Formalisation en Coq du Calcul Réseau

Soutenance de thèse – RAKOTOMALALA Lucien

15 février 2022 à 10h00

Salle des thèses, ISAE SUPAERO, 10 Av. Edouard Belin, Toulouse

Devant le jury composé de :

M. Yves BERTOT, Rapporteur
M. Emmanuel GROLLEAU, Rapporteur
Mme Sophie QUINTON, Examinatrice
Mme Sylvie BOLDO, Examinatrice
M. Jean-Paul BODEVEIX, Examinateur
M. Jean-Yves LE BOUDEC, Examinateur
M. Marc BOYER, Directeur de thèse
M. Pierre ROUX, Co-directeur de thèse

Résumé

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 que des délais de traversée ou l'absence de débordement de buffers. Le calcul réseau est une méthode mathématique permettant de réaliser de telles preuves. Elle a joué un rôle clé 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 utilisant l'algèbre tropicale. Ces résultats sont relativement simple mais déjà bien assez subtiles pour qu'il soit très facile de commettre des erreurs ou des omissions lors de preuves papier ou de calcul de valeur concrètes. 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.

Nous formalisons donc avec un tel outil les notions et propriétés fondamentales de la théorie du Calcul Réseau. Ces résultats font intervenir des propriétés sur les nombres réels, tel que des bornes supérieures et des limites de fonctions linéaires donc nous souhaitons utiliser un outil de formalisation capable d'implémenter un tel niveau mathématique. Nous utilisons l'assistant de preuve Coq. Il s'agit d'un outil disposant déjà d'un long développement dont la librairie Mathematical Components qui permet de formaliser de l'analyse sur les nombres réels et la construction de structures algébriques comme celles utilisées dans le Calcul Réseau.

Le calcul de valeurs effectives repose sur des opérations de l'algèbre min-plus sur des fonctions réelles. Des algorithmes sur des sous ensembles spécifiques peuvent être trouvés dans la littérature. De tels algorithmes et leurs implémentations sont toutefois compliqués. Plutôt que de développer une preuve de la bonne implémentation de ces algorithmes, nous prenons une implémentation existante comme Oracle et nous donnons des critères de vérifications en Coq.

Mots clés

Coq, Réseau temps réel, Calcul dans min-plus, Calcul Réseau

Un lien zoom sera disponible via le lien ci-dessous :
https://www.onera.fr/fr/staff/lucien-rakotomalala