Formal Modeling and Verification of Parameterized and Distributed Systems

Radu IOSIF (VERIMAG, Grenoble, France)
mailto:Radu.Iosif@univ-grenoble-alpes.fr
https://nts.imag.fr/index.php/Radu_Iosif

Arnaud SANGNIER (DIBRIS, Università di Genova, Italy)
mailto:arnaud.sangnier@unige.it
https://person.dibris.unige.it/sangnier-arnaud/

1 Context, goal and challenges

Applications of distributed systems are omnipresent, allowing to share resources and coordinate activities between geographically distributed parties. Furthermore, they increase the resilience of systems through fault tolerance, availability, and recovery mechanisms. Designing, understanding, and validating distributed systems is challenging because of the huge number of interactions between components, some potentially leading to unpredictable scenarios. Ensuring the correctness of distributed systems is not yet mature — to cite Lamport[1]:

> *Concurrent algorithms can be quite subtle and hard to get right, their correctness proofs require a degree of precision and rigor unknown to most mathematicians (and many computer scientists).*

Reconfiguration is inherent to modern distributed computing. Processes can be created or removed due to internal faults, redistribution of resources, workload or traffic changes. Moreover, the shape of the communication network may change. Cloud computing, IoT and edge computing vitally relly on such features.

Mechanizing the analysis and verification of distributed systems is notoriusly difficult. Recently, there has been a notable trend to apply interactive theorem provers, i.e., using proof assistants, to the task. We propose to develop a complementary set of verification methods based, on generalizations of the more mechanized methods from the *model-checking* and *automated theorem proving* communities.

It is known that even the most sophisticated state-of-the-art model-checking techniques scale poorly when the number of processes increases. Moreover, in a distributed system processes can be created or disappear at runtime. This is why in our models we do not fix the number of processes a priori. Such models support verification methods able to prove correctness *for any number of processes* in the network. Of course, it is more demanding to verify a *parametric model* than a model with a fixed number of processes.

2 Methodology and workplan

The goal is to develop new verification techniques allowing to analyse the behaviour of distributed applications using such dynamic reconfiguration. We consider the following research directions (the final research project will be defined with the successful candidate):

1. The first research direction will consist in developing logics and automated reasoning techniques that enable writing formal proofs of correctness of self-adapting distributed systems. A promising approach is using logics that describe the shape of a network (i.e., the interconnection of processes via communication channels) and how this shape changes with time. To this end, recent work of the hosting group at VERIMAG considers Graph Grammars, Monadic Second Order Logic and Separation Logic[2,3].
2. The second research direction will be developing automatic methods to verify models representing the behavior of self adapting distributed systems. Since most of the verification problems are undecidable on expressive models, it is necessary to propose approximation techniques in order to answer partially to the verification problem. A first step could be to see how to introduce dynamic reconfigurations in this model and then to find efficient approximations techniques to detect problems automatically.

Particular attention will be devoted to the implementation of practical verification tools. To this end, the candidate is expected to work on implementation and prototyping, in addition to theoretical research. It is expected that the candidates should hence have good knowledge in logics and automata theory and it would be appreciated if they have followed during their studies a course on formal methods for verification.

[1] L. Lamport. How to write a 21st century proof. *Journal of Fixed Point Theory and Applications*, 11(1):43–63, 2012.

[2] E. Ahrens, M. Bozga, R. Iosif, and J.-P. Katoen. Reasoning about distributed reconfigurable systems. *Proc. ACM Program. Lang.*, 6(OOPSLA2), 2022. https://dl.acm.org/doi/abs/10.1145/3563293

[3] M. Bozga, R. Iosif, and J. Sifakis. Verification of component-based systems with recursive architectures. *Theor. Comput. Sci.*, 940(Part):146–175, 2023. https://www.sciencedirect.com/science/article/abs/pii/S0304397522006181

3 Funding and application

The 3-year PhD scolarship between the laboratory VERIMAG in Grenoble (France) and the laboratory DIBRIS in Genova (Italy) will be funded by the French ANR project PAVEDYS (Parametric Verification of Dynamic Distributed Systems), see `https://raduiosif.github.io/PAVEDYS/`. Participation to project meetings and interaction with the groups involved in this project is to be expected.

Applications consisting of a CV and motivation letter should be sent by mail at Radu Iosif (`mailto:Radu.Iosif@univ-grenoble-alpes.fr`) and Arnaud Sangnier (`mailto:arnaud.sangnier@unige.it`). Motivation letters should be human-written and not AI-generated. Additional material, including e.g., recommendation letters and grades transcripts are not required but constitute a plus.