IN PARTNERSHIP WITH:
CNRS

Université Rennes 1

Activity Report 2018

Project-Team SUMO

SUpervision of large MOdular and distributed systems

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

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Proofs and Verification

Table of contents

Project-Team SUMO

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

Keywords:

Computer Science and Digital Science:

A1.2.2. - Supervision
A1.3. - Distributed Systems
A2.3.2. - Cyber-physical systems
A2.4.2. - Model-checking
A4.5. - Formal methods for security
A6.4. - Automatic control
A7.1. - Algorithms
A7.1.1. - Distributed algorithms
A7.2. - Logic in Computer Science
A8.2. - Optimization
A8.6. - Information theory
A8.11. - Game Theory

Other Research Topics and Application Domains:

B1.1.7. - Bioinformatics
B5.2.2. - Railway
B6.2. - Network technologies
B6.3.3. - Network Management

1. Team, Visitors, External Collaborators

Research Scientists

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

PhD Students

Hugo Bazille [Inria]
Sihem Cherrared [Orange Labs]
Emily Clement [Mitsubishi Electric, from Nov 2018]
Rodrigue Djeumen Djatcha [University of Douala]
Arij Elmajed [Nokia]
Leo Henry [Univ de Rennes I, from Oct 2018]
Abd El Karim Kecir [Inria, until Jul 2018]
Engel Lefaucheux [Univ de Rennes I, until Sep 2018]
Anirban Majumdar [CNRS, from Sep 2018]

Robert Fondze Jr Nsaibirni [University of Yaoundé]
The anh Pham [Univ de Rennes I]
Matthieu Pichené [Inria, until Feb 2018]
Arthur Queffelec [Univ de Rennes I, from Nov 2018]
Victor Roussanaly [Univ de Rennes I]
Suman Sadhukhan [Inria, from Oct 2018]
Rituraj Singh [Inria]

Interns

Ludovic Landuré [Univ de Rennes I, from May 2018 until Jul 2018]
Flavia Palmieri [Inria, from Mar 2018 until Jun 2018]
Ritam Raha [Chennai Mathematical Institute, CMI, India, from Sep 2018]

Administrative Assistant

Laurence Dinh [Inria]

Visiting Scientists

Adwait Amit Godbole [Inria, from May 2018 until Jul 2018]
Romulo Meira Goes [University of Michigan, from Feb 2018 until May 2018]
Adrian Puerto Aubel [PhD, Universita degli Studi di Milano Bicocca, Italy, from Apr 2018 until Jul 2018]
Shauna Laurene Ricker [Mount Allison Univ., Canada, from Mar 2018 until Jun 2018]
Akshay Sundararaman [IIT Bombay, from Jun 2018 until Jul 2018]

2. Overall Objectives

2.1. Overall objectives

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

2.1.1. Necessity of quantitative models

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

2.1.2. Specificities of distributed systems

While the above questions have already received partial answers, they remain largely unexplored in a distributed setting. We focus on structured systems, typically a network of dynamic systems with known interaction topology, the latter being either static or dynamic. Interactions can be synchronous or asynchronous. The state-space explosion raised by such systems has been addressed through two techniques. The first one consists in adopting true-concurrency models, which take advantage of the parallelism to reduce the size of the trajectory sets. The second one looks for modular or distributed “supervision" methods, taking the shape of a network of local supervisors, one per component. While these approaches are relatively well understood, their mixing with quantitative models remains a challenge (as an example, there exists no proper setting assembling concurrency theory with stochastic systems). This field is largely open both for modeling, analysis and verification purposes, and for distributed supervision techniques. The difficulties combine with the emergence of data-driven distributed systems (as web services or data centric systems), where the data exchanged by the various components influence both the behaviors of these components and the quantitative aspects of their reactions (e.g. QoS). Such systems call for symbolic or parametric approaches for which a theory is still missing.

2.1.3. New issues raised by large systems

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

3. Research Program

3.1. Analysis and verification of quantitative systems

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

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

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

3.2. Control of quantitative systems

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

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

3.3. Management of large or distributed systems

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

As more specific objectives, let us mention:

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

3.4. Data driven systems

Data-driven systems are systems whose behaviour depends both on explicit workflows (scheduling and durations of tasks, calls to possibly distant services, ...) and on the data processed by the system (stored data, parameters of a request, results of a request, ...). This family of systems covers workflows that convey data (business processes or information systems), transactional systems (web stores), large databases managed with rules (banking systems), collaborative environments (crowds, health systems), etc. These systems are distributed, modular, and open: they integrate components and sub-services distributed over the web, and accept requests from clients. Our objective is to provide validation and supervision tools for such systems. To achieve this goal, we have to solve several challenging tasks:

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

4. Application Domains

4.1. Smart transportation systems

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

4.2. Management of telecommunication networks and of data centers

Telecommunication-network management is a rich provider of research topics for the team, and some members of SUMO have a long background of contacts and transfer with industry in this domain. Networks are typical examples of large distributed dynamic systems, and their management raises numerous problems ranging from diagnosis (or root-cause analysis), to optimization, reconfiguration, provisioning, planning, verification, etc. They also bring new challenges to the community, for example on the modeling side: building or learning a

network model is a complex task, specifically because these models should reflect features like the layering, the multi-resolution view of components, the description of both functions, protocols and configuration, and they should also reflect dynamically-changing architectures. Besides modeling, management algorithms are also challenged by features like the size of systems, the need to work on abstractions, on partial models, on open systems, etc. The networking technology is now evolving toward software-defined networks, virtualized-network functions, multi-tenant systems, etc., which reinforces the need for more automation in the management of such systems.

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

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 crowd sourcing applications. 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 regarding the next tasks to be launched highly depend on collected data. For instance, in an epidemic-surveillance system, the aggregation of various reported disease cases may trigger alerts. Another example is crowd sourcing applications where user skills are used to complete tasks that are better performed by humans than computers. In return, this requires addressing imprecise and sometimes unreliable answers. We address several issues related to complex workflows and data. We study declarative and dynamic models that can handle workflows, data, uncertainty, and competence management.

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

4.4. Systems Biology

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

We are developing models and abstraction tools for systems biology. Studying these models suggests new reduction methods, such as considering populations instead of explicitly representing every single element into play (be it cells, molecules, etc): we thus develop algorithms handling a population symbolically, either in a continuous (probability distribution) or a discrete (parametric) way. An intermediate goal is to speed-up the 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.

4.5. Formal Verification of Smart Flexible Manufacturing Systems

Modern production/assembly lines are based on generic multipurpose programmable tools that are quickly reassembled and reprogrammed to accomodate new production processes. In a similar manner, complex products are also reengineered by assembling existing elementary functions, together with their correponding software. This modular construction principle enables a fast redesign of products or assembly chains, at the expense of possibly introducing bugs or malfunctions. Verification is thus a crucial step to guarantee the correctness of these systems. In particular, timing aspects are essential in order to both check correctness of an assembling with respect to some specification, but also in order to design software sensors that help the online monitoring of a system. The main challenges here essentially lie in the selection of appropriate verification formalisms, in the derivation of models for the systems under study, and in the size of the systems to handle.

5. Highlights of the Year

5.1. Highlights of the Year

- The ANR project TickTac led by Ocan Sankur was accepted and starts in March 2019.
- New partnership with Mitsubishi Electric (MERCE): one PhD thesis started in Fall 2018, and a member of MERCE will be hosted by SUMO in 2019.

5.1.1. Awards

BEST PAPER AWARD:

[11]
G. BACCI, P. BOUYER, U. FAHRENBERG, K. G. LARSEN, N. MARKEY, P.-A. REYNIER. *Optimal and Robust Controller Synthesis: Using Energy Timed Automata with Uncertainty*, in "FM 2018 - International Symposium on Formal Methods", Oxford, United Kingdom, LNCS, Springer, July 2018, vol. 10951, pp. 203-221 [*DOI :* 10.1007/978-3-319-95582-7_12], https://hal.archives-ouvertes.fr/hal-01889222

6. New Software and Platforms

6.1. Active Workspaces

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

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

6.2. DAXML

KEYWORDS: XML - Web Services - Distributed Software - Active documents
SCIENTIFIC DESCRIPTION: DAXML is an interpreter and implementation of Distributed Active Documents, a formalism for data centric design of Web Services. This implementation is based on a REST framework, and can run on a network of machines connected to internet and equiped with JAVA.

FUNCTIONAL DESCRIPTION: This prototype interprets distributed Active XML documents. It can be used to deploy services defined as active documents over the web.

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

6.3. Sigali

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

- Contact: Hervé Marchand

6.4. SIMSTORS

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

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

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

7. New Results

7.1. Analysis and Verification of Quantitative Systems

7.1.1. Verification of Concurrent Timed Systems

Participants : Éric Fabre, Loïc Hélouët, Karim Kecir

7.1.1.1. Combining Free Choice and Time in Petri Nets

Time Petri nets (TPNs) are a classical extension of Petri nets with timing constraints attached to transitions, for which most verification problems are undecidable. In [3], We consider TPNs under a strong semantics with multiple enablings 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 in the timed setting under a multi-enabling semantics. In particular, we show that the questions of firability (whether a chosen transition can fire), and termination (whether the net has a non-terminating run) are decidable for this class. Next, we consider the problem of robustness under guard enlargement and guard shrinking, i.e., whether a given property is preserved even if the system is implemented on an architecture with imprecise time measurement. For unbounded free choice TPNs with a multi-enabling semantics, we show decidability of robustness of firability and of termination under both guard enlargement and shrinking.

7.1.1.2. Production Systems with Concurrent Tasks

The work in [7] considers the realizability of expected schedules by production systems with concurrent tasks, bounded resources that have to be shared among tasks, and random behaviors and durations. Schedules are high level views of desired executions of systems represented as partial orders decorated with timing constraints. Production systems (production cells, train networks...) are modeled as stochastic time Petri nets STPNs with an elementary (1-bounded) semantics. We first propose a notion of time processes to give a partial order semantics to STPNs. We then consider boolean realizability: a schedule S is realizable by a net N if S embeds in a time process of N that satisfies all its constraints. However, with continuous time domains, the probability of a time process with exact dates is null. We hence consider probabilistic realizability up to a time units, that holds if the probability that N realizes S with constraints enlarged by a is strictly positive. Upon a sensible restriction guaranteeing time progress, boolean and probabilistic realizability of a schedule can be checked on the finite set of symbolic prefixes extracted from a bounded unfolding of the net. We give a construction technique for these prefixes and show that they represent all time processes of a net occurring up to a given maximal date. We then show how to verify existence of an embedding and compute the probability of its realization.

7.1.2. Testing of Timed Systems

Participants : Léo Henry, Thierry Jéron, Nicolas Markey

Partial observability and controllability are two well-known issues in test-case synthesis for interactive systems. In [25], we address the problem of partial control in the synthesis of test cases from timed-automata specifications. Building on the tioco timed testing framework, we extend a previous game interpretation of the test-synthesis problem from the untimed to the timed setting. This extension requires a deep reworking of the models, game interpretation and test-synthesis algorithms. We exhibit strategies of a game that tries to minimize both control losses and distance to the satisfaction of a test purpose, and prove they are winning under some fairness assumptions. This entails that when turning those strategies into test cases, we get properties such as soundness and exhaustiveness of the test synthesis method.

7.1.3. Analysis of Stochastic Systems

Participants : Nathalie Bertrand

A decade ago, Abdulla, Ben Henda and Mayr introduced the elegant concept of decisiveness for denumerable Markov chains. Roughly speaking, decisiveness allows one to lift most good properties from finite Markov chains to denumerable ones, and therefore to adapt existing verification algorithms to infinite-state models. Decisive Markov chains however do not encompass stochastic real-time systems, and general stochastic transition systems (STSs for short) are needed. In [4], we provide a framework to perform both the qualitative and the quantitative analysis of STSs. First, we define various notions of decisiveness, notions of fairness and of attractors for STSs, and make explicit the relationships between them. Then, we define a notion of abstraction, together with natural concepts of soundness and completeness, and we give general transfer properties, which will be central to several verification algorithms on STSs. We further design a generic construction which will be useful for the analysis of ω-regular properties, when a finite attractor exists, either in the system (if it is denumerable), or in a sound denumerable abstraction of the system. We next provide algorithms for

qualitative model-checking, and generic approximation procedures for quantitative model-checking. Finally, we instantiate our framework with stochastic timed automata (STA), generalized semi-Markov processes (GSMPs) and stochastic time Petri nets (STPNs), three models combining dense-time and probabilities. This allows us to derive decidability and approximability results for the verification of these models. Some of these results were known from the literature, but our generic approach permits to view them in a unified framework, and to obtain them with less effort. We also derive interesting new approximability results for STA, GSMPs and STPNs.

7.1.4. Opacity for Quantitative Systems

Participants : Loïc Hélouët, Hervé Marchand

7.1.4.1. Quantitative Opacity

The work in [26] considers quantitative approaches for opacity. A system satisfies opacity if its secret behaviors cannot be detected by any user of the system. Opacity of distributed systems was originally set as a boolean predicate before being quantified as measures in a probabilistic setting. This paper considers a different quantitative approach that measures the efforts that a malicious user has to make to detect a secret. This effort is measured as a distance w.r.t a regular profile specifying a normal behavior. This leads to several notions of quantitative opacity. When attackers are passive that is, when they just observe the system, quantitative opacity is brought back to a language inclusion problem, and is PSPACE-complete. When attackers are active, that is, interact with the system in order to detect secret behaviors within a finite depth observation, quantitative opacity turns out to be a two-player finite-state quantitative game of partial observation. A winning strategy for an attacker is a sequence of interactions with the system leading to a secret detection without exceeding some profile deviation measure threshold. In this active setting, the complexity of opacity is EXPTIME-complete.

7.1.4.2. Opacity with Powerful Attackers

In [27], we consider state-based opacity in a setting where attackers of a secret have additional observation capabilities allowing them to know which inputs are allowed by a system. This capability allows attackers of a system to partially disambiguate the possible set of states the system might be in, and increases the power of an attacker. We show that regular opacity (opacity of a property described by a regular language) is decidable in this setting. We then address the question of controlling a system so that it becomes opaque, and solve this question by recasting the problem in a game setting.

7.1.5. Diagnosis of Quantitative Systems

Participants : Blaise Genest, Éric Fabre, Hugo Bazille, Nicolas Markey

7.1.5.1. Diagnosis for Timed Automata

In [20], we consider the problems of efficiently diagnosing and predicting what did (or will) happen in a partially-observable one-clock timed automaton. We introduce timed sets as a formalism to keep track of the evolution of the reachable configurations over time, and build a candidate diagnoser for our timed automaton. We report on our implementation of this approach compared to the algorithm of Tripakis, *Fault diagnosis for timed automata*, 2002.

7.1.5.2. Quantitative Diagnosis for Stochastic Systems

For stochastic systems, several diagnosability properties have been defined. The simplest one, also called A-diagnosability, characterizes the fact that after each fault, detection will almost surely occur. We have considered quantitative versions of the problem in [17]. We are interested in quantifying how fast the diagnosability can be performed. For that, we give an algorithm to compute in polynomial time any moment of the distribution of the detection delay. This allows one to approximate the distribution of detection delay, and to provide lower bounds on the probability that detection takes place at most T events after the fault.

One problem with A-diagnosability is that in the worst case, a subset construction needs to be performed, leading to an exponential blow-up in the number of states. To mitigate this, we proposed in [16] different techniques that avoid this blow-up in a large number of cases.

7.2. Control of Quantitative Systems

7.2.1. Reactive Synthesis for Quantitative Systems

Participants : Hervé Marchand, Nicolas Markey

7.2.1.1. Optimal and Robust Controller Synthesis

We propose a novel framework for the synthesis of robust and optimal energy-aware controllers. The framework is based on energy timed automata, allowing for easy expression of timing-constraints and variable energy-rates. We prove decidability of the energy-constrained infinite-run problem in settings with both certainty and uncertainty of the energy-rates. We also consider the optimization problem of identifying the minimal upper bound that will permit existence of energy-constrained infinite runs. Our algorithms are based on quantifier elimination for linear real arithmetic. Using Mathematica and Mjollnir, we illustrate our framework through a real industrial example of a hydraulic oil pump. Compared with previous approaches our method is completely automated and provides improved results.

7.2.1.2. Average-Energy Games

Two-player quantitative zero-sum games provide a natural framework to synthesize controllers with performance guarantees for reactive systems within an uncontrollable environment. Classical settings include mean-payoff games, where the objective is to optimize the long-run average gain per action, and energy games, where the system has to avoid running out of energy. In [5], we study average-energy games, where the goal is to optimize the long-run average of the accumulated energy. We show that this objective arises naturally in several applications, and that it yields interesting connections with previous concepts in the literature. We prove that deciding the winner in such games is in NP∩coNP and at least as hard as solving mean-payoff games, and we establish that memoryless strategies suffice to win. We also consider the case where the system has to minimize the average-energy while maintaining the accumulated energy within predefined bounds at all times: this corresponds to operating with a finite-capacity storage for energy. We give results for one-player and two-player games, and establish complexity bounds and memory requirements.

7.2.1.3. Compositional Controller Synthesis

In [8], we present a correct-by-design method of state-dependent control synthesis for sampled switching systems. Given a target region R of the state space, our method builds a capture set S and a control that steers any element of S into R. The method works by iterated backward reachability from R. It is also used to synthesize a recurrence control that makes any state of R return to R infinitely often. We explain how the synthesis method can be performed in a compositional manner, and apply it to the synthesis of a compositional control for a concrete floor-heating system with 11 rooms and up to $2^{11} = 2048$ switching modes.

7.2.1.4. Symbolic Algorithms for Control

In [18], we put forward a new modeling technique for Dynamic Resource Management (DRM) based on discrete events control for symbolic logico-numerical systems, especially Discrete Controller Synthesis (DCS). The resulting models involve state and input variables defined on an infinite domain (Integers), thereby no exact DCS algorithm exists for safety control. We thus formally define the notion of limited lookahead, and associated best-effort control objectives targeting safety and optimization on a sliding window for a number of steps ahead. We give symbolic algorithms, illustrate our approach on an example model for DRM, and report on performance results based on an implementation in our tool ReaX.

7.2.2. Control of Stochastic Systems

Participants : Nathalie Bertrand, Blaise Genest, Nicolas Markey, Ocan Sankur

7.2.2.1. Multi-Weighted Markov Decision Processes

In [19], we study the synthesis of schedulers in double-weighted Markov decision processes, which satisfy both a percentile constraint over a weighted reachability condition, and a quantitative constraint on the expected value of a random variable defined using a weighted reachability condition. This problem is inspired by the modelization of an electric-vehicle charging problem. We study the cartography of the problem, when one parameter varies, and show how a partial cartography can be obtained via two sequences of opimization problems. We discuss completeness and feasability of the method.

7.2.2.2. Stochastic Shortest Paths and Weight-Bounded Reachability

The work in [14] deals with finite-state Markov decision processes (MDPs) with integer weights assigned to each state-action pair. New algorithms are presented to classify end components according to their limiting behavior with respect to the accumulated weights. These algorithms are used to provide solutions for two types of fundamental problems for integer-weighted MDPs. First, a polynomial-time algorithm for the classical stochastic shortest path problem is presented, generalizing known results for special classes of weighted MDPs. Second, qualitative probability constraints for weight-bounded (repeated) reachability conditions are addressed. Among others, it is shown that the problem to decide whether a disjunction of weight-bounded reachability conditions holds almost surely under some scheduler belongs to NP∩coNP, is solvable in pseudo-polynomial time and is at least as hard as solving two-player mean-payoff games, while the corresponding problem for universal quantification over schedulers is solvable in polynomial time.

7.2.2.3. Distribution-based Objectives for Markov Decision Processes

In the scope of associated team EQuaVE, we have considered quantitative control of stochastic systems [10]. More precisely, the aim is to control the MDP so that the distribution over states stays inside a safe polytope. This represents a trade off between perfect information (the system is in exactly one state) and no information (we need to consider the belief distribution over states, and further the action played by the controller cannot be based on the state). Interestingly, we get an efficient polynomial time complexity to check whether there exists a distribution from which there exists a controller keeping the MDP in the safe polytope. This is surprising as the same question from a given distribution is not known to be decidable, even if the controller is fixed. Also, we have a co-NP complexity for deciding whether for every initial distribution, there is controller keeping the distribution in the safe polytope. Finally, we showed that an alternate representation of the input polytope allows us to get a polynomial time algorithm for safety from all initial distributions.

7.3. Management of Large Distributed Systems

7.3.1. Parameterized Systems

Participants : Nathalie Bertrand, Nicolas Markey

Reconfigurable broadcast networks provide a convenient formalism for modelling and reasoning about networks of mobile agents broadcasting messages to other agents following some (evolving) communication topology. The parameterized verification of such models aims at checking whether a given property holds irrespective of the initial configuration (number of agents, initial states and initial communication topology). In [15], we focus on the synchronization property, asking whether all agents converge to a set of target states after some execution. This problem is known to be decidable in polynomial time when no constraints are imposed on the evolution of the communication topology (while it is undecidable for static broadcast networks).

During the internship of A.R. Balasubramanian, we investigated how various constraints on reconfigurations affect the decidability and complexity of the synchronization problem. In particular, we show that when bounding the number of reconfigured links between two communications steps by a constant, synchronization becomes undecidable; on the other hand, synchronization remains decidable in PTIME when the bound grows with the number of agents.

7.3.2. Smart Regulation for Urban Trains

Participants : Loïc Hélouët, Karim Kecir, Flavia Palmieri

We have launched a new thread of research for efficient regulation with the M2 internship of Flavia Palmieri. The objective is to use efficient planning techniques to perform regulation in metro networks. Usually, regulation algorithms are simple reactive rules, that build decisions from local measures of train delays. These algorithms are arbitrary decisions, which efficiency is only empirically proved. On the other hand, optimality of regulation decision with respect to some quality criterion could be achieved through optimization algorithms, associating an optimal execution date to next events (arrivals and departures) while fulfilling constraints on causal dependencies, track allocations, etc. However, these algorithms are NP-complete, and do not return answers fast enough to be used online as regulation tools (use usually expects a decision within a few seconds after a train's arrival). During this internship, we have started integrating optimal planning techniques to regulation schemes. The main idea is to perform optimization online for a subset of the next occurring events. Performance of this regulation scheme is currently under evaluation.

7.3.3. Analysis of Concurrent Systems

Participants : Éric Fabre, Loïc Hélouët, Engel Lefaucheux

7.3.3.1. Generalization of Unfolding Techniques for Petri Nets

The verification of concurrent systems relies on an adequate representation of their trajectory sets, where each trajectory is a partial order of events. Several compact structures have been proposed in the past, starting with unfoldings and event structures. While unfoldings expand both time and conflicts, they generate extremely large branching constructions. To avoid expanding conflicts where they are not meaningful, more compact structures were proposed, as merged processes and trellis processes. In [23], we examine structures that would not fully unfold time as well, thus resulting in partially unfolded nets. To do so, we proposed the notion of spread nets, (safe) Petri nets equipped with vector clocks on places and with ticking functions on transitions, and such that vector clocks are consistent with the ticking of transitions. Such nets allow one to generalize previous constructions as unfoldings and merged processes, and can be fully paremeterized to display or hide some behaviors of the net, and thus facilitate its analysis.

7.3.3.2. Hyper Partial Order Logic

In [21], we define HyPOL, a local hyper logic for partial order models, expressing properties of sets of runs. These properties depict shapes of causal dependencies in sets of partially ordered executions, with similarity relations defined as isomorphisms of past observations. This type of logics is tailored to address security properties of concurrent systems. Unsurprisingly, since comparison of projections are included, satisfiability of this logic is undecidable. We then address model checking of HyPOL and show that, already for safe Petri nets, the problem is undecidable. Fortunately, sensible restrictions of observations and nets allow us to bring back model checking of HyPOL to a decidable problem, namely model checking of MSO on graphs of bounded treewidth.

7.3.3.3. Diagnosability Analysis for Concurrent Systems

Petri nets have been proposed as a fundamental model for discrete-event systems in a wide variety of applications and have been an asset to reduce the computational complexity involved in solving a series of problems, such as control, state estimation, fault diagnosis, etc. Many of those problems require an analysis of the reachability graph of the Petri net. The basis reachability graph is a condensed version of the reachability graph that was introduced to efficiently solve problems linked to partial observation. It was in particular used for diagnosis which consists in deciding whether some fault events occurred or not in the system, given partial observations on the run of the system. However this method is, with very specific exceptions, limited to bounded Petri nets. In [28], we introduce the notion of basis coverability graph to remove this requirement. We then establish the relationship between the coverability graph and the basis coverability graph. Finally, we focus on the diagnosability problem: we show how the basis coverability graph can be used to get an efficient algorithm.

7.4. Data Driven Systems

7.4.1. Modular composition of Guarded Attribute Grammars

Participants : Éric Badouel

We investigate how the role of a user in a distributed collaborative systems modelled by a Guarded Attribute Grammar can be associated with a domain specific language (DSL) encapsulating a specific domain knowledge (expertise) and defining a set of services (a language-oriented approach). These DSLs communicate through service calls (a service-oriented approach).

Language oriented programming is an approach to software composition based on domain specific languages (DSL) dedicated to specific aspects of an application domain. In order to combine such languages we embed them into a host language (namely Haskell, a strongly typed higher-order lazy functional language). A DSL is then given by an algebraic type, whose operators are the constructors of abstract syntax trees. Such a multi-sorted signature is associated to a polynomial functor. An algebra for this functor tells us how to interpret the programs. Using Bekić's Theorem we defined in [13] a modular decomposition of algebras that leads to a class of parametric multi-sorted signatures, associated with regular functors, allowing for the modular design of DSLs.

In [12] we have addressed the problem of component reuse in the context of service-oriented programming and more specifically for the design of user-centric distributed collaborative systems modelled by Guarded Attribute Grammars. Following the contract-based specification of components we developp an approach to an interface theory for the roles in a collaborative system in three stages: we define a composition of interfaces that specifies how the component behaves with respect to its environement, we introduce an implementation order on interfaces and finally a residual operation on interfaces characterizing the systems that, when composed with a given component, can complement it in order to realize a global specification.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

8.1.1. Nokia Bell Labs - ADR SAPIENS

Several researchers of SUMO are involved in the joint research lab of Nokia Bell Labs France and Inria. We participate in the common research team SAPIENS (Smart Automated and Programmable Infrastructures for End-to-end Networks and Services), previously named "Softwarization of Everything." This team involves several other Inria teams : Convecs, Diverse and Spades. SUMO focuses on the management of reconfigurable systems, both at the edge (IoT based applications) and in the core (e.g. virtualized IMS systems). In particular, we focus on control and diagnosis issues for such systems. Two PhD students are involved in the project. Erij Elmajed (2nd year), on the topic of Diagnosis of virtualized and reconfigurable systems supervised by Éric Fabre and Armen Aghasaryan (Nokia Bell Labs). Abdul Majith (to start in January 2019) on Controller Synthesis of Adaptive Systems, supervised by Hervé Marchand, Ocan Sankur, and Dinh Thai Bui (Nokia Bell Labs).

8.1.2. Orange Labs

SUMO is participating in IOLab, the common lab of Orange Labs and Inria, dedicated to the design and management of Software Defined Networks. Our activities concern the diagnosis of malfunctions in virtualized multi-tenant networks. This collaboration supports one Cifre PhD student, Sihem Cherrared (2nd year), supervised by Eric Fabre, Gregor Goessler (Inria team Spades in Grenoble) and Sofiane Imadali (Orange Labs).

8.1.3. Alstom Transport - P22

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

8.1.4. Mitsubishi Electric Research Center Europe (MERCE)

Several researchers of SUMO are involved in a collaboration with the formal verification team of MERCE on model checking of real-time systems. The members of the formal verification team at MERCE work on different aspects of formal verification and participate to academic collaborations.

The SUMO team and MERCE have jointly supervised an M1 internship (Ludovic Landuré), and are supervising a Cifre PhD student (Emily Clement) funded by MERCE, started this fall. Reiya Noguchi, a member of MERCE will be hosted by the SUMO team in 2019.

9. Partnerships and Cooperations

9.1. Regional Initiatives

9.1.1. Rennes Métropole: Allocation d'Installation Scientifique (AIS)

- Individual grant, led by Nicolas Markey

The objective of this project is to explore two research directions in the continuity of recent works: a truly quantitative theory of formal verification on the one hand, and the development of strategy-synthesis algorithms for modular systems on the other hand.

9.2. National Initiatives

9.2.1. ANR TickTac: Efficient Techniques for Verification and Synthesis of Real-Time Systems (2019-2023)

- Led by Ocan Sankur (SUMO);
- Participants: Thierry Jéron, Nicolas Markey, Ocan Sankur
- Partners: LSV (Cachan), ISIR (Paris), LaBRI (Bordeaux), LRDE (Paris), LIF (Marseille)

The aim of TickTac is to develop novel algorithms for the verification and synthesis of real-time systems using the timed automata formalism. One of the project's objectives is to develop an open-source and configurable model checker which will allow the community to compare algorithms. The algorithms and the tool will be used on a motion planning case study for robotics.

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

- web site at http://perso.crans.org/~genest/stoch.html.
- Led by Blaise Genest (SUMO);
- Participants: Nathalie Bertrand, Blaise Genest, Éric Fabre, Matthieu Pichené;
- Partners: Inria Project Team CONTRAINTES (Rocquencourt), LaBRI (Bordeaux), and IRIF (Paris).

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

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

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

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

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

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

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

This year we have been mainly intrested in the extension of the SimGrid programming model of MPI with synchronization primitives, the formalisation in ATL, of this model, and its adaptation to dynamic partial-order-reduction methods (DPOR) that allow to reduce the explored state space. A prototype implementation of an existing method that combines DPOR with true-concurrency models has been experimented on toy examples.

9.2.5. National informal collaborations

The team collaborates with the following researchers:

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

9.3. International Initiatives

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

9.3.1.1. EQUAVE

Title: Efficient Quantitative Verification

International Partner (Institution - Laboratory - Researcher):

Indian Institute of Technology Bombay (India) - Dpt of Computer Science and Engineering - S. Akshay

Start year: 2018

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

Formal verification has been addressed for a long time. A lot of effort has been devoted to boolean verification, i.e., formal analyis of systems that check whether a given property is true or false.

In many settings, a boolean verdict is not sufficient. The notions of interest are for instance the amount of confidential information leaked by a system, the proportion of some protein after a duration in some experiment in a biological system, whether a distributed protocol satisfies some property only for a bounded number of participants... This calls for quantitative verification, in which algorithms compute a value such as the probability for a property to hold, the mean cost of runs satisfying it, the time needed to achieve a complex workflow...

A second limitation of formal verification is the efficiency of algorithms. Even for simple questions, verification is rapidly PSPACE-complete. However, some classes of models allow polynomial time verification. The key techniques to master complexity are to use concurrency, approximation, etc

The objective of this project is to study efficient techniques for quantitative verification, and develop efficient algorithms for models such as stochastic games, timed and concurrent systems,

9.3.1.2. QuantProb

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

International Partner (Institution - Laboratory - Researcher):

Technical University of Dresde (Germany), Faculty of Computer Science, Christel Baier

Start year: 2016

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

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

9.3.2. Inria International Partners

9.3.2.1. Informal International Partners

The team collaborates with the following researchers:

- Jean-François Raskin, Gilles Geeraerts (Université Libre de Bruxelles, Belgium) on multiplayer game theory and synthesis;
- Thomas Brihaye (U Mons, Belgium) on the verification of stochastic timed systems;
- Mickael Randour (U Mons, Belgium) on quantitative games for synthesis;

- Kim G. Larsen (U Aalborg, Denmark) on quantitative timed games, and on topics related to urban train systems modeling;
- Josef Widder, Marijana Laźic (TU Wien, Austria), Igor Konnov (Inria Nancy, LORIA) on the automated verification of randomized distributed algorithms.
- John Mullins (Polytechnique Montréal, Canada), on topics related to security and opacity;
- S. Akshay (IIT Bombay, India) on topics related to timed concurrent models;
- Andrea D'ariano (University Roma Tre, Italy), on topics related to train regulation.
- Alessandro Giua and Michele Pinna (Univ. Cagliari, Italy), on diagnosis and unfolding techniques for concurrent systems.

9.4. International Research Visitors

9.4.1. Visits of International Scientists

- In June 2018, S. Akshay visited the SUMO team for one week.
- Laurie Ricker (Mount Allison University, Canada) visited the team during 3 months in 2018.
- Josef Widder visited the team as an invitee of ISTIC (Université Rennes 1) : 2 weeks in September 2018.
- Romulo Meira-Goes (PhD student of S. Lafortune, University of Michigan, USA) visited our team during four months in 2018 (Synthesis of Supervisors Robust Against Sensor Deceptions Attacks).

9.4.1.1. Internships

- Flavia Palmieri, May-June 2018, Loïc Hélouët.
- M2 internship of Ritam Raha, October-December 2018, Nicolas Markey and Loïc Hélouët.
- Internship of undergraduate student Adwait Amit Godbole, Blaise Genest.

9.4.2. Visits to International Teams

In October 2018, Loïc Hélouët visited IIT Bombay and IIT Delhi for 10 days, to work within the associated team EQUAVE.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

- Éric Badouel was the General Chair of CARI 2018, Stellenbosch, South Africa.
- Hervé Marchand is a member of the IFAC Technical Committees (TC 1.3 on Discrete Event and Hybrid Systems) since 2005. Hervé Marchand is a member of the steering committee of MSR (modélisation de systèmes réactifs) since 2012 and became the president of this steering committee in November 2017;
- Nathalie Bertrand and Nicolas Markey are members of the steering committee of the Summer School MOVEP (*Modélisation et Vérification des Processus Parallèles*).

10.1.1.2. Member of the Organizing Committees

Nicolas Markey coorganized the 6th Workshop SR 2018 (Oxford, 7-8 july 2018).

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

- Hervé Marchand served on the Program Committee of WODES 2018
- Éric Badouel was member of the program committees of VECOS 2018, ATAED 2018, CARI 2018, ICTAC 2018.s
- Loïc Hélouët was member of the program Comitee of ACSD'2018.
- Thierry Jéron served on the Program Committees of the following international conferences: SAC-SVT 2018, TAP 2018.
- Nathalie Bertrand was a member of the PC of the following international events: FoSSaCS'18, ICALP'18, Highlights'18, MoRe'18 and RP'18.
- Ocan Sankur was a member of the PC of FORMATS'18 and SYNT'18.

10.1.2.2. Reviewer

In 2018, members of SUMO reviewed submissions for following conferences: VECOS, ATAED, CARI, ICTAC, CONCUR, SOFSEM, FOCS, ATVA, VMCAI, ICALP, SAC-SVT, TAP, ACSD, MFCS, STACS, WODES, HSCC, FSTTCS, CSL, AAMAS, TACAS, FoSSaCS, LICS, PODC, MORE, RP.

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

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

10.1.3.2. Reviewer - Reviewing Activities

In 2018, members of SUMO reviewed submissions for following journals: Automatica, Fundamenta Informaticae, Information and Computation, The Scientific Annals of Computer Science, Science of Computer Programming, ACM Transactions on Computational Logic, ACM Transactions on Embedded Computing Systems, Journal of Systems and Software, Mathematical Review (MathSciNet), Journal of Discrete Event Dynamical Systems, Formal Methods in System Design, Software Testing, Verification and Reliability, Journal of Logic and Computation, IEEE Transactions on Automatic Control, PLoS one, Performance Evaluation, Artificial Intelligence, Journal of Logic and Algebraic Methods in Programming, Logical Methods in Computer Science, ACM Transactions on Modeling and Computer Simulation, Journal of Systems and Software.

10.1.4. Invited Talks

Loïc Hélouët was invited to give a talk at IIT Delhi on hyperlogics on November 2018.

10.1.5. Leadership within the Scientific Community

Nathalie Bertrand is the co-head of the *Groupe de Travail Verif* (together with Pierre-Alain Reynier (LIS, Marseille)) which is a part of *GDR Informatique Mathématique (GDR-IM)*.

10.1.6. Scientific Expertise

- Eric Badouel was member of the jury discerning the Ibni Prize.
- Thierry Jéron was a reviewer for ANR.
- Blaise Genest was a reviewer for Austrian Academy of Sciences.
- Nathalie Bertrand was a reviewer for Thelam Fundand FWO (Belgium).
- Éric Fabre was a reviewer for the Ministry of Research, in the "Credit Impot Recherche" initiative.

10.1.7. Research Administration

- Éric Fabre is the co-director (with Olivier Audouin, Nokia) of the joint lab of Nokia Bell Labs France and Inria. The lab has been running for 9 years and started in Nov. 2017 its 3rd phase of joint research teams. A series of 6 new just started in 2017, for a duration of 4 years. They cover topics like network virtualization, network management, information theory, (distributed) machine learning, network security. SUMO is involved in the joint team SAPIENS.

- Loïc Hélouët is a representative of researchers in the Comité de Centre of Inria Rennes. He is also part of the bureau of the Comité de Centre, leads a working group of the comité and contributes to another. In 2018, he joined the COST-GTRI, who is in charge of evaluation of international programs such as Inria associated teams. He is the principal investigator for the french side of the EQUAVE associated team. He leads the P22 projects with Alstom Transport and is responsible for Workpackage 2 of the Headwork ANR project.
- Hervé Marchand is chairman of the *Comission des utilisateurs des moyens informatiques* (CUMI) in Rennes and member of the *Action de développement technologique*(ADT) commission in Rennes.
- Thierry Jéron is a Member Committee Substitute for COST IC1402 ARVI (Runtime Verification beyond Monitoring). He is a member of the IFIP Working Group 10.2 on Embedded Systems. He is a member of the *Comité d'orientation scientifique* (COS) Prospective of Irisa Rennes and a member of the Comité de Centre of Inria Rennes. Since 2016 he is *référent chercheur* for the Inria-Rennes research center.
- Nathalie Bertrand is elected member of the Conseil National des Universités, section 27 (computer science).

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Nathalie Bertrand, Advanced Algorithms (ALGO2), 20h, L3, Univ Rennes 1, France;

Licence: Nathalie Bertrand, Theory of Rational Languages (THLR), 26h, EPITA 2nd year, Rennes, France.

Licence: Loïc Hélouët, JAVA and algorithms, L2, 40h, INSA de Rennes, France.

Licence: Loïc Hélouët, Practical studies (development of a small project), 8h, INSA de Rennes, France.

Master: Loïc Hélouët, Algorithms, 2h, Agrégation, ENS Rennes, France;

Master: Nicolas Markey, Verification of Complex Systems (CSV), 10h, M2, Univ Rennes 1, France;

Master: Nicolas Markey, Algorithms, 14h, Agrégation, ENS Rennes, France;

Master : Nathalie Bertrand, Language Theory; Algorithms, 20h, Agrégation, ENS Rennes, France;

Master: Ocan Sankur, Verification of Complex Systems (CSV), 10h, M2, Univ Rennes 1, France;

Master: Ocan Sankur, *Travaux pratiques*, Analyse et Conception Formelle (ACF), 22h, M1, Univ Rennes 1, France;

Master: Éric Fabre, Models and Algorithms for Distributed Systems (MADS), 10h, M2, Univ Rennes 1, France;

Master: Éric Fabre Information Theory, 15h, M1, ENS Rennes, France.

10.2.2. Supervision

- PhD: Matthieu Pichené, Multi-level analysis in computational system biology : the case of HeLa cells under apoptosis treatment [2], Univ. Rennes 1. The defense took place on June 25, 2018, and was supervised by Blaise Genest.
- PhD: Engel Lefaucheux, Controlling information in probabilistic systems [1], Univ. Rennes 1. The defence took place on September 24, 2018, and was supervised by Nathalie Bertrand and Serge Haddad (ENS Paris-Saclay).
- PhD in progress: Hugo Bazille, Information flows in quantitative dynamic systems, started oct. 2016, Blaise Genest and Éric Fabre.
- PhD in progress: Sihem Cherrared, Diagnosis of multi-tenant programmable networks, started Dec. 2016, Éric Fabre, Gregor Goessler (Inria, Spades) and Sofiane Imadali (Orange).

- PhD in progress: Emily Clement, Verification and synthesis of control systems: efficiency and robustnes, started Dec. 2018, supervised by Thierry Jéron, Nicolas Markey, and David Mentré (Mitsubishi Electric)
- PhD in progress: Rodrigue Djeumen Djatcha, Collaborative Model for Urban Crowdsourcing, University of Douala, Cameroon, supervised by Éric Badouel.
- PhD in progress: Erij Elmajed, Diagnosis of reconfigurable systems, started March 2017, Éric Fabre and Armen Aghasaryan (Nokia).
- PhD in progress: Léo Henry, Optimal test-case generation with game theory, started Oct. 2018, supervised by Thierry Jéron and Nicolas Markey.
- PhD in progress: Karim Kecir, Régulation et robustesse des systèmes ferroviaires urbains, defense planned on the 1st semester 2019, supervised by Loïc Hélouët and Pierre Dersin (Alstom).
- PhD in progress: Anirban Majumdar, Games for distributed networks: models and algorithms, ENS Paris Saclay, France, supervised by Nathalie Bertrand and Patricia Bouyer.
- PhD in progress: Rituraj Singh, Data-centric Workflows for Crowdsourcing Applications, defense planned on February 2021, supervised by Loïc Hélouët.
- PhD in progress: Robert Fondze Jr Nsaibirni, A Guarded Attribute Grammar Based Model for User Centered, Distributed, and Collaborative Case Management – Case of the Disease Surveillance Process, University of Yaoundé, Cameroon, supervised by Éric Badouel.
- PhD in progress: The Anh Pham, Dynamic Formal Verification of High Performance Runtimes and Applications, started Nov. 2016, supervised by Thierry Jéron and Martin Quinson (Myriads, Inria Rennes).
- PhD in progress: Arthur Queffelec, Tradeoff between Robustness and Optimality in Strategic Reasoning, started Nov. 2018, supervised by Ocan Sankur and François Schwarzentruber (Logica, Irisa).
- PhD in progress: Victor Roussanaly, Efficient verification of timed systems, started Sep. 2017, supervised by Nicolas Markey and Ocan Sankur.
- PhD in progress: Suman Sadhukhan, Modelling and parameterized verification of mobile networks, started Oct. 2018, supervised by Nathalie Bertrand, Nicolas Markey, Ocan Sankur.

10.2.2.1. Master Students

- Ocan Sankur co-supervised the master's thesis (M2) of Arthur Queffelec.
- Thierry Jéron and Nicolas Markey supervised the master's thesis (M2) of Léo Henry.
- Nathalie Bertrand, Loïc Hélouët and Ocan Sankur supervised a training period (3 h/week during 6 months) for a group of master 1 students. The topic was application of model checking to assess the performance of regulation algorithms.
- Loïc Hélouët supervised the internship of master student Flavia Palmieri.

10.2.2.2. Other Internships

- L3 Intership of Mélanie Bratulic, supervised by Sophie Pinchinat (Logica, Irisa) and Thierry Jéron.

10.2.3. Juries

10.2.3.1. PhD Defenses

- Loïc Hélouët was an examiner in the PhD defense of Yann Duplouy, Ecole Normale Supérieure Paris-Saclay, November 2018.
- Thierry Jéron was a reviewer for the PhD thesis of Antoine EL HOKAYEM, Univ. Grenoble, December 2018.

- Nicolas Markey was a reviewer for the PhD thesis of Benedikt Brütsch (Decembre 20, 2018, Aachen, Germany; PhD student of Wolfgang Thomas); a reviewer for the PhD thesis of Petr Bezděk (on March 9, 2018, Masaryk University, Brno, Czech Republic; PhD student of Ivana Černá); and a reviewer for the PhD thesis of Nicola Gigante (January 2019, Udine, Italy; PhD student of Angelo Montanari).
- Nathalie Bertrand was an examiner for the PhD thesis of Philipp Schlehuber-Caissier, Sorbonne Université, December, 14 2018; a reviewer for the PhD thesis of L'uboš Korenčiak, Masaryk University (Czech Republic), April 2018; and an examiner for the PhD thesis of Othmane Rezine, Uppsala University, January, 12 2018.

10.2.3.2. Other Juries

- Nathalie Bertrand was in the hiring committee for CRCN positions at Inria Rennes Bretagne Atlantique in 2018. She was also in the hiring committee for a Maitre de conférences position at Université Paris-Est Créteil in spring 2018.

10.2.4. Books

Nicolas Markey co-authored the chapter on *Model Checking Real-Time Systems* in the book *Handbook of Model Checking* [29].

10.3. Popularization

10.3.1. Internal or external Inria responsibilities

Éric Badouel is the co-director (with Moussa Lo, UGB, Saint-Louis du Sénégal) of LIRIMA, the Inria International Lab for Africa. He is scientific officer for the African and Middle-East region at Inria DPEI (European and International Partnership Department). He is member of the executive board of GIS SARIMA.

10.3.2. Articles and contents

- Ocan Sankur published an article on formal verification for the Turkish Academy of Sciences: "How to verify computer systems on which our lives depend" on Nov. 2018.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] E. LEFAUCHEUX. *Controlling information in Probabilistic Systems*, Université Rennes 1, September 2018, https://hal.inria.fr/tel-01946840

[2] M. PICHENÉ. *Multi-level analysis in computational system biology : the case of HeLa cells under apoptosis treatment*, Université Rennes 1, June 2018, https://tel.archives-ouvertes.fr/tel-01935280

Articles in International Peer-Reviewed Journals

[3] S. AKSHAY, L. HÉLOUËT, R. PHAWADE. *Combining Free choice and Time in Petri Nets*, in "Journal of Logical and Algebraic Methods in Programming", November 2018, pp. 1-36 [*DOI :* 10.1016/J.JLAMP.2018.11.006], https://hal.inria.fr/hal-01931728

[4] N. BERTRAND, P. BOUYER, T. BRIHAYE, P. P. CARLIER. *When are stochastic transition systems tameable?*, in "Journal of Logical and Algebraic Methods in Programming", 2018, vol. 99, pp. 41-96 [*DOI :* 10.1016/J.JLAMP.2018.03.004], https://hal.inria.fr/hal-01938135

[5] P. BOUYER, N. MARKEY, M. RANDOUR, K. G. LARSEN, S. LAURSEN. *Average-energy games*, in "Acta Informatica", March 2018, vol. 55, n° 2, pp. 91 - 127 [*DOI :* 10.1007/s00236-016-0274-1], https://hal.archives-ouvertes.fr/hal-01889005

[6] E. FABRE, L. HÉLOUËT, E. LEFAUCHEUX, H. MARCHAND. *Diagnosability of Repairable Faults*, in "Discrete Event Dynamic Systems", 2018, vol. 28, n° 2, pp. 183-213 [*DOI :* 10.1007/s10626-017-0255-8], https://hal.inria.fr/hal-01646911

[7] L. HÉLOUËT, K. KECIR. *Realizability of schedules by stochastic time Petri nets with blocking semantics*, in "Science of Computer Programming", June 2018, vol. 157, pp. 71-102 [*DOI :* 10.1016/J.SCICO.2017.12.004], https://hal.inria.fr/hal-01942241

[8] A. LE COËNT, L. FRIBOURG, N. MARKEY, F. DE VUYST, L. CHAMOIN. *Compositional synthesis of state-dependent switching control*, in "Theoretical Computer Science", November 2018, vol. 750, pp. 53-68 [*DOI :* 10.1016/J.TCS.2018.01.021], https://hal.archives-ouvertes.fr/hal-01860379

[9] M. RENARD, Y. FALCONE, A. ROLLET, T. JÉRON, H. MARCHAND. *Optimal Enforcement of (Timed) Properties with Uncontrollable Events*, in "Mathematical Structures in Computer Science", 2019, vol. 29, n° 1, pp. 169-214 [*DOI :* 10.1017/S0960129517000123], https://hal.archives-ouvertes.fr/hal-01262444

International Conferences with Proceedings

[10] S. AKSHAY, B. GENEST, N. VYAS. *Distribution-based objectives for Markov Decision Processes*, in "LICS 2018, the 33rd Annual ACM/IEEE Symposium", Oxford, United Kingdom, Proceedings of LICS 2018, ACM Press, July 2018, pp. 36-45 [*DOI :* 10.1145/3209108.3209185], https://hal.archives-ouvertes.fr/hal-01933978

[11] *Best Paper*
G. BACCI, P. BOUYER, U. FAHRENBERG, K. G. LARSEN, N. MARKEY, P.-A. REYNIER. *Optimal and Robust Controller Synthesis: Using Energy Timed Automata with Uncertainty*, in "FM 2018 - International Symposium on Formal Methods", Oxford, United Kingdom, LNCS, Springer, July 2018, vol. 10951, pp. 203-221 [*DOI :* 10.1007/978-3-319-95582-7_12], https://hal.archives-ouvertes.fr/hal-01889222.

[12] E. BADOUEL, R. DJEUMEN DJATCHA. *Interfaces of Roles in Distributed Collaborative Systems*, in "CARI 2018 - Colloque Africain sur la Recherche en Informatique et Mathématiques Appliquées", Stellenbosch, South Africa, October 2018, pp. 182-193, https://hal.inria.fr/hal-01919465

[13] E. BADOUEL, R. DJEUMEN DJATCHA. *Modular Design of Domain-Specific Languages using Splittings of Catamorphisms*, in "ICTAC 2018 - 15th International Colloquium on the Theoretical Aspects of Computing", Stellenbosch, South Africa, B. FISCHER, T. UUSTALU (editors), LNCS, Springer, October 2018, vol. 11187, pp. 62-79 [*DOI :* 10.1007/978-3-030-02508-3_4], https://hal.inria.fr/hal-01919423

[14] C. BAIER, N. BERTRAND, C. DUBSLAFF, D. GBUREK, O. SANKUR. *Stochastic Shortest Paths and Weight-Bounded Properties in Markov Decision Processes*, in "LICS '18 - 33rd Annual ACM/IEEE Symposium on Logic in Computer Science", Oxford, United Kingdom, ACM Press, July 2018, pp. 86-94 [*DOI :* 10.1145/3209108.3209184], https://hal.archives-ouvertes.fr/hal-01883409

[15] A. BALASUBRAMANIAN, N. BERTRAND, N. MARKEY. *Parameterized verification of synchronization in constrained reconfigurable broadcast networks*, in "TACAS 2018 - International Conference on Tools and Algorithms for the Construction and Analysis of Systems", Thessaloniki, Greece, Lecture Notes in Computer Science, Springer, April 2018, vol. 10806, pp. 38-54 [*DOI :* 10.1007/978-3-319-89963-3_3], https://hal.archives-ouvertes.fr/hal-01889046

[16] H. BAZILLE, E. FABRE, B. GENEST. *Complexity reduction techniques for quantified diagnosability of stochastic systems*, in "WODES'18 - 14th IFAC Workshop on Discrete Event Systems", Castellamare di Stabi, Italy, Proceedings of WODES 2018, IFAC, May 2018, pp. 82-87 [*DOI :* 10.1016/J.IFACOL.2018.06.283], https://hal.archives-ouvertes.fr/hal-01943401

[17] H. BAZILLE, E. FABRE, B. GENEST. *Symbolically Quantifying Response Time in Stochastic Models using Moments and Semirings*, in "FOSSACS 2018 - 21st International Conference on Foundations of Software Science and Computation Structures", Thessaloniki, Greece, LNCS, Springer, April 2018, vol. 10803, pp. 403-419 [*DOI :* 10.1007/978-3-319-89366-2_22], https://hal.archives-ouvertes.fr/hal-01943440

[18] N. BERTHIER, H. MARCHAND, É. RUTTEN. *Symbolic Limited Lookahead Control for Best-effort Dynamic Computing Resource Management*, in "WODES 2018 - 14th Workshop on Discrete Event Systems", Sorrento Coast, Italy, Elsevier, May 2018, pp. 1-8 [*DOI :* 10.1016/J.IFACOL.2018.06.288], https://hal.inria.fr/hal-01807284

[19] P. BOUYER, M. GONZALEZ, N. MARKEY, M. RANDOUR. *Multi-weighted Markov Decision Processes with Reachability Objectives*, in "Gandalf 2018 - Ninth International Symposium on Games, Automata, Logics, and Formal Verification", Sarrebruck, Germany, EPTCS, September 2018, vol. 277, pp. 250 - 264 [*DOI :* 10.4204/EPTCS.277.18], https://hal.archives-ouvertes.fr/hal-01889020

[20] P. BOUYER, S. JAZIRI, N. MARKEY. *Efficient timed diagnosis using automata with timed domains*, in "RV 2018 - 18th International Conference on Runtime Verification", Limassol, Cyprus, LNCS, November 2018, vol. 11237, pp. 1-26, https://hal.archives-ouvertes.fr/hal-01889030

[21] B. BÉRARD, S. HAAR, L. HÉLOUËT. *Hyper Partial Order Logic*, in "FSTTCS 2018 - Foundations of Software Technology and Theoretical Computer Science", Ahmedabad, India, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, December 2018, vol. 122, pp. 1-29 [*DOI :* 10.4230/LIPICS.FSTTCS.2018.20], https://hal.inria.fr/hal-01884390

[22] S. CHERRARED, S. IMADALI, E. FABRE, G. GÖSSLER. *LUMEN: A Global Fault Management Framework For Network Virtualization Environments*, in "ICIN 2018 - 21st Conference on Innovation in Clouds, Internet and Networks and Workshops", Paris, France, IEEE, February 2018, pp. 1-8 [*DOI :* 10.1109/ICIN.2018.8401622], https://hal.inria.fr/hal-01851610

[23] E. FABRE, G. M. PINNA. *Toward a Uniform Approach to the Unfolding of Nets*, in "DisCoTec 2018 - 13th International Federated Conference on Distributed Computing Techniques", Madrid, Spain, June 2018, vol. 279, pp. 21-36, https://arxiv.org/abs/1810.08038 , https://hal.inria.fr/hal-01943666

[24] P. GARDY, P. BOUYER, N. MARKEY. *Dependences in Strategy Logic*, in "STACS 2018", Caen, France, LIPICS, February 2018, vol. 34, pp. 35 - 36 [*DOI :* 10.4230/LIPICS.STACS.2018.34], https://hal.archives-ouvertes.fr/hal-01889224

[25] L. HENRY, T. JÉRON, N. MARKEY. *Control strategies for off-line testing of timed systems*, in "SPIN 2018 - International Symposium on Model Checking Software", Malaga, Spain, LNCS, June 2018, vol. 10869, pp. 171-189 [*DOI :* 10.1007/978-3-319-94111-0_10], https://hal.archives-ouvertes.fr/hal-01889225

[26] L. HÉLOUËT, H. MARCHAND, J. MULLINS. *Concurrent secrets with quantified suspicion*, in "ACSD' 2018 - 18th International Conference on Application of Concurrency to System Design", Bratislava, Slovakia, June 2018, pp. 1-15, https://hal.inria.fr/hal-01757949

[27] L. HÉLOUËT, H. MARCHAND, L. S. L. RICKER. *Opacity with powerful attackers*, in "WODES 2018 - 14th IFAC Workshop on Discrete Event Systems", Sorrento, Italy, Elsevier, May 2018, pp. 464 - 471 [*DOI :* 10.1016/J.IFACOL.2018.06.341], https://hal.inria.fr/hal-01886156

[28] E. LEFAUCHEUX, A. GIUA, C. SEATZU. *Basis Coverability Graph for Partially Observable Petri Nets with Application to Diagnosability Analysis*, in "Petri Nets 2018 - International Conference on Applications and Theory of Petri Nets and Concurrency", Bratislava, Slovakia, Lecture Notes in Computer Science, Springer, June 2018, vol. 10877, pp. 164-183 [*DOI :* 10.1007/978-3-319-91268-4_9], https://hal.inria.fr/hal-01882129

Scientific Books (or Scientific Book chapters)

[29] P. BOUYER, U. FAHRENBERG, K. G. LARSEN, N. MARKEY, J. OUAKNINE, J. WORRELL. *Model Checking Real-Time Systems*, in "Handbook of model checking", Springer-Verlag, April 2018, pp. 1001-1046 [*DOI :* 10.1007/978-3-319-10575-8_29], https://hal.archives-ouvertes.fr/hal-01889280

Books or Proceedings Editing

[30] N. GMATI, E. BADOUEL, B. WATSON (editors). *Proceedings of CARI 2018 (African Conference on Research in Computer Science and Applied Mathematics)*, September 2018, https://hal.inria.fr/hal-01881376

Other Publications

[31] N. BERTRAND, I. KONNOV, M. LAZIC, J. WIDDER. *Verification of Randomized Distributed Algorithms under Round-Rigid Adversaries*, November 2018, Experiments presented in this paper were carried out using the Grid5000 testbed, supported by a scientific interest group hosted by Inria and including CNRS, RENATER and several Universities as well as other organizations, see grid5000.fr, https://hal.inria.fr/hal-01925533

[32] L. HÉLOUËT, H. MARCHAND, L. RICKER. *Opacity with powerful attackers*, March 2018, working paper or preprint, https://hal.inria.fr/hal-01738169

[33] L. HÉLOUËT, R. SINGH, Z. MIKLÓS. *Data Centric Workflows for Complex Crowdsourcing Applications*, January 2019, working paper or preprint, https://hal.inria.fr/hal-01976280