RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE STAGE EN COURS D'ETUDES

Référence : **DTIS-2025-18**
(à rappeler dans toute correspondance)

Lieu : Toulouse

Département/Dir./Serv. : DTIS/SEAS

Tél. : 05 62 25 2681

Responsable(s) du stage : Julien Brunel & David Chemouil

Email. : julien.brunel@onera.fr

DESCRIPTION DU STAGE

Thématique(s) : Ingénierie des Systèmes et des Logiciels

Type de stage : ☒Fin d'études bac+5 ☒Master 2 ☐ Bac+2 à bac+4 ☐ Autres

Intitulé : Vérification automatique de systèmes non bornés

Sujet : La présence de grande quantité de logiciels embarqués au sein de systèmes critiques rend essentielle la tâche de vérification de leur bon fonctionnement. Ce besoin est notamment présent dans les systèmes aérospatiaux et robotiques qui sont 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. L'idée est d'utiliser une approche permettant de modéliser un tel système afin de prouver qu'il satisfait bien ses exigences. Proposer une telle approche, applicable à une grande classe de systèmes, est un défi scientifique en raison du langage très riche nécessaire pour exprimer à la fois la structure et la dynamique du système, et des techniques de vérifications qui doivent pouvoir explorer un très grand nombre de configurations différentes du système.

De nombreuses approches, basées sur des langages munis de techniques de vérification formelle comme TLA+ [Lamport] ou Alloy [Jackson], ont été proposées pour analyser une vaste classe de systèmes. Ces travaux renoncent en général à l'un des deux aspects suivants :

- une vérification *automatique* : en y renonçant, l'utilisateur doit guider la preuve « manuellement » ce qui s'avère fastidieux et complexe,
- une vérification *complète* : en effet, une solution pour rendre la vérification automatique est de borner la taille du système étudié. Une erreur qui se produirait pour un système de taille supérieure à cette borne ne peut pas être détectée par la vérification, qu'on appelle alors *incomplète*.

Des travaux réalisés à l'ONERA ont par exemple étudié le système distribué pair-à-pair Chord, soit en renonçant à l'aspect automatique [FM2019] soit en renonçant à la complétude [FMCAD2018]. Plus récemment, une technique basée sur un fragment de la logique temporelle du premier ordre FO-LTL a été proposée [ATVA2016, InfComp2021,CAV2021]. Elle permet d'aller vers plus d'automatisation sans renoncer à la complétude. Toutefois, son applicabilité reste limitée à des systèmes distribués relativement simples.

Lors de ce stage, le travail consistera à :

- étudier l'approche proposée dans [CAV2021],
- identifier une classe de systèmes sur lesquels l'approche est applicable,en se basant notamment sur les systèmes aérospatiaux et robotiques étudiés à l'ONERA,
- étendre / adapter l'approche pour la rendre applicable à une classe plus grande de systèmes. Une piste prometteuse, en cours d'exploration au DTIS, consiste à généraliser l'un des cadres permettant de faire de la vérification à base de logique temporelle propositionnelle (les automates de Büchi) de manière à prendre en compte la logique du premier ordre.

Références

[CAV2021] Quentin Peyras, Jean-Paul Bodeveix, Julien Brunel, David Chemouil. Sound Verification Procedures for Temporal Properties of Infinite-State Systems.. In *33rd International Conference on Computer-Aided Verification (CAV 2021)*.

[InfComp2021] Quentin Peyras, Julien Brunel, David Chemouil. A Decidable and Expressive Fragment of Many-Sorted First-Order Linear Temporal Logic. In Information and Computation, Vol. 280, Elsevier, 2021.

[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

[ATVA2016] Denis Kuperberg, Julien Brunel, David Chemouil. On Finite Domains in First-Order Linear Temporal Logic. In 14th International Symposium on Automated Technology for Verification and Analysis (ATVA 2016), Lecture Notes in Computer Science.

[Lamport] Leslie Lamport. Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers, Addison-Wesley, 2002.

[Jackson] Daniel Jackson. Software Abstractions (revised edition) Logic, Language, and Analysis, MIT Press, 2016.

Est-il possible d'envisager un travail en binôme ? Non

Méthodes à mettre en oeuvre :

☒ Recherche théorique	☒ Travail de synthèse
☒ Recherche appliquée	☒ Travail de documentation
☐ Recherche expérimentale	☐ Participation à une réalisation

Possibilité de prolongation en thèse : Oui

Durée du stage : Minimum : 5 mois Maximum : 6 mois

Période souhaitée : printemps – été 2025

PROFIL DU STAGIAIRE

Connaissances et niveau requis :	Ecoles ou établissements souhaités :
connaissances en méthodes formelles / logique	M2 en informatique ou école d'ingénieur