2018-01057 - Static analysis of byzantine consensus

Level of qualifications required: Graduate degree or equivalent
Function: PhD Position

Context
Fault-tolerant consensus protocols (benign and byzantine) are at the core distributed systems, e.g., Amazon Dynamo, Apache Zookeeper, blockchain technologies. To ensure availability in the presence of faults, or to avoid a central authority, an application is deployed on several replicas. A client of the application communicates with any of these replicas, inducing a change in the application state. A consensus protocol is in charged to keep the replicas consistent, that is all replicas see the same set of client interactions (in the same order).

Due to the multiple sources of non-determinism, e.g., network reliability, cheating participants, the development of these systems is challenging and highly error prone. The goal of this project is to develop static analysis techniques that increase confidence in fault-tolerant byzantine protocols and implementations.

The position is within the team ANTIQUE, formed by leading experts in abstract interpretation. ANTIQUE focuses on developing automated tools to detect semantic properties of programs. The team is affiliated with INRIA Paris and is located at Ecole Normale Superieure (rue d'ULM, Paris). The working environment pairs two of the best French institutions in formal methods and programming languages. The PhD position is funded by the French National Research Agency, in the context of the project SATTA, i.e., static analysis of fault-tolerant algorithms.

Assignment
Byzantine fault-tolerant protocols are among the most challenging systems when it comes to ensuring their correctness. It is well known that the consensus problem is unsolvable over asynchronous networks under the presence of faults. Hence, algorithms and systems designers struggle to find conditions under which this problem can be solved. These conditions are incomparable, leading to different protocols. Moreover, the design of a consensus protocol is not only constrained by the network behavior, but also by requirements that come from the client. A simple example would be a client that wants the order of its commands to be preserved or not, and a more complex one being a system tolerant to malicious clients which try to destabilize it.

Designing automated verification techniques for Byzantine systems requires connecting three research areas: distributed algorithms (designing algorithmic solutions to fundamental problems), systems (focused on implementing and optimizing algorithms), and formal verification which uses mathematical models to rigorously check that the algorithms and their implementations respect the intended specifications.

The candidate's main activity consists in exploring the three research areas mentioned above and to design and implement a verification method for Byzantine protocols. The techniques preferred in the group use SMT-solvers, refinement, and abstract interpretation. The projects aim for a high degree of automation, using a reduced amount of user input. For a better knowledge of the proposed research topic please do not hesitate to contact us or to check the webpage https://www.di.ens.fr/~cezard. We are interested in theoretical and foundational solutions that can be prototyped, preferably as extensions of our current infrastructure.

The recruited person will primarily work with Cezara Dragoi. This research is embedded in a collaboration with researchers from other institutes, for example (INRIA Nancy), Josef Widder (TU Wien), Damien Zufferey (MPI Kaiserslautern).

Main activities
Main activities:
- participate at group meetings and seminars at ENS and INRIA
- read and write research papers
- prototype research ideas

Skills
Technical skills and level required: distributed systems, formal methods, SMT-solvers, abstract interpretation, are highly appreciated but not mandatory.
Languages: English (mandatory), French (optional), C++, Go, Java.
Relational skills: team work

Benefits package
- Subsidised catering service
- Partially-reimbursed public transport

General Information
- Theme/Domain: Proofs and Verification
- Town/City: Paris
- Inria Center: CRI de Paris
- Starting date: 2018-12-01
- Duration of contract: 3 years
- Deadline to apply: 2018-10-24

Contacts
- Inria Team: ANTIQUE
- Recruiter: Dragoi Cezara / cezara.dragoi@inria.fr

About Inria
Inria, the French National Institute for computer science and applied mathematics, promotes "scientific excellence for technology transfer and society". Graduates from the world's top universities, Inria's 2,000 employees rise to the challenges of digital sciences. With its open, agile model, Inria is able to explore original approaches with its partners in industry and academia and provide an efficient response to the multidisciplinary and application challenges of the digital transformation. Inria is the source of many innovations that add value and create jobs.

The keys to success
We are looking for enthusiastic candidates that pay attention to Byzantine behaviors and like formal reasoning. The candidate should enjoy team working and be passionate about learning new concepts.

Conditions for application
Defence Security:
This position is likely to be situated in a restricted area (ZRR), as defined in Decree No. 2011-1425 relating to the protection of national scientific and technical potential (PPST). Authorisation to enter an area is granted by the director of the unit, following a favourable Ministerial decision, as defined in the decree of 3 July 2012 relating to the PPST. An unfavourable Ministerial decision in respect of a position situated in a ZRR would result in the cancellation of the appointment.

Recruitment Policy:
As part of its diversity policy, all Inria positions are accessible to people with disabilities.

Warning: you must enter your e-mail address in order to save your application to Inria. Applications must be submitted online on the Inria website. Processing of applications sent from other channels is not guaranteed.