Simulation Modelling Practice and Theory 51 (2015) 45–68

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Model checking temporal knowledge and commitments in multi-agent systems using reduction

Faisal Al-Saqqar, Jamal Bentahar *, Khalid Sultan, Wei Wan, Ehsan Khosrowshahi Asl

Faculty of Engineering and Computer Science, Concordia University, Montreal, Canada

ARTICLE INFO

Article history:
Received 3 January 2014
Received in revised form 27 October 2014
Accepted 5 November 2014
Available online 29 November 2014

Keywords:
Multi-agent systems
Model checking
Knowledge
Social commitments
Verification

ABSTRACT

Though modeling and verifying Multi-Agent Systems (MASs) have long been under study, there are still challenges when many different aspects need to be considered simultaneously. In fact, various frameworks have been carried out for modeling and verifying MASs with respect to knowledge and social commitments independently. However, considering them under the same framework still needs further investigation, particularly from the verification perspective. In this article, we present a new technique for model checking the logic of knowledge and commitments (CTLKC$^+$). The proposed technique is fully-automatic and reduction-based in which we transform the problem of model checking CTLKC$^+$ into the problem of model checking an existing logic of action called ARCTL. Concretely, we construct a set of transformation rules to formally reduce the CTLKC$^+$ model into an ARCTL model and CTLKC$^+$ formulae into ARCTL formulae to get benefit from the extended version of NuSMV symbolic model checker of ARCTL. Compared to a recent approach that reduces the problem of model checking CTLKC$^+$ to another logic of action called GCTL*, our technique has better scalability and efficiency. We also analyze the complexity of the proposed model checking technique. The results of this analysis reveal that the complexity of our reduction-based procedure is PSPACE-complete for local concurrent programs with respect to the size of these programs and the length of the formula being checked. From the time perspective, we prove that the complexity of the proposed approach is P-complete with regard to the size of the model and length of the formula, which makes it efficient. Finally, we implement our model checking approach on top of extended NuSMV and report verification results for the verification of the NetBill protocol, taken from business domain, against some desirable properties. The obtained results show the effectiveness of our model checking approach when the system scales up.

1. Introduction

Multi-Agent Systems (MASs) have noticed an increase in their use in numerous real world applications since their emergence. They have been extensively and successfully used in a variety of industrial, commercial, governmental, military, and entertainment applications [52,72,42]. Such systems have long been under focus by researchers to develop systematic techniques to model them and ensure their compliance against their specifications. In fact, various approaches have been carried

---

* Corresponding author.

E-mail addresses: f_alsaqq@encs.concordia.ca (F. Al-Saqqar), bentahar@ciise.concordia.ca (J. Bentahar), k_sultan@encs.concordia.ca (K. Sultan), w_wan@encs.concordia.ca (W. Wan), e_khosr@encs.concordia.ca (E. Khosrowshahi Asl).

http://dx.doi.org/10.1016/j.simpat.2014.11.003

out to model and represent MASs. Kripke structures [44] and interpreted systems [35] are the most prominent frameworks for this purpose. These underlying models are used to traditionally interpret some logics that are used to specify and reason about desirable properties of MASs.

Technically speaking, when designing systems that are complex in nature, different aspects might need to interact and hence be modeled simultaneously [55]. However, modeling MASs when there are many different dimensions to look at simultaneously is a challenge which makes the verification of these systems a difficult task [7,43].

In this article, we exploit model checking paradigm to formally model and automatically verify MASs with respect to certain properties related to agents knowledge and their commitments in the system. Despite the fact that agents' knowledge and commitments (to do something) influence and interact with each other, they have been, till recently, addressed independently (see for example [6,33,47,70,76]). In concrete applications such as business settings, agents sometimes have to reason about their knowledge and negotiate, create, and reason about their social commitments at the same time, particularly when they are engaged in conversations. To motivate our study of modeling and incorporating knowledge and commitments in a single framework, we use situational examples that arise in practical settings of web-based applications.

Example 1. Consider the fish-market protocol [59] in which different agents (one seller and one or more buyers) are involved in interactions to reach agreement about the price of the offered fish. The protocol starts when the fisherman delivers the fish to the fish market. After that, the seller announces the prices of the available buckets of fish. Hereafter, the buyer(s) either accept the price by uttering *Yes* or reject the price by uttering *No*. No response from the buyer(s) is considered as a rejection also. Consequently, if only one buyer accepts the price, then the seller will sell him, however, if no one accepts, then the seller lowers the price. On the other hand, if more than one buyer accept the price, the seller will raise the price and so on. In such scenarios, when the buyer accepts the price (i.e., commits to pay), the seller should know that. Otherwise, the seller will lower the price even though there is an acceptance. Moreover, the buyer should know that he accepted the price, which means he has the capability to pay in order to fulfill his commitment.

Example 2. Let us take the case of buying a book online from a certain publisher as a second example. Suppose that we asked a member from our team to buy a book for us last month. He made the online order and committed to pay. The credit card debit succeeded, meaning that the agent (our team member) knows that he fulfilled his commitment to pay. The publisher company committed to send the requested book to our address. Unfortunately, the book has never arrived. The publisher claimed they had send it out, but the shipping company they dealt with could not find it in their records. As a result, we asked them to send it again. However, knowing that the book is delivered (i.e., fulfilling the commitment of delivering the book) will help avoiding such situations.

Hence, the need for tools with the ability to express the interactions between knowledge and commitments is indeed confirmed. Unlike the logic presented in [31] whose expressive power is limited to merely representing and reasoning about social commitments in MASs, recently, we have studied the interactions between knowledge and social commitments in MASs from formal semantics and verification perspectives [1]. Concretely, we introduced in [1] the CTLKC$^+$ logic, an extension of CTL [3,21] with modalities for knowledge and commitments. This logic has the ability to express and reason not only about knowledge and social commitments independently, but also about formulae combining the two modalities. The main focus of [1] is the soundness and consistency of the interactions between these two modalities and the logic as a whole. Moreover, we developed, in the same paper, a new version of interpreted systems, originally introduced in [35], as the formal model of CTLKC$^+$ over which formulae can be interpreted. This extension allows us to model agents as well as their interactions. The developed approach proposes a new definition of the social accessibility relation needed for commitments, which was introduced in [9,31] in such a way that it does not include the epistemic accessibility for knowledge in any way, yet keeping the intuition of having communication channels between interacting components. This new definition makes the logic consistent when it comes to express relationships between knowledge and commitments.

From the verification perspective, we have presented in [1] a preliminary analysis of the logic from model checking perspective. We have used a direct and intuitive reduction technique of the model checking problem of CTLKC$^+$ logic into the problem of model checking an action logic called GCTL* [14] that extends branching temporal logic. The technique is direct in the sense that GCTL* models include general action transitions that are directly mapped to the accessibility relations. We have used the automata-based model checker CWB-NC as the verification tool. However, this verification procedure has a major limit as it cannot be scaled up, which is a highly considerable problem in model checking real applications of multi-agent systems. In fact, the experiments reported in [1] are limited to only 2 agents and the state explosion problem is very quickly achieved. This is mainly due to the explicit representation of the model and properties as automata, so that the Cartesian product of the two automata, which is needed in the automata-based model checking algorithms, increases exponentially. In this article, our main objective is to overcome this scalability problem and provide space and time efficient model checking technique for CTLKC$^+$ using symbolic approaches.

Moreover, technically speaking, the reduction procedure we advocate in this paper is different from the one presented in [1]. As target logic, we use in this paper ARCTL [56], that extends the branching time logic CTL with actions. Unlike GCTL* that accommodates different action formulae, ARCTL has a restricted path formulae where only paths satisfying a particular action are considered. A reduction of a logic to ARCTL requires restrictions of the model being transformed (technical details are given in Section 4.1).