Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.5, No.4, 2015

Automatic Verification of Communicative Commitments using Reduction

Mofleh Al-Diabat[1] Faisal Al-Saqqar[2] Ashraf Al-Saggar[3]

1-Prince Hussein Bin Abdullah College for Information Technology Al al-Bayt Uinverity, Mafraq, Jordan

2-Faculty of Engineering and Computer Science Concordia University, Canada

3- Irbid Electricity Company, Jordan

Abstract

In spite of the fact that modeling and verification of the Multi-Agent Systems (MASs) have been since long under study, there are several related challenges that should still be addressed. In effect, several frameworks have been established for modeling and verifying the MASs with regard to communicative commitments. A bulky volume of research has been conducted for defining semantics of these systems. Though, formal verification of these systems is still unresolved research problem. Within this context, this paper presents the CTL^{com} that reforms the CTLC, i.e., the temporal logic of the commitments, so as to enable reasoning about the commitments and fulfillment. Moreover, the paper introduces a fully-automated method for verification of the logic by means of trimming down the problem of a model that checks the CTLcom to a problem of a model that checks the GCTL*, which is a generalized version of the CTL* with action formulae. By so doing, we take advantage of the CWB-NC automata-based model checker as a tool for verification. Lastly, this paper presents a case study drawn from the business field, that is, the NetBill protocol, illustrates its implementation, and discusses the associated experimental results in order to illustrate the efficiency and effectiveness of the suggested technique.

Keywords: Multi-Agent Systems, Model Checking, Communicative commitment's, Reduction.

1 Introduction

Communication in the Multi-Agent Systems (MASs) is a key process by which the agents coordinate their actions and behaviors to achieve their goals [50]. However, in order for autonomous and heterogeneous agents to interact with each other, they use Agent Communication Languages (ACLs), which are usually associated with a semantic memory composed of different ontologies [21, 19]. Making this communication possible raises a need for defining formal semantics for these ACLs [25]. The first attempt to define such semantics was *the Speech Acts Theory of* Searle [38]. The formal semantics of Searle were described as the *mental approach* that attempts to make rational balance between certain agent

communication notions like intention, belief, and desire. The *mental approach* suggests that the agents can read the minds of one the other [41]. Hence, the mental approaches can not verify whether or not an agent is functioning in accordance with given semantics, which is a problem known commonly as the ACL semantics verification problem [49].

Thus, a switch in the MAS community to the social approaches took place so as to outdo the drawbacks of the semantics of the ACLs that are defined by using mental approaches [41]. The social approaches,

on the other hand, are employed for defining formal semantics for the ACLs [1, 23, 30, 43, 52]. Social commitments are employed in a number of those social approaches that successfully render robust representations to model the multi-agent interactions [8, 17, 18, 20, 33, 43]. This paper uses communicative social commitments as defined in [6, 25, 27] as a tool for information transfer via message passing. These commitments are formally referred to by $C_{i \to j}\ \phi$, which means that the agent *i*, which makes the commitment (i.e., the debtor), commits to the agent *j*, namely, the creditor (i.e., the agent for which the commitment is made), that content of commitment (ϕ) holds [27].

Example 1. A merchant, *M er*, commits to deliver goods to customer, *Cus*. This commitment is expressed as $C_{Mer \to Cus}\phi$, where ϕ means 'deliver the due goods'.

During the past decade, the social commitments were efficiently used in a broad range of fields that range from development of artificial institutions [31], to modeling business processes [18], development of Web-based applications [45], and specification and modeling of multi-agent interaction protocols, known as commitment-based protocols [4, 17, 37, 52]. The commitment between agents is not simply a static entity. Rather, it is a dynamic entity whose state changes with time [32]. This dynamicity characteristic supports flexibility of the commitments. In addition, it, can be captured by manipulating the commitments by means of certain operations like *discharge, creation, release, cancellation, delegation, and assignment* [42].

This ability to manipulate and negotiate the commitments is actually the most prominent element that makes the commitment-based approaches quite flexible and powerful in capturing various interaction patterns.

However, the incentive is not only inference about the social commitments and their actions, but is also application of the automatic and formal verification methods, like model checking, so as to verify the commitments. In the open environments like the e-business context, it is actually not realistic to presume that all the autonomous agents will act in accordance with the given protocols because it is likely that they will not function according to their commitments. Furthermore, formal verification is necessary for helping the protocol designers to enforce desired agent behaviors so that these protocols adhere to the given specifications at the design time.

Various approaches have successfully addressed the aforementioned challenge, including (i) the local testing method [45], (ii) the static verification method

[37, 52], and (iii) the semi-automatic verification method [51], in order to identify the non-compliant and compliant agents at the ends of these protocols.

In other respects, modeling the MASs when there are numerous dimensions to consider

simultaneously is challenge that makes their verification a hard task [5, 34].

This paper presents a new logic namely CTL^{com} logic. In this logic, we redefine the social accessibility relationship given in [6, 25]. After that, we modify the semantics of the social commitment and fulfillment that were introduced in [6]. Thereafter, we develop a transformation procedure to model check the new logic. Finally, we apply the proposed reduction algorithm on a real case study; the NetBill (NB) protocol [44] for the verification purpose.

2 Related Previous Works

After introducing to integration of the social commitment concept by Singh in [39, 40], research on the agent communication language on the basis of the commitment had gone a long way. Singh was the first to figure out the importance of incorporating the social notion of commitments to the agents in ACLs. He differentiated between two kinds of commitments: psychological commitment (i.e., a commitment of an agent to herself/himself) as it is exploited in the Artificial Intelligence (AI), and social commitment (i.e., a commitment of one agent to another to do certain actions). Singh concluded that the psychological commitment is a very restricted form of commitments as it corresponds to a unidirectional relationship and, once committed to a certain belief or intention, the agent can not reconsider it, even if she/he gets some positive new evidence or if the commitment contradicts with her/his goal. Later, Singh's social notion of commitment was further investigated by Castelfranchi [14], with a focus on the interactions among members of groups and organizations from a social perspective. Castelfranchi paid attention to clarification of some concepts to be able to suggest descriptive ontology to the organizations theory without taking into account the computational facets of social commitments. However, the first attempt to define the semantics of ACLs in terms of social concepts was made by Singh in [41]. This attempt emphasized the conventional meaning and public perspective. Since then, social commitments in have been mostly defined for agent communication in terms of computational logics [9, 11, 43, 46]. However, other researchers have proposed different techniques such as event calculus [52]. In this section, we are primarily interested in those approaches in which commitments are defined in terms of computational logics.

In [43], Singh integrated the CTL logic with new modalities for intentions, beliefs, and commitments to formalize the MASs by showing the interactions between agents.

In [46], Verdicchio and Colombetti introduced a new logic for the ACL semantics based the social commitment. In the proposed system, they developed a new logic called CTL$^{\pm}$.

Bentahar el al. [10, 11] introduced a new definition for social accessibility relation in order to develop a new commitment logic.

El-Menshawy et al. [24] tried to overcome the limitations raised in [10, 11] by suggesting new logical language called CTL^{sc} to develop specification language for the commitment-based protocols. The proposed logic expands the CTL* with commitments and concomitant actions. Additionally, they expanded the temporal modalities of the CTL* with past-oriented temporal modalities. Semantics of the actions were not defined in recursive way as in [10, 11], that is, semantics of every action are independent of those of other actions.

Later, El-Menshawy et al. [28] defined new temporal logic called the CTLC by

expanding the CTL with operators for the social commitments, as well as for their fulfillments and violations. Their main contribution was defining new social accessibility relationship whereby that presumed presence of intermediate state between the commitment and fulfillment states. However, introduction of the intermediate state makes computation of the accessible states very complex.

The CTLC logic has also been the basis of the works presented in Bentahar et al. [6] and El-Menshawy et al. [25]. In [6], Bentahar et al. refined the CTLC by introducing a number of unshared and shared variables so that their expanded version of interpreted systems can explain the communication between the interacting agents. What is particularly appealing in their approach is that the shared variables are only employed for motivating presence of communication channels, not for establishment of a communication. In [25], on the other hand, the researchers modified the CTLC into the CTLC^{+} which enables reasoning about the communicating commitments and their fulfillments. In this paper, we modify the social accessibility relationship presented in [6, 25] by allowing both agents to use their unshared variables in the communications with other agents (i.e., establishing more commitments). Details about our new social accessibility relation are given in Section 3.

In [26], El-Menshawy et al. proposed new logic-based language for specifying the commitment-based protocols. They defined this language in terms of the ACTL* logic, which, subsequently, expands the CTL* with operators for the social commitments and associated actions.

3 Interpreted Systems and the CTL^{com} logic

Th*is* section summarizes formalism of the interpreted systems that was introduced in [29] to model the MASs, besides two extensions of this formalism, in order to account for the agent's communication by use of the social commitments given by [6, 25]. Thereafter, we introduce our new social accessibility relationship.

3.1 Interpreted Systems

Interpreted Systems (IS) is a formalism developed by Fagin et al. in [29] to model multi-agent systems. IS classifies MASs into synchronous and asynchronous.

Bentahar et al. [6] and El-Menshawy et al. [25] expanded Fagin et al.'s formalism of the interpreted systems with unshared and shared variables so as to acknowledge the communication which takes place during execution of the MASs and to give intuitive semantics for the social commitments which are established by the communications between the interacting agents. In specific, they associated a countable group, Var_i, of local variables with every agent $i \in$ Agt. After that, they used those variables to exchange messages between communicating agents.

From the technical point of view, they referred to the value of a variable, x, in the set Var_i in the local state $l_i(g)$ by $l^x(g)$. Accordingly,

$$\text{if } l_i(g) = l_i(g^1), \text{ then } l^x(g) = l^x(g^1) \text{ for all } x \in Var_i \quad (1)$$

i ***i***

They used the idea of shared and unshared variables in modeling the communication between agents in MASs [6, 25].

Our new model M, is generated from the interpreted system developed in [29] and the extensions in [6] and [25].

Definition 1 (CTL^{com} Model)**.** *A model* $M_o = (S_o, I_o, R_{to}, \{\underset{\rightarrow}{\sim_{Ij}} | (i, j) \in \{A\}$ *where A is the set of agents },* V_o).

M_o *is a tuple, where:*

- S_o , I_o, V_o *and* $R_{t\,o}$ are defined as in [29] and [6].
- *For the pair* $(i,j) \in A$, $\sim_{I \to j} \subseteq S_o \times S_o$ *represents the social accessibility relation that is defined by* $s_o \; i \to j \; s_o^1$
- iff $Var_i \cap Var_j / = \emptyset$ such that $\forall x \in Var_i \cap Var_j$, we have $l_x(s) = l_x(s_1) = l_x(s_1)$.

I i j

To explain our proposed social accessibly relation ∼i→j, the two interacting agents have to share a communication channel to exchange messages (i.e, send and receive messages).

The shared channel represents the shared variable between interacting agents.

After receiving the content of the channel, all variables shared between the agents i and j will have

the same values (i.e., lx(s) = lx(s1) = lx(s1) $\forall x \in Var_i \cap Var_j$)

i i j

Comparing to the social accessibility relationship in [6, 25], the two agents can used both the shared and unshared variables to establish their communication. Therefore, these variables can differ from s to s^1. This concept is explained in Figure 1, where two agents, ***i*** and ***j***, are communicating through a channel and their unshared and shared are the following:

Agent i :

V ari = { x1, x2, x3}; Agent j: V arj = {x11, x12 , x13 }. The variable x1 is the variable shared by the two agents. It denotes presence of communication channel between i and j. The variables X1, x2, x3 and x11, x12 , x13 are the variables unshared by the two agents.

When the communication channel is established, the value of x1 for agent ***j*** in s is changed to be equal to the value of variable x_1 for agent ***I*** in s^1. This illustrates the message passing through the channel.

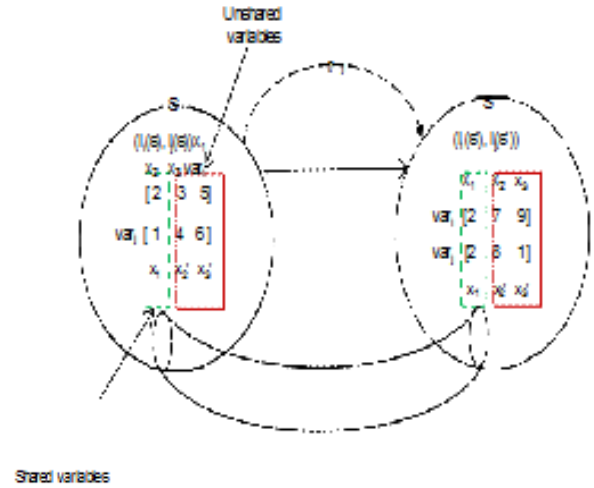


Figure 1. Our proposed accessibility relation $\sim_{i \to j}$

In the new definition of the social accessibility relation, we fix the problem found in [6, 25] that assumes that the creditor *j* could not gain a new information. In our model, both the creditor *j* and debtor *I* can get new information. We focus on the fact that only the shared variables should be the same. Therefore agents can join multiple communications.

4 CTL^{com} Logic

This section presents the semantics and syntax of the CTL^{com} logic, which is an expanding the CTL [2] logic with modalities to reason about the social commitments and their fulfillments. The syntax of CTL^{com} is defined as follows:

Definition 2 (Syntax of CTLcom).

$$\phi ::= p \mid \neg\phi \mid \phi \vee \phi \mid EX\phi \mid E(\phi U\, \phi) \mid EG\phi \mid Ci{\to}j\ \phi \mid F\ u(Ci{\to}j\ \phi).$$

where

- $p \in \Phi p$ is atomic proposition;
- The Boolean connectives ¬, and ∨ are the "not" and " or";
- E is the existential quantifier on paths;
- X, U , and G are CTL path modal connectives standing for ‘next’, ‘until’, and ‘globally’, respectively;
- The modal connective Ci→j expresses ‘commitment from i to j’; and
- The modal connective F u stands for ‘fulfillment’.

According to this logic, Ci→j ϕ is read as ‘the agent i commits to the agent j to result in

ϕ'. F u(Ci→j ϕ) is read as 'commitment Ci→j ϕ has been met'.

Other temporal modalities, e.g., F (future), and the universal path quantifier A can be defined as usual according to the foregoing definition (e.g., [16]).

Definition 3 (Satisfaction of CTL^{com})**.**

Given model M, satisfaction of the CTLcom formula ϕ in global state, s, expressed as (Mo, so) |= ϕ,

is defined recursively as follows:

- (Mo, so) |= p if and only if p ∈ V(so);
- (Mo, so) |= ¬ϕ iff (Mo, so) |= ϕ;
- (Mo, so) |= ϕ ∨ ψ iff (Mo, so) |= ϕ or (Mo, so) |= ψ;
- (Mo, so) |= EXϕ iff ∃ is a path π that begins at so such that (Mo, π(1)) |= ϕ;
- (Mo, so) |= E(ϕU ψ) iff ∃ a path π that starts at so such that for ko ≥ 0, (Mo, π(ko)) |= ψ

  and (Mo, π(j)) |= ϕ for all 0 ≤ j < k;
- (Mo, so) |= EGϕ iff ∃ a path π that begins at so such that (Mo, π(ko)) |= ϕ for all ko ≥ 0;
- (Mo, so) |= Ci→j ϕ iff ∀ the global states so1 ∈ So such that s ∼i→j so1, we have (Mo, so1) |= ϕ;
- (Mo, so) |= F u (Ci→j ϕ) iff ∃ is so1 ∈ So such that so1 ∼i→j s and (Mo, so1) |= Ci→j ϕ.

The Semantics of the CTLcom are defined using the model Mo as the same of the semantics of CTL (e.g., [2, 16])) besides two modalities for the commitments and their fulfillment. In the proposed semantics, the commitment formulas is satified if the formula ϕ holds in all accessible states from a state S1. On the other hand, the formula F u(Ci→j ϕ) is satisfied at state S0 iff a state S1 satisfies the commitment formulas and accessible using the social accessibility relation from S0.

5 Model Checking CTL^{com} Using Reduction

This section presents new technique for modeling check CTL^{com}. The formulation of the CTL^{com} model checking problem is as follows: Given a MAS which is modeled using interpreted system model M_o and a formula ϕ in CTL^{com} which represents a given property,

we want to check whether or not $M_o \models \phi$, that is, $\forall s \in I : (M_o, s) \models \phi$.

A model that checks the CTL^{com} logic can be implemented in two methods:

- Direct method by developing a new model checker or expanding an existent model checker as in [6, 36, 47].
- Formal reduction into existent model checker like in [12, 35, 48].

This study follows the formal reduction method by transforming the model checking CTL^{com} problem into a problem of a model checking existent logic, which is called Generalized CTL*, or simply GCTL* [13].

5.1 Reduction Procedure

We transform the proposed logic CTL^{com} into the GCTL* logic in order to use the CWB-NC model checker[1] of GCTL*. After that, we present the reduction (also called transformation) procedure. The GCTL* is defined as proposed in [13]:

$$S ::= p \mid \neg S \mid S \vee S \mid E\ P$$

$$P ::= \theta \mid \neg P \mid S \mid P \vee P \mid X\ P \mid P\ U\ P$$

where p is atomic proposition from Φ_p and θ is atomic action proposition from the set Φ_a. Two types of formulae are distinguished: (i) state formulae S that hold on specific state; and (ii) path formulae P that denote the temporal properties of the paths. State formulae are the legal GCTL* formulae.

The GCTL* model is defined as follows.

Definition 4 (Model of GCTL*). *A model $M_G = (S_G, Act, l_S, l_{Act}, \rightarrow, I_G)$ is tuple where S_G is non-empty group of states; Act is group of actions; $l_S : S_G \rightarrow 2^{\Phi p}$ is state-labeling function; $l_{Act} : Act \rightarrow 2^{\Phi a}$ is action-labeling function; $\rightarrow \subseteq S_G \times Act \times S_G$ is labeled transition relationship; and $I_G \subseteq S_G$ is group of initial states.*

By intuition, *SG* encompasses the reachable states of the system and *Act* expresses the atomic actions which the system may execute. In this sense, the labeling functions *lS* and *lAct* point to the atomic propositions that hold in a given state and action, respectively. The semantics of the GCTL* follow the standard convention in the temporal logic like CTL* [13]. A particular state fulfills $A\phi$ if each path beginning from this state satisfies ϕ. Furthermore, a certain path fulfills a state formula if the initial state in satisfy, and it fulfills θ if the label of the first transition on this path too fulfills θ. The time operators X and U are as usual.

The proposed reducing algorithm works as follows:

given a CTL^{com} model $Mo = (S, I, R_t, \{\sim_{l\_j} \mid (i,j) \in \mathrm{Ag}^2\}, V)$ and a CTL^{com} formula ϕ, there is a need for defining a GCTL* model $M_G = F(M)$ and a GCTL* formula $F(\phi)$ $\rightarrow$

using reduction function F such that $M \models \phi$ iff $F(M) \models F(\phi)$. The model $F(M)$ is defined as GCTL* model $M_G = (S_G, Act, l_S, l_{Act}, \to, I_G)$ as follows:

- $S_{oG} = So$;
- $I_{oG} = Io$;
- $l_{oS} = V_o$;
- We define the set Φ_a of atomic action propositions as a set of three actions: the first action is for the transition relationship. The second one is representing the social accessibility (to define the semantics of the commitment). Finally, the semantics of fulfillment is defined using the symmetric closure of social accessibility relation.

  $\Phi_a = \{E, \alpha_{1\to1}, \alpha_{1\to2}, \ldots, \alpha_{n\to n}\} \cup \{\gamma_{1\to1}, \gamma_{1\to2}, \ldots, \gamma_{n\to n}\}$, then
  $Act = \{\alpha^o, \alpha^{11}, \alpha^{nn}\} \cup \{\gamma^{11}, \gamma^{12}, \ldots, \gamma^{nn}\}$

  where α^o and α^{ij} are the three actions that are defined from
  The function l_{Act} is defined as follows:

  1. $\alpha o \in Act$, then $lAct(\alpha o) = \{E\}$,
  2. $lAct(\alpha ij) = \{\alpha i \to j\}$ for $1 \le i \le n$ and $1 \le j \le n$,
  3. $lAct(\gamma ij) = \{\gamma i \to j\}$ for $1 \le i \le n$ and $1 \le j \le n$; and

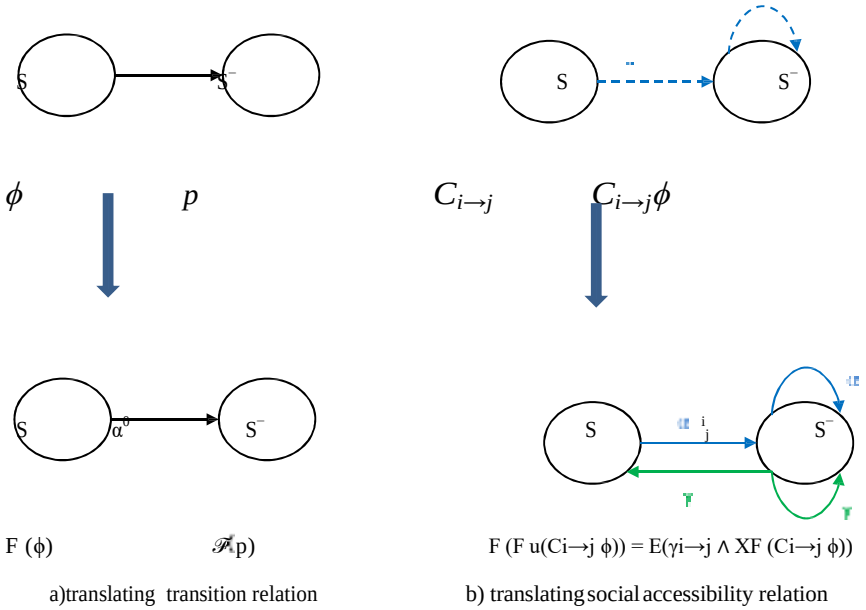
- The labeled transition $\to$ represents Rt (the temporal labeled transition), the accessibility

  1. $(s, \alpha o, s1) \in \to$ if $(s, s1) \in Rt$,
  2. $(s, \alpha ij, s1) \in \to$ if $s \sim_{i\to j} s^1$,
  3. $(s, \gamma ij, s1) \in \to$ if $(s1, \alpha ij, s)$.

Now, let us define F (ϕ) as a GCTL* formula using the CTL^{com} formula ϕ as follows

- $F(p) = p$, if p is atomic proposition;
- $F(\neg\phi) = \neg F(\phi)$;
- $F(\phi \vee \psi) = F(\phi) \vee F(\psi)$;
- $F(EX\phi) = EXF(\phi)$;
- $F(E(\phi\, U\, \psi)) = E(F(\phi)\, U\, F(\psi))$;
- $F(EG\phi) = EGF(\phi)$;

- $F(C_{i\to j}\phi) = A(\alpha_{i\to j} \wedge XF(\phi))$;
- $F(Fu(C_{i\to j}\phi)) = E(\gamma_{i\to j} \wedge XF(C_{i\to j}\phi))$.



a)translating transition relation b) translating social accessibility relation

Figure 2 transformation procedure F.

6 Case Study

One of the main objectives of this part of this study was to test effectiveness of our proposed reduction technique. We have applied the reduction technique introduced in Section 5.1 atop of the GCTL* [13]. Additionally, the case study on which we could apply this technique was the NB protocol [44], which was formerly used in [22, 26, 52] to illustrate how the commitments can specify protocols in the business settings.

6.1 Modeling NetBill Protocol

The NetBill (NB) payment protocol is adopted as an e-commerce protocol for buying and selling encrypted software through the internet [44] as illustrated in Figure 3. In this protocol, two agents are interacting to reach to an agreement for buying and selling goods at low prices. The NB starts by authenticating one seller (merchant) and one buyer or more (customers). After that, the buyer asks for special prices for certain goods from the seller. The seller prepares an offer for the requested goods and sends it to the buyer. In this case, the buyer has two options: (i) either to accept the offer (i.e., to commit to pay); or (ii) to reject the offer. If the buyer accepts the offer, then the seller delivers the digital information (requested goods) encrypted prohibiting the key (i.e., he commits to deliver the due goods). Then, the buyer organizes electronic payment order (EPO) that includes description of the received goods (i.e., abides by her/his commitment). The EPO will be verified by the NB server. Furthermore, the NB server credits the sellers' account and issues a receipt including a key for decrypting the goods. Finally, the seller sends the receipts to the buyer (i.e., adheres to her/his commitments).

6.2 Implementing the NetBill Protocol

We processed the NB protocol using our reduction technique on top of model checker CWB-NC. This tool is based on the *Alternating Büchi Tableau Automata* (ABTA), which are a variant of the alternating tree automata like the non-deterministic and deterministic Büchi automata. The tool and a detailed user manual can be downloaded from: http://www.cs.sunysb.edu/~cwb/DOWNLOADS/CWB/current/user.ps

Recently, the CWB-NC has been employed in models checking large-scale, multi-agent interaction protocols known as the commitment protocols [8, 25].

.

Syntax of the CCS language is obtained from the following BNF grammar [13]:

$$P ::= nil \mid \alpha.P \mid (P + P) \mid (P|P) \mid proc\ C = P$$

where Pdenotes the CCS process and the process nilmeans no action at all.

If Pis process and α is an action prefixing, then α.Pis process. Meanwhile, if P1and P2are processes, then so is P1 + P2using the choice operator "+", and if P1and P2are processes, then so is P1| P2using the parallel composition operator "|". The keyword procis employed to give the name *C* to the process P.

6.3 Verification Results

To verify our technique, we perform 10 experiments as shown in Table 1. We started with two agents and reported their result. After that, we increase number of agents by one and recoded the result of each experiment.

In Table 1, we have listed no of states, transitions, and the memory usage. The results showed that the state space grows exponentially when number of agents increases. Where the use of memory increases in polynomial manner. Consequently, our model checking algorithm shows high efficiency as the system grows up. The increment in memory usage is due to the increment in the number of reachable states and the mode size when number of agents is increased.

Table 1. verification results

Agents		States	Transitions	Memory (MB)
2	1(Mer.) + 1(Cust.)	24	72	4.778
3	1(Mer.) + 2(Cust.)	108	432	4.836
4	1(Mer.) + 3(Cust.)	456	2,280	4.945
5	1(Mer.) + 4(Cust.)	1,184	11,304	5.157
6	1(Mer.) + 5(Cust.)	7,696	53,872	5.727
7	1(Mer.) + 6(Cust.)	3.13E +4	2.50E +5	6.400
8	1(Mer.) + 7(Cust.)	1.27E +5	1.14E +6	6.892
9	1(Mer.) + 8(Cust.)	5.11E +5	5.11E +6	8.030
10	1(Mer.) + 9(Cust.)	2.06E +6	2.26E +7	8.961

Another fundamental objective of this paper was to use CTL^{com} to verify the

properties of the protocols that involve interactions between the agents in the MASs by using the commitments and their fulfillments. Usually, these properties express certain protocol requirements that need to be met. In effect, several properties are proposed in the literature [15, 17, 7, 27]. In this section, we check the *Safety*, *Liveness*, and *Commitment Fulfillment* properties in the NB protocol.

- Safety

  The safety property means ensuring that 'something bad will never take place'. This bad situation can be avoided using CTL^{com} as follows:

  $\phi_1 = AG\ \neg(pay \wedge AG(\neg C_{Mer \rightarrow Cus} sendReceipt))$.

- Liveness

  This property means implies that 'eventually something good will take place'. For instance, in all the paths, globally, when customer asks for a price offer, then in all the paths in the future the merchant will deliver the due goods. This property is expressed in the CTL^{com} as follows:

  $\phi_2 = AG(reqOffer \rightarrow AF(C_{Mer \rightarrow Cus} deliverGoods))$.

- Fulfillment ofCommitment

  When verifying the behaviors of the agents in terms of fulfillment of their commitments, it is critical to verify some of the conditions under which fulfillment may take place. For instance, when a customer sends payment to the merchant, the commitment is fulfilled successfully. This property can be denoted as:

  $\Phi_3 = \mathrm{EF}\,(FU(C_{Cus \rightarrow Mer} Pay))$

  Table 2 lists the outcomes of model check of the aforementioned desirable properties in the case of the NB protocol.

Table 2. Results of model checking some protocol properties

Formulae	Results	Time for MC (sec)
ϕ_1	True	< 0.01
ϕ_2	True	< 0.01
ϕ_3	True	< 0.01

We notice that the four formulae hold in the model, hence suggesting that that our proposed method is successful in expressing the properties of the protocol using CTL^{com} and that our reduction-based model checking procedure works effectively. The time that elapsed in verifying each of the formulae is close to zero and is almost the same for each tested formulae. This indicates efficiency of the underlying algorithms and the optimization methods that were employed in the CWB-NC model checker.

7 Conclusions and Suggestions for Future Work

This paper introduced new, automatic method for trimming down the problem of a model that checks the CTL^{com}, which is an extension of the CTL with modalities for the

commitments and their fulfillment. We proved the effectiveness of the proposed techniques by applying it in a real case study namely NB protocol. We have verified the NB protocol using the CWB-NC model checker. We could successfully check some of the desirable properties of the protocol expressed in the CTL^{com}. Moreover, we showed that the system is scalable since we could check up to 2.06E+6 states and 2.26 E+7 transitions. These promising outcomes confirm effectiveness of the CTL^{com} in capturing the interactions between the agents by utilizing the social commitment concepts, even in large systems.

In the future, we plan to develop a new model checking algorithms for the CTL^{com} logic. By doing this, we will become able to compare between the two techniques by using the obtained verification results. Additionally, we plan to take into consideration other actions like withdrawal, violation, delegation, and assignment. We also plan to examine the interactions between the agents in the MASs by using probabilistic communicative commitments.

References

[1] M. Alberti, M. Gavanelli, E. Lamma, P. Mello, and P. Torroni. Specification and verification of agent interaction using social integrity constraints. Electr. Notes Theor. Comput. Sci., 85(2):94–116, 2004.

[2] F. D. Anger and E. M. Clarke. New and used temporal models: An issue of time. Applied Intelligence, 3(1):5–15, 1993.

[3] C. Baier and J.-P. Katoen. Principles of Model Checking (Representation and Mind Series). The MIT Press, 2008.

[4] M. Baldoni, C. Baroglio, and E. Marengo. Behavior-oriented commitment-based protocols. In ECAI, pages 137–142, 2010.

[5] F. Be´he´, S. Galland, N. Gaud, C. Nicolle, and A. Koukam. An ontology-based metamodel for multiagent- based simulations. Simulation Modelling Practice and Theory, 40:64–85, 2014.

[6] J. Bentahar, M. El-Menshawy, H. Qu, and R. Dssouli. Communicative commitments: Model checking and complexity analysis. Knowledge-Based Systems, 35:21–34, 2012.

[7] J. Bentahar, J.-J. Meyer, and W. Wan. Model checking communicative agent-based systems. Know.-Based Syst., 22(3):142–159, Apr. 2009.

[8] J. Bentahar, J.-J. Meyer, and W. Wan. Model checking agent communication. In Specification and Verifica- tion of Multi-agent Systems, pages 67–102. Springer, 2010.

[9] J. Bentahar, B. Moulin, and B. Chaib-draa. Towards a formal framework for conversational agents. In Proceedings of the Agent Communication Languages and Conversation Policies AAMAS 2003 Workshop, 2003. July 14th 2003, 2003.

[10] J. Bentahar, B. Moulin, J.-J. C. Meyer, and B. Chaib-draa. A logical model for commitment and argu- ment network for agent communication. In Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems, AAMAS '04, pages 792–799, 2004.

[11] J. Bentahar, B. Moulin, J.-J. C. Meyer, and Y. Lespe´rance. A new logical semantics for agent communication. In Proceedings of the 7th international conference on Computational logic in multi-agent systems, pages 151–170, Berlin, Heidelberg, 2007. Springer-Verlag.

[12] J. Bentahar, H. Yahyaoui, M. Kova, and Z. Maamar. Symbolic model checking composite web services using operational and control behaviors. Expert Syst. Appl., 40(2):508–522, 2013.

[13] G. Bhat, R. Cleaveland, and A. Groce. Efficient model checking via Bu¨chi tableau automata. In G. Berry,

[14]H. Comon, and A. Finkel, editors, CAV, Lecture Notes in Computer Science, pages 38–52. Springer, 2001. [14] C. Castelfranchi. Commitments: From individual intentions to

groups and organizations. In V. R. Lesser and L. Gasser, editors, ICMAS, pages 41–48. The MIT Press, 1995.
[15] Z. Cheng. Verifying commitment-based business protocols and their compositions: model checking using promela and spin. North Carolina State University, 2006. Ph.D. thesis.
[16] E. M. Clarke, O. Grumberg, and D. A. Peled. Model checking. The MIT Press, Cambridge, 1999.
[17] N. Desai, Z. Cheng, A. K. Chopra, and M. P. Singh. Toward verification of commitment protocols and their compositions. In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS), pages 144–146, 2007.
[18] N. Desai, A. K. Chopra, and M. P. Singh. Amoeba: A methodology for modeling and evolving cross- organizational business processes. ACM Trans. Softw. Eng. Methodol., 19(2), 2009.
[19] F. Dignum and M. Greaves, editors. Issues in Agent Communication, volume 1916 of Lecture Notes in Computer Science. Springer, 2000.
[20] F. Dignum, J.-J. C. Meyer, R. Wieringa, and R. Kuiper. A modal approach to intentions, commitments and obligations: Intention plus commitment yields obligation. In DEON, pages 80–97, 1996.
[21] S. Dourlens, A. Ramdane-Cherif, and E. Monacelli. Multi levels semantic architecture for multimodal interaction. Applied Intelligence, 38(4):586–599, 2013.
[22] M. El-Menshawy, J. Bentahar, and R. Dssouli. Symbolic model checking commitment protocols using reduction. In DALT, pages 185–203, 2010.
[23] M. El-Menshawy, J. Bentahar, and R. Dssouli. Verifiable semantic model for agent interactions using social commitments. In LADS, pages 128–152, 2010.
[24] M. El-Menshawy, J. Bentahar, and R. Dssouli. Verifiable semantic model for agent interactions using social commitments. In LADS, pages 128–152, 2010.
[25] M. El-Menshawy, J. Bentahar, W. E. Kholy, and R. Dssouli. Reducing model checking commitments for agent communication to model checking ARCTL and GCTL*. Autonomous Agents and Multi-Agent Sys- tems, 27(3):375–418, 2013.
[26] M. El-Menshawy, J. Bentahar, W. E. Kholy, and R. Dssouli.Verifying conformance of multi-agent commitment-based protocols. Expert Syst. Appl., 40(1):122–138, 2013.
[27] M. El-Menshawy, J. Bentahar, H. Qu, and R. Dssouli. On the verification of social commitments and time. In Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS), pages 483–490, 2011.
[28] M. El-Menshawy, J. Bentahar, H. Qu, and R. Dssouli. On the verification of social commitments and time.In AAMAS, pages 483–490, 2011.
[29] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. Reasoning about Knowledge. The MIT Press, Cambridge, 1995.
[30] N. Fornara and M. Colombetti. A commitment-based approach to agent communication. Applied Artificial Intelligence, 18(9-10):853–866, 2004.
[31] N. Fornara, F. Vigano`, M. Verdicchio, and M. Colombetti. Artificial institutions: a model of institutional reality for open multiagent systems. Artif. Intell. Law, 16(1):89–105, 2008.
[32] A. Gnay and P. Yolum. Constraint satisfaction as a tool for modeling and checking feasibility of multiagent commitments. Applied Intelligence, 39(3):489–509, 2013.
[33] A. Gu¨nay and P. Yolum. Constraint satisfaction as a tool for modeling and checking feasibility of multiagent commitments. Applied Intelligence, 39(3):489–509, 2013.
[34] S. Konur, M. Fisher, and S. Schewe. Combined model checking for temporal, probabilistic, and real-time
logics. Theor. Comput. Sci., 503:61–88, 2013.
[35] A. Lomuscio, C. Pecheur, and F. Raimondi. Automatic verification of knowledge and time with nusmv. In Proceedings of the 20th International Joint Conference on Artifical Intelligence, IJCAI'07, pages 1384– 1389, San Francisco, CA, USA, 2007. Morgan Kaufmann Publishers Inc.
[36] A. Lomuscio and W. Penczek. Symbolic model checking for temporal-epistemic logic. In Logic Programs, Norms and Action, pages 172–195, 2012.
[37] A. U. Mallya and M. P. Singh. An algebra for commitment protocols. Autonomous

Agents and Multi-Agent Systems, 14(2):143–163, 2007.
[38] J. R. Searle. Speech acts: An essay in the philosophy of language. Cambridge, Cambridge University Press, 1969.
[39] M. P. Singh. Social and psychological commitments in multiagent systems. In AAAI Fall Symposium on Knowledge and Actions at Social and Organizational Levels, pages 104–106, 1991.
[40] M. P. Singh. A conceptual analysis of commitments in multiagent systems. Technical report, Raleigh, NC, USA, 1996.
[41] M. P. Singh. Agent communication languages: Rethinking the principles. IEEE Computer, 31(12):40–47, 1998.
[42] M. P. Singh. An ontology for commitments in multiagent systems. Artif. Intell. Law, 7(1):97–113, 1999.
[43] M. P. Singh. A social semantics for agent communication languages. In Issues in Agent Communication, pages 31–45, 2000.
[44] M. A. Sirbu. Credits and debits on the internet. IEEE Spectr., 34(2):23–29, Feb. 1997.
[45] M. Venkatraman and M. P. Singh. Verifying compliance with commitment protocols. Autonomous Agents and Multi-Agent Systems, 2(3):217–236, 1999.
[46] M. Verdicchio and M. Colombetti. A logical model of social commitment for agent communication. In Proceedings of the second international joint conference on Autonomous agents and multiagent systems, AAMAS '03, pages 528–535. ACM, 2003.
[47] W. Wan, J. Bentahar, and A. B. Hamza. Model checking epistemic and probabilistic properties of multi-agent systems. In IEA/AIE (2), pages 68–78, 2011.
[48] W. Wan, J. Bentahar, and A. B. Hamza. Model checking epistemic-probabilistic logic using probabilistic interpreted systems. Knowl.-Based Syst., 50:279–295, 2013.
[49] M. Wooldridge. Introduction to multiagent systems. Wiley, 2002.
[50] M. Wooldridge and N. R. Jennings. Intelligent agents: Theory and practice. Knowledge Engineering Review, 10(2):115–152, 1995.
[51] P. Yolum. Design time analysis of multiagent protocols. Data Knowl. Eng., 63(1):137–154, Oct. 2007.
[52] P. Yolum and M. P. Singh. Reasoning about commitments in the event calculus: An approach for specifying and executing protocols. Ann. Math. Artif. Intell., 42(1-3):227–253, 2004.