Belief in Process Algebra

Vivek Vishal
Student number: 0788625
email: v.vishal@student.tue.nl

January 19, 2012

Abstract

In this paper we present a framework to model falsehood in a system. A falsehood or lie is an intended false positive announced by a principal with an objective to deceive other principals. An utterance of lie is said to be successful if other principals believe it. The framework introduced in this paper is essentially a combination of operational model and epistemic model allowing us to express both temporal and epistemic properties. We visualize the environment when a lie is communicated through an extended version of labeled transition system. Moreover, we analyze when a lie can be successful and when it fails.

1 Introduction

To verify the properties of a model, one can consider two types of properties, namely, temporal properties and epistemic properties. Temporal properties refer to occurrence of events and their relative ordering, capturing properties such as liveness and fairness. On the other hand, epistemic properties concerns reasoning about knowledge and its related properties such as knowledge, belief, common knowledge.

The behavior of a system can easily be specified by the means of process algebra [GM11, AILS07] and its temporal properties are then verified by applying model checking techniques [CGP99] on the underlying transition system. Reasoning about knowledge is based on set of *possible worlds*. The intuitive idea behind the *possible worlds* is that besides the true state of affairs there are a number of other possible states of affairs. The *possible worlds* are formalized in terms of *Kripke structures* and the validity of a given epistemic formula depends on the world as well as a whole *Kripke structure*.

Both types of properties are extensively investigated in literature [GM11, AILS07] [FHMV95]. However most of the frameworks proposed in the literature allow for specification and reasoning. When we have to model a system in which both temporal and epistemic properties play a vital role, we need a unified framework in which we can express and verify both type of properties.

Various group-level epistemic actions such as private group announcements, announcements with suspicious outsiders, etc. are described in [BMS99], where such actions correspond to additional modalities in their object language. A new system was proposed in [BEK05] which extends the epistemic base language to allow a compositional analysis of epistemic postconditions. Lying was modeled in [DESW10] as a communicative act changing the beliefs of the agents in a multi-agent system. However, all these frameworks are confirmed to modeling and verification of epistemic properties and does not suffice the need of unified framework to support verification of both temporal and epistemic properties.

Recently some researchers have come up with a unified framework, where one can specify and verify both temporal and epistemic properties of a model. In [DMO07], explicit identities were introduced in a Process Algebra known as the Process Algebra with identities (*PAi*). The operational semantics of *PAi* is given in terms of an *Annotated Labeled Transition System* (ALTS) which is an labeled transition system extended with indistinguishability relationship among operational states. It provides a rich temporal epistemic logic $E\bar{\mu}$ for specification and verification of both temporal and epistemic properties. This framework captures unintentional information leaks where a principal learns something which was never explicitly told to it.

Our work is basically an extension of this framework by introducing the notion of lie into it. A lie is an intended false positive announced by a principal with an objective to deceive other principals from truth [DESW10]. We consider a simple case where all listeners presumes that only truth is announced. This model is very useful in many practical protocols where a principal's objective is to deceive other optimistic principals to think that a trace(or action), different from current trace(or action), has been taken .

Overview Section 2 gives a brief introduction of reasoning about knowledge and a combined framework to express both temporal and epistemic properties. The process language for specifying systems and a transition system semantics of it is introduced in section 3. Section 4 gives an example of successful lies and section 5 demonstrates the case of unsuccessful lies. Finally, we conclude the paper and present the directions of future research in section 6.

2 Preliminaries

The reasoning about knowledge is made possible by a collection of axioms and inference rules. The most common axioms are:

- ***Knowledge axiom:*** This axiom states that if a principal knows something, it has to be true.

  $$\models K_i\varphi \Rightarrow \varphi$$

  where $K_i\varphi$ represents *agent i knows the fact φ.*

- ***Distribution Axiom:*** It states that each principal knows all the logical consequences of his knowledge. If a principal knows φ and knows that φ implies ψ, then

ψ is true at all worlds he considers possible, so he knows ψ.

$$\models K_i\varphi \wedge K_i(\varphi \;\Rightarrow\; \psi) \Rightarrow K_i\psi$$

- ***Positive Introspection:*** This property state that a principal has introspection about its own knowledge, i.e., agents know that they know what they know.

$$\models K_i\varphi \Rightarrow K_iK_i\varphi$$

- ***Negative Introspection:*** This property state that if a principal does not know a fact, then he knows that he does not know that fact.

$$\models \neg K_i\varphi \Rightarrow K_i\neg K_i\varphi$$

Historically, *Distribution axiom* is known as **K**, *Knowledge axiom* is known as **T** and *Positive* and *Negative Introspection* are known as **4** and **5** respectively. We get different modal logics by considering various subsets of these axioms like **KT45, K45** etc.

Kripke Structure: A Kripke Structure K is a 5-tuple $< S,\ I,\ AP,\ \rightarrow,\ L >$, where:

- S is a set of states.
- I is the set of initial states: $I \subseteq S$.
- AP is a set of atomic propositions.
- $\rightarrow$ is a transition relation: $\rightarrow \subseteq S \times S$.
- L is a state labelling: $L : S \rightarrow 2^{AP}$.

Illustration: Let us consider a simple card showing game. Alice, Bob, and Carol each hold one of the cards p, q, r. Suppose in the actual situation, Alice, Bob and Carol, hold card p, q and r respectively. For Alice the actual world is among two worlds, one in which she holds p, Bob holds q and Carol holds r and the other worlds in which she holds p, Bob holds r and Carol holds q. These two worlds become indistinguishable to her as shown in Figure 1 by the indistinguishability relation labeled with a between worlds pqr and prq. Similarly, Bob cannot distinguish between the worlds pqr and rqp and Carol cannot distinguish between the worlds pqr and qpr. Note that we have considered only one possible scenario of actual world, i.e., pqr. However, there can be six different possible actual worlds and for each of these worlds, the players will have different perceptions. The generalized model is shown in Figure 1.

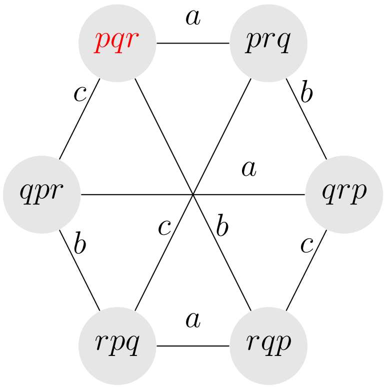

Figure 1: All possible worlds in card showing game

Transition: Now assume that Alice shows her card to Bob. This action reduces the number of possible worlds of Bob to one, i.e., actual world, as he knows his own and Alice's card, he also knows Carol's as there are only three cards. However, Alice and Carol still have two possible worlds. This action results in a transition from one Kripke structure to another.

Now Bob also shows his card to Alice, reducing her possible worlds to the actual world. This action also results in a transition from one Kripke structure to another. The transitions among Kripke structures as a result of execution of these actions is shown in Figure 2.

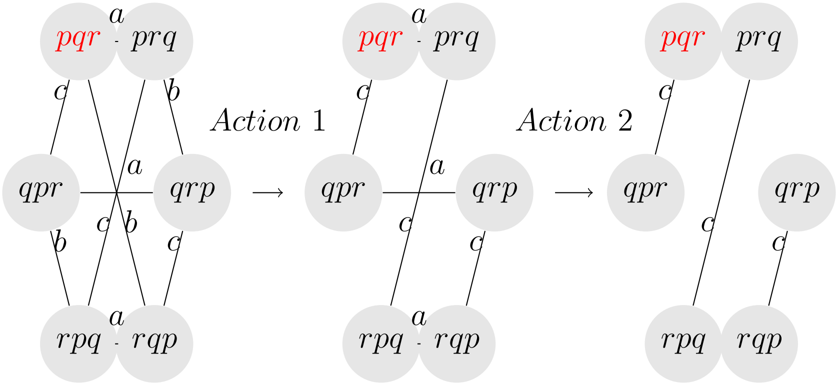

Figure 2: Transitions among Kripke structure

Comparison: In case of process algebra the transition relationship is among states upon execution of an action, shown with the help of a Labeled Transition System(LTS). However, we have seen that the transition relationship in Epistemic logic in among Kripke structures. Furthermore, LTS does not have principals as labels and does not have a in distinguishability relationship among states.

Combined framework PAi : In [DMO07], a combined framework has been presented in which one can investigate both temporal and epistemic properties of a system. This framework aims to capture information leaks within a verification framework, which requires investigation of both temporal and epistemic logic. Actions were prefixed with principals who actually know that action when it executes and for other principals the execution of that action has a public appearance, i.e., they know some action has been executed but does not know exactly which action has executed. Indistinguishability relation ship was introduced among operational states to capture epistemic properties. Consider the following example:

$$P = (1)a; (1,2)d + (1)b + (1)c.$$

P denotes the process that executes one of the actions a, b, c, where ";" denotes sequential composition and "+" denotes non-deterministic choice among processes. The actions are prefixed with the IDs of principal which are allowed to observe that action. For all other principals that action appears as public action, i.e., they know some action has been executed but does not know exactly what action. In this particular scenario only principal 1 is aware of the exact action taking place. 1 could be the principal making a choice between actions a, b and c, and 2 could be an observer who only notices that a choice has been made, but not what the outcome was. This is a process-style formalization of the private communication from epistemic modeling, where a party learns something while other parties are watching and learn that the party learned something, but not precisely what. After the first step, the process terminates or, if the first step was a, continues with the execution of d. Since principal 2 is allowed to observe the execution of d, 2 may now conclude that the first step must have been a, although 2 was not actually allowed to observe the a. Figure 3 represents three aspects of the Process P. Leftmost part of this figure

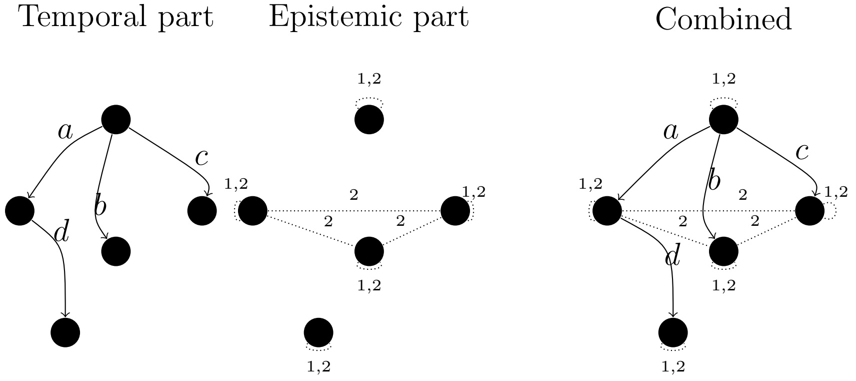

Figure 3: LTS, KS and ALTS for process P

represents temporal part showing non-deterministic choice between a, b, c and sequential composition of action a and d. Middle part consists on three Kripke structures with one, three and one worlds from top to bottom respectively. Initially, both principals knows the actual world, however after the execution of action a or b or c, 1 knows the actual world but 2 cannot distinguish among the three possible worlds. After the execution of d both principals knows the actual world as action d is visible to both. The rightmost part of the figure represents the combination of both temporal and epistemic part, known as Annoted Labeled Transition System(ALTS).

3 *PAi**: Syntax and Operational Semantics

In this section, we present the syntax and semantics of a slightly modified version of the Process Algebra with identities *(PAi)* from [DMO07] to which we refer as *PAi**. Our process algebra has all the ingredients of *PAi* except that in place of decorated actions D we use simple atomic action. We also introduce an appearance function ρ in it, which serves to model lies, i.e., actions that appears differently to different principals.

PAi* : syntax Let $\mathcal{A}ct$ be a finite set of action names. Actions can be denoted by a, b, ?a, !a, ... Question mark and exclamation mark represent the receiving and the sending parts of a communication, respectively, and an action without such marks is the outcome of the communication. Let $\mathcal{I}d$ be a finite set of *identities* denoted by i, j, ... We assume that all the identities involved in the protocol are fully aware of the protocol, i.e., they know the sequence of actions and possible points of choice that can be made as a part of execution of the protocol.

$$\begin{cases} Proc ::= 0 \mid \alpha \mid Proc; Proc \mid Proc + Proc \mid Proc || Proc \\ \alpha \;\; \epsilon \;\; \mathcal{A}ct, \\ \rho ::= \mathcal{A}ct \times Id \rightarrow \mathcal{A}ct, \end{cases} \tag{1}$$

where 0 represents the process that has terminated. Sequential composition of processes is represented by *Proc;Proc*. *Proc+Proc* represents nondeterministic choice, i.e., the first action taken from either of the two arguments will resolve the choice in favor of that argument and $Proc||Proc$ denotes parallel composition. How an action appears to a principal is denoted by ρ.

A Protocol is modeled by a process, which may have many traces of actions from the initial to the final state. If we want to model lie in this framework we have to deceive one or more principals, so that a trace taken so far appears as another possible trace of the protocol. We can do this by the use of appearance function as a part of protocol execution, i.e., if $\rho(a, i) = b$ then action a appears to i as b.

We assume that the principals present in the protocol are aware of the protocol. Lying can result in two possible cases: the first case is full proof, i.e., after the end of the execution of the protocol every principal has a consistent view of the system. In the second case,

Figure 4: SOS semantics for *PAi**

$$(\mathbf{0})\frac{}{(0,\pi)\surd} \quad (\mathbf{a})\frac{}{(\alpha,\pi) \overset{\alpha}{\Longrightarrow} (0,\pi \frown \alpha)}$$

$$(\mathbf{s0})\frac{(x_0,\pi) \overset{\alpha}{\Longrightarrow} (y_0,\pi')}{(x_0;x_1,\pi) \overset{\alpha}{\Longrightarrow} (y_0;x_1,\pi')} \quad (\mathbf{s1})\frac{(x_0,\pi)\surd \quad (x_1,\pi) \overset{\alpha}{\Longrightarrow} (y_1,\pi')}{(x_0;x_1,\pi) \overset{\alpha}{\Longrightarrow} (y_1,\pi')} \quad (\mathbf{s2})\frac{(x_0,\pi)\surd \quad (x_1,\pi')\surd}{(x_0;x_1,\pi'')\surd}$$

$$(\mathbf{n0})\frac{(x_0,\pi) \overset{\alpha}{\Longrightarrow} (y_0,\pi')}{(x_0+x_1,\pi) \overset{\alpha}{\Longrightarrow} (y_0,\pi')} \quad (\mathbf{n2})\frac{(x_0,\pi)\surd}{(x_0+x_1,\pi')\surd}$$

$$(\mathbf{p0})\frac{(x_0,\pi) \overset{\alpha}{\Longrightarrow} (y_0,\pi')}{(x_0||x_1,\pi) \overset{\alpha}{\Longrightarrow} (y_0||x_1,\pi')} \quad (\mathbf{p2})\frac{(x_0,\pi)\surd \quad (x_1,\pi')\surd}{(x_0||x_1,\pi'')\surd}$$

$$(\mathbf{p3})\frac{(x_0,\pi) \overset{?\alpha}{\Longrightarrow} (y_0,\pi') \quad (x_1,\pi) \overset{!\alpha}{\Longrightarrow} (y_1,\pi'')}{(x_0||x_1,\pi) \overset{\alpha}{\Longrightarrow} (y_0||y_1,\pi \frown \alpha)}$$

$$(\lambda\mathbf{0})\frac{}{\Phi \overset{i}{\rightsquigarrow} \Phi} \quad (\lambda\mathbf{1})\frac{\pi \overset{i}{\rightsquigarrow} \pi' \quad \rho(a) \ = \ b}{\pi \frown a \overset{i}{\rightsquigarrow} \pi' \frown b}$$

$$(\mathbf{strip})\frac{(x,\pi) \overset{(\alpha)}{\Longrightarrow} (y,\pi')}{(x,\pi) \overset{\alpha}{\rightarrow} (y,\pi')} \quad (\mathbf{A})\frac{\pi_0 \overset{i}{\rightsquigarrow} \pi_1}{(x_0,\pi_0) \overset{i}{\dashrightarrow} (x_1,\pi_1)}$$

the lie can be detected. A lie can be detected when one or more principals observes a contradictory trace which does not occur in the set of possible traces of a protocol.

***PAi** : operational semantics** We use an *Annotated labeled transition system*(ALTS) with appearance relation(ALTS*) to describe the behavior of our model. A principal identifies a sequence of trace out of many possible traces on the basis of actions appeared to him as a part of protocol execution. We consider that every principal has same viewpoint of the system.

Definition 1 (ALTS*). Given a set $\mathcal{A}ct$ of actions, an Annotated labeled transition system* ALTS* is a five tuple $\langle St, \rightarrow, A, \surd, s_0\rangle$ where,

- St is a set of operational states,
- $\rightarrow \subseteq St \times \mathcal{A}ct \times St$ is transition from one state to another
- $A \subseteq St \times \mathcal{I}d \times St$ is the appearance function.
- $\surd$ is the termination predicate.
- s_o is the initial state.

For readability, we denote statements $(s, l, s') \in \rightarrow$, $(s, i, s') \in A$ and $s \in \surd$ by $s \xrightarrow{l} s'$, $s \overset{i}{\dashrightarrow} s'$ and $s\surd$ respectively, for each $s, s' \in St$, $i \in \mathcal{I}d$ and $l \in \mathcal{A}ct$.

In Figure 4, we associate the ALTS* to *PAi** process by the means of *Structural Operational Semantics* SOS. The operational state of *PAi** is a pair (p, π), where $p \in Proc$ is a *PAi** process and π is a finite sequence of actions recording the perception of the process gathered so far. Sequencing of actions is denoted by $\frown$. We have defined auxiliary functions $\overset{\alpha}{\Longrightarrow} \subseteq St \times St$ and $\overset{i}{\rightsquigarrow} \subseteq \mathcal{A}ct^* \times \mathcal{A}ct^*$. Transition relation $\overset{\alpha}{\Longrightarrow}$ defines transitions among operational states labeled with action α. Appearance relation $\overset{i}{\rightsquigarrow}$ defines when one trace appears as another trace from the perspective of principal i. In rule ($\lambda\mathbf{0}$), Φ denotes empty sequence of actions which occurs in the initial state. Rule ($\lambda\mathbf{1}$) states when a trace appears as another trace to principal i after execution of an action and rule **(strip)** applies encapsulation by leaving out individual send and receive actions and obtain the transition relation $\rightarrow$. Deduction rule (**A**) maps the appearance function from traces to operational states.

4 Successful lies

In this section we will illustrate the concept of successful lie using as example in $PAi*$ syntax and its underlying ALTS*. Take the following $Pai*$ process:

$$\begin{array}{llll} P = a; b; c + b; b; c + b; a; c. & & & \\ \rho : a \times 1 \rightarrow a & b \times 1 \rightarrow b & c \times 1 \rightarrow c \\ \quad a \times 2 \rightarrow b & b \times 2 \rightarrow b & c \times 2 \rightarrow c \end{array}$$

P denotes the process that executes one of the traces $a; b; c,\ b; b; c,\ b; a; c$. The appearance relation ρ describes how an action appears to a principal. Let us now consider all possible cases. Suppose the first action executed is a. After the execution of a principal 1 will follow the state with trace a. However, action a appears to principal 2 as b. Therefore he will be in either of the states with trace b as shown by dashed arrow in Figure 5. Now action b executes. Principal 1 will be in a state with trace $a \frown b$, where as principal 2 will be in a state with trace $b \frown b$. The deviation of perception of principal 2 is shown by a dashed arrow. Similarly after the execution of action c, principal 1 will be in a state with trace $a \frown b \frown c$ and principal 2 will be a state with trace $b \frown b \frown c$.

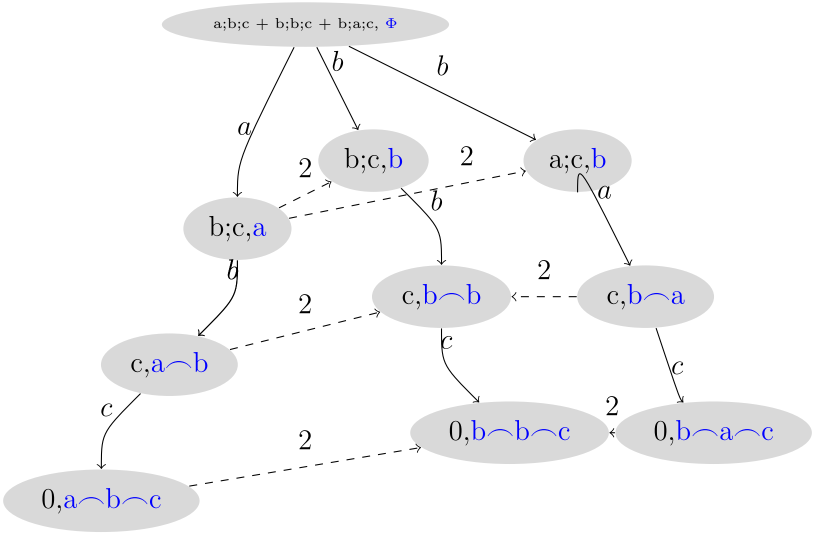

Figure 5: Successful lie.

Now let the sequence of action has being executed is $b; b; c$. As in this particular sequence of execution every action appears as it is to both the principals, both principals will follow the trace $b \frown b \frown c$.

Finally consider the trace $b; a; c$. After the execution of action b, the two states with trace b will become indistinguishable to both the principals. When action a happens, principal 1 will be in the state with trace $b \frown a$ while principal 2 will be in the state with trace $b \frown b$, as a appears to principal 2 as b. After the execution on action c, principal 1 will be in the state with trace $b \frown a \frown c$ and principal 2 have the perception of being in the state with trace $b \frown b \frown c$.

Hence we have seen that in all the possible cases of execution none of the principal arrives in a contradiction. Therefore the appearance function is consistent with the ALTS* and a lie will never be exposed. Next we will consider the case of inconsistency.

5 Inconsistent lie

In this section we will see an example of unsuccessful lie, leading one or more principals to inconsistent state. Consider the following $Pai*$ process:

$$\begin{array}{llll} Q = a; b; c + b; b; a + b; a; c. & & & \\ \rho : & a \times 1 \rightarrow a & b \times 1 \rightarrow b & c \times 1 \rightarrow c \\ & a \times 2 \rightarrow b & b \times 2 \rightarrow b & c \times 2 \rightarrow c \end{array}$$

This particular example shows inconsistent lies with respect to ALTS* shown in Figure 6. No matter which trace is executed one of the principals will be in an inconsistent state.

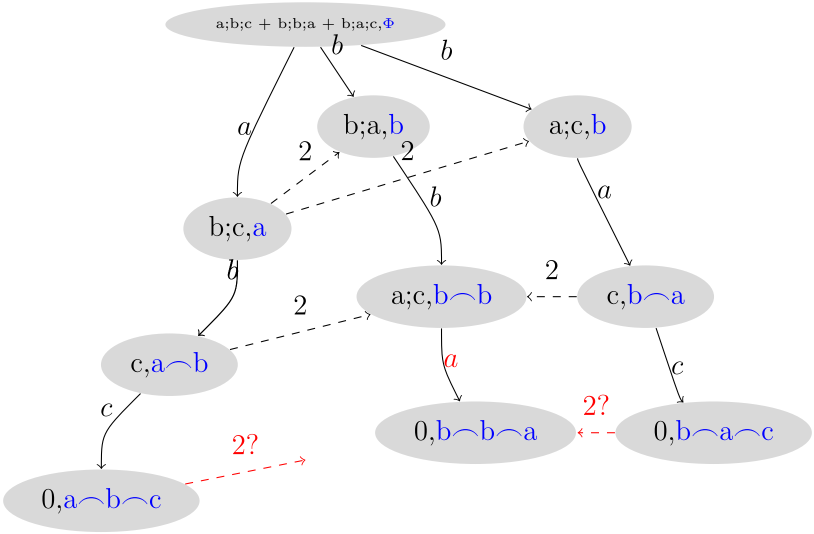

Figure 6: Inconsistent lie.

We will consider all cases of trace execution. Let the trace that is executed is $a \frown b \frown c$. After the execution of a principal 1 will be in the state led by action a. However, action a appears to principal 2 as b. Therefore he will be in either of the states led by the two b transition as shown by dashed arrow in Figure 6. Now action b executes. Principal 1 will be in the state with trace $a \frown b$, where as principal 2 will be in the state with trace $b \frown b$. The deviation of perception of principal 2 is shown by a dashed arrow. Finally action c executes. Principal 1 will be in the state with action sequence $a \frown b \frown c$ but principal 2 will be in an inconsistent state as there is no outgoing edge labeled with c from the state labeled with trace $b \frown b$.

Now let $b \frown b \frown a$ has executed. After the execution of first b action both principals will be in either of the two states led by b. Again when action b executes for the second time, both the principals will be in the state following trace $b \frown b$. Finally when action a executes, principal 1 will be in the state with trace $b \frown b \frown a$ while principal 2 will be in an inconsistent state. The action a appears as b to principal 2 according to appearance function. However there is no transition labeled with b from that state.

Finally consider the trace $b \frown a \frown c$. After the execution of first b action both principals will be in either of the two states led by b. Now action a executes. After its execution principal 1 will be in the state with trace $b \frown a$. However action a appears to principal 2 as b, so it will be in the state with trace $b \frown b$. Finally action c executes which leads principal 1 to the state with trace $b \frown a \frown c$ but principal 2 will be in an inconsistent state from where there is no outgoing transition labeled by action c.

So, we have seen that in this particular example the appearance function is not consistent with the ALTS* which results in inconsistency. Every trace execution leads to inconsistency for principal 2. There can be cases in which we have inconsistency over some trace but the other traces are consistent and different principals will have different views of consistency with respect to a particular system and appearance function.

6 Conclusion

In this paper, we presented a framework to model lie in a system. We belief that this framework can be particularly useful in protocols where trust and confidentiality is an issue. The proposed framework has two faces. The first face corresponds to lying, i.e., for a given system, how a participating principal can make the choice of appearance function in such a way that all principals have a consistent view of system. This face of the framework can be very useful while sending secure data through an insecure network. The other face corresponds to detection of lies when a principal has reached in an inconsistent state during the execution of protocol. The open question in this face is, can a principal determine the correct trace with the given knowledge of protocol and the traces that can execute as part of the protocol, when it reaches an inconsistent state. Moreover, can he determine the principal responsible of it and the appearance function used. These question can be answered, once we have developed a complete language in μ calculus with belief construct.

The $Pai*$ and $ALTS*$ introduced in this paper are more expressive and flexible than the traditional Process Algebras and *labeled transistion system*, in the sense that whatever was possible in later, is still possible and has the same meaning in the former.

Future work The appearance function introduced in this paper explicitly maps the appearance of an action to every participating principal. However in many protocols some actions have public appearance, i.e., those actions can only be visible to certain principals while other principals know that some action has been executed, but does not know exactly what action. This give rise to indistinguishability relation between operational states with respect to later category of principals. We have to introduce this relationship within our existing framework to make it more flexible and practical. Furthermore, we aim to develop an epistemic μ calculus with $belief$ construct capturing the various verification properties of the system.

References

[AILS07] Luca Aceto, Anna Ingolfsdottir, Kim Larsen, and Jiri Srba. *Reactive Syatems*. Cambridge University Press, Cambridge,U.K., 2007.

[BEK05] Johan Van Benthem, Jan Van Eijck, and Barteld Kooi. Logics of communication and change. In *Information and Computation*, pages 1620–1662, 2005.

[BMS99] Alexandru Baltag, Lawrence S. Moss, and Slawomir Solecki. The logic of public announcements, common knowledge, and private suspicions. Technical report, 1999.

[CGP99] Edmund Clarke, Orna Grumberg, and Doron Peled. *Model Checking.* MIT Press, 1999.

[DESW10] Hans Van Ditmarsch, Jan Van Eijck, Floor Sietsma, and Yanjing Wang. On the logic of lying. 2010.

[DMO07] Francien Dechesne, MohammadReza Mousavi, and Simona Orzan. Operational and epistemic approaches to protocol anlaysis: Bridging the gap. In *Proceedings of the 14th International Conference on Logic for Programming Artificial Intelligence and Reasoning (LPAR'07)*, volume 4790 of *Lecture Notes in Artificial Intelligence*, pages 226–241. Springer-Verlag, 2007.

[FHMV95] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge.* MIT Press, 1995.

[GM11] Jan Friso Groote and MohammadReza Mousavi. *Modelling and Analysis of Communicating Systems.* Department of Computer Science, TU/e, Eindhoven, 2011.