Hidden States in Reaction Systems ⋆

Roberta Gori[1], Damas Gruska[2], and Paolo Milazzo[1]

[1] Dipartimento di Informatica, Università di Pisa, Italy
[2] Department of Applied Informatics, Faculty of Mathematics, Physics and Informatics, Comenius University in Bratislava, Slovak Republic

Abstract. Pushing forward a previous investigation on security of reaction systems, we introduce new state based security properties. Assume there are some states of a reaction system that are in some sense critical, and that we want to hide whether the system reaches them. We define new security properties that guarantee that an external observer who has only a partial knowledge on the objects provided by the environment cannot infer whether a secret state is reached by the system. We also propose an effective method for verifying such properties. The verification method is based on a newly defined extension of the concept of formula based predictor to set of states.

1 Introduction

Reaction systems is a *qualitative* modeling formalism introduced by Ehrenfeucht and Rozenberg to model biological systems [1, 2]. It is based on the two opposite mechanisms of *facilitation* and *inhibition*. Facilitation means that a reaction can occur only if all its reactants are present, while inhibition means that the reaction cannot occur if any of its inhibitors is present. A *reaction system* is essentially a set of rewrite rules (*reactions*) having the form (R, I, P), where R, I and P are sets of objects representing reactants, inhibitors and products, respectively. The state of a reaction system is a finite set of objects, describing the biological entities that are present in the modeled system. The presence of an object in the state means that the corresponding biological entity is present in a number of copies as high as needed. This is the *threshold supply* assumption and characterizes reaction systems.

A reaction system evolves by means of the application of its reactions.The threshold supply assumption ensures that all the applicable reactions in a step are always applied, since they do not compete for thier reactants. The application of a set of reactions results in the introduction of all of their products in the next state of the system. The behaviour of a reaction system is driven by the (set of) contextual elements which are provided by the external environment at each step. Such elements join the current state of the system and can enable or disable reactions. The computation of the next state of a reaction system is a deterministic procedure. Consequently, if the contextual elements provided to the system at each step are know, then the whole execution of the system is determined. On the other hand, if they are not known, the overall system dynamics becomes non deterministic.

⋆ Work supported by the grant VEGA 1/0778/18 and by the project "Metodologie informatiche avanzate per l'analisi di dati biomedici" (University of Pisa, PRA 2017_44).

In previous papers [3, 4] we investigated the concept of opacity in reaction systems. Assume we have a real biochemical system described by a reaction system, and an observer having a partial information about the objects provided by the environment because of the cost of obtaining such informaton. We can distinguish two types of objects: visible *low level* (L) objects, and invisible *high level* (H) objects. We studied the detectability of H-objects, namely how much information on the presence of H-objects can be obtained by just observing the presence of L-objects in context sequences. This problem, called information flow [5], was extensively studied in security by introducing the concept of *opacity* [6, 7]. We reformulated opacity for reaction systems and proposed dynamic causality relatioships (formula based predictors) as an effective method to verify opacity properties in reaction systems.

In this paper we push forward our approach by considering sets of *secret states*. Let Sec be a set of states and assume we want to hide to an external observer whether a reaction system reaches one of such states. So, Sec is a set of secret states. As before, the observer can only see L-objects in context sequences. In order to prevent the observer to infer whether the system reaches a secret state, we have to ensure that for every context sequence leading to one of such states there exists another context sequence leading to a non-secret state that is indistinguishable from the previous one from the (limited) point of view of the observer. In other words, the two context sequences must make the same use of L-objects, which are the only ones that can be observed. We will formalize this idea in terms of two security properties called Current State Opacity and n-p Window Current state Opacity, and we will provide effective methods for verifying them based on dynamic causalities.

Dynamic causalities deal with the ways entities dynamically influence each other. Brijder, Ehrenfeucht and Rozenberg initiated an investigation on *causalities* in reaction systems [8], by introducing the idea of *predictor*. Assume that one is interested in knowing whether a particular object $s \in S$ will be present after n steps of execution of the reaction system. Since the only source of non-determinism are the contextual elements received at each step, knowing which objects will be received allows the production of s after n steps to be predicted. In [9–12] the new notion of *formula based predictor* was introduced. A formula based predictor is a propositional logic formula to be satisfied by the sequence of (sets of) elements provided by the environment. *Satisfaction of the logic formula precisely discriminates the cases in which s will be produced after n steps from those in which it will not.* In the style of [13, 14], here the notion of formula-based predictor is first naturally extended to sets of objects (states), and then it is extended to sets of states. The result is a formula based predictor that can be used to precisely characterize all context sequences that lead to one secret state in a set Sec. We apply this extended predictor for secret states in Sec to prove whether the reaction system is opaque for an observer that can only see L-objects of the context sequence provided by the environment.

2 Reaction Systems

In this section we briefly introduce reaction systems [1, 2]. Given S, a finite set of symbols, called objects, a *reaction* is a triple (R, I, P) with $R, I, P \subseteq S$, composed

of *reactants* R, *inhibitors* I, and *products* P. Reactants and inhibitors are disjoint ($R \cap I = \emptyset$) otherwise the reaction would never be applicable. The set of all possible reactions over a set S is denoted by $\mathrm{rac}(S)$. Finally, a *reaction system* is a pair $\mathcal{A} = (S, A)$, with S a finite background set, and $A \subseteq \mathrm{rac}(S)$ a set of reactions.

The state of a reaction system is a set of objects. Let $a = (R_a, I_a, P_a)$ be a reaction and T be a set of objects. The result $\mathrm{res}_a(T)$ of the application of a to T is either P_a, if T separates R_a from I_a (i.e. $R_a \subseteq T$ and $I_a \cap T = \emptyset$), or the empty set $\emptyset$ otherwise. The application of multiple reactions at the same time occurs without any competition for the used reactants (threshold supply assumption). Therefore, each reaction for which no inhibitor is present in the current state is applied, and the result of application of multiple reactions is cumulative. Given a reaction system $\mathcal{A} = (S, A)$, the result of the application of A to a set $T \subseteq S$ is defined as $\mathrm{res}_{\mathcal{A}}(T) = \mathrm{res}_A(T) = \bigcup_{a \in A} \mathrm{res}_a(T)$. An important characteristic of reaction systems is the assumption about the *non-permanency* of objects: the objects carried over to the next step are only those produced by reactions. All the other objects vanish.

The dynamics of a reaction system $\mathcal{A} = (S, A)$ is driven by the *contextual* objects, namely the objects which are supplied to the system by the external environment at each step. The dynamics is defined as an *interactive process* $\pi = (\gamma, \delta)$, with γ and δ being finite sequences of sets of objects called the *context sequence* and the *result sequence*, respectively. The sequences are of the form $\gamma = C_0, C_1, \ldots, C_n$ and $\delta = D_0, D_1, \ldots, D_n$ for some $n \geq 1$, with $C_i, D_i \subseteq S$, and $D_0 = \emptyset$. Each set D_i, for $i \geq 1$, in the result sequence is obtained from the application of reactions A to a state composed of both the results of the previous step D_{i-1} and the objects C_{i-1} from the context; formally $D_i = res_{\mathcal{A}}(C_{i-1} \cup D_{i-1})$ for all $1 \leq i \leq n$. Finally, the *state sequence* of π is the sequence $W_0, W_1, \ldots, W_n$, where $W_i = C_i \cup D_i$ for all $1 \leq i \leq n$. In the following we call $\gamma = C_0, C_1, \ldots, C_n$ a n-step context sequence.

3 Preliminaries on Predicate Logic

The aim of formula based predictors is to characterize all context sequences that lead to the production of a specific object in a given number of steps. In order to describe conditions on the presence or absence of objects in context sequences, we use objects of reaction systems as propositional symbols. Formally, we define the set F_S of propositional formulas on S in the standard way: $S \cup \{true, false\} \subseteq F_S$ and $\neg f_1, f_1 \vee f_2, f_1 \wedge f_2 \in F_S$ if $f_1, f_2 \in F_S$. Propositional formulas F_S are interpreted with respect to subsets of S. Intuitively, a subset $C \subseteq S$ is used to describe the objects that are present in (an element of) a context sequence, and this implies the truth of the corresponding propositional symbol. The formal definition of the satisfaction relation is as follows.

Definition 1. *Let $C \subseteq S$ for a set of objects S. Given a propositional formula $f \in F_S$, the satisfaction relation $C \models f$ is inductively defined as follows:*

$C \models s$ *iff* $s \in C$, $\quad C \models true$,
$C \models \neg f'$ *iff* $C \not\models f'$, $\quad C \models f_1 \vee f_2$ *iff either* $C \models f_1$ *or* $C \models f_2$,
$C \models f_1 \wedge f_2$ *iff* $C \models f_1$ *and* $C \models f_2$.

In the following $\equiv_l$ stands for the logical equivalence on propositional formulas F_S. Moreover, given a formula $f \in F_S$ we use $atom(f)$ to denote the set of propositional symbols that appear in f. The simplified version of a formula is obtained by applying the standard formula simplification procedure of propositional logic converting a formula to Disjunctive Normal Form, $\mathcal{DNF}(f)$. We recall that for any formula $f \in F_S$ the simplified formula $\mathcal{DNF}(f)$ is equivalent to f, it is minimal with respect to the number of propositional symbols and unique up to commutativity and associativity. Thus, we have $f \equiv_l \mathcal{DNF}(f)$ and $atom(\mathcal{DNF}(f)) \subseteq atom(f)$ and there exists no formula f' such that $f' \equiv_l f$ and $atom(f') \subset atom(\mathcal{DNF}(f))$.

The causes of an object in a reaction system are defined by a propositional formula on the set of objects S. First of all we define the *applicability predicate* of a reaction a as a formula describing the requirements for applicability of a, namely that all reactants have to be present and inhibitors have to be absent. This is represented by the conjunction of all atomic formulas representing reactants and the negations of all atomic formulas representing inhibitors of the considered reaction.

Definition 2. *Let $a = (R, I, P)$ be a reaction with $R, I, P \subseteq S$ for a set of objects S. The* applicability predicate *of a, denoted by $ap(a)$, is defined as follows: $ap(a) = \left(\bigwedge_{s_r \in R} s_r\right) \wedge \left(\bigwedge_{s_i \in I} \neg s_i\right)$.*

The *causal predicate* of a given object s is a propositional formula on S representing the conditions for the production of s in one step, namely that at least one reaction having s as a product has to be applicable.

Definition 3. *Let $gA = (S, A)$ be a r.s. and $s \in S$. The* causal predicate *of s in $\mathcal{A}$, denoted by $cause(s, \mathcal{A})$ (or $cause(s)$, when $\mathcal{A}$ is clear from the context), is defined as follows*[3]*: $cause(s, \mathcal{A}) = \bigvee_{\{(R,I,P) \in A | s \in P\}} ap\left((R, I, P)\right)$.*

We introduce a simple reaction system as running example.

Example 1. Let $\mathcal{A}_1 = (\{A, \ldots, G\}, \{a_1, a_2, a_3\})$ be a reaction system with

$$a_1 = (\{A\}, \{\}, \{B\}) \qquad a_2 = (\{C, D\}, \{\}, \{E, F\}) \qquad a_3 = (\{G\}, \{B\}, \{E\}) \ .$$

The *applicability predicates* of the reactions are $ap(a_1) = A$, $ap(a_2) = C \wedge D$ and $ap(a_3) = G \wedge \neg B$. Thus, the *causal predicates* of the objects are

$$cause(A) = cause(C) = cause(D) = cause(G) = false,$$
$$cause(B) = A,\ cause(F) = C \wedge D,\ cause(E) = (G \wedge \neg B) \vee (C \wedge D).$$

Note that $cause(A) = false$ given that A cannot be produced by any reaction. An analogous reasoning holds for objects C, D and G.

4 Formula Based Predictors

In the first part of this section we introduce the notion of *formula based predictor* as it was originally presented in [9]. Then, we extend the notion of predictors to

[3] We assume that $cause(s) = false$ if there is no $(R, I, P) \in A$ such that $s \in P$.

states (see Corollary 1) and to sets of states (see Corollary 2) in order to address causal dependences of the secret states set Sec that we want to hide.

A formula based predictor for an object s at step $n+1$ is a propositional formula satisfied exactly by the context sequences leading to the production of s at step $n+1$. Minimal formula based predictors can be calculated in an effective way.

Given a set of objects S, we consider a corresponding set of *labelled objects* $S \times \mathbb{N}$. For the sake of legibility, we denote $(s,i) \in S \times \mathbb{N}$ simply as s_i and we introduce $S^n = \bigcup_{i=0}^{n} S_i$ where $S_i = \{s_i \mid s \in S\}$. Propositional formulas on labelled objects S^n describe properties of n-step context sequences. The set of propositional formulas on S^n, denoted by F_{S^n}, is defined analogously to the set F_S (presented in Sect. 3) by replacing S with S^n. Similarly, the set F_{S_i} can be defined by replacing S with S_i. Given a formula $f \in F_S$, a corresponding formula $\mathit{labelled}(f,i) \in F_{S_i}$ can be obtained by replacing each $s \in S$ in f with $s_i \in S_i$.

A labelled object s_i represents the presence (or the absence, if negated) of object s in the i-th element C_i of the n-step context sequence $\gamma = C_0, C_1, \ldots C_n$. This interpretation leads to the following definition of satisfaction relation for propositional formulas on context sequences.

Definition 4. *Let $\gamma = C_0, C_1, \ldots C_n$ be a n-step context sequence and $f \in F_{S^n}$ a propositional formula. The satisfaction relation $\gamma \models f$ is defined as*

$$\{s_i \mid s \in C_i, 0 \leq i \leq n\} \models f\,.$$

As an example, let us consider the context sequence $\gamma = C_0, C_1$ where $C_0 = \{A, C\}$ and $C_1 = \{B\}$. We have that γ satisfies the formula $A_0 \wedge B_1$ (i.e. $\gamma \models A_0 \wedge B_1$) while γ does not satisfy the formula $A_0 \wedge (\neg B_1 \vee C_1)$ (i.e. $\gamma \not\models A_0 \wedge (\neg B_1 \vee C_1)$).

The latter notion of satisfaction allows us to define formula based predictor.

Definition 5 (Formula based Predictor). *Let $\mathcal{A} = (S, A)$ be a reaction system, $s \in S$ and $f \in F_{S^n}$ a propositional formula. We say that f* f-predicts s in $n+1$ steps *if for any n-step context sequence $\gamma = C_0, \ldots, C_n$*

$$\gamma \models f \Leftrightarrow s \in D_{n+1}$$

where $\delta = D_0, \ldots, D_n$ is the result sequence corresponding to γ and $D_{n+1} = res_{\mathcal{A}}(C_n \cup D_n)$.

Note that if formula f f-predicts s in $n+1$ steps and if $f' \equiv_l f$ then also f' f-predicts s in $n+1$. More specifically, we are interested in the formulas that f-predict s in $n+1$ and contain the minimal numbers of propositional symbols, so that their satisfiability can easily be verified. This is formalised by the following approximation order on F_{S^n}.

Definition 6 (Approximation Order). *Given $f_1, f_2 \in F_{S^n}$ we say that $f_1 \sqsubseteq_f f_2$ if and only if $f_1 \equiv_l f_2$ and $atom(f_1) \subseteq atom(f_2)$.*

In [9] it is shown that there exists a *unique equivalence class* of formula based predictors for s in $n+1$ steps that is minimal with respect to the order $\sqsubseteq_f$.

We now define an operator `fbp` that allows formula based predictors to be effectively computed.

Definition 7. *Let $\mathcal{A} = (S, A)$ be a r.s. and $s \in S$. We define a function* $\mathtt{fbp} : S \times \mathbb{N} \to F_{S^n}$ *as follows:* $\mathtt{fbp}(s, n) = \mathtt{fbs}(cause(s), n)$*, where the auxiliary function* $\mathtt{fbs} : F_S \times \mathbb{N} \to F_{S^n}$ *is recursively defined as follows:*

$$\begin{array}{ll}
\mathtt{fbs}(s, 0) = s_0 & \mathtt{fbs}(s, i) = s_i \vee \mathtt{fbs}(cause(s), i-1) \quad \text{if } i > 0 \\
\mathtt{fbs}((f'), i) = (\mathtt{fbs}(f', i)) & \mathtt{fbs}(f_1 \vee f_2, i) = \mathtt{fbs}(f_1, i) \vee \mathtt{fbs}(f_2, i) \\
\mathtt{fbs}(\neg f', i) = \neg \mathtt{fbs}(f', i) & \mathtt{fbs}(f_1 \wedge f_2, i) = \mathtt{fbs}(f_1, i) \wedge \mathtt{fbs}(f_2, i) \\
\mathtt{fbs}(true, i) = true & \mathtt{fbs}(false, i) = false
\end{array}$$

The function fbp gives a formula based predictor that, in general, may not be minimal with respect to the approximation order $\sqsubseteq_f$. Therefore, the calculation of a minimal formula based predictor requires the application of the standard simplification procedure that simplifies the obtained logic formula and puts it in disjunctive normal form, here called simply $\mathcal{DNF}(.)$.

Theorem 1. *Let $\mathcal{A} = (S, A)$ be a r.s.. For any object $s \in S$,*

- $\mathtt{fbp}(s, n)$ f-predicts s *in* $n + 1$ *steps;*
- $\mathcal{DNF}(\mathtt{fbp}(s, n))$ f-predicts s *in* $n + 1$ *steps and is* minimal *w.r.t.* $\sqsubseteq_f$.

Example 2. Let us consider again the reaction system $\mathcal{A}_1$ of Ex. 1. We are interested in the production of E after 4 steps. Hence, we calculate the logic formula that *f-predicts E in 4 steps* applying the function fbp:

$$\begin{array}{rl}
\mathtt{fbp}(E, 3) = & \mathtt{fbs}\big((G \wedge \neg B) \vee (C \wedge D), 3\big) \\
= & \big(\mathtt{fbs}(G, 3) \wedge \neg \mathtt{fbs}(B, 3)\big) \vee \big(\mathtt{fbs}(C, 3) \wedge \mathtt{fbs}(D, 3)\big) \\
= & \big((G_3) \wedge \neg(B_3 \vee \mathtt{fbs}(A, 2))\big) \vee (C_3 \wedge D_3) \\
= & \big(G_3 \wedge \neg B_3 \wedge \neg A_2\big) \vee (C_3 \wedge D_3)\big)
\end{array}$$

A context sequence satisfies $\mathtt{fbp}(E, 3)$ iff the execution of the reaction system leads to the production of object E after 4 steps. Furthermore, in this case the obtained formula is also minimal w.r.t. $\sqsubseteq_f$. This is because $\mathcal{DNF}(\mathtt{fbp}(E, 3)) = \mathtt{fbp}(E, 3)$. Indeed, the formula $\mathtt{fbp}(E, 3)$ cannot be further simplified and any literal cannot be canceled without obtaining a non equivalent formula.

The result of Theorem 1 can be easily extended to states. Indeed, we can characterize all the context sequences that lead to the production of the set of objects of the state. To this aim, we need to consider the context sequences that satisfy *all conditions for the production of each single object* of the set. Assume *sec* to be a state, that is, a set of objects in S then we can characterize all the context sequence leading to states in the following way.

Corollary 1. *Let $\mathcal{A} = (S, A)$ be a r.s.. Consider sec a set of objects in S,*

- $\bigwedge_{s \in sec} \mathtt{fbp}(s, n)$ f-predicts *sec in* $n + 1$ *steps;*
- $\mathcal{DNF}\left(\bigwedge_{s \in sec} \mathtt{fbp}(s, n)\right)$ f-predicts s *in* $n + 1$ *steps and is* minimal *w.r.t.* $\sqsubseteq_f$.

Moreover, the previous results can be extended to finite sets of states. Assume Sec to be a set of states $\{sec_1, sec_2, ..., sec_m\}$, for some m. We need to characterize all the context sequences that lead to some state in Sec.

Corollary 2. *Let $\mathcal{A} = (S, A)$ be a r.s.. Let Sec be a set of states $\{sec_1, sec_2, ..., sec_m\}$, for some m,*

- $\bigvee_{sec_i \in Sec} \left(\bigwedge_{s \in sec_i} \texttt{fbp}(s, n)\right)$ f-predicts *the set Sec in $n+1$ steps;*
- $\mathcal{DNF}\left(\bigvee_{sec_i \in Sec} \left(\bigwedge_{s \in sec_i} \texttt{fbp}(s, n)\right)\right)$ f-predicts *Sec in $n+1$ steps and is* minimal *w.r.t.* $\sqsubseteq_f$.

Example 3. Let us consider again the reaction system $\mathcal{A}_1$ of Examples 1 and 2. Assume we are interested in reaching the state $\{E, F\}$ after 4 steps. In Example 2 we calculated the logic formula that *f-predicts E in 4 steps* applying the function `fbp`. This resulted in the formula $\big(G_3 \wedge \neg B_3 \wedge \neg A_2\big) \vee (C_3 \wedge D_3)\big)$. Analogously, we can calculate the logic formula that *f-predicts F in 4 steps* applying the function `fbp`. This resulted in the formula $(C_3 \wedge D_3)$. Now, in order to obtain the minimal formula characterising the context sequences that lead to the state where both E and F are present, according to Corollary 1, we need to compute

$$\mathcal{DNF}(\texttt{fbp}(E, 4) \wedge \texttt{fbp}(F, 4)) =$$
$$\mathcal{DNF}\Big(\big((G_3 \wedge \neg B_3 \wedge \neg A_2) \vee (C_3 \wedge D_3)\big) \wedge (C_3 \wedge D_3)\Big) = C_3 \wedge D_3.$$

A context sequence satisfies $C_3 \wedge D_3$ iff the execution of the reaction system leads to the production of both object E and F after 4 steps.

Assume now we are interested in characterising the context sequences that either lead to state $\{E, F\}$ or to state $\{B\}$ after 4 steps. Hence, in this case $Sec = \{\{E, F\}, \{B\}\}$.

According to Corollary 2 the minimal formula can be obtained by computing

$$\mathcal{DNF}\left((\texttt{fbp}(E, 4) \wedge \texttt{fbp}(F, 4)) \vee \texttt{fbp}(B, 4)\right) =$$
$$\mathcal{DNF}((C_3 \wedge D_3) \vee A_3) = (C_3 \wedge D_3) \vee A_3.$$

Note that any sequence satisfying the formula $(C_3 \wedge D_3) \vee A_3$ leads to a state in *Sec*. Moreover, such sequences are the only ones that can lead to the production of a state in *Sec*.

5 Information flow

As in [3, 4], we now consider a reaction system $\mathcal{A} = (\mathcal{S}, \mathcal{A})$ where we assume an external observer can only detect or see some kinds of objects in the context sequence. To formally describe this situation, borrowing techniques developed for reasoning about flow based security (see [5]), we divide objects from S into two groups, namely public (low level) objects L and private (high level) objects H. It is assumed that $L \cup H = S$ and $L \cap H = \emptyset$. We assume that an observer can see only L-objects, i.e. objects from L. Moreover, we introduce an equivalence on sets of objects and on contexts sequences. Two sets of objects A, B are equivalent with respect to the set M if they contain the same objects apart from those in M. Formally, $A \equiv_M B$ iff $A \setminus M = B \setminus M$. This can be applied to reaction system contexts: we write $\gamma_1 \equiv_M \gamma_2$ if $\gamma_1 = C_0^1, ...C_n^1, ...$ and $\gamma_2 = C_0^2, ...C_n^2, ...$ and $\forall i, C_i^1 \equiv_M C_i^2$. To formalize information flow between L-objects and H-objects we exploit a concept known as *current state opacity* (see [15] for an overview paper).

5.1 Current State Opacity

Let us assume a set of states Sec with $Sec \subset 2^S$. We assume an external observer of the system who can detect or see only L objects in the context sequence, but who wants to discover whether the current state W_i is a secret state belonging to Sec. In this context a reaction system is i-current state opaque if whenever there exists a context sequence leading to a secret state of Sec, there exists an equivalent (with respect to the L object) context sequence that does not lead to a secret state in Sec. This will assure us that just observing the context sequence an external observer cannot decide whether the system will go to a secret state.

Definition 8. *(i-Step Current State Opacity) The reaction system $\mathcal{A} = (S, A)$ is i-current state opaque with respect to L and Sec iff whenever there exists an i-step context sequence γ leading to a secret state in Sec, that is, $D_{i+1} \in Sec$, there also exists an i-step context sequence γ' not leading to a state in Sec, that is, $D'_{i+1} \notin Sec$, such that $\gamma \equiv_L \gamma'$.*

Note that differently from our previous work [3, 4], here the attacker observes properties of context sequences to detect properties of the system states.

Since formula based predictors express all causal dependences of an object from all the objects of the context sequences, we can use this concept to verify if a reaction system is i-step current state opaque.

Theorem 2. *A r.s. $\mathcal{A}$ is i-current state opaque with respect to L and Sec iff*

$$\mathcal{DNF}\Big(\bigvee_{sec \in Sec}\big(\bigwedge_{s \in sec} \mathtt{fbp}(s,i)\big)\Big) = c_1 \vee c_2 \vee ... \vee c_n \text{ and}$$
$$\forall m \in \{1,...,n\}, \{A \mid A_j \in atom(c_m), \text{ with } 0 \leq j < i\} \cap (S \setminus L) \neq \emptyset.$$

Proof. We start by proving the right hand implication. Assume by contradiction that the reaction system $\mathcal{A}$ is i-current state opaque with respect to L and Sec but that there exists a c_m such that $\{A \mid A_j \in atom(c_m), \text{ with } 0 \leq j < i\} \cap (S \setminus L) = \emptyset$. Choose a minimal context sequence γ such that $\gamma \models c_m$. γ has to be minimal in the sense that it just provides the positive literals in the conjunction c_m. Note that by hypothesis, γ provides only low level L-objects. Note that $\gamma \models c_m$ implies that $\gamma \models c_1 \vee c_2 \vee ... \vee c_n = \mathcal{DNF}\Big(\bigvee_{sec \in Sec}\big(\bigwedge_{s \in sec} \mathtt{fbp}(s,i)\big)\Big)$. By applying Corollary 2 we have that the context sequence γ leads to the production of one state in Sec after i steps. However, since γ contains just low level objects L, any context sequence γ' such that $\gamma' \equiv_L \gamma$ will satisfy c_m, since c_m contains only L-objects. Then, by Corollary 2 any γ' will lead to the production of a state in Sec after i steps. Therefore $\mathcal{A}$ is not i-current state opaque. This gives a contradiction.

For proving the left hand implication, assume, by contradiction that every c_i contain at least an H object but that the reaction system $\mathcal{A}$ is not i-current state opaque with respect to a set of low level objects L and Sec. This implies that there do not exist two context sequence γ and γ' with $\gamma \equiv_L \gamma'$ such that one lead to a secret state in Sec and the other does not.

Choose a γ leading to the production of a state in Sec such that it satisfy only one particular conjunction $c_{\bar{i}}$ in the disjunction $c_1 \vee c_2 \vee ... \vee c_n$. By Corollary 2 such

γ exists and we can choose γ as the minimal context sequence satisfying a $c_{\bar{i}}$. Since by hypothesis $c_{\bar{i}}$ is a conjunction containing at least one object in $S \setminus L$ consider γ' as the context sequence satisfying the conjunction of low level objects in $c_{\bar{i}}$ but that does not satisfy the $S \setminus L$ literals in $c_{\bar{i}}$. Now, by construction $\gamma \equiv_L \gamma'$. However, $\gamma' \not\models c_{\bar{i}}$. Moreover, since we have chosen γ to be the minimal context sequence satisfying just $c_{\bar{i}}$ and $c_{\bar{i}} \in c_1 \vee c_2 \vee ... \vee c_n$ then it is simplified, we can be sure that $\gamma' \not\models c_1 \vee c_2 \vee ... \vee c_n$. Then, by Corollary 2, we have that the context sequence γ' does not lead to the production of a state in Sec. Hence, we found γ and γ' such that $\gamma \equiv_L \gamma'$ and context sequence γ leads to a secret state in Sec while context sequence γ' does not. This gives a contradiction. □

This gives us an easy method to verify if a reaction system is i-current state opaque with respect to a set of low level objects L and a secret set of states Sec. While computing $c_1 \vee c_2 \vee ... \vee c_n$ gives us a way to represent all different context sequences that lead to the production of a secret state in Sec (see Corollary 2), the condition that each conjunction in $c_1 \vee c_2 \vee ... \vee c_n$ has to contain at least one non low level object, gives us a way to automatically construct an L-equivalent context sequence that does not lead to a state in Sec. We will illustrate this construction in the next example. As a consequence of Theorem 2, we can state the following proposition.

Proposition 1. *The property of a reaction system $\mathcal{A}$ to be i-current state opaque with respect to a set of low level objects L and a secret set of states Sec is decidable.*

Example 4. Let $\mathcal{A}_2 = (\{A, \ldots, F\}, \{a_1, a_2, a_3, a_4\})$ be a reaction system with

$$a_1 = (\{A\}, \{B\}, \{C\}) \qquad a_2 = (\{A\}, \{D\}, \{C\})$$
$$a_3 = (\{D\}, \{\}, \{B\}) \qquad a_4 = (\{F\}, \{\}, \{E\})$$

and consider $L = \{A, B, E, F\}, Sec = \{\{C, E\}\}$. Note that $\mathcal{A}_2$ is 3-current state opaque even if E is caused just by a low level object F. Roughly speaking, $\mathcal{A}_2$ is i-current state opaque for each $i \geq 2$ because in that case C is always caused by an H level object. This can formally be proved by considering $\mathcal{DNF}(\texttt{fbp}(C,3) \wedge \texttt{fbp}(E,3))$

$$\begin{aligned}
\mathcal{DNF}(\texttt{fbp}(C,3) \wedge \texttt{fbp}(E,3)) &= \mathcal{DNF}\big(\texttt{fbs}\big((A \wedge \neg B) \vee (A \wedge \neg D), 3\big) \wedge \texttt{fbs}(F,3)\big) \\
&= \mathcal{DNF}\big(((\texttt{fbs}(A,3) \wedge \neg \texttt{fbs}(B,3)) \\
&\qquad \vee (\texttt{fbs}(A,3) \wedge \neg \texttt{fbs}(D,3))) \wedge \texttt{fbs}(F,3)\big) \\
&= \mathcal{DNF}\big(((A_3 \wedge \neg B_3 \wedge D_2) \vee (A_3 \wedge \neg D_3)) \wedge F_3\big) \\
&= (A_3 \wedge \neg B_3 \wedge D_2 \wedge F_3) \vee (A_3 \wedge \neg D_3 \wedge F_3)
\end{aligned}$$

Since both conjunctions $A_3 \wedge \neg B_3 \wedge D_2 \wedge F_3$ and $A_3 \wedge \neg D_3 \wedge F_3$ contain at least a high level object D then by Theorem 2 we are sure that $\mathcal{A}_2$ is 3-current state opaque.

It is worth noting that using the formula based predictor for each γ leading to the production of a secret state in Sec we can actually construct γ' with $\gamma \equiv_L \gamma'$ such that γ' does not lead to a secret state in Sec. Indeed, let $\gamma = C_1, C_2, C_3$ where C_2 and C_3 are such that $D \in C_2$, $F, A \in C_3$ and $B \notin C_3$. Consider then $\gamma' = C_1, C_2 \setminus \{D\}, C_3$, by Corollary 2, we have that γ lead to a state in Sec while γ' does not lead to the state in Sec.

The following example shows that the conditions for a system to be i-current state opaque cannot be checked on isolation. Let $\mathcal{A}_3 = (\{A, \ldots, D\}, \{a_1, a_2\})$ be the following reaction system with rules

$$a_1 = (\{A\}, \{D\}, \{B\}) \qquad a_2 = (\{A, D\}, \{\}, \{C\})$$

and consider $L = \{A, B, C\}, Sec = \{\{C\}\{B\}\}$. Note that both rules depend on one H-object D. However, the system is not i-current state opaque for any $i \geq 1$. Let us verify if a system is 3-current state opaque,

$$\begin{aligned}\mathcal{DNF}(\mathtt{fbp}(B,3) \vee \mathtt{fbp}(C,3)) &= \mathcal{DNF}\big(\mathtt{fbs}\big((A \wedge \neg D), 3\big) \vee \mathtt{fbs}\big((A \wedge D), 3\big)\big) \\ &= \mathcal{DNF}\big((\mathtt{fbs}(A,3) \wedge \neg \mathtt{fbs}(D,3) \\ &\qquad \vee (\mathtt{fbs}(A,3) \wedge \mathtt{fbs}(D,3))\big) \\ &= \mathcal{DNF}\big((A_3 \wedge \neg D_3) \vee (A_3 \wedge D_3)\big) = A_3\end{aligned}$$

In this case, the conjunction A_3 does not satisfy the claim of Theorem 2 since it does not have at least one hight level H-object. Indeed, consider any context sequence $\gamma = C_1, C_2, C_3$ where $A \in C_3$. Note that any context sequence $\gamma' \equiv_L \gamma$ will provide A at the third step. Then, by Corollary 2, any $\gamma' \equiv_L \gamma$ will lead to the state in Sec. Hence, $\mathcal{A}_3$ is not 3-state opaque.

5.2 *n-p* Window State Opacity

We now introduce a stronger notion of opacity. Assume now that an observer can observe all objects in the context sequence except for a "blurry window" on which it can observe just L-objects. Once again he wants to discover whether the state at some given step belongs to the set of secret states Sec.

We first define the concept of observational window of a context sequence. Let $\gamma = C_0, ...C_n, ..., C_p, ..., C_i$, by $\gamma_{n,p}$, for $0 \leq n \leq p$ we denote the subsequence $C_n, ..., C_p$.

Definition 9. *(n-p Window i-State Opacity) Let n and p such that $0 \leq n \leq p \leq i$.*

Reaction system $\mathcal{A} = (S, A)$ is n-p window i-state opaque with respect to L and Sec, iff whenever there exists a γ such that D_{i+1} belongs to Sec, i.e. $D_{i+1} \in Sec$, there exists γ' such that state D'_{i+1} does not belong to Sec i.e. $D_{i'+1} \notin Sec$ and $\gamma_{0,n-1} \equiv_S \gamma'_{0,n-1}$, $\gamma_{n,p} \equiv_L \gamma'_{n,p}$ and $\gamma_{p+1,i} \equiv_S \gamma'_{p+1,i}$.

Once again, formula based predictors can be used to verify if a reaction system is n-p window i-state opaque.

Theorem 3. *A reaction system $\mathcal{A}$ is n-p window i-state opaque with respect to L and Sec iff for every*

$$\begin{aligned}&\mathcal{DNF}\Big(\textstyle\bigvee_{sec \in Sec}\big(\bigwedge_{s \in sec} \mathtt{fbp}(s,i)\big)\Big) = c_1 \vee c_2 \vee ... \vee c_n \text{ and} \\ &\forall m \in \{1, ..., n\}, \{A \mid A_j \in atom(c_m), \text{ with } n \leq j \leq p\} \cap (S \setminus L) \neq \emptyset.\end{aligned}$$

As before, to verify if a reaction system is n-p window i-state opaque with respect to a set of low level objects L and a secret set of states Sec, we can check $c_1 \vee c_2 \vee ... \vee c_n$.

Proof. The proof is similar to the proof of Theorem 2, therefore it is only sketched.

For the right hand implication assume by contradiction that the reaction system $\mathcal{A}$ is n-p window i-state opaque with respect to L and Sec but the second part of the claim is false for at lest one c_m. Choose a minimal (in the sense of the proof of Theorem 2) context sequence γ such that $\gamma \models c_m$. By hypothesis, γ does not provide $S \setminus L$ objects at any step included between n and p. Note that any context sequence γ' such that $\gamma_{0,n-1} \equiv_S \gamma'_{0,n-1}$, $\gamma_{n,p} \equiv_L \gamma'_{n,p}$ and $\gamma_{p+1,i} \equiv_S \gamma'_{p+1,i}$ will satisfy c_m. Then, by Corollary 2 any γ' will lead to the production of a state in Sec after i steps. This gives a contradiction.

For proving the left hand implication, assume, by contradiction that every c_i contain at least one $S \setminus L$ object at some step included between n and p but $\mathcal{A}$ is not n-p window i-state opaque. This means that there do not exist two context sequence γ and γ' with $\gamma_{0,n-1} \equiv_S \gamma'_{0,n-1}$, $\gamma_{n,p} \equiv_L \gamma'_{n,p}$ and $\gamma_{p+1,i} \equiv_S \gamma'_{p+1,i}$ such that one lead to a secret state in Sec and the other does not.

Choose a $\gamma = C_0, ..., C_i$ leading to the production of a state in Sec such that it satisfies only one particular conjunction $c_{\bar{i}}$ in the disjunction $c_1 \vee c_2 \vee ... \vee c_n$. By Corollary 2 such γ exists. Consider $\gamma' = C_0, ..., C_{n-1}, C'_n, ..., C'_p, C_{p+1}, ..., C_i$ as the context sequence such that $C'_n, ..., C'_p$, satisfy the conjunction of low level objects only included between n and p of $c_{\bar{i}}$ but that does not satisfy the $S \setminus L$ literals of $c_{\bar{i}}$. Now, by construction $\gamma_{0,n-1} \equiv_S \gamma'_{0,n-1}$, $\gamma_{n,p} \equiv_L \gamma'_{n,p}$ and $\gamma_{p+1,i} \equiv_S \gamma'_{p+1,i}$. However, $\gamma' \not\models c_{\bar{i}}$. Following the reasoning of proof of Theorem 2, we can conclude that we have found γ and γ' such that one leads to a secret state in Sec while the other does not. This gives a contradiction. □

Therefore we can state the following.

Proposition 2. *The property of a reaction system $\mathcal{A}$ to be n-p window i-state opaque with respect to a set of low level objects L and a secret sets of state Sec is decidable.*

If a system is 0-i window i-state opaque then it is i-current state opaque.

Example 5. Consider again the reaction system $\mathcal{A}_2$, L and Sec as in Example 4. $\mathcal{A}_2$ was 3-current state opaque. However, $\mathcal{A}_2$ it is not 3-3 window i-state opaque. Recall that

$$\mathcal{DNF}(\texttt{fbp}(C,3) \wedge \texttt{fbp}(E,3)) = (A_3 \wedge \neg B_3 \wedge D_2 \wedge F_3) \vee (A_3 \wedge \neg D_3 \wedge F_3).$$

Then, $\{A \mid A_j \in atom((A_3 \wedge \neg B_3 \wedge D_2 \wedge F_3)),$ with $3 \leq j \leq 3\} \cap (S \setminus L) = \emptyset$ and Theorem 3 is not satisfied. Consider, for example, we can choose $\gamma = \{\}, \{\}, \{D\}, \{A, B, F\}$, then any γ' such that $\gamma_{0,2} \equiv_S \gamma'_{0,2}$, $\gamma_{3,3} \equiv_L \gamma'_{3,3}$ must be $\gamma' = \{\}, \{\}, \{D\}, C'_3$ with $C'_3 \supseteq \{A, B, F\}$, therefore also γ' will lead to a secret state in Sec.

Finally, note that $\mathcal{A}_2$ is n-3 window i-state opaque for any $0 \leq n \leq 2$.

6 Conclusions and further work

In this paper we have defined two state based security properties, that are, Current State Opacity and n-p Window State Opacity for reaction systems. We proposed effectively computable methods for verifying such properties based on the new notion of formula based predictor for set of secret states sets, newly defined in Section 4.

As further work we plan to elaborate other notions of opacity for reaction systems. The first one is in a sense a complement notion to n-p Window i-State Opacity. We consider an observer who can see only a small "window" of computation. If after that computation a secret state has been reached we expect that there exists seemingly the same window which leads to non-secret states. Also we plan to study the notion Initial State Opacity. In this case an observer tries to learn properties of an initial state of the computation. We believe that these concepts, borrowed by the security theory, can be also studied in the context of reaction systems. Moreover, it would be interesting to study variants of reaction systems with a limited threshold assumption and with timed properties (for a process algebra example, see [16]).

References

1. A. Ehrenfeucht, G. Rozenberg, Reaction Systems, Fundam. Inform. 75 (1-4) (2007) 263–280.
2. R. Brijder, A. Ehrenfeucht, M. G. Main, G. Rozenberg, A Tour of reaction Systems, Int. J. Found. Comput. Sci. 22 (7) (2011) 1499–1517.
3. D. Gruska, R. Gori, P. Milazzo, Studying opacity of reaction systems through formula based predictors, in: Proc. of the 26th Int. Workshop on Concurrency, Specification and Programming, CS&P, 2017.
4. D. Gruska, R. Gori, P. Milazzo, Studying opacity of reaction systems through formula based predictors, Fundamenta Informaticae To appear.
5. J. A. Goguen, J. Meseguer, Security policies and security models, Proc. of IEEE Symposium on Security and Privacy.
6. J. Bryans, M. Koutny, P. Ryan, Modelling non-deducibility using petri nets, in: 2nd Workshop on Security Issues with Petri Nets and other Computational Models, 2004.
7. J. W. Bryans, M. Koutny, L. Mazaré, P. Y. Ryan, Opacity generalised to transition systems, International Journal of Information Security 7 (6) (2008) 421–435.
8. R. Brijder, A. Ehrenfeucht, G. Rozenberg, A Note on Causalities in Reaction Systems, ECEASST 30.
9. R. Barbuti, R. Gori, F. Levi, P. Milazzo, Investigating dynamic causalities in reaction systems, Theoretical Computer Science 623 (2016) 114–145.
10. R. Barbuti, R. Gori, F. Levi, P. Milazzo, Specialized predictor for reaction systems with context properties, in: Proc. of the 24th Int. Workshop on Concurrency, Specification and Programming, CS&P 2015, 2015, pp. 31–43.
11. R. Barbuti, R. Gori, F. Levi, P. Milazzo, Specialized predictor for reaction systems with context properties, Fundamenta Informaticae 147 (2-3) (2016) 173–191.
12. R. Barbuti, R. Gori, F. Levi, P. Milazzo, Generalized contexts for reaction systems: definition and study of dynamic causalities, Acta Inf. 55 (3) (2018) 227–267.
13. R. Barbuti, R. Gori, P. Milazzo, Multiset patterns and their application to dynamic causalities in membrane systems, in: Membrane Computing - 18th Int. Conference, CMC 2017, 2017, pp. 54–73.
14. R. Barbuti, R. Gori, P. Milazzo, Predictors for flat membrane systems, Theor. Comput. Sci. 736 (2018) 79–102.
15. R. Jacob, J. Lesage, J. Faure, Overview of discrete event systems opacity: Models, validation, and quantification, Annual Reviews in Control 41 (2016) 135–146.
16. M. C. Ruiz, D. Cazorla, F. Cuartero, J. J. Pardo, H. Macia, A bounded true concurrency process algebra for performance evaluation, in: FORTE Workshops 2004, 2007, pp. 143–155.