MITSUBISHI ELECTRIC R&D CENTRE EUROPE

1, ALLEE DE BEAULIEU, CS 10806
35708 RENNES CEDEX 7, FRANCE
TEL. (+33) 02.23.45.58.58 – FAX (+33) 02.23.45.58.59

Post-doctoral position

Safe and efficient multi-paradigm concurrent programs analysis

Reference INSFT040

Overall context:

Set up in the middle of the scientific campus of Rennes, the capital of Brittany, the French branch of Mitsubishi Electric R&D Centre Europe provides advanced R&D support to the Japanese R&D centres and to the business units of Mitsubishi Electric Corporation. Within the Communication and Information Systems (CIS) division, Information and Network Systems (INS) team focuses its research interests on industrial networks design and formal methods, including the formal verification of distributed systems and concurrent programs.

Description of the research project:

Computer software has an increasing need of processing power, e.g. for image processing or distributed control, but processors speed is limited, and processing power will not increase so much in coming years. One solution is to use several processors concurrently for a same program execution, i.e., the so-called “multicore” programming or concurrent programming. However, developing such concurrent programs is error prone. Many kinds of errors can occur like deadlocks, livelocks, data races, ordering violation or atomicity violation. Detecting such kinds of errors is difficult as they are related to subtle timing conditions between the concurrent parts, which are executed in parallel on different processors and are nearly impossible to reproduce by usual testing. Moreover, concurrency in programs means an exponential increase in possible program states due to many possibilities of concurrent parts parallel execution, making testing even more difficult. The on-going project is to develop analyses for C programs, with the objective of avoiding concurrent bugs statically, by detecting for example accessed variables, aliases, required or missing data protection and by proposing adequate protection mechanisms.

Objectives:

In its current state, the project has two main drawbacks. First, for scalability reasons, the underlying pointer/alias analysis has been designed to be performant but not so precise. While using more precise techniques like abstract interpretation on the whole program would be too expensive, mixing performant and precise techniques on different portions of the source code would be valuable to reach a good trade-off. One objective of this position is to study possible approaches and implement them. Secondly, our model focuses on data protection using mutexes, that are not always appropriate in certain applications. Another objective of this position is to design and implement a memory model enabling abstract data protection, that could be instantiated to e.g. mutexes or hardware interrupts.

Another more long-term objective is to address other issues of concurrent programs that we have not tackled yet, like livelocks or axiomatization of external libraries.

Job description:

- Conduct a survey on correct-by-construction concurrent programming and *a posteriori* verification of concurrent programs;
- Propose an abstract memory model to depict data accesses, sharing and protection in C programs;
- Study mixed-analysis techniques for pointer and alias analysis;
- Participate to the development of a plug-in for helping the debugging and the verification of multi-paradigm concurrent C programs;
- Disseminate the proposed solutions through open-source software and publications in international conferences or journals.

Required education and experience:

Mandatory:

- A PhD degree in Formal Methods;
- At least 3 years of experience (including the PhD experience) in research, within public or private R&D laboratories;
- Research experience marked by publications in high-rank conferences or journals;
- High-level skills in parallel programs design and implementation.

Preferably:

- A PhD degree with a particular interest in parallel programs verification

Personal profile:

- Open-mindedness, capacity to work in a multicultural and international environment;
- Motivation to work in a dynamic industrial research environment;
- Excellent communication and interpersonal skills;
- Fluent English.

Duration: at least 12 months

Dates: April 1st, 2025

Contact: Magali BRANCHEREAU (jobs@fr.merce.mee.com)

Please send us your application (resume and cover letter) including the job opening reference: INSFT040.