Sujet de thèse

Modélisation et vérification formelles de contraintes de vol

Directrice : Christine Choppy (Paris 13)
Encadrants : Camille Coti (Paris 13), Romain Kervarc (ONERA)

1 Contexte

Pour faire face à l'augmentation du trafic aérien général, diverses pistes sont proposées visant à enrichir de davantage de données les échanges entre contrôle aérien et aéronefs. Cette approche permet de donner aux aéronefs une marge de manoeuvre à l'intérieur de contraintes fournies par le contrôle, et à ce dernier de se focaliser sur sa mission de régulation et de supervision d'ensemble, ce qui allège sa charge globale. Un tel exemple de système plus distribué a été proposé à l'ONERA sous la forme de contrats 4D [1], i.e. des trajectoires d'avion délimitées dans l'espace et dans le temps, respectant un certain nombre de contraintes (spatiales, temporelles, internes ou externes).

Les contraintes fournies par le contrôle aux aéronefs doivent pouvoir à la fois être planifiés à l'avance pour un espace aérien donné, mais également être adaptés en temps réel à la situation lorsqu'ils sont exécutés [6] : évitement de zones dangereuses, compensation de retard, ... L'idée de ces approches est que la gestion de conflit doit pouvoir se faire manière locale et distribuée, pendant que le contrôle aérien exerce une supervision d'ensemble. La planification doit également inclure une certaine robustesse à l'égard des retards ou des possibles situations d'urgence. Bien sûr, cela implique une grande quantité de vérifications à effectuer, qui ne peuvent l'être que par l'usage de méthodes formelles [3, 8]. Une difficulté particulière réside dans le fait que les propriétés à vérifier ne sont pas seulement symboliques, mais incluent des contraintes physiques et géométrique. En effet, outre des propriétés plus classiques de robustesse ou des propriétés de proportionnalité entre la rareté de l'évément perturbateur et le nombre d'aéronefs impactés par la déconflixion, il faut également garantir des propriétés incluant des paramètres physiques, comme la volabilité des trajectoires, qui vise à s'assurer que l'aéronef peut toujours inscrire une trajectoire volable dans les contraintes qui lui sont envoyées (et qu'on ne lui demande pas par exemple de patienter sur place en vol ou de monter, descendre ou virer trop abruptement). Le model-checking est une approche bien adaptée pour les problèmes de vérifications mentionnés ci-dessus, mais l'inclusion de propriétés continues difficilement discrétisables (telles que la volabilité) est une difficulté importante pour les performances de calcul.

2 But de la thèse

Diverses approches ont été proposées pour faire du model-checking face à un système complexe et des propriétés continues. Elles consistent en général à faire abstraction de certains détails afin de limiter la complexité des modèles et faciliter les raisonnements et les vérifications, puis à réintroduire ces détails ultérieurement par des opérations de raffinement qui doivent respecter certaines règles afin de préserver la sémantique des modèles [4].

L'objectif de la thèse proposée est de démontrer que ces méthodes de model-checking permettent de vérifier ces propriétés, malgré la difficulté posée par la perte de performance qu'induit en général la discrétisation de propriétés continues portant sur un grand nombre d'objets, en l'illustrant sur le cadre applicatif des contrats 4D.

Il s'agira dans un premier temps d'analyser les contraintes du système en vue de sa formalisation : sur la base de scenarii représentatifs, il faudra identifier des propriétés et appréhender la dynamique du système en traduisant des contraintes physiques sous la forme de propriétés discrètes vérifiables.

Dans un second temps, il s'agira d'extraire de ce travail des spécifications formelles et à mettre en oeuvre des techniques pour réduire la complexité du modèle [2, 7, 5] (abstraction, symétries, parallélisation, compositionnalité, ...) afin de maîtriser la complexité des vérifications à effectuer.

Enfin, dans un troisième temps, il s'agira, sur la base de ce travail, d'identifier des études de cas d'intérêt et de les analyser. Cette analyse pourra consister à développer un module de réaffectation de contrats 4D à vérifier formellement et à intégrer dans une simulation de trafic aérien. Les résultats de cette analyse pourront le cas échéant permettre de faire évoluer les propriétés et les modèles à vérifier.

3 Conditions de la thèse

Cette thèse s'effectuer en collaboration entre le LIPN (Ch. Choppy, C. Coti) et l'ONERA (R. Kervarc). Elle s'incrit dans le cadre d'une collaboration entre le LIPN (Ch. Choppy, C. Coti, L. Petrucci), le LIP6 (Sorbonne Université : F. Kordon) et l'ONERA (R. Kervac), dans le cadre de laquelle il est également prévu de déposer un projet d'ANR auquel, s'il est retenu, la thèse pourra s'intégrer.

Références

[1] Contract definition for the 4DCo-GC project. Technical report, 4DCo-GC Consortium, 2011.

[2] É. André, C. Coti, and H. G. Nguyen. Enhanced distributed behavioral cartography of parametric timed automata. In *Proc. 17th International Conference on Formal Engineering Methods*, 2015.

[3] P. Carle, C. Choppy, R. Kervarc, and A. Piel. A formal coloured Petri net model for hazard detection in large event flows. In *APSEC - Volume 1*, pages 323–330, 2013.

[4] Christine Choppy, Micaela Mayero, and Laure Petrucci. Coloured Petri net refinement specification and correctness proof with Coq. *Innovations in Systems and Software Engineering*, 6(3) :195–202, 2010.

[5] Christine Choppy, Laure Petrucci, and Alfred Sanogo. Coloured Petri nets refinements. In *PNSE+ ModPE*, pages 187–201. Citeseer, 2013.

[6] Daphna Gekht and Moshe Idan. Tactical re-planning within the 4D contracts ATC concept. In *AIAA Guidance, Navigation and Control Conference, Boston, Massachusetts*, 2013.

[7] S. Haddad, F. Kordon, L. Petrucci, J-F. Pradat-Peyre, and N. Trèves. Efficient state-based analysis by introducing bags in Petri net color domains. In *ACC*, pages 5018–5025. IEEE, 2009.

[8] L. M. Kristensen, J. Billington, L. Petrucci, Z. Qureshi, and R. Kiefer. Formal specification and analysis of airborne mission systems. In *21st IEEE Digital Avionics Systems Conference (DASC'2002)*, volume 1, pages 4.D.4–1–4.D.4–13, 2002.