Robotics and Integrated Formal Methods: Necessity meets Opportunity

Marie Farrell, Matt Luckcuck, and Michael Fisher

Department of Computer Science, University of Liverpool, UK

26th of September 2018

Robotic System Properties

Multi-dimensional:

- Embedded System

Robotic System Properties

Multi-dimensional:

- Embedded System
- Cyber-Physical System

Robotic System Properties

Multi-dimensional:

- Embedded System
- Cyber-Physical System
- Real-Time System

Robotic System Properties

Multi-dimensional:

- Embedded System
- Cyber-Physical System
- Real-Time System
- Hybrid System

Robotic System Properties

Multi-dimensional:

- Embedded System
- Cyber-Physical System
- Real-Time System
- Hybrid System
- Adaptive System

Robotic System Properties

Multi-dimensional:

- Embedded System
- Cyber-Physical System
- Real-Time System
- Hybrid System
- Adaptive System
- Autonomous System

What is an *Integrated* Formal Method

Integrated Formal Methods (iFM)

- Integrating multiple formal methods
  - *Loose*: cooperating formalisms
  - *Tight*: single formalism
- Integration of formal and non-formal methods
  - e.g. Graphical notation

Our Position

Necessity meets Opportunity

Our Position

Necessity meets Opportunity

- Based on our previous survey work…
  - Available: `https://arxiv.org/abs/1807.00048`
- Robotics:
  - Present particular challenges
  - Require integration of diverse formal methods
- Formal Methods Benefits:
  - Real-World catalyst for integration research

Outline

Next...

- Highlight four robotics challenges
  - Environment
  - Certification
  - Multi-Robot Systems
  - Reconfiguration
- Discuss integrated formal approaches
  - Current
  - Direction

Challenge One:
Modelling the Physical Environment

Modelling the Physical Environment

Challenge:

- How to specify and verify the behaviour of the robot working in a dynamic and often unknown environment

Modelling the Physical Environment

Current Approaches:

- Ignore the environment![a]
- Assume that the environment it is static and known, prior to deployment[b]
- Use predicates representing sensor data to abstract away from the environment[c]

[a] Savas Konur, Clare Dixon, and Michael Fisher. "Analysing Robot Swarm Behaviour via Probabilistic Model Checking". In: *Robotics and Autonomous Systems* 60.2 (2012), pp. 199–213.

[b] Salar Moarref and Hadas Kress-Gazit. "Decentralized control of robotic swarms from high-level temporal logic specifications". In: *Int. Symp. Multi-Robot Multi-Agent Syst.* IEEE, 2017.

[c] Michael Fisher, Louise A Dennis, and Matt Webster. "Verifying Autonomous Systems". In: *Commun. ACM* 56.9 (2013), pp. 84–93.

Modelling the Physical Environment

Formal Methods must bridge the *reality gap*:

- Model the environment using
  - e.g. Probabilistic Temporal Logic (PTL)[a]

- Monitor the environment
  - e.g. Timed Automata[b]

[a] M. Webster et al. "Toward Reliable Autonomous Robotic Assistants Through Formal Verification: A Case Study". In: *IEEE Transactions on Human-Machine Systems* 46.2 (2016), pp. 186–196.

[b] Adina Aniculaesei et al. "Towards the Verification of Safety-critical Autonomous Systems in Dynamic Environments". In: *Electron. Proc. Theor. Comput. Sci.* 232 (2016), pp. 79–90.

Challenge Two: Trust and Certification Evidence

Trust and Certification Evidence

Operating Context

1. Saftey-Critical e.g. nuclear/aerospace

2. Require public trust

Trust and Certification Evidence

Challenges:

- Formal verification must provide appropriate evidence for
  - Public Trust
  - Regulator Certification
- Which formal methods are suitable?
  - What evidence is needed?
  - What type of robotic system?

Trust and Certification Evidence

Current Approaches:

- Automatic generation of safety case
  - e.g. AUTOCERT for a pilotless aircraft[a]
- Formalising and verifying domain specific rules
  - e.g. Isabelle/HOL to formalise rules for vehicle overtaking[b]

[a] Ewen Denney and Ganesh Pai. "Automating the assembly of aviation safety cases". In: *IEEE Transactions on Reliability* 63.4 (2014), pp. 830–849.

[b] Albert Rizaldi et al. "Formalising and monitoring traffic rules for autonomous vehicles in Isabelle/HOL". In: *Integr. Form. Methods*. Vol. 10510. LNCS. 2017, pp. 50–66.

Challenge Three:
Multi-Robot Systems

Multi-Robot Systems

Types of Multi-Robot Systems

- Homogeneous robots: *Swarms*
- Heterogeneous robots: *Teams*

Multi-Robot Systems

Types of Multi-Robot Systems

- Homogeneous robots: *Swarms*
- Heterogeneous robots: *Teams*

Multi-Robot Systems

Types of Multi-Robot Systems

- Homogeneous robots: *Swarms*
- Heterogeneous robots: *Teams*

Multi-Robot Systems: Swarms

Challenges:

- Linking formal specifications
  - macroscopic (whole swarm) level
  - microscopic (individual robots) level
- State explosion when model-checking large swarms.

Multi-Robot Systems: Swarms

Current Approaches:

- Temporal logics
  - Specify and verify swarms at different levels of abstraction[a]
- Abstractions the mitigate state explosion[b]
  - Symmetry reduction
  - Counting abstraction

[a] Alan F.T. Winfield et al. "On formal specification of emergent behaviours in swarm robotic systems". In: *Int. J. Adv. Robot. Syst.* 2.4 (2005), pp. 363–370.

[b] Savas Konur, Clare Dixon, and Michael Fisher. "Analysing Robot Swarm Behaviour via Probabilistic Model Checking". In: *Robotics and Autonomous Systems* 60.2 (2012), pp. 199–213.

Multi-Robot Systems: Teams

Challenge:

- Linking specification
  - macroscopic (whole team) level
  - microscopic (individual robots) level
- Heterogeneity…

Challenge Four: Adaptation, Reconfigurability, and Autonomy

Adaptation, Reconfigurability and Autonomy

Challenge

- Specifying self-adaptive systems
  - Respond to changes in the environment
- Specifying reconfigurable systems
  - *Decide* on how best to reconfigure themselves
- Specifying reconfigurability
  - *Autonomous* decision-making

Adaptation, Reconfigurability and Autonomy

Current Approaches:

- Model-checking at runtime for self-adaptive systems[a]
- Agent-based systems to model autonomy
  - Verified using temporal logics and model-checkers
  - e.g. probabilistic model-checking of autonomous mine detector robot[b]

[a] Betty H.C. Cheng et al. "Using models at runtime to address assurance for self-adaptive systems". In: *Models@run.time*. Vol. 8378. LNCS. 2014, pp. 101–136.

[b] Paolo Izzo, Hongyang Qu, and Sandor M. Veres. "A stochastically verifiable autonomous control architecture with reasoning". In: *Conf. Decis. Control* (2016), pp. 4985–4991.

Integrated Formal Approaches to Robotic Challenges

Why iFM?

Robotic Challenges…

1. Environment

iFM Can…

Why iFM?

Robotic Challenges...

1. Environment

iFM Can...

1. Combine static and dynamic models

Why iFM?

Robotic Challenges…

1. Environment
2. Certification Evidence

iFM Can…

1. Combine static and dynamic models

Why iFM?

Robotic Challenges...

1. Environment
2. Certification Evidence

iFM Can...

1. Combine static and dynamic models
2. Provide robust evidence

Why iFM?

Robotic Challenges…

1. Environment
2. Certification Evidence
3. Multi-Robot Systems

iFM Can…

1. Combine static and dynamic models
2. Provide robust evidence

Why iFM?

Robotic Challenges…

1. Environment
2. Certification Evidence
3. Multi-Robot Systems

iFM Can…

1. Combine static and dynamic models
2. Provide robust evidence
3. Link macro- and micro- behaviour

Why iFM?

Robotic Challenges…

1. Environment
2. Certification Evidence
3. Multi-Robot Systems
4. Reconfigurable/Autonomous Systems

iFM Can…

1. Combine static and dynamic models
2. Provide robust evidence
3. Link macro- and micro- behaviour

Why iFM?

Robotic Challenges...

1. Environment
2. Certification Evidence
3. Multi-Robot Systems
4. Reconfigurable/Autonomous Systems

iFM Can...

1. Combine static and dynamic models
2. Provide robust evidence
3. Link macro- and micro- behaviour
4. Describe complex configuration and autonomy

Current Integrated Formal Approaches to Robotic Challenges

Adoption

- Event-B and PRISM
  - Reconfigurable architecture for an on-board satellite system
- CSP $\|$ B
  - Vehicle platooning
- AJPF, UPPAAL, and Spatial Calculus
  - Platoon joining and leaving procedures for a driverless car
- FSP and πADL for safety
  - Multi-agent systems
- RoboChart
  - State Charts with CSP underneath

Future Integrated Formal Approaches to Robotic Challenges

Complementary methods

- Benefits of two formal methods
  - e.g. model-checking and proof-based methods
- Benefits of formal method and existing non-formal method
  - Robust (auto-generated?) evidence for certification

Future Integrated Formal Approaches to Robotic Challenges

Heterogeneous Models

- Aimed at ROS, Swarms, Teams, etc
- Link abstract specifications of nodes…
- …with the specification of the node
- Convert between verification tools
- Challenges:

Future Integrated Formal Approaches to Robotic Challenges

Heterogeneous Models

- Aimed at ROS, Swarms, Teams, etc
- Link abstract specifications of nodes…
- …with the specification of the node (which may be heterogeneous)
- Convert between verification tools
- Challenges:
  - Different Levels of Abstraction

Future Integrated Formal Approaches to Robotic Challenges

Heterogeneous Models

- Aimed at ROS, Swarms, Teams, etc
- Link abstract specifications of nodes…
- …with the specification of the node
- Convert between verification tools
- Challenges:
  - Different Levels of Abstraction
  - Different formalisms?

Future Integrated Formal Approaches to Robotic Challenges

Heterogeneous Models

- Aimed at ROS, Swarms, Teams, etc
- Link abstract specifications of nodes…
- …with the specification of the node
- Convert between verification tools
- Challenges:
  - Different Levels of Abstraction
  - Different formalisms?
  - Different properties?

Future Integrated Formal Approaches to Robotic Challenges

Heterogeneous Models

- Aimed at ROS, Swarms, Teams, etc
- Link abstract specifications of nodes…
- …with the specification of the node
- Convert between verification tools
- Challenges:
  - Different Levels of Abstraction
  - Different formalisms?
  - Different properties?
  - Consistency of properties and information?

Necessity meets Opportunity

Necessity meets Opportunity

Who benefits?

Necessity meets Opportunity

Who benefits?

Robotics: integration of formal methods into the development process and potential solutions to the four challenges identified earlier.

Necessity meets Opportunity

Who benefits?

Robotics: integration of formal methods into the development process and potential solutions to the four challenges identified earlier.

iFM: a set of real-world targets that will help to advance the field in new and exciting directions.

More Information

Motivating Survey:

Luckcuck, M., Farrell, M., Dennis, L., Dixon, C., & Fisher, M. (2018). *Formal Specification and Verification of Autonomous Robotic Systems: A Survey*. arXiv preprint arXiv:1807.00048.

Robotics and Artificial Intelligence in Hazardous Environments:

- RAIN: `https://rainhub.org.uk/`
- ORCA: `https://orcahub.org/`
- FAIR-SPACE: `https://www.fairspacehub.org/`

RAIN
ROBOTICS AND AI IN NUCLEAR

ORCA HUB
Offshore Robotics for Certification of Assets
Remote Safety and Integrity

FAIR-SPACE

Questions?