State-Based Opacity of Real-Time Automata

Kuize Zhang ✉
Control Systems Group, Technische Universität Berlin, Germany

Abstract

State-based opacity is a special type of opacity as a confidentiality property, which describes whether an external intruder cannot make for sure whether secret states of a system have been visited by observing generated outputs, given that the intruder knows complete knowledge of the system's structure but can only see generated outputs. When the time of visiting secret states is specified as the initial time, the current time, any past time, and at most K steps prior to the current time, the notions of state-based opacity can be formulated as initial-state opacity, current-state opacity, infinite-step opacity, and K-step opacity, respectively. In this paper, we formulate the four versions of opacity for real-time automata which are a widely-used model of real-time systems, and give 2-EXPTIME verification algorithms for the four notions by defining appropriate notions of observer and reverse observer for real-time automata that are computable in 2-EXPTIME.

2012 ACM Subject Classification Theory of computation → Timed and hybrid models; Security and privacy → Formal security models

Keywords and phrases real-time automaton, state-based opacity, observer, verification

Digital Object Identifier 10.4230/OASIcs.AUTOMATA.2021.12

Funding This work was partially supported by the Alexander von Humboldt Foundation.

1 Introduction

1.1 Background

Opacity is a confidentiality property that is firstly proposed in [8] to characterize information flow security, and has been widely used to describe all kinds of scenarios in security/privacy problems. It describes whether a system can forbid an external intruder from making for sure whether some secrets have been visited by using observed outputs, given that the intruder knows complete knowledge of the system's structure but can only see outputs generated by the system. In [3], a general *run-based opacity* framework is proposed for labeled transition systems (LTSs), where such a system is opaque if for every secret run, there exists a non-secret run such that the two runs have the same observation. Later on, two special types of secrets are studied: subsets of event sequences (aka traces) and subsets of states. According to the two types of secrets, opacity is classified into *language-based opacity* and *state-based opacity*. The former refers to as for every generated secret trace, there is a non-secret generated trace such that they have the same observation; the latter means whenever a run passes through a secret state at some instant, there exists another run that does not pass any secret state at the same instant such that the two runs have the same observation.

1.2 Literature review

In order to apply opacity to different scenarios, different notions of opacity in different models have been studied, e.g., four types of state-based opacity, called *initial-state opacity* (ISO) [13], *current-state opacity* (CSO) [5], *infinite-step opacity* (InfSO) [12], and *K-step opacity* (KSO) [11] for labeled finite automata (LFAs) are proved to be decidable in PSPACE with PSPACE lower bounds in [13, 5, 12] and with an NP lower bound in [11]. Unlike LFAs, ISO of labeled Petri nets is undecidable [3, 16]. Language-based opacity is more involved, because it is already undecidable in finite LTSs (i.e., LFAs) with ϵ-labeling functions [3]. In [7],

language-based opacity is shown to be decidable in EXPTIME for LFAs when secret languages and non-secret languages are regular. Moreover, in [19, 1], ISO, CSO, InfSO, KSO, and the special language-based opacity (as in [7]) in LFAs are reduced to each other all in polynomial time, so the decision problems for the five definitions of opacity are all PSPACE-complete. Other related opacity results for untimed systems can be found in [19, 20, 2, 6], etc.

In contrast to untimed systems, in real-time systems, except for an observable transition, the execution of an unobservable transition may also cost time, so the study of opacity in real-time systems is much more complicated, and there have been rare opacity results. In [4], a notion of L-opacity (the counterpart of CSO generalized to timed automata) is proved to be undecidable for a very restrictive class of timed automata called event recording automata, in which each clock is associated with an event and when an event occurs the corresponding clock is reset. Later in [18, 17], language-based opacity of *real-time automata* (RTAs, in which there is a single clock that is reset at the occurrence of each event) is proved to be decidable, where the secret languages and non-secret languages are those recognized by RTAs, hence ISO is also decidable as a special case of the considered language-based opacity. The overall verification idea is to compute the intersection of the secret language and the complement of the non-secret language for a given RTA.

1.3 Contribution of the paper

In this paper, we formulate the above mentioned four types of state-based opacity (ISO, CSO, InfSO, and KSO) for an RTA $\mathcal{A}$ (where the ISO is the same as that in [18, 17]), and show that they are all decidable in 2-EXPTIME. The verification method used in the current paper (totally different from the one used in [18, 17]) is firstly to define and compute notions of *observer* $\mathcal{A}_{\text{obs}}$ and *reverse observer* ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ in 2-EXPTIME in the size of $\mathcal{A}$, and secondly use $\mathcal{A}_{\text{obs}}$ and ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ to verify the four notions of opacity in time linear or quadratic polynomial in the sizes of $\mathcal{A}_{\text{obs}}$ and ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$. Compared with LFAs, the transitions of RTAs carry real intervals which denote that the time consumption of a transition's execution may be any real in the corresponding interval, so that RTAs can represent real-time systems. The considerable difficulty in characterizing opacity for RTAs compared with that for LFAs just comes from the intervals in RTAs. Note that the method of using observers to verify opacity is a conventional one used in LFAs, e.g., in [10], a notion of observer (actually the powerset construction used for determinizing nondeterministic finite automata with ϵ-transitions [15]) is used to verify CSO of LFAs; in [19], a notion of reverse observer is used to verify ISO of LFAs; in [20], a notion of two-way observer (combining an observer and a reverse observer) is used to verify InfSO and KSO, all in EXPTIME. The essential technical difficulty of the current paper lies in how to define suitable notions of observer and reverse observer for RTAs and how to compute them.

The remainder is structured as follows. In Section 2, we introduce necessary notation, show the exact run length problem that belongs to NP, and also introduce based knowledge in RTAs; In Section 3, we show the main results of the paper, which include four definitions of state-based opacity for RTAs, notions of observer and reverse observer and how to compute them, and necessary and sufficient conditions for the four definitions of state-based opacity. Section 4 ends up the paper with a short conclusion.

2 Preliminaries

2.1 Notation

Symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{Q}$, $\mathbb{Q}_{\geqslant 0}$, $\mathbb{R}$, and $\mathbb{R}_{\geqslant 0}$ denote the sets of nonnegative integers, integers, positive integers, rational numbers, nonnegative rational numbers, real numbers, and nonnegative real numbers, respectively. For $a, b \in \mathbb{R} \cup \{\pm\infty\}$ such that $a \leqslant b$, we use $\langle a, b\rangle$ to denote an interval, where "$\langle$" represents "[" (left-closed) or "(" (left-open), "$\rangle$" represents "]" (right-closed) or ")" (right-open). For a finite alphabet Σ, Σ^* denotes the set of *words* over Σ including the empty word ϵ. $\Sigma^+ := \Sigma^* \backslash \{\epsilon\}$. For a word $s = s_1 s_2 \dots s_n \in \Sigma^*$, $|s|$ stands for its *length* n, s^{R} denotes the *mirror image* $s_n \dots s_2 s_1$ of s. For $s \in \Sigma^+$ and $k \in \mathbb{N}$, s^k denotes the concatenation of k copies of s. For a word $s \in \Sigma^*$, a word $s' \in \Sigma^*$ is called a *prefix* of s, denoted as $s' \sqsubset s$, if there exists another word $s'' \in \Sigma^*$ such that $s = s's''$. For $s \in \Sigma^*$ and $s' \sqsubset s$, we use $s \backslash s'$ to denote the word s'' such that $s's'' = s$. For two nonnegative integers $i \leqslant j$, $[\![i, j]\!]$ denotes the set of all integers no less than i and no greater than j; for a set S, $|S|$ denotes its cardinality and 2^S its power set.

2.2 The exact run length problem

Let **Int** be the set of nonempty intervals of $\mathbb{R}$ having left endpoints in $\mathbb{Q} \cup \{-\infty\}$ and right endpoints in $\mathbb{Q} \cup \{+\infty\}$. Note that $\pm\infty$ do not belong to any interval of **Int**. Consider a k-dimensional *duration directed graph* $G = (\mathbf{Int}^k, V, A)$, where $k \in \mathbb{Z}_+$, $\mathbf{Int}^k$ is the k-fold Cartesian product of **Int**, V a finite set of vertices, $A \subset V \times \mathbf{Int}^k \times V$ a finite set of directed edges (arcs) with weights in $\mathbf{Int}^k$. A *run* of G is defined by $v_0 \xrightarrow{z_1} v_1 \xrightarrow{z_2} \cdots \xrightarrow{z_n} v_n =: r$, where $n \in \mathbb{Z}_+$, $v_0, \dots, v_n \in V$, for all $i \in [\![1, n]\!]$, $z_i = (z_i(1), \dots, z_i(k)) \in \mathbb{R}^k$, $(v_{i-1}, int_i, v_i) \in A$ for some $int_i = (int_i(1), \dots, int_i(k)) \in \mathbf{Int}^k$, and $z_i(j) \in int_i(j)$ for all $j \in [\![1, k]\!]$. The *weight* of run r is defined by $\sum_{i=1}^n z_i$. We sometimes write $v_1 \to v_2$ to denote a run from v_1 to v_2 without specifying the intermediate vertices and vectors. For an edge $(v_1, int_{v_1v_2}, v_2) =: a \in A$, we denote $\mathrm{tail}(a) = v_1$ and $\mathrm{head}(a) = v_2$.

▶ **Problem 1** (ERL). *Given a positive integer k, a k-dimensional duration directed graph $G = (\mathbf{Int}^k, V, A)$, two vertices $v_1, v_2 \in V$, and a vector $z \in \mathbb{Q}^k$, determine whether there exists a run from v_1 to v_2 with weight z.*

We set as usual for $n \in \mathbb{Z}_+$, the size $\mathrm{size}(n)$ of n to be the length of its binary representation; then $\mathrm{size}(-n) = \mathrm{size}(n) + 1$; $\mathrm{size}(0) = 1$; for a rational number m/n, where m, n are relatively prime integers, $\mathrm{size}(m/n) = \mathrm{size}(m) + \mathrm{size}(n)$, then for a vector $z \in \mathbb{Q}^k$, its size is the sum of the sizes of its components. In addition, $\mathrm{size}(+\infty) = \mathrm{size}(-\infty) = 2$. For a duration directed graph $G = (\mathbf{Int}^k, V, A)$, for every edge $(v_1, int_{v_1v_2}, v_2) \in A$, denote $int_{v_1v_2} = (int_{v_1v_2}(1), \dots, int_{v_1v_2}(k))$, where $int_{v_1v_2}(i) = \langle a^i_{v_1v_2}, b^i_{v_1v_2}\rangle$, $a^i_{v_1v_2} \in \mathbb{Q} \cup \{-\infty\}$, $b^i_{v_1v_2} \in \mathbb{Q} \cup \{+\infty\}$, $i \in [\![1, k]\!]$. The size $\mathrm{size}(G)$ of a given graph G is equal to $|V| + \mathrm{size}(A) = |V| + \sum_{(v_1, int_{v_1v_2}, v_2) \in A}(2 + 2k + \sum_{i=1}^k (\mathrm{size}(a^i_{v_1v_2}) + \mathrm{size}(b^i_{v_1v_2})))$. Then the size of an instance (k, G, v_1, v_2, z) of the ERL problem is $\mathrm{size}(k) + \mathrm{size}(G) + 2 + \mathrm{size}(z)$.

For every edge $(v_1, int_{v_1v_2}, v_2) \in A$ (sometimes also written as $(v_1, v_2) \in A$ for short), we denote $w^1_{v_1v_2} = (a^1_{v_1v_2}, \dots, a^k_{v_1v_2}) \in (\mathbb{Q} \cup \{-\infty\})^k$ and $w^2_{v_1v_2} = (b^1_{v_1v_2}, \dots, b^k_{v_1v_2}) \in (\mathbb{Q} \cup \{+\infty\})^k$. We set as usual $-\infty < a < +\infty$, $a + (\pm\infty) = (\pm\infty) + a = \pm\infty$ for all $a \in \mathbb{R}$, $b \cdot (\pm\infty) = (\pm\infty) \cdot b = \pm\infty$ for all $0 \neq b \in \mathbb{R}$. We also set $0 \cdot (\pm\infty) = (\pm\infty) \cdot 0 = 0$. For two vectors z_1, z_2 in $(\mathbb{Q} \cup \{\pm\infty\})^k$, we write $z_1 \leqslant z_2$ and $z_2 \geqslant z_1$ if $z_1(i) \leqslant z_2(i)$ for all $i \in [\![1, k]\!]$. For $r \in \mathbb{R}$ and $z = (z(1), \dots, z(k)) \in \mathbb{R}^k$, we write $r + z = z + r = (z(1) + r, \dots, z(k) + r)$.

▶ **Lemma 1.** *The ERL problem belongs to* NP.

Proof. Consider an instance (k, G, v_1, v_2, z) of the ERL problem.

We add an edge $(v_2, \underbrace{([0,0], \ldots, [0,0])}_{k}, v_1) =: \bar{a}$, then $w^1_{\bar{a}} = w^2_{\bar{a}} = \underbrace{(0, \ldots, 0)}_{k} =: 0^k$. For each edge a in A, we define a variable x_a. For edge $\bar{a}$, we also define a variable $x_{\bar{a}}$. Consider the following inequality

$$x_{\bar{a}} w^1_{\bar{a}} + \sum_{a \in A} x_a w^1_a \leqslant z, \tag{1a}$$

$$-x_{\bar{a}} w^2_{\bar{a}} - \sum_{a \in A} x_a w^2_a \leqslant -z, \tag{1b}$$

with constraints

$$x_{\bar{a}} = 1, \tag{2a}$$

$$x_a \in \mathbb{N} \text{ for all } a \in A, \tag{2b}$$

$$\sum_{\substack{a \in A \cup \{\bar{a}\} \\ \mathrm{head}(a) = v}} x_a = \sum_{\substack{a \in A \cup \{\bar{a}\} \\ \mathrm{tail}(a) = v}} x_a \text{ for all } v \in V, \tag{2c}$$

$$\text{the edges } a \text{ such that } x_a > 0 \text{ form a strongly connected component,} \tag{2d}$$

$$\text{for every } a \in A, \text{ if } x_a > 0, \text{ then for all } i \in [\![1, k]\!], \text{ if } \langle a^i_a, b^i_a \rangle \text{ is left-open (resp., right-open), then the } i\text{-th component of (1a) (resp., (1b)) must hold strictly.} \tag{2e}$$

If $(\tilde{x}_a)_{a \in A \cup \{\bar{a}\}}$ is a solution to (1) satisfying constrains (2), then there exists a run from v_1 to v_2 having $\tilde{x}_a$ repetitive edges $a \in A$ therein with weight z by continuity of $\mathbb{R}$, i.e., (k, G, v_1, v_2, z) is a positive instance of the ERL problem. If (1) has no solution satisfying constraints (2), then (k, G, v_1, v_2, z) is a negative instance of the ERL problem.

For an edge $a \in A$ and $i \in [\![1, k]\!]$ such that $w^1_a(i) = -\infty$, we either put $x_a = 0$ into (1) (in this case, $w^1_a(i)$ is eliminated) or remove the i-th component from (1a) in case $x_a \geqslant 1$ (in this case, $x_a \geqslant 1$ implies that the i-th component of (1a) always holds no matter what values the other variables are in). For an edge $a \in A$ and $i \in [\![1, k]\!]$ such that $w^2_a(i) = +\infty$, we do similar things. Then we obtain a number $\leqslant 4^{k|A|}$ of standard integer linear programming [14, Cor. 17.1d] (i.e., of the form $Ax \leqslant b$ with constraints, where constants $A \in \mathbb{Q}^{m \times n}$, $b \in \mathbb{Q}^{m \times 1}$, variables $x \in \mathbb{N}^{n \times 1}$) that is solvable in NP. Hence inequality (1) with constraints in (2) can be solved in NP in the size of the instance (k, G, v_1, v_2, z). ◀

▶ Remark 2. For a duration directed graph G, if all intervals shrink to a singleton, then the ERL problem reduces to the NP-complete *exact path length* problem proved in [9]. The proof of Lemma 1 is inspired by the proof of the NP membership of the exact path length problem in [9] but is more involved.

In order to obtain our main results on verification of state-based opacity for RTAs, we need the following *component-length-equal run* (CLER) problem.

▶ **Problem 2** (CLER). *Given a positive integer $k > 1$, a k-dimensional duration directed graph $G = (\mathbf{Int}^k, V, A)$, two vertices $v_1, v_2 \in V$, and an edge $(v_2, int_{v_2v_3}, v_3) \in A$, determine whether there exists a run $v_1 \to v_2 \xrightarrow{w_{v_2v_3}} v_3$ whose weight has equal components in $\mathbb{Q}$, where $v_1 \to v_2$ does not contain v_3, $w_{v_2v_3}(i) \in int_{v_2v_3}(i)$ for all $i \in [\![1, k]\!]$.*

▶ **Lemma 3.** *The CLER problem belongs to* NP.

Proof. Consider a k-dimensional ($k > 1$) duration directed graph $G = (\mathbf{Int}^k, V, A)$, and an instance (k, G, v_1, v_2, v_3) of the CLER problem, where $(v_2, int_{v_2v_3}, v_3) \in A$ for some $int_{v_2v_3} \in \mathbf{Int}^k$. We next construct a $(k-1)$-dimensional duration directed graph $G' = (\mathbf{Int}^{k-1}, V, A')$, and transform the instance (k, G, v_1, v_2, v_3) of the CLER problem to an instance $(k-1, G', v_1, v_3, 0^{k-1})$ of the ERL problem. G' is obtained from G as follows: for every edge $(v', int_{v'v''}, v'') \in A$, denote $int_{v'v''} = (\langle a^1_{v'v''}, b^1_{v'v''}\rangle, \ldots, \langle a^k_{v'v''}, b^k_{v'v''}\rangle) \in \mathbf{Int}^k$, we compute $int'_{v'v''} = (\langle a^1_{v'v''} - b^k_{v'v''}, b^1_{v'v''} - a^k_{v'v''}\rangle, \ldots, \langle a^{k-1}_{v'v''} - b^k_{v'v''}, b^{k-1}_{v'v''} - a^k_{v'v''}\rangle) \in \mathbf{Int}^{k-1}$, where for all $i \in [\![1, k-1]\!]$, $\langle a^i_{v'v''} - b^k_{v'v''}, b^i_{v'v''} - a^k_{v'v''}\rangle$ is left-open (resp., right-open) if and only if either $\langle a^i_{v'v''}, b^i_{v'v''}\rangle$ is left-open or $\langle a^k_{v'v''}, b^k_{v'v''}\rangle$ is right-open (resp., either $\langle a^i_{v'v''}, b^i_{v'v''}\rangle$ is right-open or $\langle a^k_{v'v''}, b^k_{v'v''}\rangle$ is left-open). We set $A' = \{(v', int'_{v'v''}, v'') | (v', int_{v'v''}, v'') \in A\}$.

We then have (i) (k, G, v_1, v_2, v_3) is a positive instance of the CLER problem if and only if (ii) $(k-1, G', v_1, v_3, 0^{k-1})$ is an instance of the ERL problem such that in G', there exists a run $v_1 \to v_2 \xrightarrow{w'_{v_2v_3}} v_3$ with weight 0^{k-1}, where $w'_{v_2v_3}(i) \in int'_{v_2v_3}(i)$ for all $i \in [\![1, k-1]\!]$ and v_3 appears only once in the run. Note that (ii) implies that there exists a run $v_1 \to v_2 \xrightarrow{w_{v_2v_3}} v_3$ in G whose weight has equal components w in $\mathbb{R}$, where $v_1 \to v_2$ does not contain v_3, $w_{v_2v_3}(i) \in int_{v_2v_3}(i)$ for all $i \in [\![1, k]\!]$. If w is irrational, we can add a very small real number ε to all components of $w_{v_2v_3}$ such that $v_2 \xrightarrow{w_{v_2v_3}+\varepsilon} v_3$ is still a run and $w + \varepsilon \in \mathbb{Q}$, because $\mathbb{Q}$ is dense in $\mathbb{R}$, hence (i) holds. In order to check whether $(k-1, G', v_1, v_3, 0^{k-1})$ meets the satisfaction, by Lemma 1, we need to add the additional constraint $x_{(v_2,v_3)} = 1$ into the corresponding constraints (2), and then solve the corresponding inequality (1) with the modified constraints. Hence the CLER problem belongs to NP. ◀

2.3 Real-time automata

A *real-time automaton* (RTA) is a tuple $\mathcal{A} = (Q, E, Q_0, \Delta, \mu, \Sigma, \ell)$, where Q is a nonempty finite set of *states*, E a finite *alphabet* (elements of E are called *events*), $Q_0 \subset Q$ a nonempty set of *initial states*, $\Delta \subset Q \times E \times Q$ a *transition relation* (elements of Δ are called *transitions*), μ assigns to each transition $(q, e, q') \in \Delta$ (also written as $q \xrightarrow{e} q'$) a nonempty interval $\mu(e)_{qq'}$ of $\mathbb{R}_{\geqslant 0}$ with left endpoint and right endpoint being a and b, where $a \in \mathbb{Q}_{\geqslant 0}$, $b \in \mathbb{Q}_{\geqslant 0} \cup \{+\infty\}$[1], $a \leqslant b$, Σ is a finite set of *outputs*, and $\ell : E \to \Sigma \cup \{\epsilon\}$ is an *output/labeling function.* A state $q \in Q$ is called *dead* if for all $e \in E$ and $q' \in Q$, $(q, e, q') \notin \Delta$.

The size of a given $\mathcal{A}$ is defined by $|Q| + |Q_0| + |\Delta| + \text{size}(\mu) + \text{size}(\ell)$, where the sizes of $\pm\infty$ and rational numbers have been defined before, $\text{size}(\mu) = \sum_{(q,e,q')\in\Delta} \text{size}(\mu(e)_{qq'}) = \sum_{(q,e,q')\in\Delta}(2 + \text{size}(a_{q,e,q'}) + \text{size}(b_{q,e,q'}))$, $a_{q,e,q'}$ and $b_{q,e,q'}$ are the endpoints of the interval $\mu(e)_{qq'}$, 2 is used to denote the sum of the sizes of "[" (resp., "(") and "]" (resp., ")"), $\text{size}(\ell) = |\{(e, \ell(e)) | e \in E\}|$.

A transition $(q, e, q') \in \Delta$ is interpreted as when $\mathcal{A}$ is in state q and event e occurs after some time segment in $\mu(e)_{qq'}$, $\mathcal{A}$ transitions to state q'. When event $e \in E$ occurs, the *output* $\ell(e)$ of e will be observed if $\ell(e) \neq \epsilon$ (in this case we call e *observable*); while nothing will be observed if $\ell(e) = \epsilon$ (in this case we call e *unobservable*). A transition (q, e, q') is called *observable (resp., unobservable)* if e is observable (resp., unobservable). We denote by E_o and E_{uo} the sets of observable events and unobservable events, respectively. Output function ℓ is extended to $E \times \mathbb{R}_{\geqslant 0}$ as follows: $\ell((e, t)) = (\ell(e), t)$ if $e \in E_o$, $\ell((e, t)) = \epsilon$ otherwise. Then ℓ is recursively extended to E^* as $\ell(e_1 \ldots e_n) = \ell(e_1) \ldots \ell(e_n)$ and also to $(E \times \mathbb{R}_{\geqslant 0})^*$ analogously.

[1] When $b = +\infty$, the possible intervals can only be of the form $[a, +\infty)$ or $(a, +\infty)$; when $a = b$, the possible intervals can only be $[a, a] = \{a\}$.

A *path* of $\mathcal{A}$ is defined by the empty word ϵ or a sequence $q_0 \xrightarrow{e_1} q_1 \xrightarrow{e_2} \cdots \xrightarrow{e_n} q_n$, where $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$ for all $i \in [\![1, n]\!]$. A path is called a *cycle* if its start state and terminal state coincide. A *run* of $\mathcal{A}$ is either ϵ or a sequence $q_0 \xrightarrow{e_1/t_1} q_1 \xrightarrow{e_2/t_2} \cdots \xrightarrow{e_n/t_n} q_n =: \pi$, where, $n \in \mathbb{Z}_+$, $(q_{i-1}, e_i, q_i) \in \Delta$, $t_i \in \mu(e_i)_{q_{i-1}q_i}$ for all $i \in [\![1, n]\!]$. The *timed word* of run π is defined by $\tau(\pi) = (e_1, t'_1)(e_2, t'_2)\dots(e_n, t'_n)$, where $t'_i = \sum_{k=1}^{i} t_k$ for all $i \in [\![1, n]\!]$. The *weight* WT_π of π is defined by t'_n. A run is called *instantaneous* if its weight is equal to 0, and called *noninstantaneous* otherwise. A run π is called *unobservable* if $\ell(e_1 \dots e_n) = \epsilon$, and called *observable* otherwise. A path can also be defined to be either unobservable or observable analogously. We use $\mathrm{init}(\pi)$ (resp., $\mathrm{last}(\pi)$) to denote its first state q_0 (resp., last state q_n), respectively. For a set Π of runs, we use $\mathrm{init}(\Pi)$ (resp., $\mathrm{last}(\Pi)$) to denote the set of the initial states (resp., last states) of the runs of Π. The set of runs starting at $q_0 \in Q$ and ending at $q \in Q$ is denoted by $q_0 \rightsquigarrow q$. For $e_1, \dots, e_n \in E$, $q_0 \overset{e_1 \dots e_n}{\rightsquigarrow} q$ denotes the set of all runs of the form $q_0 \xrightarrow{e_1/t_1} q_1 \xrightarrow{e_2/t_2} \cdots \xrightarrow{e_{n-1}/t_{n-1}} q_{n-1} \xrightarrow{e_n/t_n} q$, where $q_1, \dots, q_{n-1} \in Q$. For two runs $\pi_1 = q_0 \xrightarrow{e_1/t_1} q_1 \xrightarrow{e_2/t_2} \cdots \xrightarrow{e_n/t_n} q_n$ and $\pi_2 = q_n \xrightarrow{e_{n+1}/t_{n+1}} q_{n+1} \xrightarrow{e_{n+2}/t_{n+2}} \cdots \xrightarrow{e_{n+m}/t_{n+m}} q_{n+m}$, we use $\pi_1\pi_2$ to denote the concatenation $q_0 \xrightarrow{e_1/t_1} q_1 \xrightarrow{e_2/t_2} \cdots \xrightarrow{e_{n+m}/t_{n+m}} q_{n+m}$ (removing either $\mathrm{last}(\pi_1)$ or $\mathrm{init}(\pi_2)$). For a run π satisfying $q_0 \in Q_0$, $\ell(\tau(\pi)) \in (\Sigma \times \mathbb{R}_{\geqslant 0})^*$ is called a *timed output sequence generated by* $\mathcal{A}$. In this case, we observe $\ell(e_i)$ at time t'_i if $e_i \in E_o$, observe nothing at time t'_i if $e_i \in E_{uo}$, $i \in [\![1, n]\!]$. We extend function τ as follows: for all $\gamma = (\sigma_1, t_1)\dots(\sigma_n, t_n) \in (\Sigma \times \mathbb{R}_{\geqslant 0})^*$,

$$\tau(\gamma) = (\sigma_1, t'_1)\dots(\sigma_n, t'_n), \tag{3}$$

where $t'_j = \sum_{i=1}^{j} t_i$ for all $j \in [\![1, n]\!]$. The *timed language* $L(\mathcal{A})$ generated by $\mathcal{A}$ is denoted by the set of timed words of all runs of $\mathcal{A}$ starting from initial states; $\mathcal{L}(\mathcal{A})$ is the set of timed output sequences generated by $\mathcal{A}$. For a sequence $\gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^*$, we use $[\gamma]$ to denote the set of runs π of $\mathcal{A}$ starting from initial states such that $\ell(\tau(\pi)) = \gamma$. For $w = (e_1, t_1)(e_2, t_2)\dots(e_n, t_n) \in (\Sigma \times \mathbb{R})^*$ and $t \in \mathbb{R}$, we define $w \pm t = t \pm w = (e_1, t_1 \pm t)(e_2, t_2 \pm t)\dots(e_n, t_n \pm t)$; define $\mathrm{init}(w) = (\mathrm{init}_L(w), \mathrm{init}_R(w)) = (e_1, t_1)$, $\mathrm{last}(w) = (\mathrm{last}_L(w), \mathrm{last}_R(w)) = (e_n, t_n)$; and also define $\tau^{-1}(w) = (e_1, t_1)(e_2, t_2 - t_1)\dots(e_n, t_n - t_{n-1})$. Hence for a run $q_0 \xrightarrow{e_1/t_1} q_1 \xrightarrow{e_2/t_2} \cdots \xrightarrow{e_n/t_n} q_n =: \pi$, $(\tau^{-1} \circ \tau)(\pi) = (e_1, t_1)(e_2, t_2)\dots(e_n, t_n)$. For $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$, we use $\mathrm{interm}(\gamma_1, \gamma_2) = \{q \in Q | (\exists \text{ runs } \pi_1, \pi_2)[(\mathrm{init}(\pi_1) \in Q_0) \wedge (\mathrm{last}(\pi_1) = \mathrm{init}(\pi_2) = q) \wedge (\ell(\tau(\pi_1)) = \gamma_1) \wedge (\ell(\tau(\pi_1\pi_2)) = \gamma_1\gamma_2) \wedge (\mathrm{WT}_{\pi_1} = \mathrm{last}_R(\gamma_1)) \wedge (\mathrm{WT}_{\pi_2} = \mathrm{last}_R(\gamma_2) - \mathrm{last}_R(\gamma_1))]\}$ to denote the set of states $\mathcal{A}$ can be in when $\mathcal{A}$ has just generated timed output sequence γ_1, given that the current observation is timed output sequence $\gamma_1\gamma_2$.

3 Main results

3.1 Current-state estimate

For $\mathcal{A}$, a subset $x \subset Q$ of states, and a sequence $\gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^+$, we define the *current-state estimate* as

$$\begin{aligned}\mathcal{M}(\mathcal{A}, \gamma | x) := \{q \in Q | (\exists q_0 \in x)(\exists n \in \mathbb{Z}_+)(\exists m \in \mathbb{N}) \\ \left(\exists \text{ a run } \pi = q_0 \xrightarrow{e_1/t_1} \cdots \xrightarrow{e_n/t_n} q_n \xrightarrow{e_{n+1}/0} \cdots \xrightarrow{e_{n+m}/0} q\right) \\ [(e_n \in E_o) \wedge (e_{n+1} \dots e_{n+m} \in (E_{uo})^*) \wedge \ell(\tau(\pi)) = \gamma]\}.\end{aligned} \tag{4}$$

Particularly for $\mathcal{A}$ and $x \subset Q$, we define the *instantaneous-state estimate* as

$$\mathcal{M}(\mathcal{A}, \epsilon|x) := x \cup \{q \in Q | (\exists q_0 \in x)(\exists n \in \mathbb{Z}_+)(\exists \text{ a run } \pi = q_0 \xrightarrow{e_1/0} \cdots \xrightarrow{e_n/0} q) \\ [e_1 \dots e_n \in (E_{uo})^*]\}. \tag{5}$$

For all $\gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^*$, $\mathcal{M}(\mathcal{A}, \gamma|Q_0)$ is also rewritten as $\mathcal{M}(\mathcal{A}, \gamma)$ for short. Intuitively, for $\gamma = (\sigma_1, t_1) \dots (\sigma_n, t_n) \in (\Sigma \times \mathbb{R}_{\geqslant 0})^+$, $\mathcal{M}(\mathcal{A}, \gamma|x)$ denotes the set of states $\mathcal{A}$ can be in when γ has just been generated by $\mathcal{A}$ since $\mathcal{A}$ started from some state of x. Hence $\mathcal{M}(\mathcal{A}, \gamma) \subset \text{last}([\gamma])$, and $\subsetneq$ may hold. In order to fit the setting of current-state estimate, after the occurrence of the last observable event e_n (i.e., e_n occurs at the current time), we only allow unobservable, instantaneous runs, which is represented by $q_n \xrightarrow{e_{n+1}/0} \cdots \xrightarrow{e_{n+m}/0} q$ and $e_{n+1} \dots e_{n+m} \in (E_{uo})^*$. Particularly, $\mathcal{M}(\mathcal{A}, \epsilon|x)$ denotes the set of states $\mathcal{A}$ can be in at the instant when $\mathcal{A}$ just transitions to some state of x (since there may exist instantaneous transitions, at the instant, $\mathcal{A}$ may be in some state outside of x).

3.2 The notions of state-based opacity

In order to define state-based opacity, we need to specify a special subset $Q_S \subset Q$ of *secret states*. The notions of state-based opacity describe the ability of an RTA $\mathcal{A}$ forbidding an external intruder from making sure whether some secret state has been visited when the intruder observes timed output sequences generated by $\mathcal{A}$, given that the intruder knows full knowledge of the structure of $\mathcal{A}$. Before defining opacity formally, we specify a special class of states from which a secret state will definitely be reached through unobservable transitions. A state q of RTA $\mathcal{A}$ is called *eventually secret* if either (1) q is secret or (2) there is an unobservable path starting from q and along each of such paths at least one secret state will be visited. Hence a state q is not eventually secret if and only if (1) $q \notin Q_S$ and (2) either there is no unobservable path starting from q or there is an unobservable path starting at q without any secret state that either ends at a dead state or contains repetitive states.

▶ **Definition 4** (ISO). *An RTA $\mathcal{A}$ is called* initial-state opaque (with respect to Q_S) *if for every $\gamma \in \mathcal{L}(\mathcal{A})$, $\text{init}([\gamma]) \not\subset Q_S$.*

▶ **Definition 5** (CSO). *An RTA $\mathcal{A}$ is called* current-state opaque (with respect to Q_S) *if every $\gamma \in \mathcal{L}(\mathcal{A})$, in $\mathcal{M}(\mathcal{A}, \gamma)$ there exists at least one non-eventual-secret state of $\mathcal{A}$.*

▶ **Definition 6** (InfSO). *An RTA $\mathcal{A}$ is called* infinite-step opaque (with respect to Q_S) *if for all $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$ such that $|\gamma_2| \geqslant 1$, $\text{interm}(\gamma_1, \gamma_2)$ contains a state q such that there is a run $q \to q' \xrightarrow{e/t} q''$ with weight $\text{init}_R(\gamma_2) - \text{last}_R(\gamma_1)$, where $q \to q'$ is unobservable and contains no secret state, e is observable and $\ell(e) = \text{init}_L(\gamma_2)$, $q'' \in \text{interm}(\gamma_1 \,\text{init}(\gamma_2), \gamma_2 \backslash \text{init}(\gamma_2))$.*

▶ **Definition 7** (KSO). *Let K be in $\mathbb{Z}_+$. An RTA $\mathcal{A}$ is called* K-step opaque (with respect to Q_S) *if for all $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$ such that $1 \leqslant |\gamma_2| \leqslant K$, $\text{interm}(\gamma_1, \gamma_2)$ contains a state q such that there is a run $q \to q' \xrightarrow{e/t} q''$ with weight $\text{init}_R(\gamma_2) - \text{last}_R(\gamma_1)$, where $q \to q'$ is unobservable and contains no secret state, e is observable and $\ell(e) = \text{init}_L(\gamma_2)$, $q'' \in \text{interm}(\gamma_1 \,\text{init}(\gamma_2), \gamma_2 \backslash \text{init}(\gamma_2))$.*

Intuitively, when an intruder observes a timed output sequence generated by an RTA $\mathcal{A}$, if $\mathcal{A}$ is initial-state opaque, then the intruder cannot make sure whether the initial state is secret; is current-state opaque, then the intruder cannot make sure after the last observable event occurred (observing $\text{last}_L(\gamma)$) and before any new observable event occurs, whether a

secret state has been visited (note that the "current time" here means the weight of any run of $[\gamma]$, so is no less than $\text{last}_R(\gamma)$ and $>$ may hold); infinite-step opaque, then the intruder cannot make sure whether a secret state was visited after observing $\text{last}_L(\gamma_1)$ and before observing $\text{init}_L(\gamma_2)$; and K-step opaque, then the intruder cannot make sure whether the state prior to at most K observed outputs is secret. Different notions have different privacy levels, so they may have different applications.

3.3 The notion of observer

In this subsection we define and compute a notion of *observer* $\mathcal{A}_{\text{obs}}$ to concatenate current-state estimates along timed output sequences generated by $\mathcal{A}$ in 2-EXPTIME in the size of $\mathcal{A}$. Later, we will use $\mathcal{A}_{\text{obs}}$ to give a necessary and sufficient condition for CSO. Before defining $\mathcal{A}_{\text{obs}}$, we need to define a notion of *pre-observer* $\mathcal{A}^{\text{pre}}_{\text{obs}}$.

▶ **Definition 8.** *For an RTA $\mathcal{A}$, we define its* pre-observer *as a deterministic automaton*

$$\mathcal{A}^{\text{pre}}_{\text{obs}} = (X, \Sigma \times \mathbb{R}_{\geqslant 0}, x_0, \delta^{\text{pre}}_{\text{obs}}), \tag{6}$$

where $X \subset 2^Q \backslash \{\varnothing\}$ is the state set, $\Sigma \times \mathbb{R}_{\geqslant 0}$ the alphabet, $x_0 = \mathcal{M}(\mathcal{A}, \epsilon) \in X$ the unique initial state, $\delta^{\text{pre}}_{\text{obs}} \subset X \times (\Sigma \times \mathbb{R}_{\geqslant 0}) \times X$ the transition relation. For all nonempty $x \subset Q$ different from x_0, $x \in X$ if and only if there is $\gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^+$ such that $x = \mathcal{M}(\mathcal{A}, \gamma)$. For all $x, x' \in X$ and $(\sigma, t) \in \Sigma \times \mathbb{R}_{\geqslant 0}$, $(x, (\sigma, t), x') \in \delta^{\text{pre}}_{\text{obs}}$ if and only if $x' = \mathcal{M}(\mathcal{A}, (\sigma, t)|x)$.

In Definition 8, after $\delta^{\text{pre}}_{\text{obs}}$ is recursively extended to $\delta^{\text{pre}}_{\text{obs}} \subset X \times (\Sigma \times \mathbb{R}_{\geqslant 0})^* \times X$, one has for all $x \in X$ and $(\sigma_1, t_1) \dots (\sigma_n, t_n) =: \gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^+$, $(x_0, \gamma, x) \in \delta^{\text{pre}}_{\text{obs}}$ if and only if $\mathcal{M}(\mathcal{A}, \tau(\gamma)) = x$, where $\tau(\gamma)$ is defined in (3), i.e., x is the set of states that $\mathcal{A}$ can be in when timed output sequence $\tau(\gamma)$ has just been generated.

Note that the alphabet $\Sigma \times \mathbb{R}_{\geqslant 0}$ is not finite, so we cannot compute the whole $\mathcal{A}^{\text{pre}}_{\text{obs}}$. Next, we define observer $\mathcal{A}_{\text{obs}}$ as a computable sub-automaton of $\mathcal{A}^{\text{pre}}_{\text{obs}}$.

▶ **Definition 9.** *For an RTA $\mathcal{A}$, consider its pre-observer* (8)*, we define its* observer *as a finite automaton*

$$\mathcal{A}_{\text{obs}} = (X, \Sigma_{\text{obs}}, x_0, \delta_{\text{obs}}), \tag{7}$$

where Σ_{obs} (resp., δ_{obs}) is a finite subset of $\Sigma \times \mathbb{Q}_{\geqslant 0}$ (resp., $\delta^{\text{pre}}_{\text{obs}}$), such that if there exists a transition from $x \in X$ to $x' \in X$ in $\delta^{\text{pre}}_{\text{obs}}$ then at least one such transition belongs to δ_{obs}.

Note that for an RTA $\mathcal{A}$, its observer may not be unique, because Σ_{obs} may not be unique; however, X and x_0 must be unique. In Definition 9, after δ_{obs} is recursively extended to $\delta_{\text{obs}} \subset X \times (\Sigma_{\text{obs}})^* \times X$, one has for all $x \in X$ and $(\sigma_1, t_1) \dots (\sigma_n, t_n) =: \gamma \in (\Sigma_{\text{obs}})^+$, $(x_0, \gamma, x) \in \delta_{\text{obs}}$ if and only if $\mathcal{M}(\mathcal{A}, \tau(\gamma)) = x$.

▶ **Theorem 10.** *For an RTA $\mathcal{A}$, its observer $\mathcal{A}_{\text{obs}}$ can be computed in* 2-EXPTIME *in the size of $\mathcal{A}$.*

Here we only give a sketch of the proof, the entire proof is put in Appendix. The initial state $x_0 = \mathcal{M}(\mathcal{A}, \epsilon)$ is trivially computable in polynomial time. We then start from x_0, find all reachable states step by step together with the corresponding transitions, which is equivalent to checking for all $x_1, x_2 \subset Q$ and $\sigma \in \Sigma$, whether there is a transition $(x_1, (\sigma, t), x_2)$ for some $t \in \mathbb{Q}_{\geqslant 0}$. In addition, we require that for all $x_1, x_2, x_3 \subset Q$, if we find two transitions $(x_1, (\sigma, t), x_2)$ and $(x_1, (\sigma, t'), x_3)$ for some $t, t' \in \mathbb{Q}_{\geqslant 0}$, then $x_2 \subset x_3$ implies $x_3 \not\subset \mathcal{M}(\mathcal{A}, (\sigma, t)|x_1)$. This guarantees that if there exists a transition from $x_1 \subset Q$ to $x_2 \subset Q$ in $\mathcal{A}^{\text{pre}}_{\text{obs}}$, then there also exists a transition from $x_1 \subset Q$ to $x_2 \subset Q$ in $\mathcal{A}_{\text{obs}}$.

3.4 The notion of reverse observer

In this subsection we define and compute a notion of *reverse observer* ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ that will be used to verify ISO. To this end, we also need to define a notion of *pre-reverse observer* ${}_{\mathsf{R}}\mathcal{A}^{\text{pre}}_{\text{obs}}$. Similarly to observer $\mathcal{A}_{\text{obs}}$, ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ can also be computed in 2-EXPTIME in the size of $\mathcal{A}$.

For an RTA $\mathcal{A}$, a subset $x \subset Q$ of states, and a sequence $\gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^+$, we define the *reverse-current-state estimate* as

$$\mathcal{M}^{\mathsf{R}}(\mathcal{A}, \gamma|x) := \{q \in Q | (\exists q' \in x)(\exists n \in \mathbb{Z}_+)(\exists m \in \mathbb{N}) \left(\exists \text{ a run } \pi = q \xrightarrow{e_1/t_1} \cdots \xrightarrow{e_n/t_n} q_n \xrightarrow{e_{n+1}/0} \cdots \xrightarrow{e_{n+m}/0} q'\right) [(e_n \in E_o) \wedge (e_{n+1} \dots e_{n+m} \in (E_{uo})^*) \wedge \ell(\tau(\pi)) = \gamma]\}. \tag{8}$$

$\mathcal{M}^{\mathsf{R}}(\mathcal{A}, \gamma|x)$ denotes the subset of states of Q starting from which at instant 0, $\mathcal{A}$ can generate timed output sequence $\gamma \in (\Sigma \times \mathbb{R}_{\geqslant 0})^+$ and can only be in any one state of x at instant $\text{last}_R(\gamma)$.

▶ **Definition 11.** *For an RTA $\mathcal{A}$, we define its* pre-reverse observer *as a deterministic automaton*

$${}_{\mathsf{R}}\mathcal{A}^{\text{pre}}_{\text{obs}} = (X_{\mathsf{R}}, \Sigma \times \mathbb{R}_{\geqslant 0}, Q, {}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}}), \tag{9}$$

where $X_{\mathsf{R}} \subset 2^Q \backslash \{\varnothing\}$ is the state set, $\Sigma \times \mathbb{R}_{\geqslant 0}$ the alphabet, Q the unique initial state, ${}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}} \subset X_{\mathsf{R}} \times (\Sigma \times \mathbb{R}_{\geqslant 0}) \times X_{\mathsf{R}}$ the transition relation. For all $x, x' \in X_{\mathsf{R}}$ and $(\sigma, t) \in \Sigma \times \mathbb{R}_{\geqslant 0}$, $(x, (\sigma, t), x') \in {}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}}$ if and only if $x' = \mathcal{M}^{\mathsf{R}}(\mathcal{A}, (\sigma, t)|x)$, i.e., x' is the subset of states of Q starting from which at instant 0, $\mathcal{A}$ can generate timed output sequence (σ, t) and can only be in any one state of x at instant t.

▶ **Definition 12.** *For an RTA $\mathcal{A}$, consider its pre-reverse observer* (9)*, we define its* reverse observer *as a finite automaton*

$${}_{\mathsf{R}}\mathcal{A}_{\text{obs}} = (X_{\mathsf{R}}, {}_{\mathsf{R}}\Sigma_{\text{obs}}, Q, {}_{\mathsf{R}}\delta_{\text{obs}}), \tag{10}$$

where ${}_{\mathsf{R}}\Sigma_{\text{obs}}$ (resp., ${}_{\mathsf{R}}\delta_{\text{obs}}$) is a finite subset of $\Sigma \times \mathbb{Q}_{\geqslant 0}$ (resp., ${}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}}$) such that for all $x_1, x_2 \in X_{\mathsf{R}}$, if there is a transition from x_1 to x_2 in ${}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}}$ then at least one such transition belongs to ${}_{\mathsf{R}}\delta_{\text{obs}}$.

In ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, ${}_{\mathsf{R}}\Sigma_{\text{obs}}$ and ${}_{\mathsf{R}}\delta_{\text{obs}}$ may not be unique but must be finite. The following result follows from a similar proof compared with that of Theorem 10.

▶ **Theorem 13.** *For an RTA $\mathcal{A}$, its reverse observer ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ can be computed in* 2-EXPTIME *in the size of $\mathcal{A}$.*

3.5 Necessary and sufficient conditions for notions of state-based opacity

In this subsection, we use the notions of observer and reverse observer to give necessary and sufficient conditions for the four notions of opacity.

▶ **Theorem 14.** *Consider an RTA $\mathcal{A}$. $\mathcal{A}$ is initial-state opaque if and only if in reverse observer ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, for every reachable state x, if $x \cap Q_0 \neq \varnothing$ then $x \cap Q_0 \nsubseteq Q_S$; $\mathcal{A}$ is current-state opaque if and only if in observer $\mathcal{A}_{\text{obs}}$, every reachable state x contains at least one non-eventual-secret state of $\mathcal{A}$.*

Proof. Consider an arbitrary $\gamma \in \mathcal{L}(\mathcal{A})$.

By definition, $\text{init}([\gamma]) = \mathcal{M}^{\mathsf{R}}(\mathcal{A}, \gamma|Q) \cap Q_0$; and in reverse observer ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, there exists $\gamma' \in ({}_{\mathsf{R}}\Sigma_{\text{obs}})^*$ such that $(Q, \gamma', \mathcal{M}^{\mathsf{R}}(\mathcal{A}, \gamma|Q)) \in {}_{\mathsf{R}}\delta_{\text{obs}}$. For every $\gamma'' \in ({}_{\mathsf{R}}\Sigma_{\text{obs}})^*$ and state x of ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ such that $(Q, \gamma'', x) \in {}_{\mathsf{R}}\delta_{\text{obs}}$, $x = \mathcal{M}^{\mathsf{R}}(\mathcal{A}, \tau((\gamma'')^{\mathsf{R}})|Q)$. Hence the set $\{x \cap Q_0 | x \text{ is reachable in } {}_{\mathsf{R}}\mathcal{A}_{\text{obs}}\}$ is equal to the set $\{\text{init}([\gamma]) | \gamma \in \mathcal{L}(\mathcal{A})\}$. Then, $\mathcal{A}$ is initial-state opaque if and only if for every reachable state x of ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, if $x \cap Q_0 \neq \varnothing$, then $x \cap Q_0 \subsetneq Q_S$.

By definition, there exists $\gamma' \in (\Sigma_{\text{obs}})^*$ such that $(x_0, \gamma', \mathcal{M}(\mathcal{A}, \gamma)) \in \delta_{\text{obs}}$. Conversely, for every $\gamma'' \in (\Sigma_{\text{obs}})^*$ and $x \in X$ such that $(x_0, \gamma'', x) \in \delta_{\text{obs}}$, one has $x = \mathcal{M}(\mathcal{A}, \tau(\gamma''))$, where $\tau(\gamma'') \in \mathcal{L}(\mathcal{A})$. Then, $\mathcal{A}$ is current-state opaque if and only if every reachable state of $\mathcal{A}_{\text{obs}}$ contains at least one non-eventual-secret state of $\mathcal{A}$. ◀

By Theorem 10, Theorem 13, and Theorem 14, the initial-state opacity and current-state opacity of an RTA $\mathcal{A}$ can be verified in time linear in the size of ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ and $\mathcal{A}_{\text{obs}}$, respectively, hence in 2-EXPTIME in the size of $\mathcal{A}$.

▶ **Theorem 15.** *Consider an RTA $\mathcal{A}$ and $K \in \mathbb{Z}_+$. $\mathcal{A}$ is infinite-step opaque if and only if for every reachable state x of observer $\mathcal{A}_{\text{obs}}$ and every transition $(x'', (\sigma, t), x')$ of reverse observer ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ with x'' being reachable in ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, if $x \cap x' \neq \varnothing$, then $x \cap x'$ contains a state $q \in Q$ such that there is a run $q \to q' \xrightarrow{e/t'} q''$ with weight t, where $q \to q'$ is unobservable and contains no secret state of Q_S, e is observable and $\ell(e) = \sigma$, $q'' \in x''$; $\mathcal{A}$ is K-step opaque if and only if the above necessary and sufficient condition for InfSO holds, and x'' additionally satisfies that there is $\gamma \in ({}_{\mathsf{R}}\Sigma_{\text{obs}})^*$ such that $|\gamma| \leqslant K - 1$ and $(Q, \gamma, x'') \in {}_{\mathsf{R}}\delta_{\text{obs}}$.*

Proof. By definition of pre-reverse observer ${}_{\mathsf{R}}\mathcal{A}^{\text{pre}}_{\text{obs}}$, one sees that for all $\gamma_1\gamma_2 \in \mathcal{L}(\mathcal{A})$ such that $|\gamma_2| \geqslant 1$, $\text{interm}(\gamma_1, \gamma_2) = \mathcal{M}(\mathcal{A}, \gamma_1) \cap x_1$, where x_1 satisfies $(Q, (\tau^{-1}(\gamma_2 - \text{last}_R(\gamma_1)))^{\mathsf{R}}, x_1) \in {}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}}$. Choose $x_2 \in X_{\mathsf{R}}$ such that $(x_2, \text{init}(\gamma_2) - \text{last}_R(\gamma_1), x_1) \in {}_{\mathsf{R}}\delta^{\text{pre}}_{\text{obs}}$. Then by definition of InfSO, one has $\mathcal{A}$ is infinite-step opaque if and only if for all such $\gamma_1\gamma_2$, x_1, and x_2, if $\mathcal{M}(\mathcal{A}, \gamma_1) \cap x_1 \neq \varnothing$, then $\mathcal{M}(\mathcal{A}, \gamma_1) \cap x_1$ contains a state $q \in Q$ such that there is a run $q \to q' \xrightarrow{e/t'} q''$ with weight $\text{init}_R(\gamma_2) - \text{last}_R(\gamma_1)$, where $q \to q'$ is unobservable and contains no secret state of Q_S, e is observable and $\ell(e) = \text{init}_L(\gamma_2)$, $q'' \in x_2$. By definitions of observer $\mathcal{A}_{\text{obs}}$ and reverse observer ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, there exist $\bar{\gamma}_1, \bar{\gamma}_2 \in (\Sigma \times \mathbb{Q}_{\geqslant 0})^*$ such that $|\bar{\gamma}_1| = |\gamma_1|$, $|\bar{\gamma}_2| = |\gamma_2|$, $(x_0, \bar{\gamma}_1, \mathcal{M}(\mathcal{A}, \gamma_1)) \in \delta_{\text{obs}}$, $(Q, \bar{\gamma}_2, x_1) \in {}_{\mathsf{R}}\delta_{\text{obs}}$, and $(x_2, \text{last}(\bar{\gamma}_2), x_1) \in {}_{\mathsf{R}}\delta_{\text{obs}}$. Then one has the necessary and sufficient condition for InfSO holds. Similarly one has the necessary and sufficient condition for KSO also holds. ◀

We next give an upper bound for K.

▶ **Proposition 16.** *Consider an RTA $\mathcal{A}$ and a positive integer $K \in \mathbb{Z}_+$. $\mathcal{A}$ is K-step opaque if and only if it is $\min\{K, 2^{|Q|}\}$-step opaque.*

Proof. By definition, if $\mathcal{A}$ is K-step opaque, then it is K'-step opaque for all $1 \leqslant K' < K$. Then the "only if" part holds.

Next we prove the "if" part. Assume $K > 2^{|Q|}$ and $\mathcal{A}$ is not K-step opaque. By Theorem 15, for observer $\mathcal{A}_{\text{obs}}$ and reverse observer ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$, there exist $\gamma_1 \in (\Sigma_{\text{obs}})^*$, $\gamma_2 \in ({}_{\mathsf{R}}\Sigma_{\text{obs}})^*$, $x_1 \in X$, $x_2, x_2' \in X_{\mathsf{R}}$, such that $(x_0, \gamma_1, x_1) \in \delta_{\text{obs}}$, $(Q, \gamma_2, x_2) \in {}_{\mathsf{R}}\delta_{\text{obs}}$, $(x_2', \text{last}(\gamma_2), x_2) \in {}_{\mathsf{R}}\delta_{\text{obs}}$, and $1 \leqslant |\gamma_2| \leqslant K$; $x_1 \cap x_2$ is nonempty and does not contain a state q of Q such that there is a run $q \to q' \xrightarrow{e/t'} q''$ with weight $\text{last}_R(\gamma_2)$, where $q \to q'$ is unobservable and contains no secret state of Q_S, e is observable and $\ell(e) = \text{last}_L(\gamma_2)$, $q'' \in x_2'$. Because ${}_{\mathsf{R}}\mathcal{A}_{\text{obs}}$ has at most $2^{|Q|}$ states, there exists $\gamma_3 \in ({}_{\mathsf{R}}\Sigma_{\text{obs}})^*$ such that $|\gamma_3| \leqslant 2^{|Q|} - 1$ and $(Q, \gamma_3, x_2') \in {}_{\mathsf{R}}\delta_{\text{obs}}$. Then also by Theorem 15, $\mathcal{A}$ is not $2^{|Q|}$-step opaque. ◀

By Theorem 10, Theorem 13, Theorem 15, and Proposition 16, for any $K \in \mathbb{Z}_+$, the infinite-step opacity and K-step opacity of an RTA $\mathcal{A}$ can be verified in 2-EXPTIME in the size of $\mathcal{A}$.

▶ **Example 17.** Consider the toy RTA $\mathcal{A}_1$ in Figure 1. When $\mathcal{A}_1$ starts at q_0, and a occurs at instant between 1 and 2, $\mathcal{A}_1$ can transition to either q_1 or q_2; but if a occurs at instant in $(2, 3]$, $\mathcal{A}_1$ can only transition to q_1.

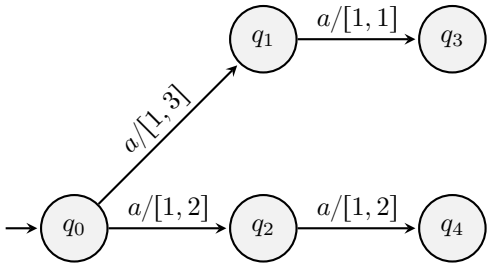

Figure 1 An RTA $\mathcal{A}_1$, where a state with an arrow from nowhere denotes an initial state, e.g., q_0; a is an observable event, $\ell(a) = a$.

One of its observers is shown in Figure 2.

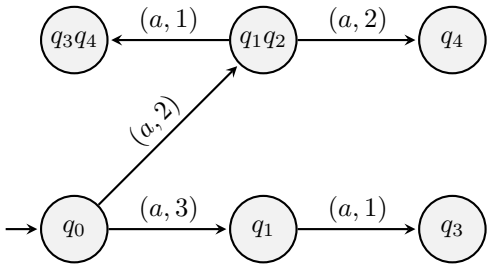

Figure 2 One observer $\mathcal{A}_{1\,\mathrm{obs}}$ of RTA $\mathcal{A}_1$ in Figure 1.

One of its reverse observers is shown in Figure 3.

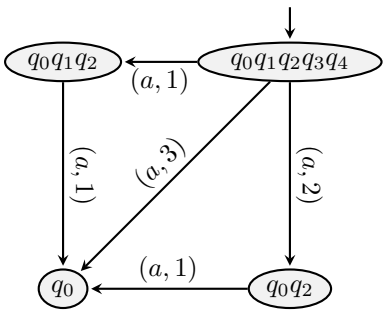

Figure 3 One reverse observer ${}_{\mathrm{R}}\mathcal{A}_{1\,\mathrm{obs}}$ of RTA $\mathcal{A}_1$ in Figure 1.

One sees two runs $q_0 \xrightarrow{a/2} q_1 \xrightarrow{a/1} q_3$ and $q_0 \xrightarrow{a/1} q_2 \xrightarrow{a/1} q_4$ of $\mathcal{A}_1$, where $2 \in \mu(a)_{q_0q_1} = [1, 3]$.

Now assume q_3 is secret, all the other states are non-secret. By definition, only q_3 is eventually secret, because there is no unobservable path starting from any other state. By observer $\mathcal{A}_{1\,\mathrm{obs}}$ and Theorem 14, $\mathcal{A}_1$ is not current-state opaque with respect to $\{q_3\}$ because

there is a reachable state $\{q_3\}$ in $\mathcal{A}_{1\,\mathrm{obs}}$ that only contains eventually secret states of $\mathcal{A}_1$ (that is, q_3). On the other hand, after observing $(a,3)(a,4)$, one can make sure that $\mathcal{A}_1$ is in state q_3 by $\mathcal{A}_{1\,\mathrm{obs}}$.

Now assume only q_1 is secret. In observer $\mathcal{A}_{1\,\mathrm{obs}}$ there is a reachable state $\{q_1\}$, in reverse observer ${}_{\mathsf{R}}\mathcal{A}_{1\,\mathrm{obs}}$ there is a reachable transition $\{q_0,\ldots,q_4\} \xrightarrow{(a,1)} \{q_0,q_1,q_2\}$. One has $\{q_1\} \cap \{q_0,q_1,q_2\} = \{q_1\}$, which contains only secret states. Then by Theorem 15, $\mathcal{A}_1$ is not infinite-step opaque with respect to $\{q_1\}$.

4 Conclusion

In this paper, we formulated four notions of state-based opacity for real-time automata, and proved that the four notions are decidable in 2-EXPTIME by defining notions of observer and reverse observer and computing them in 2-EXPTIME. The lower bounds for verifying the four notions are not known.

In addition, one can see from Theorem 10 and Theorem 13 that if an RTA $\mathcal{A}$ has no unobservable cycle, then its observers and reverse observers can be computed in EXPTIME in the size of $\mathcal{A}$ without using the ERL problem. Hence by Theorem 14 and Theorem 15, the four notions of opacity can also be verified in EXPTIME in this special case.

References

1 J. Balun and T. Masopust. Comparing the notions of opacity for discete-event systems, 2021. URL: https://arxiv.org/abs/2102.02889.

2 B. Bérard, S. Haar, S. Schmitz, and S. Schwoon. The complexity of diagnosability and opacity verification for Petri nets. *Fundamenta Informaticae*, 161(4):317–349, 2018.

3 J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. A. Ryan. Opacity generalised to transition systems. *International Journal of Information Security*, 7(6):421–435, November 2008. doi:10.1007/s10207-008-0058-x.

4 F. Cassez. The dark side of timed opacity. In Jong Hyuk Park, Hsiao-Hwa Chen, Mohammed Atiquzzaman, Changhoon Lee, Tai-hoon Kim, and Sang-Soo Yeo, editors, *Advances in Information Security and Assurance*, pages 21–30, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

5 F. Cassez, J. Dubreil, and H. Marchand. Dynamic observers for the synthesis of opaque systems. In *Automated Technology for Verification and Analysis*, pages 352–367, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

6 S. Chédor, C. Morvan, S. Pinchinat, and H. Marchand. Diagnosis and opacity problems for infinite state systems modeled by recursive tile systems. *Discrete Event Dynamic Systems*, 25(1-2):271–294, 2014.

7 F. Lin. Opacity of discrete event systems and its applications. *Automatica*, 47(3):496–503, 2011. doi:10.1016/j.automatica.2011.01.002.

8 L. Mazaré. Using unification for opacity properties. In *Proceedings of the Workshop on Issues in the Theory of Security (WITS'04)*, pages 165–176, 2004.

9 M. Nykänen and E. Ukkonen. The exact path length problem. *Journal of Algorithms*, 42(1):41–53, 2002. doi:10.1006/jagm.2001.1201.

10 A. Saboori and C. N. Hadjicostis. Notions of security and opacity in discrete event systems. In *2007 46th IEEE Conference on Decision and Control*, pages 5056–5061, December 2007. doi:10.1109/CDC.2007.4434515.

11 A. Saboori and C. N. Hadjicostis. Verification of K-step opacity and analysis of its complexity. In *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 2009 28th Chinese Control Conference*, pages 205–210, 2009. doi:10.1109/CDC.2009.5400083.

12 A. Saboori and C. N. Hadjicostis. Verification of infinite-step opacity and complexity considerations. *IEEE Transactions on Automatic Control*, 57(5):1265–1269, May 2012. doi:10.1109/TAC.2011.2173774.

13 A. Saboori and C. N. Hadjicostis. Verification of initial-state opacity in security applications of discrete event systems. *Information Sciences*, 246:115–132, 2013. doi:10.1016/j.ins.2013.05.033.

14 A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, Inc., USA, 1986.

15 M. Sipser. *Introduction to the Theory of Computation*. International Thomson Publishing, 1st edition, 1996.

16 Y. Tong, Z. Li, C. Seatzu, and A. Giua. Decidability of opacity verification problems in labeled Petri net systems. *Automatica*, 80:48–53, 2017. doi:10.1016/j.automatica.2017.01.013.

17 L. Wang and N. Zhan. *Decidability of the Initial-State Opacity of Real-Time Automata*, pages 44–60. Springer International Publishing, Cham, 2018. doi:10.1007/978-3-030-01461-2_3.

18 L. Wang, N. Zhan, and J. An. The opacity of real-time automata. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(11):2845–2856, 2018. doi:10.1109/TCAD.2018.2857363.

19 Y. Wu and S. Lafortune. Comparative analysis of related notions of opacity in centralized and coordinated architectures. *Discrete Event Dynamic Systems*, 23(3):307–339, September 2013. doi:10.1007/s10626-012-0145-z.

20 X. Yin and S. Lafortune. A new approach for the verification of infinite-step and K-step opacity using two-way observers. *Automatica*, 80:162–171, 2017. doi:10.1016/j.automatica.2017.02.037.

A Appendix

Proof. (of Theorem 10) The initial state $x_0 = \mathcal{M}(\mathcal{A}, \epsilon)$ is trivially computable in polynomial time. We then start from x_0, find all reachable states step by step together with the corresponding transitions, which is equivalent to checking for all $x_1, x_2 \subset Q$ and $\sigma \in \Sigma$, whether there is a transition $(x_1, (\sigma, t), x_2)$ for some $t \in \mathbb{Q}_{\geqslant 0}$. If it does exist, then $(x_1, (\sigma, t), x_2)$ is a transition of $\mathcal{A}_{\text{obs}}$, otherwise there is no transition $(x_1, (\sigma, t'), x_2)$ for any $t' \in \mathbb{Q}_{\geqslant 0}$ in $\mathcal{A}_{\text{obs}}$, and furthermore there is no transition $(x_1, (\sigma, t''), x_2)$ for any $t'' \in \mathbb{R}_{\geqslant 0}$ in $\mathcal{A}_{\text{obs}}^{\text{pre}}$, because $\mathbb{Q}_{\geqslant 0}$ is dense in $\mathbb{R}_{\geqslant 0}$. In addition, we require that for all $x_1, x_2, x_3 \subset Q$, if we find two transitions $(x_1, (\sigma, t), x_2)$ and $(x_1, (\sigma, t'), x_3)$ for some $t, t' \in \mathbb{Q}_{\geqslant 0}$, then $x_2 \subset x_3$ implies $x_3 \not\subset \mathcal{M}(\mathcal{A}, (\sigma, t)|x_1)$. This guarantees that if there exists a transition from $x_1 \subset Q$ to $x_2 \subset Q$ in $\mathcal{A}_{\text{obs}}^{\text{pre}}$, then there also exists a transition from $x_1 \subset Q$ to $x_2 \subset Q$ in $\mathcal{A}_{\text{obs}}$. The procedure for doing the above check is as follows.

Choose a state $x_1 = \{q_1, \ldots, q_n\} \in X$ that we have just computed, where $n \in \mathbb{Z}_+$, and $|x| = n$. Choose $\sigma \in \Sigma$. For each $i \in [\![1, n]\!]$, compute subautomaton $\mathcal{A}_{q_i}$ of $\mathcal{A}$ that consists of all paths of the form

$$q_i \xrightarrow{s_i^1} q_i^1 \xrightarrow{e_i} q_i^2 \tag{11}$$

such that $s_i^1 \in (E_{uo})^*$, $e_i \in E_o$, and $\ell(e_i) = \sigma$. Denote the set of all such q_i^2 by $\bar{x}_2$.

We next check for each $\varnothing \neq \tilde{x}_2 \subset \bar{x}_2$, whether $(x_1, (\sigma, t), \mathcal{M}(\mathcal{A}, \epsilon|\tilde{x}_2)) \in \delta_{\text{obs}}$ for some $t \in \mathbb{Q}_{\geqslant 0}$, in the order $|\tilde{x}_2|$ decreases. For every $\tilde{x}_2 \subsetneq \hat{x}_2 \subset \bar{x}_2$, if we have found a transition $(x_1, (\sigma, t'), \mathcal{M}(\mathcal{A}, \epsilon|\hat{x}_2))$ before checking $\tilde{x}_2$, then we must choose t such that $\mathcal{M}(\mathcal{A}, \epsilon|\hat{x}_2) \not\subset \mathcal{M}(\mathcal{A}, (\sigma, t)|x_1)$. In order to finish the construction of $\mathcal{A}_{\text{obs}}$, we need to do the check for at most $2^{|Q|}2^{|Q|}$ times.

[A] For each $i \in [\![1,n]\!]$, denote the number of states q_i^2 shown in (11) by $i_2 \in \mathbb{N}$, and denote these states by $q_{i,1}^2, \dots, q_{i,i_2}^2$. Here one may have $i_2 = 0$, which implies that there is no path of the form (11) starting from q_i.

[B] Nondeterministically compute asynchronous product

$$\bigotimes_{i=1}^{1'_2} \mathcal{A}_{q_1} \otimes \cdots \otimes \bigotimes_{i=1}^{n'_2} \mathcal{A}_{q_n}, \tag{12}$$

where $i'_2 \leqslant i_2$, $i \in [\![1,n]\!]$, states $q_{1,1}^2, \dots, q_{1,1'_2}^2, \dots, q_{n,1}^2, \dots, q_{n,n'_2}^2$ are pairwise different and

$$\{q_{1,1}^2, \dots, q_{1,1'_2}^2, \dots, q_{n,1}^2, \dots, q_{n,n'_2}^2\} = \tilde{x}_2,$$

this also guarantees that $\sum_{i=1}^n i'_2 \leqslant |Q|$; the states of the product are

$$(q_{1,1}, \dots, q_{1,1'_2}, \dots, q_{n,1}, \dots, q_{n,n'_2}),$$

where $q_{i,1}, \dots, q_{i,i'_2}$ are states of $\mathcal{A}_{q_i}$, $i \in [\![1,n]\!]$; there is a transition

$$\begin{matrix}(q_{1,1}, \dots, q_{1,1'_2}, \dots, q_{n,1}, \dots, q_{n,n'_2}) \\ (q'_{1,1}, \dots, q'_{1,1'_2}, \dots, q'_{n,1}, \dots, q'_{n,n'_2})\end{matrix} \xrightarrow{(e_{1,1},\dots,e_{1,1'_2},\dots,e_{n,1},\dots,e_{n,n'_2})}$$

in product (12) if and only if either one of the two conditions holds.

[a] For some $i \in [\![1,n]\!]$ and $j \in [\![1,i'_2]\!]$, $q_{i,j} \xrightarrow{e_{i,j}} q'_{i,j}$ is an unobservable transition of $\mathcal{A}_{q_i}$, for all other pairs (k,l), $e_{k,l}$ are qual to ϵ, and $q_{k,l} = q'_{k,l}$. In this case, μ assigns to the transition a vector, where the (i,j)-component is the interval $\mu(e_{i,j})_{q_{i,j}q'_{i,j}}$, for all other (k,l)-components, $\mu(e_{k,l})_{q_{k,l}q'_{k,l}} = [0,0]$.

[b] For all $i \in [\![1,n]\!]$ and $j \in [\![1,i'_2]\!]$, $q_{i,j} \xrightarrow{e_{i,j}} q'_{i,j}$ is an observable transition of $\mathcal{A}_{q_i}$. In this case, μ assigns to the transition a vector, whether the (i,j)-components are intervals $\mu(e_{i,j})_{q_{i,j}q'_{i,j}}$.

[C] In product (12), guess transition

$$\begin{matrix}(q_{1,1}^1, \dots, q_{1,1'_2}^1, \dots, q_{n,1}^1, \dots, q_{n,n'_2}^1) \\ (q_{1,1}^2, \dots, q_{1,1'_2}^2, \dots, q_{n,1}^2, \dots, q_{n,n'_2}^2),\end{matrix} \xrightarrow{(\bar{e}_{1,1},\dots,\bar{e}_{1,1'_2},\dots,\bar{e}_{n,1},\dots,\bar{e}_{n,n'_2})}$$

where $\bar{e}_{1,1}, \dots, \bar{e}_{1,1'_2}, \dots, \bar{e}_{n,1}, \dots, \bar{e}_{n,n'_2}$ are observable (i.e., item (Bb) is satisfied). Then check in product (12), whether there exists a run π_1 in

$$\begin{matrix}(q_{1,1}^1, \dots, q_{1,1'_2}^1, \dots, q_{n,1}^1, \dots, q_{n,n'_2}^1) \\ (q_{1,1}^2, \dots, q_{1,1'_2}^2, \dots, q_{n,1}^2, \dots, q_{n,n'_2}^2)\end{matrix} \xrightsquigarrow{(\bar{e}_{1,1},\dots,\bar{e}_{1,1'_2},\dots,\bar{e}_{n,1},\dots,\bar{e}_{n,n'_2})}$$

and an unobservable run π_2 in

$$(\underbrace{q_1, \dots, q_1}_{1'_2}, \dots, \underbrace{q_n, \dots, q_n}_{n'_2}) \rightsquigarrow (q_{1,1}^1, \dots, q_{1,1'_2}^1, \dots, q_{n,1}^1, \dots, q_{n,n'_2}^1) \tag{13}$$

such that the weight of $\pi_2\pi_1$ has equal components that are equal to a rational number, which actually corresponds to a positive instance $(\sum_{i=1}^n i'_2, (12), (\underbrace{q_1, \dots, q_1}_{1'_2}, \dots, \underbrace{q_n, \dots, q_n}_{n'_2}),$

$(q^1_{1,1},\ldots,q^1_{1,1'_2},\ldots,q^1_{n,1},\ldots,q^1_{n,n'_2}),(q^2_{1,1},\ldots,q^2_{1,1'_2},\ldots,q^2_{n,1},\ldots,q^2_{n,n'_2}))$ of the CLER problem (Problem 2). If Yes, then the weight is denoted by $t \in \mathbb{Q}_{\geqslant 0}$, and we find a transition

$$(x_1,(\sigma,t),\mathcal{M}(\mathcal{A},\epsilon|\tilde{x}_2)) \tag{14}$$

of $\mathcal{A}_{\text{obs}}$.

We need to do the above check (C) for at most $2^{|Q|}2^{|Q|}|Q|^{|Q|} = 2^{2|Q|^2\log|Q|}$ times (corresponding to nondeterministic computations of product (12)). Each check can be done by solving the corresponding CLER problem (Problem 2), and hence can be done in NP in the size $O((|Q|^{|Q|})^2(|E_o|^{|E_o|}+|Q||E_{uo}|)) = O(2^{|Q|^2\log|Q|}(2^{|E_o|\log|E_o|}+|Q||E_{uo}|))$ of the product (12) by Lemma 3. Hence, the total time consumption of computing $\mathcal{A}_{\text{obs}}$ is 2-EXPTIME in the size of $\mathcal{A}$. ◀