Inria international program

Annual report

Associate Team acronym: DISTOL

Period of activity: 2nd year of activity.

Principal investigator (Inria): Loïc Hélouët, (SUMO team, INRIA Rennes).

Principal investigator (partner): Madhavan Mukund (Chennai Mathematical Institute)

Other participants: LOGICA team (IRISA Rennes),

Institute of Mathematical Sciences (IMSC), Chennai, India

National University of Singapore

Teams' web site: http://www.irisa.fr/sumo/DISTOL/

1. Abstract of the scientific program

The DISTOL project (Distributed systems, stochastic models and logics) aims at gathering researchers from INRIA Rennes, two institutes in Chennai, India (CMI and IMSC) and National University of Singapore, working on formal modeling and verification of distributed systems. This project covers four main research directions. Each of these directions rely on specific and complementary competences:

- **R1** : Robustness and time issues in distributed systems models (SUMO : competences in robustness, models for distributed systems – CMI : competences in models for timed and distributed systems)
- **R2** : Applications of formal models & techniques to Web Services (SUMO : competences on modeling of Web Services – CMI : competences in modeling of Web services and verification of distributed systems)
- **R3:** Quantitative verification for distributed systems (SUMO : competences in probabilities, markovian models -NUS : competences in inference in Bayesian networks)
- **R4** : Unification of Control Theory of Distributed Systems (LOGICA : competences in logics, control theory – IMSC : competences in logics, games)

R1: Our main objective is to consider robustness for true concurrency models in a context where each process has its own measurement of time. We study timed variants of Petri nets, building on former results on this model [E-AHJLR12,E-AHJR12], and on experience gained for automata with independently evolving clocks [E-AGMK08], and address robustness problems for this model. We expect several questions to be undecidable, and plan to address these undecidability issues via reasonable restrictions ensuring the existence of (semi) decision procedures.

R2: We want to consider **realistic models for Web-Services**. We have already proposed a session model for Web Services [J-DHM11]. It describes finite sets of agents running an arbitrary number of concurrent transactions. Coverability of some (bad) configuration is decidable for this model. We first want to extend our model and decision procedures to systems with arbitrary numbers of agents. A key challenge is to build realistic but well-structured models, to allow straightforward decidability of interesting safety properties. The second objective is to consider more elaborated properties than coverability, such as **conflicts of interest** between agents, etc. Overall, we wish to propose a highly expressive model together with a decidable logic to reason on this model. The techniques used to reach this goal will build on our knowledge of Well-Structured Transition System [O-FS01], and Petri nets variants. The last and most exploratory objective is **monitoring for session systems**: from a model M of a system, an implementation *I* of this model, and a property to monitor, we want to instrument I with observers (synthesized from M) that raise an alarm when they are sure that the property is violated. Monitoring was studied for pi-calculus [O-HYC08], but it is not yet clear whether the proposed solutions apply to our setting.

R3 : In the next three years, we will develop algorithms to compute precisely probabilities of logical properties, in particular in the presence of imperfect information and/or time. We will build on our work in [J-BG11]. We will also improve the precision of approximated inference algorithms for distributed (parameterized or not) systems, and deduce formal bounds that guarantee the probability to be in an interval of bounded size. For that, we will develop the techniques we introduced in [J-PAGT11]. In particular, we will provide a decomposition algorithm such that the global approximated probability will be more accurate (through a better accuracy on each component) than by considering the system as a monolith. This has been a major objective in analysis of distributed system, but in general, it cannot be reached exactly. However, approximation gives more freedom for clustering. Last, we will develop approximated verification for logics different from PCTL, leveraging on [J-AAGT12].

R4: The goal of this research direction is a **unified theoretical framework for supervisory control theory**. We will investigate to which extent techniques from epistemic reasoning and game theory can be applied to address control problems for distributed systems. The first milestone will be to reformulate supervisory control in logical and game-theoretical terms. In that respect, epistemic logic should help to handle partial observation. The second milestone will consist in bringing together epistemic logic and imperfect information games to handle individual (i.e. subsystems) knowledge. It is a challenging task because, taking apart control theory issues, the logical foundation of games with imperfect information is an emerging field with only few results [O-GDE11,E-MPB11]. The third milestone will consist in incrementing the previous framework by considering communication mechanisms between the subsystems. In game theory, communication between players is very primitive, whereas in epistemic logic, there are powerful rigorous ways to model effects of atomic communication events on the individual knowledge. It is a challenging task to transfer this apparatus to games and will probably lead to new results in game theory but more importantly, in distributed control. The fourth milestone will consist in studying properties of the developed unified framework, both computational and in terms of expressiveness. For this, we may link the new framework with existing logical formalisms and/or game-based settings.

2. Scientific progress

We have progressed all topics of the associated team. We list below results achieved in 2014.

- **R1**: This year, we have proposed a verification framework for a timed variant of Petri nets called ***time Petri nets with Urgency*** **[3]**. Two models have been mainly considered in the literature: time Petri nets, which associate ages to tokens, constraints to arcs (intervals defining allowed ages of tokens) and allow firing a transition *t* if for each place *p* in the preset of *t*, there is a token which age satisfy the constraint associated to *p* and *t*. Time Petri nets allow for the verification of coverability properties, but cannot model urgency: tokens are simply useless when they become too old to meet constraints. On the other hand, timed Petri nets associate firing intervals to transitions, that describe the time that can elapse since enabling of a transition. Reaching the upper bound of an interval forces a transition to fire (this is called **urgency**). Unlike time Petri nets, most of properties of timed Petri nets are undecidable. We have proposed a variant of timed Petri nets with urgency, and showed that a simple separation of places into bounded/unbounded places, together with a restriction on the urgency constraints attached to transitions that consume tokens from unbounded places allow to decide reachability properties. A joint paper has been submitted (INDIA-FRANCE). Next year will be devoted to robustness in such a setting.

  - **R2**: We have progressed on the work initiated in 2013 to model transactional systems and Web-based architectures. The model proposed last year is called ***session systems***, and allows for the modeling of distributed systems in which agents collaborate within sessions. This model allows for specification of behaviors involving arbitrary numbers of agents and arbitrary number of sessions. We have shown [2] that configurations of such systems can be represented as graphs and that upon the restriction that these graphs are decomposable into connected components of bounded size, some interesting security properties can be checked. We have considered business rules such as conflicts of interest, and Chinese wall properties. These results have been presented at ACSD 2014 in June (INDIA-FRANCE).

- **R3:** Two tracks have been followed this year. Concerning inferences in Dynamic Bayesian Networks (DBN), a new inference procedure based on conditional probability have been proposed: it allows to group nodes of a DBN in non-disjoint clusters, hence not having to assume independences between any of the nodes. An intern from INDIA (Ayush Maheshwari) spent two months in the SUMO team this summer (funded by ANR STOCH-MC we are leading). He started to implement the procedure. Experiments are conducted, and a PhD student (Matthieu Pichené) has just been hired (funded by ANR STOCH-MC and Region Bretagne) to pursue the research. Concerning Markov Chains, we are close to a characterization of Markov Chains with a regular language, which allows for their easy analysis. Simply speaking, when all the eigen values of a Markov chain are roots of real, then its language is regular (INDIA-FRANCE-SINGAPORE).

- **R4** : We are working on a way to produce a controller for a distributed system, by expressing constraints as an MSO formula on the execution tree of the system. This MSO formula depicts the properties that the controller have to satisfy. It is known that MSO is undecidable on grids, which distributed processes can generate - hence we cannot hope for a general result for controller synthesis in using this method. A 20 year old conjecture is that MSO is decidable for grid free architectures, that is on systems without arbitrarily long sequences of events in parallel. In such systems, if there is a long sequence of actions, only a limited number of actions can be in parallel with all of them. We are working on this conjecture, which would solve the controller synthesis for grid free distributed systems. (FRANCE-SINGAPORE-CHINA).

  We also started to establish some formal connections between Assumption-Commitment automata (AC-automata) and Dynamic Epistemic Logic (DEL). On the one hand, epistemic transition systems and AC-automata are formal models of distributed computation where communication between processes can take place (via some sort synchronization). On the other hand, Dynamic Epistemic Logic (DEL) deals with the same phenomena but with a semantics based on event models and preconditions. The challenge is to define in a finite manner the preconditions of action models. Also, we investigated a language for specifying protocols in DEL that would allow us to determine the fragment of DEL that corresponds to AC-automata. One of our objectives is to develop methods that synthesize DEL protocols for each agent (process) solving a given (coordination) problem.

3. Next year's work program

- **R1** : We plan to extend the work on Timed Petri nets with restricted Urgency (Timed PNrU) to address robustness issues. A formal model often deals with an idealized representation of time. Robustness questions asks whether formal properties of a model are preserved by an implementation which architectural characteristics may not ensure the desired precision of the model in time measurement. It has been shown that even slight variation in time measure can completely change the overall behavior of a system. Hence a first question to ask is whether a model is robust to imperfection in time measurement. So far, solutions to robustness questions have been proposed for finite models, and solving such issues for Timed PNrU would be a major advance for this topic. Another new research direction started this year is to consider variants of Petri nets which dissociate resource use and time measurement. This would have practical interest, and in particular allow to model systems with requirements of the form "*x must occur between 10 and 20ms after y, when resource r is available*", where *r* need not be available during *10 ms*, but only at firing time.
- **R2** : We plan to pursue the work on session systems. This year's results have shown decidability of security properties for an interesting subclass of the model, that are roughly speaking nested coverability properties. We would like to extend these results to consider more elaborated properties.

On the other hand, unboundedness in session systems comes from the unboundedness in the number of contributing agents and number of initiated sessions. We would now like to focus on analysis of different models that manage and transform structured infinite data. Such models could be defined in terms of session systems, rewriting rules, or as variants of Petri nets with data. The general key issue is to rely on structure of data to ensure good properties of models (decidability of some logic or of control synthesis, diagnosability,…) that would not be granted otherwise.

- **R3:** On the Markov Chain side, next year will be devoted to finish the characterization of Markov Chains with regular language. Concerning DBNs, we will finish the experiments on our inference algorithm on non-disjoint clusters, and develop new algorithms based on Kullbach Leibler "norm" in order to find the most relevant (small) clustering. Indeed, small clusters are important for the efficiency of the inference. On the other hand, a non optimised clusterisation leads to inaccurate results.
  Finally, we will apply these results on the apoptosis pathway, in link with ANR Stoch-MC.
- **R4:** We will finalize our paper on the grid free conjecture, together with considering different class of distibuted systems. In particular, weak grid freeness allows two long sequence of actions in parallel in case they never communicate anymore. Checking an MSO formula on this class might be reducible to checking MSO for the class of grid free systems, in which case it would extend the procedure to produce controllers of distributed systems to this richer class.

4. Record of activities

In **March 2014**, L. Hélouët visited M. Mukund and N. Kumar (CMI) for one week. During this stay, the team worked on verification problems for a variant of Time Petri nets. The main objective of this work is to propose a model that can decouples time measurement and resources use. In the current semantics of TPN, time since enabling of a transition is measures as soon as the preset of the transition is filled, and on can require a transition to fire after an delay laying within an interval [a,b] after enabling. This is a problem, as places are used at the same time to model control and use of resources. We have proposed a model where time is measured as soon as a subset of the preset of a transition is filled. This allows to model requirements of the form "*x must occur between 10 and 20ms after y when resource r is available*", where r need not be available during 10 ms, but only at firing time. This work should lead to a publication in 2015.

In **April 2014**, a joint paper on session systems, a model for distributed transactional systems and Web-based systems was accepted for publication at the **ACSD** conference (in June). A complete report is available from Distol's website. This publication is an outcome of a visit of M. Mukund and S. Akshay in 2013.

From June to August 2014, Akshay Sundararaman visited the SUMO team. It was the occasion for B. Genest, L. Hélouët and S. Akshay to progress work on verification of concurrent timed systems. The result of this work is a variant of timed Petri nets that allow urgency, along with subclasses that allow verification of logical properties. This model is very powerful: it can be used to design communicating systems and take into consideration the throughput and latencies of communication channels. The result was submitted to a conference, and a full report is available from Distol's Website.

From **May to July 2014**, Rishika Garg (IIT Kampur) visited the SUMO team for a L1 internship, focusing on formal models for Web Services. DISTOL has funded the travel, and the sojourn expenses were funded by the INRIA internship program. The topic of this work was to propose a model where data is represented as structured documents, and business rules as transformations of these documents enriched with communications.

From **May to July 2014**, Dhananjay Raju, a student from CMI, did his internship in the SUMO team. His master topic was modular diagnosis, i.e. how to detect occurrences of faults when using multiple diagnosers to observe a system. D. Raju successfully defended his master.

From **May to July 2014**, Ayush Maheshwari a student from IIT Kanpur, did his internship in the SUMO team. His master topic was to develop and implement inference in DBNs for non-disjoint clusters based on conditional probabilities. His trip and sojourn were entirely funded by ANR STOCH-MC.

In **November 2014**, B. Genest visited professor P.S. Thiagarajan to progress work on quantitative verification for distributed systems, with an application to the analysis of biological pathways such as the apoptosis pathway.

In **November 2014**, G. Aucher has visited R. Ramanujam to progress work on control theory and logic.

5. Production

Publications :

[1] Manindra Agrawal, S. Akshay, Blaise Genest, P.S. Thiagarajan. Approximate Verification of the Symbolic Dynamics of Markov Chains. Accepted in JACM.

[2] L. Hélouët, S. Akshay, M. Mukund, Sessions with an unbounded number of Agents, Accepted at ACSD'14, June 2014.

[3] S. Akshay, Blaise Genest, Loïc Hélouet. Timed Petri Nets with (restricted) Urgency. (submited)

[4] D. Raju, Diagnosability of Modular Discrete Event Systems, Master Thesis, 2014.

6. Non- Public Information

All the information contained in this report can be made public.

7. Changes on the Team

On the scientific side, the obtained results and future objectives of the team remain consistent with the original program. We can list several (normal) changes occurred this year in the consortium:

- A young researcher, Bastien Maubert, has left the LOGICA team after completing his PhD.
- S. Palaniappan (who did his PhD thesis at NUS Singapore with Prof Thiagu) will start a post doc in the SUMO team in December 2014, funded by the INRIA postdoc program.
- Matthieu Pichené, a new PhD student will join SUMO in December 2014, funded by ANR Stoch-MC and Region Bretagne. He will integrate the associated team.
- Several young researchers have joined CMI and are informally connected to the activities of the team.

We are strengthening our collaboration with IIT Bombay, and in particular with S. Akshay.

8. Budget requested for the coming year

Co-Funding available in 2014:

As for 2014, we can rely on several additional sources to fund DISTOL's collaborations in 2015.

LIA Informel: Researchers from Rennes (N. Bertrand, L.Hélouët, B. Genest) are invited in the CNRS LIA Informel, which is an international collaboration between laboratories in Chennai and French laboratories. This LIA can fund several visits each year, from both sides. Researchers in Chennai (CMI & IMSC) benefit from the same funding by the LIA, and will use it to fund visits to France.

ANR: Blaise Genest is currently leading an ANR project StochMC on stochastic model checking for biological systems. A part of the funds from this ANR will be used to hire students, and fund research on topics related to the associated team (and in particular research direction **R3**).

The SUMO team has also applied for several grants from ANR this year, and most of the research projects submitted are connected to the main themes of DISTOL. Upon success a part of the funds could be used to provide means for the associated team.

INRIA/ University of Rennes 1 Chair: G. Aucher owns a chair, which gives him funds to attend conferences and for visiting partners. These funds can be used to organize visits to India.

NUS and Singapore Ministry of Educational Faculty Research: P.S. Thiagarajan received a grant of 62000 SGD (39000 euros) from the Ministry of Educational Faculty Research in Singapore to fund studies on “Approximate Analysis of Networks of Dynamical Systems”. NUS opens a special line of 50000 SGD (30000 euros) in order to welcome French researchers in the context of UMI IPAL whose NUS A/Prof Jin Song Dong is a co director, and Blaise Genest an ex member of.

IIT Bombay Grant: S. Akshay, was awarded a personal DST/INSPIRE faculty award and research grant by the Department of Science and Technology, Govt of India._ This grant will allow him to visit the SUMO team in 2015. He also has a 3 years seed grant from IIT Bombay.

Université de Rennes 1 : S. Akshay’s travel in 2014 was funded as a “professeur invité” position from université de Rennes 1. If this funding mechanism is still available in 2015, we will apply to fund long sojourns of our partners in Rennes.

Planned expenses in 2015 :

Visits: We plan bilateral visits on each research topic. The total amount devoted to visits should hence be 2000 * 5 = 10 000 euros.

Internships: We also plan to offer one or two internships for young Indian researchers, and similarly to send young researchers for an internship in India. Each internship should cost around 2000 euros (travel + accommodation).

Dissemination: We expect some publications: the work on urgency in Time Petri nets has been submitted, and we expect a publication in 2015. Achieving two or three publications with our partners in 2015 seems a reasonable objective. The total cost to present two common works is estimated to 1500 + 2000 euros (one presentation in Europe, one in a non-European country). The table below summarizes the planned expenses to run the associated team in 2015.

Expense	Cost	Nb	Total
Visits Rennes-> Partner	2000	3	6000
Visits Partner -> Rennes	2000	2	4000
Internship Rennes	2000	1	2000
Internship India	2000	1	2000
Conference (Europe)	1500	1	1500
Conference (Other countries)	2000	1	2000
Total			17 500

Required Funding from the EA Program : 10 000 euros

Appendix : References

[E-AHJLR12] S.AKshay, L. Hélouët, C. Jard, D. Lime, O.H.Roux, *Robustness of Time Petri Nets under Architectural Constraints*, in FORMATS 2012, , LNCS no 7595, pages 11-26, 2012.

[E-AHJR12] S. Akshay, L. Hélouët, C. Jard and P.A. Reynier, *Robustness of Time Petri Nets under Guard Enlargement*, in RP 2012, LNCS no 7550, pages 92-107, 2012.

[E-AGMK08] S. Akshay, B. Bollig, P. Gastin, M. Mukund, K. N. Kumar: Distributed Timed Automata with Independently Evolving Clocks. CONCUR 2008, pages 82-97, 2008.

[J-DHM11] P. Darondeau, L. Hélouët, M. Mukund. *Assembling Sessions*, In Automated Technology for Verification and Analysis (ATVA), LNCS no 6996, Pages 259-274, Taiwan, 2011.

[O-FS01] A. Finkel, Ph. Schnoebelen: Well-structured transition systems everywhere! Theoretical Computer Science no 256(1-2), pages 63-92, 2001.

[O-HYC08] K. Honda, N. Yoshida, and M. Carbone. Multiparty Asynchronous Session Types. In POPL, pages 273–284, 2008.

[J BG11] Nathalie Bertrand, Blaise Genest. Minimal Disclosure in Partially Observable Markov Decision Processes. FSTTCS 2011, P 411-422, LIPIcs, 2011.

[J-PAGT11] S. Palaniappan, S. Akshay, Blaise Genest, P.S. Thiagarajan. A Hybrid Factored Frontier Algorithm for Dynamic Bayesian Networks. IEEE/ACM CMSB 2011, pages 35-44, 2011.

[J-AAGT12] M. Agrawal, S. Akshay, Blaise Genest, P. S. Thiagarajan: Approximate Verification of the Symbolic Dynamics of Markov Chains. IEEE/ACM LICS 2012, pages 55-64, 2012.

[O-GDE11] D. P. Guelev, C. Dima, C. Enea: An alternating-time temporal logic with knowledge, perfect recall and past: axiomatisation and model-checking. Journal of Applied Non-Classical Logics 21(1), pages 93-131, 2011.

[E-MPB11] B. Maubert, S. Pinchinat and L. Bozzelli. Opacity Issues in Games with Imperfect Information. Gandalf2011, 2nd International Symposium on Games, Automata, Logics and Formal Verification, EPTCS no 54, pages 87-101, 2011.