Soutenance de thèse

Lucien RAKOTOMALALA soutiendra sa thèse de doctorat préparée au sein de l'ISAE-ONERA MOIS et intitulée «*Preuve Formelle en calcul réseau*»

Le 15 février 2022 à 10h00, salle des thèses de l'ISAE-SUPAERO

devant le jury composé de

M. Marc BOYER	Ingénieur de recherche ONERA	Directeur de thèse
M. Pierre ROUX	Ingénieur de recherche ONERA	Co-directeur de thèse
Mme Sophie QUINTON	Chargée de recherche INRIA Grenoble	
Mme Sylvie BOLDO	Directrice de recherche INRIA	
M. Yves BERTOT	Directeur de recherche INRIA	Rapporteur
M. Emmanuel GROLLEAU	Professeur ISAE-ENSMA	Rapporteur
M. Jean-Paul BODEVEIX	Maître de Conférences Université Toulouse 3	
M. Jean-Yves LE BOUDEC	Professeur Ecole Polytechnique Fédérale de Lausanne	

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 des délais de traversée 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 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 effective 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 [3]. 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.

[1] Anne Bouillard, Marc Boyer et Euriell Le Corronc. Deterministic Network Calculus : From Theory to Practical Implementation. John Wiley & Sons, Ltd, oct. 2018
[2] Assia Mahboubi et Enrico Tassi. Mathematical Components. Zenodo, jan. 2021
[3] Anne Bouillard et Eric Thierry. « An Algorithmic Toolbox for Network Calculus ». In : Discret. Event Dyn. Syst. 18.1 (2008), p. 3-49.

Mots-clés : Calcul Réseau, Coq, Réseau temps réel, Calcul dans min-plus

Summary: Nowadays aircraft need a large on-board network to communicate the many sensors and actuators that are disseminated there. As these networks have a critical function, particularly for flight controls, it is

important to guarantee certain properties such as crossing delays or the absence of overflow buffers. Network calculus is a mathematical method for performing such proofs[2]. It played a key role in the AFDX network certification, derived from ethernet, used on board the most recent aircraft (A380, A350). The network calculation is based on relatively simple mathematical results but already quite subtle enough that it is very easy to commit errors or omissions during paper proofs. Moreover, proof assistants are a good tool for mechanically checking such evidence and obtaining a very high level of confidence in their results. We would like to formalize with this tool the fundamental properties underlying the theory of network computation. These results involve relatively basic properties on real numbers, such as upper bounds or even limits of linear functions per piece. We propose to use the Coq proof assistant as well as the recent Coquelicot library[1] extending its basic real library. In the long term, this work aims to produce a network calculation tool that accompanies its results with elements that automatically provide formal proof, including on 'industrial' configurations. Once the main results of the network calculation have been formalized, the thesis could therefore focus on the realization of a similar prototype, applicable initially to simple case studies. This prototype could be based on the traces provided by the RtaW Pegase industrial tool. Translated with www.DeepL.com/Translator

Keywords : Network Calculus, Coq, Embedded Networks, Min plus computation