchmark format, the collection of benchmarks, the rules of the competition, and the five synthesis tools that participated. We present and analyze the results of the competition and draw conclusions on the state of the art. Finally, we give an outlook on future directions of SYNTCOMP.

In the invited [22], we summarize new solution concepts useful for the synthesis of reactive systems that we have introduced in several recent publications. These solution concepts are developed in the context of non-zero sum games played on graphs. They include the assume-admissible synthesis on Boolean games, synthesis under multiple environments for Markov decision processes, and multi-objective synthesis with probability thresholds for Markov decision processes with multi-dimensional weights. They are part of the contributions obtained in the inVEST project funded by the European Research Council.

7.2.3. Runtime enforcement

Participants: Hervé Marchand, Thierry Jéron.

In the [20] we generalize our line of work on runtime enforcement for timed properties. Runtime enforcement is a verification/validation technique aiming at correcting possibly incorrect executions of a system of interest. In this work we consider enforcement monitoring for systems where the physical time elapsing between actions matters. Executions are thus modelled as timed words (i.e., sequences of actions with dates). We consider runtime enforcement for timed specifications modelled as timed automata. Our enforcement mechanisms have the power of both delaying events to match timing constraints, and suppressing events when no delaying is appropriate, thus possibly allowing for longer executions. To ease their design and their correctness-proof, enforcement mechanisms are described at several levels: enforcement functions that specify the input-output behaviour in terms of transformations of timed words, constraints that should be satisfied by such functions, enforcement monitors that describe the operational behaviour of enforcement functions, and enforcement algorithms that describe the implementation of enforcement monitors.

This year we went one step ahead [33] and consider 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 runtime enforcement framework. All our results are formalized and proved in the Isabelle theorem prover.

7.2.4. Decentralized control

Participant: Hervé Marchand.

In collaboration with Laurie Ricker, we have been interested in decentralized control of discrete event systems. In decentralized discrete-event system (DES) architectures, agents fuse their local decisions to arrive at the global decision. The contribution of each agent to the final decision is never assessed; however, it may be the case that only a subset of agents, i.e., a (static) coalition, perpetually contribute towards the correct final decisions. In casting the decentralized DES control (with and without communication) problem as a cooperative game, it is possible to quantify the average contribution that each agent makes towards synthesizing the overall correct control strategy. Specifically, we explore allocations that assess contributions of non-communicating and communicating controllers for this class of problems. This allows a quantification of the contribution that each agent makes to the coalition with respect to decisions made solely based on its partial observations and decisions made based on messages sent to another agent(s) to facilitate a correct control decision [34].

7.3. Management of large distributed systems

7.3.1. Non-interference in partial order models

Participant: Loïc Hélouët.

We obtained new results on security issues such as non-interference [41]. Noninterference (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 [45], we had already demonstrated the discriminating power of partial orders, and investigated NI for High-level Message Sequence Charts (HMSCs), a partial order language for the description of distributed systems. We had proposed a general definition of security properties in terms of equivalence among observations of behaviors, and showed that equivalence, inclusion, and NI properties were undecidable for HMSCs. We defined a new formalism called *partial order automata*, that captures natural observations of distributed systems, and in particular observations of HMSCs. It generalizes HMSCs and permits assembling partial orders. We have then considered subclasses of partial order automata and HMSCs for which Non-Interference is decidable. This allowed us to exhibit more classes of HMSCs for which NI is decidable. Finally, we have defined weaker local Non-interfernce properties, describing situations where a system is attacked by a single agent, and shown that local NI is decidable. We have then refined local NI to a finer notion of causal NI that emphasizes causal dependencies between confidential actions and observations and extended it to causal NI with (selective) declassification of confidential events, which allows to consider that confidential actions need can be kept secret for a limited duration and can then be declassified. Checking whether a system satisfies local and causal NI and their declassified variants are PSPACE-complete problems.

7.3.2. Simulations for stochastic abstractions of large systems

Participants: Éric Fabre, Blaise Genest, Matthieu Pichené.

In [32], we developped a new simulation strategy to accurately simulate DBNs (Dynamic Bayesian Networks) obtained as stochastic abstractions of large systems. The DBN abstractions are given under the form of probability tables, describing the probability for a variable to take a given value given the values of some variables at the previous time point. To be able to handle large systems with many variables, there is a table for each variable (coupling between variable is not explicitely represented). This creates discrepencies when simulating variables independently. Our new algorithm simulates tuples of variables together by looking ahead for such discrepencies in order to avoid them. Such simulations are still efficient, and match more faithfully the original systems.

7.4. Data driven systems

7.4.1. Structured data nets

Participants: Éric Badouel, Loïc Hélouët, Christophe Morvan.

In [16] we proposed a Petri net extension, called Structured Data Nets (SDN), that describes transactional systems with data. In these nets, tokens are semi-structured documents. Each transition is attached to a query, guarded by patterns, (logical assertions on the contents of its preset) and transforms tokens.

We define SDNs and their semantics and consider their formal properties: coverability of a marking, termination and soundness of transactions.

Unrestricted SDNs are Turing complete, so these properties are undecidable. We thus used an order on documents, and showed that under reasonable restrictions on documents and on the expressiveness of patterns and queries, SDNs are well-structured transition systems, for which coverability, termination and soundness are decidable.

7.4.2. An active workspace model for disease surveillance

Participant: Éric Badouel.

Flexibility and change at both design- and run-time are fast becoming the Rule rather than the Exception in Business Process Models. This is attributed to the continuous advances in domain knowledge, the increase in expert knowledge, and the diverse and heterogeneous nature of contextual variables. Such processes are characterized by collaborative work and decision making between users with heterogeneous profiles on a processes designed on-the-fly. A model for such processes should thus natively support human interactions. We showed in [31] how the Active Workspaces model proposed [44] for distributed collaborative systems supports these interactions.

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. 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.

Joint Nokia Bell Labs - Inria research lab: Several members of the team are involved in the joint research lab of Nokia Bell Labs and Inria. This lab is co-directed by Éric Fabre (Inria) and Olivier Audouin (Bell Labs), and funds joint research teams over a period of 4 years. The 3rd phase of the lab is in preparation, and 6 new joint teams will be launched in the first quarter of 2017. Sumo is involved in the proposal *Softwarization of Everything* that aims at developing techniques for the programmability, the verification and the management of software-defined networks (SDN). This covers in particular the CIFRE PhD of Arij El Majed, to start in January 2017, on the topic of Root cause analysis in reconfigurable dynamic systems.

Joint Orange Labs - Inria research lab: Éric Fabre takes part to the joint research lab of Orange Labs and Inria. This lab funds around 5 new PhD grants every year. This covers in particular the CIFRE PhD of Sihem Cherrared on the topic of Fault management in multi-tenant programmable networks.

9. Partnerships and Cooperations

9.1. National Initiatives

9.1.1. ANR

ANR STOCH-MC: Model-Checking of Stochastic Systems using approximated algorithms, 2014-2018, http://perso.crans.org/~genest/stoch.htmlweb 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.

ANR HeadWorks: Human-Centric Data-oriented WORKflows , 2016-2020
Led by Université Rennes 1.
Partners: Inria Project Team VALDA (LSV and ENS-ULM), Univestité Rennes 1 (DRUID), Inria SUMO, Inria Lille (LINKs), MNHN, Foule Factory.
Headwork was accepted in 2016. Participants : Loïc Hélouët, Éric Badouel.

Partners: IRISA (DRUID), ENS ULM (VALDA), Inria SUMO, Inria Lille (LINKs), MNHN, Foule Factory.

The objective of this project is to develop techniques to facilite development, deployment, and monitring 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.

9.1.2. IPL HAC SPECIS

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.

Partners: Inria teams AVALON (Lyon), POLARIS (Grenoble), HIEPACS, STORM (Bordeaux), MEXICO (Paris), MYRIADS, SUMO (Rennes), VERIDIS (Nancy).

Participants: Thierry Jéron, The Anh Pham.

9.1.3. National informal collaborations

The team collaborates with the following researchers:

- Yliès Falcone (CORSE LIG/Inria team in Grenoble) and Antoine Rollet (Labri Bordeaux) on the enforcement of timed properties,
- Arnaud Sangnier (IRIF) on the parameterized verification of probabilistic systems,
- Béatrice Bérard (LIP6) and Serge Haddad (LSV) on problems of opacity and diagnosis.
- Thomas Chatain, on problems related to concurrency and time,
- 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/),
- Patricia Bouyer (LSV, ENS Cachan) on the analysis of probabilistic timed systems and quantitative aspects of verification,
- François Laroussinie (IRIF, UP7-Diderot) on logics for multi-agent systems.

9.2. European Initiatives

9.2.1. FP7 & H2020 Projects

Nicolas Markey is a member of Project ERC EQualIS whose principal investigator is Patricia Bouyer from LSV.

9.3. International Initiatives

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

9.3.1.1. QuantProb

Title: Quantitative analysis of non-standard properties in probabilistic models

International Partner (Institution - Laboratory - Researcher):

Technical University of Dresde (Germany) - Saxe - 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.

9.3.2. Inria International Partners

9.3.2.1. 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 and with Thomas Brihaye (University of Mons) on the analysis of probabilistic timed systems.

The team has well-established collaborations with several institutes in India. CMI (Chennai Mathematical Institute, M. Mukund and N.K. Kumar), IIT Bombay (S. Akshay).

The team is building a new collaboration with Ecole Polytechnique Montreal (J. Mullins).

9.4. International Research Visitors

9.4.1. Visits of International Scientists

L. Ricker visited the SUMO team for 2 months in May-June 2016.

9.4.1.1. Internships

Robert Nsaibirni from the University of Yaoundé I joined the team from Sept. 2016 in the context of an Eiffel grant.

9.4.2. Visits to International Teams

9.4.2.1. Research Stays Abroad

Nathalie Bertrand spent a month at the Simons Institute for the theory of computing, UC Berkeley, California. She participated to the program Logical Structure in Computation (https://simons.berkeley.edu/programs/logic2016).

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. Member of the Organizing Committees

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).

Thierry Jéron and Nicolas Markey are members of the steering committee of the european summer school MOVEP (Modélisation et Vérification des Systèmes Parallèles). Nicolas Markey was co-chair of the edition that took place in Genova in July 2016.

Thierry Jéron is member of the steering committee of FMF 2017 (Formal Methods Forum) held in Toulouse in January 2017.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Éric Badouel was Chair of conference program committee of CARI 2016.

10.1.2.2. Member of the Conference Program Committees

Éric Badouel was a member of the programme committee of ATAED 2016.

Nathalie Bertrand served on the Program Committees of the international conferences STACS'16, TACAS'16, Concur'16 and QEST'16.

Loïc Hélouët was member of the program committees of ACSD 2016 (Approaches of Concurrency for Systems Design) and SAM 2016 (System Analysis and Modeling).

Thierry Jéron served on the Program Committees of the following international conferences: ICTSS'16, RV'16, SAC-SVT 2017.

10.1.2.3. Reviewer

Nicolas Markey was reviewer for STACS 2017 and AAAI 2017.

Éric Badouel was reviewer for LICS 2016, VeCos 2016, CARI 2016, TACAS 2016, and ATAED 2016.

Loïc Hélouët was reviewer for SAM'2016, ACSD'2016, DNS'2016, STACS'2016, and ICTAC'2016

Thierry Jéron was reviewer for IEEE CASE & ISAM, CONCUR'16.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Éric Badouel is co-Editor-in-Chief of ARIMA Journal (https://arima.episciences.org/).

10.1.3.2. Reviewer - Reviewing Activities

Éric Fabre was reviewer for IEEE TAC, Automatica, JDEDS, CDC, and JONS.

Hervé Marchand was reviewer for JDEDS and Automatica.

Nathalie Bertrand was reviewer for JACM and JCSS.

Nicolas Markey was reviewer for FMSD and TCS.

Éric Badouel was reviewer for Fundamenta Informaticae and Mathematical review-AMS (MathSciNet).

Loïc Hélouët was reviewer for FAOC, TCS, TECS and Fundamenta Informaticae. He also served as reviewer for Mathematical review-AMS (MathSciNet).

Thierry Jéron was reviewer for FAOC and TECS.

10.1.4. Invited Talks

Nathalie Bertrand was invited speaker at MFPS international conference, and gave a lecture at MOVEP summer school.

Éric Badouel was invited speaker at VeCos 2016.

10.1.5. Scientific Expertise

Thierry Jéron served for the expertise of ANR and ASTRID (ANR/DGA) projects.

10.1.6. Research Administration

Éric Fabre is co-director, with Olivier Audouin, of the joint research lab of Nokia Bel Labs and Inria. He is member of the scientific board of the joint lab of Alstom Transport and Inria and member of the Bureau of the Scientific Board of Inria Rennes Bretagne Atlantique.

Hervé Marchand is chairman of the CUMI in Rennes.

Nathalie Bertrand is a nominated member of CNU27 (Conseil National des Universités, section 27).

Éric Badouel is 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 Partnerships Department and member of the executive board of GIS SARIMA.

Loïc Hélouët, Nathalie Bertrand and Ocan Sankur organize the weekly seminar 68NQRT at IRISA (40 talks each year).

Loïc Hélouët was elected representant 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.

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.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Éric Fabre

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

Master: "Information theory", 30h (eq. TD), M1, Ecole Normale Superieure de Rennes, France.

Nathalie Bertrand

Licence: "Algorithmics", 18h (eq. TD), L3, Univ. Rennes 1, France.

Master: "Prépa. Agreg.", 40h (eq. TD), Ecole Normale Superieure de Rennes, France.

Loïc Hélouët

Licence: JAVA and algorithmics, L2, 40h, INSA de Renne, France.

Licence : practical studies (development of a small project), 8h, INSA de Renne, France.

Master: "Prépa. Agreg.", 8h (eq. TD)+ mock exams, Ecole Normale Superieure de Rennes, France.

10.2.2. Supervision

- PhD in progress: Engel Lefaucheux, *Controlling information in Probabilistic Systems, Sept. 2015, Nathalie Bertrand, Serge Haddad (LSV, Cachan).*
- *PhD in progress: Karim Kecir,* Régulation et robustesse des systèmes ferroviaires urbains, May 2018, Loïc Hélouët and Pierre Dersin (Alstom).
- PhD in progress: The Anh Pham, *Dynamic Formal Verification of High Performance Runtimes and Applications, Nov. 2016, Thierry Jéron, Martin Quinson (Myriads, Inria Rennes).*
- *PhD in progress: Hugo Bazille,* Diagnosability and opacity analysis of large scale systems, Oct. 2016, Blaise Genest, Éric Fabre.
- PhD in progress: Sihem Cherrared, *Fault management in multi-tenant programmable networks, Oct. 2016, Éric Fabre, Gregor Goessler (Inria Grenoble), Sofiane Imadali (Orange Labs).*

10.2.3. Juries

Éric Fabre was reviewer in the PhD defense committee of Yoann Geoffroy, *A general framework for causality analysis based on traces, for composite systems*, Dec. 2016, Univ. Grenoble Alpes. He was also jury member for the Habilitation defense of Blaise Genest, *Taming Concurrency Using Representatives, March 2016, Univ. Rennes 1.*

Hervé Marchand was member of the PhD defences of Hassan Ibrahim, Analyse à base de SAT de la diagnosticabilité et de la prédictabilité des systèmes à événements discrets centralisés et distribués (Université Paris-Sud, Gif-sur-Yvette), December 2016 and of Toussaint Tigori, *Méthodes de génération d'exécutifs temps réel (Ecole centrale de Nantes, Nantes), in November 2016.*

Nicolas Markey was reviewer in the PhD defense committee of Thanh-Tung Tran (LaBRI; supervised by Igor Walukiewicz and Frédéric Herbreteau).

10.3. Popularization

Nathalie Bertrand gave an introductory talk on graph theory and its use to solve practical problems, to grad school students following the ISN (Introduction aux Sciences du Numérique) courses.

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 LICS'09", Los Angeles, États-Unis, 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 "CDC", 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 "STTT", 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 "TACAS", Edinburgh, Royaume-Uni, 2005, http://hal.inria.fr/inria-00564617

Publications of the year

Articles in International Peer-Reviewed Journals

[15] S. AKSHAY, L. HÉLOUËT, C. JARD, P.-A. REYNIERS. *Robustness of Time Petri Nets under Guard Enlargement*, in "Fundamenta Informaticae", 2016, vol. 143, n^{o} 3-4, https://hal.inria.fr/hal-01379431

[16] E. BADOUEL, C. MORVAN, L. HÉLOUËT. *Petri Nets with Structured Data*, in "Fundamenta Informaticae", 2016, vol. 146, n^{o} 1, 119 p. , https://hal.inria.fr/hal-01379245

[17] 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", July 2016, vol. 42, n^{o} 7, 18 p. , https://hal.inria.fr/hal-01242853

[18] R. BRENGUIER, J.-F. RASKIN, O. SANKUR. *Assume-admissible synthesis*, in "Acta Informatica", 2016 [*DOI :* 10.1007/s00236-016-0273-2], https://hal.inria.fr/hal-01373538

[19] B. BÉRARD, L. HÉLOUËT, J. MULLINS. *Non-interference in partial order models*, in "ACM Transactions on Embedded Computing Systems (TECS)", 2016, https://hal.inria.fr/hal-01379451

[20] Y. FALCONE, T. JÉRON, H. MARCHAND, S. PINISETTY. *Runtime Enforcement of Regular Timed Properties by Suppressing and Delaying Events*, in "Science of Computer Programming", March 2016 [*DOI :* 10.1016/J.SCICO.2016.02.008], https://hal.inria.fr/hal-01281727

[21] S. JACOBS, R. BLOEM, R. BRENGUIER, R. EHLERS, T. HELL, R. KÖNIGHOFER, G. A. PÉREZ, J.-F. RASKIN, L. RYZHYK, O. SANKUR, M. SEIDL, L. TENTRUP, A. WALKER. *The first reactive synthesis competition (SYNTCOMP 2014)*, in "International Journal on Software Tools for Technology Transfer", April 2016 [*DOI :* 10.1007/s10009-016-0416-3], https://hal.inria.fr/hal-01373547

Invited Conferences

[22] R. BRENGUIER, L. CLEMENTE, P. HUNTER, G. A. PÉREZ, M. RANDOUR, J.-F. RASKIN, O. SANKUR, M. SASSOLAS. *Non-Zero Sum Games for Reactive Synthesis*, in "LATA 2016 : 10th International Conference on Language and Automata Theory and Applications", Prague, Czech Republic, A.-H. DEDIU, J. JANOUŠEK, C. MARTÍN-VIDE, B. TRUTHE (editors), Lecture Notes in Computer Science, Springer, March 2016, vol. 9618, pp. 3-23 [*DOI :* 10.1007/978-3-319-30000-9_1], https://hal.inria.fr/hal-01373546

International Conferences with Proceedings

[23] S. AKSHAY, B. GENEST, L. HÉLOUËT. *Decidable Classes of Unbounded Petri Nets with Time and Urgency*, in "Application and Theory of Petri Nets and Concurrency - 37th International Conference, PETRI NETS, 2016", Torun, Poland, F. KORDON, D. MOLDT (editors), Application and Theory of Petri Nets and Concurrency - 37th International Conference, PETRI NETS, 2016, Springer, June 2016, n° 9698, pp. 301 - 322 [*DOI :* 10.1007/978-3-319-39086-4_18], https://hal.inria.fr/hal-01379414

[24] 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

[25] S. AKSHAY, L. HÉLOUËT, R. PHAWADE. *Combining Free Choice and Time in Petri Nets*, in "23rd International Symposium on Temporal Representation and Reasoning", Lyngby, Denmark, IEEE (editor), 23rd International Symposium on Temporal Representation and Reasoning, Technical University of Denmark , October 2016, https://hal.inria.fr/hal-01379440

[26] N. BERTRAND, P. BOUYER, T. BRIHAYE, P. CARLIER. *Analysing Decisive Stochastic Processes*, in "43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)", Rome, Italy, LiPICS, 2016, vol. 55, 14 p. [*DOI :* 10.4230/LIPICS.ICALP.2016.101], https://hal.inria.fr/hal-01397794

[27] 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

[28] N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Diagnosis in Infinite-State Probabilistic Systems* , in "27th International Conference on Concurrency Theory (Concur 2016)", Québec city, Canada, 27th International Conference on Concurrency Theory (Concur 2016), August 2016 [*DOI :* 10.4230/LIPICS.CONCUR.2016.37], https://hal.inria.fr/hal-01373354

[29] R. BRENGUIER, G. A. PÉREZ, J.-F. RASKIN, O. SANKUR. *Admissibility in Quantitative Graph Games*, in "36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science", Chennai, India, December 2016, https://hal.inria.fr/hal-01373542

[30] L. HÉLOUËT, K. KECIR. *Realizability of Schedules by Stochastic Time Petri Nets with Blocking Semantics*, in "37th International Conference, PETRI NETS 2016", Torun, Poland, F. KORDON, D. MOLDT (editors), Application and Theory of Petri Nets and Concurrency, Fabrice Kordon and Daniel Moldt, June 2016, n° 9698, pp. 155-175 [*DOI :* 10.1007/978-3-319-39086-4_11], https://hal.inria.fr/hal-01379424

[31] R. F. J. NSAIBIRNI, E. BADOUEL, G. TEXIER, G.-E. KOUAMOU. *Active-Workspaces: A Dynamic Collaborative Business Process Model for Disease Surveillance Systems*, in "Worldcomp'16- The 2nd International Conference on Health Informatics and Medical Systems", Las Vegas, United States, July 2016, https://hal.inria.fr/hal-01323561

[32] S. K. PALANIAPPAN, M. PICHENÉ, G. BATT, E. FABRE, B. GENEST. *A Look-Ahead Simulation Algorithm for DBN Models of Biochemical Pathways*, in "Hybrid Systems Biology, 5th International Workshop, HSB 2016", Grenoble, France, E. CINQUEMANI, A. DONZÉ (editors), Lecture Notes in Computer Science, October 2016, vol. 9957, pp. 3-15 [*DOI :* 10.1007/978-3-319-47151-8_1], https://hal.inria.fr/hal-01406115

[33] 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

[34] L. S. L. RICKER, H. MARCHAND. *Finding the weakest link(s): Coalition games for decentralized discrete-event control*, in "55th IEEE Conference on Decision and Control", Las-Vegas, United States, December 2016, https://hal.inria.fr/hal-01373709

Conferences without Proceedings

[35] E. FABRE, L. HÉLOUËT, E. LEFAUCHEUX, H. MARCHAND. *Diagnosability of Repairable Faults*, in "13th International Workshop on Discrete Event Systems", Xi'an, China, 2016, pp. 256-262, (Version Longue), https://hal.inria.fr/hal-01302562

[36] 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, April 2017, https://hal.archives-ouvertes.fr/hal-01431472

Books or Proceedings Editing

[37] M. LO, E. BADOUEL, N. GMATI (editors). *Proceedings of CARI 2016*, July 2016, 513 p. , https://hal.inria.fr/hal-01350039

Research Reports

[38] N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Diagnosis in Infinite-State Probabilistic Systems (long version)*, Inria Rennes ; LSV, ENS Cachan, June 2016, https://hal.inria.fr/hal-01334218

[39] P. BOUYER, P. HOFMAN, N. MARKEY, M. RANDOUR, M. ZIMMERMANN. *Bounding Average-energy Games*, ArXiv, October 2016, n^{o} 1610.07858, https://hal.archives-ouvertes.fr/hal-01410144

[40] P. BOUYER, V. JUGÉ, N. MARKEY. *Dynamic Complexity of Parity Games with Bounded Tree-Width*, ArXiv, October 2016, https://hal.archives-ouvertes.fr/hal-01410169

Other Publications

[41] B. BÉRARD, L. HÉLOUËT, J. MULLINS. *Non-interference in partial order models*, February 2016, working paper or preprint, https://hal.inria.fr/hal-01280043

[42] L. HÉLOUËT, K. KECIR. *Realizability of Schedules by Stochastic Time Petri Nets with Blocking Semantics (regular paper)*, March 2016, working paper or preprint, https://hal.inria.fr/hal-01284682

References in notes

[43] P. A. ABDULLA, A. NYLÉN. *Timed Petri Nets and BQOs*, in "ICATPN", LNCS, 2001, vol. 2075, pp. 53-70

[44] E. BADOUEL, L. HÉLOUËT, C. MORVAN, R. F. J. NSAIBIRNI. *Active Workspace: Distributed Collaborative Systems based on Guarded Attribute Grammars*, in "ACM SIGAPP Applied Computing Review", 2015, vol. 6, n^{o} 33, pp. 6–33

[45] B. BÉRARD, L. HÉLOUËT, J. MULLINS. *Non-interference in Partial Order Models*, in "Proc. of 15th Int. Conf. on Application of Concurrency to System Design, ACSD 2015", IEEE Computer Society, 2015, pp. 80–89

[46] 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

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

[48] A. PURI. *Dynamical Properties of Timed Automata*, in "In DEDS", 2000, vol. 10, n^{o} 1-2, pp. 87–113

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

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