RESEARCH CENTRE

Rennes - Bretagne Atlantique

IN PARTNERSHIP WITH:

Université Rennes 1, CNRS

2021 ACTIVITY REPORT

Project-Team SUMO

SUpervision of large MOdular and distributed systems

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Proofs and Verification

Contents

Project-Team SUMO

Creation of the Project-Team: 2015 January 01

Keywords

Computer sciences and digital sciences

A1.2.2. – Supervision

A1.3. – Distributed Systems

A1.5. – Complex systems

A2.3. – Embedded and cyber-physical systems

A2.4. – Formal method for verification, reliability, certification

A2.4.2. – Model-checking

A4.5. – Formal methods for security

A6.4.3. – Observability and Controlability

A6.4.6. – Optimal control

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

B5.2.2. – Railway

B6.2. – Network technologies

B6.3.3. – Network Management

B7.1. – Traffic management

B8.5.2. – Crowd sourcing

1 Team members, visitors, external collaborators

Research Scientists

- Nathalie Bertrand [Team leader, Inria, Senior Researcher, HDR]
- Éric Badouel [Inria, Researcher, HDR]
- Éric Fabre [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]

Post-Doctoral Fellow

- Aline Goeminne [CNRS, from Oct 2021]

PhD Students

- Emily Clement [Mitsubishi Electric, CIFRE]
- Léo Henry [Univ de Rennes I, until Nov 2021]
- Anirban Majumdar [CNRS, until Sep 2021]
- Abdul Majith Noordheen [Inria]
- Suman Sadhukhan [Inria, until Nov 2021]
- Bastien Thomas [Univ de Rennes I]
- Nicolas Waldburger [Univ de Rennes I, from Oct 2021]

Technical Staff

- Antoine Thebault [Inria, Engineer]

Interns and Apprentices

- Hugo Francon [CNRS, from May 2021 until Jul 2021]
- Lucie Guillou [Inria, from May 2021 until Jul 2021]
- Alban Gutierrez-Andre [CNRS, from May 2021 until Aug 2021]
- Mathieu Poirier [Inria, from Feb 2021 until Jul 2021]

Administrative Assistant

- Laurence Dinh [Inria]

External Collaborator

- Reiya Noguchi [Mitsubishi Electric, until May 2021]

2 Overall objectives

2.1 Context

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.

2.2 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.

2.3 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.

2.4 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 Introduction

Since its creation in 2015, SUMO has successfully developed formal methods for large quantitative systems, in particular addressing verification, synthesis and control problems. Our current motivation is to expand this by putting emphasis on new concerns, such as algorithm efficiency, imprecision handling, and the more challenging objective of addressing incomplete or missing models. In the following we list a selection of detailed research goals, structured into four axes according to model classes: quantitative models, large systems, population models, and data-driven models. Some correspond to the pursuit of previously obtained results, others are more prospective.

3.2 Axis 1: Quantitative models

The analysis and control of quantitative models will remain at the heart of a large part of our research activities. In particular, we have two starting collaborative projects focusing on **timed models**, namely our ANR project TickTac and our collaboration with MERCE. The main expected outcome of TickTac is an open-source tool implementing the latest algorithms and allowing for quick prototyping of new algorithms. Several other topics will be explored in these collaborations, including robustness issues, game-theoretic problems, as well as the development of efficient algorithms, *e.g.* based on CEGAR approach or specifically designed for subclasses of automata (*e.g.* automata with few clocks and/or having a specific structure, as in [38]). Inspired by our collaboration with Alstom, we also aim at developing symbolic techniques for analysing non-linear timed models.

Stochastic models are another important focus for our research. On the one hand, we want to pursue our work on the optimization of non-standard properties for Markov decision processes, beyond the traditional verification questions, and explore *e.g.* long-run probabilities, and quantiles. Also, we aim at lifting our work on decisiveness from purely stochastic [36, 37] to non-deterministic and stochastic models in order to provide approximation schemes for the probability of (repeated) reachability properties in infinite-state Markov decision processes. On the other hand, in order to effectively handle large stochastic systems, we will pursue our work on approximation techniques. We aim at deriving simpler models, enjoying or preserving specific properties, and at determining the appropriate level of abstraction for a given system. One needs of course to quantify the approximation degrees (distances), and to preserve essential features of the original systems (explainability). This is a connection point between formal methods and the booming learning methods.

Regarding **diagnosis/opacity** issues, we will explore further the quantitative aspects. For diagnosis, the theory needs extensions to the case of incomplete or erroneous models, and to reconfigurable systems, in order to develop its applicability (see Sec. 3.6). There is also a need for non-binary causality

analysis (*e.g.* performance degradations in complex systems). For opacity, we aim at quantifying the effort attackers must produce *vs* how much of a secret they can guess. We also plan to synthesize robust controllers resisting to sensor failures/attacks.

3.3 Axis 2: Large systems

Part of the background of SUMO is on the analysis and management of concurrent and modular/distributed systems, which we view as two main approaches to address state explosion problems. We will pursue the study of these models (including their quantitative features): verification of timed concurrent systems, robust distributed control of modular systems, resilient control to coalitions of attackers, distributed diagnosis, modular opacity analysis, distributed optimal planning, etc. Nevertheless, we have identified two new lines of effort, inspired by our application domains.

Reconfigurable systems. This is mostly motivated by applications at the convergence of virtualization techs with networking (Orange and Nokia PhDs). Software defined networks, either in the core (SDN/NFV) or at the edge (IoT) involve distributed systems that change structure constantly, to adapt to traffic, failures, maintenance, upgrades, etc. Traditional verification, control, diagnosis approaches (to mention only those) assume static and known models that can be handled as a whole. This is clearly insufficient here: one needs to adapt existing results to models that (sometimes automatically) change structure, incorporate new components/users or lose some, etc. At the same time, the programming paradigms for such systems (chaos monkey) incorporate resilience mechanisms, that should be considered by our models.

Hierarchical systems. Our experience with the regulation of subway lines (Alstom) revealed that large scale complex systems are usually described at a single level of granularity. Determining the appropriate granularity is a problem in itself. The control of such systems, with humans in the loop, can not be expressed at this single level, as tasks become too complex and require extremely skilled staff. It is rather desirable to describe models simultaneously at different levels of granularity, and to perform control at the appropriate level: humans in charge of managing the system by high level objectives, and computers in charge of implementing the appropriate micro-control sequences to achieve these tasks.

3.4 Axis 3: Population models

We want to step up our effort in parameterized verification of systems consisting of many identical components, so-called population models. In a nutshell our objectives summarize as "from Boolean to quantitative".

Inspired by our experience on the analysis of populations of yeasts, we aim at developping the quantitative analysis and control of population models, *e.g.* using Markov decision processes together with quantitative properties, and focusing on generating strategies with fast convergence.

As for broadcast networks, the challenge is to model the mobility of nodes (representing mobile ad hoc networks) in a faithful way. The obtained model should reflect on the one hand, the placement of nodes at a given time instant, and on the other hand, the physical movement of nodes over time. In this context, we will also use game theory techniques which allows one to study cooperative and conflictual behaviors of the nodes in the network, and to synthesize correct-by-design systems in adversarial environments.

As a new application area, we target randomized distributed algorithms. Our goal is to provide probabilistic variants of threshold automata [39] to represent fault-tolerant randomized distributed algorithms, designed for instance to solve the consensus problem. Most importantly, we then aim at developing new parameterized verification techniques, that will enable the automated verification of the correctness of such algorithms, as well as the assessment of their performances (in particular the expected time to termination).

In this axis, we will investigate whether fluid model checking and mean-field approximation techniques apply to our problems. More generally, we aim at a fruitful cross-fertilizing of these approaches with parameterized model-checking algorithms.

3.5 Axis 4: Data-driven models

In this axis, we will consider data-centric models, and in particular their application to crowd-sourcing. Many data-centric models such as Business Artifacts [40] orchestrate simple calls and answers to tasks performed by a single user. In a crowd-sourcing context, tasks are realized by pools of users, which may result in imprecise, uncertain and (partially) incompatible information. We thus need mechanisms to reconcile and fuse the various contributions in order to produce reliable information. Another aspect to consider concerns answers of higher-order: how to allow users to return intentional answers, under the form of a sub-workflow (coordinated set of tasks) which execution will provide the intended value. In the framework of the ANR Headwork we will build on formalisms such as GAG (guarded attribute grammars) or variants of business artifacts to propose formalisms adapted to crowd-sourcing applications, and tools to analyze them. To address imprecision, we will study techniques to handle fuzziness in user answers, will explore means to set incentives (rewards) dynamically, and to set competence requirements to guide the execution of a complex workflow, in order to achieve an objective with a desired level of quality.

In collaboration with Open Agora, CESPA and University of Yaoundé (Cameroun) we intend to implement in the GAG formalism some elements of argumentation theory (argumentation schemes, speech acts and dialogic games) in order to build a tool for the conduct of a critical discussion and the collaborative construction of expertise. The tool would incorporate point of view extraction (using clustering mechanisms), amendment management and consensus building mechanisms.

3.6 Transversal concern: missing models

We are concerned with one important lesson derived from our involvement in several application domains. Most of our background gets in force as soon as a perfect model of the system under study is available. Then verification, control, diagnosis, test, etc. can mobilize a solid background, or suggest new algorithmic problems to address. In numerous situations, however, assuming that a model is available is simply unrealistic. This is a major bottleneck for the impact of our research. We therefore intend to address this difficulty, in particular for the following domains.

- Model building for diagnosis. As a matter of fact, diagnosis theory hardly touches the ground to the extent that complete models of normal behavior are rarely available, and the identification of the appropriate abstraction level is unclear. Knowledge of faults and their effects is even less accessible. Also, the actual implemented systems may differ significantly from behaviors described in the norms. One therefore needs a theory for incomplete and erroneous models. Besides, one is often less bothered by partial observations than drowned by avalanches of alerts when malfunctions occur. Learning may come to the rescue, all the more that software systems may be deployed in sandpits and damaged for experimentation, thus allowing the collection of masses of labeled data. Competition on that theme clearly comes from Machine Learning techniques.

- Verification of large scale software. For some verification problems like the one we address in the IPL HAC-Specis, one does not have access to a formal model of the distributed program under study, but only to executions in a simulator. Formal verification poses new problems due to the difficulties to capture global states, to master state space explosion by gathering and exploiting concurrency information.

- Learning of stochastic models. Applications in bioinformatics often lead to large scale models, involving numerous chains of interactions between chemical species and/or cells. Fine grain models can be very precise, but very inefficient for inference or verification. Defining the appropriate levels of description/abstraction, given the available data and the verification goals, remains an open problem. This cannot be considered as a simple data fitting problem, as elements of biological knowledge must be combined with the data in order to preserve explainability of the phenomena.

- Testing and learning timed models: during conformance testing of a black-box implementation against its formal specification, one wants to detect non-conformances but may also want to learn the implementation model. Even though mixing testing and learning is not new, this is more recent and challenging for continuous-time models.

- Process mining. We intend to extend our work on process discovery using Petri net synthesis [35] by using negative information (*e.g.* execution traces identified as outliers) and quantitative information (probabilistic or fuzzy sets of execution traces) in order to infer more robust and precise models.

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 abstraction schemes allowing formal reasonning on these systems.

5 Highlights of the year

Rituraj Singh has received the BDA 2021 PhD Thesis Award.

6 New software and platforms

Participants: Loïc Hélouët, Antoine Thebault.

6.1 New software

6.1.1 MOCHY

Name: MOdels for Concurrent and HYbrid systems

Keywords: Public transport, Hybrid models, Simulation, Performance analysis

Functional Description: Allows for the modeling of hybrid systems, schedule and regulation algorithms to optimize Key Performance Indicators. Mochy addresses mainly models of transport networks, their timetables and traffic management techniques. The tool allows for the fast simulation of these regulated models, to measure performance indicators. Since version 2.0, MOCHY proposes a novel traffic management algorithm with neural networks.

Release Contributions: Co-simulation of time Petri nets and timetables (model for regulated urban train systems with a hold-on policy). Performance analysis for simple Key Performance Indicators. Traffic management with neural networks.

News of the Year: In 2021, we have released two successive versions of MOCHy, and registered it at the APP.

URL: https://adt-mochy.gitlabpages.inria.fr/mochy/

Authors: Loic Helouet, Antoine Thebault, Didier Vojtisek

Contact: Loic Helouet

7 New results

7.1 New results on Axis 1: Quantitative models

7.1.1 Verification of probabilistic systems

Participants: Nathalie Bertrand, Ocan Sankur.

Quantified Linear Temporal Logic over Probabilistic Systems with an Application to Vacuity Checking
In [24], we investigate Quantified linear temporal logic (QLTL), which is an ω-regular extension of LTL allowing quantification over propositional variables. We study the model checking problem of QLTL-formulas over Markov chains and Markov decision processes (MDPs) with respect to the number of quantifier alternations of formulas in prenex normal form. For formulas with k-1 quantifier alternations, we prove that all qualitative and quantitative model checking problems are k- EXPSPACE-complete over Markov chains and k+1-EXPTIME-complete over MDPs. As an application of these results, we generalize vacuity checking for LTL specifications from the non-probabilistic to the probabilistic setting. We show how to check whether an LTL-formula is affected by a subformula, and also study inherent vacuity for probabilistic systems.

7.1.2 Verification of Real-Time Models

Participants: Blaise Genest, Loïc Hélouët, Thierry Jéron, Nicolas Markey.

In [11] , we consider the problems of efficiently diagnosing (and predicting) what did (and will) happen after a given sequence of observations of the execution of a partially observable one-clock timed automaton. This is made difficult by the facts that timed automata are infinite-state systems, and that they can in general not be determinized. We introduce timed markings as a formalism to keep track of the evolution of the set of reachable configurations over time. We show how timed markings can be used to efficiently represent the closure under silent transitions of such automata. We report on our implementation of this approach compared to the approach of Tripakis (Fault diagnosis for timed automata, in: Damm, Olderog (eds) Formal techniques in real-time and fault-tolerant systems, Springer, Berlin, 2002) and provide some insight to a generalization of our approach to n-clock timed automata.

In [8], 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.

In [13], we study games with reachability objectives under energy constraints. We first prove that under strict energy constraints (either only lower-bound constraint or interval constraint), those games are LOGSPACE-equivalent to energy games with the same energy constraints but without reachability objective (i.e., for infinite runs). We then consider two relaxations of the upper-bound constraints (while keeping the lower-bound constraint strict): in the first one, called weak upper bound, the upper bound is absorbing, i.e., when the upper bound is reached, the extra energy is not stored; in the second one, we allow for temporary violations of the upper bound, imposing limits on the number or on the amount of violations.

7.1.3 Resilience of Timed Systems

Participants: Blaise Genest, Loïc Hélouët.

[17] addresses reliability of timed systems in the setting of resilience, that considers the behaviors of a system when unspecified timing errors such as missed deadlines occur. Given a fault model that allows transitions to fire later than allowed by their guard, a system is universally resilient (or self-resilient) if after a fault, it always returns to a timed behavior of the non-faulty system. It is existentially resilient if after a fault, there exists a way to return to a timed behavior of the non-faulty system, that is, if there exists a controller which can guide the system back to a normal behavior. We show that universal resilience of

timed automata is undecidable, while existential resilience is decidable, in EXPSPACE. To obtain better complexity bounds and decidability of universal resilience, we consider untimed resilience, as well as subclasses of timed automata.

7.2 New results on Axis 2: Large Systems Models

7.2.1 Planning Problems

Participants: Ocan Sankur.

The Connected Multi-Agent Path Finding (CMAPF) problem asks for a plan to move a group of agents in a graph while respecting a connectivity constraint. In [25], we study a generalization of CMAPF in which the graph is not entirely known in advance, but is discovered by the agents during their mission. We present a framework introducing this notion and study the problem of searching for a strategy to reach a configuration in this setting. We prove the problem to be PSPACE-complete when requiring all agents to be connected at all times, and NEXPTIME-complete in the decentralized case, regardless of whether we consider a bound on the length of the execution.

7.2.2 Synthesis of Supervisors Robust Against Sensor Deception Attacks

Participants: Hervé Marchand.

In [14], we consider feedback control systems where sensor readings may be compromised by a malicious attacker intending on causing damage to the system. We study this problem at the supervisory layer of the control system, using discrete event systems techniques. We assume that the attacker can edit the outputs from the sensors of the system before they reach the supervisory controller. In this context, we formulate the problem of synthesizing a supervisor that is robust against the class of edit attacks on the sensor readings and present a solution methodology for this problem. This methodology blends techniques from games on automata with imperfect information with results from supervisory control theory of partially-observed discrete event systems. Necessary and sufficient conditions are provided for the investigated problem.

7.2.3 Compositional model checking of an SDN platform

Participants: Abdul Majith, Hervé Marchand, Ocan Sankur.

Software-Defined Network (SDN) technology provides the possibility to turn the network infrastructure into a dynamic programmable fabric capable of meeting the application needs in real-time. Thanks to the independence of the control plane from the data plane, the control entity, generally called as controller, has also the flexibility to implement proprietary complex algorithms. Within such a dynamic and complex environment, [23] (long version [33]) advocates for applying formal verification methods and more precisely composition model checking to ensure the correct behavior of the overall SDN system at design phase. To illustrate this purpose, it proposes to build different comprehensive formal models of a typical SDN platform selected here as a study object. Thorough performance results related to each model are provided and discussed. Thanks to such formal verifications, it is possible to pinpoint issues such as the one regarding network isolation within a complex SDN architecture. Although dealing with formal methods, this document attempts to strike a balance between theory, experimental work and network architecture discussion.

7.2.4 A Simulation-Optimization Framework for Traffic Disturbance Recovery in Metro Systems.

Participants: Loïc Hélouët.

In [16], we analyse how train delays propagate in a metro network due to disturbances and disruptions when different recovery strategies are implemented. Metro regulators use traffic management policies to recover from delays as fast as possible, return to a predefined schedule, or achieve an expected regularity of train arrivals and departures. We use as a metro traffic simulator SIMSTORS, which is based on a Stochastic Petri Net variant and simulates a physical system controlled by traffic management algorithms. To model existing metro networks, SIMSTORS has been mainly used with rule-based traffic management algorithms. In this work, we enhance traffic management strategies. We integrate SIMSTORS and the AGLIBRARY optimization solver in a closed-loop framework. AGLIBRARY is a deterministic solver for managing complex scheduling and routing problems. We formulate the real-time train rescheduling problem by means of alternative graphs, and use the decision procedures of AGLIBRARY to obtain rescheduling solutions. Several operational issues have been investigated throughout the use of the proposed simulation-optimization framework, among which how to design suitable periodic or event-based rescheduling strategies, how to setup the traffic prediction horizon, how to decide the frequency and the length of the optimization process. The Santiago Metro Line 1, in Chile, is used as a practical case study. Experiments with this framework in various settings show that integrating the optimization algorithms provided by AGLIBRARY to the rule-based traffic management embedded in SIMSTORS optimizes performance of the network, both in terms of train delay minimization and of service regularity.

7.3 New results on Axis 3: Population Models

Participants: Nathalie Bertrand, Anirban Majumdar, Bastien Thomas.

7.3.1 Broadcast networks

Broadcast networks allow one to model networks of identical nodes communicating through message broadcasts. Their parameterized verification aims at proving a property holds for any number of nodes, under any communication topology, and on all possible executions. In [9], we focus on the coverability problem which dually asks whether there exists an execution that visits a configuration exhibiting some given state of the broadcast protocol. Coverability is known to be undecidable for static networks, i.e. when the number of nodes and communication topology is fixed along executions. In contrast, it is decidable in PTIME when the communication topology may change arbitrarily along executions, that is for reconfigurable networks. Surprisingly, no lower nor upper bounds on the minimal number of nodes, or the minimal length of covering execution in reconfigurable networks, appear in the literature. In this paper we show tight bounds for cutoff and length, which happen to be linear and quadratic, respectively, in the number of states of the protocol. We also introduce an intermediary model with static communication topology and non-deterministic message losses upon sending. We show that the same tight bounds apply to lossy networks, although, reconfigurable executions may be linearly more succinct than lossy executions. Finally, we show NP-completeness for the natural optimisation problem associated with the cutoff.

7.3.2 Verification of Fault-tolerant Distributed Algorithms

Distributed algorithms typically run over arbitrary many processes and may involve unboundedly many rounds, making the automated verification of their correctness challenging. In the following papers, we addressed the verification of (randomized) fault-tolerant distributed algorithms.

Building on domain theory, in [20] we introduce a framework that abstracts infinite-state distributed systems that represent distributed algorithms into finite-state guard automata. The soundness of the

approach corresponds to the Scott-continuity of the abstraction, which relies on the assumption that the distributed algorithms are layered. Guard automata thus enable the verification of safety and liveness properties of fault-tolerant distributed algorithms.

Randomized fault-tolerant distributed algorithms pose a number of challenges for automated verification: (i) parameterization in the number of processes and faults, (ii) randomized choices and probabilistic properties, and (iii) an unbounded number of asynchronous rounds. This combination makes verification hard. Challenge (i) was recently addressed in the framework of threshold automata.

In [10], we extend threshold automata to model randomized consensus algorithms that perform an unbounded number of asynchronous rounds. For non-probabilistic properties, we show that it is necessary and sufficient to verify these properties under round-rigid schedules, that is, schedules where processes enter round r only after all processes finished round r - 1. For almostsure termination, we analyze these algorithms under round-rigid adversaries, that is, fair adversaries that only generate round-rigid schedules. This allows us to do compositional and inductive reasoning that reduces verification of the asynchronous multi-round algorithms to model checking of a one-round threshold automaton. We apply this framework and automatically verify the following classic algorithms: Ben-Or's and Bracha's seminal consensus algorithms for crashes and Byzantine.

Weak adversaries are a way to model the uncertainty due to asynchrony in randomized distributed algorithms. They are a standard notion in correctness proofs for distributed algorithms, and express the property that the adversary (scheduler), which has to decide which messages to deliver to which process, has no means of inferring the outcome of random choices, and the content of the messages. In [19], we introduce a model for randomized distributed algorithms that allows us to formalize the notion of weak adversaries. It applies to randomized distributed algorithms that proceed in rounds and are tolerant to process failures. For this wide class of algorithms, we prove that for verification purposes, the class of weak adversaries can be restricted to simple ones, so-called round-rigid adversaries, that keep the processes tightly synchronized. As recently a verification method for round-rigid adversaries has been introduced, our new reduction theorem paves the way to the parameterized verification of randomized distributed algorithms under the more realistic weak adversaries.

7.4 New results on Axis 4: Data-driven Models

7.4.1 Lazy Services: A Service Oriented Architecture based on Incremental Computations and Commitments

Participants: Éric Badouel.

In [34] we develop a notion of data-driven lazy services by building up from the model of guarded attributed grammars that we previously introduced in the context of distributed collaborative systems. We abstract from this model and limit somewhat its expressiveness so that it can comply more broadly to SOA principles. We introduce an improvement on subscription management to optimize the distributed implementation of lazy services. A service oriented architecture (SOA) aims to structure complex distributed systems in terms of re-usable components, called services. To guarantee a good service interoperability these services must be weakly coupled and their description must be separated from their implementations. The interface of a service provides information on how it can be invoked: the logical location where it can be invoked, the supported communication protocol and the types of its input (parameters) and output (result). Traditionally, a service can only be invoked when its parameters are fully defined and, symmetrically, these services only return their results after they have been totally processed. In this work, we promote a more liberal view of services by allowing them to consume their data lazily (i.e., as they need it) and produce their results incrementally (i.e., as they are produced).

7.4.2 Crowdsourcing

Participants: Loïc Hélouët, Rituraj Singh.

Reducing the Cost of Aggregation in Crowdsourcing. Crowdsourcing is a way to solve problems that need human contribution. Crowdsourcing platforms distribute replicated tasks to workers, pay them for their contribution, and aggregate answers to produce a reliable conclusion. A fundamental problem is to infer a consensual answer from the set of returned results. Another problem is to obtain this answer at a reasonable cost: unlimited budget allows hiring experts or large pools of workers for each task but a limited budget forces to use resources at best. Last, crowdsourcing platforms have to detect and ban malevolent users (also known as "spammers") to achieve good accuracy of their answers. This paper considers crowdsourcing of simple Boolean tasks. We first define a probabilistic inference technique, that considers difficulty of tasks and expertise of workers when aggregating answers. We then propose CrowdInc, a greedy algorithm that reduces the cost needed to reach a consensual answer. CrowdInc distributes resources dynamically to tasks according to their difficulty. The algorithm solves batches of simple tasks in rounds that estimate workers expertize, tasks difficulty, and synthesizes a plausible aggregated conclusion and a confidence score using Expectation Maximization. The synthesized values are used to decide whether more workers should be hired to increase confidence in synthesized answers. We show on several benchmarks that CrowdInc achieves good accuracy, reduces costs and we compare its performance to existing solutions. We then use the estimation of CrowdInc to detect spammers and study the impact of spammers on costs and accuracy.

Cost and Quality Assurance in Crowdsourcing Workflows.

Crowdsourcing platforms provide tools to replicate and distribute micro tasks (simple, independent work units) to crowds and assemble results. However, real-life problems are often complex: they require to collect, organize or transform data, with quality and costs constraints. work considers dynamic realization policies for complex crowdsourcing tasks. Workflows provide ways to organize a complex task in phases and guide its realization. The challenge in [22, 21] is then to deploy a workflow on a crowd, i.e., allocate workers to phases so that the overall workflow terminates, with good accuracy of results and at a reasonable cost. Standard "static" allocation of work in crowdsourcing affects a fixed number of workers per micro-task to realize and aggregates the results. In [15], we define new dynamic worker allocation techniques that consider progress in a workflow, quality of synthesized data, and remaining budget. Evaluation on a benchmark shows that dynamic approaches outperform static ones in terms of cost and accuracy.

7.5 New results on Transversal Concern: Missing Models

7.5.1 Self-modeling

Participants: Éric Fabre.

[12] considers the fault diagnosis problem in large scale telecommunication networks. The focus is on software defined networks (SDN) deployed over a cloud infrastructure, for example through containers via Kubernetes. Numerous approaches to root-cause analysis for such systems rely on learning techniques, which hardly resist to the changing structure of these networks and fails at providing explanations. To circumvent these limitations, we aim at model-based methods, capable of explaining fault propagations from root causes down to symptom patterns. This raises several difficulties: how to automatically build a model of such a system, how to track its evolution, what is the appropriate modeling granularity, how to validate the model (soundness and completeness), and finally how to use it for diagnosis purposes. This paper develops a “self-modeling" methodology for these large systems, capturing resources dependencies from physical/virtual equipment up to software components and high-level functions and procedures like the opening of a call session. This model is translated into a Bayesian network, used as the support for diagnosis algorithms. The approach is illustrated on a real case: vIMS, a virtualized version of the IP Multimedia Subsystem.

8 Bilateral contracts and grants with industry

8.1 Bilateral contracts with industry

Nokia Bell Labs - ADR SAPIENS.

Participants: Éric Fabre, Hervé Marchand, Abdul Majith, Ocan Sankur.

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 study control and diagnosis issues for such systems. A PhD student is involved in the project: Abdul Majith (started in January 2019) on Controller Synthesis of Adaptive Systems, supervised by Hervé Marchand, Ocan Sankur and Dinh Thai Bui (Nokia Bell Labs).

Mitsubishi Electric Research Center Europe (MERCE).

Participants: Emily Clement, Thierry Jéron, Nicolas Markey, Ocan Sankur.

Several researchers of SUMO are involved in a collaboration on the verification of real-time systems with the "Information and Network Systems" Team (INSv) led by David Mentré of the "Communication & Information Systems (CIS)" Division of MERCE Rennes). The members of the team at MERCE work on different aspects of formal verification. Currently the SUMO team and MERCE jointly supervise a Cifre PhD student (Emily Clement) funded by MERCE since fall 2018; the thesis is about robustness of reachability in timed automata and will be defended in the beginning of 2022. Moreover we collaborate with Reiya Noguchi, a young engineer, who was member of MERCE, on leave of a Japanese operational division of Mitsubishi and hosted by the SUMO team one day per week since the beginning of 2019; Reiya returned in Japan this year but we continue the collaboration with him. We work with him and Merce on the consistency of timed requirements.

Orange Labs.

Participants: Éric Fabre.

SUMO takes part in I/O Lab, 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.

IPSCO (Intelligent Support Processes and Communities)

Participants: Éric Badouel.

- Duration: 2021 -> 2023
- Partners: Academy: University of Rennes I/IRISA with Diverse team (Coordinator) and SUMO team; Industry: Jamespot and Logpickr

The IPSCO project aims to develop a new customer support platform for digital companies and public services. Both by setting up intelligent mechanisms for filtering and processing requests from the public (customers and partners) and by providing a reflective vision of the processes implemented in the responses to these requests. In addition, to provide a robust response to small teams, the solution will enable the effective management of expert user communities to foster their autonomy and the emergence of best practices.

9 Partnerships and cooperations

9.1 International initiatives

9.1.1 Associate Teams in the framework of an Inria International Lab or in the framework of an Inria International Program

FUCHSIA

Participants: Éric Badouel.

Title: Flexible user-centric higher-order systems for collective intelligence in agencies

Duration: 2019 -> 2023

Coordinator: Georges-Edouard Kouamou

Partners:

- Université de Yaoundé

Inria contact: Eric Badouel

Summary: Fuchsia is an associate team (2019-2022) between Inria Sumo team in Rennes, ENSP (Ecole Nationale Supérieure Polytechnique) in Yaoundé and Epicentre/Médecins sans frontiers hosted by the IIL LIRIMA. The scientific objective of the team is to deploy flexible, adaptive and user-centric workflow systems on the Internet to enable groups to make smart decisions and coordinate their actions. The proposed solutions, based on the model of Guarded Attribute Grammars, should provide support for information gathering, deliberation and decision-making. Various applications are considered: urban crowdsourcing, choreography of services, and crisis management systems in collaboration with Epicentre. Three PhD theses have been defended in the framework of this collaboration and two other theses are being completed and should be defended in 2022.

9.1.2 Inria associate team not involved in an IIL or an international program

QASL

Participants: Nathalie Bertrand, Nicolas Markey.

Duration: 2020 -> 2024

Coordinator: Nicolas Markey

Partners:

- University of Naples "Federico II"

Inria contact: Nicolas Markey

Summary: Model checking aims at verifying that the executions of a computer system (usually modelled as a labelled transition system) satisfy a given property. Those properties are most often expressed using temporal logics, which provide a powerful way of specifying constraints on the occurrence of events for an execution to be valid. When reasoning about systems made of several components, we usually do not want to consider all executions: instead, we want to only consider those executions that can be triggered by some of the components as a reaction to the behaviours of other components. In an analogy with game theory (where players are components, executions are plays and valid behaviours correspond to winning conditions), temporal logics have been extended to reason about strategies; Strategy Logic can for instance express rich properties including antagonism and cooperation between groups of players. Our objectives in this project is to augment Strategy Logic with quantitative aspects: in that setting, properties are not true or false, but they take vakues reflecting the quality or efficiency of strategies and their associated executions. Checking such quantitative properties usually has very high complexity, if doable at all. Our recent works led to positive results, which we will extend in this associate team.

9.2 National initiatives

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

  Participants: Emily Clement, Léo Henry, Thierry Jéron, Nicolas Markey, Ocan Sankur.

  - link to web site
  - Led by Ocan Sankur (SUMO);
  - Partners: LMF (Paris-Saclay), 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.

- **ANR HeadWork**: Human-Centric Data-oriented WORKflows (2016-2022)

  Participants: Éric Badouel, Loïc Hélouët, Rituraj Singh.

  - link to website
  - Led by David Gross-Amblard (Université Rennes 1);
  - Partners: IRISA team Druid (Rennes), Inria Project-Teams Valda (Paris), SUMO (Rennes) and 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.

- **ANR MAVeriQ**: Methods of Analysis for Verification of Quantitative properties (2021-2025)

Participants: Nathalie Bertrand, Éric Fabre, Blaise Genest, Loïc Hélouët, Nicolas Markey.

- link to website
- Led by Aldric Degorre (IRIF); Local coordinator Éric Fabre.
- Partners: IRIF, LMF, Inria Rennes/IRISA, LACL, Verimag.

The objective of this project is to develop unified frameworks for quantitative verification of timed, hybrid, and stochastic systems. We believe such a unification is possible because common patterns are used in many cases. The project targets in particular:

- systematization of quantitative properties and their use cases
- substantial progress in the algorithms of quantitative verification;
- practical methodology for stating and verifying quantitative properties of systems.

The aim of MAVeriQ is to progress towards this unification, by gathering skills on timed and stochastic systems and on quantitative verification under a common roof, to jointly address open challenges in quantitative model-checking and quantitative validation. One such challenge we will address is robustness of quantitative models, that is, resilience to small perturbations, which is crucial for implementability. Unified methods developed in the project (such as robustness analysis and simulation techniques) will be showcased in different case studies in the domain of CPS (in particular automotive control),showing that such a system can be verified in different ways without leaving this framework.

National informal collaborations
The team collaborates with the following researchers:

- Patricia Bouyer (LMF, ENS Paris-Saclay) on quantitative aspects of verification and game models for parameterized systems;
- Yliès Falcone (University Grenoble-Alpes) and Victor Roussanaly (Inria Rhône Alpes) on the distributed timed monitoring.

10 Dissemination

Participants: Éric Badouel, Nathalie Bertrand, Éric Fabre, Blaise Genest, Loïc Hélouët, Thierry Jéron, Hervé Marchand, Nicolas Markey, Ocan Sankur.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

- Nathalie Bertrand and Nicolas Markey are members of the steering committee of the school MOVEP;
- Blaise Genest is in the steering committee of FMAI, the International Workshop on Formal Methods in Artificial Intelligence.
- Hervé Marchand is a member of the IFAC Technical Committee (TC 1.3 on Discrete Event and Hybrid Systems) as well as the IEEE DES CDC committee. He is the president of the steering committee of MSR (modélisation de systèmes réactifs).

10.1.2 Scientific events: selection

Chair of conference program committees

- Éric Badouel was the Scientific Chair of CRI'2021 (Yaoundé).

Membership in conference program committees

- Éric Badouel was in the program committee of VECoS'21;
- Nathalie Bertrand was in the program committee of FoSSaCS'21, ICALP'21 and Gandalf'21;
- Blaise Genest was in the program committee of FMAI'21;
- Loïc Hélouët was in the program committee of Petri Nets'21 and ICWS'21.
- Thierry Jéron was in the program committee of ICTSS'21 and SAC-SVT'21;
- Hervé Marchand was in the program committee of MSR'21, ACCC'21 and CDC'21;
- Nicolas Markey was in the program committee of LATA'20-21 and RV'21;
- Ocan Sankur was in the program committee of FSTTCS'21 and AAAI'21.

Reviewing All members of the team regularly write reviews for the main conferences in our areas of expertise (LICS, ICALP, CAV, Concur, FTTCS, STACS, FoSSaCS, RV, WoDES, CDC, ...).

10.1.3 Journal

Membership in editorial boards

- Since July 2021, Nathalie Bertrand is an editorial board member for Journal of Logical and Algebraic Methods in Programming (JLAMP). Since November 2021 she is an editorial board member for Theoretical Computer Science (TCS);
- Hervé Marchand is associate editor of the journal Discrete Event Dynamical Systems - Theory and applications (JDEDS).

Reviewing activities

- Éric Badouel wrote reviews for Discrete Event and Dynamic Systems (DEDS) and Theoretical Computer Science (TCS) and for CRI, VECoS and ICATPN;
- Nathalie Bertrand wrote reviews for LMCS;
- Éric Fabre wrote reviews for JDEDS, Automatica, TAC, TNSM.
- Loïc Hélouët wrote reviews for Fundamenta Informaticae.
- Thierry Jéron wrote a review for STVR;
- Hervé Marchand wrote reviews for JDEDS, Automatica and IEEE Transactions on Automatic Control.
- Nicolas Markey wrote reviews for LMCS
- Ocan Sankur wrote reviews for Acta Informatica, IEEE Transactions on Automatic Control.

10.1.4 Invited talks

Nathalie Bertrand: OPODIS'21, December 2021. *Distributed algorithms: a challenging playground for model checking.*

10.1.5 Leadership within the scientific community

- Éric Badouel is the co-director (with Amel Ben Abda, Tunis) of LIRIMA, the Inria International Lab for Africa. He is the scientific officer for the African and Middle-East region at Inria DRI (International Partnership Department);
- Nathalie Bertrand is the co-head of the French working group on verification ("GT-Vérif" of GDR IM);
- Éric Fabre is the co-director of the joint research lab of Nokia Bell Labs and Inria;
- Blaise Genest is co-Director of program DesCartes, a CNRS@CREATE programme in Singapore comprising 80 professors/researchers (half from France and half from Singapore), 30 PhD students and 50 postdoctorates.

10.1.6 Scientific expertise

- Éric Fabre was in the selection committee for bilateral projects of the French-Germany research programme in AI.
- Éric Fabre is reviewer for the CIR program of the Ministry of Research (tax reductions for research activities in private companies).
- Loïc Hélouët is reviewer for ANR;
- Thierry Jéron reviewed a PRCI (international) project for ANR, the French research council;
- Thierry Jéron evaluated a CIFRE project for ANRT, the French reasearch and technology council;
- Nicolas Markey was an expert committee member for project evaluation for the Auvergne-Rhone-Alpes region and for the Poland National Science Center.

10.1.7 Research administration

- Éric Badouel is a member of the executive board of GIS SARIMA.
- Éric Fabre is a member of the Evaluation Committee of Inria.
- Thierry Jéron is a member of the Comité d'orientation scientifique (COS) of IRISA;
- Nicolas Markey is the head of the D4 department of IRISA ("Languages and Software Engineering").

10.2 Teaching - Supervision - Juries

10.2.1 Teaching

- Master: Nathalie Bertrand, Algorithms, and Symbolic AI, 18h, Agrégation, ENS Rennes, France;
- Master: Éric Fabre, Information Theory and Coding, 24h, ENS Rennes, France.
- Master: Loïc Hélouët, Verification and proofs, 14h, Agrégation, ENS Rennes, France;
- Master: Nicolas Markey, Algorithms, 18h, Agrégation, ENS Rennes, France;
- Master: Nicolas Markey, Computability and Complexity, 18h, Agrégation, ENS Rennes, France;
- Master: Ocan Sankur, Travaux pratiques, Analyse et Conception Formelle (ACF), 26h, M1, Univ Rennes 1, France;
- Master: Ocan Sankur, Travaux dirigés et pratiques, Modeling and verification of finite automata (MVFA), 20h, M1, ENS Rennes, France;
- Master: Ocan Sankur, Logic, 12h, Agrégation, ENS Rennes, France.

10.2.2 Supervision

Post-Doc

- Post-doc: Aline Goeminne (supervised by Nicolas Markey and Ocan Sankur), working on Timed Network Congestion Games (funded by ANR project TickTac)

PhD Students.

- PhD: Rituraj Singh, Data centric workflows for crowdsourcing applications [30], defended in May 2021, supervised by Loïc Hélouët and Zoltan Miklos (DRUIDE team, IRISA). Best PhD award at the BDA'21 conference.
- PhD: Anirban Majumdar, Verification and Synthesis of Parameterized Concurrent Systems [27]. Defended in Oct. 2021 at ENS Paris-Saclay, supervised by Nathalie Bertrand and Patricia Bouyer (LSV/LMF, ENS Paris-Saclay).
- PhD: Arthur Queffelec, Connected Multi-Agent Path Finding : How robots get away with texting and driving [28], defended in Nov. 2021, supervised by François Schwarzentruber and Ocan Sankur.
- PhD: Léo Henry, Optimal test-case generation with game theory [26], defended in Dec. 2021, supervised by Thierry Jéron and Nicolas Markey.
- PhD: Suman Sadhukhan, A verification viewpoint on network congestion games [29], defended in Dec. 2021, supervised by Nathalie Bertrand, Nicolas Markey and Ocan Sankur.

- PhD in progress: Emily Clement, Verification and synthesis of control systems: efficiency and robustnes, started in Dec. 2018, supervised by Thierry Jéron, Nicolas Markey and David Mentré (Mitsubishi Electric).
- PhD in progress: Abdul Majith, Control of Adaptive Systems, started in Jan. 2019, supervised by Hervé Marchand, Ocan Sankur and Dinh Thai-Bui (Nokia Bell Labs).
- PhD in progress: Bastien Thomas, Automated verification of randomized distributed algorithms, started in Oct. 2019, supervised by Nathalie Bertrand and Josef Widder (Informal Systems, Austria).
- PhD in progress: Nicolas Waldburger, Parameterized verification of distributed algorithms under fairness conditions, started in Oct. 2021, supervised by Nathalie Bertrand, Nicolas Markey and Ocan Sankur.

Master Students.
Past Master Students.

- Parany Agrawal, an M1 student at Chennai Mathematical Institute was supervised by Loïc Hélouët.
- Pierre Bourse, an M1 student at ENS Rennes, was supervised by Léo Henry, Thierry Jéron and Nicolas Markey 2h/week during 6 months, until May 2021 for his M1 research project. The topic was machine learning extended to timed automata.
- Lucie Guillou, an M1 student at ENS Rennes, was supervised by Nathalie Bertrand, in collaboration with A. R. Balasubramanian and Chana Weil-Kennedy (TU Munich). The topic was the compared expressivity of parameterized models.
- Alban Gutierrez-André, an M1 student at Université de Rennes 1, was supervised by Ocan Sankur in spring 2021, on an internship on multi-agent path finding with partial knowledge.
- Mathieu Poirier, an M2 student at ENS Rennes, was supervised by Éric Badouel for his M2 internship from February to June 2021.

Current Master Students.

- Arthur Dumas, an M1 student at ENS Rennes, is supervised by Nicolas Markey and Ocan Sankur 2h/week during 6 months, since September 2021. The topic is network congestion games with local observation.

- Enzo Erlich, an M1 student at ENS Rennes, is supervised by Loïc Hélouët for his M1 research project. The topic is on resilience of timed systems with repeated delays.

- Gregory Gobin, an M2 student at ENS Rennes, is supervised by Thierry Jéron and Martin Quinson (Myriads project team) since october 2021. His intership topic is the mixing of unfolding based dynamic par-tial order reduction and bounded model-checking for asynchronous distributed programs.

- Naïm Moussaoui, an M1 student at ENS Rennes, is supervised by Thierry Jéron and Martin Quinson (Myriads project team) 2h/week during 6 months, since October 2021. The topic is unfolding-based dynamic partial order reduction for checking liveness properties on asynchronous distributed programs.

Bachelor Students.

- Hugo Francon (may 2021 - july 2021), L3 student at ENS Rennes, was supervised by Nathalie Bertrand and Nicolas Markey, on synchronizing words under LTL constraints.

10.2.3 Juries

- Nathalie Bertrand took part in the HDR committee of Barbara Fila in July 2021.

- Nathalie Bertrand took part in the following PhD committees (all online): Ilina Stoilkovska - *reviewer* - March 2021. TU Wien (AT). Zeinab Ganjei - april 2021. Linkoping University (SE). Léo Exibard - September 2021. Université Libre de Bruxelles (BE) and Marseille.

- Nathalie Bertrand took part in the jury of the Concur Test-of-Time award 2021 [19].

- Nathalie Bertrand was a committee member for a professor position at ENS Rennes and a professor position at Univ Rennes 1. She was a jury member for Inria young researcher competition (CRCN & IFSP) at Rennes Bretagne Atlantique.

- Éric Fabre was an evaluator in Computer Science for the entrance examination at ENS.

- Éric Fabre was president of the jury for Amine Echraibi's PhD defense. IMT Atlantique & Université Rennes 1, Dec. 2021.

- Éric Fabre was in the selection committee for Inria Starting Research Positions.

- Blaise Genest was reviewer of the PhD of Mamhoud Bentriou (Centrale Supelec / Université Paris Saclay)

- Thierry Jéron was a committee member for a professor position at Ecole Centrale Nantes /LS2N.

- Nicolas Markey was the president of jury of Arthur Queffelec's PhD defense. Université de Rennes 1, Nov. 2021.

- Ocan Sankur was in Aline Goeminne's PhD committee - Université de Mons. April 2021.

10.3 Popularization

10.3.1 Internal or external Inria responsibilities

- Loïc Hélouët is responsible of "Mission Jeunes Chercheurs" at Inria Rennes. He is an elected member of the "Comité de Centre" at Inria Rennes and member of the CNHSCT of Inria. He is also representative of Inria in the MathSTIC doctoral school council.
- Thierry Jéron is “référent chercheur” for Inria Rennes since 2016.
- Hervé Marchand is an elected member of the "Comité de Centre" at Inria Rennes.

10.3.2 Education

Several members of the team took part in the organization of “J’peux pas, j’ai informatique”, a 1-day event for maths and computer-science teachers in secondary schools and high schools, about gender stereotypes in computer science.

11 Scientific production

11.1 Major publications

[1] E. Badouel, L. Bernardinello and P. Darondeau. *Petri Net Synthesis*. Text in Theoretical Computer Science, an EATCS Series. Springer, Nov. 2015, p. 339. DOI: 10.1007/978-3-662-47967-4. URL: https://hal.inria.fr/hal-01237142.

[2] C. Baier, N. Bertrand, C. Dubslaff, D. Gburek and 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. URL: https://hal.archives-ouvertes.fr/hal-01883409.

[3] H. Bazille, B. Genest, C. Jegourel and J. Sun. ‘Global PAC Bounds for Learning Discrete Time Markov Chains’. In: *CAV 2020*. Vol. LNCS. CAV 2020 12225. Los Angeles, United States, 2020, pp. 304–326. URL: https://hal.archives-ouvertes.fr/hal-03065571.

[4] N. Bertrand, M. Dewaskar, B. Genest, H. Gimbert and A. Godbole. ‘Controlling a population’. In: *Logical Methods in Computer Science* 15.3 (2019), pp. 1–30. DOI: 10.23638/LMCS-15(3:6)2019. URL: https://hal.archives-ouvertes.fr/hal-02350251.

[5] P. Bouyer, U. Fahrenberg, K. G. Larsen, N. Markey, J. Ouaknine and J. Worrell. ‘Model Checking Real-Time Systems’. In: *Handbook of model checking*. Springer-Verlag, Apr. 2018, pp. 1001–1046. DOI: 10.1007/978-3-319-10575-8_29. URL: https://hal.archives-ouvertes.fr/hal-01889280.

[6] E. Fabre, L. Hélouët, E. Lefaucheux and H. Marchand. ‘Diagnosability of Repairable Faults’. In: *13th International Workshop on Discrete Event Systems*. (Version Longue). Xi’an, China, 2016, pp. 256–262. URL: https://hal.inria.fr/hal-01302562.

[7] S. Pinisetty, Y. Falcone, T. Jéron and H. Marchand. ‘Runtime Enforcement of Regular Timed Properties’. In: *Software Verification and Testing, track of the Symposium on Applied Computing ACM-SAC 2014*. Gyeongju, South Korea: ACM, Mar. 2014, pp. 1279–1286. URL: https://hal.inria.fr/hal-00907571.

11.2 Publications of the year

International journals

[8] G. Bacci, P. Bouyer, U. Fahrenberg, K. Larsen, N. Markey and P.-A. Reynier. ‘Optimal and robust controller synthesis using energy timed automata with uncertainty’. In: *Formal Aspects of Computing* 33.1 (Jan. 2021), pp. 3–25. DOI: 10.1007/s00165-020-00521-4. URL: https://hal.archives-ouvertes.fr/hal-03240104.

[9] N. Bertrand, P. Bouyer and A. Majumdar. 'Reconfiguration and Message Losses in Parameterized Broadcast Networks'. In: *Logical Methods in Computer Science* 17.1 (18th Mar. 2021), pp. 1–18. URL: https://hal.archives-ouvertes.fr/hal-03240099.

[10] N. Bertrand, I. Konnov, M. Lazic and J. Widder. 'Verification of Randomized Consensus Algorithms under Round-Rigid Adversaries'. In: *International Journal on Software Tools for Technology Transfer* 23 (Oct. 2021), pp. 797–821. DOI: 10.1007/s10009-020-00603-x. URL: https://hal.inria.fr/hal-03480268.

[11] P. Bouyer, L. Henry, S. Jaziri, T. Jéron and N. Markey. 'Diagnosing timed automata using timed markings'. In: *International Journal on Software Tools for Technology Transfer* 23.2 (Apr. 2021), pp. 229–253. DOI: 10.1007/s10009-021-00606-2. URL: https://hal-centralesupelec.archives-ouvertes.fr/hal-03321763.

[12] S. Cherrared, S. Imadali, E. Fabre and G. Gössler. 'SFC Self-Modeling and Active Diagnosis'. In: *IEEE Transactions on Network and Service Management* 18.3 (Sept. 2021), pp. 2515–2530. DOI: 10.1109/TNSM.2021.3086424. URL: https://hal.inria.fr/hal-03352706.

[13] L. Hélouët, N. Markey and R. Raha. 'Reachability games with relaxed energy constraints'. In: *Information and Computation* (Oct. 2021), pp. 1–20. DOI: 10.1016/j.ic.2021.104806. URL: https://hal.inria.fr/hal-03482420.

[14] R. Meira-Goes, S. Lafortune and H. Marchand. 'Synthesis of Supervisors Robust Against Sensor Deception Attacks'. In: *IEEE Transactions on Automatic Control*. IEEE Transactions on Automatic Control (2021), p. 12. DOI: 10.1109/TAC.2021.3051459. URL: https://hal.inria.fr/hal-03153391.

[15] R. Singh, L. Hélouët and Z. Miklos. 'Reducing the Cost of Aggregation in Crowdsourcing'. In: *Transactions on Large-Scale Data- and Knowledge-Centered Systems* (Oct. 2021), pp. 1–38. URL: https://hal.archives-ouvertes.fr/hal-03482460.

[16] M. L. Tessitore, M. Sama, A. D'Ariano, L. Hélouët and D. Pacciarelli. 'A Simulation-Optimization Framework for Traffic Disturbance Recovery in Metro Systems'. In: *Transportation research. Part C, Emerging technologies* (2021). URL: https://hal.inria.fr/hal-03482456.

International peer-reviewed conferences

[17] S. Akshay, B. Genest, L. Hélouët, S. Krishna and S. Roychowdhury. 'Resilience of Timed Systems'. In: FSTTCS 2021 - 41st IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science. Virtual Conference due to COVID, India, 15th Dec. 2021, pp. 1–22. DOI: 10.4230/LIPIcs.FSTTCS.2021.33. URL: https://hal.inria.fr/hal-03439247.

[18] N. Bertrand, L. de Alfaro, R. J. Van Glabbeek, C. Palamidessi and N. Yoshida. 'CONCUR Test-Of-Time Award 2021'. In: Concur 2021 - International Conference on Concurrency Theory. Paris, France, 23rd Aug. 2021, pp. 1–3. URL: https://hal.inria.fr/hal-03480255.

[19] N. Bertrand, M. Lazic and J. Widder. 'A Reduction Theorem for Randomized Distributed Algorithms Under Weak Adversaries'. In: VMCAI 2021 - 22nd International Conference on Verification, Model Checking, and Abstract Interpretation. Copenhagen, Denmark, 12th Jan. 2021, pp. 219–239. DOI: 10.1007/978-3-030-67067-2_11. URL: https://hal.inria.fr/hal-03150397.

[20] N. Bertrand, B. Thomas and J. Widder. 'Guard Automata for the Verification of Safety and Liveness of Distributed Algorithms'. In: Concur 2021 - International Conference on Concurrency Theory. Paris, France, 23rd Aug. 2021, pp. 1–17. DOI: 10.4230/LIPIcs.CONCUR.2021.15. URL: https://hal.inria.fr/hal-03480241.

[21] L. Hélouët, Z. Miklos and R. Singh. 'Cost and Quality Assurance in Crowdsourcing Workflows (Extended Abstract)'. In: BDA 2021 - 37 eme Conférence sur la Gestion des Données - Principes, Technologies, Applications. Paris, France, 25th Oct. 2021, pp. 1–2. URL: https://hal.inria.fr/hal-03482426.

[22] L. Hélouët, Z. Miklos and R. Singh. 'Cost and Quality in Crowdsourcing Workflows'. In: PETRI NETS 2021 - 42nd International Conference on Applications and Theory of Petri Nets and Concurrency. Vol. 12734. Lecture Notes in Computer Science. Paris, France: Springer International Publishing, 16th June 2021, pp. 33–54. DOI: 10.1007/978-3-030-76983-3_3. URL: https://hal.inria.fr/hal-03482424.

[23] A. Majith, O. Sankur, H. Marchand and T. Dinh. 'Compositional model checking of an SDN platform'. In: DRCN 2021 - 17th International Conference on the Design of Reliable Communication Networks. Milan, Italy, 19th Apr. 2021, pp. 1–8. URL: https://hal.inria.fr/hal-03229532.

[24] J. Piribauer, C. Baier, N. Bertrand and O. Sankur. 'Quantified Linear Temporal Logic over Probabilistic Systems with an Application to Vacuity Checking'. In: CONCUR 2021 - 32nd International Conference on Concurrency Theory. Paris, France, 13th Aug. 2021, pp. 1–18. DOI: 10.4230/LIPIcs.CONCUR.2021.7. URL: https://hal.archives-ouvertes.fr/hal-03408379.

[25] A. Queffelec, O. Sankur and F. Schwarzentruber. 'Planning for Connected Agents in a Partially Known Environment'. In: AI 2021 - 34th Canadian Conference on Artificial Intelligence. Vancouver / Virtual, Canada, 8th June 2021, pp. 1–23. URL: https://hal.archives-ouvertes.fr/hal-03205744.

Doctoral dissertations and habilitation theses

[26] L. Henry. 'There and back again : formal methods and model learning for real-time systems'. Université Rennes 1, 3rd Dec. 2021. URL: https://hal.archives-ouvertes.fr/tel-03508039.

[27] A. Majumdar. 'Vérification et synthèse de systèmes concurrents paramétrés'. Université Paris-Saclay, 30th Sept. 2021. URL: https://tel.archives-ouvertes.fr/tel-03412980.

[28] A. Queffelec. 'Connected Multi-Agent Path Finding: How Robots Get Away with Texting and Driving'. IRISA, équipe LogicA, 11th Oct. 2021. URL: https://tel.archives-ouvertes.fr/tel-03517091.

[29] S. Sadhukhan. 'A Verification Viewpoint on Network Congestion Games'. Inria Rennes, 9th Dec. 2021. URL: https://tel.archives-ouvertes.fr/tel-03495144.

[30] R. Singh. 'Data Centric Workflows for Crowdsourcing Application'. Université de Rennes 1, 7th May 2021. URL: https://hal.inria.fr/tel-03274867.

Reports & preprints

[31] N. Bertrand, V. Gramoli, I. Konnov, M. Lazic, P. Tholoniat and J. Widder. *Compositional Verification of Byzantine Consensus*. 4th Mar. 2021. URL: https://hal.archives-ouvertes.fr/hal-03158911.

[32] N. Bertrand, B. Thomas and J. Widder. *Guard Automata for the Verification of Safety and Liveness of Distributed Algorithms (long version)*. Inria, 2021, pp. 1–33. URL: https://hal.inria.fr/hal-03283388.

[33] A. Majith, O. Sankur, H. Marchand and T. Dinh. *Compositional model checking of SDN platform*. 26th Feb. 2021. URL: https://hal.inria.fr/hal-03153317.

[34] J. Ngoufo Tagueu, E. Badouel, A. Puerto Aubel and M. T. Tchendji. *Lazy Services: A Service Oriented Architecture based on Incremental Computations and Commitments*. Sept. 2021. URL: https://hal.inria.fr/hal-03353118.

11.3 Cited publications

[35] E. Badouel and U. Schlachter. 'Incremental Process Discovery using Petri Net Synthesis'. In: *Fundamenta Informaticae* 154.1-4 (June 2017), pp. 1–13. DOI: 10.3233/FI-2017-1548. URL: https://hal.inria.fr/hal-01599760.

[36] N. Bertrand, P. Bouyer, T. Brihaye and P. Carlier. 'Analysing Decisive Stochastic Processes'. In: *ICALP 2016 - 43rd International Colloquium on Automata, Languages, and Programming*. Vol. 55. LiPIcs. Rome, Italy: LZI, 2016, 101:1–101:14. DOI: 10.4230/LIPIcs.ICALP.2016.101. URL: https://hal.inria.fr/hal-01397794.

[37] N. Bertrand, P. Bouyer, T. Brihaye and P. Carlier. 'When are stochastic transition systems tameable?' In: *Journal of Logical and Algebraic Methods in Programming* 99 (2018), pp. 41–96. DOI: 10.1016/j.jlamp.2018.03.004. URL: https://hal.inria.fr/hal-01938135.

[38] P. Bouyer, N. Markey, N. Perrin and P. Schlehuber-Caissier. 'Timed automata abstraction of switched dynamical systems using control funnels'. In: *Real-Time Systems* 53.3 (May 2017), pp. 327–353. DOI: 10.1007/s11241-016-9262-3. URL: http://dx.doi.org/10.1007/s11241-016-9262-3.

[39] I. V. Konnov, M. Lazic, H. Veith and J. Widder. 'A short counterexample property for safety and liveness verification of fault-tolerant distributed algorithms'. In: *POPL 2017 - 44th ACM SIGPLAN Symposium on Principles of Programming Languages*. ACM, 2017, pp. 719–734.

[40] A. Nigam and N. S. Caswell. 'Business artifacts: An approach to operational specification'. In: *IBM Systems Journal* 42.3 (2003), pp. 428–445.