Opacity of Nondeterministic Transition Systems: A (Bi)Simulation Relation Approach

Kuize Zhang, *Senior Member, IEEE*, Xiang Yin, *Member, IEEE*, and Majid Zamani, *Senior Member, IEEE*

***Abstract*—In this paper, we propose several opacity-preserving (bi)simulation relations for nondeterministic transition systems (NTSs) in terms of initial-state opacity, current-state opacity, K-step opacity, and infinite-step opacity. We also show how one can leverage quotient constructions to compute such relations. As a result, although the opacity verification problem for infinite NTSs is generally undecidable, if one can find such an opacity-preserving relation from an infinite NTS to a finite one, the (lack of) opacity of the infinite NTS can be easily verified over the finite one, which is decidable.**

***Index Terms*—(Bi)simulation relation, nondeterministic transition system, opacity.**

I. Introduction

The notion of opacity is introduced in the analysis of cryptographic protocols [9], and describes the ability that a system forbids leaking secret information. Given a system, we assume that an intruder (outside the system) can only observe the external behaviors of the system, i.e., the outputs of the system, but cannot see the states of the system directly. Then, intuitively the system is called opaque if the intruder cannot determine whether some states of the system prior to the current time step are secret via observing the outputs prior to the current time step.

For discrete-event systems (DESs) in the framework of finite automata, the opacity problem has been widely investigated. In different practical situations, opacity of DESs can be formulated as whether a system can prevent an intruder from observing whether the initial state (resp., the current state, each state within K steps prior to the current state for some positive integer K, each state prior to the current state) of the system is secret, i.e., the so-called initial-state [13] (resp. current-state [10], K-step [11], and infinite-step [12]) opacity. It is known that the existing algorithms for verifying these types of opacity have exponential time complexity (cf., the above-mentioned references and [19]). Unfortunately, it is unlikely that there exist polynomial time algorithms for verifying them since the problems of determining initial-state opacity, K-step opacity, and infinite-step opacity of DESs are all PSPACE complete [10]–[13]. When the original system is not opaque, several different approaches have also been proposed to enforce opacity (see, e.g., [5], [15], [16], [18], [21]).

Nondeterministic transition systems (NTSs), particularly nondeterministic finite transition systems (NFTSs), play a fundamental role as a unified modeling framework in the verification and controller synthesis of hybrid systems [6], [14], and model checking [1]. Note that for general infinite-state NTSs, the opacity verification problem is undecidable [2], e.g., the initial-state opacity and current-state opacity for labeled Petri nets are undecidable [17]. Recently, opacity has also been investigated for other infinite-state systems, e.g., pushdown systems [7] and recursive tile systems [3], where classes of infinite-state systems are identified for which opacity is decidable. However, for finite-state systems, e.g., finite automata, though PSPACE-hard, the opacity verification problem is always decidable [10]–[13].

Since the opacity verification problem for general NTSs is undecidable and even for NFTSs is PSPACE-hard, in this paper we develop a theory based on (bi)simulation relations to verify opacity using (potentially *simpler*) NFTSs. Since the classical notions of (bi)simulation relations [14] do not necessarily preserve opacity, in this framework we first introduce stronger versions of (bi)simulation relations that preserve opacity. As a result, if one can find an NFTS (bi)simulating an infinite-state NTS in the sense of the stronger version, then the opacity of the NTS (undecidable in general) can be verified over the NFTS (decidable). In addition, if one can find a smaller NFTS (bi)simulating a larger NFTS in the sense of the stronger version, then the opacity of the larger NFTS can be efficiently verified over the smaller one. Particularly, we modify the existing quotient-based construction [14] to synthesize quotient systems of NTSs (resp. NFTSs) in terms of the proposed opacity-preserving (bi)simulation relations to implement the above-mentioned idea.

Intuitively, for two NTSs Σ_1 and Σ_2, Σ_2 simulates Σ_1 if each output sequence generated by Σ_1 can also be generated by Σ_2; Σ_2 bisimulates Σ_1 if Σ_2 simulates Σ_1 and vice versa (cf., [14]). Usually, (bi)simulation relation can be used to abstract a large-scale system to a smaller one. Then, in some sense the smaller system can take place of the larger one in analysis and synthesis (cf., [4], [14], [20]). In this paper, we first define new notions of opacity-preserving (bi)simulation relations, then we use the proposed notions to give some necessary and sufficient conditions for the opacity of NTSs. Hence, if one can find an appropriate opacity-preserving (bi)simulation relation from the original infinite-state NTS Σ_1 to an NFTS Σ_2 (resp. from the original NFTS Σ_1 to an NFTS Σ_2 with remarkably smaller size than that of Σ_1), then

Manuscript received February 9, 2018; revised February 12, 2018, August 26, 2018, and December 4, 2018; accepted March 24, 2019. Date of publication April 2, 2019; date of current version December 3, 2019. This work was supported in part by the German Research Foundation through Grant ZA 873/1-1, the National Natural Science Foundation of China under Grant 61803259, Grant 61833012, and Grant 61603109, and the Natural Science Foundation of Heilongjiang Province of China under Grant LC2016023. This paper (results in sections III-D and III-E) was presented in part at the 56th IEEE Conference on Decision and Control, Melbourne, Australia, December 12–15, 2017. Recommended by Associate Editor Carla Seatzu. *(Corresponding author: Kuize Zhang.)*

K. Zhang is with the ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm 10044, Sweden, and also with the College of Automation, Harbin Engineering University, Harbin 150001, China (e-mail: kuzhan@kth.se).

X. Yin is with the Department of Automation and Key Laboratory of System Control and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: yinxiang@sjtu.edu.cn).

M. Zamani is with the Computer Science Department, University of Colorado Boulder, Boulder, CO 80309, USA, and also with the Department of Computer Science, Ludwig Maximilian University of Munich, Munich 80539, Germany (e-mail: majid.zamani@colorado.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TAC.2019.2908726

the opacity of Σ_1 can be checked (resp. much faster) by verifying that of Σ_2. In details, we first define a new notion of initial-state opacity-preserving (InitSOP) simulation relation from one NTS to another NTS, which is actually not the classical simulation relation [14]. Second, because the InitSOP simulation relation does not suffice to preserve the other three types of opacity, we define also a notion of infinite-step opacity-preserving (InfSOP) bisimulation relation that preserves the other three types of opacity and is actually a stronger version of the classical bisimulation relation [14]. In addition, we show that under some mild assumptions, the simulation/bisimulation relation from an NTS to its quotient system becomes InitSOP simulation/InfSOP bisimulation relation, which provides a constructive scheme for computing opacity-preserving abstractions of NTSs or large NFTSs. A preliminary investigation of our results on only InfSOP bisimulation relation appeared in [23]. In this paper, we present a detailed and mature description of the results announced in [23], including investigating other notions of opacity (initial-state, current-state, and K-step opacity).

The remainder of this paper is organized as follows. In Section II, the basic notions of NTSs/NFTSs and (bi)simulation relation are introduced. In Section III, we show the main results of the paper, i.e, the notions of opacity-preserving (bi)simulation relations, and their implementation based on quotient systems. Section IV shows how to use a two-way observer technique [19] to verify the opacity of NFTSs. Section V concludes the paper.

II. Preliminaries

We use the following notations throughout the paper:

1) $\emptyset$: the empty set;
2) $\mathbb{N}$: the set of natural numbers;
3) $\mathbb{R}$: the set of real numbers;
4) $[a,b] := \{a, a+1, \ldots, b\}$, where $a, b \in \mathbb{N},\ a \leq b$;
5) $|X|$: the cardinality of set X.

NTSs are defined as in [8] and[14] with some modifications to accommodate for secret states.

Definition 1: An NTS Σ is a septuple $(X, X_0, S, U, \rightarrow, Y, h)$ consisting of the following:

1) a (potentially infinite) set X of states;
2) a (potentially infinite) subset $X_0 \subseteq X$ of initial states;
3) a (potentially infinite) subset $S \subseteq X$ of secret states;
4) a (potentially infinite) set U of inputs;
5) a transition relation $\rightarrow \subseteq X \times U \times X$;
6) a set Y of outputs;
7) an output map $h : X \rightarrow Y$.

In an NTS, for a state $x \in X$, the output $h(x)$ also means the observation at x. An NTS is called an NFTS if X and U are finite sets. Elements of $\rightarrow$ are called transitions. Let X^* be the set of strings of finite length over X including the string ϵ of length 0 and X^+ be $X^* \setminus \{\epsilon\}$. For each $\xi \in X^*$, $|\xi|$ denotes the length of ξ. For each $\xi \in X^*$, for all integers $0 \leq i \leq j \leq |\xi| - 1$, we use $\xi[i,j]$ to denote $\xi(i)\xi(i+1)\ldots\xi(j)$ for short. Sets U^*, U^+, Y^*, and Y^+ are defined analogously. Given an input sequence $\alpha \in U^*$, a string $\xi \in X^*$ is called a run over α if $|\xi| - 1 \leq |\alpha|$, $\xi(0) \in X_0$, and for all $i \in [0, |\xi| - 2]$, $(\xi(i), \alpha(i), \xi(i+1)) \in \rightarrow$. Particularly, a run $\xi \in X^*$ over input sequence $\alpha \in U^*$ is said to be maximal if either $|\xi| - 1 = |\alpha|$ or $(\xi(|\xi| - 1), \alpha(|\xi| - 1), x') \notin \rightarrow$ for any $x' \in X$. For a run ξ, $h(\xi(0))\ldots h(\xi(|\xi| - 1))$ is called an output sequence generated by the system. Transitions generated by α and ξ can be denoted as $\xi(0) \xrightarrow{\alpha(0)} \xi(1) \xrightarrow{\alpha(1)} \cdots \xrightarrow{\alpha(|\xi|-2)} \xi(|\xi| - 1)$ (or $\xi(0) \xrightarrow{\alpha} \xi(|\xi| - 1)$ for short). A state $x \in X$ is called reachable from an initial state $x_0 \in X_0$ if there exists $\alpha \in U^*$ such that $x_0 \xrightarrow{\alpha} x$. An NTS is called total if for all $x \in X$ and $u \in U$, there exists $x' \in X$ such that $(x, u, x') \in \rightarrow$. Hence, after a total NTS starts running, it never stops. However, for a nontotal NTS, after it starts running, it may stop; and once it stops, it never starts again. We assume that the termination of running can be observed, and use a new state ϕ to denote it. In order to describe this phenomenon, we extend a nontotal NTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ to a total NTS $\Sigma_{\text{aug}} := (X \cup \{\phi\}, X_0, S, U, \rightarrow_{\text{aug}}, Y \cup \{\phi\}, h_{\text{aug}})$ as its augmented system, where $\phi \notin X \cup U \cup Y$, $\rightarrow \subseteq \rightarrow_{\text{aug}}$, $\rightarrow_{\text{aug}} \setminus \rightarrow = \{(\phi, u, \phi) | u \in U\} \cup \{(x, u, \phi) | (x, u, x') \notin \rightarrow \text{ for any } x' \in X\}$, $h_{\text{aug}}|_X = h$ (i.e., the restriction of h_{aug} to X equals h), and $h_{\text{aug}}(\phi) = \phi$. Particularly, for a total NTS, its augmented system, also denoted by Σ_{aug}, is the NTS itself.

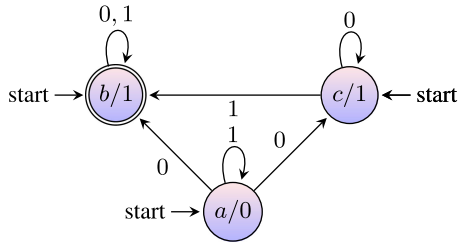

Fig. 1. State transition diagram of the NFTS in Example 2.1.

An NTS can be represented by its state transition diagram, i.e., a directed graph whose vertices correspond to the states and their associated outputs of the NTS and whose edges correspond to state transitions. Each edge is labeled with the inputs associated with the transition, a state directly connected from "start" means an initial state, and a double circle (or rectangle) denotes a secret state. We give an example to depict these concepts.

Example 2.1: Consider NFTS $(X, X_0, S, U, \rightarrow, Y, h)$, where $X = \{a, b, c\}$, $X_0 = X$, $S = \{b\}$, $U = Y = \{0, 1\}$, $\rightarrow = \{(a,1,a), (a,0,b), (a,0,c), (b,0,b), (b,1,b), (c,0,c), (c,1,b)\}$, $h(a) = 0$, $h(b) = h(c) = 1$ (see Fig. 1).

Here, we recall the classical notions of (bi)simulation relations (see for example, [14]).

Definition 2 (Simulation): Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U_i, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called a simulation relation from Σ_1 to Σ_2 if the following condition holds:

1) for every $x_{1,0} \in X_{1,0}$, there exists $x_{2,0} \in X_{2,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$, if there is a transition $x_1 \xrightarrow{u_1}_1 x_1'$ in Σ_1 then there exists a transition $x_2 \xrightarrow{u_2}_2 x_2'$ in Σ_2 satisfying $(x_1', x_2') \in \sim$.

Under a simulation relation $\sim \subseteq X_1 \times X_2$ from Σ_1 to Σ_2, we say Σ_2 simulates Σ_1, and denote it by $\Sigma_1 \preceq_{\mathsf{S}} \Sigma_2$.

Definition 3 (Bisimulation): Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U_i, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called a bisimulation relation between Σ_1 and Σ_2 if the following condition holds:

1) for every,
   a) $x_{1,0} \in X_{1,0}$, there exists $x_{2,0} \in X_{2,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   b) $x_{2,0} \in X_{2,0}$, there exists $x_{1,0} \in X_{1,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$,
   a) if there exists a transition $x_1 \xrightarrow{u_1}_1 x_1'$ in Σ_1 then there exists a transition $x_2 \xrightarrow{u_2}_2 x_2'$ in Σ_2 satisfying $(x_1', x_2') \in \sim$;
   b) if there exists a transition $x_2 \xrightarrow{u_2}_2 x_2'$ in Σ_2 then there exists a transition $x_1 \xrightarrow{u_1}_1 x_1'$ in Σ_1 satisfying $(x_1', x_2') \in \sim$.

Under a bisimulation relation $\sim \subseteq X_1 \times X_2$ between Σ_1 and Σ_2, we say Σ_2 bisimulates Σ_1 and vice versa, and denote it by $\Sigma_1 \cong_{\mathsf{S}} \Sigma_2$.

From Definitions 2 and 3, one can readily see that if Σ_2 simulates Σ_1 then each output sequence generated by Σ_1 can be generated by

Σ_2 as well; and if Σ_2 bisimulates Σ_1 then the set of output sequences generated by Σ_1 coincides with that generated by Σ_2.

Here, we recall notions of quotient relations and quotient systems [14] with some modifications, which will be used later to show one of the main results of the paper.

Definition 4 (Quotient system): Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS and $\sim \subseteq X \times X$ an equivalence relation on X satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. The quotient system of Σ by $\sim$, denoted by $\Sigma_\sim$, is defined as the system $\Sigma_\sim = (X_\sim, X_{\sim,0}, S_\sim, U, \rightarrow_\sim, Y, h_\sim)$ satisfying the following:

1) $X_\sim = X/\sim = \{[x] | x \in X\}$;
2) $X_{\sim,0} = \{[x] | x \in X, [x] \cap X_0 \neq \emptyset\} = \{[x] | x \in X_0\}$;
3) $S_\sim = \{[x] | x \in X, [x] \cap S \neq \emptyset\} = \{[x] | x \in S\}$;
4) for all $[x], [x'] \in X_\sim$ and $u \in U$, there exists transition $[x] \xrightarrow{u}_\sim [x']$ in $\Sigma_\sim$ if and only if there exists transition $\bar{x} \xrightarrow{u} \bar{x}'$ in Σ for some $\bar{x} \in [x]$ and $\bar{x}' \in [x']$;
5) $h_\sim([x]) = h(\bar{x})$ for every $\bar{x} \in [x]$;

where for every $x \in X$, $[x]$ denotes the equivalence class generated by x, i.e., $[x] := \{x' \in X | (x', x) \in \sim\}$.

It can be seen that for all $x, x' \in X$, 1) either $[x] = [x']$ or $[x] \cap [x'] = \emptyset$; 2) $x \in [x']$ if and only if $[x] = [x']$. Then, the set of all distinct equivalence classes corresponding to $\sim$ partitions X. Note that in [14], there is no item for $S_\sim$, since the system Σ considered in [14] does not have secret states. From Definition 4, one can easily verify that the number of states in the quotient system $\Sigma_\sim$ is less than or equal to that in Σ.

Consider an NTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ and its quotient system $\Sigma_\sim = (X_\sim, X_{\sim,0}, S_\sim, U, \rightarrow_\sim, Y, h_\sim)$ defined by an equivalence relation $\sim \subseteq X \times X$ satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. By defining a quotient relation

$$\sim_Q := \{(x, [x]) | x \in X\} \subseteq X \times X_\sim \tag{1}$$

the following result, borrowed from [14], holds.

Proposition 2.2: Consider an NTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ and its quotient system $\Sigma_\sim = (X_\sim, X_{\sim,0}, S_\sim, U, \rightarrow_\sim, Y, h_\sim)$ defined by an equivalence relation $\sim \subseteq X \times X$ satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. Under quotient relation $\sim_Q$ defined in (1), $\Sigma_\sim$ simulates Σ. Moreover, $\Sigma_\sim$ bisimulates Σ under $\sim_Q$ if and only if Σ bisimulates Σ under $\sim$.

In the sequel, with these preliminaries, we present our main results.

III. Opacity-Preserving (Bi)Simulation Relations

A. Concepts of Opacity

In this section, we formulate the notions of opacity of NTSs.

Definition 5 (InitSO): Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS. System Σ is said to be initial-state opaque if for every $x_0 \in X_0 \cap S$, every $\alpha \in U^*$, and every maximal run $x_0 \dots x_k \in X^*$ over α with $k \leq |\alpha|$, there exists a maximal run $x'_0 \dots x'_k \in X^*$ also over α such that $x'_0 \notin S$, and $h(x_j) = h(x'_j)$ for every $j \in [0, k]$.

Intuitively, if a system Σ is initial-state opaque, then the intruder cannot make sure whether the initial state is secret or not.

Definition 6 (CSO): Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS. System Σ is said to be current-state opaque if for every $x_0 \in X_0$, every $\alpha \in U^*$, and every run $x_0 \dots x_{|\alpha|} \in X^*$ over α, if $x_{|\alpha|} \in S$ then there exists a run $x'_0 \dots x'_{|\alpha|} \in X^*$ also over α such that $x'_{|\alpha|} \notin S$, and $h(x_j) = h(x'_j)$ for every $j \in [0, |\alpha|]$.

Intuitively, if a system Σ is current-state opaque, then the intruder cannot make sure whether the current state is secret.

Definition 7 (KSO): Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS. System Σ is said to be K-step opaque for a given positive integer K if for every $x_0 \in X_0$, every $\alpha \in U^*$, every run $x_0 \dots x_{|\alpha|} \in X^*$ over α, and every $i \in [K', |\alpha|]$, if $x_i \in S$ then there exists a run $x'_0 \dots x'_{|\alpha|} \in X^*$ also over α such that $x'_i \notin S$, and $h(x_j) = h(x'_j)$ for every $j \in [0, |\alpha|]$, where $K' = \max\{0, |\alpha| - K\}$.

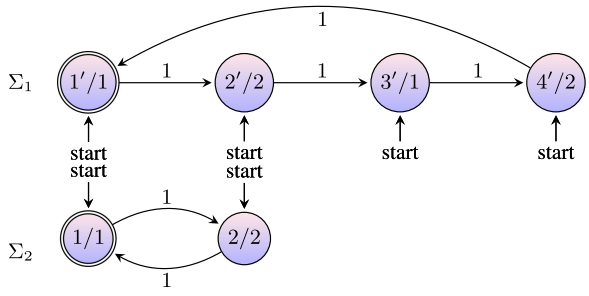

Fig. 2. State transition diagrams of two NFTSs in the proof of Proposition 3.1.

Definition 8 (InfSO): Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS. System Σ is said to be infinite-step opaque if for every $x_0 \in X_0$, every $\alpha \in U^*$, every maximal run $x_0 \dots x_k \in X^*$ over α with $k \leq |\alpha|$, and every $i \in [0, k]$, if $x_i \in S$ then there exists a maximal run $x'_0 \dots x'_k \in X^*$ also over α such that $x'_i \notin S$, and $h(x_j) = h(x'_j)$ for every $j \in [0, k]$.

Intuitively, if a system Σ is infinite (resp. K)-step opaque, then the intruder cannot make sure whether any state (within K steps) prior to the current state is secret.

It is readily seen that an NTS Σ is initial-state (resp. current-state, K-step, infinite-step) opaque if and only if its augmented system Σ_{aug} is initial-state (resp. current-state, K-step, infinite-step) opaque. Hence, without loss of generality, we can consider only total NTSs in what follows.

B. InitSOP (bi)Simulation Relations

In this section, we characterize the InitSOP simulation relation.

One of the main goals of this section is to provide a simulation-based method for verifying the initial-state opacity of NTSs. Particularly, for two NTSs Σ_1 and Σ_2, we are interested in providing a new notion of simulation relation such that Σ_2 simulating Σ_1 implies that if Σ_1 is initial-state opaque then Σ_2 is also initial-state opaque. In other words, lack of opacity in Σ_2 implies lack of opacity in Σ_1. Hence, the central problem is whether the classical simulation relation preserves initial-state opacity. We next show that generally the classical simulation relation does not preserve initial-state opacity.

Proposition 3.1: The simulation relation (cf., Definition 2) does not preserve initial-state opacity.

Proof: We provide a counterexample to prove the statement. Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$, shown in Fig. 2, where $X_1 = \{1', 2', 3', 4'\} = X_{1,0}, S_1 = \{1'\}, X_2 = \{1, 2\} = X_{2,0}, S_2 = \{1\} = U, Y = \{1, 2\}$.

By Definition 5, system Σ_1 is initial-state opaque, because for input sequence $\alpha := 1 \dots 1 \in U^*$, for run $x_1 := 1'2'3' \dots$ over α, there is a unique run $x_2 := 3'4'1' \dots$ over α such that they produce the same output sequence $121 \dots$, where $1' \in X_{1,0} \cap S_1$ and $3' \in X_{1,0} \setminus S_1$ are initial states. Again by Definition 5, system Σ_2 is not initial-state opaque, because for secret state 1, there exists no other state producing the same output as 1. On the other hand, it can be readily verified that under relation $\sim = \{(1', 1), (2', 2), (3', 1), (4', 2)\}$, Σ_2 simulates Σ_1. Hence, simulation relation does not preserve initial-state opacity. Similarly, one can readily show that relation $\sim^{-1} = \{(1, 1'), (2, 2'), (1, 3'), (2, 4')\}$ is a simulation relation from Σ_2 to Σ_1. Hence, the simulation relation does not preserve the lack of initial-state opacity either. ■

Since the simulation relation does not preserve (lack of) initial-state opacity, we propose a variant of this notion to make it InitSOP.

Definition 9 (InitSOP simulation relation): Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$

is called an IntiSOP simulation relation from Σ_1 to Σ_2 if the following condition holds:

1) for all,
   a) $x_{1,0} \in X_{1,0} \setminus S_1$, there exists $x_{2,0} \in X_{2,0} \setminus S_2$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   b) $x_{2,0} \in X_{2,0} \cap S_2$, there exists $x_{1,0} \in X_{1,0} \cap S_1$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$,
   a) for every transition $x_1 \xrightarrow{u}_1 x_1'$, there exists transition $x_2 \xrightarrow{u}_2 x_2'$ such that $(x_1', x_2') \in \sim$;
   b) for every transition $x_2 \xrightarrow{u}_2 x_2'$, there exists transition $x_1 \xrightarrow{u}_1 x_1'$ such that $(x_1', x_2') \in \sim$.

Note that 1) of Definition 9 and 1) of Definition 2 are not comparable. Hence, Definition 9 is not the classical simulation relation. Note also that 3) of Definition 9 is stronger than 3) of Definition 2. Though stronger, 3) of Definition 9 is somehow necessary for preserving initial-state opacity.

Theorem 3.2: Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. Assume that there exists an InitSOP simulation relation $\sim \subseteq X_1 \times X_2$ from Σ_1 to Σ_2. If Σ_1 is initial-state opaque then Σ_2 is also initial-state opaque.

Proof: Assume there exists an InitSOP simulation relation $\sim \subseteq X_1 \times X_2$ from Σ_1 to Σ_2 and system Σ_1 is initial-state opaque. Next, we prove that Σ_2 is also initial-state opaque.

For system Σ_2, we arbitrarily choose input sequence $\alpha \in U^*$, states $x_{2,0}, x_{2,1}, \ldots, x_{2,|\alpha|} \in X_2$ such that

$$x_{2,0} \xrightarrow{\alpha(0)}_2 x_{2,1} \xrightarrow{\alpha(1)}_2 \cdots \xrightarrow{\alpha(|\alpha|-1)}_2 x_{2,|\alpha|} \tag{2}$$

and $x_{2,0} \in X_{2,0} \cap S_2$.

By 1b), 2), and 3b) of Definition 9, there exist $x_{1,0} \in X_{1,0} \cap S_1$, $x_{1,j} \in X_1$, $j \in [1, |\alpha|]$ such that $h_1(x_{1,k}) = h_2(x_{2,k})$ for all k in $[0, |\alpha|]$, and

$$x_{1,0} \xrightarrow{\alpha(0)}_1 x_{1,1} \xrightarrow{\alpha(1)}_1 \cdots \xrightarrow{\alpha(|\alpha|-1)}_1 x_{1,|\alpha|}. \tag{3}$$

Since Σ_1 is initial-state opaque, there exist $x_{1,0}' \in X_{1,0} \setminus S_1, x_{1,j}' \in X_1, j \in [1, |\alpha|]$ such that $h_1(x_{1,k}) = h_1(x_{1,k}')$ for all k in $[0, |\alpha|]$, and $x_{1,0}' \xrightarrow{\alpha(0)}_1 x_{1,1}' \xrightarrow{\alpha(1)}_1 \cdots \xrightarrow{\alpha(|\alpha|-1)}_1 x_{1,|\alpha|}'$.

By 1a), 2), and 3a) of Definition 9, there exist $x_{2,0}' \in X_{2,0} \setminus S_2$ and $x_{2,1}', \ldots, x_{2,|\alpha|}' \in X_2$ such that $h_1(x_{1,k}') = h_2(x_{2,k}')$, for all $k \in [0, |\alpha|]$, and $x_{2,0}' \xrightarrow{\alpha(0)}_2 x_{2,1}' \xrightarrow{\alpha(1)}_2 \cdots \xrightarrow{\alpha(|\alpha|-1)}_2 x_{2,|\alpha|}'$. Hence, $\forall j \in [0, |\alpha|] : h_2(x_{2,j}) = h_2(x_{2,j}')$, and Σ_2 is initial-state opaque. ■

In Definition 9, in addition to requiring equivalent observation at two related states, i.e., condition 2), we also have four conditions 1a), 1b), 3a), and 3b). In particular, conditions 3a) and 3b) are similar to those in the standard bisimulation relation. The question then arises as why we need such strong conditions for InitSOP *simulation* relation. In the next four examples, we show that these conditions are all necessary to make it InitSOP even for one direction.

Example 3.3: Recall the NFTSs shown in Fig. 2. We showed that Σ_2 simulates Σ_1, Σ_1 is initial-state opaque, but Σ_2 not. We directly see that the simulation relation $\sim = \{(1', 1), (2', 2), (3', 1), (4', 2)\}$ in the proof of Proposition 3.1 from Σ_1 to Σ_2 does not satisfy 1a) of Definition 9, since for state $3' \in X_{1,0} \setminus S_1$, the unique state 1 satisfying $(3', 1) \in \sim$ does not belong to $X_{2,0} \setminus S_2$. We also see that relation $\sim$ satisfies all other items of Definition 9. Hence, 1a) in Definition 9 is necessary to make it InitSOP.

Example 3.4: Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$, shown in Fig. 3, where $X_1 = \{1, 2, 3, 4, 5, 6\}$, $X_{1,0} = \{1, 2, 3, 4\}$, $S_1 = \{1\}$; $X_2 = \{1', 2', 3', 4', 5', 6'\} = X_{2,0}$, $S_2 = \{5', 6'\}$, $U = \{1\}$, $Y = \{1, 2, 3\}$. For system Σ_1, it can be verified that relation $\{(1, 3), (3, 1), (2, 4), (4, 2), (5, 6), (6, 5)\}$ is a bisimulation relation between Σ_1 and itself, then for each run starting from state 1, there is a run starting from state 3 such that these two runs produce the same output sequence, i.e., Σ_1 is initial-state opaque. It is evident that system Σ_2 is not initial-state opaque, since if the initial output is three then one knows that the initial states of Σ_2 are secret. Now, consider relation $\sim = \{(1, 1'), (2, 2'), (3, 3'), (4, 4'), (5, 5'), (6, 6')\}$. One can verify that $\sim$ satisfies all items of Definition 9 other than 1b). Hence, 1b) in Definition 9 is also necessary to make it InitSOP.

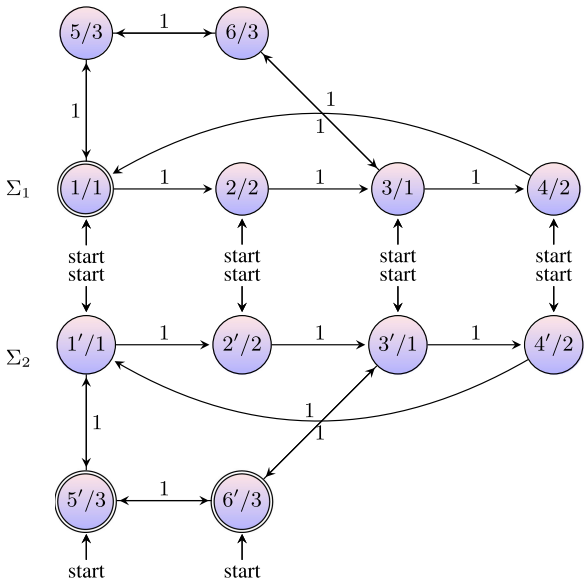

Fig. 3. State transition diagrams of two NFTSs in Example 3.4.

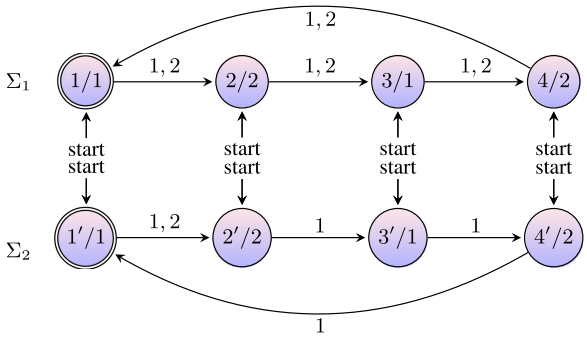

Fig. 4. State transition diagrams of two NFTSs in Example 3.5.

Example 3.5: Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$, shown in Fig. 4, where $X_1 = \{1, 2, 3, 4\} = X_{1,0}$, $S_1 = \{1\}$; $X_2 = \{1', 2', 3', 4'\} = X_{2,0}$, $S_2 = \{1'\}$, $U = \{1, 2\}$, $Y = \{1, 2\}$. For system Σ_1, it is directly obtained that for each input sequence $\alpha \in U^*$, and each run starting from state 1 over α, there is a run starting from state 3 also over α, i.e., Σ_1 is initial-state opaque. For system Σ_2, consider input sequence 2 and run $1'2'$ over input sequence 2. However, there is no run starting from $3'$ over input sequence 2, impling that Σ_2 is not initial-state opaque. Now, consider relation $\sim = \{(1, 1'), (2, 2'), (3, 3'), (4, 4')\}$. One can show that $\sim$ satisfies all items of Definition 9 other than 3a). Therefore, 3a) in Definition 9 is also necessary to make it InitSOP.

Example 3.6: Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$, shown in Fig. 5, where $X_1 = \{1, 2, 3, 4\} = X_{1,0}$, $S_1 = \{1\}$; $X_2 = \{1', 2', 3', 4'\} = X_{2,0}$, $S_2 = \{1'\}$, $U = \{1, 2\}$, $Y = \{1, 2\}$. We already showed that system Σ_1 is initial-state opaque in the

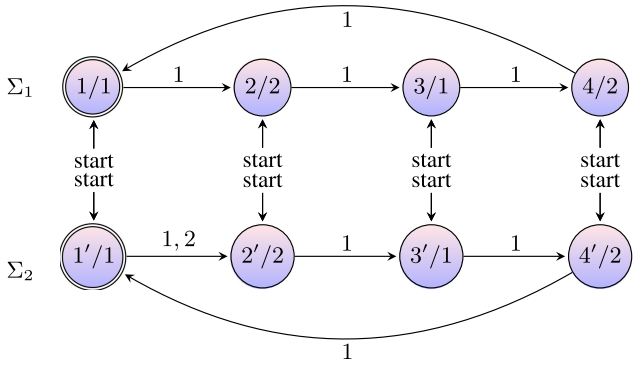

Fig. 5. State transition diagrams of two NFTSs in Example 3.6.

proof of Proposition 3.1, and system Σ_2 is not initial-state opaque in Example 3.5. Now, consider relation $\sim = \{(1,1'),(2,2'),(3,3'),(4,4')\}$. One can verify that $\sim$ satisfies all items of Definition 9 other than 3b). Hence, 3b) in Definition 9 is also necessary to make it InitSOP.

One can conclude from Examples 3.3, 3.4, 3.6, and 3.5 that in order to make Definition 9 InitSOP, all items 1a), 1b), 3a), and 3b) are necessary. Therefore, the simulation relation introduced in Definition 9 is a weak relation in terms of requiring minimal conditions preserving initial-state opacity of NTSs.

It is easy to see that Definition 9 can only guarantee unidirectional preservation of initial-state opacity. Analogously, we can define an InitSOP bisimulation relation that ensures the bidirectional preservation of initial-state opacity as in Definition 10, a stronger version of bisimulation relation.

Definition 10 (InitSOP bisimulation relation): Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called an InitSOP bisimulation relation between Σ_1 and Σ_2 if the following condition holds:

1) for all,
   a) $x_{1,0} \in X_{1,0} \cap S_1$, there exists $x_{2,0} \in X_{2,0} \cap S_2$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   b) $x_{1,0} \in X_{1,0} \setminus S_1$, there exists $x_{2,0} \in X_{2,0} \setminus S_2$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   c) $x_{2,0} \in X_{2,0} \cap S_2$, there exists $x_{1,0} \in X_{1,0} \cap S_1$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   d) $x_{2,0} \in X_{2,0} \setminus S_2$, there exists $x_{1,0} \in X_{1,0} \setminus S_1$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$,
   a) for every transition $x_1 \xrightarrow{u}_1 x_1'$, there exists transition $x_2 \xrightarrow{u}_2 x_2'$ such that $(x_1', x_2') \in \sim$;
   b) for every transition $x_2 \xrightarrow{u}_2 x_2'$, there exists transition $x_1 \xrightarrow{u}_1 x_1'$ such that $(x_1', x_2') \in \sim$.

Remark 1: Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. One can readily verify from Definition 10 that a relation $\sim \subseteq X_1 \times X_2$ is called an InitSOP bisimulation relation between Σ_1 and Σ_2 if $\sim$ is an InitSOP simulation relation from Σ_1 to Σ_2 and[1] $\sim^{-1}$ is an InitSOP simulation relation from Σ_2 to Σ_1.

Similar to Theorem 3.2, the following theorem follows from Definition 10.

Theorem 3.7: Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. Assume that there exists an InitSOP bisimulation relation $\sim \subseteq X_1 \times X_2$ between Σ_1 and Σ_2. Then, Σ_1 is initial-state opaque if and only if Σ_2 is also initial-state opaque.

[1]Given a relation $\sim \subseteq X_1 \times X_2$, $\sim^{-1}$ denotes the inverse relation defined by $\sim^{-1} = \{(x_2, x_1) \in X_2 \times X_1 \mid (x_1, x_2) \in \sim\}$.

Proof: Since Σ_1 simulates Σ_2 and vice versa as in Definition 9, the proof is a simple consequence of the proof of Theorem 3.2. ■

C. InitSOP Quotient Relations

From the results in the aforementioned section, one can verify initial-state opacity of system Σ_2 by verifying it over system Σ_1 (resp. verify lack of initial-state opacity of system Σ_1 by verifying it over system Σ_2) provided that there exists an InitSOP simulation relation from Σ_1 to Σ_2. In this section, we show that the quotient relation defined in (1) from an NTS to its quotient system is an InitSOP bisimulation relation under certain mild assumptions. Hence, one can leverage the existing bisimulation algorithms provided in [14] with some modifications to construct InitSOP abstractions (if existing).

Theorem 3.8: Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS and $\sim \subseteq X \times X$ be an equivalence relation on X satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. Assume that

$$\text{for all } x \in S \text{ and } x' \in X, \text{ if } (x, x') \in \sim \text{ then } x' \in S. \tag{4}$$

Then $\sim_{\mathsf{Q}}$ is an InitSOP bisimulation relation between Σ and $\Sigma_\sim$ if and only if relation $\sim$ satisfies

$$\forall (x, x') \in \sim, \forall\, x \xrightarrow{u} x'', \exists\, x' \xrightarrow{u} x''' \text{ with } (x'', x''') \in \sim . \tag{5}$$

Proof: By assumption (4), we have for all $x \in X$, either $[x] \subseteq S$ or $[x] \cap S = \emptyset$.

(if:) Assume $\sim$ satisfies (5). We next prove that $\sim_{\mathsf{Q}}$ is an InitSOP bisimulation relation between Σ and $\Sigma_\sim$.

For each $x_0 \in X_0 \cap S$, we have $[x_0] \in X_{\sim,0} \cap S_\sim$, i.e., 1a) of Definition 10 holds. For each $x_0' \in X_0 \setminus S$, by (4), $x_0' \in X_{\sim,0} \setminus S_\sim$, i.e., 1b) of Definition 10 holds.

For each $[x_0] \in X_{\sim,0} \cap S_\sim$, there exists $x' \in X_0$ satisfying $x_0 \sim x'$; by (4), $x_0 \in S$, then we also have $x' \in S$, i.e., 1c) of Definition 10 holds. Similarly 1d) of Definition 10 holds.

Condition 2) in Definition 10 naturally holds.

For each $x \in X$, we have $(x, [x]) \in \sim_{\mathsf{Q}}$.

If there exists transition $x \xrightarrow{u} x'$ in Σ, then there exists transition $[x] \xrightarrow{u}_\sim [x']$ in $\Sigma_\sim$, and $(x', [x']) \in \sim_{\mathsf{Q}}$, i.e., 3a) in Definition 10 holds.

If there exists transition $[x] \xrightarrow{u}_\sim [x']$ in $\Sigma_\sim$, then there exists transition $x'' \xrightarrow{u} x'''$ in Σ satisfying that $x \sim x''$ and $x' \sim x'''$. By (5), there exists transition $x \xrightarrow{u} x''''$ such that $x''' \sim x''''$, then $x' \sim x''''$ and $(x'''', [x']) \in \sim_{\mathsf{Q}}$, i.e., 3b) in Definition 10 holds, which completes the "if" part.

(only if:) Assume that $\sim_{\mathsf{Q}}$ is an InitSOP bisimulation relation between Σ and $\Sigma_\sim$. Next, we prove (5) holds. For each $(x, x') \in \sim$ and each transition $x \xrightarrow{u} x''$ in Σ, we have $(x, [x']) \in \sim_{\mathsf{Q}}$, and there exists transition $[x'] \xrightarrow{u}_\sim [x''']$ in $\Sigma_\sim$ satisfying $(x'', [x''']) \in \sim_{\mathsf{Q}}$. Then, $(x'', x''') \in \sim$, i.e., (5) holds. ■

D. InfSOP Bisimulation Relations

We have given InitSOP (bi)simulation relation. Next, we study whether InitSOP (bi)simulation relation preserves the other three types of opacity; and if not, we propose new (bi)simulation relations that preserve the other three types of opacity.

Similarly to initial-state opacity, the classical bisimulation relation does not preserve the other three types of opacity. See the NFTSs shown in the proof of Proposition 3.1 (cf., Fig. 2). One can easily verify that Σ_2 in Fig. 2 is not current-state opaque, or K-step opaque for any positive integer K, or infinite-step opaque. However, Σ_1 in Fig. 2 is current-state opaque, K-step opaque for any positive integer K, and infinite-step opaque. In addition, under the relation $\sim = \{(1,1'),(2,2'),(1,3'),(2,4')\}$, Σ_2 bisimulates Σ_1. Hence, the following result holds.

Proposition 3.9: The bisimulation relation (cf., Definition 3) does not preserve current-state opacity, K-step opacity, or infinite-step opacity.

Since all these three types of opacity require that the intruder cannot make sure whether the current state is secret, the previous InitSOP (bi)simulation relation does not suffice to preserve them either. In this section, we strengthen the InitSOP bisimulation relation to make it preserve these three types of opacity.

Definition 11 (InfSOP bisimulation relation): Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called an InfSOP bisimulation relation between Σ_1 and Σ_2 if the following condition holds:

1) for all,
   a) $x_{1,0} \in S_1 \cap X_{1,0}$, there exists $x_{2,0} \in S_2 \cap X_{2,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   b) $x_{1,0} \in X_{1,0} \setminus S_1$, there exists $x_{2,0} \in X_{2,0} \setminus S_2$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   c) $x_{2,0} \in S_2 \cap X_{2,0}$, there exists $x_{1,0} \in S_1 \cap X_{1,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   d) $x_{2,0} \in X_{2,0} \setminus S_2$, there exists $x_{1,0} \in X_{1,0} \setminus S_1$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$,
   a) for every transition $x_1 \xrightarrow{u}_1 x_1' \in S_1$, there exists transition $x_2 \xrightarrow{u}_2 x_2' \in S_2$ such that $(x_1', x_2') \in \sim$;
   b) for every transition $x_1 \xrightarrow{u}_1 x_1' \in X_1 \setminus S_1$, there exists transition $x_2 \xrightarrow{u}_2 x_2' \in X_2 \setminus S_2$ such that $(x_1', x_2') \in \sim$;
   c) for every transition $x_2 \xrightarrow{u}_2 x_2' \in S_2$, there exists transition $x_1 \xrightarrow{u}_1 x_1' \in S_1$ such that $(x_1', x_2') \in \sim$;
   d) for every transition $x_2 \xrightarrow{u}_2 x_2' \in X_2 \setminus S_2$, there exists transition $x_1 \xrightarrow{u}_1 x_1' \in X_1 \setminus S_1$ such that $(x_1', x_2') \in \sim$.

Intuitively, condition 1) ensures that each initial secret (nonsecret) state in Σ_1 has a corresponding initial secret (nonsecret) state in Σ_2 such that they are in the relation, and vice versa; condition 3) guarantees that each transition to a secret (nonsecret) state in Σ_1 has a corresponding transition to a secret (nonsecret) state in Σ_2, and vice versa. Conditions 1) and 3) make bisimulation relation preserve infinite-step opacity, which is shown in the following theorem.

Theorem 3.10: Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. If there exists an InfSOP bisimulation relation $\sim \subseteq X_1 \times X_2$ between Σ_1 and Σ_2, then Σ_1 is infinite-step opaque if and only if Σ_2 is infinite-step opaque.

Proof: Assume there exists an InfSOP bisimulation relation $\sim \subseteq X_1 \times X_2$ between Σ_1 and Σ_2 and system Σ_1 is infinite-step opaque. Now, we show that Σ_2 is also infinite-step opaque.

For system Σ_2, we arbitrarily choose input sequence $\alpha \in U^*$, states $x_{2,0} \in X_{2,0}$ and $x_{2,1}, \ldots, x_{2,|\alpha|} \in X_2$ such that

$$x_{2,0} \xrightarrow{\alpha(0)}_2 x_{2,1} \xrightarrow{\alpha(1)}_2 \cdots \xrightarrow{\alpha(|\alpha|-1)}_2 x_{2,|\alpha|}$$

and $x_{2,l} \in S_2$ for some $l \in [0, |\alpha|]$. Consider an arbitrary $x_{2,i} \in S_2$ in the above-mentioned sequence, where $i \in [0, |\alpha|]$.

By 1c), 1d), 2), 3c), and 3d) of Definition 11, there exist $x_{1,0} \in X_{1,0}$, $x_{1,j} \in X_1$, $j \in [1, |\alpha|]$ such that $x_{1,i} \in S_1$, $h_1(x_{1,k}) = h_2(x_{2,k})$, $k \in [0, |\alpha|]$, and

$$x_{1,0} \xrightarrow{\alpha(0)}_1 x_{1,1} \xrightarrow{\alpha(1)}_1 \cdots \xrightarrow{\alpha(|\alpha|-1)}_1 x_{1,|\alpha|}.$$

Since Σ_1 is infinite-step opaque, there exist $x'_{1,0} \in X_{1,0}$, $x'_{1,j} \in X_1$, $j \in [1, |\alpha|]$ such that $x'_{1,i} \in X_1 \setminus S_1$, $h_1(x_{1,k}) = h_1(x'_{1,k})$, $k \in [0, |\alpha|]$, and

$$x'_{1,0} \xrightarrow{\alpha(0)}_1 x'_{1,1} \xrightarrow{\alpha(1)}_1 \cdots \xrightarrow{\alpha(|\alpha|-1)}_1 x'_{1,|\alpha|}.$$

By 1a), 1b), 2), 3a), and 3b) of Definition 11, there exist $x'_{2,0} \in X_{2,0}$ and $x'_{2,1}, \ldots, x'_{2,|\alpha|} \in X_2$ such that

$$x'_{2,0} \xrightarrow{\alpha(0)}_2 x'_{2,1} \xrightarrow{\alpha(1)}_2 \cdots \xrightarrow{\alpha(|\alpha|-1)}_2 x'_{2,|\alpha|}$$

and $x'_{2,i} \in X_2 \setminus S_2$ and $h_1(x'_{1,k}) = h_2(x'_{2,k})$, $k \in [0, |\alpha|]$. Hence, $h_2(x_{2,j}) = h_2(x'_{2,j})$, $j \in [0, |\alpha|]$, and Σ_2 is infinite-step opaque.

Symmetrically, assume that there exists an InfSOP bisimulation relation $\sim \subseteq X_1 \times X_2$ between Σ_1 and Σ_2 and system Σ_2 is infinite-step opaque, we can prove that Σ_1 is also infinite-step opaque. ■

By the similarity of Definitions 6, 7, and 8, the following corollary follows.

Corollary 3.11: Consider two NTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. If there exists an InfSOP bisimulation relation $\sim \subseteq X_1 \times X_2$ between Σ_1 and Σ_2, then Σ_1 is current-state (resp. K-step) opaque if and only if Σ_2 is current-state (resp. K-step) opaque.

Remark 2: Note that although we add several additional conditions in Definition 11 to make the bisimulation relation preserving these three types of opacity, these conditions are somehow necessary. That is, without some of them, the bisimulation relation may not preserve those notions of opacity any more. Taking the two NFTSs shown in Fig. 2 for example, bisimulation relation $\sim = \{(1', 1), (2', 2), (3', 1), (4', 2)\}$ satisfies 1a), 1c), 1d), 2), 3a), and 3d), but does not satisfy 1b), 3b), or 3c).

Remark 3: Note that since the preservation of infinite-step opacity always requires a bidirectional relation, so we directly study the InfSOP bisimulation relation. A detailed study of relevant notions of (bi)simulation relations for preserving current-state and K-step opacity are left for future investigations.

E. InfSOP Quotient Relations

In this section, we again use the quotient relation from an NTS to its quotient system to implement the InfSOP bisimulation relation.

Theorem 3.12: Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NTS and $\sim \subseteq X \times X$ be an equivalence relation on X satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. Assume that for all $x \in S$ and $x' \in X$, if $(x, x') \in \sim$ then $x' \in S$. Then, $\sim_{\mathsf{Q}}$ is an InfSOP bisimulation relation between Σ and $\Sigma_\sim$ if and only if $\sim$ is an InfSOP bisimulation relation between Σ and itself.

Proof: Similar to Theorem 3.8, by assumption we have for all $x \in X$, either $[x] \subseteq S$ or $[x] \cap S = \emptyset$.

(if:) Assume that $\sim$ is an InfSOP bisimulation relation between Σ and itself. Next, we prove that $\sim_{\mathsf{Q}}$ is also an InfSOP bisimulation relation between Σ and $\Sigma_\sim$ according to Definition 11.

For all $x \in X_0 \cap S$, we have $[x] \in X_{\sim,0} \cap S_\sim$, and $(x, [x]) \in \sim_{\mathsf{Q}}$, i.e., 1a) in Definition 11 holds.

For all $x \in X_0 \setminus S$, by assumption we have $[x] \in X_{\sim,0} \setminus S_\sim$, and $(x, [x]) \in \sim_{\mathsf{Q}}$, i.e., 1b) in Definition 11 holds.

For all $[x] \in X_{\sim,0} \cap S_\sim$, we have $[x] \cap X_0 \neq \emptyset$, and $[x] \subseteq S$, then there exists $\bar{x} \in [x]$ such that $\bar{x} \in X_0 \cap S$, and $(\bar{x}, [x]) \in \sim_{\mathsf{Q}}$, i.e., 1c) in Definition 11 holds.

For all $[x] \in X_{\sim,0} \setminus S_\sim$, we have $[x] \cap X_0 \neq \emptyset$, and $[x] \cap S = \emptyset$, then there exists $\bar{x} \in [x]$ such that $\bar{x} \in X_0 \setminus S$, and $(\bar{x}, [x]) \in \sim_{\mathsf{Q}}$, i.e., 1d) in Definition 11 holds.

Now, consider an arbitrary pair $(\bar{x}, [x]) \in \sim_{\mathsf{Q}}$, i.e., $\bar{x} \sim x$. By definition we have $h(\bar{x}) = h(x) = h_\sim([x])$, i.e., 2) of Definition 11 holds.

Now, consider an arbitrary pair $(\bar{x}, [x]) \in \sim_{\mathsf{Q}}$, i.e., $\bar{x} \in [x]$.

For every transition $\bar{x} \xrightarrow{u} \bar{x}' \in S$, where $u \in U$, we have $[x] \xrightarrow{u}_\sim [\bar{x}'] \in S_\sim$, and $(\bar{x}', [\bar{x}']) \in \sim_{\mathsf{Q}}$, i.e., 3a) in Definition 11 holds.

For every transition $\bar{x} \xrightarrow{u} \bar{x}' \in X \setminus S$, where $u \in U$, we have $[x] \xrightarrow{u}_\sim [\bar{x}'] \in X_\sim \setminus S_\sim$ by assumption, and $(\bar{x}', [\bar{x}']) \in \sim_{\mathsf{Q}}$, i.e., 3b) in Definition 11 holds.

For every transition $[x] \xrightarrow{u}_\sim [x'] \in S_\sim$, where $u \in U$, there exists transition $\hat{x} \xrightarrow{u} \hat{x}' \in S$ such that $\hat{x} \in [x]$ and $\hat{x}' \in [x']$. Since

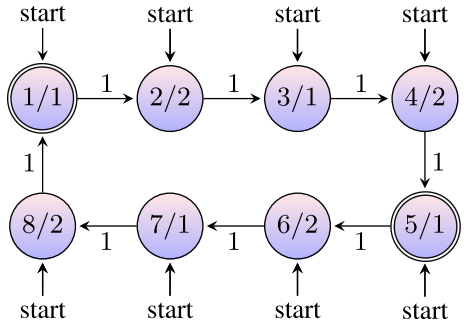

Fig. 6. State transition diagram of the NFTS in Example 3.13.

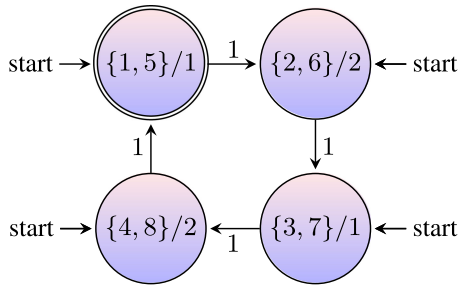

Fig. 7. State transition diagram of the quotient system of the NFTS in Example 3.13 shown in Fig. 6.

$(\bar{x}, \hat{x}) \in\sim$, and $\sim$ is InfSOP, there exists transition $\bar{x} \xrightarrow{u} \bar{x}' \in S$ such that $(\hat{x}', \bar{x}') \in\sim$, hence $(\bar{x}', [x']) \in\sim_{\mathsf{Q}}$, i.e., 3c) in Definition 11 holds.

For every transition $[x] \xrightarrow{u}_{\sim} [x'] \in X_{\sim} \setminus S_{\sim}$, where $u \in U$, there exists transition $\hat{x} \xrightarrow{u} \hat{x}' \in X \setminus S$ such that $\hat{x} \in [x]$ and $\hat{x}' \in [x']$. Since $(\bar{x}, \hat{x}) \in\sim$, and $\sim$ is InfSOP, there exists transition $\bar{x} \xrightarrow{u} \bar{x}' \in X \setminus S$ such that $(\hat{x}', \bar{x}') \in\sim$, hence $(\bar{x}', [x']) \in\sim_{\mathsf{Q}}$, i.e., 3d) in Definition 11 holds. Hence, $\sim_{\mathsf{Q}}$ is InfSOP.

(only if:) Assume that $\sim_{\mathsf{Q}}$ is an InfSOP bisimulation relation between Σ and $\Sigma_{\sim}$. Now, we show that $\sim$ is also an InfSOP bisimulation relation between Σ and itself according to Definition 11. Since $\sim$ is an equivalence relation, we have $(x, x) \in\sim$ for all $x \in X$.

For all $x \in X_0 \cap S$, we have $(x, x) \in\sim$, i.e., 1a) in Definition 11 holds. Similarly, 1b), 1c), and 1d) in Definition 11 hold.

By the definition of $\sim$, we have $h(x_1) = h(x_2)$ for all $(x_1, x_2) \in\sim$. Hence, 2) in Definition 11 holds.

Now, consider an arbitrary pair $(x_1, x_2) \in\sim$.

For every transition $x_1 \xrightarrow{u} x_1' \in S$, where $u \in U$, we have $[x_1] \xrightarrow{u}_{\sim} [x_1'] \in S_{\sim}$. Since $\sim_{\mathsf{Q}}$ is InfSOP, and $(x_2, [x_1]) \in\sim_{\mathsf{Q}}$, there exists transition $x_2 \xrightarrow{u} x_2' \in S$ such that $(x_2', [x_1']) \in\sim_{Q}$, then $(x_1', x_2') \in\sim$, i.e., 3a) in Definition 11 holds.

For every transition $x_1 \xrightarrow{u} x_1' \in X \setminus S$, where $u \in U$, we have $[x_1] \xrightarrow{u}_{\sim} [x_1'] \in X_{\sim} \setminus S_{\sim}$ by assumption. Since $\sim_{\mathsf{Q}}$ is InfSOP, and $(x_2, [x_1]) \in\sim_{\mathsf{Q}}$, there exists transition $x_2 \xrightarrow{u} x_2' \in X \setminus S$ such that $(x_2', [x_1']) \in\sim_{Q}$, then $(x_1', x_2') \in\sim$, i.e., 3b) in Definition 11 holds.

Symmetrically, 3c) and 3d) in Definition 11 hold. Hence, $\sim$ is an InfSOP bisimulation relation between Σ and itself. ■

Example 3.13: Consider NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ shown in Fig. 6, where $X = \{1, 2, 3, 4, 5, 6, 7, 8\} = X_0$, $S = \{1, 5\}$, $U = \{1\}$, $Y = \{1, 2\}$. It can be readily seen that the equivalence relation $\sim = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7), (8,8), (1,5), (5,1), (2,6), (6,2), (3,7), (7,3), (4,8), (8,4)\} \subseteq X \times X$ is an InfSOP bisimulation relation between Σ and itself. Under this relation, the quotient system of Σ is $\Sigma_{\sim} = (X_{\sim}, X_{\sim,0}, S_{\sim}, U, \rightarrow_{\sim}, Y, h_{\sim})$, where $X_{\sim} = X/\sim = X_{\sim,0}$, $X/\sim = \{\{1,5\}, \{2,6\}, \{3,7\}, \{4,8\}\}$, $S_{\sim} = \{\{1,5\}\}$, which is shown in Fig. 7. It can be easily seen that $\Sigma_{\sim}$ is infinite-step opaque. Therefore, the original NFTS Σ is also infinite-step opaque due to the results in Theorem 3.12.

IV. Verification of Opacity of NFTSs Using Two-Way Observers

In Section III, we propose several opacity-preserving (bi)simulation relations, which could be used potentially to verify opacity for a class of infinite NTSs over their finite abstractions. In this section, we show how to verify various notions of opacity for NFTSs by adopting the idea of two-way observer, which was originally proposed in the framework of finite automata [19]. Due to space constraints, all proofs in this section have been omitted and they are available in [22].

Note that the output function $h : X \rightarrow Y$ partitions X into at most $|Y|$ observational equivalence classes. For each $y \in Y$, we denote by $X_y := \{x \in X | h(x) = y\}$ the set of states producing output y and denote by $X_{0,y} := \{x \in X_0 | h(x) = y\}$ the set of initial states producing output y.

Let $q \in 2^X$ be a set of states and $u \in U$ be an input. We denote by $\mathrm{Succ}(q, u)$ the set of states that can be reached from q under input u and by $\mathrm{Pre}(q, u)$ the set of states that can reach q under input u, i.e.,

$$\begin{aligned} \mathrm{Succ}(q, u) &:= \{x \in X | \exists x' \in q \text{ such that } (x', u, x) \in\rightarrow\} \\ \mathrm{Pre}(q, u) &:= \{x \in X | \exists x' \in q \text{ such that } (x, u, x') \in\rightarrow\}. \end{aligned} \tag{6}$$

In order to verify different notions of opacity, we need to compute the set of all possible current-state estimates and the set of all possible initial-state estimates from each current-state estimate. This can be implemented by constructing the product of the observer of the original system (using both state and input information) with the observer of the reversed system.

Formally, for an NFTS $(X, X_0, S, U, \rightarrow, Y, h)$, we define a new so-called verification NFTS (without secret states)

$$\Sigma_V = (X_V, X_{V,0}, U_V, \rightarrow_V, Y_V, h_V) \tag{7}$$

where

1) $X_V \subseteq \{(q_1, q_2) \in 2^X \times 2^X | \exists y_1, y_2 \in Y \text{ such that } q_1 \subseteq X_{y_1} \text{ and } q_2 \subseteq X_{y_2}\}$ is the set of states;
2) $X_{V,0} = \{X_{0,y_1} \in 2^X | y_1 \in Y\} \times \{X_{y_2} \in 2^X | y_2 \in Y\}$ is the set of initial states;
3) $U_V = (U \times \{\epsilon\}) \cup (\{\epsilon\} \times U)$ is the set of inputs;
4) $\rightarrow_V \subseteq X_V \times U_V \times X_V$ is the transition relation defined as follows: For any $(q_1, q_2), (q_1', q_2') \in X_V$ and $u \in U$,
   a) $((q_1, q_2), (u, \epsilon), (q_1', q_2')) \in\rightarrow_V$ if $q_2' = q_2$ and $\exists y \in Y$ such that $q_1' = \mathrm{Succ}(q_1, u) \cap X_y \neq \emptyset$, and
   b) $((q_1, q_2), (\epsilon, u), (q_1', q_2')) \in\rightarrow_V$ if $q_1' = q_1$ and $\exists y \in Y$ such that $q_2' = \mathrm{Pre}(q_2, u) \cap X_y \neq \emptyset$;
5) $Y_V = Y \times Y$ is the set of outputs;
6) $h_V : X_V \rightarrow Y_V$ is defined for each $(q_1, q_2) \in X_V$ as $h_V((q_1, q_2)) = (y_1, y_2)$, where (y_1, y_2) is the unique pair such that $q_1 \subseteq X_{y_1}$ and $q_2 \subseteq X_{y_2}$. Particularly, we denote $h_{V,1}((q_1, q_2)) := y_1$ and $h_{V,2}(q_1, q_2)) := y_2$.

For any given NFTS Σ as in Definition 1, we construct the corresponding NFTS Σ_V as in (7). For any given initial state (q_0^1, q_0^2) of Σ_V in $X_{V,0}$, an input sequence $\alpha = (u_0^1, u_0^2) \dots (u_{|\alpha|-1}^1, u_{|\alpha|-1}^2)$ in $(U_V)^*$, and states $(q_1^1, q_1^2), \dots, (q_{|\alpha|}^1, q_{|\alpha|}^2) \in X_V$ such that

$$(q_0^1, q_0^2) \xrightarrow{(u_0^1, u_0^2)}_V \cdots \xrightarrow{(u_{|\alpha|-1}^1, u_{|\alpha|-1}^2)}_V (q_{|\alpha|}^1, q_{|\alpha|}^2) \tag{8}$$

we have that the left component $q_0^1 \xrightarrow{u_0^1}_V \cdots \xrightarrow{u_{|\alpha|-1}^1}_V q_{|\alpha|}^1$ aggregates all runs of Σ starting from some initial state of q_0^1 over $u_0^1 \dots u_{|\alpha|-1}^1$ and producing the output sequence $h_{V,1}((q_0^1, q_0^2)) \dots h_{V,1}((q_{|\alpha|}^1, q_{|\alpha|}^2))$

(note that repetition of states of the form $x \xrightarrow{\epsilon} x$ may exist), and the right component $q_0^2 \xrightarrow{u_0^2}_V \cdots \xrightarrow{u_{|\alpha|-1}^2}_V q_{|\alpha|}^2$ aggregates the mirror images of all runs of Σ ending at some state of q_0^2 over $u_{|\alpha|-1}^2 \ldots u_0^2$ and producing the output sequence $h_{V,2}((q_{|\alpha|}^1, q_{|\alpha|}^2)) \ldots h_{V,2}((q_0^1, q_0^2))$ (note that repetition of states of the form $x \xrightarrow{\epsilon} x$ may also exist). Hence, $q_{|\alpha|}^1 \cap q_{|\alpha|}^2$ is the set of all states of maximal runs in the original NFTS over input sequence $u_0^1 \ldots u_{|\alpha|-1}^1 u_{|\alpha|-1}^2 \ldots u_0^2$ between $u_{|\alpha|-1}^1$ and $u_{|\alpha|-1}^2$ with the same observation sequence. Based on this direct observation and preliminary definitions, the following proposition holds.

Proposition 4.1: For NFTS (7), for any input sequence $\alpha = (u_0^1, u_0^2) \ldots (u_{|\alpha|-1}^1, u_{|\alpha|-1}^2) \in U_V^*$, and any transitions

$$(q_0^1, q_0^2) \xrightarrow{(u_0^1, u_0^2)}_V \cdots \xrightarrow{(u_{|\alpha|-1}^1, u_{|\alpha|-1}^2)}_V (q_{|\alpha|}^1, q_{|\alpha|}^2)$$

where $(q_0^1, q_0^2) \in X_{V,0}$, we have

1) $q_{|\alpha|}^1 = \{x_{|\alpha|} \in X | \exists x_0 \in q_0^1$ such that $x_0 \xrightarrow{u_0^1} \cdots \xrightarrow{u_{|\alpha|-1}^1} x_{|\alpha|}$ and $\forall i \in [0, |\alpha|], h(x_i) = h_{V,1}((q_i^1, q_i^2))\}$;
2) $q_{|\alpha|}^2 = \{x_0 \in X | \exists x_{|\alpha|} \in q_0^2$ such that $x_0 \xrightarrow{u_{|\alpha|-1}^2} \cdots \xrightarrow{u_0^2} x_{|\alpha|}$ and $\forall i \in [0, |\alpha|], h(x_{|\alpha|-i}) = h_{V,2}((q_i^1, q_i^2))\}$.

By Proposition 4.1, we obtain the following four theorems used for verifying the four types of opacity for NFTSs.

Theorem 4.2: NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ is current-state opaque if and only if $\forall (q^1, q^2) \in X_V, q^1 \not\subseteq S$.

Theorem 4.3: NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ is initial-state opaque if and only if $\forall (q^1, q^2) \in X_V, q^2 \cap X_0 \neq \emptyset \Rightarrow q^2 \cap X_0 \not\subseteq S$.

Theorem 4.4: NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ is infinite-step opaque if and only if $\forall (q^1, q^2) \in X_V, q^1 \cap q^2 \neq \emptyset \Rightarrow q^1 \cap q^2 \not\subseteq S$.

Theorem 4.5: NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ is K-step opaque if and only if, for any $x_{V,0} \in X_{V,0}$ and any sequence $x_{V,0} \xrightarrow{(u_0^1, u_0^2) \ldots (u_{n-1}^1, u_{n-1}^2)}_V (q^1, q^2)$ such that $|u_0^2 \ldots u_{n-1}^2| \leq K$, we have $q^1 \cap q^2 \neq \emptyset \Rightarrow q^1 \cap q^2 \not\subseteq S$.

Remark 4: Let us discuss the complexity for the verifications of notions of opacity using the above-mentioned theorems. In the worst case, Σ_V contains at most $4^{|X|}$ states and $2|Y||U|4^{|X|}$ transitions. Also, we note that Σ_V is a pure shuffle in the sense that its first and its second components are independent. Therefore, to verify current-state opacity (respectively, initial-state opacity), we just need to construct the first component (respectively, the second component) of Σ_V. Hence, the time complexity for the verifications of current-state opacity and initial-state opacity are both $O(|Y||U|2^{|X|})$. To verify infinite-step opacity, however, we need to construct automaton Σ_V completely for both components. Hence, the complexity is $O(|Y||U|4^{|X|})$. To verify K-step opacity, we need to construct parts of Σ_V that can be reached from initial states within K-steps in the second component. Therefore, the complexity for verifying K-step opacity is $O(\min\{2^{|X|}, (|U||Y|)^K\}|U||Y|2^{|X|})$.

V. Conclusion

In this paper, we proposed new notions of initial-state and infinite-step opacity-preserving (bi)simulation relations from an NTS to another NTS, and used the quotient system construction to potentially compute such relations. Hence, although the verification of opacity of NTSs is generally undecidable, if we find such a relation between an NTS and an NFTS, we can verify the opacity (or lack of opacity) of the NTS over the NFTS, which is decidable. A detailed study of relevant notions of (bi)simulation relations for preserving current-state and K-step opacity are left for future investigations.

Although the construction of proposed relations here based on quotient systems can be used to deal with some classes of NTSs, generally it is not easy to check the existence of appropriate quotient relations implementing them. So in order to make these opacity-preserving (bi)simulation relations applicable to more classes of NTSs, e.g., nonlinear control systems, further works on different algorithms on the construction of NFTSs for NTSs deserve more attention.

References

[1] C. Baier and J. P. Katoen, *Principles of Model Checking*. Cambridge, MA, USA: MIT Press, 2008.

[2] J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. A. Ryan, "Opacity generalised to transition systems," *Int. J. Inf. Secur.*, vol. 7, no. 6, pp. 421–435, Nov. 2008.

[3] S. Chédor, C. Morvan, S. Pinchinat, and H. Marchand, "Diagnosis and opacity problems for infinite state systems modeled by recursive tile systems," *Discrete Event Dyn. Syst.*, vol. 25, no. 1/2, pp. 271–294, 2014.

[4] A. Girard and G. J. Pappas, "Approximation metrics for discrete and continuous systems," *IEEE Trans. Autom. Control*, vol. 52, no. 5, pp. 782–798, May 2007.

[5] Y. Ji, X. Yin, and S. Lafortune, "Opacity enforcement using nondeterministic publicly-known edit functions," *IEEE Trans. Autom. Control*, 2019.

[6] M. Kloetzer and C. Belta, "A fully automated framework for control of linear systems from temporal logic specifications," *IEEE Trans. Autom. Control*, vol. 53, no. 1, pp. 287–297, Feb. 2008.

[7] K. Kobayashi and K. Hiraishi, "Verification of opacity and diagnosability for pushdown systems," *J. Appl. Math.*, vol. 2013, 2013, Art. no. 654059.

[8] H. Lin and P. J. Antsaklis, "Hybrid dynamical systems: An introduction to control and verification," *Found. Trends Syst. Control*, vol. 1, no. 1, pp. 1–172, 2014.

[9] L. Mazaré, "Using unification for opacity properties," in *Proc. Workshop Issues Theory Secur.*, 2004, pp. 165–176.

[10] A. Saboori and C. N. Hadjicostis, "Notions of security and opacity in discrete event systems," in *Proc. 46th IEEE Conf. Decis. Control*, Dec. 2007, pp. 5056–5061.

[11] A. Saboori and C. N. Hadjicostis, "Verification of K-step opacity and analysis of its complexity," *IEEE Trans. Autom. Sci. Eng.*, vol. 8, no. 3, pp. 549–559, Jul. 2011.

[12] A. Saboori and C. N. Hadjicostis, "Verification of infinite-step opacity and complexity considerations," *IEEE Trans. Autom. Control*, vol. 57, no. 5, pp. 1265–1269, May 2012.

[13] A. Saboori and C. N. Hadjicostis, "Verification of initial-state opacity in security applications of discrete event systems," *Inf. Sci.*, vol. 246, pp. 115–132, 2013.

[14] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*, 1st ed. New York, NY, USA: Springer, 2009.

[15] S. Takai and Y. Oka, "A formula for the supremal controllable and opaque sublanguage arising in supervisory control," *SICE J. Control, Measu. Syst. Integration*, vol. 1, no. 4, pp. 307–311, 2008.

[16] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Current-state opacity enforcement in discrete event systems under incomparable observations," *Discrete Event Dyn. Syst., Theory Apl.*, vol. 28, pp. 161–182, Jun. 2018.

[17] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Decidability of opacity verification problems in labeled Petri net systems," *Automatica*, vol. 80, pp. 48–53, 2017.

[18] X. Yin and S. Lafortune, "A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems," *IEEE Trans. Autom. Control*, vol. 61, no. 8, pp. 2140–2154, Aug. 2016.

[19] X. Yin and S. Lafortune, "A new approach for the verification of infinite-step and K-step opacity using two-way observers," *Automatica*, vol. 80, pp. 162–171, 2017.

[20] M. Zamani, G. Pola, M. Mazo, and P. Tabuada, "Symbolic models for nonlinear control systems without stability assumptions," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1804–1809, Jul. 2012.

[21] B. Zhang, S. Shu, and F. Lin, "Maximum information release while ensuring opacity in discrete event systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 12, no. 4, pp. 1067–1079, Jul. 2015.

[22] K. Zhang, X. Yin, and M. Zamani, "Opacity of nondeterministic transition systems: A (bi)simulation relation approach," 2018. [Online]. Available: https://arxiv.org/abs/1802.03321

[23] K. Zhang and M. Zamani, "Infinite-step opacity of nondeterministic finite transition systems: A bisimulation relation approach," in *Proc. 56th IEEE Conf. Decis. Control*, Dec. 2017, pp. 5615–5619.