Science of Computer Programming ••• (••••) •••–•••

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

Formal reasoning about resilient goal-oriented multi-agent systems

L. Laibinis [a,*], I. Pereverzeva [b], E. Troubitsyna [b]

[a] Vilnius University, Dep. of Computer Science, Didlaukio 47, 08303 Vilnius, Lithuania
[b] Åbo Akademi University, Information Technologies, Vesilinnantie 3, 20520 Turku, Finland

ARTICLE INFO

Article history:
Received 26 May 2016
Received in revised form 26 May 2017
Accepted 30 May 2017
Available online xxxx

Keywords:
Formal reasoning
Multi-agent systems
Goal-oriented development
System resilience
Event-B

ABSTRACT

In this paper we present our formalisation of a resilient goal-oriented multi-agent system and its essential properties. The formalisation covers the notions of system goals and agents, various formal structures (functions and relations) defining different interrelationships between these notions, as well as constraints on the system dynamics allowing a multi-agent system to become more reconfigurable and thus resilient in order to achieve the system goals. The formalisation results in establishing connections between goals at different levels of abstraction, system architecture and agent responsibilities. The proposed formal systematisation of the involved concepts can be seen as generic guidelines for formal development of reconfigurable systems. Moreover, we demonstrate how such guidelines can be interpreted within the Event-B framework.

1. Introduction

Resilience is an ability of a system to remain trustworthy despite changes [17]. It is an evolution of dependability concept that puts an emphasis on the ability of a system to adapt to different operating conditions. In this paper, we view adaptability as an ability of a system to reconfigure and continue to function in the presence of faults and other changes. Our aim is to propose a comprehensive theoretical study of relevant aspects of the system architecture and its dynamic behaviour to facilitate formal development of reconfigurable distributed systems.

We consider distributed systems that are composed of asynchronously communicating heterogeneous components. The components interact with each other to execute functions required from the system. Moreover, to facilitate system resilience, the system components cooperatively perform fault tolerance activities as well as exchange information about their current status. The cooperative nature of the component behaviour makes it convenient to consider them as collaborating agents and the overall distributed system as a multi-agent system correspondingly.

Often research on multi-agent systems [39,48] focuses on studying the emerging behaviour, i.e., it adopts a bottom-up approach that investigates whether agent interactions give rise to the desired behaviour or properties. In our work, we take an opposite approach: we aim at deriving the architectural and behavioural constraints to guarantee system resilience, i.e., ensure that the system, besides correct execution of its functions in the nominal conditions, can also reconfigure and remain operational in the presence of faults and other changes.

* Corresponding author.
E-mail addresses: linas.laibinis@mif.vu.lt (L. Laibinis), inna.pereverzeva@abo.fi (I. Pereverzeva), elena.troubitsyna@abo.fi (E. Troubitsyna).

http://dx.doi.org/10.1016/j.scico.2017.05.008
0167-6423/

We rely on the goal-oriented paradigm because it provides us with a suitable conceptual basis for our reasoning. Goals are functional and non-functional[1] objectives that the system should achieve [44,46]. High-level goals representing the overall system objectives can be decomposed into sub-goals. Decomposition facilitates unfolding of the layered system architecture and reasoning about system properties at different levels of abstraction. It also allows us to eventually derive constraints on the agent behaviour and ensure that their collaboration guarantees achieving the desired goals. The goal-oriented framework also provides us with an especially suitable basis for reasoning about reconfigurability. In particular, it allows us to define reconfigurability as an ability of agents to redistribute their responsibilities to ensure goal reachability.

Reasoning about reconfigurability within the goal-oriented multi-agent framework spans over a large set of inter-twined concepts addressing both system architecture and its dynamic behaviour. Therefore, there is a clear need for a formal systematic study of these complex interdependencies. This is the task that we tackle in this paper. Namely, we propose a systematic set-theoretic formalisation of the reconfigurability concept for multi-agent goal-oriented framework. The formalisation results in establishing connections between goals at different levels of abstraction, system architecture and agent responsibilities. The proposed formal systematisation of these concepts can be also seen as generic guidelines for formal development of reconfigurable systems. In this paper, we demonstrate how such guidelines can be interpreted within the Event-B framework [2].

The paper is structured as follows. Section 2 overviews the kind of systems and their properties we are interested in studying and briefly describes an illustrative example of such systems – a multi-robotic cleaning system. In Section 3 we gradually present our formalisation of a resilient goal-oriented multi-agent system and its reconfiguration mechanisms. Section 4 discusses how the formalised notions can be represented in a concrete formal framework – Event-B. Finally, we overview the related work and give some concluding remarks in Section 5.

2. Resilient goal-oriented multi-agent systems

Resilience is an ability of a system to remain trustworthy despite changes [17]. To react on such changes, the system needs to reconfigure. The reconfiguration might be reactive or proactive. In the former case, reconfiguration is usually triggered by a component failure and the system should reconfigure to achieve fault tolerance, i.e., perform error recovery. In the latter case, the system might attempt to execute some of its services more efficiently, e.g., by deploying the available idle components. In both cases, the system components should collaborate to ensure system resilience.

In this paper, we study reconfigurability as an essential mechanism of achieving resilience of distributed systems. Since the collaborative aspect of the component behaviour is important for our study, we represent system components as agents and the overall system as a multi-agent system correspondingly.

Agents are autonomous software components that asynchronously communicate with each other. Each agent has a certain functionality that it provides. In this paper, we consider heterogeneous multi-agent systems, i.e., agents may have different functionalities. Moreover, some agents might play a role of supervisors of another agent or a group of agents. As a result of reconfiguration, an agent might receive additional responsibilities, i.e., it could become involved into an execution of tasks that were not assigned to it initially. We assume that agents are co-operative, i.e., they always accept new responsibilities. At the same time, the agents are unreliable, i.e., they might fail and cease performing their functions. This might trigger system reconfiguration. As a result, the responsibilities of the failed agents can be re-allocated to the healthy ones. If an agent is healthy and idle, it can be deployed to perform the functions of failed agents or it might also become engaged in an execution of some other task, e.g., to improve the system performance and/or increase the likelihood of successful task completion.

While developing a multi-agent system (MAS) [39,48], we should establish a link between the system requirements and agent behaviour. It is widely recognised that the goal-oriented development framework facilitates achieving this. The key concept of the framework is the notion of a goal – a functional or non-functional objective that a system should satisfy. Goals also constitute a convenient mechanism for structuring requirements via goal decomposition [44]. In the decomposition process, the high-level system goals are iteratively decomposed into subgoals. Moreover, the low-level subgoals can be directly linked with the behaviour of agents, i.e., they can be used to derive requirements and constraints on the agent behaviour.

The goal-oriented framework [44,46] provides us with a suitable basis for reasoning about reconfigurable multi-agent systems. It enables reasoning about the system behaviour at different levels of abstraction. At the same time, goal-decomposition process facilitates incremental unfolding of the system architecture. It also helps us to build a hierarchy of agents according to their responsibilities in achieving certain kind of goals. Moreover, the goal-oriented framework allows us to formulate reconfigurability as an ability of agents to redistribute their responsibilities to ensure goal reachability.

To summarise, in the rest of the paper we aim at studying the systems that have the following characteristics:

- There is a number of main (global) goals defined for the system. The goals can be decomposed into a subset of corresponding subgoals;
- The system consists of a number of agents – autonomic software components;

[1] The non-functional aspect is not considered in the paper.

Please cite this article in press as: L. Laibinis et al., Formal reasoning about resilient goal-oriented multi-agent systems, Sci. Comput. Program. (2017), http://dx.doi.org/10.1016/j.scico.2017.05.008