ONERA
THE FRENCH AEROSPACE LAB

www.onera.fr

PROPOSITION DE SUJET DE THESE

Intitulé : Preuve formelle en calcul réseau

Référence : **TIS-DTIS-2018-07**
(à rappeler dans toute correspondance)

Laboratoire d'accueil à l'ONERA :

Domaine : Réseau embarqué et vérification formelle — Lieu (centre ONERA) : Toulouse

Département : Département Traitement de l'Information et Systèmes**}**

Unité : Langage Architecture et Preuve pour les Systèmes embarqués — Tél. : 05 62 25 29 05

Responsable ONERA : Pierre Roux — Email : pierre.roux@onera.fr

Directeur de thèse envisagé :

Nom : Marc Boyer

Adresse : DTIS

Tél. : 05 62 25 26 36 Email : marc.boyer@onera.fr

Sujet : De nos jours les avions ne peuvent se passer d'un important réseau embarqué pour faire communiquer les nombreux capteurs et actionneurs qui y sont disséminés. Ces réseaux ayant une fonction critique, en particulier pour les commandes de vol, il est important d'en garantir certaines propriétés telles des délais de traversé ou l'absence de débordement de buffers. Le calcul réseau est une méthode mathématique permettant de réaliser de telles preuves [2]. Elle a joué un rôle clef dans la certification du réseau AFDX, dérivé de l'ethernet, utilisé à bord des avions les plus récents (A380, A350).

Le calcul réseau se base sur des résultats mathématiques relativement simples mais déjà bien assez subtils pour qu'il soit très facile de commettre des erreurs ou des omissions lors de preuves papier. Par ailleurs, les assistants de preuve sont un bon outil pour réaliser une vérification mécanique de ce genre de preuves et obtenir un très haut niveau de confiance dans leurs résultats.

On souhaite donc formaliser avec un tel outil les propriétés fondamentales à la base de la théorie du calcul réseau. Ces résultats font intervenir des propriétés relativement basiques sur les nombres réels, telles des bornes supérieures voire des limites de fonctions linéaires par morceaux. On se propose pour cela d'utiliser l'assistant de preuve Coq ainsi que la récente librairie Coquelicot [1] étendant sa librairie de réels de base.

Ces travaux visent à long terme la réalisation d'un outil de calcul réseau accompagnant ses résultats d'éléments permettant d'en réaliser automatiquement une preuve formelle, y compris sur des configurations « industrielles ». Une fois les résultats principaux du calcul réseaux formalisés, la thèse pourra donc s'intéresser à la réalisation d'un tel prototype, applicable tout d'abord à des cas d'étude simples. Ce prototype pourrait s'appuyer sur les traces fournies par l'outil industriel RtaW Pegase.

Références

[1] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond.

Coquelicot: A User-Friendly Library of Real Analysis for Coq.
Mathematics in Compute Science, 9(1):41–62, March 2015.
[2] Jean-Yves Le Boudec and Patrick Thiran.
Network calculus: a theory of deterministic queuing systems for the internet,
volume 2050. Springer Science & Business Media, 2001.

Collaborations extérieures : INRIA Grenoble – Rhône Alpes

PROFIL DU CANDIDAT

Formation : Informatique

Spécificités souhaitées :