

Internship 2023: Enhancing verification for modular distributed programming

Marc Shapiro (marc.shapiro@lip6.fr), Ahmed Bouajjani (abou@irif.fr), Laurent Proserpi (laurent.proserpi@lip6.fr)

Keywords

Distributed systems; distributed programming; programming languages and verification; composition; system architecture

Background

Distributed systems are increasingly widespread and critical. A typical distributed system is a composition of communicating, concurrent modules; this enhances scalable performance, modularity, clear APIs, elasticity and flexibility. However, composition is hard because of concurrency, failures, and lack of guarantees such as type checking.

Accordingly, our group aims to develop a programming environment that both leverages the strengths of distributed computing, and helps to tackle its issues. Such an environment should enable the developer to reason about individual components and about the behaviour of their composition, while preserving performance and programmer control.

Our Varda distributed programming environment is designed to reconcile performance and strong abstractions. A Varda program specifies a system as an *architecture* of independently-developed *components*. Each component has a well-specified *protocol* interface and high-level *safety constraints*. Furthermore, the developer specifies the system's *orchestration*, i.e., how components are created, destroyed, where they are located, how they interact, and what invariants must be maintained. A Varda system can be re-architected flexibly thanks to transparent interception.

Research perspectives

Currently, Varda performs a limited repertoire of static verifications (e.g., session types), and inserts dynamic assertions for some others (e.g., preconditions and postconditions). Hooks can be used to extend the compiler, e.g., with other kinds of static verification.

The goal of the internship is to improve the verification capabilities of the Varda compiler. The intern shall work on two fronts: improving its type system, and exporting a Varda architecture as a formal model to an external checker (e.g., TLC, Coq or P), in order to statically verify invariants.

Requirements and application

The internship research will be advised by Ahmed Bouajjani, of IRIF and Marc Shapiro, of Sorbonne-Université and Inria. It will take place in Paris, France. Speaking French is not required.

The candidate should ideally be interested in distributed systems and be familiar with compilation and formal approaches (e.g. model-checking).

From the practical point of view, they should also have a basic experience in software programming in OCaml (Vardac is written in OCaml) and usage of collaborative tools such as git.

Please provide the following information:

- A resume or Curriculum Vitæ.
- A motivation letter.
- A list of courses and grades of the last two years of study (an informal transcript is OK).