Titre : Méthodes formelles pour la conception de systèmes robotiques robustes

Encadrants

— ONERA : David Doose
— LaBRI : Olivier Ly, Frédéric Herbreteau

Sujet

Contexte

La conception et le développement de systèmes robotiques modernes est une problématique complexe, car elle regroupe au sein d'une même entité physique ("le robot") de nombreuses activités issues de domaines de recherche variés. En effet, la majorité des systèmes robotiques actuels possèdent des algorithmes de décision intelligents, des algorithmes de planification, de perception, de contrôle, souvent un middleware robotique, des éléments de communication, des tâches temps-réel, etc. De plus, ces systèmes robotiques sont amenés à interagir avec des humains ou à être déployés au contact d'humains ou sur des sites sensibles. Il devient donc indispensable d'apporter des garanties sur le fonctionnement de ces systèmes. Les méthodes de vérification formelle permettent d'obtenir une garantie par preuve et sont donc intéressantes pour avoir un haut niveau de confiance dans le bon fonctionnement de ces systèmes.

La complexité intrinsèque et la diversité des systèmes robotiques rend souvent impossible l'analyse "monobloc" complète du système, c'est pourquoi il est courant de décomposer le système complet en sous-parties pour lesquelles il existe des méthodes d'analyses bien définies.

Les différents systèmes robotiques que nous mettons en œuvre suivent généralement la représentation en strates suivantes :

— intelligence et décision, haut niveau et planification ;
— modélisation et implémentation des différentes capacités des robots (Skills) ;
— définition et implémentation des éléments fonctionnels ;
— middleware robotique (ROS2) ;
— modélisation, analyses et exécution de tâches temps-réel.

Différents travaux récents fournissent des techniques et outils permettant d'adresser l'analyse d'une couche. Cependant, le cloisonnement des différentes analyses est un frein à l'analyse complète du système. En effet, certaines propriétés de bon fonctionnement du système ne peuvent être étudiées qu'avec des analyses raisonnant simultanément sur les différentes strates.

Sujet

Ces dernières années, l'équipe SEAS de l'ONERA a mené différents travaux qui ont conduit à définir un langage de spécification des capacités (*skills*) des ro-

bots [LDG20 ; Alb+21]. Ce langage (Robot Language) sert actuellement de support pour différentes vérifications sur les architectures robotiques de l'ONERA, et également de point d'entrée pour la génération automatique de code ROS2. Le code ainsi généré est, par construction, conforme à la spécification. Nous avons aussi développé des méthodes d'analyses de systèmes temps-réel, adaptées aux spécificités du middleware ROS2 [Var+22], ainsi qu'une bibliothèque permettant l'exécution correcte de ces nouveaux modèles d'exécution temps-réel [Var+21].

Au LaBRI, l'équipe MTV a une riche expérience de développement de techniques et d'outils de vérification formelle, notament AltaRica [Tea] et plus récemment TChecker [HP] qui implémente des algorithmes *state-of-the-art* de vérification d'automates temporisés [HSW22 ; Gov+22 ; HSW16 ; Her+20]. Quand à l'équipe DART, elle développe des travaux autour de la robotique agricole et des robots humanoïdes : l'équipe Rhoban a été sacrée championne du monde de football *kid-size* à 4 reprises ces dernières années. Récemment, les équipes MTV et DART ont initié des travaux communs autour de la "robustesse des systèmes autonomes" au sein du Réseau de Recherche Impulsion ROBSYS de l'Université de Bordeaux.

L'objectif de cette thèse est dans un premier temps d'identifier les limitations du découpage en couches pour l'analyse, puis, dans un second temps, de proposer de nouvelles méthodes transverses. Plus précisément, des travaux récents mettent en avant deux pistes de recherches prometteuses.

La première suggère de disposer d'une méthode d'analyse permettant à la fois de modéliser ou spécifier les contraintes et objectifs des algorithmes de décision haut niveau et les capacités bas niveau du robot, afin d'analyser plus précisément son comportement réel. Plusieurs approches peuvent être envisagées à partir d'un modèle "Robot Language", allant de la vérification formelle d'algorithmes de décision à la synthèse d'une intelligence correcte par construction.

La seconde piste porte sur les couches basses et l'exécution temps réel du système. D'une part, il existe des méthodes d'analyse du comportement des tâches temps réel (étude d'ordonnançabilité). D'autre part, il existe des méthodes formelles d'analyse de systèmes temps-réels, basées par exemple sur les automates temporisés ou les réseaux de Petri, et sur la logique temporelle/temporisée. Cependant, coupler ces deux approches pour produire des ordonnancements corrects vis-à-vis de spécifications temporelles ou temporisées est toujours un problème de recherche ouvert.

Il existe souvent de bonnes raisons pour lesquelles il n'est pas possible de coupler certaines analyses. Dans certains cas, le problème devient trop complexe pour être analysé sur des systèmes réels. Dans d'autres cas le problème devient simplement indécidable. L'objectif de cette thèse est donc d'augmenter l'expressivité des modèles et des spécifications tout en préservant la décidabilité des problèmes de vérification ou de synthèse, afin de permettre l'analyse de propriétés de robustesse de systèmes robotiques. En particulier, des approches compositionnelles exploitant la structuration en couches pourront être envisagées.

Références

[Alb+21] Alexandre Albore, David Doose, Christophe Grand, Charles Lesire et Augustin Manecy. "Skill-Based Architecture Development for Online Mission Reconfiguration and Failure Management". In : *2021 IEEE/ACM 3rd International Workshop on Robotics Software Engineering (RoSE)*. IEEE. 2021, p. 47-54.

[Gov+22] R. Govind, Frédéric Herbreteau, B. Srivathsan et Igor Walukiewicz. "Abstractions for the local-time semantics of timed automata : a foundation for partial-order methods". In : *LICS '22 : 37th Annual ACM/IEEE Symposium on Logic in Computer Science, Haifa, Israel, August 2 - 5, 2022*. Sous la dir. de Christel Baier et Dana Fisman. ACM, 2022, 24 :1-24 :14.

[Her+20] Frédéric Herbreteau, B. Srivathsan, Thanh-Tung Tran et Igor Walukiewicz. "Why Liveness for Timed Automata Is Hard, and What We Can Do About It". In : *ACM Trans. Comput. Log.* 21.3 (2020), 17 :1-17 :28.

[HP] Frédéric Herbreteau et Gérald Point. *TChecker : a model-checker for timed automata*. https ://github.com/ticktac-project/tchecker.

[HSW16] Frédéric Herbreteau, B. Srivathsan et Igor Walukiewicz. "Better abstractions for timed automata". In : *Inf. Comput.* 251 (2016), p. 67-90.

[HSW22] Frédéric Herbreteau, B. Srivathsan et Igor Walukiewicz. "Checking Timed Büchi Automata Emptiness Using the Local-Time Semantics". In : *33rd International Conference on Concurrency Theory, CONCUR 2022, September 12-16, 2022, Warsaw, Poland*. Sous la dir. de Bartek Klin, Slawomir Lasota et Anca Muscholl. T. 243. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 12 :1-12 :24.

[LDG20] Charles Lesire, David Doose et Christophe Grand. "Formalization of robot skills with descriptive and operational models". In : *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. IEEE. 2020, p. 7227-7232.

[Tea] The AltaRica Team. *AltaRica project : methods and tools for AltaRica language*. https ://altarica.labri.fr.

[Var+21] Benoit Varillon, Jean-Baptiste Chaudron, David Doose et Charles Lesire. "Corail, Real-Time ROS2". In : *ROSCon (Lighting Talk)*. 2021.

[Var+22] Benoit Varillon, Jean-Baptiste Chaudron, David Doose et Charles Lesire. "Real-Time Polling Task : Design and Analysis". In : *Euromicro DSD/SEAA*. IEEE. 2022.