Modeling and Verifying Probabilistic Social Commitments in Multi-Agent Systems

Khalid Ibrahim Sultan

A Thesis

in

The Department

of

Electrical and Computer Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy at

Concordia University

Montréal, Québec, Canada

January 2015

CONCORDIA UNIVERSITY

Division of Graduate Studies

This is to certify that the thesis prepared

By: **Khalid Ibrahim Sultan**

Entitled: **Modeling and Verifying Probabilistic Social Commitments in Multi-Agent Systems**

and submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Dr. Gösta Grahne

_____ Dr. Elhadi Shakshuki

_____ Dr. Olga Ormandjieva

_____ Dr. Rachida Dssouli

_____ Dr. Abdessamad Ben Hamza

_____ Dr. Jamal Bentahar

Approved by _____

Chair of the ECE Department

_____ 2015 _____

Dean of Engineering

ABSTRACT

Modeling and Verifying Probabilistic Social Commitments in Multi-Agent Systems

Khalid Ibrahim Sultan, Ph.D.

Concordia University, 2015

Interaction among autonomous agents in Multi-Agent Systems (MASs) is the key aspect for solving complex problems that an individual agent cannot handle alone. In this context, social approaches, as opposed to the mental approaches, have recently received a considerable attention in the area of agent communication. They exploit observable social commitments to develop a verifiable formal semantics by which communication protocols can be specified. However, existing approaches for defining social commitments tend to assume an absolute guarantee of correctness so that systems run in a certain manner. That is, social commitments have always been modeled with the assumption of certainty. Moreover, the widespread use of MASs increases the interest to explore the interactions between different aspects of the participating agents such as the interaction between agents' knowledge and social commitments in the presence of uncertainty. This results in having a gap, in the literature of agent communication, on modeling and verifying social commitments in probabilistic settings.

In this thesis, we aim to address the above-mentioned problems by presenting a practical formal framework that is capable of handling the problem of uncertainty in social commitments. First, we develop an approach for representing, reasoning about, and verifying probabilistic social commitments in MASs. This includes defining a new logic called the probabilistic logic of commitments (PCTLC), and a reduction-based model checking procedure for verifying the proposed logic. In the reduction technique, the problem of

model checking PCTLC is transformed into the problem of model checking PCTL so that the use of the PRISM (Probabilistic Symbolic Model Checker) is made possible. Formulae of PCTLC are interpreted over an extended version of the probabilistic interpreted systems formalism. Second, we extend the work we proposed for probabilistic social commitments to be able to capture and verify the interactions between knowledge and commitments. Properties representing the interactions between the two aspects are expressed in a new developed logic called the probabilistic logic of knowledge and commitment (PCTL^{kc}). Third, we develop an adequate semantics for the group social commitments, for the first time in the literature, and integrate it into the framework. We then introduce an improved version of PCTL^{kc} and extend it with operators for the group knowledge and group social commitments. The new refined logic is called PCTL$^{\text{kc+}}$. In each of the latter stages, we respectively develop a new version of the probabilistic interpreted systems over which the presented logic is interpreted, and introduce a new reduction-based verification technique to verify the proposed logic. To evaluate our proposed work, we implement the proposed verification techniques on top of the PRISM model checker and apply them on several case studies. The results demonstrate the usefulness and effectiveness of our proposed work.

ACKNOWLEDGEMENTS

With a great sense of pride and relief I have finally crowned my PhD with this thesis. Immeasurable appreciation and deep gratitude are extended to the following persons who, in one way or another, have contributed in making this thesis possible.

First of all, I would like to express my sincere gratitude to Dr. Jamal Bentahar for accepting to supervise my thesis. This dissertation would not have been possible without his help. I am really grateful to him for the trust he put on me, for the support he offered me, and for guiding me in finding my place in the academic world.

I would also like to thank Dr. E. Shakshuki, Dr. O. Ormandjieva, Dr. R. Dssouli, and Dr. A. Ben Hamza for accepting to serve in the examination committee. Without objective judgment by knowledgeable people, scientific work loses all value.

This thesis was funded by the Ministry of Higher Education and Scientific Research in Libya through the Libyan - North American Scholarship Program. I would like to take this opportunity to thank them for their financial support. I am also grateful for all research facilities that have been provided to me at Concordia University to carry out this work.

I have been surrounded by wonderful friends and colleagues who provided me with a fertile environment to study and innovate. My gratefulness extends to all my friends in Montreal as well as my colleagues in the Multi-Agent Systems and Web Services laboratory at Concordia University.

More especially, I owe a huge debt of gratitude to my beloved parents and to all my family members back home for their support, encouragement and, most of all, their prayers throughout the course of my studies.

Last, but surely not least, special thanks go to my wife (Asma) and my wonderful children (Boshra, Malik, Lujain, and Rahaf) for their endless patience, love, and support.

TABLE OF CONTENTS

LIST OF TABLES x

LIST OF FIGURES xi

LIST OF ACRONYMS xii

1 Introduction **1**

1.1 Context of Research 1

1.1.1 Multi-Agent Systems (MASs) 1

1.1.2 Agent Communication Languages (ACLs) 3

1.2 Motivations 4

1.3 Problem and Research Questions 6

1.4 Objectives 8

1.5 Methodology 9

1.6 Contributions 12

1.7 Thesis Organization 13

2 Background **14**

2.1 Social Commitments 14

2.2 Reasoning about Knowledge 17

2.3 Modeling Techniques 18

2.3.1 Interpreted Systems 19

2.3.2 Discrete Time Markov Chains (DTMCs) 23

2.3.3 Markov Decision Processes (MDPs) 24

2.4 System Specification 26

2.4.1 Temporal Logics 26

2.5 Model Checking 31
2.5.1 Probabilistic Model Checking 33
2.5.2 Model Checking Tools 34
2.6 Summary 37

3 Probabilistic Social Commitments **38**
3.1 Introduction 38
3.2 The Probabilistic Logic of Commitments (PCTLC) 43
3.2.1 Syntax of PCTLC 46
3.2.2 Semantics of PCTLC 47
3.3 Model Checking PCTLC using Reduction 51
3.3.1 Transforming the Model $\mathfrak{M}_1$ 53
3.3.2 Reducing PCTLC Formulae into PCTL Formulae 55
3.4 Implementation 58
3.4.1 Oblivious Transfer Protocol 58
3.4.2 Oblivious Transfer Protocol Properties 59
3.4.3 Experimental Results 61
3.5 Related Work 64
3.5.1 Adding Commitment Operators to Existing Logics 64
3.5.2 Probabilistic Commitments 69
3.5.3 Comparison 71
3.6 Summary 73

4 The Interaction between Probabilistic Commitments and Knowledge **74**
4.1 Introduction 75
4.2 The Probabilistic Logic of Knowledge and Commitment (PCTL^{kc}) 79

4.2.1 Syntax of PCTL^{kc} . . . 81
4.2.2 Semantics of PCTL^{kc} . . . 82
4.3 Model Checking PCTL^{kc} Using Reduction . . . 88
4.3.1 Transforming the Model $\mathfrak{M}_2$ . . . 89
4.3.2 Reducing PCTL^{kc} Formulae into PCTL Formulae . . . 91
4.4 Implementation . . . 95
4.4.1 NetBill Protocol . . . 96
4.4.2 NetBill Protocol Properties . . . 97
4.4.3 Experimental Results . . . 99
4.4.4 Discussion . . . 101
4.5 Related Work . . . 101
4.5.1 Probabilistic Knowledge in MASs . . . 102
4.5.2 The Interaction between Knowledge and Social Commitments . . . 104
4.5.3 Comparison . . . 106
4.6 Summary . . . 107

5 On Probabilistic Group Social Commitments 109

5.1 Introduction . . . 109
5.2 The New Probabilistic Logic of knowledge and Commitment (PCTL^{kc+}) . . . 115
5.2.1 Syntax of PCTL^{kc+} . . . 118
5.2.2 Social Commitments Classification . . . 119
5.2.3 Group Knowledge . . . 121
5.2.4 Semantics of PCTL^{kc+} . . . 122
5.3 Model Checking PCTL^{kc+} using Reduction . . . 129
5.3.1 Transforming the Model $\mathfrak{M}_3$ . . . 130
5.3.2 Reducing PCTL^{kc+} Formulae into PCTL Formulae . . . 133

5.4 Implementation 137
5.4.1 Online Shopping System 137
5.4.2 System Properties 138
5.4.3 Experimental Results 140
5.5 Summary 144

6 Conclusion and Future Work **146**
6.1 Conclusion 146
6.2 Future Work 148

Bibliography **152**

LIST OF TABLES

3.1 Verification results of the oblivious transfer protocol 61

3.2 Results of model checking some properties for Oblivious Transfer Protocol 64

3.3 Comparison between our approach for the probabilistic commitments and the related work 71

3.4 Comparison between PCTLC and existing logics in terms of the adopted logic 71

3.5 Comparison between PCTLC and existing approaches in terms of the used verification tool 72

4.1 Experimental results for NetBill protocol with PRISM 99

4.2 Verifying some PCTL^{kc} properties for the NetBill protocol in case of two agents 100

4.3 Comparison between PCTL^{kc} and the related work 107

5.1 Verification results of the online shopping system 141

5.2 Results of model checking some properties for the online shopping system . 143

5.3 Model checking group commitment formulae 143

LIST OF FIGURES

1.1 The Proposed Framework 11

2.1 Social accessibility relations as defined in [9, 34] 22
2.2 The modified version of social accessibility relations as in [1] 23
2.3 Qualitative model checking overview 33
2.4 Probabilistic model checking overview 34

3.1 A schematic view of the probabilistic social commitment approach 43
3.2 The proposed reduction technique of model checking PCTLC 52
3.3 Translating relations in $\mathfrak{M}_1$ model into actions in the MDP model 53
3.4 Model construction time for oblivious transfer protocol 62
3.5 Time for model checking some properties for oblivious transfer protocol . . 65

4.1 An approach for the interaction between knowledge and commitments . . . 79
4.2 The proposed reduction technique of model checking PCTL^{kc} 89
4.3 Translating relations in $\mathfrak{M}_2$ into labeled transitions in the MDP model . . . 90
4.4 The Modified NetBill protocol 97
4.5 Model construction time for the NetBill protocol 100

5.1 A schematic view of the probabilistic group social commitment approach . 116
5.2 Accessibility relations for group social commitment 121
5.3 Examples of translating relations in $\mathfrak{M}_3$ into labeled transitions 130
5.4 A model for the case of one supplier and one customer 138
5.5 Model construction time for the online shopping system 142

LIST OF ACRONYMS

ACL	Agent Communication Language
AI	Artificial Intelligence
ARCTL	Action Restricted Computation Tree Logic
BDD	Binary Decision Diagram
BNF	Backus-Naur Form
CTL	Computation Tree Logic
CTLC	Computation Tree Logic of Commitment
CTLK	Computation Tree Logic of Knowledge
CTLKC	Computation Tree Logic of Knowledge and Commitment
CWB-NC	Concurrency WorkBench of New Century
DTMC	Discrete-Time Markov Chain
FIPA	Foundation for Intelligent Physical Agents
ISPL	Interpreted Systems Programming Language
KQML	Knowledge Query and Manipulation Language
LTL	Linear Temporal Logic
MAS	Multi-Agent System
MCK	Model Checking Knowledge
MCMAS	Model Checker for Multi-Agent Systems
MDP	Markov Decision Process
NuSMV	New Symbolic Model Verifier
PCTL	Probabilistic Computation Tree Logic
PCTLC	Probabilistic Computation Tree Logic of Commitment
PCTLK	Probabilistic Computation Tree Logic of Knowledge

PO-DTMC	Partially Observable Discrete-Time Markov Chain
POMDP	Partially Observable Markov Decision Process
PRISM	PRobabilistIc Symbolic Model checker
PSPASE	Polynomial Space
SMV	Symbolic Model Verifier
SPIN	Simple Promela INterpreter
TS	Transition System
UML	Unified Modeling Language

Chapter 1

Introduction

In this chapter, we introduce the context of our research, which falls in the area of agent communication within Multi-Agent Systems (MASs). More precisely, it is concerned with modeling and verifying social commitments –as a means of communication among agents– in the presence of probabilistic behavior. We also identify the motivations, problem statement, and research questions that we address in this thesis. Then, we list our objectives and discuss our methodology. Finally, we conclude this chapter by providing the thesis outline.

1.1 Context of Research

1.1.1 Multi-Agent Systems (MASs)

Nowadays, the use of distributed environments to solve complex real world problems using entities called agents is on rise [16, 86]. Agents are active, social, and adaptable computer systems situated in some dynamic environment and capable of autonomous actions [122]. Ideally, an agent has to be [123]:

- Reactive: able to respond to changes in its environment.

- Pro-active: capable to behave with respect to its goals (goal-directed behavior).
- Social: able to interact and communicate with others.
- Autonomous: able to operate without direct intervention of others.

In addition to being autonomous, agents are possibly heterogeneous; that is, agents may be independently designed by different programmers and hence it is difficult to make assumptions about their present or future behavior. A multi-agent system (MAS) consists of a set of these autonomous entities, which interact with each other and their surrounding environment to achieve their (joint) objectives [122]. In an open system, autonomous agents can freely enter and exit different interactions at any time [44]. In principle, open MASs provide no guarantees about the behavior of their agents. This means that when agents are working together, such as carrying out a business protocol, an agent's misbehavior may potentially create an exception for another agent and obstruct its proper working. However, one can look at multi-agent systems from different perspectives. From the computing perspective, a MAS is a computational paradigm and an advance in computer science. From the software engineering perspective, multi-agent technology is a new software engineering paradigm providing new abstractions for different phases of software development process. MASs approaches can be seen as very efficient and modular ways of modeling and implementing systems as they are capable of designing and programming autonomous agents with different abilities, behaviors, and intentions. From the artificial intelligence perspective, MASs provide better understanding and modeling of social intelligence and emergent behaviors.

1.1.2 Agent Communication Languages (ACLs)

Communication is a fundamental aspect for autonomous agents in MASs to coordinate with one another to solve complex problems that are difficult for an individual agent to tackle. Therefore, communication among agents is a key element to build effective MASs. In many realistic settings, agents need to interact to realize their goals. The type of interaction among the agents varies according to the goals of these interacting parties and the context of the transactions they are performing. An agent may cooperate with other agents to perform a certain task, compete with others to achieve a shared goal, or do a combination of both in order to perform individual or group tasks.

The importance of defining a standard framework for agent communication has been widely recognized. However, there have been many attempts in the literature to agree on standards for agent communication. Semantics of ACLs are defined either internally (privately) in terms of agents' beliefs and goals, or externally (publicly) in terms of agents' social commitments. Approaches defined using the former type of semantics are called mental approaches because they focus on the minds of interacting agents, while those defined using the latter one are called social approaches because they consider the social context of the interacting parties. In contrast to mental approaches such as those that are built using FIPA-ACL[1] and KQML (Knowledge Query and Manipulation Language) [42], social commitments proved to be a powerful representation for agent interactions [12, 80, 127]. They provide a social semantics that abstracts away from the agents internal states and offers social and observable meaning to the messages being exchanged among agents. In the context of this thesis, we focus on the kind of communication in which the semantics of messages is defined publicly, i.e., in terms of social commitments.

[1] See FIPA-ACL (Foundation for Intelligent Physical Agents - Agent Communication Language) specifications (1997,1999,2001,2002), http://www.fipa.org/repository/aclspecs.php3

1.2 Motivations

Our review of the social commitments literature has revealed a gap in handling probabilistic social commitments in MASs. We have noticed that though social commitments have been the subject of a vast research activity for more than a decade, current proposals to represent and verify social commitments, for instance [9, 11, 13, 23, 24, 32, 34, 98, 113], assume typical settings in which agents behave in an ideal manner, and consequently commitments among interacting agents are treated under the assumption of certainty. However, in the formulation of agent-based systems, the role of uncertainty is crucial for an efficient and coherent resolution of complex problems. Simply put, agents in MASs overcome complex problems thanks to their individual capabilities to be autonomous and to adapt their behavior with the changing of the environment in which they live and interact. Practically speaking, agents cannot always observe all the changes in the environment, but instead each agent can only have a partial view of other agents' behavior [48]. Indeed, the presence of imperfect information about the environment leads autonomous agents to make estimations about the observable world as part of their autonomous decision making processes [114]. This means that agents inevitably meet uncertainty during their work, or in many cases, for the high complexity of the problem, the information they handle is (or needs to be) approximate.

This unpredictable behavior of MASs raises different important questions. The interesting issue that we are mainly focusing on is how social commitments can be tackled in such systems. In reality, due to agents' autonomy, a request to create a social commitment is not always followed by the creation of that commitment. The same principle applies to fulfilling an established commitment. That is, in some situations, even if there is some state of affairs (i.e., content of a commitment) that an agent wants to bring about, its actions might not reliably drive the state of affairs into the desired state [125]. Consequently, the

problem of specifying and verifying social commitments is made more complicated by the presence of uncertainty.

The interaction between social commitments and agents' knowledge is also not receiving sufficient attention from the researchers in MASs community. For instance, the addition of epistemic reasoning to social commitments has not been widely considered yet. In fact, the ability to perform knowledge reasoning over commitments is one of the major advantages of addressing the relationship between the two concepts which ultimately helps ensure agents' awareness about their commitments and the fulfillments of these commitments. The vast majority of existing proposals have been carried out to address each of knowledge and commitments independently (see for example [5, 9, 26, 34, 51, 55, 62, 77, 90, 116]). However, it has been demonstrated that these two concepts (i.e., knowledge and commitments) are closely influencing each other in various practical settings such as e-commerce applications [1]. Therefore, their interaction needs to be specified and verified in a systematic way. The only two existing approaches, to the best of our knowledge, to model such interactions between knowledge and commitments either neglect the probabilistic features of MASs by assuming an absolute degree of correctness so that systems under consideration behave in an ideal manner [1], or adopt a different kind of commitments called "internal commitment" rather than the "social commitments" that we consider in this thesis [95]. The notion of "internal commitment" refers to a commitment of an agent to itself [99].

Another issue that has attracted our attention while reviewing the literature is the limitation of the current approaches to handle group social commitments. Although the notion of "group" has been, in one way or another, attached to commitments in several proposals [31, 94, 124, 128], the semantics of "group social commitments" has never been materialized in the past. The need to formalize "group social commitments" stems from the importance of the concept of "group" in real settings as we will see later in Chapter 5.

To address the above shortcomings, a major challenge in our research is to accurately represent and verify social commitments in the presence of uncertainty. Another ambitious challenge is to formally capture and verify the interaction between social commitments and agents' knowledge in probabilistic MASs. Yet another challenge is to define an appropriate semantics for social commitments under the scope of a group (i.e., one-to-many commitment schemes) and then study the relationship between individual and group social commitments and knowledge in probabilistic settings.

1.3 Problem and Research Questions

The main problem we are addressing in this thesis is the problem of handling *probabilistic social commitments* in MASs. To ensure having effective commitment-based interactions in open and heterogeneous systems, these commitments need to be represented and verified while keeping uncertainty in mind.

Current research initiatives focus mainly on extending conventional temporal logics such as LTL [91] and CTL [38], and CTL* [39] to express social commitments [5, 9, 34, 51, 90, 113]. The downside of the current extended logics resides in their expressiveness. In fact, existing commitment logics can neither express probabilistic social commitments nor capture the interaction between commitments and knowledge in probabilistic MASs. Besides, these logics lack the ability to deal with group-commitment scenarios and instead they are limited to the common one-to-one commitment scheme.

To circumvent this downside, we need to come up with a probabilistic logic equipped with a social operator –for commitments and their fulfilments– that is expressive enough to represent and reason about social commitments in the presence of uncertainty.

In order to do so, some questions arise. We name these research questions: R1, R2,

R3, ... etc. The first question is: **how can we define a logic that is capable of specifying social commitments employed in uncertain settings?** [R1]. In the literature, there is no such work that considers dealing with social commitments in the presence of probabilistic behavior. Thus, our thinking was directed towards existing conventional logics to investigate the possibility of exploiting them to help define the new logic. However, **which temporal logic to choose** is the second question to be answered [R2]. Existing probabilistic temporal logics such as PCTL [57] and PCTL* [3] consider neither commitments nor agent communication. We propose to extend PCTL with modal operators for commitments and their fulfillments. This process is achieved by combining two existing logics together. However, any logic needs to be associated with a computational model over which formulae of the logic are interpreted. So, our third question is: **which computational model to use in order to model the target MASs?** [R3]. The underlying computational model considered throughout this thesis is the one of interpreted system formalism [40], suitably extended whenever necessary. Furthermore, to verify the proposed logic, we need to answer the following question: **which formal verification technique to use?** [R4]. In fact, there are three main verification techniques to verify systems against given requirements in the literature, namely testing, theorem proving, and model checking. Model checking has some advantages over others since it is fully automated and systematically checks all system states. On the other hand, in testing, it is hard to generate exhaustive test cases, and theorem proving requires expertise and is only semi-automatic. So, we use model checking as a means of formal verification. However, **which model checking technique to adopt** [R5] should be answered as many techniques are already in use. Current proposals use only qualitative model checking to ensure the correctness of commitment-based interactions in MASs. However, since our approach is built on PCTL, we propose a reduction-based probabilistic model checking technique in which the problem of model checking our logic is

reduced to the one of PCTL. Finally, to check the effectiveness of our approach, we need to implement the proposed model checking technique. Hence, we need to answer the question: **which model checker to use in order to verify the proposed logic?** [R6]. In our work, we adopt the PRISM model checker[2] as it already allows for analyzing and verifying probabilistic systems, and it also performs symbolic model checking of PCTL in which it manipulates sets of states rather than single states. Such sets are efficiently represented and transformed by means of Binary Decision Diagrams (BDDs) [81], which help alleviate the state space problem associated with model checking.

1.4 Objectives

The main objectives of this research are:

1. Proposing a new meaningful, declarative, and verifiable logic with an expressive power that allows for representing and reasoning about commitments and their fulfillments in the presence of uncertainty.

2. Developing a new version of interpreted systems that can effectively model systems under consideration.

3. Investigating the relationship between the probabilistic social commitments and probabilistic knowledge in agent-based systems.

4. Defining a proper semantics for the group social commitments.

5. Introducing a new model checking technique for verifying social commitments expressed in terms of the proposed logic.

[2]http://www.prismmodelchecker.org

1.5 Methodology

As an improvement over existing solutions, the research presented in this dissertation targets social commitments employed in systems exhibiting probabilistic behavior. We address the problem of specifying probabilistic social commitment in MASs by developing a novel logic called the probabilistic logic of commitments (PCTLC) that can represent and reason about social commitments in the face of uncertainty. The introduction of the new logic is motivated by the fact that the needed modal operators for reasoning about probabilistic social commitments and their fulfillments cannot be expressed using existing temporal logics. To build PCTLC, we advocate the technique of combining two existing logics in a new logic. Particulary, we adopt the independent join technique [8, 46, 47]. The reason why we use this technique is because it ensures the preservation of important properties of the logics being combined [69]. In this perspective, we combine a logic of commitment called CTLC [9, 34] and a probabilistic logic called PCTL [57]. This process can be seen as adding a probabilistic operator to the ingredients of the logic of commitment (CTLC), or vise versa (i.e., adding a commitment operator to the ingredients of the probabilistic logic PTLC). We model target systems using the formalism of interpreted systems. However, the original version of interpreted systems introduced by Fagin et. al in [40] does not capture the probabilistic behavior of MASs and also does not account for the communication between interacting agents. Therefore, we combine two extended versions of the original formalism introduced respectively by Halpern [55] and Wan et al. [116] to capture the stochastic behavior of the system, and Bentahar et al. [9] and El-Menshawy et al. [34] to model the communication between interacting parties.

Furthermore, our approach evaluates social commitments at the design level as to help reduce the cost of the development process and increase robustness of target systems. This is achieved by formally verifying some given PCTLC-based properties using a model

checking technique. Model checking was chosen due to the reasons stated earlier in Section 1.4. However, model checking can be generally performed by one of the following methods. 1) Direct method in which new dedicated model checking algorithms are developed in order to verify social commitments, or 2) Indirect method which is also called reduction-based method or translation-based method. Indirect model checking techniques involve devising some reduction rules to reduce the problem of model checking the logic at hand to that of an existing logic in order to use current model checkers [77]. Certainly, each method has its own benefits with respect to the logic being verified. In this thesis we follow the latter method because it is easy to use and allows the re-use of existing model checkers [34]. Later in Chapters 3, 4, and 5, we show how the indirect method can effectively and efficiently verify probabilistic social commitments.

Our proposed model checking procedure for PCTLC includes instantiating a set of reduction rules that transform the problem of model checking PCTLC to the problem of model checking an existing probabilistic logic called PCTL. By so doing, we gain the privilege of re-using the available PRISM model checker.

The proposed logic of social commitment (PCTLC) is then extended by an epistemic operator to be able to express and reason about the interaction between knowledge and social commitments in the presence of uncertainty. The idea is that, we have various logics for each of knowledge and social commitments independently in the literature, so we combine a probabilistic logic of knowledge and a probabilistic logic of commitments in a single logic that we call the probabilistic logic of knowledge and commitment PCTL^{kc}. On that basis, we again construct a set of transformation rules to reduce the problem of model checking the proposed logic PCTL^{kc} to that of PCTC so that formulae expressing properties written in PCTL^{kc} can be model checked using PRISM by checking their corresponding formulae of PCTL.

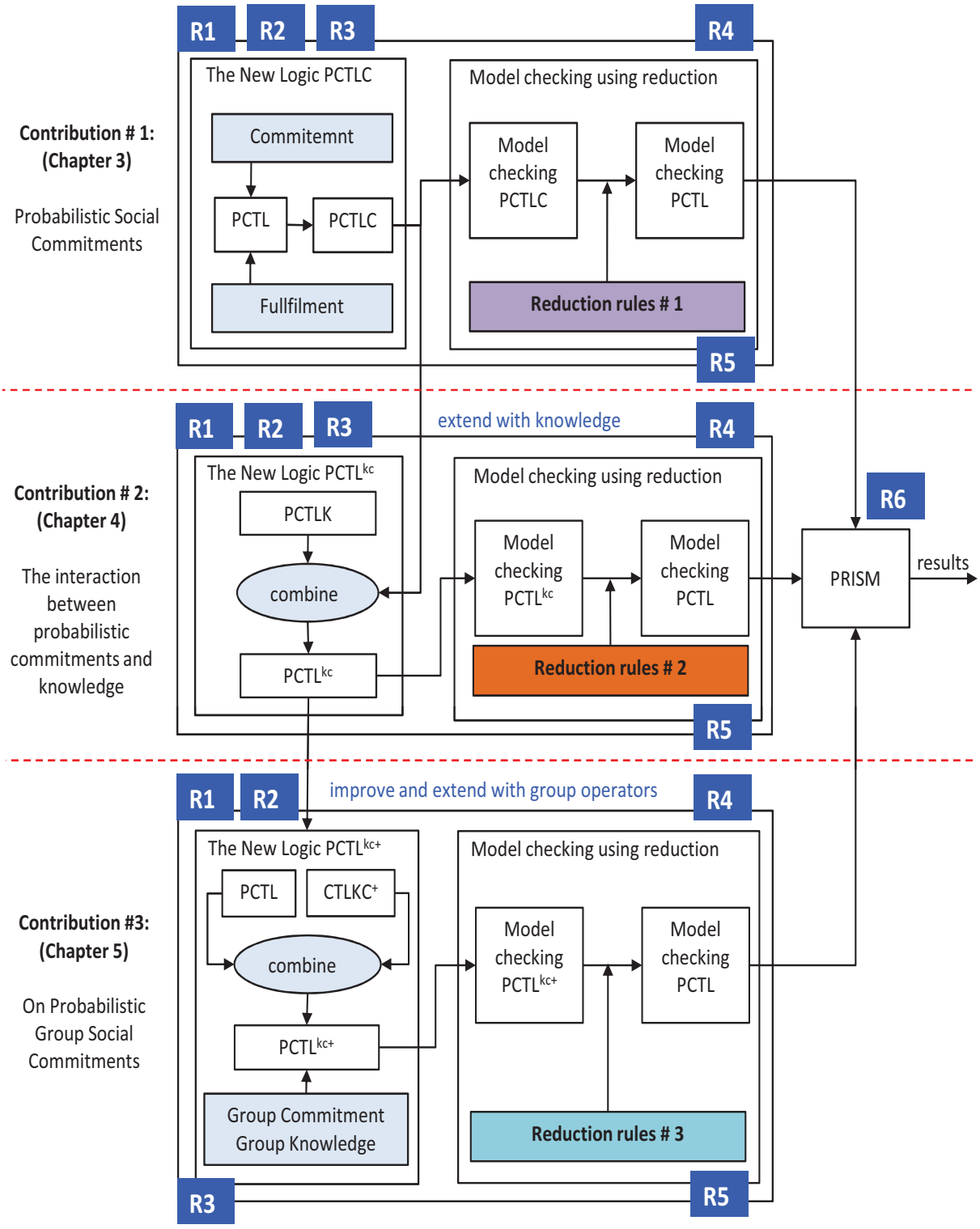

Figure 1.1: The Proposed Framework

To be able to handle social commitments when the scope of interacting agents is extended from the common one-to-one scheme to one-to-many scheme, we develop a semantics for the group social commitment operator and integrate it to the framework. We also add a group knowledge operator in order for the new logic to be more expressive and effective. The improved and refined logic is called the new logic of knowledge and commitments (PCTL$^{\text{kc+}}$). Moreover, we generalise the model checking technique proposed for PCTL^{kc} to verify the new logic (PCTL$^{\text{kc+}}$) with the group operators.

Finally, each proposed reduction technique is implemented independently on top of the PRISM tool and applied to a concrete case study. Figure 1.1 depicts the structure of the proposed work, links contributions to each other, and maps them to thesis chapters. Moreover, this figure shows where we answer each of the research questions presented in Section 1.3.

1.6 Contributions

We have developed a set of methods to pursue our objectives and to fill the research gap identified above. The majority of the work presented in this thesis has been published in the proceedings of various international conferences and refereed international journals. In summary, the main contributions are:

1. A new logic called the probabilistic logic of commitments (PCTLC) that can represent and reason about social commitments in the presence of uncertainty [107].

2. A new logic called the probabilistic logic of knowledge and commitment (PCTL^{kc}) whose expressive power helps capture the interaction between knowledge and social commitments in probabilistic MASs [106]

3. A Semantics for group social commitment [104].

4. An improved version of the logic of knowledge and commitments enriched with epistemic and social group operators (PCTL^{kc+}). The distinguished feature of the new logic lies in its ability of not only expressing the interaction between individual (basic) social commitments and knowledge, but also expressing the interaction between group social commitments and knowledge in the presence of uncertainty [104].

5. Three reduction-based model checking techniques for PCTLC [103], PCTL^{kc} [106], and PCTL^{kc+} [105] respectively.

6. Implementation of the three proposed model checking techniques on top of the PRISM model checker using concrete case studies.

1.7 Thesis Organization

The remainder of this thesis is organized as follows. Chapter 2 describes the background needed for our research. Chapter 3, presents a formal approach for handling probabilistic social commitments in MASs. In Chapter 4, we introduce a probabilistic approach for capturing and verifying the interaction between knowledge and social commitments. Chapter 5 presents an improved version of the approach presented in Chapter 4 and then extends it to accommodate group knowledge and group commitments. Chapter 6 concludes the thesis and identifies hints for future directions.

Chapter 2

Background

This chapter reviews the background needed for our thesis. We explain all concepts, techniques, and tools that are used throughout this thesis. In Section 2.1, the concept of social commitments as a means of communication between interacting agents is discussed. Section 2.2 is devoted to briefly review reasoning about knowledge in MASs. In Section 2.3 some modeling formalisms including Interpreted Systems, we use in this thesis, are reviewed. Temporal logics for systems specification are also presented in this section. Section 2.5, describes the concept of model checking. Also, a review of some prominent existing model checkers is given in this section. Finally, we conclude this chapter in Section 2.6.

2.1 Social Commitments

The interoperability requirement in MASs has led to the introduction of various standardized agent communication languages (ACLs). The early proposals for defining the semantics of ACLs like KQML [42] and FIPA ACL[1] are developed using agent's mental states like beliefs, desires and intentions. These are now called mentalistic approaches because their

[1] See FIPA-ACL specifications (1997,1999,2001,2002), http://www.fipa.org/repository/aclspecs.php3

focus are on the minds of the individuals participating in the interaction. A major weakness of these approaches is that they assume that *agents can read each other minds* [96]. Actually, in open environments where heterogeneous agents are made by different vendors and possibility using different technologies, it seems impossible to trust other agents completely or to make strong assumptions about their internal structure. This raises a serious verification problem for such approaches [99, 122]. To overcome this drawback, some researchers took the initiative to think about other ways for defining ACLs [96]. As a result, social commitments have come to emergence. Social commitments are basically modeled as public information conveyed by an agent to another one. More specifically, a social commitment is an agreement between an agent, namely *debtor*, to another agent, *creditor*, in which the debtor engages towards the creditor to bring about a certain property [18, 101]. In addition to being social, commitments are also public, and objective [23]. These properties of social commitments help heterogeneous agents attribute the same meaning to the messages being exchanged so that the meaning is expressed using concepts that do not depend on an individual agent's internal structure. Importantly, a commitment between two agents is not just a static entity, but rather a dynamic one whose state changes over time as events occurs [54, 111]. This dynamicity feature supports commitments' flexibility and can be captured through the manipulation of commitments via some operations such as *creation*, *fulfillment*, *cancellation*, *release*, *assignment*, and *delegation* [97]. In particular, a debtor may *create* a commitment, thus activating it, or *fulfill* a commitment, thus discharging it. However, for different reasons, a debtor might fail to fulfill its commitment; thus, it becomes violated. Given a commitment, its creditor can freely *assign* it to another creditor, and its debtor may *delegate* it to a another debtor. Furthermore, a debtor may *cancel* a commitment; whereas, a creditor can *release* the debtor from the commitment at any time.

Commitment-based approaches to ACLs have been around for about twenty years.

Defining semantics of ACLs using the notion of social commitments has its roots back to the work of Singh [98] in which he was the first to formalize a commitment-based ACL in temporal logic. Since then, social commitments have gained more and more popularity as a communication approach that makes no assumptions on the agents' internal states. To develop such approaches, various commitment logics that extend CTL (Computation Tree Logic), LTL (Lineal Temporal Logic), and CTL* (superset of CTL and LTL) have been introduced. Examples of efforts on this line can be found in [13, 51, 90, 98, 113]. These logics have been successful in specification and verification of systems from different areas such as commitment-based protocols [5, 32, 45, 127], modeling business processes [28, 108] and agent-based web services [10]. However, the common limitation of theses proposals is that they neglect the uncertainty aspects of MASs and tend to assume typical behavior instead. In broad terms, uncertainty is a crucial aspect in MASs and has an impact not only on the behavior of the participating agents but also on the communication process that occur among these agents.

In this thesis, we consider the notion of "social commitments" that is meant for communication. That is, the notion of commitments as a foundation for understanding interactions among agents. Therefore, we use communicative social commitments, also called illocutionary social commitments, as defined in [9, 34]. Those commitments are formally denoted by $C_{i\to j}\varphi$, meaning that agent i, the debtor, commits to agent j, the creditor, to bring about φ, where φ is the content of the commitment. Different notations with the same meaning can be found in [28, 44, 98]. This notion of "social commitments" should not be confused with some related notions such as "Internal Commitments", "Norms", and "Obligations". In traditional Artificial Intelligence (AI), a commitment was understood as the commitment of a single agent to some belief or to some course of action [76]. In this

direction, “internal commitment” [18, 99] which refers to a commitment of an agent to itself has been widely used in the domain of AI. Norms, which are formal specifications of deontic statements that aim at regulating the interactions among agents, have also received a considerable attention in AI and MASs domains [7, 100, 110]. Obligations, on the other hand, have long been used as explicit mechanisms for influencing the behavior of interacting parties and providing some stability and reliability in their interactions [29]. Some researchers consider that commitments are somewhat like direct obligations [30, 99].

In contrast, the interesting feature that differentiates social commitments from the aforementioned notions is that a social commitment is directed from one party (the debtor) to another one (the creditor) which reflects the intuition that the debtor is committed to doing something for the creditor. These commitments are illocutionary in the sense that they are used as means of conveying information among interacting agents. Moreover, communicative commitments are equipped with a grounded semantics because the social accessibility relation has an intuitive and computational interpretation that makes its model checking possible.

2.2 Reasoning about Knowledge

knowledge logics (also known as epistemic logics) are focused on reasoning about the knowledge that agents may have about themselves, the world, or other agents [40]. These logics have been shown to be a useful framework for the analysis of distributed algorithms and security protocols. Generally, an epistemic logic captures the essence of knowledge through modal operators. In this line, the contribution of Jaakko Hintikka in [58] is recognized as the first attempt to investigate the logic of knowledge as a modal logic. Since then, researchers in AI and MASs have carried out numerous proposals to represent the evolution of knowledge [26, 40, 55, 62, 77, 78, 83, 116]. Formally, agent i knows something

is denoted by $K_i\ \varphi$. From a verification perspective, model checking the logic of knowledge was first mooted by Halpern and Vardi [56]. Since that time theoretical aspects of model checking the logic of knowledge and its combinations with temporal logic have been studied.

In addition to reasoning about what one agent knows, it is often useful to be able to reason about the *common knowledge*: the things that everyone knows, and that everyone knows that everyone knows, etc. Everyone knows can be defined as an abbreviation:
$E_G\varphi \equiv K_1\varphi \wedge \ldots K_n\varphi$, where G is a group of agents, and n is the number of agents in G.
The common knowledge operator C_G is defined in terms of E_G as follows:
$C_G \equiv E_G\varphi \wedge E_G^2\varphi \wedge \cdots \wedge E_G^k \wedge \ldots$, where E_G^k is read: "everyone in G knows φ to degree k".

2.3 Modeling Techniques

Transition Systems (TSs) are typically used as models to describe the behavior of systems [22]. They are the underlying models for all various non-real time models. TSs are modeled as directed graphs where nodes reflect the states, and edges represent the transitions. A state describes some information about the systems at a given moment of its behavior. Whereas, a transition describes how the systems can evolve from one state to another. A TS is a tuple $\mathbb{T} = (S, Act, \rightarrow, I, AP, \mathrm{L})$, where S is a set of states, Act is a set of actions, $\rightarrow \subseteq S \times Act \times S$ is the transition relation, $I \subseteq S$ is a set of initial states, AP is a set of atomic propositions, and $\mathrm{L} : S \rightarrow 2^{AP}$ is a labeling function [4]. In order to model random phenomena, transition systems are enriched with probabilities. This can be done in different ways. In the rest of this section, we review some probabilistic models that are used throughout our thesis.

2.3.1 Interpreted Systems

The formalism of interpreted systems introduced by Fagin el al. [40] provides a useful framework to locally model autonomous and heterogeneous agents who interoperate within a global system via sending and receiving messages. This thesis builds on this formalism for various reasons:

- It is a suitable formalism for modelling agent-based systems as it provides a good level of abstraction that allows focusing more on modeling the key characteristics of the interacting agents along the evolution of their social commitments [37].
- It has been successfully used to reason about various aspects of MASs such as time, knowledge, commitments, and correct behavior.
- Interpreted systems are computationally grounded [120], meaning that the semantics of interpreted systems maps directly to the paths of the system, and vice-versa.
- Interpreted systems can be easily extended. The original version introduced by Fagin et al. [40] has been extended in various ways as we will see below. This property of being readily extensible is important for us as we always need to extend it as required.

Suppose a set $\mathtt{Agt} = \{1,\ldots,n\}$ of n agents. 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 $i \in \mathtt{Agt}$ 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 $i \in \mathtt{Agt}$ are performed in compliance with a local protocol $\mathscr{P}_i : L_i \rightarrow 2^{Act_i}$, which assign a set of enabled local actions to a local state. Intuitively, this set corresponds to the actions that are enabled in a given local 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 $\mathscr{P}_e$. A tuple $g = (l_1, \ldots, l_n, l_e) \in (L_1 \times \ldots \times L_n \times L_e)$ where $l_i \in L_i$ for each $i \in \mathtt{Agt}$ 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 (i.e., a snapshot of the global system at a specific time).

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

$$\tau_i : L_i \times L_e \times Act_i \rightarrow L_i \tag{2.1}$$

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

$$\tau : G \times ACT \rightarrow G \tag{2.2}$$

where $ACT = Act_1 \times \ldots \times Act_n$ and each component $a \in ACT$ is called a "joint action", which is a tuple of actions (one for each agent), and $G = L_1 \times \ldots \times L_n \times L_e$ 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, $I \in G$ is an initial global state for the system.

Bentahar et al. [9] and El-Menshawy et al. [34] extended Fagin et al.'s formalism of interpreted systems with 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 established through communication between interacting agents. They specifically associated with each agent $i \in \mathtt{Agt}$ a countable set Var_i of local variables. Then, they used those variables to represent communication channels through which messages are sent and received. Technically, they denoted the value of a variable x

in the set Var_i at local state $l_i(g)$ by $l_i^x(g)$. Thus,

$$\text{if } l_i(g) = l_i(g'), \text{ then } l_i^x(g) = l_i^x(g') \text{ for all } x \in Var_i \tag{2.3}$$

The idea is that, 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 $Var_i \cap Var_j \neq \emptyset$. For a variable $x \in Var_i \cap Var_j$, $l_i^x(g) = l_j^x(g')$ means the values of x in $l_i(g)$ for agent i and in $l_j(g')$ for agent 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. The key point is that shared variables are only used to motivate the existence of communication channels, not the establishment of communication. Figure 2.1 depicts the idea of using shared and unshared variables for establishing communication channels between interacting agents. The three conditions upon which a communication channel between i and j exists are listed below:

For each pair $(i, j) \in \mathtt{Agt}^2$, $\sim_{i \to j} \subseteq S \times S$ is a social accessibility relation. $s \sim_{i \to j} s'$ is defined by the following conditions:

1. $l_i(s) = l_i(s')$.

2. $Var_i \cap Var_j \neq \emptyset$ such that $\forall x \in Var_i \cap Var_j$ we have $l_i^x(s) = l_j^x(s')$.

3. $\forall y \in Var_j - Var_i$ we have $l_j^y(s) = l_j^y(s')$.

Recently, Al-Saqqar et al. [1] have modified the definition of social accessibility relations given in [9, 34] in such a way that the new definition does no longer depend on the unshared variables but rather depends merely on the shared variables between the

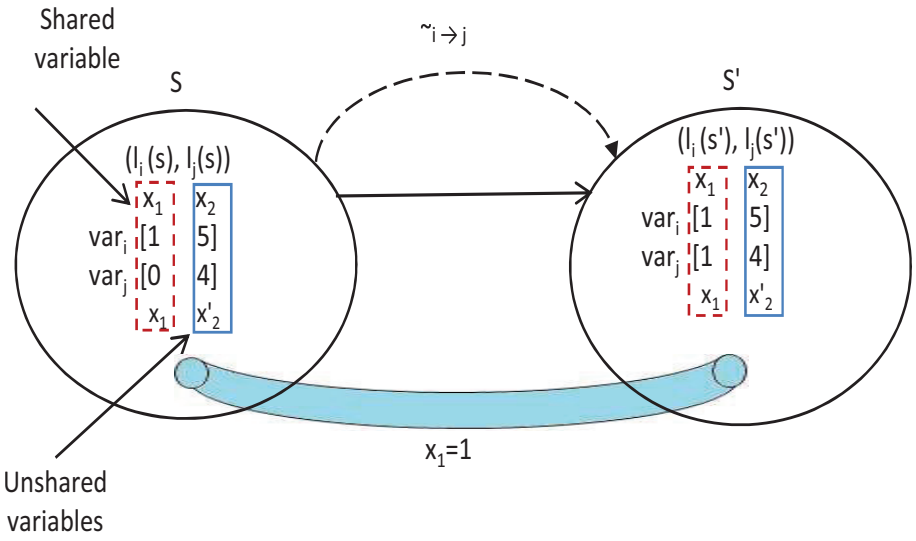

Figure 2.1: Social accessibility relations as defined in [9, 34]

interacting agents as shown in Figure 2.2. The new condition upon which a communication channel is established is stated below:

$s \approx_{i\to j} s'$ iff $Var_i \cap Var_j \neq \emptyset$ such that $\forall x \in Var_i \cap Var_j$ we have $l_i^x(s) = l_i^x(s') = l_j^x(s')$, where $\approx_{i\to j} \subseteq S \times S$ is the new social accessibility relation [1].

The original version of interpreted systems formalism was also extended by Halpern et al. [55] and further by Wan et al. [116] to model the stochastic behavior of MASs. Accordingly, the local evolution function is defined as follows:

$$\tau_i : L_i \times Act_i \times L_i \to [0,1] \tag{2.4}$$

such that for all $l_i \in L_i$, we have $\sum_{l_i' \in L_i} \tau_i(l_i, a^{l_i \to l_i'}, l_i') = 1$ wherein $a^{l_i \to l_i'}$ is the local action labeling a transition between local states l_i and l_i' of agent i.

Moreover, the global evolution function is defined as follows:

$$\tau : G \times ACT \times G \to [0,1] \tag{2.5}$$

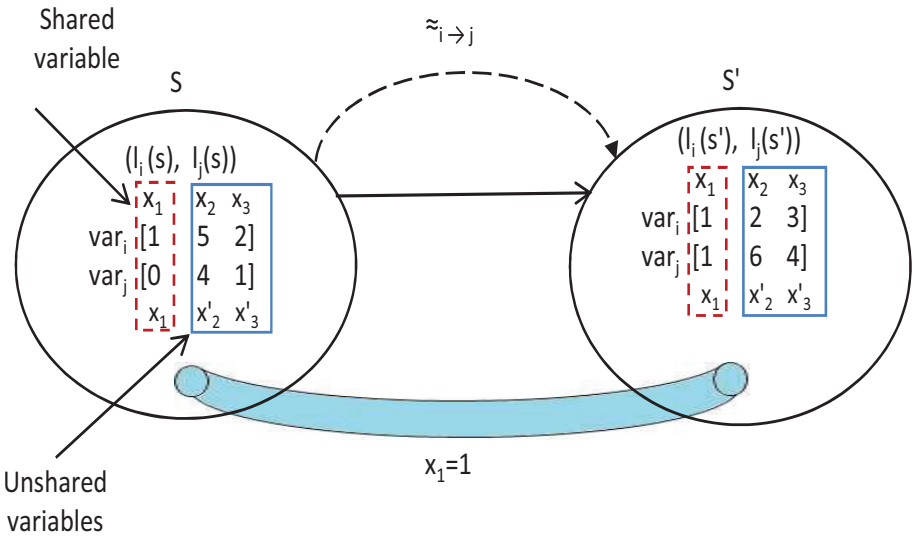

Figure 2.2: The modified version of social accessibility relations as in [1]

The sum of the probabilities over all possible transitions from a given state g must be 1: for all $g \in G$, $\sum_{g' \in G} \tau(g, a^{g \to g'}, g') = 1$ where $a^{g \to g'}$ is the action labeling the transition between the two global states g and g' of the system.

Such a modified version of the interpreted systems formalism is called *probabilistic interpreted systems* [55]. In the formalism of probabilistic interpreted systems, the transition probability matrix can be computed by [116]:

$$\tau(g, a^{g \to g'}, g') = \prod_{i \in \mathtt{Agt}} \tau_i(l_i(g), a^{l_i(g) \to l_i(g')}, l_i(g')) \tag{2.6}$$

2.3.2 Discrete Time Markov Chains (DTMCs)

DTMCs are commonly used as models for probabilistic systems. A DTMC is a transition system that defines the probability of moving from one state to another.

Definition 2.1 (DTMC)**.** Given a set of atomic propositions AP, a DTMC can be defined as a 4-tuple $\mathbf{D} = (S, \bar{s}, \mathbf{P}, L)$ where:

- S is a nonempty and finite set of states;
- $\bar{s}$ is the initial state;
- $\mathbf{P} : S \times S \to [0,1]$ is the transition probability matrix, such that for every state $s \in S$, we have $\sum_{s' \in S} \mathbf{P}(s,s') = 1$;
- $L : S \to 2^{AP}$ is a labelling function which assigns to each state $s \in S$ the set $L(s)$ of atomic propositions that are valid in the state.

DTMCs are stochastic models of systems that change their states at discrete-times $(n = 0,1,2,\dots)$ and have the following property: if the system enters state s at time n, it stays there for exactly one unit of time and then jumps to state s' at time $n+1$ with probability $\mathbf{P}(s,s')$, regardless of its history up to and including time $n-1$ [71]. The definition shows that states are labelled with atomic propositions which indicate the status of the system (e. g., waiting, sending). The system can change its states according to a probability distribution given by the transition probability matrix $\mathbf{P}$. Each element $\mathbf{P}(s,s')$ of the transition probability matrix gives the probability of making a transition from state s to state s'. A transition from state s to s' can only take place if $\mathbf{P}(s,s') > 0$. However, if $\mathbf{P}(s,s') = 0$, no such transition is possible. Again, the probabilities from a given state must sum up to 1, i.e. $\sum_{s' \in S} \mathbf{P}(s,s') = 1$.

2.3.3 Markov Decision Processes (MDPs)

MDPs can be seen as transition systems in which in any state a nondeterministic choice between probability distributions exists.

Definition 2.2 (MDP)**.** Given a set of atomic propositions AP, an MDP model $\mathbf{M}$ can be defined as a 5-tuple, $\mathbf{M} = (\mathbb{S}, AC, \mathsf{P}_t, I_i, L)$, where:

- $\mathbb{S}$ is a nonempty and finite set of states.
- $\mathsf{P}_t : \mathbb{S} \times AC \times \mathbb{S} \to [0,1]$ is the transition probability function, such that for every state $s \in \mathbb{S}$ and action $\theta \in AC$, we have $\sum_{s' \in \mathbb{S}} \mathsf{P}_t(s, \theta, s') \in \{0,1\}$.
- AC is a set of actions. At state $s \in \mathbb{S}$, the action θ is enabled iff $\sum_{s' \in \mathbb{S}} \mathsf{P}_t(s, \theta, s') = 1$.
- I_i is an initial state.
- $L : \mathbb{S} \to 2^{AP}$ is a state labeling function.

MDPs possess the Markov property, which requires that any information necessary to predict the effects of all events is captured in the state. In other words, the effects of an event in a state depend only on that state and not on the prior history. However, the major difference between MDPs and DTMCs is the choice of actions. While a DTMC describes the state transitions of a stochastic system, it does not capture the fact that the agent can choose an appropriate course of action in order to change the system's state. However, for an MDP, at every state one or more actions are available, and each action is associated with a probability distribution over the successor states. That is, MDPs are not augmented with a unique probability measure. Reasoning about probabilities of sets of paths of an MDP relies on the resolution of the nondeterminism. In order to define the semantics of such an MDP, the notion of *adversary* is used. An adversary (also referred to as scheduler, policy, or strategy [4, 112]) is an entity that resolves the nondeterministic choices in MDPs. Being in a state of the system, an adversary determines the next step to be taken. Informally, at each step, the adversary picks an action, and then the next state is picked according to the probability distribution associated with the action. In our work, we focus on a special class of adversaries called *Memoryless Adversary* [43] where the choice of action depends only on the state and independent of what has happened in the history. An adversary is said to

be memoryless if it always selects the same action in a given state. The induced adversaries are basically DTMC models.

A partially observable Markov decision process (POMDP) is a variant of MDPs. Actually, a POMDP is an MDP in which the agent is unable to observe the current state. Instead, the agent must maintain a probability distribution over the set of possible states, based on a set of observations and observation probabilities, and the underlying MDP. A POMDP model [65] can be described as a tuple $(\mathrm{S}, \mathbb{A}, \mathrm{T}, \mathbf{R}, \Omega, \mathrm{O})$, where:

- S, $\mathbb{A}$, T, and **R** describe an MDP;
- Ω is a finite set of observations that the agent can experience of its world; and
- $\mathrm{O} : \mathrm{S} \times \mathbb{A} \to \prod(\Omega)$ is the observation function, which gives, for each action and resulting state, a probability distribution over possible observations.

2.4 System Specification

In this section, we describe some logics for specifying requirements of transition-based systems. The discussed logics use atomic propositions and connective operators to describe systems properties in states.

2.4.1 Temporal Logics

Temporal logic is a modal logic with modal operators to describe the temporal order of occurrence of events. The two commonly used temporal logics are Linear Temporal Logic (LTL) [91] and Computation Tree Logic (CTL) [38]. They differ from each other based on the way the notion of time is handled. LTL describes temporal relations on one execution path; whereas, in CTL it is possible to quantify over the paths with respect to a given state.

Below, we review the two logics and then review a probabilistic extension of CTL called PCTL [57].

a. LTL (Linear Temporal Logic)

In LTL, time is considered to be a linear sequence. Each moment in time has a unique possible future. Thus, temporal operators are provided for describing events along a single time line. The syntax of LTL is defined by the following BNF grammar [4]:

$$\varphi ::= true \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \bigcirc \varphi \mid \varphi \; U \; \varphi \mid$$

where: $p \in AP$ is an atomic proposition. $\bigcirc$ and U stand for "next time" and "until" respectively. The formula $\bigcirc\varphi$ holds at the current state if φ holds in the next state. The formula $\varphi U \psi$ holds at the current state, if there is some future moment for which ψ holds and φ holds at all moments until that future moment. $\Diamond\varphi$, which stands for eventually φ holds, can be derived using the U operator as follows: $\Diamond\varphi \equiv$ true U φ. Also, the $\Box\varphi$, which stands for "always φ, or globally φ", can be derived as follows: $\Box\varphi \equiv \neg\Diamond \neg\varphi$. The Boolean connectives $\neg$ and $\vee$ are defined in the usual way.

Semantics of LTL. Formulae of LTL stand for properties of paths. Therefore, a path can either satisfy an LTL-formula or not. Let $\mathbb{T} = (S, Act, \rightarrow, I, AP, \mathrm{L})$ be a transition system where S is a nonempty set of states, Act is a set of actions, $\rightarrow \subseteq S \times Act \times S$ is the transition relation, $I \subseteq S$ is a set of initial states, AP is a set of atomic propositions, and $\mathrm{L} : S \rightarrow 2^{AP}$ is a labeling function. Given $s, s' \in S$, $(s, s') \in \rightarrow$ means that s' is an immediate successor of s. A path π in $\mathbb{T}$ is an infinite sequence of states $\pi = (s_0, s_1, \ldots)$ such that $(s_i, s_{i+1}) \in \rightarrow$ for all $i \geq 0$. $\pi(i)$ is the $(i+1)$-th state in π, and $\pi_i = \pi(i), \pi(i+1), \ldots$ is the suffix of π starting at $\pi(i)$. The satisfaction of an LTL-formula φ with respect to the path π in the transition system $\mathbb{T}$ is denoted by $(\mathbb{T}, \pi) \models \varphi$, which is inductively defined as follows:

$- \; (\mathbb{T}, \pi) \models p \qquad iff \quad p \in \mathrm{L}(\pi(0)),$

$-\ (\mathbb{T},\pi) \models \neg\varphi \qquad iff \quad (\mathbb{T},\pi) \not\models \varphi,$

$-\ (\mathbb{T},\pi) \models \varphi_1 \wedge \varphi_2 \quad iff \quad (\mathbb{T},\pi) \models \varphi_1$ and $(\mathbb{T},\pi) \models \varphi_2,$

$-\ (\mathbb{T},\pi) \models \bigcirc\varphi \qquad iff \quad (\mathbb{T},\pi(1)) \models \varphi,$

$-\ (\mathbb{T},\pi) \models (\varphi_1\ U\ \varphi_2)$ *iff* $\exists\, k \geq 0$ such that $(\mathbb{T},\pi(k)) \models \varphi_2$ and $\forall\, 0 \leq i < k, (\mathbb{T},\pi(i)) \models \varphi_1.$

An LTL-formula φ holds at state s in the model $\mathbb{T}$, written $(\mathbb{T},s) \models \varphi$, iff all paths starting from s satisfy φ. Moreover, the model $\mathbb{T}$ satisfies φ iff φ holds in all paths emanating from an initial state. We say that φ is valid in $\mathbb{T}$, written $\models \varphi$ when for all $s \in S$, we have $(\mathbb{T},s) \models \varphi$.

b. CTL (Computation Tree Logic)

In contrast to LTL, CTL advocates a tree-like structure time, allowing some instants to have more than a single successor. Thus, it distinguishes between state formulae and path formulae. The syntax of CTL is given by the following BNF grammar [4]:

$$\varphi ::= true \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathrm{E}\psi \mid \mathrm{A}\psi$$

$$\psi ::= \bigcirc\varphi \mid \varphi\ U\ \varphi \mid$$

Intuitively, state formulae express a property of a state, while a path formulae express a property of a computation path where a computation path is an infinite sequence of states. $\bigcirc$ and U are defined as in LTL. Notice that, in CTL, a path quantifier (either A which stands for *all paths*, or E which stands for *some path*) is immediately followed by a single one of the usual linear temporal operators $\Box$, $\Diamond$, $\bigcirc$, or U in order to construct a well formed state formula.

Semantics of CTL. The semantics of CTL is given via the satisfaction relation "$\models$". Given a transition system $\mathbb{T} = (S, Act, \rightarrow, I, AP, \mathrm{L})$, where S is a nonempty set of states, Act is a set of actions, $\rightarrow \subseteq S \times Act \times S$ is the transition relation, $I \subseteq S$ is a set of initial states, AP is a set of atomic propositions, and $\mathrm{L} : S \rightarrow 2^{AP}$ is a labeling function. A path π in $\mathbb{T}$ is

also an infinite sequence of states $\pi = (s_0, s_1, \dots)$ such that $(s_i, s_{i+1}) \in \rightarrow$ for all $i \geq 0$. $\pi(i)$ is the $(i+1)$-th state in π, and $\pi_i = \pi(i), \pi(i+1), \dots$ is the suffix of π starting at $\pi(i)$. The set of paths starting at state s is denoted by $\Pi(s)$. The satisfaction relation $(\mathbb{T}, s) \models \varphi$, which means that the formula φ holds at the state s in the model $\mathbb{T}$, is defined inductively as follows:

$-\ (\mathbb{T}, s) \models p \qquad iff \quad p \in \mathrm{L}(s)$,

$-\ (\mathbb{T}, s) \models \neg\varphi \qquad iff \quad (\mathbb{T}, s) \not\models \varphi$,

$-\ (\mathbb{T}, s) \models \varphi_1 \wedge \varphi_2 \quad iff \quad (\mathbb{T}, s) \models \varphi_1$ and $(\mathbb{T}, s) \models \varphi_2$,

$-\ (\mathbb{T}, s) \models \exists\psi \qquad iff \quad (\mathbb{T}, \pi) \models \psi$ for some $\pi \in \Pi(s)$,

$-\ (\mathbb{T}, s) \models \forall\psi \qquad iff \quad (\mathbb{T}, \pi) \models \psi$ for all $\pi \in \Pi(s)$.

Like LTL, the satisfaction relation $\models$ for path formulae is defined by:

$-\ (\mathbb{T}, \pi) \models \bigcirc\varphi \qquad iff \quad (\mathbb{T}, \pi(1)) \models \varphi$,

$-\ (\mathbb{T}, \pi) \models (\varphi_1\ U\ \varphi_2)$ *iff* $\exists\, k \geq 0$ such that $(\mathbb{T}, \pi(k)) \models \varphi_2$ and $\forall\, 0 \leq i < k, (\mathbb{T}, \pi(i)) \models \varphi_1$.

State formula $\exists\psi$ is valid in state s if and only if there exists some path starting in s that satisfies ψ. In contrast, state formula $\forall\psi$ is valid in state s if and only if all paths starting in s satisfy ψ.

c. PCTL (Probabilistic Computation Tree Logic)

PCTL [57] is an extension of CTL with a probability operator. It is used to express properties of probabilistic systems. The syntax of PCTL is defined by the following BNF grammar [4]:

$$\varphi ::= true \mid p \mid \neg\varphi \mid \varphi \wedge \varphi \mid \mathbb{P}_{\bowtie k}(\psi)$$

$$\psi ::= \bigcirc\varphi \mid \varphi\ U\ \varphi \mid \varphi\ U^{\leq m}\ \varphi$$

where: $p \in AP$ is an atomic proposition and $\mathbb{P}_{\bowtie k}$ is a probabilistic operator. $\bowtie \in \{<, \leq, >, \geq\}$. $k \in [0,1]$ is a probability bound or threshold. $m \in \mathbb{N}^+$ is a positive integer number

reflecting the maximum number of transitions needed to reach a certain state. φ and ψ are state and path formulae respectively. $\bigcirc, U$ and $U^{\leq m}$ stand for "next time", "until" and "bounded until" path modal connectives respectively.

Semantics of PCTL. Given a probabilistic model such as a Markov chain $\mathbf{M} = (S, \mathtt{P}, I, AP, L)$ where S is a finite set of states, $\mathtt{P}$ is the transition probability matrix, $I \subseteq S$ is a set of initial states, AP is a set of atomic propositions, and $\mathrm{L} : S \rightarrow 2^{AP}$ is a labeling function. Let φ and ψ be PCTL state and path formulae respectively. The satisfaction relation $\models$ is defined for a PCTL state formula φ inductively as follows:

$-\ (\mathbf{M}, s) \models p \qquad iff \quad p \in \mathrm{L}(s),$

$-\ (\mathbf{M}, s) \models \neg\varphi \qquad iff \quad (\mathbf{M}, s) \not\models \varphi,$

$-\ (\mathbf{M}, s) \models \varphi_1 \wedge \varphi_2 \quad iff \quad (\mathbf{M}, s) \models \varphi_1 \text{ and } (\mathbf{M}, s) \models \varphi_2,$

$-\ (\mathbf{M}, s \models \mathbb{P}_{\bowtie k}(\psi) \quad iff \ Prob_s(\psi) \bowtie k, \text{where: } Prob_s(\psi) = Prob_s\{\pi \in \Pi(s) \mid \pi \models \psi\}.$

For a path $\pi \in \mathbf{M}$, the satisfaction relation is defined as follows:

$-\ (\mathbf{M}, \pi) \models \bigcirc\varphi \qquad iff \ (\mathbf{M}, \pi(1)) \models \varphi,$

$-\ (\mathbf{M}, \pi) \models \varphi_1\ U^{\leq m}\ \varphi_2 \quad iff \ \exists\, k \leq m \ \text{ s.t. } \ \pi(k) \models \varphi_2 \text{ and } \forall i < k, (\mathbf{M}, \pi(i)) \models \varphi_1,$

$-\ (\mathbf{M}, \pi) \models \varphi_1\ U\ \varphi_2 \qquad iff \ \exists\, m \geq 0 \ \text{ s.t. } \ (\mathbf{M}, \pi) \models \varphi_1\ U^{\leq m}\ \varphi_2.$

Combining Logics

Logic combination is emerging as a relevant research topic in many disciplines. Multi-modal logics can be constructed by combining existing logics in several ways [47]. In this thesis, we advocate the independent join (or fusion) technique [46]. 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 which extends the expressive power of each one?

The combination of two logics using this technique is denoted by $\mathbf{A} \oplus \mathbf{B}$. Given two

logics **A** and **B**, their languages $\mathscr{L}_{\mathbf{A}}$ and $\mathscr{L}_{\mathbf{B}}$, and their corresponding axiomatic systems $\mathscr{H}_{\mathbf{A}}$ and $\mathscr{H}_{\mathbf{B}}$, the logic $\mathbf{A} \oplus \mathbf{B}$ is the smallest logic with the following properties:

- The language of the combined logic is the union of $\mathscr{L}_{\mathbf{A}}$ and $\mathscr{L}_{\mathbf{B}}$.
- The resultant logic from the combination is axiomatised by the set of axioms $\mathscr{H}_{\mathbf{A}} \cup \mathscr{H}_{\mathbf{B}}$ which means that no "interaction" axiom is needed, i.e., axioms involving mixed operators are not necessarily required.

If $\mathscr{L}_{\mathbf{A}}$ and $\mathscr{L}_{\mathbf{B}}$ are interpreted in Kripke frames $\mathrm{F}_1 = (W, R_{11}, \ldots, R_{1n})$ and $\mathrm{F}_2 = (W, R_{21}, \ldots, R_{2m})$, the semantics of the combined logic $\mathbf{A} \oplus \mathbf{B}$ can be interpreted over the Kripke frame $\mathrm{F} = (W, R_{11}, \ldots, R_{1n}, R_{21}, \ldots, R_{2m})$ obtained by the "fusion" of the two frames F_1 and F_2. Using this technique ensures the preservation of important properties (such as soundness, completeness, and decidability, etc.) of the logics being combined as they are defined in the literature [69].

2.5 Model Checking

Verification is one of the important aspects of ACLs. Generally, for ACL standards to gain acceptance, it must be possible to determine whether or not any agent-based system that claims to conform to an ACL standard actually does so. An ACL is said to be verifiable if it enjoys this property [119, 121]. In this section, we review a verification technique, namely model checking, that is utilized in this research to verify our proposed logics.

Model checking is a formal, automatic technique to verify whether or not system design models satisfy given requirements [17, 22]. In other words, it is the problem of establishing whether or not a given formula φ is true in a given model M. Its value lies in its ability to verify various aspects (such as time, knowledge, commitments, etc) of target systems [69]. Typically, a model checking process involves three phases:

1. **Modeling:** To convert a design into a formalism so that mathematical computation and logical deduction can be performed.

2. **Specification:** To specify the properties that the model must satisfy.

3. **Verification:** To verify whether the model holds the specification.

Despite its success in verifying hardware and software systems from different domains, model checking is generally a resource-intensive process that requires a large amount of memory and processing time. This is essentially due to the fact that the systems' state space may grow exponentially with the number of variables combined with the presence of concurrent behaviors, which may hinder the verification process. This phenomenon is known as the *state explosion problem*. To alleviate this problem, several techniques have been explored in the literature [4]. Binary Decision Diagrams BDD, Partial Ordered Reduction, Compositional Reasoning, Symmetry and Induction are some well-known approaches. However, one of the most promising solutions aim at optimizing model checking algorithms by introducing symbolic data structures based on binary decision diagrams (BDDs) [22, 81]. Moreover, an ordered BDD (OBDD) is one which has an ordering for some list of variables. Model checking using BDDs is called *symbolic model checking*. It emphasizes that sets of states are represented symbolically. It is more efficient than using merely individual states. The idea is to represent states and set of states as Boolean Formulae which, in turn, can be readily encoded as BDDs. To elaborate, let $Sat(\varphi) = \{s \in S \mid M, s \models \varphi)$ be a set of states satisfying φ. Given a CTL formula φ and a CTL model $M = (S, R_t, V, I)$, the idea is to compute the set $Sat(\varphi)$ of states satisfying φ in M, which is represented in BDDs, and then compare it against the set of initial states I in M that is also represented in BDD. If I $\subseteq$ $Sat(\varphi)$, then the model M satisfies the formula φ; otherwise, a counter-example is generated to show the path in which the model does not satisfy the formula. This type of

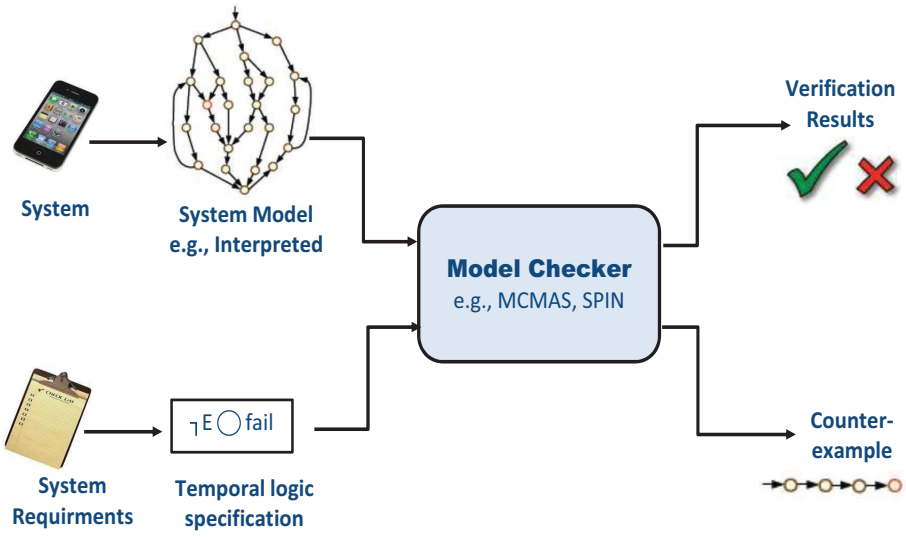

Figure 2.3: Qualitative model checking overview

model checking when the result is given as "Yes" or "No" (i. e. whether or not the property is satisfied) is called qualitative or non-probabilistic model checking. An overview of this type of model checking is given in Figure 2.3.

2.5.1 Probabilistic Model Checking

In addition to qualitative model checking, quantitative (or probabilistic) model checking techniques based on probabilistic model checkers have recently gained popularity [4]. Probabilistic model checking is an automatic formal verification technique for the analysis of systems exhibiting stochastic behavior [59]. It offers the capability for interpreting the satisfiability of a given property in terms of quantitative results. In fact, the probabilistic model checking technique is similar to conventional model checking as discussed earlier. The major difference is that a probabilistic model contains additional information on the likelihood of transitions between states, or to be more specific, it can model probabilistic behavior. An overview of the probabilistic model checking procedure is given in Figure 2.4. It shows that

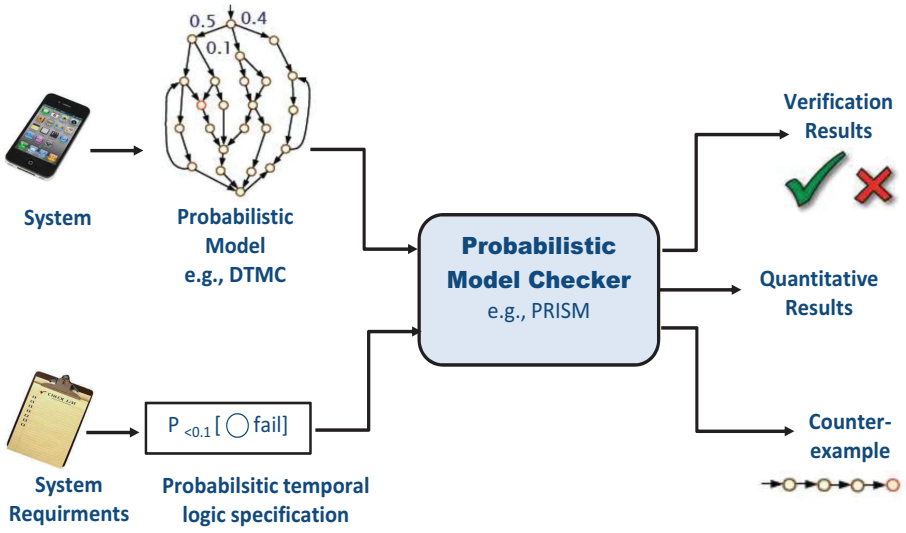

Figure 2.4: Probabilistic model checking overview

a probabilistic model checker takes as input a property and a model and delivers the result "Yes" or "No", or some probability.

2.5.2 Model Checking Tools

There have been various model checking tools (also known as Model Checkers) in the literature. In this section, we review some of the most widely used model checkers.

- **MCMAS**

  MCMAS (Model Checker for Multi-Agent Systems) [79] is an OBDD-based symbolic model checker developed for the purpose of verifying epistemic properties of multi-agent systems. It supports branching-time temporal logic CTL. It also supports interpreted systems as an underling formalism for modeling target systems. The dedicated programming language used for describing a MAS in MCMAS is called ISPL (Interpreted Systems Programming Language). MCMAS was originally designed to handle the logic of knowledge CTLK and the branching-time temporal logic CTL.

Recently, it has been extended by implementing some new algorithms that allow it to accept commitment formulae and hence to verify social commitments. The new extended version is called MCMASC (MCMAS for commitments). [37].

- **NuSMV**

  NuSMV [21], an extension version of SMV [81], is a well-known and widely trusted model checker. It is written in ANSI C language. As an input language, NuSMV accepts files written in SMV language. While the SMV tool was originally developed to implement the OBDD-based symbolic model checking for CTL, NuSMV implements also bounded model checking techniques for LTL – in addition to the symbolic model checking techniques for CTL. This feature distinguishes it the most from SMV. Nevertheless, both SMV and NuSMV allow for a compact description of systems under consideration using modules, which may be composed to describe the evolution of states.

- **SPIN**

  The SPIN [60] model checker is one of the most used tools for tracing software defects in concurrent system designs. It was introduced in the 1980s at Bell Labs. Later, it has been made available to the public. The original version of SPIN has been continually under development and improvement. SPIN's programming language is called PROMELA. [61] details the theoretical foundations of SPIN and presents the user manual. The main characteristics of SPIN are:

  ◇ It is designed for the temporal logic LTL.

  ◇ It is an automata-based model checker.

  ◇ It implements various optimization strategies, including on-the-fly model checking and partial order reduction.

- **PRISM**

  PRISM [73] stands for Probabilistic Symbolic Model Checker. It is the leading tool in the area of probabilistic model checking. The tool is widely used for checking probabilistic specifications over probabilistic models. The specifications can be expressed either in PCTL or in Continuous Stochastic Logic (CSL) [4, 43]. Systems models can be described using the PRISM language as Discrete-Time Markov Chains (DTMCs), Continuous-Time Markov Chains (CTMCs), or Markov Decision Processes (MDPs). PRISM has been successfully used to analyse systems with a wide range of application domains, including communication and multimedia protocols, randomised distributed algorithms, security protocols, and many others. PRISM is the most appropriate tool for our work thanks to its capability of verifying probabilistic properties, and accepting formulae written in PCTL. Using PRISM, it is possible to either determine if a probability satisfies a given bound or obtain the actual value.

- **MCK**

  MCK (stands for Model Checking Knowledge) is a model checker for the logic of knowledge, developed at the School of Computer Science and Engineering at the University of New South Wales [48]. It is implemented using OBDD-based symbolic algorithms. In the epistemic dimension, agents may use their observations in a variety of ways to determine what they know: observation alone, observation and clock, and perfect recall of all observations. The former way (observation alone) is to evaluate an agent's knowledge based merely on its current observation. The second way (observation and clock) is to compute an agent's knowledge based both on its current observation and the current clock value. The latter way (perfect recall of all observations) is to compute an agent's knowledge based on the complete record of all its observations.

In the temporal dimension, specification formulae may use either linear time temporal logic (LTL), or the branching-time logic (CTL). Recently, MCK was extended by Huang et al. [62] to permit the verification of knowledge in the presence of probabilistic behavior.

2.6 Summary

In this chapter, we introduced the background and concepts needed for the rest of my thesis. As social commitments are the main focus of this research, it is important, again, to emphasis that the notion of "social commitments" we consider in this thesis is the communicative social commitments that are public and observable. In the next chapter, we propose a new probabilistic approach for handling social commitments in the presence of uncertainty.

Chapter 3

Probabilistic Social Commitments

In this chapter[1], we establish a formal approach that allows us to precisely address probabilistic social commitments in MASs. The proposed approach is based on a new logic called the Probabilistic Computation Tree Logic of Commitments (PCTLC), or simply the Probabilistic Logic of Commitments. This logic is intended to be used for specifying, reasoning about, and verifying social commitments in the presence of uncertainty. PCTLC extends PCTL [57] with a commitment modality. We model MASs using a new version of interpreted systems that merges two extended versions of the original formalism namely, the probabilistic interpreted systems [55, 116], and the communicative interpreted systems [9, 34]. Finally, we propose a model checking technique for verifying PCTLC.

3.1 Introduction

In order to represent and reason about social commitments in MASs, commitment logics that extend CTL (Computation Tree Logic), LTL (Linear Temporal Logic), and CTL* (superset of CTL and LTL), have been proposed, see for example [13, 51, 90, 98, 113].

[1]The results of this chapter have been published in the journal of Applied Soft Computing [103], and in SoMet_13 [107].

However, current logics are merely related to specifying and verifying social commitments under the assumption of reliable behavior. That is, they assume an absolute, non-probabilistic running of systems under consideration. Unfortunately, this is not always the case. Heterogeneous and autonomous intelligent components in agent societies make it challenging to precisely analyze random or unreliable agent behaviors. This is because agents' actions are based on observing the environment changes and in many situations agents cannot observe all changes in the environment. Instead, each agent can only have a partial view of other agents' behaviors [75]. In such cases, agents make estimations about the observable world as part of their autonomous decision making processes. Moreover, when the system being modeled is an open system, i.e., interacts with an environment, then uncertainty in transitions may arise due to imperfect information about the environment [114]. Consequently, the problem of representing and verifying social commitments is made more complicated by the presence of transition 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. Moreover, from the communication perspective, commitments themselves are likely to be subject to probabilistic events. Xuan and Lesser [125] have highlighted some sources of uncertainty that make a commitment between two agents probabilistic:

1. The first source of uncertainty is related to the debtor's action(s). That is, debtor's action(s) might not always lead to the fulfilment of the commitment.

2. The second source comes from the agent decision processes. Debtors beliefs and desires might change such that continuing to pursue fulfilling the commitment for others becomes irrational. Debtors' beliefs about the commitment context include, for example, the degree that the agent to whom the commitment was made is still relying on its fulfillment. To the creditor, this can cause problems because its action(s)

may depend on the honoring of the commitment by the debtor.

3. The third form of uncertainty comes from the incomplete knowledge of the debtor about the creditor or about the environment within which the agent interacts.

Consequently, one cannot assume that all autonomous agents will behave as expected, and thus commitments among communicating parties cannot be treated under the assumption of certainty. Modeling uncertainty can be achieved using different tools including fuzzy logic as in [25, 66], and probabilities as in [41, 67, 89]. On the one hand, fuzzy logic is specifically designed to deal with imprecision of facts (or the membership in vaguely defined sets). Its use in MASs has been investigated by some researchers. In [49], the authors exploited fuzzy logic in designing intelligent agents that communicate with each other using a mental approach that uses KQML [42] as the underlying communication language. However, mental approaches suffer from the semantics verification problem [121]. That is, they cannot verify whether an agent is acting according to a given semantics or not [122]. In our work, we adopt social approaches that are based on observable social commitments.

On the other hand, probability is an important component in the design and analysis of complex systems across a broad spectrum of application domains, including communication and multimedia protocols, randomised distributed algorithms, security protocols, and dynamic power management. It is commonly used to model unreliable or unpredictable behavior. Probability deals with the chance of happening for an event or a condition (i.e., likelihood of some event or condition). Although probability has proven to be a powerful technique in handling different aspects of MASs [70, 116], its value in addressing social commitments for agent communication is yet to be investigated. In our research, we use probabilities to model the uncertainty because we are concerned with the likelihood of the fulfilment of the commitment. That is, when a social commitment between two agents takes place, we are interested to know about the chance of fulfilling that commitment at a certain

state in the system. Additionally, using probabilities to handle the uncertainty of social commitments provides us with the privilege of exploiting existing probabilistic logics and model checkers. However, it is worth mentioning that probability assignments are not the focus of this research. Probability values can be obtained from historical data using some techniques such as the algorithm proposed in [84] which allows us to compute the fixed probabilities between two states based on some other probabilities.

To motivate our study of modeling and verifying social commitments in the face of uncertainty, we use two situational examples that arise in practical settings such as web-based systems and mobile applications.

Example 1. Let us consider the Online Shopping System [52] which aims at providing services for purchasing online items. In the web-based Online Shopping System, customers can request to purchase one or more items from the supplier. Having selected an item, the customer commits towards the supplier to pay in order for the request to take place. Once the order is paid, the supplier confirms the order, and commits to deliver the requested item and enters a planned shipping date. Finally, when the order is shipped, the customer is notified. Because of the uncertainty associated to the underlying infrastructures of both commitments (i.e., the internet through which the payment is made and the transport system used for the delivery of purchased goods), there is no guarantee that these commitments will be fulfilled. Therefore, reasoning about and verifying the commitments to pay and to deliver have to be tackled with probability in mind so that the degree of fulfilling each commitment can be measured.

Example 2. In the field of mobile applications which are complex in nature, addressing social commitments should be paired with the consideration of uncertainty of transitions and commitments. Let us consider a simple scenario where a receiver agent and a sender agent have an agreement, in which the receiver agrees to pay the sender in return of the

delivery of a requested service. This can be represented as a social commitment, in which the receiver will be committed to the sender to pay upon obtaining the requested service. In such a scenario, because of the presence of stochastic behavior in mobile applications, the commitment to pay is not going to be surely satisfied.

The scenarios described above cannot be represented by existing conventional commitment logics because of the uncertainty aspect in both systems. Consequently, they cannot be verified. To cope with the situation, we need a probabilistic commitment logic that accounts for uncertainty, and a probabilistic model checking procedure to verify properties expressed in the new logic.

The ultimate objective of this chapter is to introduce a logical approach that is capable of addressing probabilistic social commitments in MASs. This is done as follows. First, we present a new probabilistic logic called PCTLC to express and reason about social commitments when uncertainty is a key factor. The introduction of PCTLC logic was driven by the fact that current probabilistic temporal logics such as PCTL [57] and PCTL* [3] consider neither commitments nor agent communication. PCTLC extends PCTL with modalities for commitments and their fulfillments. We model probabilistic MASs by a formalism resulted from extending the interpreted systems introduced by Fagin et al. [40]. This extension considers agents uncertainty and their communication abilities. Properties to be verified (i.e., social commitments) are specified using the probabilistic logic of commitment PCTLC. Second, we introduce a formal and automatic, probabilistic model checking technique for probabilistic commitment-based agent interactions. Our proposed verification method is a reduction-based model checking technique and consists of transforming the problem of model checking PCTLC into the problem of model checking PCTL [57] so that the use of PRISM is made possible. This reduction encompasses two main steps. In the first step, we devise a set of formal rules to transform the PCTLC model into an MDP model. Then, we

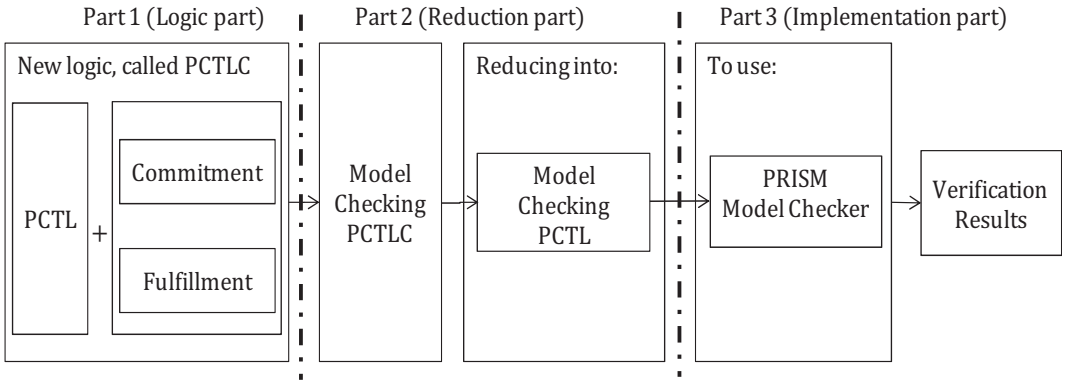

Figure 3.1: A schematic view of the probabilistic social commitment approach

reduce the MDP into DTMC to be as an input to the PRISM model checker. In the latter step, we transform PCTLC formulae into PCTL formulae based on some rules developed specifically for this purpose. As argued in [34], the main advantage of the reduction techniques compared to the direct ones is that they are easy to implement and allow the re-use of the existing model checkers. Third, we implement the proposed model checking approach on top of the PRISM model checker and then apply it on a concrete case study, namely Oblivious Transfer Protocol [92] from cryptography domain. Figure 3.1 gives an overview of the proposed approach.

3.2 The Probabilistic Logic of Commitments (PCTLC)

In this section, we present a new modal logic called the probabilistic logic of commitments (PCTLC) to address probabilistic social commitments in MASs. The logic we introduce extends the probabilistic branching-time logic PCTL [57] with a commitment modality. To do so, we merge two existing logic namely PCTL [57] and CTLC [9, 34] using the independent join technique [46]. The independent join combines logics as they are defined in the literature. Thus, it ensures the preservation of each logic's properties in the new logic.

Hereafter, we first present the syntax of our new logic, and then we define its semantics. Before going further, we define a new version of interpreted systems formalism with abilities to account for the uncertainty aspect in target MASs and to model the social interactions between communicating parties.

The PCTLC model is generated based on two extensions of the interpreted systems formalism [40] introduced in [9, 34], and [55, 116] as discussed in Chapter 2.

Definition 3.1 (Models)**.** Given a set of atomic propositions $AP = (p, q, r, \ldots)$, the model $\mathfrak{M}_1 = (S, I, \mathtt{P}, \{\sim_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, v)$ is a tuple where:

- $S \subseteq L_1 \times \ldots \times L_n$ 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.
- $\mathtt{P} : S \times S \to [0,1]$ is a total transition probability function defined as $\mathtt{P}(s,s') = \tau(s, a^{s\to s'}, s')$ iff there exists a joint action $a = (a_1, \ldots, a_n) \in ACT$ such that $\sum_{i\in \mathtt{Agt}} \tau_i(l_i(s), a^{l_i(s)\to l_i(s')}, l_i(s')) > 0$ and $\sum_{s'\in S} \mathtt{P}(s,s') = 1$ for all $s \in S$.
- For each pair $(i,j) \in \mathtt{Agt}^2$, $\sim_{i\to j} \subseteq S \times S$ is a social accessibility relation. $s \sim_{i\to j} s'$ is defined by the following conditions:
  1. $l_i(s) = l_i(s')$.
  2. $Var_i \cap Var_j \neq \emptyset$ such that $\forall x \in Var_i \cap Var_j$, we have $l_i^x(s) = l_j^x(s')$.
  3. $\forall y \in Var_j - Var_i$, we have $l_j^y(s) = l_j^y(s')$.
- $v : S \to 2^{AP}$ is a function valuating states with atomic propositions.

Our model $\mathfrak{M}_1$ can be thought of as a labeled state-transition system in which each transition from s to s' is annotated with a probability value in the matrix $\mathtt{P}$ indicating the likelihood

of its occurrence wherein the transition is assumed to take a discrete time-step. This means that there is no notion of real time, while reasoning about discrete time is possible through state variables keeping track of time and counting transition steps. It is also important to mention that every state in $\mathfrak{M}_1$ has at least one outgoing transition to avoid deadlocks. Moreover, all terminating/final states are modeled with a self-loop.

`Computation paths`. We can unfold the model $\mathfrak{M}_1$ into a set of paths. A path through the model $\mathfrak{M}_1$ is a non-empty (finite or infinite) sequence $\pi = s_0\ s_1\ \ldots$ of global states such that $\mathtt{P}(s_r, s_{r+1}) > 0$ for all $r \geq 0$. Also, $\pi(r)$ denotes the $(r+1)^{th}$ state of π, i.e., $\pi(r) = s_r$ for all $r \geq 0$.

`Probability Space`. Let Ω be a sample set (or the set of possible outcomes of an experiment). A pair (Ω, F) is said to be a *sample space* if F is a σ-algebra of measurable subsets of Ω, which are closed under countable union and complement and often built from basic events called *cylinders* (the elements of F are called *events*). A triple $(\Omega, \mathrm{F}, \mu)$ is a *probability space* if μ is a probability measure over F, i.e., $0 \leq \mu(A) \leq 1$ for all $A \in \mathrm{F}$ such that:

- $\mu(\emptyset) = 0$,
- $\mu(\Omega) = 1$, and
- $\mu(\bigcup_{k=1}^{\infty} A_k) = \Sigma_{k=1}^{\infty} \mu(A_k)$ for disjoint A_k.

The probability matrix `P` induces a probability space on the set of infinite paths $\Pi(s)$, which start in the state s, using the cylinder construction [4] as follows. An observation of a finite path determines a basic event (cylinder). Suppose $s = s_0$; for $\pi = s_0\ s_1\ \ldots\ s_n$, we

define the probability measure $Prob_s\{\pi\}$ for the π-cylinder as follows:

$$Prob_s\{\pi\} = \begin{cases} 1 \quad \text{if } \pi \text{ consists of a single state} \\ \prod_{r=0}^{n-1} \mathtt{P}(s_r, s_{r+1}) \quad \text{otherwise.} \end{cases} \tag{3.1}$$

This extends to a unique measure $Prob_s$ on the set of infinite paths $\Pi(s)$ w.r.t countable union and complement [74].

3.2.1 Syntax of PCTLC

Definition 3.2 (PCTLC syntax)**.** Given a set of atomic propositions AP, the PCTLC formulae are defined by the following BNF grammar:

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathscr{C} \mid \mathbb{P}_{\bowtie k}(\psi) \mid \mathbb{P}_{\bowtie k}(\mathscr{C})$$
$$\psi ::= \bigcirc\varphi \mid \varphi \; U \; \varphi \mid \varphi \; U^{\leq m} \; \varphi$$
$$\mathscr{C} ::= C_{i\to j}\varphi \mid Fu(C_{i\to j}\varphi)$$

where: $p \in AP$ is an atomic proposition and $\mathbb{P}_{\bowtie k}$ is a probabilistic operator where $\bowtie \in \{<, \leq, >, \geq\}$ and $k \in [0,1]$ is a probability bound or threshold. $m \in \mathbb{N}^+$ is a positive integer number reflecting the maximum number of transitions needed to reach a certain state. φ and ψ are state and path formulae interpreted over the states and paths of $\mathfrak{M}_1$ respectively. The Boolean connectives $\neg$ and $\vee$ are defined in the usual way. Formulae $\mathscr{C}$, called social formulae, are special state formulae in PCTLC that can express social properties using the modal connectives $C_{i\to j}$ and $Fu(C_{i\to j})$ standing for "commitment" and "fulfillment of commitment" respectively. $\bigcirc, U$ and $U^{\leq m}$ stand for "next time", "until" and "bounded until" path modal connectives respectively.

The intuitive meanings of the temporal and probabilistic operators are straightforward from PCTL [63]. $C_{i\to j}\varphi$ is read as "agent i commits towards agent j that φ". $Fu(C_{i\to j}\varphi)$ is read as "the commitment $C_{i\to j}\varphi$ is fulfilled". The probabilistic operator $\mathbb{P}_{\bowtie k}(\mathscr{C})$ on social formulae $\mathscr{C}$ states the degree of the commitment and the fulfillment of the commitment: how much the agent is confident about its commitment and fulfilling its commitment respectively.

PCTLC logic allows us to express properties like $C_{i\to j}\varphi \supset (\mathbb{P}_{\geq 0.95}(\top\, U^{\leq 13} Fu(C_{i\to j}\varphi)))$ which means when a commitment about φ is held, then the probability that the commitment is fulfilled within 13 discrete-time steps is at least 0.95, where $\supset$ stands for the logical implication.

3.2.2 Semantics of PCTLC

The semantics of our PCTLC is interpreted over the probabilistic model $\mathfrak{M}_1$ which was introduced above. Given a model $\mathfrak{M}_1 = (S, \mathtt{P}, I, \{\sim_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, \nu)$, then $(\mathfrak{M}_1, s) \models \varphi$ states that "a state s in the model $\mathfrak{M}_1$ satisfies the state formula φ, $(\mathfrak{M}_1, \pi) \models \psi$ means that "a path π in the model $\mathfrak{M}_1$ satisfies the path formula ψ, and $(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k}(\psi)$ means that "a state s in the model $\mathfrak{M}_1$ satisfies $\mathbb{P}_{\bowtie k}(\psi)$ if the probability of taking a path from s that satisfies ψ is in the interval specified by $\bowtie k$". When the model $\mathfrak{M}_1$ is clear from the context, we simply write the satisfaction relation $\models$ as follows: $s \models \varphi$ and $\pi \models \psi$. Furthermore, for a given pair $(i, j) \in \mathtt{Agt}^2$ of agents, we denote the number of accessible states s' from a given state s such that $s \sim_{i\to j} s'$ by $|s \sim_{i\to j} s'|$. The sample space of such pair of agents at s is the set of possible accessible states of (i, j) at s and is equal to $|s \sim_{i\to j} s'|$. We also define $|s \models \varphi|$ as follows:

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

Definition 3.3 (**Satisfaction**). Satisfaction of a PCTLC formula in the model $\mathfrak{M}_1$ is conductively defined as follows:

- For a non-probabilistic state formula:

  $s \models p$ *iff* $p \in \nu(s)$;

  $s \models \varphi_1 \vee \varphi_2$ *iff* $s \models \varphi_1$ or $s \models \varphi_2$;

  $s \models \neg\varphi$ *iff* $s \not\models \varphi$;

  $s \models C_{i\to j}\varphi$ *iff* $\forall s' \in S$ s.t. $s \sim_{i\to j} s'$, we have $s' \models \varphi$;

  $s \models Fu(C_{i\to j}\varphi)$ *iff* $\exists s' \in S$ s.t. $s' \sim_{i\to j} s$ and $s' \models C_{i\to j}\varphi$;

- For a path formula:

  $\pi \models \bigcirc\varphi$ *iff* $\pi(1) \models \varphi$;

  $\pi \models \varphi_1\ U^{\leq m}\ \varphi_2$ *iff* $\exists\, k \leq m$ s.t. $\pi(k) \models \varphi_2$ and $\forall i < k, \pi(i) \models \varphi_1$;

  $\pi \models \varphi_1\ U\ \varphi_2$ *iff* $\exists\, m \geq 0$ s.t. $\pi \models \varphi_1\ U^{\leq m}\ \varphi_2$;

- For a probabilistic operator working over a path formula:

  $s \models \mathbb{P}_{\bowtie k}(\psi)$ *iff* $Prob_s(\psi) \bowtie k$ where: $Prob_s(\psi) = Prob_s\{\pi \in \Pi(s) \mid \pi \models \psi\}$;

- For a probabilistic operator working over a social formula, where the set of events F is the set of states satisfying a formula, and assuming that the probabilities of accessible states from state s are equally distributed:

  $s \models \mathbb{P}_{\bowtie k}(C_{i\to j}\varphi)$ *iff* $Prob(s \models C_{i\to j}\varphi) \bowtie k$, where:

  $$Prob(s \models C_{i\to j}\varphi) = \frac{\sum_{s \sim_{i\to j} s'} |s' \models \varphi|}{|s \sim_{i\to j} s'|};$$

  $s \models \mathbb{P}_{\bowtie k}(Fu(C_{i\to j}\varphi))$ *iff* $Prob(s \models Fu(C_{i\to j}\varphi)) \bowtie k$, where:

  $Prob(s \models Fu(C_{i\to j}\varphi)) = Prob_s\{\pi \in \Pi(s') \mid s' \sim_{i\to j} s$ and $\pi = s' \ldots s$ and $s' \models C_{i\to j}\varphi\}$

Note that, the probabilistic commitment is computed based on the number of accessible states that satisfy the content over the whole number of accessible states, which reflects the uncertainty of the agent over the accessible states, so that over the commitment. On the other hand, probabilistic fulfillment 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 3.1.

If $(\mathfrak{M}_1, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to j}\varphi))$ *and* $(\mathfrak{M}_1, s) \models Fu(C_{i\to j}\varphi)$*, then the state s is not reachable from the commitment state.*

Theorem 3.1 (Probabilistic and Conventional Commitments Equivalences)**.**

1. $(\mathfrak{M}_1, s) \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi) \quad \textit{iff} \quad (\mathfrak{M}_1, s) \models C_{i\to j}\varphi$
2. $(\mathfrak{M}_1, s) \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi) \quad \textit{iff} \quad (\mathfrak{M}_1, s) \models C_{i\to j}\neg\varphi$
3. $(\mathfrak{M}_1, s) \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi) \quad \textit{iff} \quad (\mathfrak{M}_1, s) \models \neg C_{i\to j}\neg\varphi \wedge \neg C_{i\to j}\varphi$

Proof.

- First equivalence.

  "$\Longrightarrow$". Assume $s \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$. By the PCTLC semantics, it follows that $Prob(s \models C_{i\to j}\varphi) \geq 1$. Thus, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \geq 1$. This means that for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \models \varphi$, and hence $s \models C_{i\to j}\varphi$.

  "$\Longleftarrow$". Assume $s \models C_{i\to j}\varphi$. By the PCTLC semantics, it follows that for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \models \varphi$ (i.e. all accessible states from s satisfy φ). Consequently, $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = |s \sim_{i\to j} s'|$. Therefore, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \geq 1$ and hence, $s \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$.

- Second equivalence.

  "$\Longrightarrow$". Assume $s \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$. By the PCTLC semantics, it follows that $Prob(s \models C_{i\to j}\varphi) \leq 0$. Thus, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \leq 0$. Since the set of the accessible states from s is not empty, then $\sum_{s\sim_{i\to j}s'} |s' \models \varphi|$ must be 0 (i.e. φ is not true in any of the accessible states). Consequently, for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \not\models \varphi$, which means $s' \models \neg\varphi$. Hence, $s \models C_{i\to j}\neg\varphi$.

  "$\Longleftarrow$". Assume $s \models C_{i\to j}\neg\varphi$. By the PCTLC semantics, it follows that for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \not\models \varphi$. Since the set of the accessible states from s is not empty, then $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \leq 0$. Hence, $s \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$.

- Third equivalence.

  "$\Longrightarrow$". Assume $s \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$. By the PCTLC semantics, it follows that $0 < Prob(s \models C_{i\to j}\varphi) < 1$. Thus, $0 < \frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} < 1$. This means that it would never be the case that $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = |s \sim_{i\to j} s'|$ nor $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = 0$. Consequently, there exist some $s', s'' \in S$ such that $s \sim_{i\to j} s'$ and $s \sim_{i\to j} s''$ and $s' \models \varphi$ and $s'' \models \neg\varphi$. Hence, it is impossible to have $\bar{s} \models \neg\varphi$ or $\bar{s} \models \varphi$ for all $\bar{s} \in S$ such that $s \sim_{i\to j} \bar{s}$. Consequently, $s \not\models C_{i\to j}\neg\varphi$ and $s \not\models C_{i\to j}\varphi$. Hence $s \models \neg C_{i\to j}\neg\varphi$ and $s \models \neg C_{i\to j}\varphi$.

  "$\Longleftarrow$". Assume $s \models \neg C_{i\to j}\varphi$. By the PCTLC semantics, it follows that there exists $s' \in S$ such that $s \sim_{i\to j} s'$ and $s' \models \neg\varphi$. Consequently, it would never be the case that $s' \models \varphi$ for all $s' \in S$ such that $s \sim_{i\to j} s'$. Therefore, $1 > \frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|}$. Now assume $s \models \neg C_{i\to j}\neg\varphi$. Therefore, $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = 0$ would never be he case as some accessible states should satisfy φ. Consequently, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} > 0$. Thus, $0 < \frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} < 1$. Hence, $s \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$.

□

Theorem 3.2 (Probabilistic and Conventional Fulfillment Equivalences)**.**

1. $(\mathfrak{M}_1, s) \models \mathbb{P}_{>0}(Fu(C_{i\to j}\varphi))$ *iff* $(\mathfrak{M}_1, s) \models Fu(C_{i\to j}\varphi)$ *and* s *is reachable from the commitment state.*

2. $(\mathfrak{M}_1, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to j}\varphi))$ *iff* $(\mathfrak{M}_1, s) \models \neg Fu(C_{i\to j}\varphi)$ *or* s *is not reachable from the commitment state.*

Proof.

The proofs of these equivalences are direct from Proposition 3.1 and the above semantics.

□

3.3 Model Checking PCTLC using Reduction

When designing communicating agent-based systems that are complex, and stochastic in nature, formal verification is generally recognized as one of the best design support technologies, and a valuable tool towards having efficient systems in terms of ensuring the compliance of system design models against the given requirements.

Given a multi-agent system represented as a probabilistic interpreted system $\mathfrak{M}_1$ and a specification φ in PCTLC describing a desirable property, the problem of probabilistic model checking PCTLC can be defined as: 1) establishing whether or not $(\mathfrak{M}_1, I) \models \varphi$, i.e., if $I \in Sat(\varphi)$ where $Sat(\varphi)$=$\{s \in S \mid \mathfrak{M}_1, s \models \varphi\}$ is the set of states satisfying φ, 2) comparing the probability of satisfying φ with a probability threshold $\bowtie k$, where $Sat(\mathbb{P}_{\bowtie k}(\varphi)) = \{s \in S \mid Prob_s(\varphi) \bowtie k\}$, or 3) computing the probability of φ, $(\mathfrak{M}_1, s) \models \mathbb{P}_{=?}(\varphi)$. Note that answers to the second and third queries can be: (1) truth values, when the specification simply asks for a comparison to a probability threshold, or (2) quantitative, returning the actual probability.

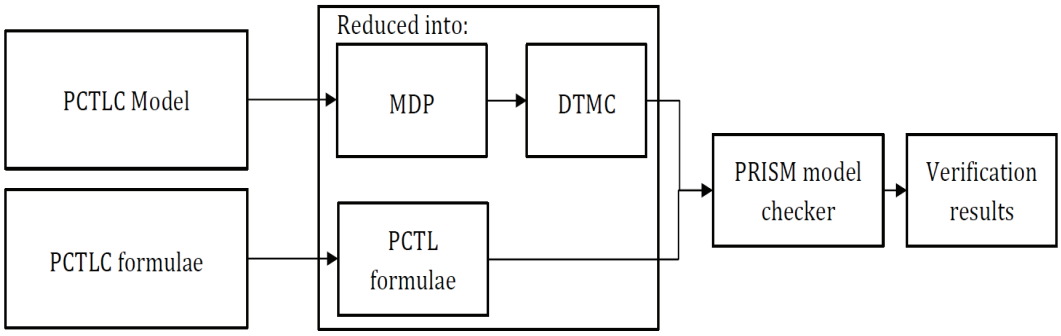

Figure 3.2: The proposed reduction technique of model checking PCTLC

Figure 3.2 depicts the workflow of our reduction technique. As mentioned before, the idea is to reduce the problem of probabilistic model checking PCTLC to the problem of probabilistic model checking PCTL in order to be able to use the PRISM model checker. Concretely, the proposed reduction technique consists of two processes (see Figure 3.2). In the former process, we transform our model $\mathfrak{M}_1$ into an MDP model. MDPs are the standard models for describing systems with probabilistic and nondeterministic behavior [93]. At every state of an MDP, one or more actions are available, and each action is associated with a probability distribution over the successor states. That is, MDPs are not augmented with a unique probability measure. Reasoning about probabilities of sets of paths of an MDP relies on the resolution of the nondeterminism. In order to define the semantics of such an MDP, as in [43], we use the notion of adversary to factor out the nondeterminism and consider the probability of some behavior of the MDP (i.e., allowing us to place a well-defined probability on the set of paths for each adversary). Informally, at each step, the adversary picks an action, and then the next state is picked according to the probability distribution associated with the action. In this work, we focus on a special class of adversaries called *Memoryless Adversary* where the choice of action depends only on the state and independent of what has happened in the history (i.e., which path led to the

current state). An adversary is said to be memoryless if it always selects the same action in a given state. The resulting adversaries are basically DTMC models for which we can define a 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 PCTLC formulae into PCTL formulae (see Section 3.3.2).

3.3.1 Transforming the Model $\mathfrak{M}_1$

Given $\mathfrak{M}_1 = (S, \mathtt{P}, I, \{\sim_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, v)$, and a PCTLC formula φ, we define an MDP model $\mathfrak{M}'_1 = \mathscr{H}(\mathfrak{M}_1)$ and PCTL formula $\mathscr{H}(\varphi)$ using the transformation function $\mathscr{H}$ such that $\mathfrak{M}_1 \models \varphi$ iff $\mathscr{H}(\mathfrak{M}_1) \models \mathscr{H}(\varphi)$. Recall that the model $\mathfrak{M}'_1$ is an MDP model $= (\mathbb{S}, AC, \mathsf{P}_t, I_i, L)$. Now, the model $\mathfrak{M}'_1$ can be defined using the function $\mathscr{H}$ as follows:

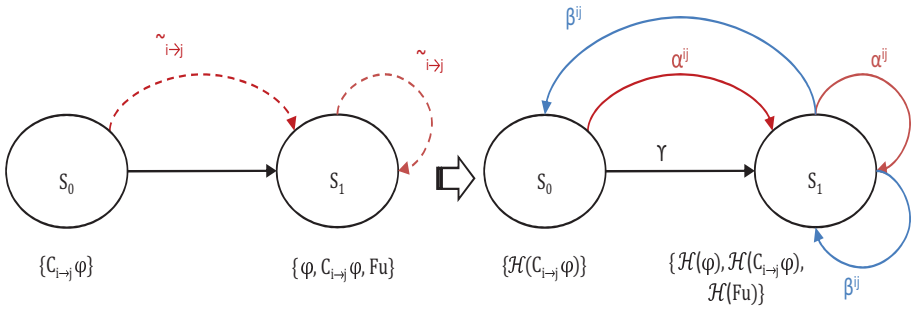

Figure 3.3: Translating relations in $\mathfrak{M}_1$ model into actions in the MDP model

- $\mathbb{S}$=S; I_i=I; L=v.
- The set of atomic action propositions AT is defined as follows:

  $AT = \{\varepsilon\} \cup \{\alpha_{1\to 1}, \alpha_{1\to 2}, \ldots, \alpha_{n\to n}\} \cup \{\beta_{1\to 1}, \beta_{1\to 2}, \ldots, \beta_{n\to n}\}$. Consequently, the set of actions $AC = \{\gamma\} \cup \{\alpha^{11}, \alpha^{12}, \ldots, \alpha^{nn}\} \cup \{\beta^{11}, \beta^{12}, \ldots, \beta^{nn}\}$ where n is the number of agents, $1 \leq i \leq n$, and $1 \leq j \leq n$. Actions γ, α^{ij}, and β^{ij} denote transitions

defined, respectively, from the probabilistic transition relation P, the accessibility relation $\sim_{i\to j}$, and the transition added when there exists a transition labeled with α^{ij} and needed to define the transformation of the formula $Fu(C_{i\to j})$. Note that, ε is the atomic action forming γ, $\alpha_{i\to j}$ is the atomic action forming α^{ij}, and $\beta_{i\to j}$ is the atomic action forming β^{ij}.

- P_t combines the probabilistic transition relations of P and the probabilistic relations obtained from translating accessibility relations $\sim_{i\to j}$ to transitions labeled with α^{ij} and probabilistic transitions labeled with β^{ij}. The probability of each transition labeled with α^{ij} is equal to the probability of each other transition labeled with α^{ij} emanating from the same state which is calculated by dividing one over the number of transitions labeled with α^{ij} (i.e., equal distribution). The probabilities of transitions labeled with β^{ij} are calculated in the same way. For states $s, s' \in \mathbb{S}$ and action $\theta \in AC$, the function P_t is defined as follows:

$$\mathsf{P}_t(s,\theta,s') = \begin{cases} \mathtt{P}(s,s'), & \text{if } \theta = \gamma \\ \frac{1}{|s\sim_{i\to j} s'|}, & \text{if } \theta = \alpha^{ij} \\ \frac{1}{|s'\sim_{i\to j} s|}, & \text{if } \theta = \beta^{ij}. \end{cases}$$

Now, we define three different adversaries as follows: σ_t to be used for interpreting temporal formulae, σ_c to be used for interpreting commitment formulae, and σ_{fu} to be used for interpreting fulfillment formulae. It is worth to mention that when defining σ_c and σ_{fu}, some rules need to be set. To define σ_c at a state, action α^{ij} has to be among the enabled actions at that state. Then, the memoryless adversary σ_c picks the action α^{ij} at this state, and γ at all other states. Meaning that, defining adversary σ_c at a state rather than a commitment state (the state where $C_{i\to j}\varphi$ holds) would not be possible. The same principle

applies to $\sigma_f u$. However, σ_t always picks action γ at every state in $\mathfrak{M}'_1$. The induced model of applying the adversary σ over $\mathfrak{M}'_1$ is a DTMC model.

Hereafter, we introduce our reduction rules that translate PCTLC formulae to PCTL formulae w.r.t a given adversary.

3.3.2 Reducing PCTLC Formulae into PCTL Formulae

Given the adversary σ_t, the PCTLC formulae are transformed inductively into PCTL as follows:

$\mathscr{H}(p) = p$, if p is an atomic proposition,

$\mathscr{H}(\neg\varphi) = \neg\mathscr{H}(\varphi)$,

$\mathscr{H}(\mathbb{P}_{\bowtie k}(\varphi \vee \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{H}(\varphi) \vee \mathscr{H}(\psi))$,

$\mathscr{H}(\mathbb{P}_{\bowtie k} \bigcirc \varphi) = \mathbb{P}_{\bowtie k} \bigcirc \mathscr{H}(\varphi)$,

$\mathscr{H}(\mathbb{P}_{\bowtie k}(\varphi\ U\ \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{H}(\varphi) U \mathscr{H}(\psi))$,

$\mathscr{H}(\mathbb{P}_{\bowtie k}(\varphi\ U^{\leq m}\ \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{H}(\varphi) U^{\leq m} \mathscr{H}(\psi))$,

It is important to note that, the social formulae $(C_{i\rightarrow j}, Fu)$ are not transformed into PCTL by making use of σ_t because σ_t does not capture the social accessibility relation and instead it captures only the temporal transitions at every state in the model $\mathfrak{M}'_1$.

Given the adversary σ_c, the PCTLC commitment formulae are transformed inductively into PCTL as follows:

$\mathscr{H}(C_{i\rightarrow j}\varphi) = \mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(\varphi))$,

$\mathscr{H}(\mathbb{P}_{\bowtie k} C_{i\rightarrow j}\varphi) = \mathbb{P}_{\bowtie k}(\bigcirc\mathscr{H}(\varphi))$,

The reason behind translating a commitment formula $C_{i\rightarrow j}\varphi$ to next operator $\bigcirc$ followed by $\mathscr{H}(\varphi)$ is that by having transformed the social accessibility relation $\sim_{i\rightarrow j}$ into a transition labeled with action α^{ij}, it is obvious that all next states of the commitment state through the transition labeled with α^{ij} satisfy $\mathscr{H}(\varphi)$ (see Figure 3.3). Hence, with respect

to σ_c, which is a DTMC model that ignores all transitions at the commitment state except those labeled with α^{ij}, we clearly see that the commitment state is converted into a state whose all successor states satisfy $\mathscr{H}(\varphi)$.

Given the adversary σ_{fu}, the PCTLC fulfillment formulae are transformed inductively into PCTL as follows:

$$\mathscr{H}(Fu(C_{i\to j}\varphi)) = \mathbb{P}_{>0}(\bigcirc\mathscr{H}(C_{i\to j}\varphi)) = \mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(\varphi))),$$

$$\mathscr{H}(\mathbb{P}_{\bowtie k}Fu(C_{i\to j}\varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc\mathscr{H}(C_{i\to j}\varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(\varphi))).$$

$Fu(C_{i\to j}\varphi)$ is transformed to next operator $\bigcirc$ followed by $\mathscr{H}(C_{i\to j}\varphi)$ because w.r.t σ_{fu}, there exists a state next to the fulfillment state in which $\mathscr{H}(C_{i\to j}\varphi)$ holds. Notice that the added transitions, labeled with β^{ij}, always go from the fulfillment state to a state where $\mathscr{H}(C_{i\to j}\varphi)$ is satisfied (they go either to the commitment state or to the fulfilment state itself where in both states the formula $\mathscr{H}(C_{i\to j}\varphi)$ holds). This can be easily seen in Figure 3.3. Indeed, this intuitively complies with the fact that for a commitment to be fulfilled, the commitment itself has to be created before and still alive at the moment of fulfilling it (i.e., at the fulfillment state).

Theorem 3.3 (Satisfaction Equivalence)**.**

Let σ_t, σ_c, and σ_{fu} be the DTMC models corresponding to the adversaries that capture respectively temporal formulae, commitment formulae, and fulfillment formulae. The following equivalences hold:

$(\mathfrak{M}_1, s) \models p$ *iff* $(\sigma_t, s) \models p$

$(\mathfrak{M}_1, s) \models \neg\varphi$ *iff* $(\sigma_t, s) \models \neg\mathscr{H}(\varphi)$

$(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k}(\varphi \vee \psi)$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}\mathscr{H}(\varphi) \vee \mathbb{P}_{\bowtie k}\mathscr{H}(\psi)$

$(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k}\bigcirc\varphi$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}\bigcirc\mathscr{H}(\varphi)$

$(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k}(\varphi\ U\ \psi)$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}(\mathscr{H}(\varphi)\ U\ \mathscr{H}(\psi))$

$(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k}(\varphi\ U^{\leq m}\ \psi)$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}(\mathscr{H}(\varphi)\ U^{\leq m}\ \mathscr{H}(\psi))$

$(\mathfrak{M}_1, s) \models C_{i\to j}\varphi$ *iff* $(\sigma_c, s) \models \mathbb{P}_{\geq 1}(\bigcirc \mathscr{H}(\varphi))$

$(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k} C_{i\to j}\varphi$ *iff* $(\sigma_c, s) \models \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{H}(\varphi))$

$(\mathfrak{M}_1, s) \models Fu(C_{i\to j}\varphi)$ *iff* $(\sigma_{fu}, s) \models \mathbb{P}_{>0}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{H}(\varphi)))$

$(\mathfrak{M}_1, s) \models \mathbb{P}_{\bowtie k} Fu(C_{i\to j}\varphi)$ *iff* $(\sigma_{fu}, s) \models \mathbb{P}_{\bowtie k}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{H}(\varphi))$

This theorem emphasizes that each formula has to be associated with an adversary (i.e., a DTMC model) over which the formula can be interpreted. The proof of the theorem with regard to PCTL formulae is straightforward as PCTL formulae are also PCTLC formulae. For commitment formulae, the proof is given in Theorem 3.4 that discusses the soundness of the transformation rules.

Theorem 3.4 (Soundness and Completeness of $\mathscr{H}$)**.** *Let $\mathfrak{M}_1$ and Φ be respectively a PCTLC model and formula and let $\mathscr{H}(\mathfrak{M}_1)$ and $\mathscr{H}(\Phi)$ be the corresponding model and formula in PCTL. We have $\mathfrak{M}_1 \models \Phi$ iff $\mathscr{H}(\mathfrak{M}_1) \models \mathscr{H}(\Phi)$.*

Proof. Our aim here is to prove that the proposed reduction technique is sound (i.e., the necessary condition) and complete (i.e., the sufficient condition). We prove this by induction on the structure of the formula Φ. The case of PCTLC formulae that are also PCTL formulae is straightforward. In what follows, we analyze two cases: $\Phi = C_{i\to j}\varphi$ and $\Phi = Fu(C_{i\to j}\varphi)$.

- $\Phi = C_{i\to j}\varphi$. We have $(\mathfrak{M}_1, s) \models C_{i\to j}\varphi$ iff $(\mathfrak{M}_1, s') \models \varphi$ for every $s' \in S$ such that $s \sim_{i\to j} s'$. Consequently, $(\mathfrak{M}_1, s) \models C_{i\to j}\varphi$ iff $(\mathfrak{M}'_1, s') \models \mathscr{H}(\varphi)$ for every $s' \in \mathbb{S}$ such that $(s, \alpha^{ij}, s') \in \mathsf{P}_t$. Now, w.r.t the adversary σ_c that is defined to interpret commitment formulae over $\mathfrak{M}'_1$, every infinite path $\pi \in \Pi^{\sigma_c}(s)$ satisfies that $\pi(1) = s'$ and $(\mathfrak{M}'^{\sigma_c}_1, \pi(1)) \models \mathscr{H}(\varphi)$. Then, $(\mathfrak{M}'^{\sigma_c}_1, s) \models \bigcirc \mathscr{H}(\varphi)$ for all $\pi \in \Pi^{\sigma_c}(s)$. As the path quantifier A is not defined in PCTL, and we have $\mathbb{P}_{\geq 1}$ (weaker than A) instead, so we obtain $(\mathfrak{M}'^{\sigma_c}_1, s) \models \mathbb{P}_{\geq 1}(\bigcirc \mathscr{H}(\varphi))$.

- $\Phi = Fu(C_{i\to j}\varphi)$. We have $(\mathfrak{M}_1, s) \models Fu(C_{i\to j}\varphi)$ iff there exists $s' \in S$ such that $s' \sim_{i\to j} s$ and $(\mathfrak{M}_1, s') \models C_{i\to j}\varphi$. Consequently, $(\mathfrak{M}_1, s) \models Fu(C_{i\to j}\varphi)$ iff there exists $s' \in \mathbb{S}$ such that $(s, \beta^{ij}, s') \in \mathsf{P}_t$ and $(\mathfrak{M}'_1, s') \models \mathscr{H}(C_{i\to j}\varphi)$. Now, w.r.t the adversary σ_{fu} which is defined to interpret fulfillment formulae over $\mathfrak{M}'_1$, we obtain at least one infinite path $\pi \in \Pi^{\sigma_{fu}}(s)$ that satisfies $\pi(1) = s'$ and $(\mathfrak{M}'^{\sigma_{fu}}_1, \pi(1)) \models \mathscr{H}(C_{i\to j}\varphi)$. Since E is equivalent to $\mathbb{P}_{>0}$ and $\mathscr{H}(C_{i\to j}\varphi)$ is equivalent to $\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(\varphi))$, so we obtain $(\mathfrak{M}'^{\sigma_{fu}}_1, s) \models \mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(\varphi)))$.

□

3.4 Implementation

In this section, we apply our model checking approach on Oblivious Transfer Protocol [92]. For the purpose of providing experimental results demonstrating the effectiveness and efficiency of our reduction technique, we verify some properties of oblivious transfer protocol, expressed originally in PCTLC logic.

3.4.1 Oblivious Transfer Protocol

Oblivious transfer protocol was introduced in cryptography to allow a sender to send some information to a receiver in such a way that the sender remains oblivious to what is received. We study the oblivious transfer protocol due to Rivest [92] in which the sender (Alice) has two secret values m_0 and m_1. The receiver (Bob) would like to know one of the two values without telling Alice which value he learned. This protocol has been the subject of analysis for some probabilistic properties [62]. Rivest's solution uses a trusted initializer (Ted) who participates only in the initial setup to help both agents by providing them with some random material. The random material includes two random strings (r_0 and r_1) — with the same length as Alice's messages— to be sent to Alice in the setup phase. Then, Ted

flips a bit (d) and sends it to Bob along with a random string rd. Now, for Bob to request mc ($c = 0$ or 1), he sends Alice the bit $e = c \oplus d$ ($\oplus$ is the exclusive OR logical gate: it takes as input two bits and its output is 0 if the two bits are equal, and 1 otherwise). Then, Alice responds with the values $f_0 = m_0 \oplus r_e$ and $f_1 = m_1 \oplus r_{1-e}$. Upon receiving f_0 and f_1, Bob can compute $mc = f_c \oplus rd$. Having done so, Alice will have no idea as to which message Bob chose, and Bob will have learned nothing about m_{1-c} (Alice's other message).

In order to use the PRISM model checker to verify and analyze *Oblivious Transfer Protocol*, the latter has to be encoded into the PRISM input language. Simply, we treat the *Sender* (Alice) and *Receiver* (Bob) in the protocol as agents. Then, each agent is translated into a *module* in the PRISM language. Moreover, each agent is comprised of variables that determine its local states. For example, Bob's variables are: bool *S_req*: send request, bool *R_ack*: receive acknowledgement, bit d: 0 or 1, bit c: 0 or 1, bit e: 0 or 1, bool *S_e*: send bit e, string *rd*: random variable obtained form Ted in the initial setup, *R_f*: receive f_0 and f_1. The global model is obtained by the synchronization between all modules (agents).

3.4.2 Oblivious Transfer Protocol Properties

One of the main motivations of this chapter is to verify properties expressed as PCTLC formulae. Gurin and Pitt [53] expressed that verifying protocol properties can be performed at design time. This kind of verification aims to prove that some property will hold for all the interactions that correctly follow the protocol. Our proposed model checking technique mainly accommodates compliance by design-time verification of interaction properties. In fact, there have been various catalogs of properties proposed in the literature [11, 19, 27]. In our work, we check *safety*, *Liveness*, and *reachability* properties in the Oblivious Transfer Protocol as they are popular examples of protocol properties. These properties reflect some requirements of the oblivious transfer protocol that have to be met.

- `Property 1: Safety` "Something bad will never occur".

  This property can be generally expressed in CTL by the formula $A\Box\neg p$ which is equivalent to $\mathbb{P}_{\geq 1}(\Box\neg p)$ in PCTLC where p represents a bad situation. Such bad situations include, for example, when Alice fulfills her commitment of using the bit e (received from Bob) along with the random variables r_0, r_1 (obtained from Ted in the initial setup) for calculating f_0 and f_1, but Bob does not use the random variable rd to compute his requested value mc. This bad situation can be avoided using PCTLC as follows:

  $$\varphi_1 = \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond Fu(C_{A\rightarrow B}(use - e)) \wedge \mathbb{P}_{\geq 1}\Box\neg(use - rd)]$$

- `Property 2: Liveness` "Something good will eventually happen".

  This property expresses that some good situation will eventually occur. For example, in all computation paths it is always the case that if Alice fulfills her commitment of using the bit e and the random strings r_0, r_1 for calculating and delivering f_0 and f_1, then in all paths in the future Bob can use f_0 and f_1 to compute his requested value mc. This can be expressed as follows:

  $$\varphi_2 = \mathbb{P}_{\geq 1}\Box[\mathbb{P}_{>0}\Diamond Fu(C_{A\rightarrow B}(use - e)) \supset \mathbb{P}_{\geq 1}\Diamond(comp - mc)]$$

- `Property 3: Reachability` "Some particular situation can be reached".

  This property comes in the form $E\Diamond p$ which is equivalent to $\mathbb{P}_{>0}\Diamond p$ in PCTLC where p is the situation that needs to be reached. For example, once Alice commits towards Bob to use the bit e in calculating f_0 and f_1, there should be a possibility from the initial state for Alice to eventually reach the fulfillment state where she can fulfill her commitment towards Bob. This property can be expressed as follows:

  $$\varphi_3 = \mathbb{P}_{>0}\Diamond Fu(C_{A\rightarrow B}(use - e))$$

Table 3.1: Verification results of the oblivious transfer protocol

Exp.#	#Agents	#States	#Transitions	Const. Time (s)
Exp.1	2	25	75	0.016
Exp.2	4	625	3125	0.047
Exp.3	6	$1.6*10^4$	$1.1*10^5$	0.079
Exp.4	8	$3.9*10^5$	$3.5*10^6$	0.188
Exp.5	10	$9.7*10^6$	$1.1*10^8$	0.344
Exp.6	12	$2.4*10^8$	$3.1*10^9$	0.547
Exp.7	14	$6.1*10^9$	$9.2*10^{10}$	0.859
Exp.8	16	$1.5*10^{11}$	$2.6*10^{12}$	1.11
Exp.9	18	$3.8*10^{12}$	$7.2*10^{13}$	1.5
Exp.10	20	$9.5*10^{13}$	$2*10^{15}$	2.531
Exp.11	22	$2.3*10^{15}$	$5.5*10^{16}$	3.531
Exp.12	24	$6*10^{16}$	$1.5*10^{18}$	5.609

3.4.3 Experimental Results

We have carried out 12 experiments. Our experiments were performed on a Dell laptop equipped with 32-bit Windows XP with 4 GB of RAM and Genuine Intel(R) CPU at 2.4 GHz. Table 3.1 reports the results of the performed experiments wherein (Exp.#) denotes the experiment number, (#Agent) denotes the number of agents, (#States) denotes the number of reachable states, (#Transitions) denotes the number of transitions, and (Construction Time) denotes the time needed for building the simulated model in seconds. We started our experiments with only two agents; Alice (sender) and Bob (Receiver). In this interaction, Bob requests a value (information) from Alice and then Alice responses to Bob and sends him the requested value in such a way that both agents respect the rules of the protocol for encrypting and decrypting the information.

In the second experiment, we added two more agents (receivers) who also request some values from Alice. For the rest of the experiments, each time we add two more agents (receivers) till we reach the maximum number of agents (24 agents) with which we can

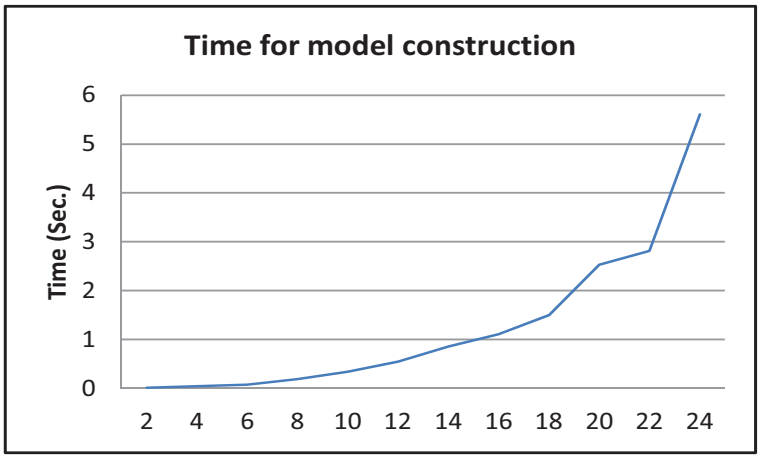

Figure 3.4: Model construction time for oblivious transfer protocol

successfully build the model.

In every experiment, we monitor the changes occurring in (#States), (#Transitions), and (Construction Time) respectively. From Table 3.1, we notice that the state space (represented in terms of reachable states) increases exponentially as the number of agents increases (cf. Figure 3.4). Likewise, the number of transitions also increases exponentially as more agents are added. However, the time (in seconds) needed for building the model increases polynomially, which shows the effectiveness of our model checking approach when the system scales up (about $6 * 10^{16}$ states). The cause of this time increase in building the model when more agents are added is that the number of reachable states and the size of the model are increased. Moreover, the more we become closer to the state explosion point as in experiments 20, 22, and 24, the higher time is need for building the model. This reflects the fact that the model size in these experiments turns out to be much bigger.

It is worth noticing that starting from experiment #2 we re-write the desirable properties φ_1, φ_2, and φ_3 in a parameterized form, as follows (n is the number of agents in the experiment):

$$\varphi_1' = \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond \bigwedge_{i=1}^{n} Fu(C_{A\rightarrow B_i}(use - e_i)) \wedge \mathbb{P}_{\geq 1}\Box\neg(use - rd_i)]$$

$$\varphi_2' = \mathbb{P}_{\geq 1}\Box[\mathbb{P}_{>0}\Diamond \bigwedge_{i=1}^{n} Fu(C_{A\rightarrow B_i}(use - e_i)) \supset \mathbb{P}_{\geq 1}\Diamond(comp - mc_i)]$$

$$\varphi_3' = \mathbb{P}_{>0}\Diamond \bigwedge_{i=1}^{n} Fu(C_{A\rightarrow B_i}(use - e_i))$$

However, for the purpose of model checking using our reduction technique, every defined formula needs to be transformed according to the reduction rules presented in Section 3.3.2. Below we show the transformed forms of φ_1, φ_2, and φ_3 respectively in the case of two agents (i.e., experiment #1).

$$\mathscr{H}(\varphi_1) = \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond\mathscr{H}(Fu(C_{A\rightarrow B}(use - e))) \wedge \mathbb{P}_{\geq 1}\Box\neg\mathscr{H}(use - rd)].$$

$$= \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond(\mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(use - e)))) \wedge \mathbb{P}_{\geq 1}\Box\neg\mathscr{H}(use - rd)].$$

$$= \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond(\mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc(use - e)))) \wedge \mathbb{P}_{\geq 1}\Box\neg(use - rd)].$$

$$\mathscr{H}(\varphi_2) = \mathbb{P}_{\geq 1}\Box[\mathbb{P}_{>0}\Diamond\mathscr{H}(Fu(C_{A\rightarrow B}(use - e))) \supset \mathbb{P}_{\geq 1}\Diamond\mathscr{H}(comp - mc)].$$

$$= \mathbb{P}_{\geq 1}\Box[\mathbb{P}_{>0}\Diamond(\mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(use - e)))) \supset \mathbb{P}_{\geq 1}\Diamond\mathscr{H}(comp - mc)].$$

$$= \mathbb{P}_{\geq 1}\Box[\mathbb{P}_{>0}\Diamond(\mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc(use - e)))) \supset \mathbb{P}_{\geq 1}\Diamond(comp - mc)].$$

$$\mathscr{H}(\varphi_3) = \mathbb{P}_{>0}\Diamond\mathscr{H}(Fu(C_{A\rightarrow B}(use - e))).$$

$$= \mathbb{P}_{>0}\Diamond[\mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{H}(use - e)))].$$

$$= \mathbb{P}_{>0}\Diamond[\mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc(use - e)))].$$

Table 3.2 shows the results in terms of verification time (in seconds) of model checking the above defined properties when the number of agents varies from a simple interaction scenario of two agents to more complicated scenarios of 24 agents. The total execution time can be easily obtained by summing up the construction time to build the simulated model reported in Table 3.1 and the verification time of the considered formulae. For instance, in Exp. 12 with 24 agents, the total execution time of verifying φ_1, φ_2, and φ_3 is $5.609 + 2.609 + 2.453 + 2.118 = 12.789$ s.

Notice that the three properties hold in all conducted experiments, meaning that our approach is successful in expressing and verifying system properties using PCTLC. Clearly,

Table 3.2: Results of model checking some properties for Oblivious Transfer Protocol

Exp.#	#Agents	Time for MC φ_1	Time for MC φ_2	Time for MC φ_3
1	2	<0.001	<0.001	<0.001
2	4	0.015	0.016	0.015
3	6	0.032	0.031	0.032
4	8	0.046	0.047	0.062
5	10	0.078	0.093	0.078
6	12	0.11	0.141	0.172
7	14	0.203	0.188	0.219
8	16	0.359	0.328	0.343
9	18	0.453	0.403	0.5
10	20	1.062	0.797	0.719
11	22	1.813	1.125	1.106
12	24	2.609	2.453	2.118

as depicted in Figure 3.5, the time for model checking the three properties is similar which increases polynomially till we reach the case of 20 agents then it grows up dramatically. However, these results demonstrate the scalability of our reduction-based model checking technique to verify commitments and their fulfilments in uncertain setting for agent communication.

3.5 Related Work

The work of this chapter is related to a number of other proposals in the literature. In this section, we give a brief overview of the most relevant ones.

3.5.1 Adding Commitment Operators to Existing Logics

Singh in [98] extends CTL logic by adding operators for social commitments, beliefs, and intentions in order to formally model the interactions between interacting parties in a MAS. By doing so, he was able to develop a specification language for commitment-based protocols. The author defines three different accessibility relations to intuitively capture the

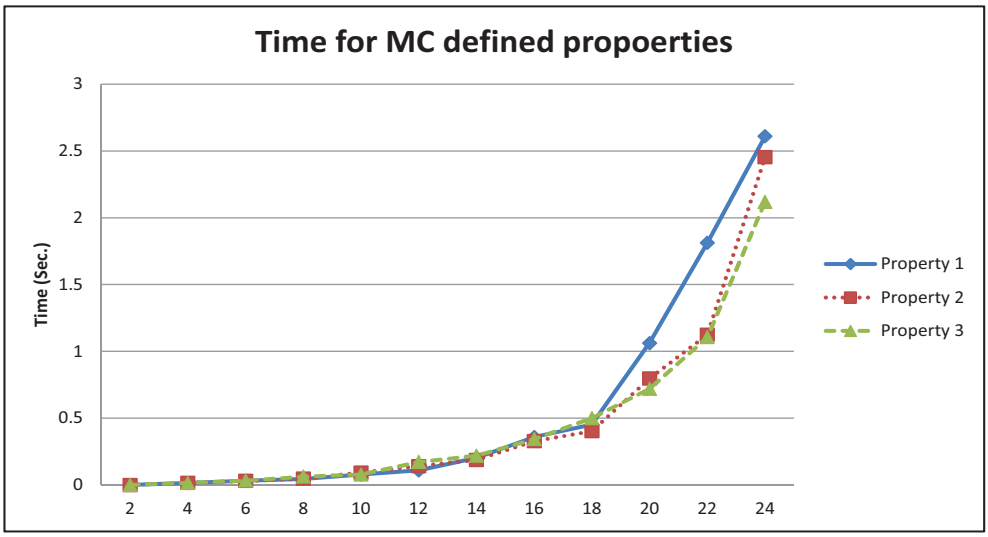

Figure 3.5: Time for model checking some properties for oblivious transfer protocol

meaning of the new modalities. With respect to the commitment, the author claims that a commitment is satisfied at a certain state if and only if the content of the commitment is true along all accessible paths defined using an accessibility relation and emanating from the commitment state (the state where the commitment holds). Though the author claims that the proposed semantics is verifiable, no concrete approach for verifying or model checking the semantics is presented.

Bentahar and his colleagues in [13, 14] present an approach that extends CTL* with an operator for commitments and their actions, and two operators for argument and dynamic logic respectively. To define a semantics for the commitment modality, they present a new definition for the accessibility relations. Moreover, their semantics is defined in terms of the computations (paths) along which the commitment is satisfied.

Cheng in [19] introduce a model checking method using the SPIN model checker (Simple Promela Interpreter [60]) to verify commitment-based business protocols and their compositions based on LTL logic. In this method, commitments are not expressed directly

in the logic as we propose in our work. Instead, they are simply abstracted as variables. Consequently, the intrinsic meaning of commitments is not captured.

In [27], Desai and his group highlight some protocol properties and classify them into general properties and protocol-specific properties in order to verify the correctness of commitment protocols. The presented properties are defined in terms of Propositional Linear Temporal logic (LTL). Then, they outline a technique for verifying commitment protocols and their compositions against these properties. The proposed approach involves using the SPIN model checker as a tool for the formal verification. Among the general properties that they are successfully able to verify are the deadlocks (which may result from the contradictory between the axioms used in protocol composition) and livelocks properties. As in [19], commitments are simply abstracted using variables.

El-Menshawy and his colleagues in [32] tried to overcome the limitations raised in [13, 14]. They propose a new logical language called CTL^{*sc} to develop a specification language for commitment-based protocols. Their new logic extends CTL* with commitments and their associated actions. Furthermore, they extend the temporal modalities of CTL* with past-directed temporal modalities. The semantics of actions is not defined in a recursive way as in [13, 14], i.e., the semantics of each action does not depend on other actions. Based on their new logic, the authors develop a Social Negotiation Protocol (SNP) that merges a set of dialogue games, commitment actions and dialogue actions. Then, they present an automatic verification technique to verify the SNP using symbolic model checking in which they verified some given properties such as Reachability, Safety, and Liveness. They implemented their proposed verification technique using the NuSMV[21] and MCMAS[79] symbolic model checkers. Their experimental results show the ability of the proposed approach to handle large state spaces of 10^{16}. However, the work does not consider the uncertainty issue associated with the protocol.

In a later work, El-Menshawy et al. [36] defined a new temporal logic called CTLC by extending CTL with operators for social commitments and their fulfilments and violations. In terms of defining CTLC, their main contribution is the definition of a new social accessibility relation. They define a new accessibility relation in which they assume the existence of an intermediate state between the commitment state and the fulfillment state. The debtor, in their accessibility definition, is uncertain about the current state so he looks for the intermediate state (different from the current state) in which it does not matter for him being in the commitment state, the intermediate state, or the fulfillment state (i.e., the local states of the debtor in the three global states are indistinguishable). However, for the creditor it does not matter being in the intermediate state or in the fulfillment state as being in one of them is the same for him. Introducing the intermediate state makes the computation of the accessible states very complex. The authors verified the proposed logic using a symbolic model checking algorithm they developed for this purpose. They also extended the MCMAS model checker to be capable of interpreting the new modalities. By so doing, they were able to show that the problem of model checking CTLC is polynomial-time reducible to the problem of model checking CTLK (Computation Tree Logic of Knowledge [88]). However, the stochastic aspect of the system being verified has not been addressed.

CTLC logic [36] has also been the focus of El-Menshawy et al. [33, 34] and Bentahar et al. [9] to verify and model check commitment-based protocols. In [33], the authors investigate the use of symbolic model checkers to verify the compliance of commitment protocols against some given properties such as liveness and safety. To do so, they reduce the problem of model checking CTLC to the problem of model checking either CTLK or ARCTL (an extension of CTL with action formulae [87]) where both are extensions of CTL. This allowed them to use MCMAS (suitable for CTLK), and NuSMV (suitable for ARCTL). On the other hand, Bentahar et al. [9] refined CTLC by introducing a set of

shared and unshared variables so that their extended version of interpreted systems can account for the communication among the interacting agents. Technically, they associate with each agent a countable set of local variables. Then, they use those variables to represent communication channels through which messages are sent and received. Furthermore, they analyzed the time complexity of CTLC model checking in explicit models such as Kripke-like structures, and its space complexity for concurrent programs. Their proposed model checking algorithms are implemented on top of the MCMAS model checker. El-Menshawy et al. [34] also modified CTLC into CTLC^{+} that allows reasoning about communicating commitments and their fulfilments. In their work, they introduce a formal reduction technique to reduce the problem of model checking CTLC^{+} to the problem of model checking ARCTL and the problem of model checking GCTL*. This allows them to take a benefit of existing model checkers such as the extended NuSMV symbolic model checker (suitable for ARCTL) and the CWB-NC automata-based model checker (suitable for GCTL*). Moreover, they analyzed the complexity of model checking CTLC^{+} for concurrent programs with respect to the size of such programs and the length of the formulae and proved it to be PSPASE-complete. Our work extends those proposals by considering the probabilistic aspect of social commitments.

Focusing on business models, Telang and Singh [109] propose an expressive and declarative approach capable of specifying business models at a high level of abstraction using the notion of social commitments. In particular, they specify business models using CTL logic, and model check operational interactions (a set of business interactions) specified as UML sequence diagrams. They map each model business to a temporal logic specification based on the progression of the states of the relevant commitments. Concretely, they capture the business model as an aggregation of business patterns. Then, they map each pattern to a CTL-based specification. To verify agent interactions, the authors

use the NuSMV model checker to compute whether operational models correctly support a business model. In this work, commitments are translated into NuSMV variables instead of introducing a new commitment modality as we do in our proposal.

In [35], the authors propose a new logical-based language to specify commitment-based protocols. The presented language is defined in terms of ACTL^{*c} logic which in turn extends CTL* with operators for social commitments and their actions. Like in [34], the authors also present a formal reduction-based verification technique to transfer the problem of model checking ACTL^{*c} to the problem of model checking GCTL*. They implement their automatic reduction-based model checking approach on top of the CWB-NC model checker. Like in their proposal in [34], agents are assumed to be certain about their commitments.

In [50], Gerard and Singh introduce an approach that specify commitment protocols and their refinements using guarded messages. The meaning of each message is defined as a set of actions. They use CTL as the underlying logic in which the specification is defined. The authors propose a model checking technique to seek whether a protocol refines another protocol correctly under certain conditions or not. The proposed tool "Proton" was implemented on top of the MCMAS model checker. The commitments, which supposed to be certain, are modeled as objects which are mapped into domain variables in ISPL (the input language of MCMAS).

3.5.2 Probabilistic Commitments

Uncertainty in commitments has to date received little attention by researches of MASs community. Herein, we review some existing proposals that treat commitments in the presence of uncertainty.

In [117], 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 [118] 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 underling 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 $C_{ij}(s) = \langle t, \rho \rangle$ 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 ρ" [118]. By making use of these probabilistic commitments, agents can make promises to each other even if they cannot fully guarantee service provision.

Unlike the proposals in [117, 118], we precisely use social commitments as a means

Table 3.3: Comparison between our approach for the probabilistic commitments and the related work

Approach	Formal	Uncertainty	Verification
[13, 14, 98]	√		
[9, 19, 27, 32, 33, 34, 35, 36, 50, 109]	√		√
[117, 118]		√	
Ours	√	√	√

Table 3.4: Comparison between PCTLC and existing logics in terms of the adopted logic

Approach	LTL	CTL	CTL*	ARCTL	PCTL	None
[19, 27]	√					
[9, 33, 34, 36, 50, 98, 109]		√				
[13, 14, 32]			√			
[35]				√		
[117, 118]						√
Ours					√	

of communication between the interacting agents. In addition, these proposals do not consider the verification aspect of commitments. However, we address the commitments between communicating parties from a formal perspective. That is, we integrate a commitment modality to probabilistic logic so that the verification of such commitments becomes achievable by means of model checking.

3.5.3 Comparison

We compare our work to the existing approaches by taking into consideration the following criteria: Formalization, Uncertainty, and Verification. Formalization reflects the use of formal logics such as LTL, CTL, CTL*, ARCTL or PCTL to represent and specify the commitments. Uncertainty property indicates whether the probabilistic behavior is considered or not. Finally, Verification confirms the presentation of a formal verification technique to verify the proposed approach. Table 3.3 shows a summary about the comparison between our work and the existing approaches based on the criteria described above.

Table 3.5: Comparison between PCTLC and existing approaches in terms of the used verification tool

Approach	SPIN	MCMAS	NuSMV	CWB-NC	PRISM	None
[19, 27]	√					
[9, 32, 33, 36, 50]		√				
[32, 33, 34, 109]			√			
[35]				√		
[13, 14, 98, 117, 118]						√
Ours					√	

In terms of formalization, our approach shares with most of the surveyed proposals the idea of extending existing temporal logics with new modalities for the commitments and their fulfilments. However, the main feature that distinguishes it from others lies in the logic being extended to handle social commitments. While others adopt conventional, non-probabilistic logics such as LTL, CTL, and CTL*, ours is the only work that builds on a probabilistic logic, namely PCTL. Table 3.4 compares between our approach and other proposals with respect to the underlying logic that has been extended to specify social commitments.

From the verification perspective, like proposals in [33, 34, 35], we adopt a formal reduction technique as the underlying basis for our model checking to translate the problem of model checking our logic to the problem of model checking an existing logic. However, to the best of our knowledge, non of the existing approaches has verified social commitments in the presence of uncertainty. Therefore, our approach outperforms the related approaches as it is the first attempt to tackle the verification problem of the probabilistic social commitments. Table 3.5 displays a comparison between our approach and the existing ones in terms of the used model checkers.

3.6 Summary

In this chapter, we introduced a new model checking technique for social commitments among agents interacting in uncertain settings. We specified properties for such systems using Probabilistic Computation Tree Logic of Commitments (PCTLC). The PCTLC logic extends PCTL with a social operator for commitments and their fulfillments. Target systems are modeled using a new version of interpreted systems which incorporates and extends two different versions of interpreted systems formalism to capture the probabilistic behavior of MASs, and account for the communication between interacting entities. The proposed model checking technique consists of a set of reduction rules to formally reduce the problem of model checking PCTLC to the problem of model checking PCTL so that the use of the PRISM model checker is made possible. The proposed verification approach was evaluated through implementing the reduction tool on top of the PRISM model checker and then applying it on a real case study from the cryptography domain namely the oblivious transfer protocol. The obtained results show the effectiveness of the proposed technique. In particular, we were successfully able to verify some desirable properties expressed originally in PCTLC. We also showed that the proposed reduction technique is scalable as we were able to perform the model checking for models made of up to $1.56 * 10^{18}$ states and transitions.

In the next chapter, we investigate how our approach for probabilistic social commitments can be exploited to handle the interaction between social commitments and agents' knowledge in MASs.

Chapter 4

The Interaction between Probabilistic Commitments and Knowledge

In this chapter[1], we put forward a method for capturing and verifying the interactions between the concepts of knowledge and social commitments in probabilistic MASs. The proposed method allows us to figure out the impact of knowledge and social commitments on each other in the presence of uncertainty. To express the two concepts simultaneously in systems exhibiting probabilistic behavior, we define a new modal logic called the Probabilistic Computation Tree Logic of Knowledge and Commitments (PCTL^{kc}), or simply the Probabilistic Logic of Knowledge and Commitments, which combines the probabilistic logic of commitments (PCTLC) that has been introduced in Chapter 3 and the existing probabilistic logic of knowledge (PCTLK) [115, 116] in a single tool. In the current chapter, MASs are modeled using a new version of interpreted systems that captures the probabilistic behavior and accounts for the communication between interacting components. Based on the proposed logic, we introduce a new model checking procedure to check the compliance of target systems against some desirable properties.

[1]The results of this chapter have been published in the journal of Expert Systems with Applications [106].

4.1 Introduction

The rapid increase of using software agents and 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 [69]. Among other aspects, knowledge and social commitments are of a great interest in MASs. Social commitments have been a vital approach in agent societies to capture the communication between interacting agents for more than a decade. On the other hand, knowledge has been addressed in distributed systems since 1960s [116]. Recently, Al-Saqqar et al. [1] have demonstrated that these two concepts are closely interacting with each other in various real life scenarios.

Despite the large amount of work that has been done to model and represent various aspect of probabilistic MAS, 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 [40] 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 some 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 [55] and further in [115, 116] to capture the probabilistic behavior of epistemic MASs. Recently, it has been extended in [9] and [34] to account for the communication 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 through 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 [62]. 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 [64]. This is important because, in general, every action has both types of effect. However, solving these models comes at a very high computational cost [82]. In this chapter, 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.

In terms of computational logics, most current proposals address each of knowledge and commitments in MASs independently (see for example [5, 9, 26, 34, 51, 55, 62, 77, 90, 116]). However, 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. Nevertheless, it is a challenge 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 [102].

Applying model checking techniques that were originally introduced for standard logics, such as LTL [91], CTL [38], or PCTL [57], to the verification of the interaction between knowledge and social commitments in presence of uncertainty is not straightforward

as non of these logics can capture and express the relationship between knowledge and social commitments in probabilistic settings. In this chapter, we introduce a model checking technique to address this open issue.

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 [69]. In particular, we use the independent join (or fusion) technique [46]. Given two logics $\mathbb{A}$ and $\mathbb{B}$, we combine them in a new logic $\mathbb{A} \oplus \mathbb{B}$

which extends the expressive power of each one. In our case, suppose $\mathbb{A}$ addresses probabilistic epistemic properties of agents and $\mathbb{B}$ 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 new combined logic is defined, we use the PRISM tool [73] as the formal verification tool to verify it after its reduction to PCTL, the probabilistic branching-time logic [57].

The contributions of this chapter 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 [40]. Those versions are introduced respectively by 1) Halpern [55] and extended later by Wan et al. [115, 116] to capture the stochastic behavior of the system; and 2) by Bentahar et al. [9] and El-Menshawy et al. [34] 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 reason about the interaction between knowledge and social commitments. The logic we define combines the Probabilistic Computation Tree Logic of Knowledge PCTLK [115, 116] and the Probabilistic Computation Tree Logic of Commitments PCTLC [107]. PCTLK and PCTLC are, in turn, extensions of the Probabilistic Computation Tree Logic PCTL [57] 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 (PCTL^{kc}). The introduced technique is a reduction-based in which the problem of model checking PCTL^{kc} 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^{kc} to MDPs to

be suitable for the PRISM model checker. We also devise some other rules to reduce each PCTL^{kc} 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^{kc}. Figure 4.1 gives an overview of the proposed approach.

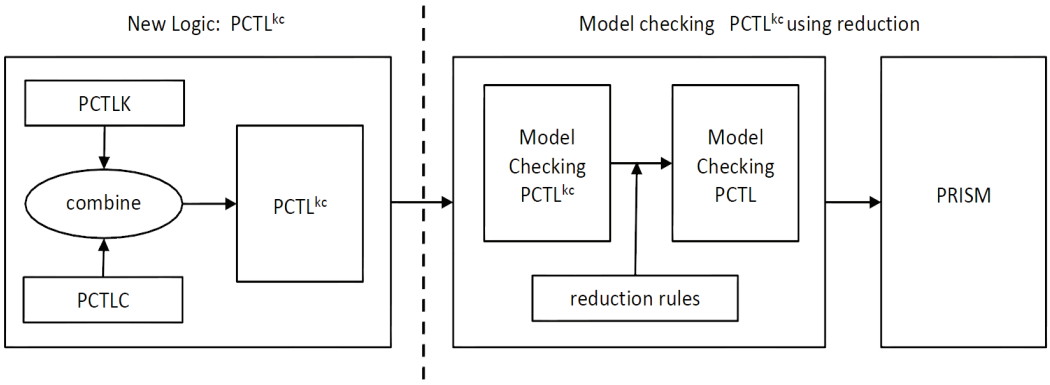

Figure 4.1: An approach for the interaction between knowledge and commitments

The work presented in this chapter 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.

4.2 The Probabilistic Logic of Knowledge and Commitment (PCTL^{kc})

In this section, we introduce our new probabilistic logic of knowledge and commitment (PCTL^{kc}). The modal logic we introduce can express knowledge and social commitments simultaneously in the presence of uncertainty. It combines two existing probabilistic logics namely, the probabilistic logic of knowledge PCTLK [115, 116] and the probabilistic logic

of commitments PCTLC [103, 107]. We first present the syntax of our new logic, and then we define its semantics. We also define a new version of the probabilistic interpreted systems formalism over which the semantics of PCTL^{kc} can be interpreted.

As we said earlier, the new logic PCTL^{kc} contains a knowledge modality that doesn't exist in the logic defined previously in Chapter 3. Therefore, we need first to define the model of PCTL^{kc}. In fact, the PCTL^{kc} model is generated from an extended version of probabilistic interpreted systems [55, 116] enriched by the social accessibility relations introduced in [9, 34] as discussed in Chapter 2.

Definition 4.1 (Models)**.** Given a set of atomic propositions $\Phi_p = (p, q, r, \ldots)$ and a set of agents $\mathtt{Agt} = \{1, \ldots, n\}$, the model $\mathfrak{M}_2 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\sim_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, V)$ is a tuple where:

- $S \subseteq L_1 \times \ldots \times L_n$ 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.

- $\mathbf{P} : S \times S \to [0, 1]$ is a total transition probability function defined as $\mathbf{P}(s, s') = \tau(s, a^{s\to s'}, s')$ iff there exists a joint action $a = (a_1, \ldots, a_n) \in ACT$ such that $\sum_{i\in \mathtt{Agt}} \tau_i(l_i(s), a^{l_i(s)\to l_i(s')}, l_i(s')) > 0$ and $\sum_{s'\in S} \mathbf{P}(s, s') = 1$ for all $s \in S$.

- $\sim_i \subseteq S \times S$ is the epistemic accessibility relation for the agent i, such that for two global states s and s', we have: $s \sim_i s'$ iff $l_i(s) = l_i(s')$.

- For each pair $(i, j) \in \mathtt{Agt}^2$, $\sim_{i\to j} \subseteq S \times S$ is a serial social accessibility relation. $s \sim_{i\to j} s'$ is defined by the following conditions:

  1. $l_i(s) = l_i(s')$.

2. $Var_i \cap Var_j \neq \emptyset$ such that $\forall x \in Var_i \cap Var_j$ we have $l_i^x(s) = l_j^x(s')$.

3. $\forall y \in Var_j - Var_i$ we have $l_j^y(s) = l_j^y(s')$.

- $\nu : S \rightarrow 2^{\Phi_p}$ is a function valuating states with atomic propositions.

The difference between our new model $\mathfrak{M}_2$ and the model $\mathfrak{M}_1$ that has been proposed in Chapter 3 is that $\mathfrak{M}_2$ has the ability to model agents' knowledge in the system –in addition to modeling the commitment-based communication among interacting parties– thanks to the epistemic accessibility relations that are integrated in the model. Technically, $\mathfrak{M}_2$ in an extended version of $\mathfrak{M}_1$ with epistemic accessibility relations. Computation paths of $\mathfrak{M}_2$ and probability space are defined as in Chapter 3.

4.2.1 Syntax of PCTL^{kc}

The logic we introduce in this section can be seen as an extension to the logic presented in Chapter 3 by adding an epistemic operator to PCTLC [103, 107]. The resulting logic, i.e., PCTL^{kc}, will have the power to not only express the individual aspects of knowledge and social commitments in independent formulae, but also express combinations of the two concepts in the same formulae.

Definition 4.2 (Syntax)**.** Given a set of atomic propositions Φ_p. Let $\mathtt{Agt} = \{1, \ldots, n\}$ be a set of agents. The PCTL^{kc} formulae are defined by the following BNF grammar:

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathscr{K} \mid \mathscr{C} \mid \mathbb{P}_{\bowtie k}(\psi) \mid \mathbb{P}_{\bowtie k}(\mathscr{K}) \mid \mathbb{P}_{\bowtie k}(\mathscr{C})$$

$$\psi ::= \bigcirc\varphi \mid \varphi \; U \; \varphi \mid \varphi \; U^{\leq m} \; \varphi$$

$$\mathscr{K} ::= K_i\varphi$$

$$\mathscr{C} ::= C_{i \rightarrow j}\varphi \mid Fu(C_{i \rightarrow j}\varphi)$$

where $p \in \Phi_p$ is an atomic proposition and $\mathbb{P}_{\bowtie k}$ is a probabilistic operator where $\bowtie \in \{<, \leq, >, \geq\}$ and $k \in [0,1]$ is a probability bound or threshold. $m \in \mathbb{N}^+$ is a positive integer number reflecting the maximum number of transitions needed to reach a certain state. φ and ψ are state and path formulae interpreted over the states and paths of $\mathfrak{M}_2$ respectively. The Boolean connectives $\neg$ and $\vee$ are defined in the usual way. Formulae $\mathscr{K}$ are state formulae called knowledge (epistemic) formulae and used to express the epistemic properties through the K_i operator which stands for agent i knows. Formulae $\mathscr{C}$, called social formulae, are special state formulae in PCTL^{kc} that can express social properties using the modal connectives $C_{i\to j}$ and $Fu(C_{i\to j})$ standing for "commitment" and "fulfillment of commitment" respectively. $\bigcirc, U$ and $U^{\leq m}$ stand for "next time", "until" and "bounded until" path modal connectives respectively.

4.2.2 Semantics of PCTL^{kc}

Given a model $\mathfrak{M}_2 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\sim_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, \nu)$, then $(\mathfrak{M}_2, s) \models \varphi$ states that "a state s in the model $\mathfrak{M}_2$ satisfies a state formula φ, $(\mathfrak{M}_2, \pi) \models \psi$ means that "a path π in the model $\mathfrak{M}_2$ satisfies a path formula ψ, and $(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k}(\psi)$ means that "a state s in $\mathfrak{M}_2$ satisfies $\mathbb{P}_{\bowtie k}(\psi)$ if the probability of taking a path from s that satisfies ψ is in the interval specified by $\bowtie k$". When the model $\mathfrak{M}_2$ is clear from the context, we simply write the satisfaction relation $\models$ as follows: $s \models \varphi$ and $\pi \models \psi$. Furthermore, for a given pair $(i,j) \in \mathtt{Agt}^2$ of agents, we denote the number of socially accessible states s' from a given state s such that $s \sim_{i\to j} s'$ by $|s \sim_{i\to j} s'|$. 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:

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

Definition 4.3 (**Satisfaction**). Satisfaction of a PCTL^{kc} formula in the model $\mathfrak{M}_2$ is recursively defined as follows:

$s \models p$ *iff* $p \in v(s)$;

$s \models \varphi_1 \vee \varphi_2$ *iff* $s \models \varphi_1$ or $s \models \varphi_2$;

$s \models \neg\varphi$ *iff* $s \not\models \varphi$;

$s \models K_i\varphi$ *iff* $\forall s' \in S$ s.t. $s \sim_i s'$ we have $s' \models \varphi$;

$s \models C_{i\to j}\varphi$ *iff* $\forall s' \in S$ s.t. $s \sim_{i\to j} s'$, we have $s' \models \varphi$;

$s \models Fu(C_{i\to j}\varphi)$ *iff* $\exists s' \in S$ s.t. $s' \sim_{i\to j} s$ and $s' \models C_{i\to j}\varphi$;

$\pi \models \bigcirc\varphi$ *iff* $\pi(1) \models \varphi$;

$\pi \models \varphi_1\ U^{\leq m}\ \varphi_2$ *iff* $\exists k \leq m$ s.t. $\pi(k) \models \varphi_2$ and $\forall i < k, \pi(i) \models \varphi_1$;

$\pi \models \varphi_1\ U\ \varphi_2$ *iff* $\exists m \geq 0$ s.t. $\pi \models \varphi_1\ U^{\leq m}\ \varphi_2$;

$s \models \mathbb{P}_{\bowtie k}(\psi)$ *iff* $Prob_s(\psi) \bowtie k$ where: $Prob_s(\psi) = Prob_s\{\pi \in \Pi(s) \mid \pi \models \psi\}$;

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:

$s \models \mathbb{P}_{\bowtie k}(K_i\varphi)$ *iff* $Prob(s \models K_i\varphi) \bowtie k$ where: $Prob(s \models K_i\varphi) = \frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s \sim_i s'|}$;

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:

$s \models \mathbb{P}_{\bowtie k}(C_{i\to j}\varphi)$ *iff* $Prob(s \models C_{i\to j}\varphi) \bowtie k$ where: $Prob(s \models C_{i\to j}\varphi) = \frac{\sum_{s\sim_{i\to j} s'} |s' \models \varphi|}{|s \sim_{i\to j} s'|}$;

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

$s \models \mathbb{P}_{\bowtie k}(Fu(C_{i\to j}\varphi))$ *iff* $Prob(s \models Fu(C_{i\to j}\varphi)) \bowtie k$; where:

$$Prob(s \models Fu(C_{i\to j}\varphi)) = Prob_s\{\pi \in \Pi(s') \mid s' \sim_{i\to j} s \text{ and } \pi = s' \ldots s \text{ and } s' \models C_{i\to j}\varphi\}$$

The probabilistic knowledge is computed in such a way to reflect the indistinguishability property of the epistemic accessibility relations. 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 4.1.

If $(\mathfrak{M}_2, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to j}\varphi))$ *and* $(\mathfrak{M}_2, s) \models Fu(C_{i\to j}\varphi)$*, then s is not reachable from the commitment state.*

Theorem 4.1. *Epistemic Equivalences*

1. $(\mathfrak{M}_2, s) \models \mathbb{P}_{\geq 1}(K_i\phi)$ *iff* $(\mathfrak{M}_2, s) \models K_i\phi$
2. $(\mathfrak{M}_2, s) \models \mathbb{P}_{\leq 0}(K_i\phi)$ *iff* $(\mathfrak{M}_2, s) \models K_i\neg\phi$
3. $(\mathfrak{M}_2, s) \models \mathbb{P}_{]0,1[}(K_i\ \phi)$ *iff* $(\mathfrak{M}_2, s) \models \neg K_i\neg\phi \wedge \neg K_i\phi$

Proof.

- First equivalence.

  "$\Rightarrow$". Assume $s \models \mathbb{P}_{\geq 1}(K_i\varphi)$. By the semantics of PCTL^{kc}, it follows that $Prob(s \models K_i\varphi) \geq 1$. Therefore, $\frac{\sum_{s\sim_i s'} |s'\models\varphi|}{|s\sim_i s'|} \geq 1$. This means $\forall s' \in S$ such that $s \sim_i s'$, we have $s' \models \varphi$ (as $\sim_i$ is reflexive, so s' could be s itself). Thus, $s \models K_i\varphi$.

  "$\Leftarrow$". Assume $s \models K_i\varphi$. By the PCTL^{kc} semantics, it follows that for all $s' \in S$ such that $s \sim_i s'$, we have $s' \models \varphi$ (i.e. all accessible states from s satisfy φ). Consequently, $\sum_{s\sim_i s'} |s' \models \varphi| = |s \sim_i s'|$. Therefore, $\frac{\sum_{s\sim_i s'} |s'\models\varphi|}{|s\sim_i s'|} \geq 1$ and hence $s \models \mathbb{P}_{\geq 1}(K_i\varphi)$.

- Second equivalence.

  " $\Rightarrow$ ". Assume $s \models \mathbb{P}_{\leq 0}(K_i\varphi)$. By the PCTL^{kc} semantics, it follows that $Prob(s \models K_i\varphi) \leq 0$. Thus, $\frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s\sim_i s'|} \leq 0$. Since $\sim_i$ is reflexive, so the set of the accessible states from s is not empty, therefore $\sum_{s\sim_i s'} |s' \models \varphi|$ must be 0 (i.e. φ is not true in any of the accessible states). Consequently, for all $s' \in S$ such that $s \sim_i s'$, we have $s' \not\models \varphi$, which means $s' \vDash \neg\varphi$. Hence, $s \models K_i\neg\varphi$.

  " $\Leftarrow$ ". Assume $s \models K_i\neg\varphi$. By the PCTL^{kc} semantics, it follows that $\forall s' \in S$ such that $s \sim_i s'$, we have $s' \not\models \varphi$. Since the set of the accessible states from s is not empty, then $\frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s\sim_i s'|} \leq 0$. Hence, $s \models \mathbb{P}_{\leq 0}(K_i\varphi)$.

- Third equivalence.

  " $\Rightarrow$ ". Assume $s \models \mathbb{P}_{]0,1[}(K_i\varphi)$. By the PCTL^{kc} semantics, it follows that $0 < Prob(s \models K_i\varphi) < 1$. Thus, $0 < \frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s\sim_i s'|} < 1$. This means that it would never be the case that $\sum_{s\sim_i s'} |s' \models \varphi| = |s \sim_i s'|$ nor $\sum_{s\sim_i s'} |s' \models \varphi| = 0$. Consequently, there exist some $s', s'' \in S$ such that $s \sim_i s'$ and $s \sim_i s''$ and $s' \models \varphi$ and $s'' \models \neg\varphi$. Hence, it is impossible to have $\bar{s} \models \neg\varphi$ or $\bar{s} \models \varphi$ for all $\bar{s} \in S$ such that $s \sim_i \bar{s}$. Consequently, $s \not\models K_i\neg\varphi$ and $s \not\models K_i\varphi$. Hence $s \models \neg K_i\neg\varphi$ and $s \models \neg K_i\varphi$.

  " $\Leftarrow$ ". Assume $s \models \neg K_i\varphi$. By the PCTL^{kc} semantics, it follows that there exists $s' \in S$ such that $s \sim_i s'$ and $s' \models \neg\varphi$. Consequently, it would never be the case that for all $s' \in S$ such that $s \sim_i s'$ we have $s' \models \varphi$. Therefore, $1 > \frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s\sim_i s'|}$. Now assume $s \models \neg K_i\neg\varphi$. Therefore, $\sum_{s\sim_i s'} |s' \models \varphi| = 0$ would never be the case as some accessible states should satisfy φ. Consequently, $\frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s\sim_i s'|} > 0$. Thus, $0 < \frac{\sum_{s\sim_i s'} |s' \models \varphi|}{|s\sim_i s'|} < 1$. Hence, $s \models \mathbb{P}_{]0,1[}(K_i\varphi)$.

□

Theorem 4.2. *Commitment Equivalences*

1. $(\mathfrak{M}_2, s) \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi) \quad \textit{iff} \quad (\mathfrak{M}_2, s) \models C_{i\to j}\varphi$

2. $(\mathfrak{M}_2, s) \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi) \quad \textit{iff} \quad (\mathfrak{M}_2, s) \models C_{i\to j}\neg\varphi$

3. $(\mathfrak{M}_2, s) \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi) \quad \textit{iff} \quad (\mathfrak{M}_2, s) \models \neg C_{i\to j}\neg\varphi \wedge \neg C_{i\to j}\varphi$

Proof.

- First equivalence.

  " $\Rightarrow$ ". Assume $s \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$. By the PCTL^{kc} semantics, it follows that $Prob(s \models C_{i\to j}\varphi) \geq 1$. Thus, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \geq 1$. This means that for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \models \varphi$, and hence $s \models C_{i\to j}\varphi$.

  " $\Leftarrow$ ". Assume $s \models C_{i\to j}\varphi$. By the PCTL^{kc} semantics, it follows that for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \models \varphi$ (i.e. all accessible states from s satisfy φ). Consequently, $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = |s \sim_{i\to j} s'|$. Therefore, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \geq 1$ and hence, $s \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$.

- Second equivalence.

  " $\Rightarrow$ ". Assume $s \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$. By the PCTL^{kc} semantics, it follows that $Prob(s \models C_{i\to j}\varphi) \leq 0$. Thus, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \leq 0$. Since the set of the accessible states from s is not empty, then $\sum_{s\sim_{i\to j}s'} |s' \models \varphi|$ must be 0 (i.e. φ is not true in any of the accessible states). Consequently, for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \not\models \varphi$, which means $s' \models \neg\varphi$. Hence, $s \models C_{i\to j}\neg\varphi$.

  " $\Leftarrow$ ". Assume $s \models C_{i\to j}\neg\varphi$. By the PCTL^{kc} semantics, it follows that for all $s' \in S$ such that $s \sim_{i\to j} s'$, we have $s' \not\models \varphi$. Since the set of the accessible states from s is not empty, then $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} \leq 0$. Hence, $s \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$.

- Third equivalence.

  " $\Rightarrow$ ". Assume $s \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$. By the PCTL^{kc} semantics, it follows that $0 < Prob(s \models C_{i\to j}\varphi) < 1$. Thus, $0 < \frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} < 1$. This means that it would never be the case that $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = |s \sim_{i\to j} s'|$ nor $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = 0$. Consequently, there exist some $s', s'' \in S$ such that $s \sim_{i\to j} s'$ and $s \sim_{i\to j} s''$ and $s' \models \varphi$ and $s'' \models \neg\varphi$. Hence, it is impossible to have $\bar{s} \models \neg\varphi$ or $\bar{s} \models \varphi$ for all $\bar{s} \in S$ such that $s \sim_{i\to j} \bar{s}$. Consequently, $s \not\models C_{i\to j}\neg\varphi$ and $s \not\models C_{i\to j}\varphi$. Hence $s \models \neg C_{i\to j}\neg\varphi$ and $s \models \neg C_{i\to j}\varphi$.

  " $\Leftarrow$ ". Assume $s \models \neg C_{i\to j}\varphi$. By the PCTL^{kc} semantics, it follows that there exists $s' \in S$ such that $s \sim_{i\to j} s'$ and $s' \models \neg\varphi$. Consequently, it would never be the case that $s' \models \varphi$ for all $s' \in S$ such that $s \sim_{i\to j} s'$. Therefore, $1 > \frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|}$. Now assume $s \models \neg C_{i\to j}\neg\varphi$. Therefore, $\sum_{s\sim_{i\to j}s'} |s' \models \varphi| = 0$ would never be he case as some accessible states should satisfy φ. Consequently, $\frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} > 0$. Thus, $0 < \frac{\sum_{s\sim_{i\to j}s'} |s'\models\varphi|}{|s\sim_{i\to j}s'|} < 1$. Thus, $s \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$.

□

Theorem 4.3. *Fulfillment Equivalences*

1. $(\mathfrak{M}_2, s) \models \mathbb{P}_{>0}(Fu(C_{i\to j}\varphi))$ *iff* $(\mathfrak{M}_2, s) \models Fu(C_{i\to j}\varphi)$ *and s is reachable from the commitment state.*

2. $(\mathfrak{M}_2, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to j}\varphi))$ *iff* $(\mathfrak{M}_2, s) \models \neg Fu(C_{i\to j}\varphi)$ *or s is not reachable from the commitment state.*

Proof.

The proofs of these equivalences are direct from Proposition 4.1 and the above semantics.

□

4.3 Model Checking PCTL^{kc} Using Reduction

In this section, we present our reduction technique to model checking PCTL^{kc}. Given a MAS represented as a probabilistic interpreted system $\mathfrak{M}_2$ and a desirable property φ written in PCTL^{kc}, the problem of probabilistic model checking PCTL^{kc} can be defined as: 1) establishing whether $(\mathfrak{M}_2, I) \models \varphi$, i.e., if $I \in Sat(\varphi)$ where $Sat(\varphi)$=$\{s \in S \mid \mathfrak{M}_2, s \models \varphi\}$ is the set of states satisfying φ; 2) comparing the probability of satisfying φ with a probability threshold $\bowtie k$, where $Sat(\mathbb{P}_{\bowtie k}(\varphi)) = \{s \in S \mid Prob_s(\varphi) \bowtie k\}$; or 3) computing the probability of φ, $(\mathfrak{M}_2, s) \models \mathbb{P}_{=?}(\varphi)$. Note that answers to the second and third queries can be: (1) truth values, when the specification simply asks for a comparison to a probability threshold; or (2) quantitative, returning the actual probability.

Figure 4.2 depicts the structure of our proposed reduction technique. The idea is to reduce the problem of probabilistic model checking PCTL^{kc} to the problem of probabilistic model checking 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 $\mathfrak{M}_2$ into an MDP model. MDPs are the standard models for describing systems with probabilistic and nondeterministic behavior [93]. Then, we use the notion of adversary as in [72] to resolve the nondeterminism 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^{kc} formulae into PCTL formulae. This is basically achieved by constructing a set of rules that formally transforms the PCTL^{kc} formulae into corresponding ones in PCTL.

In a nutshell, the proposed model checking procedure is as follows. Given $\mathfrak{M}_2 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\sim_{i \to j}\}_{(i,j) \in \mathtt{Agt}^2}, \nu)$, and PCTL^{kc} formula φ, we have to define an MDP model $\mathfrak{M}'_2 = \mathscr{F}(\mathfrak{M}_2)$ and PCTL formula $\mathscr{F}(\varphi)$ using the transformation function $\mathscr{F}$ such

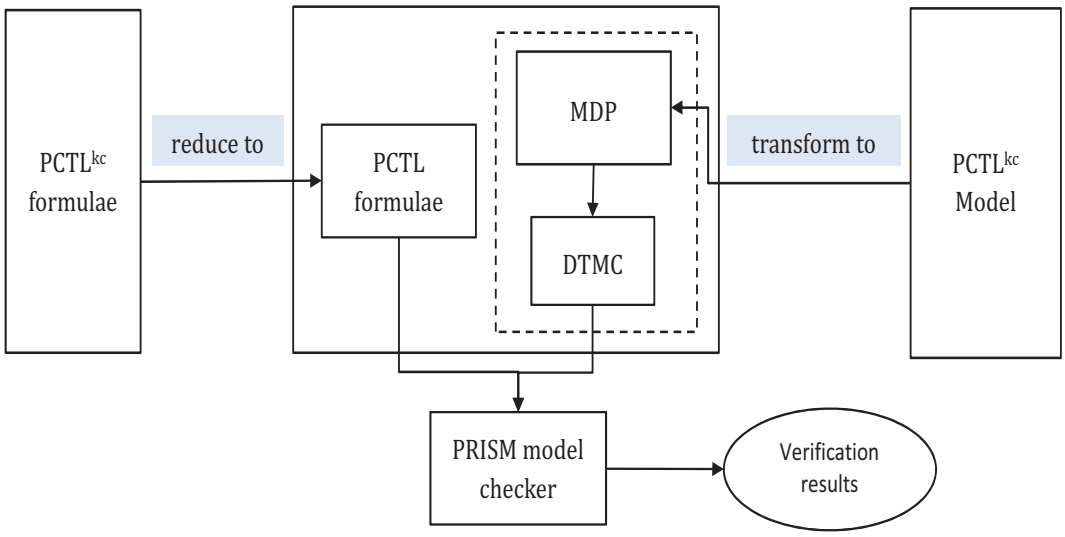

Figure 4.2: The proposed reduction technique of model checking PCTL^{kc}

that $\mathfrak{M}_2 \models \varphi$ iff $\mathscr{F}(\mathfrak{M}_2) \models \mathscr{F}(\varphi)$.

4.3.1 Transforming the Model $\mathfrak{M}_2$

In order to transform our model $\mathfrak{M}_2 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\sim_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, v)$ into an MDP model $\mathfrak{M}'_2 = (\mathbb{S}, Act, \mathsf{P}_t, I_i, L)$, we need to define the set of actions Act. 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 $\mathfrak{M}_2$ into labeled transitions in $\mathfrak{M}'_2$. Labels (also called actions) are used to distinguish between different types of relations. Consequently, the three relations in $\mathfrak{M}_2$, namely transition relation, epistemic accessibility relation, and social accessibility relation are translated into labeled transitions in $\mathfrak{M}'_2$. Moreover, whenever we have a labeled transition representing a social accessibility relation we add the symmetric closure of it to interpret the fulfilment of the commitment. As depicted in Figure 4.3 (assuming that n is the number of agents, $1 \leq i \leq n$, and $1 \leq j \leq n$), actions $\delta, \alpha^i, \beta^{ij}$, and γ^{ij} denote transitions defined, respectively, from the probabilistic transition relation $\mathbf{P}$, the epistemic accessibility relation $\sim_i$ (to capture the semantics of knowledge), the social

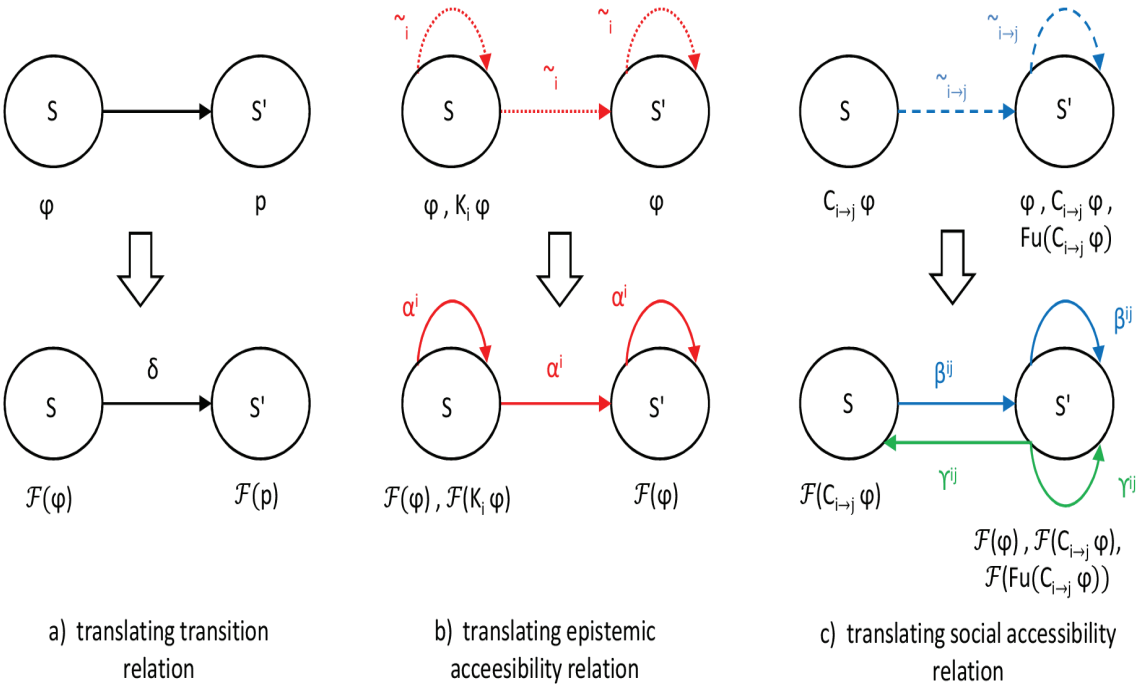

Figure 4.3: Translating relations in $\mathfrak{M}_2$ into labeled transitions in the MDP model

accessibility relation $\sim_{i\to j}$ (to capture the semantics of commitment), and the symmetric closure of the social accessibility relation (to capture the semantics of fulfilment).

The MDP model $\mathfrak{M}'_2 = (\mathbb{S}, Act, \mathsf{P}_t, I_i, L)$ can now be defined as follows:

- $\mathbb{S}$=S; I_i=I; L=ν.
- $Act = \{\delta\} \cup \{\alpha^1, \alpha^2, \ldots, \alpha^n\} \cup \{\beta^{11}, \beta^{12}, \ldots, \beta^{nn}\} \cup \{\gamma^{11}, \gamma^{12}, \ldots, \gamma^{nn}\}$ where n is the number of agents.
- We define P_t as the union of the transitions labeled with δ (i.e., the probabilistic transitions of **P**) with the probabilistic transitions labeled with α^i, probabilistic transitions labeled with β^{ij}, and probabilistic transitions labeled with γ^{ij}. The probabilities of transitions labeled with δ are not manipulated but rather inherited from the probabilistic transition function **P**. However, for transitions labeled with α^i and emanating

from the same state are given equal probabilities (i.e., equal distribution) which reflect the uncertainty of the agent over the accessible states, so that over the content of the knowledge. Meaning that, the probability of each transition annotated by α^i is equal to the probability of each other transition labeled with α^i emanating from the same state which is calculated by dividing one over the number of transitions labeled with α^i. The probabilities of transitions labeled with β^{ij} and γ^{ij} are calculated in the same way. For states $s, s' \in \mathbb{S}$ and action $\theta \in Act$, the function P_t is defined as follows:

$$\mathsf{P}_t(s,\theta,s') = \begin{cases} \mathbf{P}(s,s'), & \text{if } \theta = \delta \\ \frac{1}{|s \sim_i s'|}, & \text{if } \theta = \alpha^i \\ \frac{1}{|s \sim_{i\to j} s'|}, & \text{if } \theta = \beta^{ij} \\ \frac{1}{|s' \sim_{i\to j} s|}, & \text{if } \theta = \gamma^{ij}. \end{cases}$$

The induced model of applying the adversary σ over $\mathfrak{M}'_2$ is a DTMC model. Specifically, four adversaries are defined; σ_t over which temporal formulae are interpreted, σ_e to capture epistemic formulae, σ_c to capture commitment formulae, and σ_f to capture fulfillment formulae. These adversaries are defined based on the following rules. To define σ_t, action δ is selected at every state in $\mathfrak{M}'_2$. For σ_e, action α^i has to be among the enabled actions at the knowledge state. Then, the adversary picks up α^i at that knowledge state and δ at every other state. Adversaries σ_c, and σ_f are defined in the same way.

4.3.2 Reducing PCTL^{kc} Formulae into PCTL Formulae

In this section, we introduce our reduction rules that translate PCTL^{kc} formulae to PCTL formulae w.r.t given adversary σ. Given the adversary σ_t, the PCTL^{kc} formulae are transformed inductively into PCTL as follows:

$\mathscr{F}(p) = p$, if p is an atomic proposition,

$\mathscr{F}(\neg\varphi) = \neg\mathscr{F}(\varphi)$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}(\varphi \vee \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi) \vee \mathscr{F}(\psi))$,

$\mathscr{F}(\mathbb{P}_{\bowtie k} \bigcirc \varphi) = \mathbb{P}_{\bowtie k} \bigcirc \mathscr{F}(\varphi)$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}(\varphi\ U\ \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi) U \mathscr{F}(\psi))$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}(\varphi\ U^{\leq m}\ \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi) U^{\leq m} \mathscr{F}(\psi))$,

Note that σ_t is a DTMC model that is used to interpret only PCTL formulas. It cannot be used to capture the transformed formulas of knowledge and commitment as it ignores all relations except those labeled by δ (i.e., transition relations of **P**).

Given the adversary σ_e, the PCTL^{kc} epistemic formula is transformed inductively into PCTL as follows:

$\mathscr{F}(K_i\varphi) = \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}K_i\varphi) = \mathbb{P}_{\bowtie k}(\bigcirc\mathscr{F}(\varphi))$,

As mentioned earlier, the adversary σ_e is a DTMC model that captures only action α^i at the knowledge state and δ at all other states. Intuitively, transitions labeled with α^i represent epistemic accessibility relations and, in fact, epistemically accessible states from the knowledge state must satisfy φ. Back to Figure 4.3 (b), it is readily seen that all next states to the knowledge state through transitions labeled with α^i satisfy $\mathscr{F}(\varphi)$. This explains why knowledge formula $K_i\ \varphi$ is transformed to next operator followed by the transformation of the content of the knowledge ($i.e., \bigcirc\mathscr{F}(\varphi)$) in all paths emanating from the knowledge state.

Given the adversary σ_c, the PCTL^{kc} commitment formula is transformed inductively into PCTL as follows:

$\mathscr{F}(C_{i\rightarrow j}\varphi) = \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}C_{i\rightarrow j}\varphi) = \mathbb{P}_{\bowtie k}(\bigcirc\mathscr{F}(\varphi))$,

Similar to the case of knowledge formula, Figure 4.3 (c) illustrates the intuitions behind transforming the commitment formula $C_{i\to j}\varphi$ to $\bigcirc\mathscr{F}(\varphi)$ in all baths emerging from the commitment state.

Given the adversary σ_f, the PCTL^{kc} fulfillment formula is transformed inductively into PCTL as follows:

$$\mathscr{F}(Fu(C_{i\to j}\varphi)) = \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(C_{i\to j}\varphi)) = \mathbb{P}_{\geq 1}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))),$$

$$\mathscr{F}(\mathbb{P}_{\bowtie k}Fu(C_{i\to j}\varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc\mathscr{F}(C_{i\to j}\varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))).$$

Though the semantics of the fulfillment operator in PCTL^{kc} requires the existence of a path containing the fulfilment state which must be socially accessible from the commitment state, in this transformation we notice that all next states to the fulfilment state through transitions labeled with γ^{ij} should satisfy the commitment formula ($C_{i\to j}\varphi$). The reason of that is because in our transformation process, the transitions labeled with γ^{ij} came as a result of adding the symmetric closure of transitions labeled with β^{ij} in order to capture the semantics of the fulfilment. Therefore, all added transitions should satisfy the commitment formula ($C_{i\to j}\varphi$) (see Figure 4.3 (c)).

Theorem 4.4 (Equivalences Satisfaction)**.**

Let σ_t, σ_e, σ_c, and σ_f be the DTMC models corresponding to the adversaries that capture respectively, temporal formulae, epistemic formulae, commitment formulae, and fulfilment formulae in the model $\mathfrak{M}'_2$. The following equivalences hold:

$(\mathfrak{M}_2, s) \models p$ *iff* $(\sigma_t, s) \models p$

$(\mathfrak{M}'_2, s) \models \neg\varphi$ *iff* $(\sigma_t, s) \models \neg\mathscr{F}(\varphi)$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k}(\varphi \vee \psi)$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}\mathscr{F}(\varphi) \vee \mathbb{P}_{\bowtie k}\mathscr{F}(\psi)$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k}\bigcirc\varphi$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}\bigcirc\mathscr{F}(\varphi)$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k}(\varphi\ U\ \psi)$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi)\ U\ \mathscr{F}(\psi))$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k}(\varphi\ U^{\leq m}\ \psi)$ *iff* $(\sigma_t, s) \models \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi)\ U^{\leq m}\ \mathscr{F}(\psi))$

$(\mathfrak{M}_2, s) \models K_i\varphi$ *iff* $(\sigma_e, s) \models \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k} K_i\varphi$ *iff* $(\sigma_e, s) \models \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(\varphi))$

$(\mathfrak{M}_2, s) \models C_{i\to j}\varphi$ *iff* $(\sigma_c, s) \models \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k} C_{i\to j}\varphi$ *iff* $(\sigma_c, s) \models \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(\varphi))$

$(\mathfrak{M}_2, s) \models Fu(C_{i\to j}\varphi)$ *iff* $(\sigma_f, s) \models \mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$

$(\mathfrak{M}_2, s) \models \mathbb{P}_{\bowtie k} Fu(C_{i\to j}\varphi)$ *iff* $(\sigma_f, s) \models \mathbb{P}_{\bowtie k}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$

Notice that each formula has to be interpreted over a DTMC model (adversary) that is used to solve the nondeterminism in $\mathfrak{M}'_2$ based on the type of the formula (i.e., temporal, epistemic, or social). The proof of the theorem with regard to PCTL formulae is straightforward as PCTL formulae are also PCTL^{kc} formulae. However, for epistemic and social formulae, the proof is given in Theorem 4.5.

Theorem 4.5 (Soundness and Completeness of $\mathscr{F}$)**.** *Let $\mathfrak{M}_2$ and Φ be respectively a PCTL^{kc} model and formula and let $\mathscr{F}(\mathfrak{M}_2)$ and $\mathscr{F}(\Phi)$ be the corresponding model and formula in PCTL. We have $\mathfrak{M}_2 \models \Phi$ iff $\mathscr{F}(\mathfrak{M}_2) \models \mathscr{F}(\Phi)$.*

Proof.

To prove the soundness of the proposed reduction technique, we have to prove that the following three cases are sound: $\Phi = K_i\varphi$, $\Phi = C_{i\to j}\varphi$ and $\Phi = Fu(C_{i\to j}\varphi)$. We prove this by induction on the structure of the formula Φ. The case of PCTL^{kc} formulae that are also PCTL formulae is straightforward.

- $\Phi = K_i\ \varphi$. We have $(\mathfrak{M}_2, s) \models K_i\ \varphi$ iff $(\mathfrak{M}_2, s') \models \varphi$ for every $s' \in S$ such that $s \sim_i s'$. Therefore, $(\mathfrak{M}_2, s) \models K_i\ \varphi$ iff $(\mathscr{F}(\mathfrak{M}_2), s) \models \mathscr{F}(K_i\ \varphi)$. Recall that $\mathscr{F}(\mathfrak{M}_2) = \mathfrak{M}'_2$. Now, $(\mathfrak{M}'_2, s) \models \mathscr{F}(K_i\ \varphi)$ iff for every $s' \in \mathbb{S}$ such that $(s, \alpha^i, s') \in \mathsf{P}_t$, we have $(\mathfrak{M}'_2, s') \models \mathscr{F}(\varphi)$. However, w.r.t the semantics of σ_e which is an adversary defined to interpret commitment formulae over $\mathfrak{M}'_2$, it follows that every infinite path $\pi \in$

$\Pi^{\sigma_e}(s)$ satisfies that $\pi(1) = s'$ and $(\sigma_e, \pi(1)) \models \mathscr{F}(\varphi)$. Thus, $(\sigma_e, s) \models \bigcirc\mathscr{F}(\varphi)$ for all $\pi \in \Pi^{\sigma_e}(s)$. As the path quantifier A is not defined in PCTL, and we have $\mathbb{P}_{\geq 1}$ instead, so we obtain $(\sigma_e, s) \models \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$.

- $\Phi = C_{i\to j}\varphi$. We have $(\mathfrak{M}_2, s) \models C_{i\to j}\varphi$ iff $(\mathfrak{M}_2, s') \models \varphi$ for every $s' \in S$ such that $s \sim_{i\to j} s'$. Consequently, $(\mathfrak{M}_2, s) \models C_{i\to j}\varphi$ iff $(\mathfrak{M}'_2, s) \models \mathscr{F}(C_{i\to j}\varphi)$. It follows that, $(\mathfrak{M}'_2, s) \models \mathscr{F}(C_{i\to j}\varphi)$ iff for every $s' \in \mathbb{S}$ such that $(s, \beta^{ij}, s') \in \mathsf{P}_t$, we have $(\mathfrak{M}'_2, s') \models \mathscr{F}(\varphi)$. Now, based on the adversary σ_c which is defined to interpret commitment formulae over $\mathfrak{M}'_2$, every infinite path $\pi \in \Pi^{\sigma_c}(s)$ satisfies that $\pi(1) = s'$ and $(\sigma_c, \pi(1)) \models \mathscr{F}(\varphi)$. Thus, $(\sigma_c, s) \models \bigcirc\mathscr{F}(\varphi)$ for all $\pi \in \Pi^{\sigma_c}(s)$. As the path quantifier A is not defined in PCTL, and we have $\mathbb{P}_{\geq 1}$ instead, so we obtain $(\sigma_c, s) \models \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$.

- $\Phi = Fu(C_{i\to j}\varphi)$. We have $(\mathfrak{M}_2, s) \models Fu(C_{i\to j}\varphi)$ iff there exists $s' \in S$ such that $s' \sim_{i\to j} s$ and $(\mathfrak{M}_2, s') \models C_{i\to j}\varphi$. Consequently, $(\mathfrak{M}'_2, s) \models \mathscr{F}(Fu(C_{i\to j}\varphi))$ iff there exists $s' \in \mathbb{S}$ such that $(s, \gamma^{ij}, s') \in \mathsf{P}_t$ and $(\mathfrak{M}'_2, s') \models \mathscr{F}(C_{i\to j}\varphi)$. Now, w.r.t the adversary σ_f which is defined to interpret fulfillment formulae over $\mathfrak{M}'_2$, we obtain at least one infinite path $\pi \in \Pi^{\sigma_f}(s)$ that satisfies $\pi(1) = s'$ and $(\sigma_f, \pi(1)) \models \mathscr{F}(C_{i\to j}\varphi)$. Since E is equivalent to $\mathbb{P}_{>0}$ and $\mathscr{F}(C_{i\to j}\varphi)$ is equivalent to $\mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$, so we obtain $(\sigma_f, s) \models \mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi)))$.

□

4.4 Implementation

In this section, a case study is implemented using PRISM [73] to verify knowledge, commitments, and interactions between the two concepts in probabilistic MASs. We apply the approach using the NetBill protocol as in [34, 80, 126]. NetBill protocol 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 with NetBill protocol, 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. As we said before, those probabilities could be generally obtained after observing the system behavior for long time. We will introduce this modified probabilistic NetBill protocol next.

4.4.1 NetBill Protocol

The basic NetBill 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. Having received 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. Accepting the offer means that the customer commits to send the payment to the merchant ($C_{Cus \to Mer}Pay$). We assume that only 90% of payment commitments will be fulfilled ($Fu(C_{Cus \to Mer}Pay)$) 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 ($C_{Mer \to Cur}Deliver$). Suppose that 99% of deliveries are successful, which means that the merchant fulfills its commitments ($Fu(C_{Mer \to Cur}Deliver)$). If the delivery fails, the merchant violates its commitment and in this case the merchant should

refund the customer. Figure 4.4 depicts the model of the modified NetBill protocol.

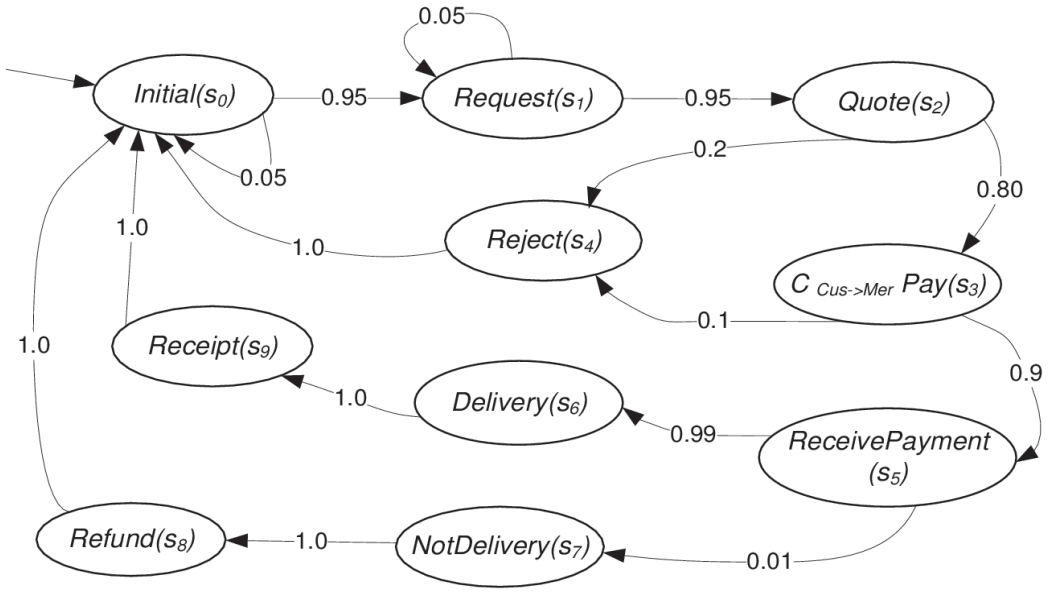

Figure 4.4: The Modified NetBill protocol

With the PRISM modeling language, we translate every agent into a *module* and the entire MAS is defined as a system with *agent modules* which are all synchronized.

To formalize the protocol, the scenario is encoded using the probabilistic interpreted systems $\mathfrak{M}_2$ introduced earlier in Definition 4.1. Two basic modules, *module Mer1* and *module Cur1* are defined according to their probabilistic transitions. They represent the customer agent *Cus1* and the merchant agent *Mer1* respectively. Other agents can just refer to these two basic agents and use *module renaming* function to duplicate a module.

4.4.2 NetBill Protocol Properties

- `Safety property`: When designing a system, we may set a confidence interval to allow some mistakes for properties because it seems impossible for human beings not to make any mistake in the real world. 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 $Cus1$ sends the payment to the merchant $Mer1$ without the merchant being aware of that. The following property can avoid this bad situation:

$\varphi_1 = \mathbb{P}_{=1}\ [\neg(Fu(C_{Cus1 \to Mer1} Pay) \wedge (\neg K_{Mer1} Pay))]$.

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:

$\varphi_2 = \mathbb{P}_{=1}\ [\neg(Fu(C_{Cus1 \to Mer1} Pay) \wedge (\neg K_{Cus1} Pay))]$.

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

$\varphi_3 = \mathbb{P}_{\geq 0.99}\ [\neg(Fu(C_{Cus1 \to Mer1} Pay) \wedge \neg(C_{Mer1 \to Cur1} Delivery))]$.

- `Liveness property:` Contrast to *safety property*, a *liveness property* means “a good thing will eventually happen". For example, when the merchant commits to deliver the goods to the customer, it will eventually deliver them. This property is expressed as follows:

  $\varphi_4 = \mathbb{P}_{\geq 0.99}(C_{Mer1 \to Cus1} Deliver \Rightarrow \mathbb{P}_{\geq 0}[\mathrm{F}\ Fu(C_{Mer1 \to Cus1} Deliver)])$.

- `Reachability property:` One good example for the reachability property for the NetBill protocol is that the merchant will eventually commit towards the customer to deliver the required goods, which should be reached from the initial state. This property can be expressed as follows:

  $\varphi_5 = \mathbb{P}_{\geq 0}\ [\mathrm{F}\ C_{Mer1 \to Cus1} Deliver]$

Table 4.1: Experimental results for NetBill protocol with PRISM

Number of Agents	Model		Construction	
	#States	#Transitions	Iterations	Time (sec)
2	19	39	7	0.001
3	108	432	10	0.008
4	979	$3.2*10^3$	13	0.011
5	$6.1*10^3$	$24*10^3$	16	0.024
6	$38*10^3$	$171*10^3$	19	0.028
7	$230*10^3$	$1.1*10^6$	22	0.035
8	$1.4*10^6$	$7.8*10^6$	25	0.049
9	$8.4*10^6$	$52*10^6$	28	0.071
10	$50*10^6$	$343*10^6$	31	0.097
15	$392*10^9$	$3.8*10^{12}$	46	0.498

- `Quantitative properties:` One important usage for probabilistic model checking is to compute the actual probability of some behaviors of the system. We can calculate the probability for eventually the customer $Cus1$ commits to send the payment to the merchant $Mer1$ and eventually the customer fulfills the commitment:

  $\varphi_6 = \mathbb{P}_{=?}$ [F $C_{Cur1 \to Mer1} Pay$]

  $\varphi_7 = \mathbb{P}_{=?}$ [F $Fu(C_{Cur1 \to Mer1} Pay)$]

4.4.3 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 experiments were performed on a Toshiba Portégé computer with 2.00 GHz Intel Core2 Duo T6400 processor and 3GB 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 4.1. 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 indicates the time

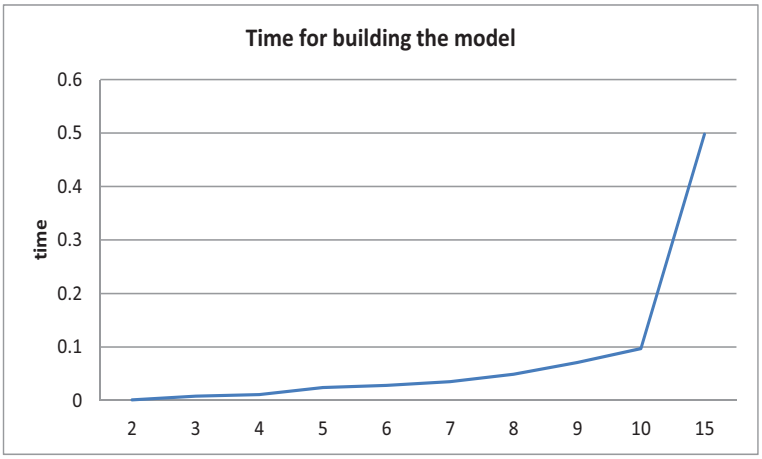

Figure 4.5: Model construction time for the NetBill protocol

Table 4.2: Verifying some PCTL^{kc} properties for the NetBill protocol in case of two agents

Formulae	Results	Time for MC (sec)
φ_1	True	0.001
φ_2	True	0.001
φ_3	True	0.008
φ_4	True	0.001
φ_5	True	0.008
φ_6	0.80	0.002
φ_7	0.72	0.001

for converting the PRISM model into a symbolic model and iterations required to find the reachable states. We have noticed that the state space increases exponentially as the number of agents increases. However, the time needed for constructing the model increases polynomially as more agents are added as shown in Figure 4.5.

We verified properties expressing some requirements of the NetBill protocol that involve probabilistic knowledge and commitments. We checked *Safety, liveness,* and *Reachability* properties as discussed above. Table 4.2 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.

4.4.4 Discussion

As we have seen in this chapter, a probabilistic logic for addressing the interaction between knowledge and social commitments in MASs was introduced. The described approach represents the first attempt in the literature to reason about and verify the interaction between the two concepts in the presence of uncertainty. However, from a consistency point of view, the logic we proposed seems to be inconsistent and suffers from some paradoxes like those identified in [1]. The problem is that, one of the underlying logics of PCTL^{kc}, which is PCTLC [107], is built using the social accessibility relation given in [9, 34] which, in fact, over specifies and over constrains the concept of illocutionary communication.

In the next chapter, we see how we will overcome the aforementioned problem by extending a consisting logic of knowledge and commitment called CTLKC^{+} [1] by a probabilistic operator so that capturing and reasoning about the interaction between the concepts of knowledge and social commitments by means of a consistence probabilistic logic becomes possible. Moreover, the logic we introduce in Chapter 5 incorporates the concepts of group social commitments and group knowledge to the framework.

4.5 Related Work

The work presented in this chapter can be related to three perspectives in the literature: probabilistic knowledge, probabilistic commitments, and the interaction between the two aspects. In this section, we review the relevant work with respect to probabilistic knowledge and the interaction between probabilistic knowledge and probabilistic commitments. However, for the relevant work on probabilistic commitments, it has been discussed in Chapter 3, Section 3.5.

4.5.1 Probabilistic Knowledge in MASs

Delgado and Benevides in [26] 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 adds two modalities on top of PCTL; one for the knowledge, and one for the commitments and their fulfilments. Therefore, dimension of system's aspects that our logic can handle is larger than that of K-PCTL making it more expressive. 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 [62], Huang and his colleagues extended the MCK model checker [48] 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 exiting PRISM model checker, we do not add a computational cost that is associated to extending the existing version of it.

Wan et al. [116] 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 PCTLK 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 forumla, 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.

4.5.2 The Interaction between Knowledge and Social Commitments

Little work has been done towards the problem of capturing and verifying the interactions between knowledge and social commitments in MASs.

In [95], Schmidt and his colleagues investigated the problem of formalizing the interaction between knowledge and commitments within agent dynamic logic. Apparently, the commitment adopted in this work is not a social commitment but rather an internal commitment as the one presented by Castelfranchi in [18]. The term "internal commitment" refers to a commitment of an agent to itself [99]. Using their proposed Agent Dynamic Logic (ADL), the authors were able to express some combinations between knowledge and commitments such as $Comm_i\ (\alpha) \rightarrow K_i\ Comm_i\ (\alpha)$ which expresses that agent i knows (K_i) about his internal commitment ($Comm_i$) to perform the action α. However, from a communication perspective, the internal commitment is neither communicative nor public because it is not created as an agreement between two agents so that an agent can commit towards the other to bring about a certain property. In contrast, our work focuses primary on the notion of "social commitment" [98] which has been used as a means of communication between interacting agents in MASs. Unlike internal commitments, which are private and concern a particular agent, social commitments are public and observable engagements from one agent to another agent or a group of agents to bring about something. Furthermore, unlike [95], we study such an interaction —between the two concepts— in systems exhibiting probabilistic behaviors.

Al-Saqqar et al. [1] have made the first attempt towards studying the relationship between knowledge and communicative social commitments from a logical perspective. In particular, they combined a logic of knowledge (called CTLK [77]) and a logic of commitments (called CTLC [9]) in a single tool called CTLKC. Having analyzed some postulates with different combinations between the two concepts expressed in CTLKC, the authors

identified a set of paradoxes that makes their combined logic inconsistent. To overcome this problem, they mitigated the over-specification problem that arises in the social accessibility relation given in [9, 34]. Intuitively and broadly speaking, a social accessibility relation for two agents i and j does exist between two global states s_1 and s_2 in the system, if there is a communication channel between the local states of i and j in the global states s_1 and s_2 respectively. Based on a new social accessibility relation, they presented a new semantics for the commitment ($C_{i\to j}\varphi$) and fulfilment ($Fu(C_{i\to j}\varphi)$) operators, where $C_{i\to j}\varphi$ means that agent i commits towards agent j to bring about φ, and $Fu(C_{i\to j}\varphi)$ expresses the fulfillment of such a commitment. These changes have been integrated into a new consistent logic named CTLKC$^+$. Having defined the new logic, the authors have been successfully able to reason about various combinations between knowledge $K_i\varphi$, which means that agent i knows φ, and social commitments as follows:

- $C_{i\to j}\varphi \Rightarrow K_i(C_{i\to j}\varphi)$ where $i \neq j$.
- $Fu(C_{i\to j}\varphi) \Rightarrow K_i\varphi$ where $i \neq j$.
- $Fu(C_{i\to j}\varphi) \Rightarrow K_j\varphi$ where $i \neq j$.

Then, the authors introduced a reduction model checking technique in which they transformed the problem of model checking their new logic (CTLKC$^+$) into the problem of model checking an existing logic called GCTL* [15], and computed the complexity of the reduction technique. They used the automata-based model checker CWB-NC as the verification tool.

The verification of CTLKC$^+$ was further investigated in [2]. The authors used a symbolic model checking technique based on reducing the problem of model checking CTLKC$^+$ into that of ARCTL. Then, they used the extended NuSMV to verify some given properties written in CTLKC$^+$. Their approach was carried out automatically using a JAVA

transformation tool. This allowed them to overcome the scalability problem of automata-based model modeling checking techniques, which is a highly considerable problem in model checking real applications of multi-agent systems. The complexity analysis of the proposed reduction-based technique was also provided.

Unlike this work that tends to assume ideal behavior for MASs so it limits its application to reliable environments, ours considers the unreliable behavior of MASs. Therefore, we add a probabilistic modality to the logic to be able to reason about some desirable properties in the presence of uncertainty. Our proposal subsumes the one in [1] because probability values range from 0 to 1 (when probability is equal to 1, the system becomes certain). Therefore, 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.

4.5.3 Comparison

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 systems 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 4.3 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.

Table 4.3: Comparison between PCTL^{kc} and the related work

Approach	Knowledge	Commitment	Uncertainty	Formal	Verification
[117, 118]		√	√		
[62]		√	√	√	√
[26]	√		√	√	
[116]	√		√	√	√
[1]	√	√		√	√
Our approach	√	√	√	√	√

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 represent and verify the interaction between knowledge and social commitments in the face of uncertainty. Moreover, the new probabilistic interpreted systems introduced in this chapter helps MASs developers to have rich modeling with respect to 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.

4.6 Summary

In this chapter, we presented a novel technique for specifying and evaluating the interaction between knowledge and social commitments in stochastic MASs. The proposed technique allows us, for the first time in the literature, to perform epistemic reasoning on social commitments in probabilistic MASs. This helps ensure agents' awareness about their commitments and the fulfillments of these commitments. In particular, we first 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^{kc}, 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^{kc} is transformed (by the use of some rules) 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 results have initially confirmed the expressive capabilities of PCTL^{kc} in handling the interaction between knowledge and social commitments in probabilistic settings. Moreover, the scalability of the proposed model checking technique was evaluated and models having up to 4×10^{11} states can be effectively verified.

In the next chapter, we refine and extend the approach presented for the interaction between individual knowledge and commitments to accommodate group knowledge and group commitments as well.

Chapter 5

On Probabilistic Group Social Commitments

In this chapter[1], we improve and extend the work presented in Chapter 4 by refining the probabilistic logic of knowledge and commitment (PCTL^{kc}) and then extending the refined logic further by operators for group knowledge and group commitment. In this respect, we define a semantics for the group social commitment operator and integrate it into the resulting logic. The developed logic is called the new probabilistic logic of knowledge and commitment (PCTL^{kc+}). Finally, we introduce a new formal verification technique that considers the new group modalities and implement it on top of the PRISM model checker.

5.1 Introduction

One of the major challenges in building complex software products such as Multi-Agent Systems (MASs) is to advance error detection at early stages of their life-cycles. MASs

[1]Part of the results presented in this chapter, namely PCTL^{kc+} logic, has been published in SoMet_14 [104]. The results of model checking PCTL^{kc+} have been sumbitted to the Engineering Applications of Artificial Intelligence journal [105]

community has witnessed an important shift in defining the semantics of ACLs from the so-called mental approaches that is hard to verify [98] to social approaches which exploit observable and verifiable social commitments. However, the increasing demand to use social commitments as a means of communication among interacting parties [6, 20, 54] requires reasoning about and verifying the relationship between social commitments and some other systems' aspects such as agents' knowledge and uncertainty especially in the case of having group-commitment scenarios. In addition to verifying the interactions between social commitments and knowledge in the presence of uncertainty, the ultimate objective of this chapter is to verify the interactions between the two elements when the scope of interacting agents goes beyond the common agent-to-agent (i.e., one-to-one) scheme.

In order to effectively capture and express the interactions between individual and group social commitments and knowledge in probabilistic MASs, we propose a new modal logic called the new probabilistic logic of knowledge and commitments $\text{PCTL}^{\text{kc+}}$ which is built by combining a consistent logic of knowledge and commitment CTLKC^{+} [1] with a well established probabilistic temporal logic PCTL [57]. The resulting logic is extended further to accommodate operators for the group knowledge and group commitments.

At present, there is a relatively large gap in addressing the concepts of knowledge and social commitments simultaneously in MASs, especially with the presence of uncertainty. Existing approaches that address the interaction between knowledge and social commitments either limit the scope of interacting agents to the widely used one-to-one commitment scheme and ignore the uncertainty aspect of MASs [1], or adopt a different kind of commitments called "internal commitment" rather than the "social commitments" that we consider in this thesis [95]. Furthermore, although the notion of "group" is important in the multi-agent community [94, 128], group social commitments has not been formalized and verified yet. As knowledge and social commitments influence each other in many real world

applications [1], their interactions need to be reasoned about and verified in a systematic manner. As we said before, uncertainty in MASs may arise due to imperfect information about the environment in which agents interact. Besides, in some situations, it happens that even if there is some state of affairs (i.e., content of a commitment) that an agent wants to bring about, its actions might not reliably drive the state of affairs into the desired state [103]. Consequently, commitments themselves become stochastic and the degree to which the commitment can be satisfied is not always guaranteed.

To motivate our study of representing and verifying the interaction between individual and group knowledge and social commitments in probabilistic MASs when taking into account one-to-many commitments, let us consider the following simple example. A professor teaching an engineering course with a capacity of 20 students. Various scenarios could happen within this context.

- `Scenario 1`: while the professor was explaining some new concepts in the course, one of the students asked the professor to provide him with more material regarding these concepts. The professor then promised to email the student some references the next day. This promise can be considered as a commitment from the professor towards the student to provide him with extra material for the new concepts.

- `Scenario 2`: in the lecture before the mid-term exam, students requested the professor to exclude some material and shorten the duration of the exam accordingly. At the end of the lecture, the professor agreed to exclude some parts of the covered material and to make the exam one hour long. This agreement can be considered as a commitment from the professor to the group of students who are registered in this course. Right after the class, the professor posted in the course web site an update confirming what they agreed on.

In the first scenario, obviously both the professor and student are aware of the commitment

(sending extra materiel). However, in the second scenario, every student registered in the course, and not necessarily present during the lecture, has to know about this agreement (commitment) to avoid wasting time studying excluded parts. In fact, because of some unexpected factors like absence of the professor on the day of the exam, email delivery failure, power outage, etc, there is no guarantee that these commitments are going to be surely fulfilled. Therefore, it is important to have a logic system with the ability to not only express the interaction between knowledge and social commitments, but also to handle the concepts of knowledge and commitments within the scope of a group when uncertainty matters. Once such a logic is defined, it can be invested as the underlying logic for a verification technique to verify some desirable and useful properties expressing combinations of knowledge and social commitments under uncertainty.

The work presented in this chapter can be seen as extension and continuation of the work presented in Chapter 4 where reasoning about and verifying interactions between individual knowledge and social commitments in probabilistic MASs were first introduced. In Chapter 4, we proposed a probabilistic logic called PCTL^{kc} whose expressiveness power allowed us to formulate combinations of the two concepts in the presence of uncertainty. PCTL^{kc} logic was built by fusing two logics, namely PCTLC [107] and PCTLK [116] using the independent join technique [46]. However, as pointed out in [1], the social accessibility relations given in [9, 34], have an over-specification problem, and consequently the PCTL^{kc} logic suffers from some paradoxes as it adopts the aforementioned accessibility relations.

To elaborate, there exist some situations that are not desirable in real settings but with the use of PCTL^{kc}, they are valid. One major problem in PCTL^{kc} is that agents commit everything they know to others, which brings the lack of privacy into being. Formally, this is represented by the following postulate:

- $K_i\varphi \Rightarrow C_{i\rightarrow j}\varphi$, where $i \neq j$.

The validity of this postulate is based on the fact that by establishing communication channels through which commitments are supposed to be exchanged, the epistemic relation needed to define the semantics of knowledge is also established. This is not reasonable in open environments where agents are selfish. Another problem is that agents commit everything known by others. That is, when an agent knows that another agent knows something, the first agent commits to bring about what the other agent knows, formally:

- $K_i K_j \varphi \Rightarrow C_{i \to j} \varphi$ where $i \neq j$.

Such a postulate should be avoided in MASs because it is not realistic for an agent to commit for something that is out of its capabilities. Moreover, this postulate can result in serious circumstances if agent j is malicious, so it can express incorrect knowledge about the other agent, obliging it to establish unwanted commitment.

On the other hand, we have some reasonable situations that should be always valid but with the use of PCTL^{kc} they can be unsatisfied. One example in this respect is when agents should be always aware about the fulfillment of their own commitments.

- $Fu(C_{i \to j} \varphi) \Rightarrow K_i Fu(C_{i \to j} \varphi)$ where $i \neq j$

It is realistic for this postulate to be valid because any agent should be aware of its fulfillment actions in order to prevent fulfilling the same commitment again and again. However, this postulate is not valid in PCTL^{kc} because of the same reasons mentioned earlier. Consequently, PCTL^{kc} fails to efficiently handle some practical situations in which knowledge and social commitments need to interact.

The problem is that one of the underlying logics of PCTL^{kc}, which is PCTLC [107], is built using the social accessibility relations given in [9, 34], which in fact over specifies and over constrains the concept of illocutionary communication. In a recent work, Al-Saqqar et al. [1] have figured out that although the social accessibilities presented in [9, 34] function

perfectly when the concern is to model social commitments independently, they have some limitations when combined with the epistemic accessibility relations in the same model. The authors in [1] modified the social accessibility relations proposed in [9, 34] in order to prevent the unintended emergence of the epistemic accessibility relations from the social accessibility relations when the two accessibilities combined in the same model. Technically speaking, they relaxed the conditions upon which the social accessibility relations are established in order to decouple the social accessibility relations from the epistemic accessibility relations. The new definition of social accessibilities does no longer depend on the unshared variables but rather depends merely on the shared variables between the interacting agents as discussed in Chapter 2. The new condition upon which a communication channel is established is stated below:

$s \approx_{i \to j} s'$ iff $Var_i \cap Var_j \neq \emptyset$ such that $\forall x \in Var_i \cap Var_j$ we have $l_i^x(s) = l_i^x(s') = l_j^x(s')$, where $\approx_{i \to j} \subseteq S \times S$ is the social accessibility relation. It has been proven that with the new social accessibilities, the resulting logic is consistent [1].

The work presented in this chapter differs from the one proposed in Chapter 4 in the following points:

1. While the logic presented in Chapter 4 suffers from some paradoxes, the current work builds upon a consistent logic of knowledge and commitment CTLKC$^+$ [1] which ensures having a paradox-free logic.

2. The new logic allows us to reason about commitments among multiple agents instead of limiting the scope to merely two agents. The concept of group knowledge is also integrated to the framework allowing us to reason about the knowledge in the case of group of agents.

3. In the current work, we generalize the model checking technique that has been proposed in Chapter 4 to fit the new group commitment operators as well.

The contributions of this chapter are threefold. First, we present a new probabilistic logic called (PCTL^{kc+}) with expressiveness abilities to capture and represent the interactions between individual and group knowledge and social commitments. Second, we introduce a formal verification technique for the probabilistic logic PCTL^{kc+}. The proposed technique is based on reducing the problem of model checking PCTL^{kc+} to the problem of model checking PCTL. This is achieved through 1) advocating a set of transformation rules that transform the PCTL^{kc+} model into a Markov Decision Process (MDP), and then converting the obtained MDP into a DTMC using the notion of "adversary" [43]; 2) reducing PCTL^{kc+} formulae into PCTL formulae based on a set of formal reduction rules. Third, we implement our reduction model checking technique on top of PRISM and apply it on a concrete case study, namely the online shopping system [52]. We then check some system's properties written as PCTL^{kc+} formulae using the PRISM model checker by checking their corresponding PCTL formulae. Figure 5.1 depicts a schematic view of our proposed framework.

5.2 The New Probabilistic Logic of knowledge and Commitment (PCTL^{kc+})

To overcome the inconsistency problem of PCTL^{kc}, we develop a new logic called the new probabilistic logic of knowledge and commitment (PCTL^{kc+}). To build PCTL^{kc+}, there are two obvious resources available in the literature: 1) the traditional temporal logics that have been developed for knowledge and social commitments independently or together such as CTLC [9], CTLK [77], and CLTKC^{+} [1]; and 2) the existing probabilistic logics available in the literature such as PCTL [57], PCLTK [116], and PCTLC [103]. Unfortunately, none of these resources is perfectly suitable for the task. The former resource neglects

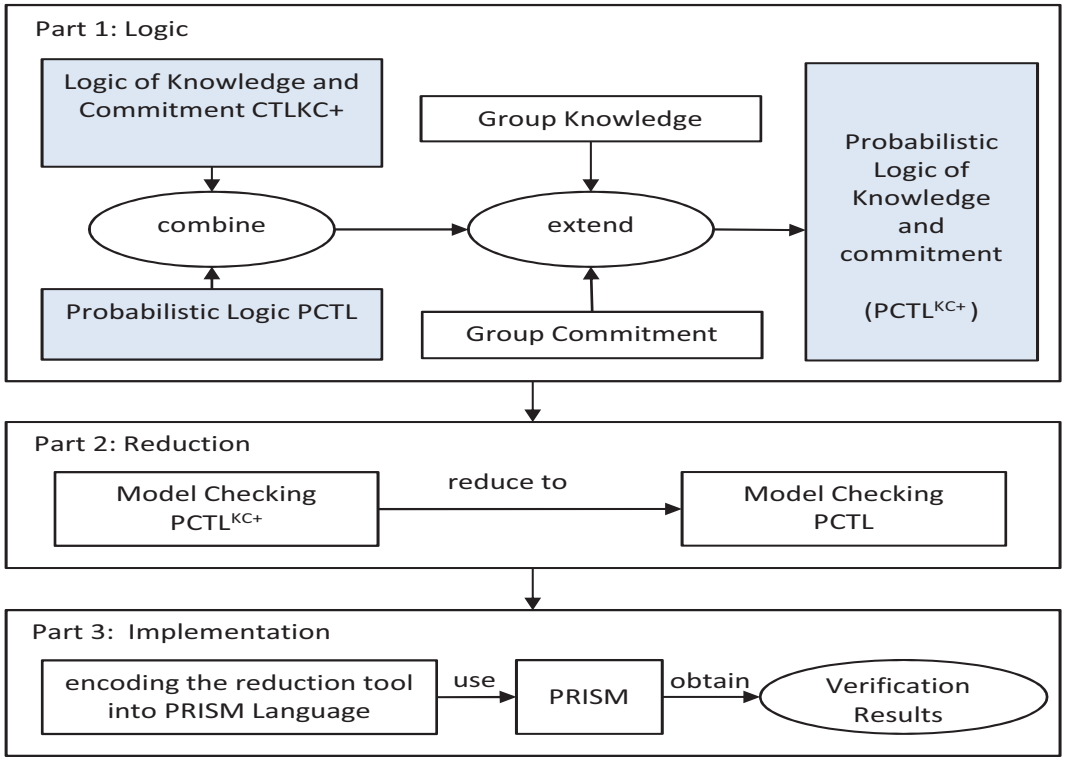

Figure 5.1: A schematic view of the probabilistic group social commitment approach

the uncertainty aspects in MASs, while the latter doesn't capture the interaction between knowledge and social commitments. Therefore, we propose a solution that draws upon both resources. In particular, we combine an existing consistent logic of knowledge and commitment CTLKC^{+} [1] with a well established probabilistic temporal logic PCTL [57]. Then, we extend the resulting combined logic by adding new operators for the group knowledge and group commitment.

Before going further, let us first describe a new probabilistic model over which PCTL^{kc+} formulae can be interpreted. This model is an extension of the formalism of interpreted systems [40] with the concepts of epistemic accessibility and social accessibility relations. Concretely, the model of PCTL^{kc+} is generated from combining two extended versions of the interpreted systems formalism. These extended formalisms are the extended version

introduced in [55, 116] and a modified version of the extended version given in [9, 34] due to Al-Saqqar et al. [1].

Definition 5.1 (PCTL$^{\text{kc+}}$ Model)**.**
Given a set of atomic propositions $\Phi_p = (p, q, r, \ldots)$ and a set of agents $\mathtt{Agt} = \{1, \ldots, n\}$, the model $\mathfrak{M}_3 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\approx_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, \nu)$ is a tuple where:

- $S \subseteq L_1 \times \ldots \times L_n$ is a countable set of all reachable global states of 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.

- $\mathbf{P} : S \times S \to [0, 1]$ is a total transition probability function defined as $\mathbf{P}(s, s') = \tau(s, a^{s\to s'}, s')$ iff there exists a joint action $a = (a_1, \ldots, a_n) \in ACT$ such that $\sum_{i\in \mathtt{Agt}} \tau_i(l_i(s), a^{l_i(s)\to l_i(s')}, l_i(s')) > 0$ and $\sum_{s'\in S} \mathbf{P}(s, s') = 1$ for all $s \in S$.

- $\sim_i \subseteq S \times S$ is the epistemic accessibility relation for the agent i, such that for two global states s and s', we have: $s \sim_i s'$ iff $l_i(s) = l_i(s')$.

- For each pair $(i, j) \in \mathtt{Agt}^2$, $\approx_{i\to j} \subseteq S \times S$ is the social accessibility relation which is defined as follows: $s \approx_{i\to j} s'$ iff $Var_i \cap Var_j \neq \emptyset$ such that $\forall x \in Var_i \cap Var_j$ we have $l_i^x(s) = l_i^x(s') = l_j^x(s')$.

- $\nu : S \to 2^{\Phi_p}$ is a valuation function.

The new model $\mathfrak{M}_3$ differs from the model $\mathfrak{M}_2$, presented in Chapter 4, in one particular point which is the social accessability relation. While $\mathfrak{M}_2$ uses the social accessibility relation $\sim_{i\to j}$ that has been introduced in [9, 34], the new model adopts the one $\approx_{i\to j}$ proposed in [1] in order to overcome the over-specification problem appeared in $\sim_{i\to j}$.

5.2.1 Syntax of PCTL$^{\mathbf{kc+}}$

Definition 5.2 (PCTL$^{\text{kc+}}$ syntax)**.** Let $\Phi_p = \{p, q, \dots\}$ be a set of atomic propositions, and $\mathtt{Agt} = \{1, \dots, n\}$ be a set of agents. The syntax of PCTL$^{\text{kc+}}$, which is a combination of PCTLK [116] and PCTLC [103, 107] augmented with further operators for the group knowledge, is given by the following grammar:

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathscr{K} \mid \mathscr{C} \mid \mathbb{P}_{\bowtie k}(\psi) \mid \mathbb{P}_{\bowtie k}(\mathscr{K}) \mid \mathbb{P}_{\bowtie k}(\mathscr{C})$$

$$\psi ::= \bigcirc\varphi \mid \varphi \; U \; \varphi \mid \varphi \; U^{\leq m} \; \varphi$$

$$\mathscr{K} ::= K_i \; \varphi \mid E_G \; \varphi$$

$$\mathscr{C} ::= C_{i \to j} \; \varphi \mid C_{i \to G} \; \varphi \mid Fu(C_{i \to j} \; \varphi) \mid Fu(C_{i \to G} \; \varphi)$$

where;

– $p \in \Phi_p$ is an atomic proposition

– $i, j \in \mathtt{Agt}$.

– $G \subseteq \mathtt{Agt}$.

– $\mathbb{P}_{\bowtie k}$ is a probabilistic operator and $\bowtie \in \{<, \leq, >, \geq\}$.

– $k \in [0, 1]$ is a probability bound or threshold.

$m \in \mathbb{N}^+$ is a positive integer number reflecting the maximum number of transitions needed to reach a certain state.

– The Boolean connectives $\neg$ and $\vee$ are defined in the usual way.

– φ and ψ are state and path formulae interpreted over the states and paths of $\mathfrak{M}_3$ respectively.

– The modal connectives $\mathscr{K}$ and $\mathscr{C}$ stand for “epistemic" and “social" operators, respectively.

In this logic, formulae $\mathscr{K}$ are state formulae and used to express the epistemic properties through the operators; K_i which stands for agent i knows, E_G which stands for everyone knows. Modal connectives $C_{i\to j}$ and $C_{i\to G}$ are called social formulae and stand for "commitment" from a debtor towards a single creditor, and "commitment" from a debtor to a group of creditors, respectively. Likewise, modal connectives $Fu(C_{i\to j})$ and $Fu(C_{i\to G})$ stand for "fulfillment" of the commitment $C_{i\to j}$ and "fulfillment" of the commitment $C_{i\to G}$, respectively. $\bigcirc, U$ and $U^{\leq m}$ stand for "next time", "until" and "bounded until" path modal connectives respectively.

5.2.2 Social Commitments Classification

Social commitments for agent communication have been always looked at within the scope of one-to-one. However, back to our motivating example, we realize that in addition to the usual agent-to-agent scheme, there are certain situations where group-agent commitments are needed. In this chapter, we are interested to move beyond the scope of one-to-one and investigate the case of committing to multiple agents. The idea of investigating other schemes of social commitments rather than the one-to-one commitment scheme seems to be both technically interesting and intuitively appealing. In what follows, we distinguish between two different flavors of social commitments, namely basic (or individual) social commitment and group social commitment.

Definition 5.3 (Basic Social Commitment)**.**

A basic social commitment is an agreement between two agents namely, `debtor` and `creditor` such that the `debtor` engages towards the `creditor` to bring about a certain property.

This is the simplest form of social commitments and has long been investigated in the literature. The commitment in this case can be represented using the following operator:

$C_{i \to j}\ \varphi$ where i denotes the debtor, j denotes the creditor, and φ denotes the content of the commitment. The fulfillment of such a commitment is written as follows: $Fu(C_{i \to j}\ \varphi)$. However, as the common form of social commitments is the basic social commitment, we can simply use “social commitments" to refer to “basic (or individual) social commitments".

Definition 5.4 (Group Social Commitment)**.**

A group social commitment is an agreement between a `debtor` and a group of `creditors` to bring about a certain property.

This kind of commitments indicates the involvement of multiple agents in the same commitment. The creditor is a group of independent agents that join together as a single party due to their shared interests in the commitment at hand. A group social commitment is represented using the following notation: $C_{i \to G}\ \varphi$, where i denotes the debtor, G denotes a group of creditors, and φ denotes the content of the commitment. The fulfillment of such a commitment is given by the notation $Fu(C_{i \to G}\ \varphi)$. Technically, a group social commitment can be seen as the conjunction of individual basic social commitments from the debtor i to each agent in the group of creditors G. Formally, $C_{i \to G}\ \varphi \equiv \bigwedge_{j \in G} C_{i \to j}\ \varphi$. An intuitive explanation of the operator $C_{i \to G}\ \varphi$ is as follows: for a group social commitment to be held at a certain state, the content of the commitment must be true at every accessible state from the commitment state with respect to the group. This implies that none of the group members could be excluded from having all accessible states satisfy the content of the commitment. Consequently, it is obvious that for a state to be socially accessible from the commitment state with respect to the group, it has to be socially accessible with respect to at least one of the agents of the group. Therefore, we resolve the accessibility problem resulted from having group commitments by taking the union of the social accessibility relations of each single agent in the group. This in turn leads us to define the group social accessibility relation based on the social accessibility relations presented in Definition 5.1.

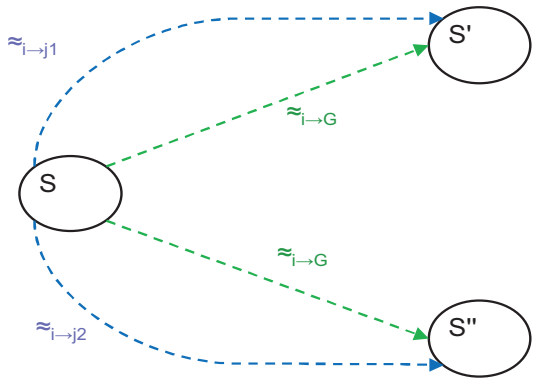

Figure 5.2: Accessibility relations for group social commitment

Let $G \subseteq \texttt{Agt}$ be a group of agents. We define the group social accessibility relation from the social accessibility relation $\approx_{i\to j}$ as follows:

Definition 5.5 (Social Accessibility Relations for Group Social Commitment)**.**

- $\approx_{i\to G}$ is the union of the social accessibility relations between agent i and each agent in the group G: $\approx_{i\to G} = \bigcup_{j\in G} \approx_{i\to j}$.

Notice that group social commitments have all the properties of basic social commitments with an additional constraint that they can involve more than two agents. However, a group social commitment involving only two agents is equivalent to the basic social commitment. Figure 5.2 depicts the idea of group social accessibility ($G = \{j_1, j_2\}$).

5.2.3 Group Knowledge

In this work, we limit the scope of group knowledge to the concept of “Everyone Knows" introduced in [40]. “Everyone Knows" is denoted by $E_G\ \varphi$ and means that everyone in the group G knows φ. Technically, “Everyone knows" can be seen as the conjunction of the individual knowledge of each agent in the group. Formally, $E_G\ \varphi \equiv \bigwedge_{i\in G} K_i\ \varphi$.

Before we proceed to present the semantics of PCTL$^{\text{kc+}}$, we need to define the epistemic accessibility relation for $E_G\ \varphi$. Let $G \subseteq \texttt{Agt}$ be a group of agents. We define the epistemic accessibility relation for $E_G\ \varphi$ from the epistemic accessibility relation $\sim_i$ as follows [116]:

Definition 5.6 (Epistemic Accessibility Relation for Everyone Knows)**.**

- $\sim_G^E$ is the union of group $G's$ accessibility relations: $\sim_G^E = \bigcup_{i \in G} \sim_i$.

5.2.4 Semantics of PCTL$^{\text{kc+}}$

Given a model $\mathfrak{M}_3 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\approx_{i \to j}\}_{(i,j) \in \texttt{Agt}^2}, v)$, then $(\mathfrak{M}_3, s) \models \varphi$ states that "a state s in the model $\mathfrak{M}_3$ satisfies a state formula φ, $(\mathfrak{M}_3, \pi) \models \psi$ means that "a path π in the model $\mathfrak{M}_3$ satisfies a path formula ψ, and $(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k}(\psi)$ means that "a state s in $\mathfrak{M}_3$ satisfies $\mathbb{P}_{\bowtie k}(\psi)$ if the probability of taking a path from s that satisfies ψ is in the interval specified by $\bowtie k$". When the model $\mathfrak{M}_3$ is clear from the context, we simply write the satisfaction relation $\models$ as follows: $s \models \varphi$ and $\pi \models \psi$. Furthermore, we denote the number of socially accessible states s' from a given state s such that $s \approx_{i \to j} s'$ by $|s \approx_{i \to j} s'|$, and $s \approx_{i \to G} s'$ by $|s \approx_{i \to G} s'|$. We also denote the number of epistemically accessible states s' from a given state s such that $s \sim_i s'$ by $|s \sim_i s'|$. Similarly, we denote the number of states s' that are accessible from a given state s through $\sim_G^E$ by $|s \sim_G^E s'|$. Finally, we define $|s \models \varphi|$ as follows:

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

Definition 5.7 (**Satisfaction**)**.** Satisfaction of a PCTL$^{\text{kc+}}$ formula in the model $\mathfrak{M}_3$ is conductively defined as follows:

$s \models p$ *iff* $p \in \nu(s)$;

$s \models \varphi_1 \vee \varphi_2$ *iff* $s \models \varphi_1$ or $s \models \varphi_2$;

$s \models \neg\varphi$ *iff* $s \not\models \varphi$;

$s \models K_i\varphi$ *iff* $\forall s' \in S$ s.t. $s \sim_i s'$, we have $s' \models \varphi$;

$s \models E_G\ \varphi$ *iff* $\forall s' \in S$ s.t. $s \sim_G^E s'$, we have $s' \models \varphi$;

$s \models C_{i\to j}\varphi$ *iff* $\forall s' \in S$ s.t. $s \approx_{i\to j} s'$, we have $s' \models K_i\varphi \wedge K_j\varphi$;

$s \models C_{i\to G}\varphi$ *iff* $\forall s' \in S$ s.t. $s \approx_{i\to G} s'$, we have $s' \models K_i\varphi \wedge E_G\ \varphi$;

$s \models Fu(C_{i\to j}\varphi)$ *iff* there exists $s' \in S$ such that $s' \approx_{i\to j} s$ and $s' \models C_{i\to j}\ \varphi$ or
there exists $s'' \in S$ and $s'' \sim_i s$ such that $s'' \models Fu(C_{i\to j}\ \varphi)$ or
there exists $s'' \in S$ and $s'' \sim_j s$ such that $s'' \models Fu(C_{i\to j}\ \varphi)$;

$s \models Fu(C_{i\to G}\ \varphi)$ *iff* there exists $s' \in S$ such that $s' \approx_{i\to G} s$ and $s' \models C_{i\to G}\ \varphi$ or
there exists $s'' \in S$ and $s'' \sim_i s$ such that $s'' \models Fu(C_{i\to G}\ \varphi)$ or
there exists $s'' \in S$ and $s'' \sim_G^E s$ such that $s'' \models Fu(C_{i\to G}\ \varphi)$;

$\pi \models \bigcirc\varphi$ *iff* $\pi(1) \models \varphi$;

$\pi \models \varphi_1\ U^{\leq m}\ \varphi_2$ *iff* $\exists k \leq m$ s.t. $\pi(k) \models \varphi_2$ and $\forall i < k, \pi(i) \models \varphi_1$;

$\pi \models \varphi_1\ U\ \varphi_2$ *iff* $\exists m \geq 0$ s.t. $\pi \models \varphi_1\ U^{\leq m}\ \varphi_2$;

$s \models \mathbb{P}_{\bowtie k}(\psi)$ *iff* $Prob_s(\psi) \bowtie k$ where: $Prob_s(\psi) = Prob_s\{\pi \in \Pi(s) \mid \pi \models \psi\}$;

• 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:

$s \models \mathbb{P}_{\bowtie k}(K_i\ \varphi)$ *iff* $Prob(s \models K_i\varphi) \bowtie k$ where: $Prob(s \models K_i\varphi) = \frac{\Sigma_{s\sim_i s'}\,|s' \models \varphi|}{|s \sim_i s'|}$;

$s \models \mathbb{P}_{\bowtie k}(E_G\ \varphi)$ *iff* $Prob(s \models E_G\ \varphi) \bowtie k$ where: $Prob(s \models E_G\ \varphi) = \frac{\Sigma_{s\sim_G^E s'}\,|s' \models \varphi|}{|s \sim_G^E s'|}$;

• 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 accessible

from s and satisfy the formula:

$s \models \mathbb{P}_{\bowtie k}(C_{i\to j}\varphi)$ *iff* $Prob(s \models C_{i\to j}\varphi) \bowtie k$ where: $Prob(s \models C_{i\to j}\varphi) = \frac{\sum_{s\approx_{i\to j}s'} |s'\models K_i\varphi\wedge K_j\varphi|}{|s\approx_{i\to j}s'|}$;

$s \models \mathbb{P}_{\bowtie k}(C_{i\to G}\varphi)$ *iff* $Prob(s \models C_{i\to G}\varphi) \bowtie k$ where: $Prob(s \models C_{i\to G}\varphi) = \frac{\sum_{s\approx_{i\to G}s'} |s'\models K_i\varphi\wedge E_G\varphi|}{|s\approx_{i\to G}s'|}$;

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

$s \models \mathbb{P}_{\bowtie k}(Fu(C_{i\to j}\varphi))$ *iff* $Prob(s \models Fu(C_{i\to j}\varphi)) \bowtie k$; where:

$$Prob(s \models Fu(C_{i\to j}\varphi)) = Prob_s\{\pi \in \Pi(s') \mid s' \approx_{i\to j} s \text{ and } \pi = s'\ldots s \text{ and } s' \models C_{i\to j}\varphi\};$$

$s \models \mathbb{P}_{\bowtie k}(Fu(C_{i\to G}\varphi))$ *iff* $Prob(s \models Fu(C_{i\to G}\varphi)) \bowtie k$; where:

$$Prob(s \models Fu(C_{i\to G}\varphi)) = Prob_s\{\pi \in \Pi(s') \mid \quad s' \approx_{i\to G} s \text{ and } \pi = s'\ldots s \text{ and } s' \models C_{i\to G}\varphi\}$$

Again as in Chapter 4, in the case of the knowledge, the uncertainty is computed in such a way that it reflects the indistinguishability property of the epistemic accessibility relations. Hence, the uncertainty is computed based on the probability of epistemic accessibility relations which is calculated 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. Likewise, probabilistic commitment is 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 5.1.

If $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to j}\varphi))$ *and* $(\mathfrak{M}_3, s) \models Fu(C_{i\to j}\varphi)$*, then s is not reachable from the commitment state.*

Theorem 5.1 (Epistemic Equivalences)**.**

1. $(\mathfrak{M}_3, s) \models \mathbb{P}_{\geq 1}(K_i\ \varphi)$ *iff* $(\mathfrak{M}_3, s) \models K_i\ \varphi$
2. $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(K_i\ \varphi)$ *iff* $(\mathfrak{M}_3, s) \models K_i\ \neg\varphi$
3. $(\mathfrak{M}_3, s) \models \mathbb{P}_{]0,1[}(K_i\ \varphi)$ *iff* $(\mathfrak{M}_3, s) \models \neg K_i\ \neg\varphi \wedge \neg K_i\ \phi$
4. $(\mathfrak{M}_3, s) \models \mathbb{P}_{\geq 1}(E_G\ \varphi)$ *iff* $(\mathfrak{M}_3, s) \models E_G\ \varphi$
5. $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(E_G\ \varphi)$ *iff* $(\mathfrak{M}_3, s) \models E_G\ \neg\varphi$
6. $(\mathfrak{M}_3, s) \models \mathbb{P}_{]0,1[}(E_G\ \varphi)$ *iff* $(\mathfrak{M}_3, s) \models \neg E_G\ \neg\varphi \wedge \neg E_G\ \varphi$

Proof. We prove the first three equivalences, the same method can be used to prove the others.

- First equivalence.

  " $\Rightarrow$ ". Assume $(\mathfrak{M}_3, s) \models \mathbb{P}_{\geq 1}(K_i\varphi)$. By the semantics of PCTL$^{\text{kc+}}$, it follows that $Prob((\mathfrak{M}_3, s) \models K_i\ \varphi) \geq 1$. Therefore, $\frac{\Sigma_{s\sim_i s'}|(\mathfrak{M}_3, s')\models\varphi|}{|s\sim_i s'|} \geq 1$. This means that $\forall s' \in S$ such that $s \sim_i s'$, we have $(\mathfrak{M}_3, s') \models \varphi$ (as $\sim_i$ is reflexive, so s' could be s itself). Thus, $(\mathfrak{M}_3, s) \models K_i\ \varphi$.

  " $\Leftarrow$ ". Assume $(\mathfrak{M}_3, s) \models K_i\ \varphi$. By the PCTL$^{\text{kc+}}$ semantics, it follows that for all

$s' \in S$ such that $s \sim_i s'$, we have $(\mathfrak{M}_3, s') \models \varphi$ (i.e. all accessible states from s satisfy φ). Consequently, $\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi| = |s \sim_i s'|$. Therefore, $\frac{\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi|}{|s \sim_i s'|} \geq 1$ and hence $(\mathfrak{M}_3, s) \models \mathbb{P}_{\geq 1} K_i \varphi$).

- Second equivalence.

  " $\Rightarrow$ ". Assume $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(K_i \varphi)$. By the PCTL$^{\text{kc+}}$ semantics, it follows that $Prob((\mathfrak{M}_3, s) \models K_i \varphi) \leq 0$. Thus, $\frac{\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi|}{|s \sim_i s'|} \leq 0$. Since $\sim_i$ is reflexive, so the set of the accessible states from s is not empty. Therefore, $\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi|$ must be 0 (i.e., φ is not true in any of the accessible states). Consequently, for all $s' \in S$ such that $s \sim_i s'$, we have $(\mathfrak{M}_3, s') \not\models \varphi$, which means $(\mathfrak{M}_3, s') \models \neg\varphi$. Hence, $(\mathfrak{M}_3, s) \models K_i \neg\varphi$.

  " $\Leftarrow$ ". Assume $(\mathfrak{M}_3, s) \models K_i \neg\varphi$. By the PCTL$^{\text{kc+}}$ semantics, it follows that $\forall s' \in S$ such that $s \sim_i s'$, we have $(\mathfrak{M}_3, s') \not\models \varphi$. Since the set of the accessible states from s is not empty, then $\frac{\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi|}{|s \sim_i s'|} \leq 0$. Hence, $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(K_i \varphi)$.

- Third equivalence.

  " $\Rightarrow$ ". Assume $(\mathfrak{M}_3, s) \models \mathbb{P}_{]0,1[}(K_i \varphi)$. By the PCTL$^{\text{kc+}}$ semantics, it follows that $0 < Prob(s \models K_i \varphi) < 1$. Thus, $0 < \frac{\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi|}{|s \sim_i s'|} < 1$. This means that it would never be the case that $\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi| = |s \sim_i s'|$ nor $\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi| = 0$. Consequently, there exist some $s', s'' \in S$ such that $s \sim_i s'$ and $s \sim_i s''$ and $(\mathfrak{M}_3, s') \models \varphi$ and $(\mathfrak{M}_3, s'') \models \neg\varphi$. Hence, it is impossible to have $(\mathfrak{M}_3, \bar{s}) \models \neg\varphi$ or $(\mathfrak{M}_3, \bar{s}) \models \varphi$ for all $\bar{s} \in S$ such that $s \sim_i \bar{s}$. Consequently, $(\mathfrak{M}_3, s) \not\models K_i \neg\varphi$ and $(\mathfrak{M}_3, s) \not\models K_i \varphi$. Hence $(\mathfrak{M}_3, s) \models \neg K_i \neg\varphi$ and $(\mathfrak{M}_3, s) \models \neg K_i \varphi$.

  " $\Leftarrow$ ". Assume $(\mathfrak{M}_3, s) \models \neg K_i \varphi$. By the PCTL$^{\text{kc+}}$ semantics, it follows that there exists $s' \in S$ such that $s \sim_i s'$ and $(\mathfrak{M}_3, s') \models \neg\varphi$. Consequently, it would never be the case that for all $s' \in S$ such that $s \sim_i s'$ we have $(\mathfrak{M}_3, s') \models \varphi$. Therefore, $1 > \frac{\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi|}{|s \sim_i s'|}$. Now assume $(\mathfrak{M}_3, s) \models \neg K_i \neg\varphi$. Therefore, $\sum_{s \sim_i s'} |(\mathfrak{M}_3, s') \models \varphi| =$

0 would never be the case as some accessible states should satisfy φ. Consequently, $\frac{\sum_{s\sim_i s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\sim_i s'|} > 0$. Thus, $0 < \frac{\sum_{s\sim_i s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\sim_i s'|} < 1$. Hence, $(\mathfrak{M}_3,s) \models \mathbb{P}_{]0,1[}(K_i\varphi)$.

□

Theorem 5.2 (Commitment Equivalences)**.**

1. $(\mathfrak{M}_3,s) \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$ *iff* $(\mathfrak{M}_3,s) \models C_{i\to j}\varphi$
2. $(\mathfrak{M}_3,s) \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$ *iff* $(\mathfrak{M}_3,s) \models C_{i\to j}\neg\varphi$
3. $(\mathfrak{M}_3,s) \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$ *iff* $(\mathfrak{M}_3,s) \models \neg C_{i\to j}\neg\varphi \wedge \neg C_{i\to j}\varphi$
4. $(\mathfrak{M}_3,s) \models \mathbb{P}_{\geq 1}(C_{i\to G}\varphi)$ *iff* $(\mathfrak{M}_3,s) \models C_{i\to G}\varphi$
5. $(\mathfrak{M}_3,s) \models \mathbb{P}_{\leq 0}(C_{i\to G}\varphi)$ *iff* $(\mathfrak{M}_3,s) \models C_{i\to G}\neg\varphi$
6. $(\mathfrak{M}_3,s) \models \mathbb{P}_{]0,1[}(C_{i\to G}\varphi)$ *iff* $(\mathfrak{M}_3,s) \models \neg C_{i\to G}\neg\varphi \wedge \neg C_{i\to G}\varphi$

Proof. We prove the first three equivalences, the same method can be used to prove the others.

- First equivalence.

  " $\Rightarrow$ ". Assume $(\mathfrak{M}_3,s) \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$. By the PCTL$^{\text{kc+}}$ semantics, it follows that $Prob((\mathfrak{M}_3,s) \models C_{i\to j}\varphi) \geq 1$. Thus, $\frac{\sum_{s\approx_{i\to j} s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j} s'|} \geq 1$. This means that for all $s' \in S$ such that $s \approx_{i\to j} s'$, we have $(\mathfrak{M}_3,s') \models \varphi$, and hence $(\mathfrak{M}_3,s) \models C_{i\to j}\varphi$.

  " $\Leftarrow$ ". Assume $(\mathfrak{M}_3,s) \models C_{i\to j}\varphi$. By the PCTL$^{\text{kc+}}$ semantics, it follows that for all $s' \in S$ such that $s \approx_{i\to j} s'$, we have $(\mathfrak{M}_3,s') \models \varphi$ (i.e. all accessible states from s satisfy φ). Consequently, $\sum_{s\approx_{i\to j} s'} |(\mathfrak{M}_3,s') \models \varphi| = |s \approx_{i\to j} s'|$. Therefore, $\frac{\sum_{s\approx_{i\to j} s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j} s'|} \geq 1$ and hence, $(\mathfrak{M}_3,s) \models \mathbb{P}_{\geq 1}(C_{i\to j}\varphi)$.

- Second equivalence.

  " $\Rightarrow$ ". Assume $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$. By the PCTL$^{\text{kc+}}$ semantics, it follows that $Prob((\mathfrak{M}_3, s) \models C_{i\to j}\varphi) \leq 0$. Thus, $\frac{\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j}s'|} \leq 0$. Since the set of the accessible states from s is not empty, then $\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3, s') \models \varphi|$ must be 0 (i.e. φ is not true in any of the accessible states). Consequently, for all $s' \in S$ such that $s \approx_{i\to j} s'$, we have $(\mathfrak{M}_3, s') \nvDash \varphi$, which means $(\mathfrak{M}_3, s') \vdash \neg\varphi$. Hence, $(\mathfrak{M}_3, s) \models C_{i\to j}\neg\varphi$.

  " $\Leftarrow$ ". Assume $(\mathfrak{M}_3, s) \models C_{i\to j}\neg\varphi$. By the PCTL$^{\text{kc+}}$ semantics, it follows that for all $s' \in S$ such that $s \approx_{i\to j} s'$, we have $(\mathfrak{M}_3, s') \nvDash \varphi$. Since the set of the accessible states from s is not empty, then $\frac{\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j}s'|} \leq 0$. Hence, $(\mathfrak{M}_3, s') \models \mathbb{P}_{\leq 0}(C_{i\to j}\varphi)$.

- Third equivalence.

  " $\Rightarrow$ ". Assume $(\mathfrak{M}_3, s) \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$. By the PCTL$^{\text{kc+}}$ semantics, it follows that $0 < Prob((\mathfrak{M}_3, s) \models C_{i\to j}\varphi) < 1$. Thus, $0 < \frac{\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j}s'|} < 1$. This means that it would never be the case that $\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3, s') \models \varphi| = |s \approx_{i\to j} s'|$ nor $\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3, s') \models \varphi| = 0$. Consequently, there exist some $s', s'' \in S$ such that $s \approx_{i\to j} s'$ and $s \approx_{i\to j} s''$ and $(\mathfrak{M}_3, s') \models \varphi$ and $(\mathfrak{M}_3, s'') \models \neg\varphi$. Hence, it is impossible to have $(\mathfrak{M}_3, \bar{s}) \models \neg\varphi$ or $(\mathfrak{M}_3, \bar{s}) \models \varphi$ for all $\bar{s} \in S$ such that $s \approx_{i\to j} \bar{s}$. Consequently, $s \nvDash C_{i\to j}\neg\varphi$ and $(\mathfrak{M}_3, s) \nvDash C_{i\to j}\varphi$. Hence $(\mathfrak{M}_3, s) \models \neg C_{i\to j}\neg\varphi$ and $(\mathfrak{M}_3, s) \models \neg C_{i\to j}\varphi$.

  " $\Leftarrow$ ". Assume $(\mathfrak{M}_3, s) \models \neg C_{i\to j}\varphi$. By the PCTL$^{\text{kc+}}$ semantics, it follows that there exists $s' \in S$ such that $s \approx_{i\to j} s'$ and $(\mathfrak{M}_3, s') \models \neg\varphi$. Consequently, it would never be the case that $(\mathfrak{M}_3, s') \models \varphi$ for all $s' \in S$ such that $s \approx_{i\to j} s'$. Therefore, $1 > \frac{\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j}s'|}$. Now assume $(\mathfrak{M}_3, s) \models \neg C_{i\to j}\neg\varphi$. Therefore, $\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3, s') \models \varphi| = 0$ would never be he case as some accessible states should satisfy φ. Consequently, $\frac{\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j}s'|} > 0$. Thus, $0 < \frac{\sum_{s\approx_{i\to j}s'} |(\mathfrak{M}_3,s')\models\varphi|}{|s\approx_{i\to j}s'|} < 1$. Thus, $(\mathfrak{M}_3, s) \models \mathbb{P}_{]0,1[}(C_{i\to j}\varphi)$.

□

Theorem 5.3 (Fulfillment Equivalences)**.**

1. $(\mathfrak{M}_3, s) \models \mathbb{P}_{>0}(Fu(C_{i\to j}\varphi))$ *iff* $(\mathfrak{M}_3, s) \models Fu(C_{i\to j}\varphi)$ *and s is reachable from the commitment state.*

2. $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to j}\varphi))$ *iff* $(\mathfrak{M}_3, s) \models \neg Fu(C_{i\to j}\varphi)$ *or s is not reachable from the commitment state.*

3. $(\mathfrak{M}_3, s) \models \mathbb{P}_{>0}(Fu(C_{i\to G}\varphi))$ *iff* $(\mathfrak{M}_3, s) \models Fu(C_{i\to G}\varphi)$ *and s is reachable from the commitment state.*

4. $(\mathfrak{M}_3, s) \models \mathbb{P}_{\leq 0}(Fu(C_{i\to G}\varphi))$ *iff* $(\mathfrak{M}_3, s) \models \neg Fu(C_{i\to G}\varphi)$ *or s is not reachable from the commitment state.*

Proof. The proofs of these equivalences are direct from Proposition 5.1 and the above semantics.

□

5.3 Model Checking PCTL^{kc+} using Reduction

In this section, we generalize the model checking technique for the logic of knowledge and social commitments proposed in Chapter 4 to cover more complex cases, such as group knowledge and group commitment. As we have seen in the previous section, the semantics of our new logic PCTL^{kc+} is defined over an extended version of interpreted systems $\mathfrak{M}_3$. The idea of our proposed verification technique is based mainly on reducing the problem of model checking PCTL^{kc+} to the problem of model checking PCTL. This however involves two processes. First, we define transformation rules to transform PCTL^{kc+} model ($\mathfrak{M}_3$) to an MDP model to be suitable for PRISM, the probabilistic model checker of PCTL. The solution of an MDP comes in the form of an "adversary" [43] which is described as a

mapping of states to probability distributions over actions. Second, we construct a set of rules to reduce PCTL^{kc+} formulae to PCTL formulae.

In a nutshell, our proposed model checking procedure is as follows. Given $\mathfrak{M}_3 = (S, \mathbf{P}, I, \sim_1, \ldots, \sim_n, \{\approx_{i\to j}\}_{(i,j)\in \mathtt{Agt}^2}, v)$, and PCTL^{kc+} formula φ, we have to define an MDP model $\mathfrak{M}'_3 = \mathscr{F}(\mathfrak{M}_3)$ and PCTL formula $\mathscr{F}(\varphi)$ using the transformation function $\mathscr{F}$ such that $\mathfrak{M}_3 \models \varphi$ iff $\mathscr{F}(\mathfrak{M}_3) \models \mathscr{F}(\varphi)$.

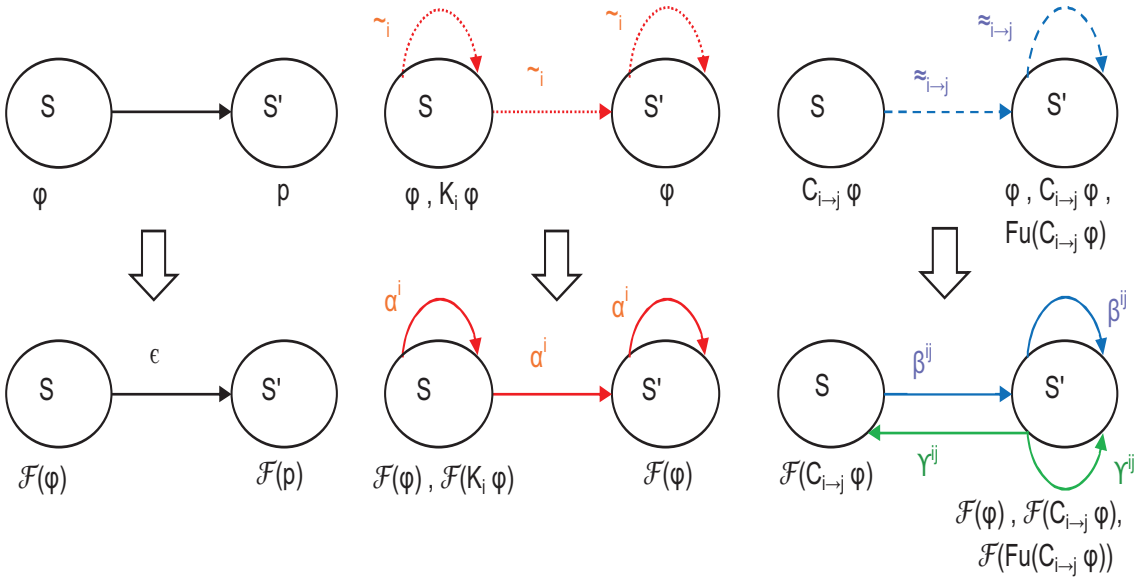

Figure 5.3: Examples of translating relations in $\mathfrak{M}_3$ into labeled transitions

5.3.1 Transforming the Model $\mathfrak{M}_3$

As done in Chapter 4, given an MDP model $\mathfrak{M}'_3 = (\mathbb{S}, Act, \mathsf{P}_t, I_i, L)$, a major step in transforming $\mathfrak{M}_3$ into $\mathfrak{M}'_3$ is to define the set of actions Act. The idea is to map each relation in $\mathfrak{M}_3$ into a corresponding action in Act; more specifically, to translate each relation in $\mathfrak{M}_3$ into a labeled transition in $\mathfrak{M}'_3$. Then, these labels (also called actions) are used to form the set Act in $\mathfrak{M}'_3$. Consequently, the different relations in $\mathfrak{M}_3$ namely, probabilistic transition

relations, epistemic accessibility relations, and social accessibility relations, are translated into labeled transitions in $\mathfrak{M}'_3$. Moreover, to interpret the fulfillment of a commitment, we need to add the symmetric closure of the transition resulted from translating the social accessibility relation. Figure 5.3 (where n is the number of agents, $1 \leq i \leq n$, and $1 \leq j \leq n$) explains the process of translating the probabilistic transition relation $\mathbf{P}$, epistemic accessibility relations $\sim_i$, and social accessibility relations $\approx_{i \to j}$ into labeled transitions. More precisely, the action ε denotes a transition defined from the probabilistic transition relation $\mathbf{P}$, action α^i denotes a transition defined from the epistemic accessibility relation $\sim_i$, action β^{ij} denotes a transition defined from the social accessibility relation $\approx_{i \to j}$, and action γ^{ij} denotes a transition added to capture the semantics of the fulfillment of a basic commitment. Likewise, the epistemic accessibility relation $\sim^E_G$, and the social accessibility relation $\approx_{i \to G}$ are translated in the same way where the action α^E_G denotes a transition defined from the epistemic accessibility relation $\sim^E_G$, action β^G denotes a transition defined from the social accessibility relation $\approx_{i \to G}$, and the action γ^G denotes a transition added to capture the semantics of the fulfillment of a group commitment. Consequently, the model $\mathfrak{M}'_3 = (\mathbb{S}, Act, \mathsf{P}_t, I_i, L)$ can now be defined as follows:

- $\mathbb{S}$=S; I_i=I; L=ν.
- $Act = \{\varepsilon\} \cup \{\alpha^1, \alpha^2, \ldots, \alpha^n, \alpha^E_G\} \cup \{\beta^{11}, \beta^{12}, \ldots, \beta^{nn}, \beta^G\} \cup \{\gamma^{11}, \gamma^{12}, \ldots, \gamma^{nn}, \gamma^G\}$ where n is the number of agents.
- P_t can be defined as the union of the transitions labeled with ε, transitions labeled with α^i, transitions labeled with α^E_G, transitions labeled with β^{ij}, transitions labeled with β^G, transitions labeled with γ^{ij}, and transitions labeled with γ^G. The probabilities of transitions labeled with ε are not manipulated but rather inherited from the

probabilistic transition function **P**. However, transitions labeled with α^i and emanating from the same state are given equal probabilities which reflect the indistinguishably property of epistemic relations over equivalent states. Thus, the probability of each transition annotated by α^i is equal to the probability of each other transition labeled with α^i emanating from the same state which is calculated by dividing one over the number of transitions labeled with α^i. The probabilities of transitions labeled with α^E_G, β^{ij}, β^G, γ^{ij}, and γ^G are calculated in the same way. For states $s, s' \in \mathbb{S}$ and action $\theta \in Act$, the function P_t is defined as follows:

$$\mathsf{P}_t(s,\theta,s') = \begin{cases} \mathbf{P}(s,s'), & \text{if } \theta = \varepsilon \\ \frac{1}{|s \sim_i s'|}, & \text{if } \theta = \alpha^i \\ \frac{1}{|s \sim^E_G s'|}, & \text{if } \theta = \alpha^E_G \\ \frac{1}{|s \approx_{i \to j} s'|}, & \text{if } \theta = \beta^{ij} \\ \frac{1}{|s \approx_{i \to G} s'|}, & \text{if } \theta = \beta^G \\ \frac{1}{|s' \approx_{i \to j} s|}, & \text{if } \theta = \gamma^{ij} \\ \frac{1}{|s' \approx_{i \to G} s|}, & \text{if } \theta = \gamma^G \end{cases}$$

As mentioned earlier, the non-deterministic choices in MDP are resolved using the adversary by picking one enabled transition at each state, which induces a DTMC model. Technically speaking, the adversary is a function from the state set S to the action set Act such that it chooses in any state s one of the enabled actions. In particular, we define seven adversaries (σ_ε, σ_e, σ^E_G, σ_c, σ^G_c, σ_f, σ^G_f) that are used to define DTMCs from the obtained MDP model as follows: σ_ε captures only the semantics of regular temporal formulae, σ_e captures the semantics of the knowledge formulae, σ^E_G captures the semantics of the operator everyone in the group knows, σ_c captures he semantics of the basic commitment,

σ_c^G captures the semantics of group social commitment, σ_f captures the semantics of the fulfillment of the basic commitment, and σ_f^G captures the semantics of the fulfillment of group commitment. Concretely, we set the adversary σ_ε in such a way that always selects the transitions labeled by ε at each state in the model. This results in a DTMC model that captures only probabilistic temporal transitions inherited from **P** and ignores all transitions obtained by translating the various accessibility relations. The adversary σ_e always picks the action α^i at the state s and then selects the action ε at all following states (i.e., first the transitions resulted from the accessibility relations $\sim_i$ are considered, and then the normal transitions), and so on for the other adversaries.

To this end, we introduce our reduction rules that translate each PCTL$^{\text{kc+}}$ formula to PCTL formula w.r.t a given adversary.

5.3.2 Reducing PCTL$^{\text{kc+}}$ Formulae into PCTL Formulae

The PCTL$^{\text{kc+}}$ formulae are reduced inductively into PCTL as follows:

$\mathscr{F}(p) = p$, if p is an atomic proposition,

$\mathscr{F}(\neg\varphi) = \neg\mathscr{F}(\varphi)$,

$\mathscr{F}(\varphi \vee \psi) = \mathscr{F}(\varphi) \vee \mathscr{F}(\psi)$,

$\mathscr{F}(\mathbb{P}_{\bowtie k} \bigcirc \varphi) = \mathbb{P}_{\bowtie k} \bigcirc \mathscr{F}(\varphi)$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}(\varphi\ U\ \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi) U \mathscr{F}(\psi))$,

$\mathscr{F}(\mathbb{P}_{\bowtie k}(\varphi\ U^{\leq m}\ \psi)) = \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi) U^{\leq m} \mathscr{F}(\psi))$.

$\mathscr{F}(K_i\ \varphi) = \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$\mathscr{F}(\mathbb{P}_{\bowtie k} K_i\ \varphi) = \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(\varphi))$.

$\mathscr{F}(E_G\ \varphi) = \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$\mathscr{F}(\mathbb{P}_{\bowtie k} E_G\ \varphi) = \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(\varphi))$.

$\mathscr{F}(C_{i \to j}\ \varphi) = \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$\mathscr{F}(\mathbb{P}_{\bowtie k} C_{i\to j}\ \varphi) = \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(\varphi))$.

$\mathscr{F}(C_{i\to G}\ \varphi) = \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$\mathscr{F}(\mathbb{P}_{\bowtie k} C_{i\to G}\ \varphi) = \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(\varphi))$.

$\mathscr{F}(Fu(C_{i\to j}\ \varphi)) = \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(C_{i\to j}\ \varphi)) = \mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$

$\mathscr{F}(\mathbb{P}_{\bowtie k} Fu(C_{i\to j}\ \varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(C_{i\to j}\ \varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$.

$\mathscr{F}(Fu(C_{i\to G}\ \varphi)) = \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(C_{i\to G}\ \varphi)) = \mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$

$\mathscr{F}(\mathbb{P}_{\bowtie k} Fu(C_{i\to G}\ \varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc \mathscr{F}(C_{i\to G}\ \varphi)) = \mathbb{P}_{\bowtie k}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$.

To complete the reduction process, each PCTL formula has to be interpreted over a DTMC model $\mathscr{D} = (S, \bar{s}, \mathbf{P}, L)$. This is achieved by indicating which adversary is associated with which formula. In the following, $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} \varphi$ means that the PCTL formula φ holds in the model $\mathscr{D}$ obtained by applying the adversary σ_ε at state s. The following theorem is a direct consequence of the definition of $\mathscr{F}$ and can be easily proved by induction on the structure of the formula.

Theorem 5.4 (Transformation Satisfaction)**.**

Considering the following adversaries: σ_ε, σ_c, σ_c^G, σ_f, σ_f^G, σ_e, *and* σ_G^E *(which are DTMCs capturing temporal, commitment, and epistemic formulae in the model* $\mathfrak{M}_3$*), the following equivalences hold:*

$(\mathfrak{M}_3, s) \models p$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} p$

$(\mathfrak{M}_3, s) \models \neg\varphi$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} \neg\mathscr{F}(\varphi)$

$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k}(\varphi \vee \psi)$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} \mathbb{P}_{\bowtie k}\mathscr{F}(\varphi) \vee \mathbb{P}_{\bowtie k}\mathscr{F}(\psi)$

$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} \bigcirc \varphi$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} \mathbb{P}_{\bowtie k} \bigcirc \mathscr{F}(\varphi)$

$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k}(\varphi\ U\ \psi)$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi)\ U\ \mathscr{F}(\psi))$

$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k}(\varphi\ U^{\leq m}\ \psi)$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_\varepsilon} \mathbb{P}_{\bowtie k}(\mathscr{F}(\varphi)\ U^{\leq m}\ \mathscr{F}(\psi))$

$(\mathfrak{M}_3, s) \models K_i\varphi$ *iff* $(\mathfrak{M}'_3, s) \models_{\sigma_e} \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$

$$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} K_i \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_e} \mathbb{P}_{\bowtie k}(\mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$$

$$(\mathfrak{M}_3, s) \models E_G \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_G^E} \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$$

$$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} E_G \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_G^E} \mathbb{P}_{\bowtie k}(\mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$$

$$(\mathfrak{M}_3, s) \models C_{i \to j} \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_c} \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$$

$$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} C_{i \to j} \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_c} \mathbb{P}_{\bowtie k}(\mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$$

$$(\mathfrak{M}_3, s) \models C_{i \to G} \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_c^G} \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))$$

$$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} C_{i \to j} \varphi \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_c^G} \mathbb{P}_{\bowtie k}(\mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$$

$$(\mathfrak{M}_3, s) \models Fu(C_{i \to j} \varphi) \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_f} \mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$$

$$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} Fu(C_{i \to j} \varphi) \textit{ iff } (\mathfrak{M}'_3, s) \models_{\sigma_f} \mathbb{P}_{\bowtie k}(\mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))))$$

$$(\mathfrak{M}_3, s) \models Fu(C_{i \to G} \varphi) \quad \textit{iff } (\mathfrak{M}'_3, s) \models_{\sigma_f^G} \mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi)))$$

$$(\mathfrak{M}_3, s) \models \mathbb{P}_{\bowtie k} Fu(C_{i \to j} \varphi) \textit{ iff } (\mathfrak{M}'_3, s) \models_{\sigma_f^G} \mathbb{P}_{\bowtie k}(\mathbb{P}_{\geq 1}(\bigcirc \mathbb{P}_{\geq 1}(\bigcirc \mathscr{F}(\varphi))))$$

This theorem emphasizes that each translated PCTL$^{\text{kc+}}$ formula must be interpreted over an appropriate DTMC. That is, if the PCTL$^{\text{kc+}}$ formula includes only temporal operators, then the corresponding PCTL formula is interpreted over the DTMC obtained by only considering the normal transitions (i.e., σ_ε). Moreover, if the formula has the form of $K_i\ \varphi$, then the corresponding PCTL formula is interpreted over the DTMC obtained by considering first the transitions resulted from translating epistemic accessibility relations $\sim_i$ and then the normal transitions, which shows why the K operator is translated into the next operator $\bigcirc$. The same intuition holds for the other epistemic and social formulae.

Theorem 5.5 (Soundness and Completeness of $\mathscr{F}$)**.**
Let $\mathfrak{M}_3$ and Φ be respectively PCTL^{kc+} model and formula and let $\mathscr{F}(\mathfrak{M}_3)$ and $\mathscr{F}(\Phi)$ be the corresponding model and formula in PCTL. We have $\mathfrak{M}_3 \models \Phi$ iff $\mathscr{F}(\mathfrak{M}_3) \models \mathscr{F}(\Phi)$.

Proof. To prove the soundness (i.e., the necessary condition) and completeness (i.e., the sufficient condition) of the proposed reduction technique, we prove that the following three cases are sound and complete: $\Phi = K_i\varphi$, $\Phi = C_{i \to j}\varphi$ and $\Phi = Fu(C_{i \to j}\varphi)$. We prove this

by induction on the structure of the formula Φ. The cases when $\Phi = E_G\varphi$, $\Phi = C_{i\to G}\varphi$, and $\Phi = Fu(C_{i\to G}\varphi)$ can be proved in a similar way. The cases of PCTL$^{\text{kc+}}$ formulae that are also PCTL formulae are straightforward.

- $\Phi = K_i\ \varphi$. We have $(\mathfrak{M}_3, s) \models K_i\ \varphi$ iff $(\mathfrak{M}_3, s') \models \varphi$ for every $s' \in S$ such that $s \sim_i s'$. Therefore, $(\mathfrak{M}_3, s) \models K_i\ \varphi$ iff $(\mathscr{F}(\mathfrak{M}_3), s) \models \mathscr{F}(K_i\ \varphi)$. We know that $\mathscr{F}(\mathfrak{M}_3) = \mathfrak{M}'_3$. Now, $(\mathfrak{M}'_3, s) \models \mathscr{F}(K_i\ \varphi)$ iff for every $s' \in \mathbb{S}$ such that $(s, \alpha^i, s') \in \mathsf{P}_t$, we have $(\mathfrak{M}'_3, s') \models \mathscr{F}(\varphi)$. However, w.r.t the semantics of σ_e which is a DTMC defined to interpret commitment formulae over $\mathfrak{M}'_3$, it follows that every infinite path $\pi \in \Pi^{\sigma_e}(s)$ satisfies that $\pi(1) = s'$ and $(\sigma_e, \pi(1)) \models \mathscr{F}(\varphi)$. Thus, $(\sigma_e, s) \models \bigcirc\mathscr{F}(\varphi)$ for all $\pi \in \Pi^{\sigma_e}(s)$. As the path quantifier A is not defined in PCTL, and we have $\mathbb{P}_{\geq 1}$ instead, so we obtain $(\sigma_e, s) \models \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$.

- $\Phi = C_{i\to j}\varphi$. We have $(\mathfrak{M}_3, s) \models C_{i\to j}\varphi$ iff $(\mathfrak{M}_3, s') \models \varphi$ for every $s' \in S$ such that $s \approx_{i\to j} s'$. Consequently, $(\mathfrak{M}_3, s) \models C_{i\to j}\varphi$ iff $(\mathfrak{M}'_3, s) \models \mathscr{F}(C_{i\to j}\varphi)$. It follows that, $(\mathfrak{M}_3, s) \models \mathscr{F}(C_{i\to j}\varphi)$ iff for every $s' \in \mathbb{S}$ such that $(s, \beta^{ij}, s') \in \mathsf{P}_t$, we have $(\mathfrak{M}'_3, s') \models \mathscr{F}(\varphi)$. Now, based on the adversary σ_c which is a DTMC defined to interpret commitment formulae over $\mathfrak{M}_3$, every infinite path $\pi \in \Pi^{\sigma_c}(s)$ satisfies that $\pi(1) = s'$ and $(\sigma_c, \pi(1)) \models \mathscr{F}(\varphi)$. Thus, $(\sigma_c, s) \models \bigcirc\mathscr{F}(\varphi)$ for all $\pi \in \Pi^{\sigma_c}(s)$. As the path quantifier A is not defined in PCTL, and we have $\mathbb{P}_{\geq 1}$ instead, so we obtain $(\sigma_c, s) \models \mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$.

- $\Phi = Fu(C_{i\to j}\varphi)$. We have $(\mathfrak{M}_3, s) \models Fu(C_{i\to j}\varphi)$ iff there exists $s' \in S$ such that $s' \approx_{i\to j} s$ and $(\mathfrak{M}_3, s') \models C_{i\to j}\varphi$. Consequently, $(\mathfrak{M}_3, s) \models \mathscr{F}(Fu(C_{i\to j}\varphi))$ iff there exists $s' \in \mathbb{S}$ such that $(s, \gamma^{ij}, s') \in \mathsf{P}_t$ and $(\mathfrak{M}'_3, s') \models \mathscr{F}(C_{i\to j}\varphi)$. Now, w.r.t the adversary σ_f which is a DTMC defined to interpret fulfillment formulae over $\mathfrak{M}_3$, we obtain at least one infinite path $\pi \in \Pi^{\sigma_f}(s)$ that satisfies $\pi(1) = s'$ and $(\sigma_f, \pi(1)) \models$

$\mathscr{F}(C_{i\to j}\varphi)$. Since E is equivalent to $\mathbb{P}_{>0}$ and $\mathscr{F}(C_{i\to j}\varphi)$ is equivalent to $\mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi))$, so we obtain $(\sigma_f, s) \models \mathbb{P}_{>0}(\bigcirc\mathbb{P}_{\geq 1}(\bigcirc\mathscr{F}(\varphi)))$.

□

5.4 Implementation

We consider the web-based online shopping system [52] as a case study to evaluate the effectiveness of our proposed verification technique.

5.4.1 Online Shopping System

The online shopping system aims at providing an online shopping environment for customers. Customers can request to purchase one or more items from the supplier. By requesting an item, the customer commits towards the supplier to pay in order for the request to take place. Once the order is paid, the supplier confirms the order, and commits to deliver the requested item and enters a planned shipping date. Finally, when the order is shipped, the customer is notified. Requested item is either successfully delivered or refund is issued otherwise.

Because of the uncertainty associated to the underlying infrastructures of both commitments (i.e., the internet through which the payment is made and the transport system through which the delivery of purchased goods is done), there is no guarantee that these commitments are going to be fulfilled. Reasoning about and verifying the commitment to pay and the commitment to deliver have to be tackled with uncertainty in mind so that the degree of fulfilling each commitment can be measured, and so on.

We verify the online shopping system by means of the reduction-based model check technique proposed in Section 5.3. Figure 5.4 depicts a model for an interaction scenario

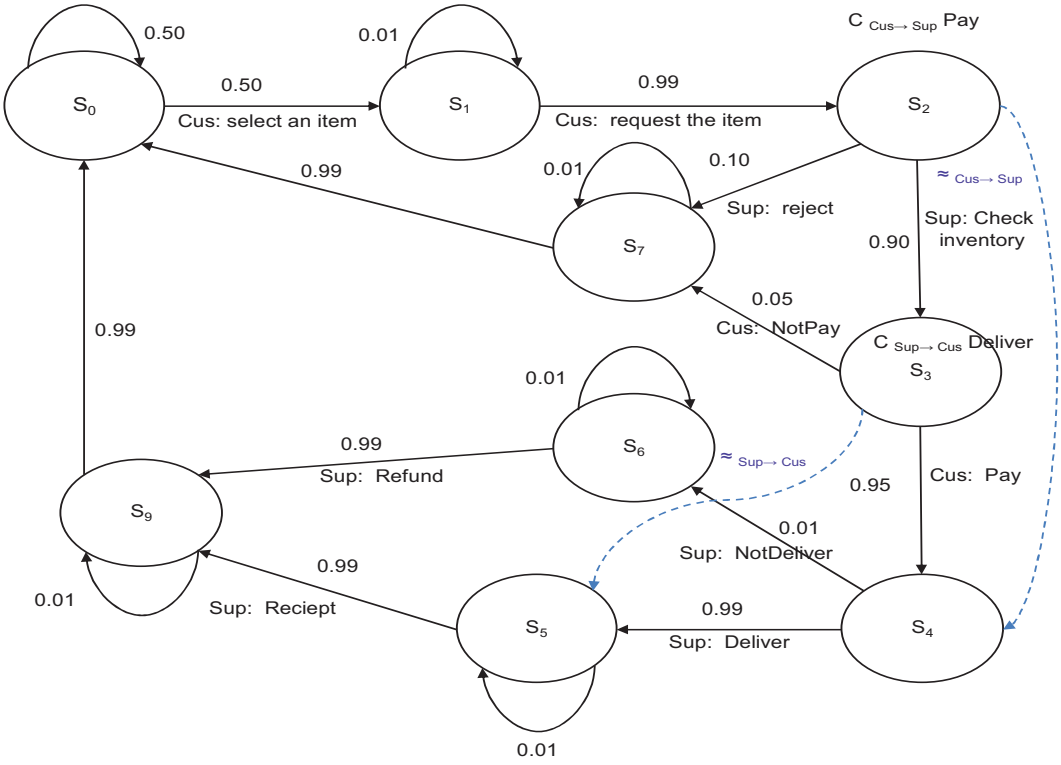

Figure 5.4: A model for the case of one supplier and one customer

between one supplier and one customer. In every experiment, we enlarge the system by increasing the number of customers only. For simplicity, we assume that all customers perform the same commitment, which is the commitment to pay for the requested item, respectively. We also assume that the supplier commits to all customers (i.e. a group commitment) to deliver the requested items. This allows us to verify both classes of commitment; basic social commitments and group social commitments.

5.4.2 System Properties

Properties that capture the probabilistic behavior of the online shopping system have been verified using PRISM in various proposals, for instance [85]. In this section, special emphasis is given to properties related to the concepts of knowledge and social commitments.

Concretely, we verify some system's properties such as *Safety*, *Liveness*, and *Reachability* that involve probabilistic knowledge, probabilistic commitments, and combinations of both. For the case of social commitments, our verification covers both basic and group social commitments. All defined properties are expressed in PCTL^{kc+}.

- `Safety Property:` Verifying formulae expressing this property in the system models ensures avoiding the appearance of bad situations in the real systems. One bad situation that need to be verified is when the (Cus) fulfills his commitment to pay for the requested order but the (Sup) does not commit to deliver the requested item. This situation can be expressed in PCTL^{kc+} as follows:
  $\varphi_2 = \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond Fu(C_{cus\rightarrow sup}(Pay)) \wedge \mathbb{P}_{\geq 1}\Box\neg(C_{sup\rightarrow cus}(Deliver))]$

- `Liveness Property:` In all computation paths it is always the case that if the customer commits to pay for the requested item, then in the future the customer will eventually make the payment. This can be expressed in PCLT^{kc+} as follows:
  $\varphi_3 = \mathbb{P}_{\geq 1}[(C_{cus\rightarrow sup}(Pay)) \supset \mathbb{P}_{\geq 1}\Diamond Fu(C_{cus\rightarrow sup}(Pay))]$

- `Reachability Property:` One possible example with regard to the online shopping system is that if the customer (Cus) commits towards the supplier (Sup) to pay for the requested item, the state at which the customer can fulfill his commitment should be reached from the initial state. That is, there should be a possibility from the initial state for the customer to reach the fulfilment state. This can be formally expressed in PCLT^{kc+} as follows:
  $\varphi_1 = \mathbb{P}_{>0}\Diamond Fu(C_{cus\rightarrow sup}(Pay))$.

Furthermore, thanks to the probabilistic model clacking technique, we can also get the satisfiability of given formulae in terms of quantitative results. That is, checking whether a

given formula holds in the model with a threshold (at least 0.95% for example) is achievable. Let us consider the following examples:

- Once the customer fulfills his commitment to pay, he will be aware about the payment with at least 0.95%.

  $\varphi_4 = P_{>0.95}\ Fu(C_{cus \rightarrow sup}(Pay)) \supset K_{cus}Pay$

- Once the customer fulfills his commitment to pay, the supplier will be aware about the payment with at least 0.98%.

  $\varphi_5 = P_{>0.98}\ Fu(C_{cus \rightarrow sup}(Pay)) \supset K_{sup}Pay$

5.4.3 Experimental Results

The online shopping system is encoded into the PRISM input language as follows. Supplier agent (Sup) and Customer agent (Cus) are mapped into *modules* in the PRISM language. Each agent's actions are used to determine the behavior of the agent (i.e., his local states). For example, Supplier's actions (variables) are: *Accept*: Accept the request, *Reject*: Reject the request, *Deliver*: Deliver the requested item, *Receipt*: Send receipt, *Refund*: Refund in case of not delivery. The global model is obtained by the synchronization between all modules (agents).

Our implementation was performed on a TOSHIBA laptop equipped with 32-bit Windows XP with 1 GB of RAM and Genuine Intel(R) CPU at 1.6 GHz. Table 5.1 reports the results of 15 experiments wherein (Exp.#) denotes the experiment number, (#Agent) denotes the number of agents, (#States) denotes the number of reachable states, (#Transitions) denotes the number of transitions, and (Construction Time) denotes the time needed for building the simulated model in seconds.

Table 5.1: Verification results of the online shopping system

Exp.#	#Agents	#States	#Transitions	Const. Time (s)
Exp.1	2	30	74	0.031
Exp.2	3	210	700	0.039
Exp.3	4	1470	6102	0.047
Exp.4	5	$1.02 * 10^4$	$5.10 * 10^4$	0.063
Exp.5	6	$7.20 * 10^4$	$4.15 * 10^5$	0.078
Exp.6	7	$5.04 * 10^5$	$3.31 * 10^6$	0.109
Exp.7	8	$3.52 * 10^6$	$2.60 * 10^7$	0.189
Exp.8	9	$2.47 * 10^7$	$2.03 * 10^8$	0.328
Exp.9	10	$1.73 * 10^8$	$1.56 * 10^9$	0.516
Exp.10	11	$1.21 * 10^9$	$1.19 * 10^{10}$	0.765
Exp.11	12	$8.47 * 10^9$	$9.01 * 10^{10}$	1.406
Exp.12	13	$5.93 * 10^{10}$	$6.79 * 10^{11}$	2.219
Exp.13	14	$4.15 * 10^{11}$	$5.09 * 10^{12}$	6.094
Exp.14	15	$2.91 * 10^{12}$	$3.8 * 10^{13}$	8.046
Exp.15	16	$2.03 * 10^{13}$	$2.82 * 10^{14}$	13.406

First experiment started with only two agents; One supplier (Sup) and one Customer (Cus). In the rest of experiments, we add one more customer (Cus) each time and report the changes occurring in the size of the model and the time needed for building the model. These results show that (#States) and (#Transitions) grow up exponentially as the system is augmented with more agents. However, the (Construction Time) increases polynomially till we reach a point close to the state explosion, then it grows up dramatically. Figure 5.5 shows the increase in the construction time as more agents join the system. This dramatic change in the time needed to build the model reflects the fact that the model size becomes massive.

Table 5.2 reports the model checking results for the defined formulae (φ_1 to φ_5) for the case of two agents (one customer and one supplier). All formulae hold in the model as expected, which reflects the success of our proposed model checking technique in verifying

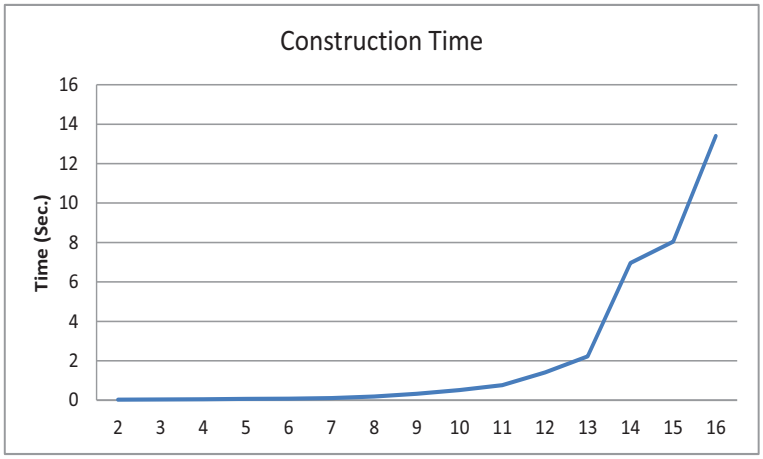

Figure 5.5: Model construction time for the online shopping system

the system properties expressed using the probabilistic logic PCTL^{kc+}. Moreover, as shown in Table 5.2, although the model checking time varies from one formula to another, it is still short compared to the time needed for building the model.

For scalability purposes, starting from experiment #2, we re-write the above-defined formulae in a parameterized form as follows:

$$\varphi'_1 = \mathbb{P}_{>0}\Diamond \bigwedge_{i=1}^{n} Fu(C_{cus_i \to sup}(Pay_i)).$$

$$\varphi'_2 = \mathbb{P}_{\geq 1}\Box\neg[\mathbb{P}_{>0}\Diamond \bigwedge_{i=1}^{n} Fu(C_{cus_i \to sup}(Pay_i)) \wedge \mathbb{P}_{\geq 1}\Box\neg(C_{sup \to cus_i}(Deliver_i))]$$

$$\varphi'_3 = \mathbb{P}_{\geq 1}[\bigwedge_{i=1}^{n} (C_{cus_i \to sup}(Pay_i)) \supset \mathbb{P}_{\geq 1}\Diamond Fu(C_{cus_i \to sup}(Pay_i))]$$

$$\varphi'_4 = P_{>0.95} \bigwedge_{i=1}^{n} Fu(C_{cus_i \to sup}(Pay_i)) \supset K_{cus_i} Pay_i$$

$$\varphi'_5 = P_{>0.98} \bigwedge_{i=1}^{n} Fu(C_{cus_i \to sup}(Pay_i)) \supset K_{sup} Pay_i$$

where n is the number of agents in the experiment.

To be able to verify group social commitments, which is one of the main motivations of this chapter, we need models of one supplier agent interacting with two or more customer agents by means of social commitments. Table 5.3 reports the results of verifying group social commitments for experiment #2 and experiment #3 using the proposed reduction

Table 5.2: Results of model checking some properties for the online shopping system

Formulae	Results	Time for MC (Sec.)
φ_1	true	0.06
φ_2	true	0.13
φ_3	true	0.11
φ_4	true	0.06
φ_5	true	0.07

technique. In experiment #2, we have one supplier (Sup) committing to two customers (Cus_1) and (Cus_2) to deliver the goods. The commitment should be fulfilled in the future to meet the liveness property. Likewise, in experiment #3, we have one supplier (Sup) committing to three customers (Cus_1), (Cus_2), and (Cus_3) to deliver the requested items.

$\varphi_6 = \mathbb{P}_{\geq 1}[(C_{sup \to \{cus_1, cus_2\}}(Deliver)) \supset \mathbb{P}_{\geq 1} \Diamond Fu(C_{sup \to \{cus_1, cus_2\}}(Deliver))]$

$\varphi_7 = \mathbb{P}_{\geq 1}[(C_{sup \to \{cus_1, cus_2, cus_3\}}(Deliver)) \supset \mathbb{P}_{\geq 1} \Diamond Fu(C_{sup \to \{cus_1, cus_2, cus_3\}}(Deliver))]$

We were also successful in verifying formulae expressing the interaction between knowledge and group social commitments for experiment #2 and experiment #3 as shown below.

$\varphi_8 = \mathbb{P}_{\geq 1}[Fu(C_{sup \to \{cus_1, cus_2\}}(Deliver)) \supset K_{cus_1}(Deliver) \wedge K_{cus_2}(Deliver)]$

$\varphi_9 = \mathbb{P}_{\geq 1}[Fu(C_{sup \to \{cus_1, cus_2, cus_3\}}(Deliver)) \supset K_{cus_1}(Deliver) \wedge K_{cus_2}(Deliver) \wedge K_{cus_3}(Deliver)]$

Where, φ_8 states that the fulfilment of a group commitment (the commitment from *sup* to cus_1 and cus_2 to deliver) implies that every creditor in the group will know about the content of the commitment (i.e., cus_1 and cus_2 will know about the delivery). Similarly, φ_9 states the same meaning in the case when *sup* fulfills its commitment to three customers.

Table 5.3: Model checking group commitment formulae

Exp.#	#Agents	Formulae	Results
Exp.2	1 Sup, 2 Cus	φ_6	true
Exp.3	1 Sup, 3 Cus	φ_7	true
Exp.2	1 Sup, 2 Cus	φ_8	true
Exp.3	1 Sup, 3 Cus	φ_9	true

5.5 Summary

In this chapter, we introduced a formal approach for specifying and verifying the interactions between basic (individual) and group social commitments and knowledge in probabilistic MASs. The proposed approach encompasses three main parts. In the first part, we presented a new probabilistic logic of knowledge and commitments ($PCLT^{kc+}$). The expressive power of $PCLT^{kc+}$ outperforms those of existing logics because of its ability to express and specify not only the concepts of knowledge and social commitments independently, but also their interactions in the presence of uncertainty. Also, being enriched by operators for the group knowledge and group commitments, $PCLT^{kc+}$ allows handling more complicated commitment scenarios with respect to the number of participating agents. We categorized social commitments into two classes based on the number of participating agents; basic social commitment (the common one-to-one scheme) and group social commitment (one-to-many scheme). We then presented a formal semantics for the group social commitment. With such a classification of social commitments, we gain an insight into different ways to utilize commitments among communicating parties. In contrast, exiting solutions for social commitments restrict themselves to the common one-to-one commitment scheme.

In the second part, we proposed a sound and complete reduction-based model checking technique for the new logic. The proposed technique consists of reducing the problem of model checking $PCLT^{kc+}$ to the problem of model checking PCTL. The soundness and completeness of the reduction technique were proven. Finally, in the third part, we used the PRISM tool to implement our reduction technique and check $PCLT^{kc+}$ formulae by checking their corresponding PCTL formulae without adding new computation cost. In terms of scalability, we showed that our reduction technique is scalable as we were successfully able to apply it on models of size up to 10^{13} states and 10^{14} transitions. To conclude, the two main findings of this chapter are:

1. Simply combining a probabilistic logic of knowledge and a probabilistic logic of commitments to capture the interactions between the concept of knowledge and social commitments in probabilistic MASs is not quite working as excepted.

2. Representing group social commitments and the interactions between group social commitments and knowledge in the presence of uncertainty become attainable by the use of our proposed framework.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In this thesis, we have put forward a formal framework for agent communication using a commitment-based approach in order to enable effective agent interactions in open, heterogeneous, and dynamic systems when uncertainty matters. The main purpose of this framework is to essentially specify and reason about social commitments in probabilistic settings, so they can be formally verified. As an improvement over the existing solutions, our proposed framework targets systems exhibiting probabilistic behavior and considers commitments among a group of agents. The framework is composed of three main components. First, we presented a new probabilistic approach for tackling social commitments in the presence of uncertainty. To specify probabilistic social commitments, we defined a new logic called the probabilistic logic of commitments (PCTLC). Our new logic is interpreted over a new extended version of probabilistic interpreted systems. Furthermore, we introduced a new reduction-based model checking technique for the new logic and implemented it on top of the PRISM model checker. Then, by using the proposed reduction technique,

we showed how to evaluate some systems' properties representing probabilistic social commitments – expressed in terms of the new logic – against system design models obtained using our extended version of probabilistic interpreted systems.

The second component of our framework focused on the interaction between knowledge and social commitments in probabilistic MASs. We introduced a new logic called the probabilistic logic of knowledge and commitment (PCTL^{kc}) to represent and reason about such interactions. PCTL^{kc} logic is interpreted over a new version of probabilistic interpreted systems that has epistemic accessibility relations and social accessability relations at its core. To verify the new logic, we developed a verification technique based on model checking and implemented it using the PRISM tool. Our interest in the first and second contributions was focused on the common two-agent commitment scenarios (i.e. agent-to-agent scheme).

In the third part of the framework, we improved and extended our work in the second part as follows:

1. We refined and improved PCTL^{kc} to overcome the inconsistency problem appeared when taking the recent work of Al-Saqqar et al. [1] into consideration. Therefore, in this part, we adopted CTLKC^{+} [1] as a basis for our new logic and combined it with PCTL.

2. We extended the scope of interacting agents from agent-to-agent to agent-to-many. This allowed us to investigate different commitment schemes such as the case of committing to multiple agents. In this respect, we defined an adequate semantics for group social commitments for the first time in the literature.

Based on the new semantics of group social commitments and the consistent logic of knowledge and commitment presented in [1], we presented a new probabilistic logic of knowledge and commitment called (PCTL^{kc+}). The new logic accommodates new operators for

group social commitments and group knowledge in addition to the modalities already found in PCTL^{kc}. The expressiveness power of PCTL^{kc+} outperforms those of existing logics because of its ability not only to capture and express the combinations of knowledge and social commitments in the presence of uncertainty, but also to express formulae involving group social commitments. Formulae of PCTL^{kc+} are interpreted over a new extended version of probabilistic interpreted systems. Our new version of interpreted systems integrates a modified version of social accessabilities that accounts for basic social commitments, group social commitments, and knowledge. To evaluate the new logic (PCTL^{kc+}), we proposed a reduction-based model checking technique and implemented it on top of PRISM.

Furthermore, we proved the soundness of all proposed verification techniques. Also, using different case studies we were successfully able to demonstrate the effectiveness and usefulness of our proposed work and evaluate the scalability of the introduced verification techniques.

Finally, as the proposed framework permits addressing probabilistic social commitments as well as their interaction with knowledge when the scope of interacting parties moves beyond the common one-to-one scheme, we believe that it will advance the literature of agent communication and help MASs designers build more effective and efficient systems.

6.2 Future Work

There is still a long way to go in order to develop a comprehensive framework for probabilistic social commitments in MASs. In the future, we plan to extend our work by investigating several directions.

First, time complexity and space complexity of our proposed verification techniques are not analysed yet. Therefore, we intend to compute the complexity of the proposed

reduction techniques of the three components.

Second, we are planning to extend our framework to support more commitment schemes such as many-to-one and many-to-many commitments. This is extremely important because in real settings there exist situations where performing such commitment scenarios contributes towards improving the efficiency of MASs.

Third, integrating more commitment actions (such as assign, delegate, ..etc) [98] are of a great interest to investigate. This helps ensure that all possible commitment operations employed in probabilistic environments are adequately dealt with.

Forth, we intend to explore the interaction between social commitments and norms in probabilistic systems.

Fifth, another direction that we intend to explore is the probabilistic conditional social commitments. Conditional social commitment is still in its infancy [68] and investigating it in systems exhibiting stochastic behavior is an open point for research.

Finally, we plan to extend the PRISM model checker to accommodate our new operators (i.e. commitment and group commitment) and then develop dedicated verification algorithms for the proposed logics and implement them directly into PRISM. So doing will allow us to compare the results obtained from the indirect method (reduction-based techniques) with the results of the direct method (dedicated algorithms).

Publications in refereed journals and conferences

Journals

- K. Sultan, J. Bentahar, M. El-Menshawy, "Model Checking Probabilistic Social Commitments for Intelligent Agent Communication", Journal of Applied Soft Computing, Elsevier, 2014.

- K. Sultan, J. Bentahar, W. Wan, F. Al-Saqqar, "Modeling and Verifying Probabilistic Multi- Agent Systems using Knowledge and Social Commitments", Journal of Expert Systems with Applications, Elsevier, 2014.

- F. Al-Saqqar, J. Bentahar, K. Sultan, M. El-Menshawy, "On the Interaction between Knowledge and Social Commitments in Multi-Agent Systems", Applied Intelligence Journal, Springer, 2014.

- F. Al-Saqqar, J. Bentahar, K. Sultan, W. Wan, E. Khosrowshahi Asl, "Model Checking Temporal Knowledge and Commitments in Multi-Agent Systems Using Reduction", Simulation Modeling Practice and Theory Journal, Elsevier, 2015.

Conferences

- K. Sultan, J. Bentahar, O. Marey, "A Probabilistic Logic to Reason about the Interaction between Knowledge and Social Commitments in MASs", In the Proc. of The 13th International Conference on Intelligent Software Methodologies, Tools, and Techniques (SOMET_14), Langkawi, Malaysia, 2014.

- M. Mbarki, O. Marey, J. Bentahar, K. Sultan, "Agent Types and Adaptive Negotiation Strategies in Argumentation-Based Negotiation", In the Proc. of the IEEE International Conference on Tools with Artificial Intelligence (ICTAI), Limassol, Cyprus, 2014.

- K. Sultan, M. El-Menshawy, J. Bentahar, "Reasoning about Social Commitments in the Presence of Uncertainty", In the Proc. of The 12th International Conference on Intelligent Software Methodologies, Tools, and Techniques (SOMET_13), Budapest, Hungary, 2013.

Articles in process for publication in refereed journals

- K. Sultan, J. Bentahar, R. Mizouni, "Model Checking the Interaction Between Individual and Group Knowledge and Commitments in Probabilistic Multi-Agent Systems", Engineering Applications of Artificial Intelligence, Elsevier, (submitted: August 2014).

- O. Marey, J. Bentahar, E. Khosrowshahi Asl, K. Sultan, R. Dssouli, "Decision Making under Subjective Uncertainty in Argumentation-Based Negotiation. Ambient Intelligence and Humanized Computing, (submitted: November 2014).

Bibliography

[1] Faisal Al-Saqqar, Jamal Bentahar, Khalid Sultan, and Mohamed El-Menshawy. On the interaction between knowledge and social commitments in multi-agent systems. *Appl. Intell.*, 41(1):235–259, 2014.

[2] Faisal Al-Saqqar, Jamal Bentahar, Khalid Sultan, Wei Wan, and Ehsan Khosrowshahi Asl. Model checking temporal knowledge and commitments in multi-agent systems using reduction. *Simulation Modelling Practice and Theory*, 51:45 – 68, 2015.

[3] Christel Baier. On algorithmic verification methods for probabilistic systems. Habilitation thesis, Fakultät für Mathematik & Informatik, Universität Mannheim, 1998.

[4] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT Press, 2008.

[5] Matteo Baldoni, Cristina Baroglio, and Elisa Marengo. Behavior-oriented commitment-based protocols. In *ECAI*, pages 137–142, 2010.

[6] Matteo Baldoni, Cristina Baroglio, Elisa Marengo, Viviana Patti, and Federico Capuzzimati. Engineering commitment-based business protocols with the 2CL methodology. *Autonomous Agents and Multi-Agent Systems*, 28(4):519–557, 2014.

[7] Tina Balke, Célia da Costa Pereira, Frank Dignum, Emiliano Lorini, Antonino Rotolo, Wamberto Vasconcelos, and Serena Villata. Norms in MAS: Definitions and Related Concepts. In *Normative Multi-Agent Systems*, pages 1–31. 2013.

[8] Brandon Bennett, Anthony G. Cohn, Frank Wolter, and Michael Zakharyaschev. Multi-dimensional modal logic as a framework for spatio-temporal reasoning. *Applied Intelligence*, 17(3):239–251, 2002.

[9] Jamal Bentahar, Mohamed El-Menshawy, Hongyang Qu, and Rachida Dssouli. Communicative commitments: Model checking and complexity analysis. *Knowledge-Based Systems*, 35:21 – 34, 2012.

[10] Jamal Bentahar, Zakaria Maamar, Wei Wan, Djamal Benslimane, Philippe Thiran, and Sattanathan Subramanian. Agent-based communities of web services: an argumentation-driven approach. *Service Oriented Computing and Applications*, 2(4):219–238, 2008.

[11] Jamal Bentahar, John-Jules Ch. Meyer, and Wei Wan. Model checking communicative agent-based systems. *Knowledge-Based Systems*, 22(3):142–159, 2009.

[12] Jamal Bentahar, John-Jules Ch. Meyer, and Wei Wan. Model checking agent communication. In *Specification and Verification of Multi-agent Systems*, pages 67–102. Springer US, 2010.

[13] Jamal Bentahar, Bernard Moulin, John-Jules Ch. Meyer, and Brahim Chaib-draa. A logical model for commitment and argument network for agent communication. In *AAMAS*, pages 792–799, 2004.

[14] Jamal Bentahar, Bernard Moulin, John-Jules Ch. Meyer, and Yves Lespérance. A new logical semantics for agent communication. In *CLIMA*, pages 151–170, 2007.

[15] Girish Bhat, Rance Cleaveland, and Alex Groce. Efficient model checking via büchi tableau automata. In Gérard Berry, Hubert Comon, and Alain Finkel, editors, *CAV*, volume 2102 of *Lecture Notes in Computer Science*, pages 38–52. Springer, 2001.

[16] Pratik K. Biswas. Towards an agent-oriented approach to conceptualization. *Appl. Soft Comput.*, 8(1):127–139, 2008.

[17] Rafael H. Bordini, Michael Fisher, Willem Visser, and Michael Wooldridge. Verifying multi-agent programs by model checking. *Autonomous Agents and Multi-Agent Systems*, 12(2):239–256, 2006.

[18] Cristiano Castelfranchi. Commitments: From individual intentions to groups and organizations. In Victor R. Lesser and Les Gasser, editors, *ICMAS*, pages 41–48. The MIT Press, 1995.

[19] Zhengang Cheng. *Verifying commitment-based business protocols and their compositions: model checking using promela and spin*. PhD thesis, 2006. North Carolina State University.

[20] Federico Chesani, Paola Mello, Marco Montali, and Paolo Torroni. Representing and monitoring social commitments using the event calculus. *Autonomous Agents and Multi-Agent Systems*, 27(1):85–130, 2013.

[21] Alessandro Cimatti, Edmund M. Clarke, Enrico Giunchiglia, Fausto Giunchiglia, Marco Pistore, Marco Roveri, Roberto Sebastiani, and Armando Tacchella. NuSMV: An open source tool for symbolic model checking. In *CAV*, pages 359–364, 2002.

[22] Edmund M. Clarke, Orna Grumberg, and Doron Peled. *Model checking*. MIT Press, Cambridge, Massachusetts, 1999.

[23] Marco Colombetti. A commitment-based approach to agent speech acts and conversations. In *Proceedings of the Workshop on Agent Languages and Conversational Policies*, pages 21–29, 2000.

[24] Marco Colombetti, Nicoletta Fornara, and Mario Verdicchio. A social approach to communication in multiagent systems. In João Leite, Andrea Omicini, Leon Sterling, and Paolo Torroni, editors, *Declarative Agent Languages and Technologies*, volume 2990 of *Lecture Notes in Computer Science*, pages 191–220. Springer Berlin Heidelberg, 2004.

[25] Marcelo França Corrêa, Marley B. R. Vellasco, and Karla Figueiredo. Multi-agent systems with reinforcement hierarchical neuro-fuzzy models. *Autonomous Agents and Multi-Agent Systems*, 28(6):867–895, 2014.

[26] Carla Delgado and Mario Benevides. Verification of epistemic properties in probabilistic multi-agent systems. In *Multiagent System Technologies*, pages 16–28. 2009.

[27] Nirmit Desai, Zhengang Cheng, Amit K. Chopra, and Munindar P. Singh. Toward verification of commitment protocols and their compositions. In *AAMAS*, pages 144–145, 2007.

[28] Nirmit Desai, Amit K. Chopra, and Munindar P. Singh. Amoeba: A methodology for modeling and evolving cross-organizational business processes. *ACM Trans. Softw. Eng. Methodol.*, 19(2):1–40, 2009.

[29] Frank Dignum, David Kinny, and Liz Sonenberg. Motivational attitudes of agents: On desires, obligations, and norms. In Barbara Dunin-Keplicz and Edward Nawarecki, editors, *From Theory to Practice in Multi-Agent Systems*, volume 2296

of *Lecture Notes in Computer Science*, pages 83–92. Springer Berlin Heidelberg, 2002.

[30] Frank Dignum, John-Jules Ch. Meyer, Roel Wieringa, and Ruurd Kuiper. A modal approach to intentions, commitments and obligations: Intention plus commitment yields obligation. In *DEON*, pages 80–97, 1996.

[31] Barbara Maria Dunin-Keplicz and Rineke Verbrugge. *Teamwork in Multi-Agent Systems: A Formal Approach*. Wiley Publishing, 1st edition, 2010.

[32] Mohamed El-Menshawy, Jamal Bentahar, and Rachida Dssouli. Verifiable semantic model for agent interactions using social commitments. In *LADS*, pages 128–152, 2010.

[33] Mohamed El-Menshawy, Jamal Bentahar, and Rachida Dssouli. Symbolic model checking commitment protocols using reduction. In *DALT*, pages 185–203, 2011.

[34] Mohamed El-Menshawy, Jamal Bentahar, Warda El Kholy, and Rachida Dssouli. Reducing model checking commitments for agent communication to model checking ARCTL and GCTL*. *Autonomous Agents and Multi-Agent Systems*, 27(3):375–418, 2013.

[35] Mohamed El-Menshawy, Jamal Bentahar, Warda El Kholy, and Rachida Dssouli. Verifying conformance of multi-agent commitment-based protocols. *Expert Syst. Appl.*, 40(1):122–138, 2013.

[36] Mohamed El-Menshawy, Jamal Bentahar, Hongyang Qu, and Rachida Dssouli. On the verification of social commitments and time. In *AAMAS*, pages 483–490, 2011.

[37] Mohamed El-Menshawy Mohamed. *Model Checking Logics of Social Commitments for Agent Communication*. PhD thesis, 2012. Concordia University.

[38] Ernest Allen Emerson. Temporal and modal logic. In *Handbook of Theoretical Computer Science*, pages 996–1072. Elsevier, 1995.

[39] Ernest Allen Emerson and Joseph Y. Halpern. "Sometimes" and "Not Never" revisited: On branching versus linear time temporal logic. *J. ACM*, 33(1):151–178, 1986.

[40] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning About Knowledge*. The MIT Press, Cambridge, 1995.

[41] Lihua Feng and Gaoyuan Luo. Application of possibility-probability distribution in risk analysis of landfall hurricane -a case study along the east coast of the united states. *Appl. Soft Comput.*, 11(8):4563 – 4568, 2011.

[42] Tim Finin, Richard Fritzson, Don McKay, and Robin McEntire. KQML as an agent communication language. In *CIKM*, pages 456–463. ACM, 1994.

[43] Vojtech Forejt, Marta Z. Kwiatkowska, Gethin Norman, and David Parker. Automated verification techniques for probabilistic systems. In *SFM*, pages 53–113. 2011.

[44] Nicoletta Fornara and Macro Colombetti. A commitment-based approach to agent communication. *Applied Artificial Intelligence*, 18:853–866, 2004.

[45] Nicoletta Fornara and Marco Colombetti. Protocol specification using a commitment based acl. In *Workshop on Agent Communication Languages*, volume 2922 of *Lecture Notes in Computer Science*, pages 108–127. Springer, 2004.

[46] Massimo Franceschet, Angelo Montanari, and Maarten de Rijke. Model checking for combined logics with an application to mobile systems. *Automated Software Engineering*, 11(3):289–321, 2004.

[47] Dov M. Gabbay. *Many-Dimensional Modal Logics: Theory and Applications*. Studies in Logic and the Foundations of Mathematics Series. Elsevier North Holland, 2003.

[48] Peter Gammie and Ron van der Meyden. MCK: Model checking the logic of knowledge. In Rajeev Alur and DoronA. Peled, editors, *Computer Aided Verification*, volume 3114 of *Lecture Notes in Computer Science*, pages 479–483. Springer Berlin Heidelberg, 2004.

[49] Arnulfo Alanis Garza, Oscar Castillo, and José Mario García Valdez. Multi-agent system based on psychological models for mobile robots. In *Soft Computing for Intelligent Control and Mobile Robotics*, pages 143–159. 2011.

[50] Scott N. Gerard and Munindar P. Singh. Formalizing and verifying protocol refinements. *ACM Trans. Intell. Syst. Technol.*, 4(2):21:1–21:27, 2013.

[51] Laura Giordano, Alberto Martelli, and Camilla Schwind. Specifying and verifying interaction protocols in a temporal action logic. *Applied Logic*, 5(2):214–234, 2007.

[52] Hassan Gomaa. *Software Modeling and Design: UML, Use Cases, Patterns, and Software Architectures*. Cambridge University Press, 2011.

[53] Frank Guerin and Jeremy Pitt. Proving properties of open agent systems. In *AAMAS*, pages 557–558, 2002.

[54] Akin Günay and Pinar Yolum. Constraint satisfaction as a tool for modeling and checking feasibility of multiagent commitments. *Appl. Intell.*, 39(3):489–509, 2013.

[55] Joseph Y. Halpern. *Reasoning about Uncertainty*. MIT Press, Cambridge, Massachusetts, 2003.

[56] Joseph Y. Halpern and Moshe Y. Vardi. Model checking vs. theorem proving: A manifesto, 1991.

[57] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6(5):512–535, 1994.

[58] Jaakko Hintikka. *Knowledge and Belief*. Ithaca, N.Y.,Cornell University Press, 1962.

[59] Andrew Hinton, Marta Kwiatkowska, Gethin Norman, and David Parker. PRISM: A tool for automatic verification of probabilistic systems. In *TACAS*, pages 441–444, 2006.

[60] Gerard Holzmann. The model checker SPIN. *IEEE Transactions on Software Engineering*, 23:279–295, 1997.

[61] Gerard Holzmann. *The SPIN Model Checker: Primer and Reference Manual*. Addison-Wesley Professional, first edition, 2003.

[62] Xiaowei Huang, Cheng Luo, and Ron van der Meyden. Symbolic model checking of probabilistic knowledge. In *TARK*, pages 177–186, 2011.

[63] Bengt Jonsson and Kim Guldstrand Larsen. Specification and refinement of probabilistic processes. In *LICS*, pages 266–277, 1991.

[64] Leslie Pack Kaelbling, Michael L. Littman, and Anthony R. Cassandra. Partially observable markov decision processes for artificial intelligence. In *Reasoning with Uncertainty in Robotics*, pages 146–163, 1995.

[65] Leslie Pack Kaelbling, Michael L. Littman, and Anthony R. Cassandra. Planning and acting in partially observable stochastic domains. *Artificial Intelligence*, 101:99–134, 1998.

[66] Fakhreddine O. Karray and Clarence De Silva. *Soft Computing and Intelligent Systems Design: Theory, Tools and Applications*. Addison-Wesley, 1st edition, 2004.

[67] M. Karthikeyan and P. Aruna. Probability based document clustering and image clustering using content-based image retrieval. *Appl. Soft Comput.*, 13(2):959 – 966, 2013.

[68] Warda El Kholy, Jamal Bentahar, Mohamed El-Menshawy, Hongyang Qu, and Rachida Dssouli. Modeling and verifying choreographed multi-agent-based web service compositions regulated by commitment protocols. *Expert Syst. Appl.*, 41(16):7478–7494, 2014.

[69] Savas Konur, Michael Fisher, and Sven Schewe. Combined model checking for temporal, probabilistic, and real-time logics. *Theoretical Computer Science*, 503:61–88, 2013.

[70] Anand J. Kulkarni and Kang Tai. Probability collectives: A multi-agent approach for solving combinatorial optimization problems. *Appl. Soft Comput.*, 10(3):759–771, 2010.

[71] Vidyadhar G. Kulkarni. *Modeling and Analysis of Stochastic Systems*. Chapman & Hall, Ltd., London, UK, UK, 1995.

[72] Marta Z. Kwiatkowska. Model checking for probability and time: from theory to practice. In *LICS*, pages 351–, 2003.

[73] Marta Z. Kwiatkowska, Gethin Norman, and David Parker. PRISM: Probabilistic symbolic model checker. In *Computer Performance Evaluation / TOOLS*, pages 200–204, 2002.

[74] Marta Z. Kwiatkowska, Gethin Norman, and David Parker. Stochastic model checking. In *SFM*, pages 220–270, 2007.

[75] Chang-Shing Lee and Vincenzo Loia. Special issue on computational intelligence agents. *Applied Intelligence*, 30(3):189–190, 2009.

[76] Hector J. Levesque, Philip R. Cohen, and José H. T. Nunes. On acting together. In *Proceedings of the 8th National Conference on Artificial Intelligence*, pages 94–99, 1990.

[77] Alessio Lomuscio, Charles Pecheur, and Franco Raimondi. Automatic verification of knowledge and time with nusmv. In *IJCAI*, pages 1384–1389, 2007.

[78] Alessio Lomuscio and Wojciech Penczek. Symbolic model checking for temporal-epistemic logic. In *Logic Programs, Norms and Action*, pages 172–195, 2012.

[79] Alessio Lomuscio and Franco Raimondi. MCMAS: A model checker for multi-agent systems. In *TACAS*, pages 450–454, 2006.

[80] Ashok U. Mallya and Munindar P. Singh. An algebra for commitment protocols. *Autonomous Agents and Multi-Agent Systems*, 14(2):143–163, 2007.

[81] Kenneth McMillan. *Symbolic Model Checking: An Approach to the State Explosion Problem*. PhD thesis, 1992. Carnegie Mellon University.

[82] Francisco S. Melo, Matthijs T. J. Spaan, and Stefan J. Witwicki. QueryPOMDP: POMDP-based communication in multiagent systems. In *EUMAS*, pages 189–204, 2011.

[83] John-Jules Ch Meyer and Wiebe Van Der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge University Press, New York, NY, USA, 1995.

[84] Olga Ormandjieva, Vangalur S. Alagar, and Mao Zheng. Early quality monitoring in the development of real-time reactive systems. *Journal of Systems and Software*, 81(10):1738–1753, 2008.

[85] Samir Ouchani, Otmane Aït Mohamed, and Mourad Debbabi. A formal verification framework for sysml activity diagrams. *Expert Syst. Appl.*, 41(6):2713–2728, 2014.

[86] Sooyong Park and Vijayan Sugumaran. Designing multi-agent systems: a framework and application. *Expert Syst. Appl.*, 28(2):259–271, 2005.

[87] Charles Pecheur and Franco Raimondi. Symbolic model checking of logics with actions. In *MoChArt*, pages 113–128, 2006.

[88] Wojciech Penczek and Alessio Lomuscio. Verifying epistemic properties of multi-agent systems via bounded model checking. *Fundamenta Informaticae*, 55(2):167–185, 2003.

[89] Igor Perko, Miro Gradisar, and Samo Bobek. Evaluating probability of default: Intelligent agents in managing a multi-model system. *Expert Syst. Appl.*, 38(5):5336–5345, 2011.

[90] Duc Quang Pham and James Harland. Temporal linear logic as a basis for flexible agent interactions. In *AAMAS*, pages 124–131, 2007.

[91] Amir Pnueli. The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, pages 46–57, Washington, DC, USA, 1977. IEEE Computer Society.

[92] Ronald L. Rivest. Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. Technical report, Unpublished manusecript, 1999.

[93] Martijn J. Rutten, Marta Z. Kwiatkowska, Gethin Norman, and David Parker. *Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems*, volume 23 of *CRM Monograph Series*. American Mathematical Society, 2004.

[94] Víctor Sánchez-Anguix, Vicente Julián, Vicente J. Botti, and Ana García-Fornes. Tasks for agent-based negotiation teams: Analysis, review, and challenges. *Eng. Appl. of AI*, 26(10):2480–2494, 2013.

[95] Renate A. Schmidt, Dmitry Tishkovsky, and Ullrich Hustadt. Interactions between knowledge, action and commitment within agent dynamic logic. *Studia Logica*, 78(3):381–415, 2004.

[96] Munindar P. Singh. Agent communication languages: Rethinking the principles. *Computer*, 31(12):40–47, 1998.

[97] Munindar P. Singh. An ontology for commitments in multiagent systems: Toward a unification of normative concepts. *Artificial Intelligence and Law*, 7:97–113, 1999.

[98] Munindar P. Singh. A social semantics for agent communication languages. In *Issues in Agent Communication*, pages 31–45. Springer-Verlag, 2000.

[99] Munindar P. Singh. Semantical considerations on dialectical and practical commitments. In *AAAI*, pages 176–181. AAAI Press, 2008.

[100] Munindar P. Singh, Matthew Arrott, Tina Balke, Amit K. Chopra, Rob Christiaanse, Stephen Cranefield, Frank Dignum, Davide Eynard, Emilia Farcas, Nicoletta Fornara, Fabien Gandon, Guido Governatori, Hoa Khanh Dam, Joris Hulstijn, Ingolf Krüger, Ho-Pun Lam, Michael Meisinger, Pablo Noriega, Bastin Tony Roy Savarimuthu, Kartik Tadanki, Harko Verhagen, and Serena Villata. The uses of norms. In *Normative Multi-Agent Systems*, pages 191–229. 2013.

[101] Munindar P. Singh and Michael N. Huhns. *Service-Oriented Computing: Semantics, Processes, Agents*. John Wiley & Sons Ltd, 2005.

[102] Songzheng Song, Jianye Hao, Yang Liu, Jun Sun, Ho-Fung Leung, and Jin Song Dong. Analyzing multi-agent systems with probabilistic model checking approach. In *ICSE*, pages 1337–1340, 2012.

[103] Khalid Sultan, Jamal Bentahar, and Mohamed El-Menshawy. Model checking probabilistic social commitments for intelligent agent communication. *Appl. Soft Comput.*, 22:397 – 409, 2014.

[104] Khalid Sultan, Jamal Bentahar, and Omar Marey. A probabilistic logic to reason about the interaction between knowledge and social commitments in MASs. In *SoMeT*, pages 132–147, 2014.

[105] Khalid Sultan, Jamal Bentahar, and Rabeb Mizouni. Model checking the interaction between individual and group knowledge and commitments in probabilistic multi-agent systems. *Engineering Applications of Artificial Intelligence*, pages 1–28, 2014 (Submitted).

[106] Khalid Sultan, Jamal Bentahar, Wei Wan, and Faisal Al-Saqqar. Modeling and verifying probabilistic multi-agent systems using knowledge and social commitments. *Expert Syst. Appl.*, 41(14):6291–6304, 2014.

[107] Khalid Sultan, Mohamed El-Menshawy, and Jamal Bentahar. Reasoning about social commitments in the presence of uncertainty. In *SoMeT*, pages 29–35, 2013.

[108] Pankaj R. Telang and Munindar P. Singh. Business modeling via commitments. In *SOCASE*, pages 111–125, 2009.

[109] Pankaj R. Telang and Munindar P. Singh. Specifying and verifying cross-organizational business models: An agent-oriented approach. *IEEE Transactions on Services Computing*, 5(3):305–318, 2012.

[110] Bas Testerink, Mehdi Dastani, and John-Jules Ch. Meyer. Norms in distributed organizations. In *Coordination, Organizations, Institutions, and Norms in Agent Systems*, pages 120–135, 2013.

[111] Paolo Torroni, Federico Chesani, P. Yolum, Marco Gavanelli, Munindar P. Singh, Evelina Lamma, M. Alberti, and P. Mello. *Modelling Interactions via Commitments and Expectations*. IGI Global, 2009.

[112] Moshe Y. Vardi. Automatic verification of probabilistic concurrent finite state programs. In *IEEE 26th Annual Symposium on Foundations of Computer Science*, pages 327–338, Oct 1985.

[113] Mario Verdicchio and Marco Colombetti. A logical model of social commitment for agent communication. In *AAMAS*, pages 528–535, 2003.

[114] Peter Walley. Measures of uncertainty in expert systems. *Artificial Intelligence*, 83(1):1–58, 1996.

[115] Wei Wan, Jamal Bentahar, and Abdessamad Ben Hamza. Quantitative model checking of knowledge. In *SoMeT*, pages 91–107, 2012.

[116] Wei Wan, Jamal Bentahar, and Abdessamad Ben Hamza. Model checking epistemic-probabilistic logic using probabilistic interpreted systems. *Knowledge-Based Systems*, 50:279–295, 2013.

[117] Stefan J. Witwicki and Edmund H. Durfee. Commitment-driven distributed joint policy search. In *AAMAS*, pages 492–499, 2007.

[118] Stefan J. Witwicki and Edmund H. Durfee. Commitment-based service coordination. *IJAOSE*, 3(1):59–87, 2009.

[119] Michael Wooldridge. Verifiable semantics for agent communication languages. In Yves Demazeau, editor, *ICMAS*, pages 349–356. IEEE Computer Society, 1998.

[120] Michael Wooldridge. Computationally grounded theories of agency. In *Fourth International Conference on MultiAgent Systems*, pages 13–20, 2000.

[121] Michael Wooldridge. Semantic issues in the verification of agent communication languages. *Autonomous Agents and Multi-Agent Systems*, 3, 2000.

[122] Michael Wooldridge. *An introduction to multiagent systems*. John Wiley & Sons, Chichester, UK., 2 edition, 2009.

[123] Michael Wooldridge and Nicholas Jennings. Intelligent agents: Theory and practice. *Knowledge Engineering Review*, 10(2):115–152, 1995.

[124] Ben Wright. Together, Is Anything Possiblel A Look at Collective Commitments for Agents. In *ICLP*, pages 476–480, 2012.

[125] Ping Xuan and Victor R. Lesser. Incorporating uncertainty in agent commitments. In *ATAL*, pages 57–70, 1999.

[126] Pınar Yolum and Munindar P Singh. Commitment machines. In *Intelligent Agents VIII*, pages 235–247. Springer, 2002.

[127] Pinar Yolum and Munindar P. Singh. Reasoning about commitments in the event calculus: An approach for specifying and executing protocols. *Annals of Mathematics and Artificial Intelligence*, 42(1-3):227–253, 2004.

[128] Junyan Yu and Long Wang. Group consensus in multi-agent systems with switching topologies and communication delays. *Systems & Control Letters*, 59(6):340–348, 2010.