Formal Methods for the Verification of Self-Adapting 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:sangnier@irif.fr
https://www.irif.fr/~sangnier/main-sangnier.html

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.

Self-adapting systems initiate and carry out reconfiguration sequences automatically, in order to avoid expensive or even mission-critical downtimes, required by manual reconfiguration. The verification techniques developped in this thesis will be designed with such dynamic reconfiguration aspects in mind.

2 Methodology and workplan

The goal is to develop new verification techniques allowing to analyse the behaviour of distributed applications using such dynamic reconfiguration. Two possible research directions are possible for this internship.

The first one 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. Recent work of the hosting group at VERIMAG considers a variant of *Separation Logic*[2] equipped with a special connective that decomposes a structure into sub-structures with disjoint interpretations of the relations from the signature. This logic has been used to write Hoare-style proofs of correctness of dynamic reconfiguration programs[3] and check absence of concurrency errors in infinite sets of configurations[4].

The other research direction will be based on developing automatic methods to verify models representing the behavior of self adapting distributed system,s. Since most of the verification problems are undecidable on expressive models, it will be 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] https://en.wikipedia.org/wiki/Separation_logic

[3] 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

[4] 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

This internship might lead to a 3-year PhD scolarship between the laboratory VERIMAG in Grenoble (France) and the laboratory DIBRIS in Genova (Italy), funded by the French ANR project PAVEDYS (Parametric Verification of Dynamic Distributed Systems).

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:sangnier@irif.fr`).