UNIVERSITÉ DE RENNES 1

Direction de la Recherche et de l'Innovation

Appel à projets - Année 2021

Contrats doctoraux «Ordinaires»

ECOLE DOCTORALE : MathSTIC **POLE DE RECHERCHE : MathSTIC**

Unité de recherche d'accueil

Unité de Recherche : Irisa/Inria RBA

Equipe : Sumo

Encadrement

Directeur de thèse : Nicolas Markey **Unité de recherche** : Irisa (UMR 6074)

Employeur/Établissement d'origine :CNRS

HDR : • oui ~~• non~~ **Nb de thèses en cours** : 3

Mail : nicolas.markey@irisa.fr **Tél.** : +33 (0)2 99 84 22 76

Co-directeur de thèse : Nathalie Bertrand **Unité de recherche** : Inria RBA

Employeur/Établissement d'origine : Inria

HDR : • oui ~~• non~~ **Nb de thèses en cours** : 2

Mail : nathalie.bertrand@inria.fr **Tél.** : +33 (0)2 99 84 22 81

Sujet

Titre : Verification of distributed algorithms with fair schedulers

Mots clés : parameterized verification, model checking, automata theory, logics, Petri nets

Cotutelle internationale (oui/non) : non **Si oui, préciser l'établissement et le pays de rattachement** :

Sollicitation d'un cofinancement EDUC (oui/non) : non

Descriptif (15-30 lignes) :
Contexte socioéconomique et scientifique ; Les hypothèses et questions posées ; Les grandes étapes de la thèse et démarche ; Approches méthodologiques et techniques envisagées

Context

Distributed algorithms are algorithms executed asynchronously by several identical components that interact and communicate e.g. by rendez-vous, message broadcast, or shared variables. They are heavily used in numerous applications such as telecommunications, cloud computing or blockchain technologies. Such algorithms usually have simple objectives, such as selecting a leader among the participants or agreeing on a proposed value. Still, in the area of distributed algorithms, proving correctness properties of such algorithms usually relies on ad hoc manual proofs. One of the main difficulties lies in the fact that the number of components is seen as a parameter, and that the aim is to prove correctness for any value of this parameter.

In the area of model checking, parameterized verification has been a very active field over the last few years [BJK+15, BMR+16, LR16, BKL+19, BEH+20]: it precisely aims at developing model-checking techniques to verify properties of parameterized systems, made of an arbitrary number of copies of one component (usually represented as a finite transition system). Automated verification techniques would avoid errors in the highly non-trivial task analyzing of distributed algorithms. However, modelling real-life distributed algorithms and proving their correctness is still mostly out-of-reach of formal verification

techniques, either because the models considered are not expressive enough, or because the techniques are not adapted (e.g. they do not take fairness into account), or because they are not efficient enough.

Objectives

Our aim is to develop automated parameterized-verification techniques to formally prove properties of distributed algorithms. A possible target is to be able to automatically prove correctness of Aspnes' consensus algorithm [Asp02], in which a network of components have to reach a consensus using shared variables.

A model-checking technique has recently been developed to verify termination of consensus algorithms for a bounded number of shared registers [BMR+16]. It addresses fairness issues by considering a randomized scheduler. However, this technique does not apply to Aspnes' algorithm, which requires two registers per round (hence arbitrarily many registers). Our aim is to build on such existing work to develop and analyze (complexity-wise) novel verification techniques that would apply to distributed algorithms such as Aspnes'.