Modeling and verifying probabilistic Multi-Agent Systems using knowledge and social commitments

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

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

Abstract

Multi-Agent Systems (MASs) have long been modeled through knowledge and social commitments independently. In this paper, we present a new method that merges the two concepts to model and verify MASs in the presence of uncertainty. To express knowledge and social commitments simultaneously in uncertain settings, we define a new multi-modal logic called Probabilistic Computation Tree Logic of Knowledge and Commitments (PCTL\textsubscript{kc}) in short which combines two existing probabilistic logics namely, probabilistic logic of knowledge PCTLK and probabilistic logic of commitments PCTLC. To model stochastic MASs, we present a new version of interpreted systems that captures the probabilistic behavior and accounts for the communication between interacting components. Then, we introduce a new probabilistic model checking procedure to check the compliance of target systems against some desirable properties written in PCTL\textsubscript{kc} and report the obtained verification results. Our proposed model checking technique is reduction-based and consists in transforming the problem of model checking PCTL\textsubscript{kc} into the problem of model checking a well established logic, namely PCTL. So doing provides us with the privilege of re-using the PRISM model checker to implement the proposed model checking approach. Finally, we demonstrate the effectiveness of our approach by presenting a real case study. This framework can be considered as a step forward towards closing the gap of capturing interactions between knowledge and social commitments in stochastic agent-based systems.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

The rapid increase of using software agents and Multi-Agent Systems (MASs) nowadays has led to the increasing demand of finding principled techniques for modeling and verifying such systems. Generally, to build effective open MASs, several aspects which have direct influence on the efficiency and effectiveness of the entire system must be taken into account (Konur, Fisher, & Schewe, 2013). Among other aspects, knowledge and social commitments are of great interest in MASs. Recently, Al-Saqqar et al., have demonstrated that these two concepts are closely interacting with each other in various real life scenarios (Al-Saqqar, Bentahar, Sultan, & El Menshawy, 2014). Social commitments have been a vital approach in agent societies to capture the communication between interacting agents for more than a decade. Social commitments are modeled as public information conveyed by one agent, namely debtor, to another agent, creditor, in which the debtor engages towards the creditor to bring about a certain property (Singh & Huhns, 2005). A commitment between two agents is not just a static entity, but rather a dynamic one whose state changes over time (Gnay & Yolum, 2013). This dynamicity feature supports commitments' flexibility and can be captured through the manipulation of commitments via some operations such as, creation, discharge, cancellation, release, assignment, and delegation (Singh, 2000). On the other hand, reasoning about knowledge has been addressed in distributed systems since 1960s (Wan, Bentahar, & Hamza, 2013).

However, though various approaches have been carried out in the literature to model and represent stochastic MASs, none of the existing approaches addresses the concepts of knowledge and social commitments simultaneously. In fact, the problem of reasoning about and verifying the interaction between knowledge and social commitments in the presence of uncertainty has not been investigated yet. Interpreted systems formalism (Fagin, Halpern, Moses, & Vardi, 1995) and Partially Observable Markov Decision Processes POMDPs (a variant of MDP) are the most prominent traditions in the area of modeling and representing stochastic MASs. These models are used to traditionally interpret some logics defined to specify and reason about given properties of MASs. On
the one hand, interpreted systems formalism provides a natural and yet efficient way for modeling MASs at different levels of abstractions (i.e., local and global). It has been extended in Halpern (2003) and further in Wan, Bentahar, and Hamza (2012, 2013) to capture the probabilistic behavior of epistemic MASs. Recently, it has been extended in Bentahar, El-Menshawy, Qu, and Dssouli (2012) and El-Menshawy, Bentahar, El Kholy, and Dssouli (2013a) to account for the communications that occur between interacting parties in conventional MASs. The distinct point of the extended versions of this formalism is that knowledge and commitments can be captured thought the use of what is called accessibility relations. The accessibility relation for knowledge denotes the existence of equivalent states for a given agent. That is, states where the agent cannot distinguish between being in which one of them. For commitments, accessibility relations capture the existence of communication channel between the communicating agents and the transferring of information from the sender to the receiver. On the other hand, POMDPs have been widely used to model the uncertainty of knowledge and behavior for stochastic agents (Huang, Luo, & van der Meyden, 2011). Recently, some researchers invested POMDPs to model multi-agent influences (Witwicki, Chen, Durfee, & Singh, 2012). An important point of POMDPs is that there is no distinction drawn between actions taken to change the state of the world and actions taken to gain information (Kaelbling, Littman, & Cassandra, 1996). This is important because, in general, every action has both types of effect. However, solving these models comes at a very high computational cost (Melo, Spaan, & Wittwicki, 2011).

In this paper, we aim to examine the use of interpreted systems formalism to capture not only knowledge and commitments independently, but also the interactions (combinations) of the two aspects in stochastic systems. We also intent to verify these interactions by means of model checking. Model checking is an automatic formal verification technique for finite state concurrent systems (Baier & Katoen, 2008). In addition to qualitative model checking, quantitative verification techniques using probabilistic model checkers have recently gained popularity. Probabilistic model checking offers the capability for interpreting the satisfiability of a given property on stochastic systems in terms of quantitative means (Ouchani, Mohamed, & Debbabi, 2014).

1.1. Motivations

Although a plenty of work has been carried out to address each of knowledge and commitments in MASs independently (see for example (Baldoni, Baroglio, & Marengo, 2010; Bentahar et al., 2012; Delgado & Benevides, 2009; El-Menshawy et al., 2013a; Giordano, Martelli, & Schwind, 2007; Halpern, 2003; Huang et al., 2011; Lomuscio, Pecheur, & Raimondi, 2007; Pham & Harland, 2007; Wan et al., 2013)), in so many real world settings, these two concepts need to interact with each other in order to ensure rich modeling at local (agent) and global (MAS) levels. To model and verify such interactions between knowledge and social commitments, the only existing approach (Al-Saqkar et al., 2014) ignores the probabilistic features of MASs, and instead assumes an absolute degree of correctness so that systems behave in a typical manner. However, it is challenging to guarantee the correctness of the system's behavior due to the complex nature of the autonomous and heterogenous agents, especially when they have probabilistic characteristics (Marey, Bentahar, Dssouli, & Mbarki, 2014; Song et al., 2012). Consequently, the problem of capturing different aspects simultaneously is made more complicated by the presence of uncertainty which makes agents uncertain about the effects of their actions on their peers and not fully aware of the situations other agents are encountering.

The motivation for the incorporation of knowledge and commitments in a probabilistic logic is provided by the fact that these two concepts not only have an impact on each other, but also their interaction is crucial in various real scenarios. For instance, in the field of mobile applications, which are complex in nature, there exist situations when accounting for the interaction between knowledge and commitments improves the output of such applications. Let us consider a simple scenario where receiver and sender agents share an agreement, in which the receiver agrees to pay the sender in return of the delivery of a service he has requested. This can be represented as a commitment, in which the receiver will be committed to the sender to pay once the service is made available for him. Now, if everything goes well and the receiver successfully makes his payment, the sender has to know that the payment is made so that he does not ask the receiver to pay again. Moreover, the receiver (who made the payment) has to know that he has fulfilled his commitment to avoid making multiple payments, and so on. However, those interactions are stochastic. For instance, the commitment to pay is not going to be surely satisfied. To effectively specify such properties in the face of uncertainty, the need for a logical tool that can express probabilistic knowledge and commitments simultaneously is indeed confirmed. Rather than building a logic from scratch to address the underlying aspects, we combine logics dealing with these two individual units in a single logic. We advocate the approach of combining existing logics because it ensures the preservation of important properties of the logics being combined (Konur et al., 2013). In particular, we use the independent join (or fusion) technique (Franceschet, Montanari, & de Rijke, 2004). The problem of combining logics based on the independent join technique is as follows. Given two logics $A$ and $B$, how do we combine them into one logic $A \otimes B$ which extends the expressive power of each one?. In our case, suppose $A$ addresses probabilistic epistemic properties of agents and $B$ addresses the social aspects (i.e., probabilistic commitments and their fulfilments) between interacting agents. Their combination should be able to not only express epistemic and social properties, but also express the interaction between the two concepts (i.e., express them in a single formula). Once the combined logic is defined, we use the PRISM probabilistic model checker (Kwiatkowska, Norman, & Parker, 2002) as the formal verification tool to verify it after its reduction to PCTL, the probabilistic logic of branching time (Hansson & Jonsson, 1994). Our choice of PRISM is motivated by its popularity to check probabilistic specifications over probabilistic models. Systems’ specifications can be expressed either in the Probabilistic Computation Tree Logic (PCTL) or in a continuous stochastic logic (CSL) (Baier & Katoen, 2008). System models can be described using the PRISM language as Discrete-Time Markov Chains (DTMCs), Continuous-Time Markov Chains (CTMCs), Markov Decision Processes (MDPs), or Probabilistic Timed Automata (PTA) (Forejt, Kwiatkowska, Norman, & Parker, 2011).

1.2. Contributions

The contributions of this paper are threefold. First, we present a new probabilistic version of interpreted systems to model MASs using the dimensions of knowledge and social commitments. The developed version merges two extended versions of the original formalism of interpreted systems introduced by Fagin and his colleagues (Fagin et al., 1995). Those versions are introduced respectively by (1) Halpern (2003) and extended later by Wan et al. (2012), Wan et al. (2013) to capture the stochastic behavior of the system; and (2) by Bentahar et al. (2012) and El-Menshawy et al. (2013a) to model the communication between interacting parties. Second, We introduce a new logic called Probabilistic Logic of Knowledge and Commitment (PCTL$^{kc}$) to be able to capture and

$$\frac{A}{C8}$$
reason about the interaction between knowledge and social commitments. The logic we define combines the Probabilistic Computation Tree Logic of Knowledge PCTLK (Wan et al., 2012, 2013) and the Probabilistic Computation Tree Logic of Commitment PCTLC (Sultan, El-Meneshy, & Bentahar, 2013). PCTLK and PCTLC are, in turn, extensions of the Probabilistic Computation Tree Logic PCTL (Hansson & Jonsson, 1994) with an epistemic modality for the knowledge and a social modality for the commitments and their fulfilments respectively. Third, we introduce a new model checking technique to verify the proposed logic (PCTLC). The introduced technique is a reduction-based in which the problem of model checking PCTL is transformed into the problem of model checking an existing logic called PCTL. To achieve this reduction, new rules have been laid down to transform the models of PCTL to MDPs to be suitable for the PRISM model checker. We also devise some other rules to reduce each PCTL formula into PCTL formula. By so doing, we can build on the existing PRISM model checker by automating our translation to verify some given properties written originally in our new logic PCTL.

The work presented in this article represents a new trend in the direction of capturing interactions between various aspects in MASs. It can be seen as a first attempt to combine the notions of probability, knowledge, and commitments in a single tool giving a new expressive power—in terms of expressing the individual aspects as well as their combinations in the presence of uncertainty—and is therefore subject to new intuitions.

The strengths of the proposed work lie in the following points:

1. It combines (for the first time in the literature) probability, knowledge, and social commitments in a single logic system whose expressive power outperforms those of the existing logics in MASs field. In addition to the ability of expressing knowledge and commitments independently, the proposed logic has the capability to express and reason about the interaction between the two concepts.
2. The scalability of the proposed model checking technique, in terms of the number of agents and the model size, is promising (15 agents and about $4 \times 10^{11}$ states).

However, one of the potential weaknesses of the approach is being suitable only for the design time, but not for the runtime because we are only dealing with a model of the system, not the real system itself. The state explosion problem is another issue that the proposed approach could not completely eliminate because even the results demonstrate that the approach is scalable, it still suffers from the fact that the number of states increases exponentially with the number of agents.

**Paper Organization.** The remainder of this paper is organized as follows. Section 2 surveys the current related work. The interpreted systems formalism along with two extended versions of it are presented in Section 3. Section 4 is devoted to introducing our new probabilistic logic of knowledge and commitments as well as introducing a model checking procedure for verifying the proposed logic. Section 5 describes the experimental results of model checking the new logic. Finally, Section 6 concludes this paper and provides hints for possible future work.

## 2. Related work

In this section, we review the state-of-the-art related to probabilistic knowledge, probabilistic commitments, and the interactions between the two aspects in MASs. Then, we compare our framework to the existing ones. This survey is by no means exhaustive or comprehensive but, however, lists the most relevant work to ours.

### 2.1. Probabilistic knowledge in MASs

Delgado and Benevides in Delgado and Benevides (2009) defined a probabilistic logic called K-PCTL which extends PCTL with an epistemic operator for the knowledge. For modeling their target systems, the authors proposed an approach that represents each agent in the system as a DTMC with synchronization actions. In their DTMC model, each state either has a synchronized action with probability 1 or regular probabilistic transitions. Having two different actions in a single DTMC forced them to transform it into an MDP model. From the semantics point of view, K-PCTL formulae are interpreted over MDP models which are augmented with accessibility relations, so that probabilities over paths can be defined. However, the uncertainty of the knowledge cannot be measured as the accessibility relations are not probabilistic. Our approach differs from this one in four main points. First, our logic integrates two modalities on top of PCTL; one for the knowledge, and one for the commitments and their fulfilments. Therefore, our logic has a larger dimension of system’s aspects making it more expressive than K-PCTL. Second, our logic permits the probabilistic operator to precede each of the knowledge modality and the social modality so that we can quantitatively reason about the two aspects which again increases its expressive power. Third, we model the target systems using probabilistic interpreted systems. Forth, we propose a concrete model checking technique in which we transform the problem of model checking our logic to the problem of model checking an existing logic allowing us to re-use the PRISM tool instead of just suggesting to extend it.

In Huang et al. (2011), Huang and his colleagues extended the MCK model checker (Gamunie & Meyden, 2004) with subjective probability relative to agent knowledge using interpreted partially observed discrete-time Markov chain (PO-DTMC). PO-DTMC is based on partial observations with assumption on synchronous with perfect recall. To specify properties of probabilistic interpreted systems, the authors use a logic that combines temporal and knowledge modalities with a probabilistic operator. In their approach, the set of accessible states is defined as states of a special agent, called the environment, while the remaining agents observe the environment and perform actions based on their observations. Then, probabilistic knowledge is expressed by a rational linear combination of every agents’ probabilities in the system: every agent has its own probability for each accessible state, which is supposed to be known. Unlike this work, in our approach we do not assume that accessibility transitions are probabilistic because this information is not always accessible to agents and sometimes hard to quantify. Instead, we compute the probabilistic knowledge based on the number of accessible states as they are equally accessible. Moreover, by re-using the existing PRISM mode checker, we do not add a computational cost that is associated to extending the existing version of it.

Wan et al. (2013) has also addressed the verification of epistemic properties in agent environments against the background of participating parties. They propose PCTLK, a probabilistic, epistemic, branching-time logic which extends CTL with probabilistic and epistemic modalities. To verify the proposed logic, the authors introduced a reduction-based model checking technique to translate the problem of model checking PCTL into the problem of model checking PCTL. Their reduction procedure involves two processes. First, they transform the probabilistic interpreted systems into an MDP which is transformed further to a DTMC. Second, they translate each PCTLK formula into a corresponding PCTL formula. To model check a PCTLK formula, they check its transformed PCTL formula over the DTMC model. They demonstrated the applicability of their proposed verification technique by applying it on a well known case study and implementing it using the PRISM model checker. Our work is similar to this work, except that we have a
social modality in our proposed logic for the commitments and their fulfilments which makes it more expressive than PCTLK.

2.2. Probabilistic commitments in MASs

In Witwicki and Durfee (2007), Witwicki and Durfee presented a commitment-based methodology for approximating the optimal joint policy in agent coordination. They proposed a technique to decompose large mathematical programs that encodes the decision problems of all agents into (1) a search for optimal commitments regarding each agent’s outgoing influences; and (2) a search for optimal local policies that respect the commitments decided upon. For a given set of commitments, they add constraints to the traditional linear program formulation of MDPs to guarantee that a feasible policy respects the commitments. Each agent can then solve its linear program separately.

In another work, Witwicki and Durfee (2009) investigated the use of probabilistic commitments in service orientation. They proposed a commitment-based negotiation mechanism based on uncertain durations by which service providers agree to provide a service within a given time and certain probability. The commitment between service providers and service requesters use temporal and probabilistic parameters to summarize expectations over future agent activities. Agents (providers and requesters) then benefit from these commitments to build policies about how to achieve (for providers) or utilize (for requesters) these anticipated service outcomes. MDPs were adopted as the underlying models for modeling their agent-based systems. While the semantics of the commitments was not formally described (i.e., in term of logic), they have given a definition for the probabilistic commitment as follows. “A probabilistic temporal service commitment \( C_i(s) = (t, \rho) \) is a guarantee that agent \( i \) will perform (for agent \( j \)) the actions necessary to deliver service \( s \) by time \( t \) with probability no less than \( \rho \)” (Witwicki & Durfee, 2009). By making use of these probabilistic commitments, agents can make promises to each other even if they cannot fully guarantee service provision.

The relationship between commitments and probability was also investigated in Sultan et al. (2013) to reason about agent interactions in uncertain settings. In particular, the authors integrated a probabilistic operator into a logic of commitment called CTLKC (Bentahar et al., 2012; El-Menshawy, Bentahar, El Kholy, & Dssouli, 2013b). This allowed them to reason about commitments in stochastic systems. To model the uncertainty of transitions and commitments, they paired the probabilistic interpreted systems (Halpern, 2003; Wan et al., 2013) with social accessibility relations introduced in this paper helps MASs to capture and verify the interaction between knowledge and social commitments in the face of uncertainty. Moreover, the new probabilistic interpreted systems introduced in this paper helps MASs developers have rich modeling power. Original work does not take probabilistic behavior into consideration, so it limits its application to reliable environments, we target stochastic systems where uncertainty plays a vital role. Moreover, our proposal subsumes the one in Al-Saqqar et al. (2014) because probability values range from 0 to 1 (when probability is equal to 1, the system becomes certain). So, our framework outperforms this proposal in the sense that not only qualitative reasoning about the interaction between knowledge and commitments is achievable but also quantitative reasoning becomes possible.

2.4. Comparison and discussion

We compare our framework to the existing proposals by taking into consideration five criteria: Knowledge, Commitments, Uncertainty, Formalization, and Verification. Knowledge property shows whether the approach addresses epistemic properties of the system or not. Commitments property indicates whether it addresses the social commitments or not. Uncertainty reflects target systems whose behavior is probabilistic. Formalization indicates the use of formal logics, or formal methods in general. Finally, Verification confirms the presentation of a formal verification technique to verify the proposed approach. Table 1 shows a summary about the comparison between our framework and the existing approaches based on the criteria described above. We observe that our framework outperforms the related approaches as it satisfies all the listed criteria.

To summarize, the advancement of our work over existing work lies in the expressiveness power of the proposed logic which allows autonomous agents in MASs to capture and verify the interaction between knowledge and social commitments. That is, not only modeling knowledge and social commitments independently in the presence of uncertainty is possible, but also modeling the interaction between them has become possible by making use of our proposed probabilistic model.

3. Probabilistic interpreted systems and PCTL<sub>kc</sub>

In this section, we recall the interpreted systems formalism (Fagin et al., 1995) and two extensions of this formalism (1) to capture the communication between cooperating autonomous components in terms of social commitments introduced in Bentahar et al. (2012); El-Menshawy et al. (2013b); and (2) to reason about the probabilistic agents behavior presented in (Halpern, 2003) and extended further in (Wan et al., 2012). Afterwards, we present the syntax and semantics of our proposed probabilistic logic (PCTL<sub>kc</sub>).
3.1. Interpreted systems

The formalism of interpreted systems is a framework for modeling systems composed of autonomous agents interacting with each other. The original version of the formalism introduced by Fagin and his colleagues (Fagin et al., 1995) provides a useful framework to locally model autonomous and heterogeneous agents who interoperate within a global system via sending and receiving messages. The formalism can be summarized as follows. Suppose a system composed of agents (i.e., $Agt = \{1, \ldots, n\}$). At all times, each agent in the system is assumed to be in some local state, which intuitively records the complete information that the agent can access at that time. Specifically, each agent $i \in Agt$ is characterized by countable sets $L_i$ and $Act_i$ of local states and actions respectively in which the set $Act_i$ is mainly used to account for the temporal evolution of the system. Also, local actions for each $i \in \text{Agt}$ are performed in compliance with a local protocol $\mathcal{P}_i : L_i \rightarrow 2^{\mathcal{A}l}$, which specifies a set of enabled local actions in a given global state. Furthermore, the environment in which agents live may be modeled by means of a special agent $e$. Associated with $e$ are a set of local states $L_e$, a set of actions $Act_e$, and a protocol $\mathcal{P}_e$. A tuple $g = (l_1, l_2, \ldots, l_n) \in (L_1 \times \cdots \times L_n \times L_e)$ where $l_i \in L_i$ for each $i \in \text{Agt}$ and $l_e \in L_e$ is called a “global state” and represents the instantaneous configuration of all agents in the system at a given time.

The local evolution function $\tau_i$ that determines the transitions for an individual agent $i$ between its local states is defined as follows:

$$\tau_i : L_i \times L_i \times Act_i \rightarrow L_i$$

Similarly, the global evolution function of the system is defined as follows:

$$\tau : G \times ACT \times G \rightarrow \{0, 1\}$$

where $ACT = Act_1 \times \cdots \times Act_n$ and each component $a \in ACT$ is called a “joint action”, which is a tuple of actions (one for each agent) and $G = L_1 \times \cdots \times L_n \times L_e$ denotes a set of global states. The notation $l_i(g)$ is used to represent the local state of agent $i$ in the global state $g$. In addition, $l_i \in G$ is an initial global state for the system. For simplification, we remove the environment agent from the interpreted system formalism as done in Lomuscio et al. (2007).

The proposals in Bentahar et al. (2012) and El-Menshawy et al. (2013b) enriched Fagin et al.’s formalism of interpreted systems by shared and unshared variables in order to account for communication that occurs during the execution of MASs and to provide an intuitive semantics for social commitments that are made through communication between interacting agents. Technically speaking, they associated with each agent $i \in Agt$ a countable set $Var_i$ of local variables in order to represent communication channels through which messages are sent and received. Moreover, they denoted the value of a variable $x$ in the set $Var_i$ at local state $l_i(g)$ by $l_i^v(g)$. Thus,

$$l_i(g) = l_i(g'), \quad \text{then} \quad l_i^v(g) = l_i^v(g') \quad \text{for all} \ x \in Var_i$$

Intuitively, for two agents $i$ and $j$ to communicate, they should share a communication channel, which is represented by shared variables between $i$ and $j$. In this perspective, a communication channel between $i$ and $j$ does exist iff $\text{Var}_i \cap \text{Var}_j \neq \emptyset$. For a variable $x \in \text{Var}_i \cap \text{Var}_j$, $l_i^v(g) = l_j^v(g')$ means the values of $x$ in $l_i(g)$ for $i$ and in $l_j(g')$ for $j$ are the same. This intuitively represents the existence of a communication channel between $i$ (in $g$) and $j$ (in $g'$) through which the variable $x$ has been sent by one of the two agents to the other, and as a consequence of this communication, $i$ and $j$ will have the same value for this variable. However, shared variables are only used to motivate the existence of communication channels, not the establishment of communication.

The stochastic behavior of the system is captured by the following global evolution function as follows (Halpern, 2003; Wan et al., 2013):

$$\tau : G \times ACT \times G \rightarrow \{0, 1\}$$

Markovian properties are satisfied in the above function as the sum of the probabilities over all possible transitions from $g$ must be 1: for all $g \in G$, $\sum_{g' \in G} \tau(g, a^{\text{of}-x}, g') = 1$ where $a^{\text{of}-x}$ is the action labeling the transition between the two global states $g$ and $g'$ of the system. Moreover, we define the local evolution function as follows:

$$\tau_i : L_i \times Act_i \times L_i \rightarrow \{0, 1\}$$

such that for all $l_i \in L_i$, we have $\sum_{l_i} \tau_i(l_i, a^{\text{of}-l_i}, l'_i) = 1$ wherein $a^{\text{of}-l_i}$ is the local action labeling a transition between local states $l_i$ and $l'_i$ of agent $i$. Such modified version of the interpreted systems formalism is called probabilistic interpreted systems (Halpern, 2003). In the formalism of probabilistic interpreted systems, the transition probability matrix can be computed by Wan et al. (2013):

$$\tau(g, a^{\text{of}-x}, g') = \prod_{l_i \in \text{Agt}} \tau_i(l_i(g), a^{\text{of}-l_i}g, l_i(g'))$$

The PCTL$^k$ model is generated from an extended version of probabilistic interpreted systems (Halpern, 2003; Wan et al., 2013) enriched by a social accessibility relation (Bentahar et al., 2012; El-Menshawy et al., 2013b) as discussed above.

4. The logic PCTL$^k$

This section introduces the logic PCTL$^k$ (Probabilistic Computation Tree Logic of Knowledge and Commitment). We first define the models of PCTL$^k$ and, then, present the syntax and semantics of PCTL$^k$.

**Definition 1. (Models)**Given a set of atomic propositions $\Phi_0 = \{p, q, r, \ldots\}$ and a set of agents $Agt = \{1, \ldots, n\}$, the model $M = (S, P, I, \sim_1, \ldots, \sim_n, \sim_{ij-1}, I_{ij}(\text{Agt}^2), \nu)$ is a tuple where:

- $S \subseteq L_1 \times \cdots \times L_n$ is a countable set of all reachable global states for the system. A state $s$ is reachable iff there exists a sequence of transitions from an initial state to $s$ in which the probability of each transition is greater than 0.
- $I \in S$ is an initial global state for the system.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Knowledge</th>
<th>Commitment</th>
<th>Uncertainty</th>
<th>Formal</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Witwicki and Durfee (2007, 2009)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sultan et al. (2013)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Huang et al. (2011)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delgado and Benevides (2009)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wan et al. (2013)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Al-Saaqer et al. (2014)</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Our framework</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The presented model $M$ can be seen as a labeled transition system in which each transition from a state to another is given a probability value in the matrix $P$ indicating the likelihood of its occurrence wherein the transition is assumed to take a discrete time-step. It is also important to mention that every state in $M$ has at least one outgoing transition to avoid deadlocks. Also, all terminating/final states are modeled with a self-loop.

### 4.1. Semantics of PCTL\kappa

Given a model $M = (S, P, I, \sim_1, \ldots, \sim_n, \{\sim_{i,j}\}_{i,j \in \mathbb{A}}, \gamma)$, then $(M, s) \models \varphi$ states that "a state $s$ in the model $M$ satisfies a state formula $\varphi$. $(M, s) \models \psi$ means that "a path $\pi$ in the model $M$ satisfies a path formula $\psi$, and $(M, s) \models \mu_{\psi}K\varphi$ means that "a state $s$ in $M$ satisfies $\varphi$ in the interval specified by $\psi$. When the model $M$ is clear from the context, we simply write the satisfaction relation $\models$ as follows: $s \models \varphi$ and $s \models \psi$. Furthermore, for a given pair $(i, j) \in \mathbb{A} \times \mathbb{A}$ of agents, we denote the number of socially accessible states $s'$ from a given state $s$ such that $s \sim_{i,j} s'$ by $|s \sim_{i,j} s'|$. We also denote the number of epistemically accessible states $s'$ from a given state $s$ such that $s \sim_{i} s'$ by $|s \sim_{i} s'|$.

Finally, we define $s \models \varphi$ as follows:

$$s \models \varphi = \begin{cases} 1, & \text{if } s \models \varphi \\ 0, & \text{otherwise} \end{cases}$$

In what follows, we define the semantics of PCTL\kappa formulae.

- $s \models p$ iff $p \in \gamma(s)$.
- $s \models \varphi_1 \lor \varphi_2$ iff $s \models \varphi_1$ or $s \models \varphi_2$.
- $s \models \neg \varphi$ iff $s \not\models \varphi$.
- $s \models K\varphi$ iff $\forall s' \in S$ s.t. $s \sim s'$ we have $s' \models \varphi$.
- $s \models L_{\varphi}C\varphi$ iff $\exists s' \in S$ s.t. $s \sim_{s'} s$ and $s' \models C\varphi$.
- $s \models \nu_{\psi}K\varphi$ iff $\exists m \in S$ s.t. $\forall \pi(k) \models \varphi$ and $\forall i < k, \pi(i) \models \varphi$.
- $s \models P(\varphi) \iff \text{Prob}(\varphi) \geq k$ where $\text{Prob}(\varphi) = \text{Prob}(\pi \in \Pi(s) | s \models \varphi)$.

For a probabilistic operator working on an epistemic formula, where the set of all accessible states from $s$ is our sample space and the set of events $F$ is the set of states accessible from $s$ and satisfy the formula:

$$s \models P_{\psi}K\varphi \iff \text{Prob}(s \models K\varphi) \geq k \text{ where } \text{Prob}(s \models K\varphi) = \frac{\sum_{s' \in F} |s' \models \varphi|}{|S|}$$

For a probabilistic operator working over a commitment formula, where the set of all accessible states from $s$ is our sample space and the set of events $F$ is the set of states satisfying the formula:

$$s \models P_{\psi}C_{i,j} \varphi \iff \text{Prob}(s \models C_{i,j} \varphi) \geq k \text{ where } \text{Prob}(s \models C_{i,j} \varphi) = \frac{\sum_{s' \in F} |s' \models \varphi|}{|S|}$$

For a probabilistic operator working over a fullfilment formula, assuming that accessible states are also reachable:

$$s \models P_{\psi}F_{\psi}(C_{i,j} \varphi) \iff \text{Prob}(s \models F_{\psi}(C_{i,j} \varphi)) \geq k$$
where:

\[
\text{Prob}(s \models \text{Fu}(C_{i,j}\varphi)) = \text{Prob}_i(\pi \in \Pi(s')) | s' \sim_{i,j} s \\
\text{and } \pi = s \cdot \ldots \cdot s \text{ and } s' \models C_{i,j}\varphi)
\]

Notice that probabilistic knowledge is computed so that it reflects the indistinguishability property of the epistemic accessibility relation. Therefore, the probability is computed based on the number of accessible states satisfying the content of the knowledge over the number of equivalent states, as all the states are equally accessible. Probabilistic commitment is also computed based on the number of accessible states that satisfy the content over the whole number of accessible states, which demonstrates the uncertainty of the agent over the accessible states, so that over the commitment. Probabilistic fulfillment, however, is computed using the probabilistic transitions of the path linking the commitment state to the fulfillment state.

The following proposition is straightforward from the semantics:

**Proposition 1.** If \((M, s) \models P_{\geq 0}(\text{Fu}(C_{i,j}\varphi))\) and \((M, s) \equiv \text{Fu}(C_{i,j}\varphi)\), then \(s\) is not reachable from the commitment state.

**Theorem 1. Epistemic Equivalences**

1. \((M, s) \equiv P_{\geq 0}(\text{Fu}(C_{i,j}\varphi)) \text{ iff } (M, s) \equiv \text{Fu}(C_{i,j}\varphi)
2. \((M, s) \equiv P_{\geq 0}(\text{Fu}(C_{i,j}\varphi)) \text{ iff } (M, s) \equiv \text{Fu}(C_{i,j}\varphi)
3. \((M, s) \equiv P_{\geq 0}(\text{Fu}(C_{i,j}\varphi)) \text{ iff } (M, s) \equiv \text{Fu}(C_{i,j}\varphi)

**Proof.**

- **First equivalence.** \(\Rightarrow\). Assume \(s \models P_{\geq 0}(K_{i}\varphi)\). By the semantics of PCTL\(^{ki}\), it follows that \(\text{Prob}(s \models K_{i}\varphi) \geq 1\). Therefore, \(\sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). This means \(\forall s' \in S \text{ such that } s' \models \varphi\), we have \(s' \models \varphi\) (as \(\sim_{i,j}\) is reflexive, so \(s' \models \varphi\) could be stated itself). Thus, \(s \models K_{i}\varphi\).

- **Second equivalence.** \(\leftarrow\Rightarrow\). Assume \(s \models K_{i}\varphi\). By the PCTL\(^{ki}\) semantics, it follows that for all \(s \in S\) such that \(s_{\sim_{i,j}} s', \text{we have } s' \models \varphi\) (i.e., all accessible states from \(s\) satisfy \(\varphi\)). Consequently, \(\sum_{s' \models \varphi} | s' \models \varphi | = | s_{\sim_{i,j}} s' |\). Thus, \(\sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). Consequently, \(s \models P_{\geq 0}(K_{i}\varphi)\).

- **Third equivalence.** \(\leftarrow\). Assume \(s \models P_{\geq 0}(K_{i}\varphi)\). By the PCTL\(^{ki}\) semantics, it follows that \(0 < \text{Prob}(s \models K_{i}\varphi) < 1\). Therefore, \(0 < \sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). This means that it would never be the case that \(\forall s' \in S\) such that \(s_{\sim_{i,j}} s',\text{ we have } s' \models \varphi\). Consequently, \(s' \models \varphi\) for all \(s \in S\) such that \(s_{\sim_{i,j}} s\).

**Theorem 2. Commitment Equivalences**

1. \((M, s) \equiv \text{P}_{\geq 0}(\text{Fu}(C_{i,j}\varphi)) \text{ iff } (M, s) \equiv \text{Fu}(C_{i,j}\varphi)
2. \((M, s) \equiv \text{P}_{\geq 0}(\text{Fu}(C_{i,j}\varphi)) \text{ iff } (M, s) \equiv \text{Fu}(C_{i,j}\varphi)
3. \((M, s) \equiv \text{P}_{\geq 0}(\text{Fu}(C_{i,j}\varphi)) \text{ iff } (M, s) \equiv \text{Fu}(C_{i,j}\varphi)

**Proof.**

- **First equivalence.** \(\Rightarrow\). Assume \(s \models \text{P}_{\geq 0}(C_{i,j}\varphi)\). By the PCTL\(^{ki}\) semantics, it follows that \(\text{Prob}(s \models C_{i,j}\varphi) \geq 1\). Thus, \(\sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). This means that for all \(s' \in S\) such that \(s_{\sim_{i,j}} s', \text{ we have } s' \models \varphi\), and hence \(s \models C_{i,j}\varphi\).

- **Second equivalence.** \(\leftarrow\Rightarrow\). Assume \(s \models C_{i,j}\varphi\). By the PCTL\(^{ki}\) semantics, it follows that for all \(s' \in S\) such that \(s_{\sim_{i,j}} s', \text{ we have } s' \models \varphi\) (i.e., all accessible states from \(s\) satisfy \(\varphi\)). Consequently, \(\sum_{s' \models \varphi} | s' \models \varphi | = | s_{\sim_{i,j}} s' |\). Therefore, \(\sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). Consequently, \(\sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). This means that it would never be the case that \(\forall s' \in S\) such that \(s_{\sim_{i,j}} s',\text{ we have } s' \models \varphi\). Consequently, \(s' \models \varphi\) for all \(s \in S\) such that \(s_{\sim_{i,j}} s\).

- **Third equivalence.** \(\leftarrow\). Assume \(s \models \text{P}_{\geq 0}(C_{i,j}\varphi)\). By the PCTL\(^{ki}\) semantics, it follows that \(0 < \text{Prob}(s \models C_{i,j}\varphi) < 1\). Therefore, \(0 < \sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 1\). This means that it would never be the case that \(\forall s' \in S\) such that \(s_{\sim_{i,j}} s',\text{ we have } s' \models \varphi\). Consequently, \(s' \models \varphi\) for all \(s \in S\) such that \(s_{\sim_{i,j}} s\). Therefore, \(1 > \sum_{s' \models \varphi} \prod_{i,j} s' \geq \varphi \geq 0\). Consequently, \(s' \models \varphi\) for all \(s \in S\) such that \(s_{\sim_{i,j}} s\). Therefore, \(s \models \text{C}_{i,j}\varphi\). Consequently, \(s \models \text{C}_{i,j}\varphi\). Hence \(s \models \text{C}_{i,j}\varphi\) and \(s \models \text{C}_{i,j}\varphi\).
The idea is to reduce the problem of probabilistic model checking to the problem of probabilistic model checking in PCTL in order to use the PRISM model checker. Concretely, the proposed reduction technique consists of two processes. In the former one, we transform our model into an MDP model. MDPs are the standard models for describing systems with probabilistic and nondeterministic behavior (Rutten, Kwiatkowska, Norman, & Parker, 2004). Then, we use the notion of adversary as in Kwiatkowska (2003) to factor out the nondeterminism and consider the probability of some behavior of the MDP. The resulting adversaries are basically DTMC models for which we can define a unique probability measure over paths. The obtained DTMC models will be the input of the PRISM model checker. In the latter process of the reduction technique, we transform PCTL\textsuperscript{kc} formulae into PCTL formulae. This is basically achieved by constructing a set of rules that formally transforms the PCTL\textsuperscript{kc} formulae into corresponding ones in PCTL.

Before showing how to transform (M) into an MDP, we recall the definition of the MDP model as follows (Baier & Katoen, 2008):

**Definition 3 (MDP).** Given a set of atomic propositions AP, an MDP is a tuple M = (S, P, I, L, l, I) where:

- S is a nonempty and finite set of states
- P : S × Act × S → [0, 1] is the transition probability function, such that for every state s ∈ S and action θ ∈ Act, we have \( \sum_{s' ∈ S} P(s, θ, s') = 1 \).
- Act is a set of actions.
- I is an initial state.
- L : S → 2\(AP\) is a state labeling function.

An action θ ∈ Act is enabled in state s if and only if \( \sum_{s' ∈ S} P(s, θ, s') = 1 \). For any state s ∈ S, it is required that Act(s) ≠ ∅ where Act(s) denotes the set of enabled actions in s.

It is quite obvious from Definition 3 that the MDP model \( \tilde{M} \) (i.e., \( \mathcal{F}(M) \)) has a set of actions Act for which we don’t have an equivalent one in \( \text{PCTL}^{\text{kc}} \) model M. Therefore, one of the main steps that we perform in this transformation is to define the set Act. The idea is that, we translate different relations in M into labeled transitions in \( \tilde{M} \). Labels (also called actions) are used to distinguish between different types of relations. Consequently, the three relations in M, namely transition relation, epistemic accessibility relation, and social accessibility relation are translated into labeled transitions in \( \tilde{M} \). Moreover, whenever we have a labeled transition representing a social accessibility relation we add the symmetric closure of it to interpret the fulfillment of the commitment. As depicted in Fig. 2, assuming that n is the number of agents, 1 ≤ i ≤ n, and 1 ≤ j ≤ n, then actions δ, δ’, β, and γ denote...
transitions defined, respectively, from the probabilistic transition relation $P$, the epistemic accessibility relation $\sim$ (to capture the semantics of knowledge), the social accessibility relation $\sim_{soc}$ (to capture the semantics of commitment), and the symmetric closure of the social accessibility relation (to capture the semantics of fulfilment).

The model $\tilde{M} = (S, Act, P, I, I_i)$ can now be defined as follows:

- $S = S; I = I; L = V$.
- $Act = \{\delta, \alpha', \alpha, \beta\}$.
- $P(S, S') \subseteq S \times S$, is a nonempty and finite set of states.
- $I : S \times S \rightarrow [0, 1]$ is the transition probability matrix, such that for every state $s \in S$, we have $\sum_{s'} I(s, s') = 1$.
- $I_i : S \rightarrow 2^A$ is a labeling function which assigns to each state $s \in S$ the set $I_i(s)$ of atomic propositions that are valid in the state.

Each element $P(s, s')$ of the transition probability matrix gives the probability of making a transition from state $s$ to state $s'$. The probabilities from state $s$ must sum up to 1, i.e. $\sum_{s'} P(s, s') = 1$.

Before we proceed to present the transformation of PCTL into DTMC, we briefly review PCTL logic (Hansson & Jonsson, 1994). PCTL is an extension of CTL with a probability operator. The syntax of PCTL is defined by the following BNF grammar (Baier & Katoen, 2008):

$$\varphi ::= \neg \varphi \lor \varphi \land \varphi$$

$$\psi ::= \diamond \varphi \lor U \varphi \land U^m \varphi$$

The state formulae and path formulae are similar to PCTL without considering the knowledge and social operators.

Now, we introduce our reduction rules that translate PCTL into PCTL model $M$ given adversary $\sigma$. Given the adversary $\sigma$, the PCTL formulae are transformed inductively into PCTL as follows:

- $F(p) = p$, if $p$ is an atomic proposition,
- $F(\neg \varphi) = \neg F(\varphi)$,
- $F(\boxdot \varphi \land \psi) = \boxdot F(\varphi) \land F(\psi)$,
- $F(\boxdot \varphi \land \psi) = \boxdot F(\varphi) \land F(\psi)$,
- $F(\boxdot \varphi \land \psi) = \boxdot F(\varphi) \land F(\psi)$,
- $F(\boxdot \varphi \land \psi) = \boxdot F(\varphi) \land F(\psi)$.

Note that $\sigma$ is a DTMC model that is used to interpret only PCTL formulas. It can not be used to capture the transformed formulas of

![Fig. 2. Translating relations into labeled transitions.](image-url)
knowledge and commitment as it ignores all relations except those labeled by $\delta$ (i.e., transition relations of $P$).

Given the adversary $\sigma_1$, the PCTL$^E$ epistemic formula is transformed inductively into PCTL as follows:

$F(C_{i_1}(\varphi)) = P_{s_1}(\bigcirc F(\varphi))$

$F(P_{s_1}C_{i_1}(\varphi)) = P_{s_1}(P_{s_1} \bigcirc F(\varphi))$.  

As mentioned earlier, the adversary $\sigma_1$ is a DTMC model that captures only action at the knowledge state and $\delta$ at all other states. Intuitively, transitions labeled with $\delta$ represent epistemic accessibility relations and, in fact, epistemically accessible states from the knowledge state must satisfy $\varphi$. Back to Fig. 2 (b), it is readily seen that all next states to the knowledge state through transitions labeled with $\delta$ satisfy $F(\varphi)$. This explains why knowledge formula $C_{i_1}(\varphi)$ is transformed to next operator followed by the satisfaction of the content of the knowledge (i.e., $\bigcirc F(\varphi)$) in all paths emanating from the knowledge state.

Given the adversary $\sigma_1$, the PCTL$^E$ commitment formula is transformed inductively into PCTL as follows:

$F(C_{i_1}(\varphi)) = P_{s_1}(\bigcirc F(\varphi))$

$F(P_{s_1}C_{i_1}(\varphi)) = P_{s_1}(P_{s_1} \bigcirc F(\varphi))$.  

Similar to the case of knowledge formula, Fig. 2 (c) illustrates the intuitions behind transforming the commitment formula $C_{i_1}(\varphi)$ to $\bigcirc F(\varphi)$ in all baths emerging from the commitment state. Given the adversary $\sigma_1$, the PCTL$^E$ fulfillment formula is transformed inductively into PCTL as follows:

$F(\mu u(C_{i_1}(\varphi))) = P_{s_1}(\bigcirc F(\varphi))$

$F(P_{s_1}\mu u(C_{i_1}(\varphi))) = P_{s_1}(P_{s_1} \bigcirc F(\varphi))$.  

Though the semantics of the fulfillment in the PCTL$^E$ requires the existence of a path containing the fulfillment state which is socially accessible from the commitment state, here in the transformation we notice that all next states to the fulfillment state through transitions labeled with $\mu u$ should satisfy the commitment formula $C_{i_1}(\varphi)$. The reason of that is because in our transformation process, the transitions labeled with $\mu u$ came as a result of adding the symmetric closure of transitions labeled with $\mu u$ in order to capture the semantics of the fulfillment. Therefore, all added transitions should satisfy the commitment formula $C_{i_1}(\varphi)$ (see Fig. 2 (c)).

**Theorem 5** (Soundness of $F$). Let $M$ and $\Phi$ be respectively a PCTL$^E$ model and formula and let $F(M)$ and $F(\Phi)$ be the corresponding model and formula in PCTL. We have $M \models \Phi \iff F(M) \models F(\Phi)$. 

**Proof.** To prove the soundness of the proposed reduction technique, we have to prove that the following three cases are sound: $F = K_{\sigma_1}$, $F = C_{i_1}(\varphi)$ and $F = \mu u(C_{i_1}(\varphi))$. We prove this by induction on the structure of the formula $\Phi$. The case of PCTL$^E$ formulae that are also PCTL formulae is straightforward.

- $F = K_{\sigma_1}$. We have $(M, s) \models K_{\sigma_1}(\varphi) \iff (M, s) \models \varphi$ for every $s' \in S$ such that $s \rightarrow s'$. Therefore, $(M, s) \models K_{\sigma_1}(\varphi) \iff F(M, s) \models F(K_{\sigma_1}(\varphi))$. Recall that $F(M) = M$. Now, $(M, s) \models F(K_{\sigma_1}(\varphi))$ for every $s' \in S$ such that $(s, s') \in P_{s_1}$, we have $(M, s') \models F(\varphi)$. However, w.r.t the semantics of $\sigma_1$ which is an adversary defined to interpret commitment formulae over $M$, it follows that every infinite path $\pi \in \Pi^{s_1}(s)$ satisfies that $\pi(1) = s'$ and $(\sigma_1, \pi(1)) \models F(\varphi)$. Thus, $(\sigma_1, s) \models F(\varphi)$ for all $\pi \in \Pi^{s_1}(s)$. As the path quantifier $A$ is not defined in PCTL, and we have $P_{s_1}$ instead, so we obtain $(\sigma_1, s) \models P_{s_1}(\bigcirc F(\varphi))$.

- $F = C_{i_1}(\varphi)$. We have $(M, s) \models C_{i_1}(\varphi) \iff (M, s) \models \varphi$ for every $s' \in S$ such that $s \rightarrow_{i_1} s'$. Consequently, $(M, s) \models C_{i_1}(\varphi) \iff (M, s) \models F(C_{i_1}(\varphi))$. It follows that, $(M, s) \models F(C_{i_1}(\varphi))$ for every $s' \in S$ such that $(s, s') \in P_{s_1}$, we have $(M, s') \models F(\varphi)$. Now, based on the adversary $\sigma_1$, which is defined to interpret commitment formulae over $M$, every infinite path $\pi \in \Pi^{s_1}(s)$ satisfies that $\pi(1) = s'$ and $(\sigma_1, \pi(1)) \models F(\varphi)$. Thus, $(\sigma_1, s) \models F(\varphi)$ for all $\pi \in \Pi^{s_1}(s)$. As the path quantifier $A$ is not defined in PCTL, and we have $P_{s_1}$ instead, so we obtain $(\sigma_1, s) \models P_{s_1}(\bigcirc F(\varphi))$.

- $F = \mu u(C_{i_1}(\varphi))$. We have $(M, s) \models \mu u(C_{i_1}(\varphi)) \iff$ there exists $s' \in S$ such that $s \rightarrow_{i_1} s$ and $(\sigma_1, s) \models C_{i_1}(\varphi)$. Consequently, $(M, s) \models F(C_{i_1}(\varphi))$ there exists $s' \in S$ such that $(s, s') \in P_{s_1}$ and $(M, s') \models F(\varphi)$. Now, w.r.t the adversary $\sigma_1$ which is defined to interpret commitment formulae over $M$, we obtain at least one infinite path $\pi \in \Pi^{s_1}(s)$ that satisfies $\pi(1) = s'$ and $(\sigma_1, \pi(1)) \models F(\varphi)$. Since $E$ is equivalent to $P_{s_0}$ and $F(C_{i_1}(\varphi))$ is equivalent to $P_{s_1}(\bigcirc F(\varphi))$, so we obtain $(\sigma_1, s) \models P_{s_0}(P_{s_1}(\bigcirc F(\varphi)))$. 

5. Case study

In this section, a case study is implemented using PRISM (Kwiatkowska et al., 2002) to verify knowledge, commitments, and interactions between the two concepts in probabilistic MASs. We apply the approach using the NetBill protocol as in El-Menshawy et al. (2013b), Mallya and Singh (2007), Yolum and Singh (2002). NetBill protocol which is is developed for buying and selling encrypted software through the internet. We add probability to the original protocol so that the protocol will be closer to the real world situation. There are many interactions and communications between a buyer and a seller, and they are subject to several stochastic events, such as a buyer’s request for a quote could be successfully received by the seller in only 95% of the cases. Another example is the buyer will satisfy his delivery commitment with 98% of probability. Those probabilities are generally obtained after observing the system behavior for long time. We will introduce this modified probabilistic NetBill protocol next.

5.1. Protocol Description and Encoding

The basic protocol involves one customer agent $Cus$ and one merchant agent $Mer$ interacting to finish an online shopping
process. This protocol can also be applied to more than one customer and one merchant. A customer Cus requests a quote from the merchant Mer for an item to initialize the protocol. We assume that 5% of these requirements will fail to be sent to the merchant due to internet connection issues. The merchant replies to the successfully delivered request by presenting a quote for the requested item. After a customer gets the quote, we assume that 20% of customers reject the offer and end the protocol without any purchase. The other 80% of customers accept the offer, which means the customer commits to send the payment to the merchant \( (\text{CCus} \rightarrow \text{MerPay}) \).

By statistics, 90% payment commitments will be fulfilled \( (\text{Fu}(\text{CCus} \rightarrow \text{MerPay})) \) and 10% will be nullified. Both customer and merchant agents will be aware if the customer fulfills its commitments. When the merchant agent receives the payment, then it will commit to deliver the items to the customer \( (\text{Cmer} \rightarrow \text{CurDeliver}) \). Suppose that 99% of deliveries are successful, which means that the merchant fulfills its commitments \( (\text{Fu}(\text{Cmer} \rightarrow \text{CurDeliver})) \). Then, the merchant sends the receipt to the customer. If the delivery fails, the merchant violates its commitment. The merchant shall refund the customer. Fig. 3 depicts the model of the modified NetBill protocol.

With the PRISM modeling language, we translate every agent into a module as shown in Fig. 4, and the entire Multi-Agent System is defined as a system with agent modules which are all synchronized. We use labels to define the epistemic relations and social accessibility relation. To illustrate, label Al1s1 includes a set of states that are equivalent for agent Al at s1, while label Al1A2s0C contains a set of states that are socially accessible with respect to the commitment from agent Al to agent A2 at global state \( (s0) \).

![Fig. 3. The modified NetBill protocol.](https://sourceforge.net/projects/knowledgencommitment/files/PRISM/)

![Fig. 4. A code fragment showing encoding the merchant agent into a module in PRISM.](https://sourceforge.net/projects/knowledgencommitment/files/PRISM/)

1 https://sourceforge.net/projects/knowledgencommitment/files/PRISM/
5.2. Experimental Results

We verified several probabilistic epistemic and commitment properties as well as combinations made up from both properties for the NetBill protocol. The presented experimental results were performed on PRISM 4.0.1 on a Toshiba Portégé computer with 2.00 GHz Intel Core2 Duo T6400 processor and 3 GB memory under 64-bit Windows Vista Operating System.

We have conducted 10 experiments for the protocol using up to 15 agents. The results are in Table 2. Model statistics data (number of states and number of transitions) and model construction information (iteration and construction time) are reported. The model statistics data reflect the state space, while the construction information (iteration and construction time) are reported. The model of states and number of transitions) and model construction information.

Table 2
Experimental results for NetBill protocol with PRISM.

<table>
<thead>
<tr>
<th>Number of Agents</th>
<th>Model States</th>
<th>Transitions</th>
<th>Construction Iterations</th>
<th>Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>19</td>
<td>39</td>
<td>7</td>
<td>0.001</td>
</tr>
<tr>
<td>3</td>
<td>108</td>
<td>432</td>
<td>10</td>
<td>0.008</td>
</tr>
<tr>
<td>4</td>
<td>979</td>
<td>3,275</td>
<td>13</td>
<td>0.011</td>
</tr>
<tr>
<td>5</td>
<td>6,171</td>
<td>24,226</td>
<td>16</td>
<td>0.024</td>
</tr>
<tr>
<td>6</td>
<td>37,939</td>
<td>170,921</td>
<td>19</td>
<td>0.028</td>
</tr>
<tr>
<td>7</td>
<td>230,427</td>
<td>1,171,848</td>
<td>22</td>
<td>0.035</td>
</tr>
<tr>
<td>8</td>
<td>1,391,059</td>
<td>7,882,271</td>
<td>25</td>
<td>0.049</td>
</tr>
<tr>
<td>9</td>
<td>8,372,091</td>
<td>52,298,510</td>
<td>28</td>
<td>0.071</td>
</tr>
<tr>
<td>10</td>
<td>50,310,259</td>
<td>343,422,773</td>
<td>31</td>
<td>0.097</td>
</tr>
<tr>
<td>15</td>
<td>391,782,573,111</td>
<td>3,798,832,009,133</td>
<td>46</td>
<td>0.498</td>
</tr>
</tbody>
</table>

5.3. Discussion

This event is critical without any uncertainty. Therefore, we set the probability to 1. A similar formula is when the customer fulfills its commitments, but it turns out that it is not aware of:

\[ \phi_7 = P_{\geq 0.99} [Fu(C_{Mer1} \rightarrow \text{Deliver}) \land \neg (C_{Mer1} \land \neg (F_{Mer1}))]. \]

With 1% tolerance for missing delivery, we can define the third safety property in our logic as follows:

\[ \phi_5 = P_{\geq 0.99} [Fu(C_{Mer1} \rightarrow \text{Deliver}) \land \neg (C_{Mer1} \land \neg (F_{Mer1} \land \neg (F_{Mer1}))]. \]

- **Safety property.**

This property express that “a bad thing will never occur in the system”. It seems impossible for human beings not to make any mistake in the real world. Therefore, when we design a system, we may set a confidence interval to allow some mistakes for properties. For example, “with 99% chance, the system will not fail” instead of “the system will never fail”. In our protocol, one bad situation is when the customer Cus sends the payment to the merchant Mer1 without the merchant being aware of that. The following property can avoid this bad situation:

\[ \phi_1 = P_{\geq 0.99} [\neg (Fu(C_{Cus1} \rightarrow \text{Mer1}) \land \neg (K_{Mer1}))]. \]

Table 3 shows the results of model checking the above desirable properties for the probabilistic NetBill protocol for a system that includes one customer and one merchant.

Table 3
Results of model checking some protocol properties.

<table>
<thead>
<tr>
<th>Formulae</th>
<th>Results</th>
<th>Time for MC (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \phi_1 )</td>
<td>True</td>
<td>0.001</td>
</tr>
<tr>
<td>( \phi_2 )</td>
<td>True</td>
<td>0.001</td>
</tr>
<tr>
<td>( \phi_3 )</td>
<td>True</td>
<td>0.008</td>
</tr>
<tr>
<td>( \phi_4 )</td>
<td>True</td>
<td>0.001</td>
</tr>
<tr>
<td>( \phi_5 )</td>
<td>True</td>
<td>0.002</td>
</tr>
<tr>
<td>( \phi_6 )</td>
<td>0.72</td>
<td>0.001</td>
</tr>
</tbody>
</table>

6. Conclusion

In this paper, we presented a new framework for specifying, representing, and ultimately verifying the interaction between knowledge and social commitments in stochastic MASs. In theory,
our research contributions are as follows. First, we developed a new version of interpreted systems that captures the probabilistic behavior of knowledge and commitments and accounts for the communication between interacting parties. Second, we defined a new logical framework that merges concepts of probabilistic knowledge and probabilistic commitments in a single logic called PCTL^\text{mod}, so that complex formulae including both modalities can be expressed. Third, we introduced a new model checking technique to formally verify the compliance of MASs against some given properties expressed using the new logic. The proposed model checking procedure is reduction-based, in which the problem of model checking PCTL^\text{mod} is transformed into the problem of model checking an existing logic, namely PCTL. The key advantage of such a reduction is gaining the privilege to re-use a well known model checker such as PRISM. The soundness of the proposed reduction technique was provided. Moreover, we demonstrated the effectiveness of the proposed framework by applying it to the NetBill protocol, a concrete case study from e-business domain. The obtained results have initially confirmed the expressive capabilities of PCTL^\text{mod} in modeling and verifying the interactions between knowledge and social commitments in probabilistic settings. The scalability of the proposed model checking approach was also evaluated and models having up to 4 × 10^11 states can be effectively verified.

The distinguishing feature of the proposed approach over existing approaches lies in its ability to not only express and verify each of the individual concepts, i.e., knowledge and commitments, but also to capture and verify the interactions between the two aspects in the face of uncertainty. So, the impact of this research is reflected on the way knowledge and social commitments in MASs are captured, modeled, represented, and reasoned about. This results in gaining rich modeling at local (agent) and global (MAS) levels. Thus, more complex systems with uncertainty can be effectively and efficiently modeled and verified against vital properties, including safety, deadlock freedom and liveness.

The presented framework can be used in many practical MAS applications where uncertainty is a key issue such as multi-agent robotics systems (Cena, Cárdenas, Pazmiño, Puglisi, & Santonja, 2013; Yu & Weng, 2013), agent-based B2B applications (Bentahar, Alam, Maamar, & Narendra, 2010), agent-based communities of web services (Bentahar et al., 2008), and agent-based collaborative systems (Paletta & Herrera, 2011). Communication between interacting robotics or agent-based business applications and services in multi-agent settings can be captured in terms of social commitments instead of using mentalistic approaches that suffer from the un-verifiability problem (El-Menshawy, Bentahar, & Dossouli, 2009). In addition to allowing autonomous robotics and agent-based applications and services to be aware of their commitments, our approach will provide them with the ability to reason about and verify this awareness as well as the commitments themselves in the presence of uncertainty. Business processes composed based on MASs and service paradigms (Coria, Castellanos-Garzón, & Corcheda, 2014; Xu, Ji, Zhang, & Nie, 2013) is another area in which our approach can be fairly invested. Communication is a fundamental element in business processes employing social commitments as means of communication (Desai, Chopra, & Singh, 2009).

As future directions, we aim to investigate the use of other techniques to assess the uncertainty aspect of our MAS such as fuzzy logic as in Mengual, Marbán, Eibe, and Ruiz (2013) and neural networks as in Pan, Lai, Yang, and Wu (2013). We also aim to develop dedicated algorithms for the added modalities and integrate them into the PRISM model checker, so that we can compare the results of the two methods. Finally, including group knowledge and group commitments to the framework is another issue we aim to investigate.

References


Lomuscio, A., Pecheur, C., & Raimondi, F., 2007. Automatic verification of knowledge and time with NuSMV. In IJCAI (pp. 1384–1389).


