RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE SUJET DE THESE

Intitulé : Un atelier dédié à la spécification et vérification formelles d'algorithmes distribués

Référence : **TIS-DTIS-2025-33**
(à rappeler dans toute correspondance)

Début de la thèse : rentrée 2025	**Date limite de candidature :**

Mots clés

spécification formelle ; preuve formelle ; vérification semi-automatique ; algorithmes distribués

Profil et compétences recherchées

Master / ingénieur informatique ou logique

Présentation du projet doctoral, contexte et objectif

La quantité croissante des systèmes distribués au sein des systèmes critiques rend essentielle la tâche de vérification de leur bon fonctionnement. Ce besoin est notamment présent dans les systèmes aérospatiaux et robotiques étudiés au sein du département DTIS à l'ONERA. Des études en cours portent par exemple sur l'analyse de systèmes embarqués dans des drones, ou l'analyse de protocoles utilisés par une constellation de satellites d'observation terrestre. Une composante majeure de ces systèmes repose sur l'utilisation d'algorithmes de coordination, partage d'informations, communication, reconfiguration, etc. Leur correction est donc un problème fondamental. Toutefois, établir cette correction formellement demeure une tâche très ardue en pratique. Outre la difficulté intrinsèque à établir une preuve de correction de ces algorithmes, les approches et outils formels (TLA+ [Lamport], Event-B [Abrial], Alloy [Jackson], Why3 [Filliâtre], Dafny [Leino]...) existants présentent tous des lacunes à divers niveaux, tels qu'un langage de spécification peu approprié, ou manquant de concepts dédiés, ou encore des techniques de vérification peu adaptées (notamment pour les propriétés de vivacité, énonçant que des situations espérées finiront effectivement par se produire) ou automatiques mais incomplètes (n'apportant des preuves que pour des systèmes de petite taille).

Des travaux réalisés à l'ONERA ont par exemple étudié le système distribué pair-à-pair Chord [Stoica], tout d'abord en renonçant à la complétude [FMCAD2018], puis en renonçant à l'aspect automatique [FM2019]. Des travaux en cours entre l'ONERA et l'IRIT s'intéressent maintenant à un modèle plus complexe du même algorithme. Dans ce contexte, des pistes prometteuses pour l'élaboration d'un langage de spécification formelle dédié aux algorithmes distribués ainsi que pour une approche de preuve semi-automatique (combinaison d'indices saisis par l'utilisateur et de solveurs automatiques puissants) ont été tracées.

Lors de ce doctorat, le travail consistera à :

- Étudier les travaux précédents sur le protocole Chord (et autres algorithmes distribués représentatifs) ;
- Étudier les approches essentielles de spécification et vérification formelles utiles dans le contexte des algorithmes distribués ;
- Proposer un concept de langage, et méthode vérification associée.

Références

[FM2019] Jean-Paul Bodeveix, Julien Brunel, David Chemouil, Mamoun Filali. Mechanically Verifying the Fundamental Liveness Property of the Chord Protocol. In 3rd World Congress on Formal Methods (FM 2019), Lecture Notes in Computer Science.

[FMCAD2018] Julien Brunel, David Chemouil, Jeanne Tawa. Analyzing the Fundamental Liveness Property of the Chord Protocol. In 18th Conference on Formal Methods in Computer-Aided Design (FMCAD 2018), IEEE Press

Collaborations envisagées	
Pr Jean-Paul Bodeveix IRIT	
Laboratoire d'accueil à l'ONERA Département : Traitement de l'information et Systèmes Lieu (centre ONERA) : Toulouse **Contact** : David Chemouil, Julien brunel Tél. : 05 62 25 29 36 Email : David.chemouil@onera.fr	**Directeur de thèse** Nom : David Chemouil Laboratoire : Tél. : 05 62 25 29 36 Email : David.chemouil@onera.fr

Pour plus d'informations : https://www.onera.fr/rejoindre-onera/la-formation-par-la-recherche