Proceedings of the
2nd Workshop on Artificial Intelligence and Formal Verification, Logics, Automata and Synthesis (OVERLAY),
September 25, 2020

Verifying Autonomous Robots: Challenges and Reflections

Clare Dixon[1]

[1]Department of Computer Science, The University of Manchester, UK,
clare.dixon@manchester.ac.uk

Abstract

Autonomous robots such as robot assistants, healthcare robots, industrial robots, autonomous vehicles etc. are being developed to carry out a range of tasks in different environments. The robots need to be able to act autonomously, choosing between a range of activities. They may be operating close to or in collaboration with humans, or in environments hazardous to humans where the robot is hard to reach if it malfunctions. We need to ensure that such robots are reliable, safe and trustworthy. In this talk I will discuss experiences from several projects in developing and applying verification techniques to autonomous robotic systems. In particular we consider: a robot assistant in a domestic house, a robot co-worker for a cooperative manufacturing task, multiple robot systems and robots operating in hazardous environments.

1 Introduction

Autonomous robots are being developed to carry out tasks in many areas of society and have the potential to be very beneficial. They may have to operate in unknown and dynamic environments some of which may be hazardous to humans. They may also have to collaborate with or operate close to humans. As well as developing the robots themselves we must also make sure that they are functionally correct, safe, reliable, robust and trustworthy. A short paper describing this work can be found at [8].

Verification aims to show that the system requirements do actually hold in the designed or implemented system. Informally verification is often described as *Did we build the system right?*. Techniques we may use to verify systems include both formal and non-formal verification. Formal verification involves a mathematical analysis of systems using tools and techniques such as model checkers and theorem provers (see for example [10]). Non-formal verification includes techniques such as simulation based testing and physical testing of the real system (see for example [1] for a survey of testing practices and challenges for robot systems). Simulation based testing involves testing runs of the system within a simulator where tests can be generated in different ways to assess different aspects of the system and analyse their coverage. Physical testing involves testing the system in the lab or in an environment similar to the one it will be deployed in.

2 Approach

We advocate a modular approach to robot architectures with a separation of the decision making aspects from the lower level control. With a modular approach different types of verification can be used for different components (see for example [3, 9, 4]), termed *heterogeneous verification*, as some subsystems may be more critical than others and some verification techniques may be more appropriate than others for these subsystems. Further we propose using a combination of different types of verification, termed *corroborative verification*, for example formal verification via model checking, simulation based testing and real robot experiments to improve the confidence in the overall system [18].

We have applied verification techniques to a number of different types of robot systems including robot assistants; robots in hazardous environments; robot swarms and wireless sensor networks. For the robot assistants we focused two use cases, a domestic robot assistant located in a smart house and collaborative manufacture. For the former we applied model checking to the robot decision making aspects [16, 17, 6, 11] and carried out user validation about the participant's trust in the robot using two scenarios where the robot appeared faulty or not [14]. For the collaborative manufacture use case we examined a robot to human handover task developing the corroborative verification approach [18] using probabilistic model checking, simulation based testing [2] and end user experiments with the robot.

With respect robots in hazardous environments such as space or nuclear we have applied the modular heterogeneous verification approach [3] using first-order logic to specify the assumptions on inputs and guarantees on outputs for each module so that we can ensure that the system architecture satisfies these [9, 4, 5]. Further we have applied formal verification via model checking to an astronaut rover team working scenario [19]

With respect to robot swarms we have applied model checking to algorithms for swarm coherence and foraging [7, 13] and and to synchronisation properties for wireless sensor networks [12, 15].

3 Conclusions

We briefly discussed our approach to verification of robotics and autonomous systems and their application to particular use cases. We advocate the use of different verification techniques together, both formal and non-formal, to improve the confidence in systems as well as also a modular approach using different types of verification for different subsystems. Many challenges remain including how to better design robots for verification, improved routes to standards and certification, how to cope with the state space explosion for formal verification, modelling uncertain and unstructured environments, how to deal with systems that learn, and trust in such systems including both over and under trusting such systems.

Acknowledgments

The work discussed in this document was carried out collaboratively with researchers on the following funded research projects: Trustworthy Robot Systems[1]; Science of Sensor Systems Software[2]; Future AI and Robotics Hub for Space and Robotics[3]; and Artificial Intelligence for Nuclear[4]

This work was funded by the Engineering and Physical Sciences Research Council (EPSRC) under the grants Trustworthy Robot Systems (EP/K006193/1) and Science of Sensor Systems Software (S4 EP/N007565/1) and by the UK Industrial Strategy Challenge Fund (ISCF), delivered by UKRI and managed by EPSRC under the grants Future AI and Robotics Hub for Space (FAIR-SPACE EP/R026092/1) and Robotics and Artificial Intelligence for Nuclear (RAIN EP/R026084/1)

[1] www.robosafe.org
[2] www.dcs.gla.ac.uk/research/S4/
[3] www.fairspacehub.org
[4] rainhub.org.uk

References

[1] Afsoon Afzal, Claire Le Goues, Michael Hilton, and Christopher Steven Timperley. A study on challenges of testing robotic systems. In *13th IEEE International Conference on Software Testing, Validation and Verification, ICST 2020, Porto, Portugal, October 24-28, 2020*, pages 96–107. IEEE, 2020.

[2] D. Araiza-Illan, D. Western, A. G. Pipe, and K. Eder. Coverage-driven verification - an approach to verify code for robots that directly interact with humans. In N. Piterman, editor, *Hardware and Software: Verification and Testing - 11th International Haifa Verification Conference, HVC 2015, Haifa, Israel, November 17-19, 2015, Proceedings*, volume 9434 of *Lecture Notes in Computer Science*, pages 69–84. Springer, 2015.

[3] R. C. Cardoso, M. Farrell, M. Luckcuck, A. Ferrando, and M. Fisher. Heterogeneous verification of an autonomous curiosity rover. In *NASA Formal Methods Symposium (NFM)*, 2020.

[4] R. C. Cardoso, M. Farrell, M. Luckcuck, A. Ferrando, and M. Fisher. Heterogeneous verification of an autonomous curiosity rover. In *Proceedings of the NASA Formal Methods Symposium*. Springer, 2020.

[5] Rafael C. Cardoso, Louise A. Dennis, Marie Farrell, Michael Fisher, and Matt Luckcuck. Towards compositional verification for modular robotic systems. In *Second Workshop on Formal Methods for Autonomous Systems*, 2020.

[6] C. Dixon, M. Webster, J. Saunders, M. Fisher, and K. Dautenhahn. "The Fridge Door is Open"- Temporal Verification of a Robotic Assistant's Behaviours. In M. Mistry, A. Leonardis, M. Witkowski, and C. Melhuish, editors, *Advances in Autonomous Robotics Systems*, volume 8717 of *Lecture Notes in Computer Science*, pages 97–108. Springer, 2014.

[7] C. Dixon, A.F.T. Winfield, M. Fisher, and C. Zeng. Towards Temporal Verification of Swarm Robotic Systems. *Robotics and Autonomous Systems*, 2012.

[8] Clare Dixon. Verifying autonomous robots: Challenges and reflections (invited talk). In Emilio Muñoz-Velasco, Ana Ozaki, and Martin Theobald, editors, *27th International Symposium on Temporal Representation and Reasoning, TIME 2020, September 23-25, 2020, Bozen-Bolzano, Italy*, volume 178 of *LIPIcs*, pages 1:1–1:4. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

[9] M. Farrell, R. C. Cardoso, L. A. Dennis, C. Dixon, M. Fisher, G. Kourtis, A. Lisitsa, M. Luckcuck, and M. Webster. Modular verification of autonomous space robotics. In *Assurance of Autonomy for Robotic Space Missions Workshop*, 2019.

[10] M. Fisher. *An Introduction to Practical Formal Methods Using Temporal Logic*. Wiley, 2011.

[11] P. Gainer, C. Dixon, K. Dautenhahn, M. Fisher, U. Hustadt, J. Saunders, and M. Webster. Cruton: Automatic verification of a robotic assistant's behaviours. In L. Petrucci, C. Seceleanu, and A. Cavalcanti, editors, *Critical Systems: Formal Methods and Automated Verification, Proceedings of FMICS-AVoCS*, volume 10471 of *Lecture Notes in Computer Science*, pages 119–133. Springer, 2017.

[12] P. Gainer, S. Linker, C. Dixon, U. Hustadt, and M. Fisher. Multi-Scale Verification of Distributed Synchronisation. *Formal Methods in System Design*, 2020.

[13] S. Konur, C. Dixon, and M. Fisher. Analysing Robot Swarm Behaviour via Probabilistic Model Checking. *Robotics and Autonomous Systems*, 60(2):199–213, 2012.

[14] M. Salem, G. Lakatos, F. Amirabdollahian, and K. Dautenhahn. Would You Trust a (Faulty) Robot?: Effects of Error, Task Type and Personality on Human-Robot Cooperation and Trust. In *International Conference on Human-Robot Interaction (HRI)*, pages 141–148, Portland, Oregon, USA, 2015. ACM/IEEE.

[15] M. Webster, M. Breza, C. Dixon, M. Fisher, and J. McCann. Exploring the effects of environmental conditions and design choices on iot systems using formal methods. *Journal of Computational Science*, 2020.

[16] M. Webster, C. Dixon, M. Fisher, M. Salem, J. Saunders, K. Koay, and K. Dautenhahn. Formal verification of an autonomous personal robotic assistant. In *Proceedings of Workshop on Formal Verification in Human Machine Systems (FVHMS)*. AAAI, 2014.

[17] M. Webster, C. Dixon, M. Fisher, M. Salem, J. Saunders, K. L. Koay, K. Dautenhahn, and J. Saez-Pons. Toward Reliable Autonomous Robotic Assistants Through Formal Verification: A Case Study. *IEEE Transactions on Human-Machine Systems*, 46(2):186–196, April 2016.

[18] M. Webster, D. Western, D. Araiza-Illan, C. Dixon, K. Eder, M. Fisher, and A. Pipe. A corroborative approach to verification and validation of human–robot teams. *International Journal of Robotics Research*, 39(1):73–99, 2020.

[19] Matt Webster, Louise Dennis, Clare Dixon, Michael Fisher, Richard Stocker, and Maarten Sierhuis. Formal verification of astronaut-rover teams for planetary surface operations. In *IEEE Aerospace Conference (Aeroconf)*, 2020.