

Accepted Manuscript

Learning middleware models for verification of distributed control programs

Ali Khalili, Massimo Narizzano, Lorenzo Natale, Armando Tacchella

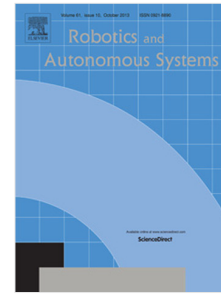
PII: S0921-8890(16)30038-0
DOI: <http://dx.doi.org/10.1016/j.robot.2017.01.016>
Reference: ROBOT 2793

To appear in: *Robotics and Autonomous Systems*

Received date : 22 January 2016
Revised date : 9 November 2016
Accepted date : 19 January 2017

Please cite this article as: A. Khalili, et al., Learning middleware models for verification of distributed control programs, *Robotics and Autonomous Systems* (2017), <http://dx.doi.org/10.1016/j.robot.2017.01.016>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Learning Middleware Models for Verification of Distributed Control Programs

Ali, Khalili¹, Massimo, Narizzano¹, Lorenzo Natale², Armando, Tacchella¹

Abstract

A substantial effort is underway to make robots useful outside controlled environments and without direct human supervision. In practice, this can happen only after a rigorous certification process which ensures that several requirements, e.g., operation safety, are met. Automated verification of control programs can be part of cost-effective methodologies to support certification, but it is widely recognized as difficult to attain in robotics, because of several traits that characterize robot design and implementation. One such trait is the widespread usage of middleware to implement control programs in a distributed fashion. In these cases, the challenge of verification is made steep mainly by the fact that the correctness of control software depends on middleware components whose structured models might not be available, or too difficult to obtain from their documentation.

Our proposal is to ease the application of automated verification techniques by identifying abstract middleware models in the form of finite-state automata. The identification procedure is itself largely automated, and the only prerequisite is for the middleware to be available for controlled experimentation. Once middleware models are computed, behaviors that would lead to unsafe operation can be spotted automatically on a composition of identified middleware and control software models using model checking techniques. The approach is based on our tool AIDE — Automata IDentification Engine — to identify abstract middleware models, and the model checker SPIN to verify control units. To validate our approach, we consider four different case studies built on YARP publish-subscribe middleware. Our results confirm that AIDE enables the extension of precise engineering methods to distributed control software in robotics.

Keywords: Distributed Control Software, Software Testing and Verification, Automata-based Inference, Model Checking

Email addresses: khalili.ir@gmail.com (Ali, Khalili), massimo.narizzano@unige.it (Massimo, Narizzano), lorenzo.natale@iit.com (Lorenzo Natale), armando.tacchella@unige.it (Armando, Tacchella)

¹DIBRIS, Università degli Studi di Genova, Via Opera Pia 13 16145, Genoa, Italy

²iCub Facility, Istituto Italiano di Tecnologia, Via Morego 30 16163, Genoa, Italy

Download English Version:

<https://daneshyari.com/en/article/4948722>

Download Persian Version:

<https://daneshyari.com/article/4948722>

[Daneshyari.com](https://daneshyari.com)