Abstraction-Based Verification of Approximate Preopacity for Control Systems

Junyao Hou, Siyuan Liu, *Graduate Student Member, IEEE*, Xiang Yin, *Member, IEEE*, and Majid Zamani, *Senior Member, IEEE*

***Abstract*—In this letter, we consider the problem of verifying pre-opacity for discrete-time control systems. Pre-opacity is an important information-flow security property that secures the intention of a system to execute some secret behaviors in the future. Existing works on pre-opacity only consider non-metric discrete systems, where it is assumed that intruders can distinguish different output behaviors precisely. However, for continuous-space control systems whose output sets are equipped with metrics (which is the case for most real-world applications), it is too restrictive to assume precise measurements from outside observers. In this letter, we first introduce a concept of approximate pre-opacity by capturing the security level of control systems with respect to the measurement precision of the intruder. Based on this new notion of pre-opacity, we propose a verification approach for continuous-space control systems by leveraging abstraction-based techniques. In particular, a new concept of approximate pre-opacity preserving simulation relation is introduced to characterize the distance between two systems in terms of preserving pre-opacity. This new system relation allows us to verify pre-opacity of complex continuous-space control systems using their finite abstractions. We also present a method to construct pre-opacity preserving finite abstractions for a class of discrete-time control systems under certain stability assumptions.**

***Index Terms*—Discrete event systems, opacity, formal abstractions.**

Manuscript received 14 September 2022; revised 17 November 2022; accepted 7 December 2022. Date of publication 20 December 2022; date of current version 4 January 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62061136004, Grant 62173226, and Grant 61833012; in part by the German Research Foundation under Grant ZA 873/7-1; and in part by the National Science Foundation under Grant ECCS-2015403. Recommended by Senior Editor C. Seatzu. *(Junyao Hou and Siyuan Liu contributed equally to this work.) (Corresponding author: Xiang Yin.)*

Junyao Hou and Xiang Yin are 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).

Siyuan Liu is with the Department of Electrical and Computer Engineering, Technical University of Munich, 85737 Ismaning, Germany, and also with the Department of Computer Science, Ludwig Maximilian University of Munich, 80539 Munich, Germany.

Majid Zamani is with the Department of Computer Science, Ludwig Maximilian University of Munich, 80539 Munich, Germany, and also with the Department of Computer Science, University of Colorado Boulder, Boulder, CO 80309 USA.

Digital Object Identifier 10.1109/LCSYS.2022.3230770

I. Introduction

CYBER-PHYSICAL systems (CPS) are the technological backbone of the increasingly interconnected and smart world where security vulnerability can be catastrophic. However, the tight interaction between embedded control software and the physical environment in CPS may expose numerous attack surfaces for malicious exploitation. In the last decade, the analysis of various security properties for CPS has drawn considerable attention in the literature [3], [9]. The concept of opacity was originally introduced in computer science literature [11] for the analysis of cryptographic protocols. Afterwards, opacity was widely investigated in the domain of discrete-event systems (DES) since it allows researchers to analyze the information-flow security for dynamical systems in a formal way [6]. Roughly speaking, opacity is a confidentiality property that characterizes whether or not a dynamical system will reveal some potentially sensitive behavior to an external malicious observer (intruder) based on the information flow.

In the past decades, different notions of opacity were proposed in the literature to capture different security requirements in the context of DES, including language-based notions in [8] and state-based notions in [7], [12], [13]. The recent results in [2], [15] show that these notions are transformable to each other. Corresponding to the different opacity notions, various verification and synthesis approaches were also developed in the DES literature; see [5], [6], [8], [9], [10] and the references therein. Although the majority of the above-mentioned works on opacity are applied to DES models with discrete state sets, the analysis of opacity for control systems with continuous state sets has become the subject of many studies recently [1], [9], [17]. In particular, a new concept of *approximate opacity* is proposed in [17] which is more applicable to control systems since it allows us to quantitatively evaluate the security level of control systems whose outputs are physical signals. More recently, a new concept of opacity, called *pre-opacity*, was proposed in [16] to characterize whether or not the secret intention of the system can be revealed. In other words, different from the other opacity notions which consider the current or past secret behaviors of the system, pre-opacity captures whether or not an outside observer can be prematurely certain that the system will conduct some secret behaviors in the future. In fact, in many practical scenarios, systems are indeed more interested in hiding their

intentions to do something particularly important in the future. Nevertheless, the results developed in [16] are again tailored to DES models with discrete state sets, which prevents it from being applied to real-world CPS with continuous state sets.

Our contribution. In this letter, we consider the problem of verifying pre-opacity for discrete-time control systems. Motivated by the limitations of the results in [16], we first introduce a new concept called *approximate K-step pre-opacity* which is more applicable to control systems. To be more specific, unlike discrete-event systems whose state sets are discrete and outputs are logic events, control systems are in general metric systems whose state and output sets are physical signals. Therefore, the notion of pre-opacity in [16] is too restrictive by assuming that one can always precisely distinguish between two outputs in the context of control systems. Note that the verification of pre-opacity for control systems is in general undecidable. In this letter, we propose an abstraction-based pre-opacity verification approach for continuous-space control systems. In particular, we first propose a notion of *approximate K-step pre-opacity preserving simulation relation*, which is a system relation that can be used to characterize the closeness between two systems in terms of preserving pre-opacity. Based on this system relation, one can verify pre-opacity of a complex control system using its finite abstraction, instead of directly applying verification algorithms on the original control system which is undecidable. Moreover, for the class of incrementally input-to-state stable nonlinear control systems, we show that one can always construct finite abstractions which preserve pre-opacity of the control systems. The proposed abstraction-based methodology is the first in the literature that provides a sound way for verifying pre-opacity of discrete-time control systems with continuous state spaces.

II. Preliminaries

A. Notation

We denote by $\mathbb{N}$ and $\mathbb{R}$ the set of non-negative integers and real numbers, respectively. They are annotated with subscripts to restrict them in the usual way, e.g., $\mathbb{R}_{\geq 0}$ denotes the set of non-negative real numbers. Given a vector $x \in \mathbb{R}^n$, we denote by $\|x\|$ the infinity norm of x. A set $B \subseteq \mathbb{R}^m$ is called a *box* if $B = \prod_{i=1}^{m} [c_i, d_i]$, where $c_i, d_i \in \mathbb{R}$ with $c_i < d_i$ for each $i \in \{1, \ldots, m\}$. For any set $A = \bigcup_{j=1}^{M} A_j$ of the form of finite uion of boxes, where $A_j = \prod_{i=1}^{n} [c_i^j, d_i^j]$, we define $span(A) = \min\{span(A_j) | j = 1, \ldots, M\}$, where $span(A_j) = \min\{|d_i^j - c_i^j| | i = 1, \ldots, m\}$. For any $\mu \leq span(A)$, define $[A]_\mu = \bigcup_{j=1}^{M} [A_j]_\mu$, where $[A_j]_\mu = [\mathbb{R}^m]_\mu \cap A_j$ and $[\mathbb{R}^m]_\mu = \{a \in \mathbb{R}^m | a_i = k_i \mu, k_i \in \mathbb{Z}, i = 1, \ldots, m\}$. We denote the different classes of comparison functions by $\mathcal{K}$, $\mathcal{K}_\infty$ and $\mathcal{KL}$, where $\mathcal{K} = \{\gamma : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : \gamma \text{ is continuous, strictly increasing and } \gamma(0) = 0\}$; $\mathcal{K}_\infty = \{\gamma \in \mathcal{K} : \lim_{r \to \infty} \gamma(r) = \infty\}$; $\mathcal{KL} = \{\beta : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} : \text{ for each fixed } s, \text{ the map } \beta(r, s) \text{ belongs to class } \mathcal{K} \text{ with respect to } r \text{ and, for each fixed nonzero } r, \text{ the map } \beta(r, s) \text{ is decreasing with respect to } s \text{ and } \beta(r, s) \to 0 \text{ as } s \to \infty\}$.

B. System Model

In this letter, the system model that can be used to describe both continuous-space and finite control systems is a *tuple*

$$S = (X, X_0, U, \longrightarrow, Y, H),$$

where X is a (possibly infinite) set of states, $X_0 \subseteq X$ is a (possibly infinite) set of initial states, U is a (possibly infinite) set of inputs, $\longrightarrow \subseteq X \times U \times X$ is a transition relation, Y is a (possibly infinite) set of outputs, and $H : X \to Y$ is the output function. For the sake of simplicity, we also denote a transition $(x, u, x') \in \longrightarrow$ by $x \xrightarrow{u} x'$, where we say that x' is a u-successor, or simply successor, of x. For each state $x \in X$, we denote by $U(x)$ the set of all inputs defined at x, i.e., $U(x) = \{u \in U : \exists x' \in X \text{ s.t. } x \xrightarrow{u} x'\}$, and by $U_u^{post}(x)$ the set of u-successors of state x. A system S is said to be

- *metric*, if the output set Y is equipped with a metric $\mathbf{d} : Y \times Y \to \mathbb{R}_{\geq 0}$;
- *finite* (or *symbolic*), if X and U are finite sets;

A finite state run of a system S generated from initial state $x_0 \in X_0$ under input sequence $u_1, \ldots, u_n$ is a sequence of transitions $x_0 \xrightarrow{u_1} x_1 \xrightarrow{u_2} \cdots \xrightarrow{u_n} x_n$, where $x_i \xrightarrow{u_{i+1}} x_{i+1}$ for all $0 \leq i \leq n-1$. The corresponding output run is a sequence of outputs $H(x_0)H(x_1)\cdots H(x_n)$.

C. Exact Pre-Opacity

In many scenarios, the system wants to hide its intention to reach some *secret* states at some future instants in the presence of a malicious intruder (outside observer). In this letter, we adopt a state-based formulation of secrets. Specifically, we assume that $X_S \subseteq X$ is a set of secret states. In the sequel, we incorporate the secret state set X_S in the system definition and use $S = (X, X_0, X_S, U, \longrightarrow, Y, H)$ to denote a metric system. We consider that the intruder knows the dynamics of the system and can observe the output sequences of the system, but cannot actively affect the behavior of the system. To characterize whether or not the secret intention of a system can be revealed, a notion of K-step pre-opacity is proposed in [16] and recalled as follows.

Definition 1: Consider a system $S = (X, X_0, X_S, U, \longrightarrow, Y, H)$ and a constant $K \in \mathbb{N}$. We say that S is *K-step pre-opaque* if for any finite sequence $x_0 \xrightarrow{u_1} x_1 \xrightarrow{u_2} \cdots \xrightarrow{u_n} x_n$, any non-negative integer $t \geq K$, there exist a finite sequence $x_0' \xrightarrow{u_1'} x_1' \xrightarrow{u_2'} \cdots \xrightarrow{u_n'} x_n' \xrightarrow{u_n'} \cdots \xrightarrow{u_{n+t}'} x_{n+t}'$ such that

$$H(x_i) = H(x_i'), \forall i = \{0, \ldots, n\},$$

and $x_{n+t}' \notin X_S$.

Intuitively, pre-opacity requires that the intruder can never predict that the system will visit a secret state for some specific future instant. The above definition of K-step pre-opacity requires that for any behavior of the system and any $t \geq K$, there exists a behavior whose prefix generates *exactly* the same output and will reach a non-secret state in exact t steps. Thus, in the remainder part of this letter, we will refer to this definition as *exact pre-opacity*. Interested readers are referred to [16, Sec. V] for an illustrative example on the application of exact pre-opacity. A detailed discussion on the relationships

between pre-opacity and other notions of opacity can be found in [16, Fig. 3].

D. Approximate Pre-Opacity

The notion of exact pre-opacity introduced in the previous subsection essentially assumes that the intruder can always measure each output or distinguish between two different outputs precisely. However, for metric systems whose outputs are physical signals, due to the imperfect measurement precision of potential outside observers (which is the case for almost every physical system), it is very difficult to distinguish two observations if their difference is very small. Therefore, in the following definition, we propose a "weak" and "robust" version of pre-opacity called *δ-approximate pre-opacity* which is more applicable to metric systems.

Definition 2: Consider a system $S = (X, X_0, X_S, U, \longrightarrow, Y, H)$ and a constant $\delta \in \mathbb{R}_{\geq 0}$. We say that S is *δ-approximate K-step pre-opaque* if for any finite sequence $x_0 \xrightarrow{u_1} x_1 \xrightarrow{u_2} \cdots \xrightarrow{u_n} x_n$, any non-negative integer $t \geq K$, there exist a finite sequence $x'_0 \xrightarrow{u'_1} x'_1 \xrightarrow{u'_2} \cdots \xrightarrow{u'_n} x'_n \xrightarrow{u'_n} \cdots \xrightarrow{u'_{n+t}} x'_{n+t}$ such that

$$\max_{i\in\{0,\ldots,n\}} \mathbf{d}(H(x_i), H(x'_i)) \leq \delta,$$

and $x'_{n+t} \notin X_S$.

When $\delta = 0$, approximate pre-opacity boils down to the exact version in Definition 1. We use the following example to illustrate the notions of exact and approximate pre-opacity.

Example 1: Consider system $S = (X, X_0, X_S, U, \longrightarrow, Y, H)$ shown in Figure 1, where $X = \{A, B, C, D, E, F, G, H\}$, $X_0 = \{A, E\}$, $X_S = \{C, H\}$, $U = \{u, u'\}$, $Y = \{1.1, 1.2, 2.1, 2.3, 2.9, 3.1, 4.0, 4.2\} \subseteq \mathbb{R}$ equipped with metric $\mathbf{d}$ defined by $\mathbf{d}(y_1, y_2) = |y_1 - y_2|$, $\forall y_1, y_2 \in Y$. We mark all secret states by red and the output of each state is specified by a value associated to it. First, one can check that S is not exact K-step pre-opaque for any $K \in \mathbb{N}$, since we know immediately that the system is at secret state when value 3.1 or 4.0 is observed. Next, consider an intruder with measurement precision $\delta = 0.2$. We claim that S is 0.2-approximate 1-step pre-opaque. For example, consider a finite path $A \xrightarrow{u} B$ which generates output path [1.1][2.3] and will reach a secret state in 1 step. However, the intruder cannot predict for sure that the system will be at a secret state in 1 step since there is another path $E \xrightarrow{u} F$ generating an indistinguishable output path[1.2][2.1], but will reach a non-secret state $G \notin X_S$. Similarly, when observing [1.2][2.1] (generated by the finite path $E \xrightarrow{u} F$), the intruder cannot predict for sure that the system will be at a secret state after 2 steps either, since there exists another path $A \xrightarrow{u} B \xrightarrow{u} C \xrightarrow{u} D$ which will reach non-secret state D in 2 steps. This protects the possible secret intention of executing $E \xrightarrow{u} F \xrightarrow{u} G \xrightarrow{u} H$.

III. Approximate Simulation Relation for K-Step Pre-Opacity

In the last section, we introduced notions of exact and approximate pre-opacity for control systems. However, the (approximate) pre-opacity is in general hard (or even infeasible) to check for control systems since there is no systematic way in the literature to check pre-opacity for systems with infinite state sets so far. On the other hand, existing tools and algorithms (such as [16]) in DES literature can be leveraged to check pre-opacity for finite systems. Therefore, to solve the pre-opacity verification problem for control systems, it would be more feasible to verify pre-opacity on their finite abstractions and then carry back the result to the concrete ones. The key to the construction of such finite abstraction is the establishment of formal relations between the concrete and abstract systems.

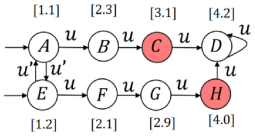


Fig. 1. Example to illustrate δ-approximate K-step pre-opacity.

In this section, we first propose a new system relation called *approximate K-step pre-opacity preserving simulation relation*, and then show the usefulness of the proposed system relation in terms of verifying pre-opacity.

Definition 3 (Approximate K-step Pre-Opacity Preserving Simulation Relation): Consider two metric systems $S_a = (X_a, X_{a0}, X_{aS}, U_a, \xrightarrow[a]{}, Y_a, H_a)$ and $S_b = (X_b, X_{b0}, X_{bS}, U_b, \xrightarrow[b]{}, Y_b, H_b)$ with the same output sets $Y_a = Y_b$ and metric $\mathbf{d}$. Given $\varepsilon \in \mathbb{R}_{\geq 0}$, a relation $R \subseteq X_a \times X_b$ is called an ε-approximate K-step pre-opacity preserving simulation relation (ε-AKP simulation relation) from S_a to S_b if

1) a) $\forall x_{a0} \in X_{a0}, \exists x_{b0} \in X_{b0} : (x_{a0}, x_{b0}) \in R$;
   b) $\forall x_{b0} \in X_{b0}, \exists x_{a0} \in X_{a0} : (x_{a0}, x_{b0}) \in R$;
2) $\forall (x_a, x_b) \in R : \mathbf{d}(H_a(x_a), H_b(x_b)) \leq \varepsilon$;
3) For any $(x_a, x_b) \in R$, we have
   a) $\forall x_a \xrightarrow[a]{u_a} x'_a, \exists x_b \xrightarrow[b]{u_b} x'_b : (x'_a, x'_b) \in R$;
   b) $\forall x_b \xrightarrow[b]{u_b} x'_b, \exists x_a \xrightarrow[a]{u_a} x'_a : (x'_a, x'_b) \in R$.
   c) $\forall x_b \xrightarrow[b]{u_b} x'_b \in X_b \backslash X_{bS}, \exists x_a \xrightarrow[a]{u_a} x'_a \in X_a \backslash X_{aS} : (x'_a, x'_b) \in R$.

We say that S_a is ε-AKP simulated by S_b, denoted by $S_a \preceq^{\varepsilon}_A S_b$, if there exists an ε-AKP simulation relation R from S_a to S_b. A (finite) system S_b that simulates S_a through the ε-AKP simulation relation is called a pre-opacity preserving (finite) abstraction of S_a. Note that the proposed ε-AKP simulation relation is still a one-sided relation because conditions 1) and 3) are asymmetric.

The following theorem shows how to use the above proposed simulation relation in terms of verifying pre-opacity.

Theorem 1: Consider two metric systems $S_a = (X_a, X_{a0}, X_{aS}, U_a, \xrightarrow[a]{}, Y_a, H_a)$ and $S_b = (X_b, X_{b0}, X_{bS}, U_b, \xrightarrow[b]{}, Y_b, H_b)$ with the same output sets $Y_a = Y_b$ and metric $\mathbf{d}$ and let $\varepsilon, \delta \in \mathbb{R}_{\geq 0}$. If $S_a \preceq^{\varepsilon}_A S_b$, then we have:

$$S_b \text{ is } \delta\text{-approximate } K\text{-step pre-opaque}$$
$$\Rightarrow S_a \text{ is } (\delta + 2\varepsilon)\text{-approximate } K\text{-step pre-opaque.}$$

Proof: Let us consider an arbitrary initial state $x_0 \in X_{a0}$, an arbitrary finite run $x_0 \xrightarrow[a]{u_1} x_1 \xrightarrow[a]{u_2}, \ldots \xrightarrow[a]{u_n} x_n$ in S_a, and any non-negative integer $t \geq K$. Since $S_a \preceq^{\varepsilon}_A S_b$, by conditions 1)-a), 2) and 3)-a) in Definition 3, there exists an initial state

$x'_0 \in X_{b0}$ and a finite run $x'_0 \xrightarrow[b]{u'_1} x'_1 \xrightarrow[b]{u'_2} \cdots \xrightarrow[b]{u'_n} x'_n$ in S_b such that

$$\forall i \in \{0, \ldots, n\} : \mathbf{d}(H_a(x_i), H_b(x'_i)) \leq \varepsilon. \tag{1}$$

Since S_b is δ-approximate K-step pre-opaque, by Definition 2, for any non-negative integer $t \geq K$, there exist an initial state $x''_0 \in X_{b0}$ and a finite run $x''_0 \xrightarrow[b]{u''_1} x''_1 \xrightarrow[b]{u''_2} \cdots \xrightarrow[b]{u''_n} x''_n \xrightarrow[b]{u''_n} x''_{n+1} \cdots \xrightarrow[b]{u''_{n+t}} x''_{n+t}$ such that $x''_{n+t} \in X_b \backslash X_{bS}$ and

$$\max_{i \in \{0,\ldots,n\}} \mathbf{d}(H_b(x'_i), H_b(x''_i)) \leq \delta. \tag{2}$$

Again, since $S_a \preceq^{\varepsilon}_A S_b$, by conditions 1)-b), 2), 3)-b) and 3)-c) in Definition 3, there exists an initial state $x'''_0 \in X_{a0}$ and a finite run $x'''_0 \xrightarrow[a]{u'''_1} x'''_1 \xrightarrow[a]{u'''_2} \cdots \xrightarrow[a]{u'''_n} x'''_n \xrightarrow[a]{u'''_n} x'''_{n+1} \cdots \xrightarrow[a]{u'''_{n+t}} x'''_{n+t}$ such that $x'''_{n+t} \in X_a \backslash X_{aS}$ and

$$\forall i \in \{0, \ldots, n+t\} : \mathbf{d}(H_a(x'''_i), H_b(x''_i)) \leq \varepsilon. \tag{3}$$

Combining inequalities (1), (2), (3), and using the triangle inequality, we have

$$\max_{i \in \{0,\ldots,n\}} \mathbf{d}(H_a(x_i), H_a(x'''_i)) \leq \delta + 2\varepsilon. \tag{4}$$

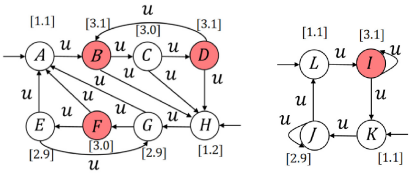
Since $x_0 \in X_{a0}$ and $x_0 \xrightarrow[a]{u_1} x_1 \xrightarrow[a]{u_2} \cdots \xrightarrow[a]{u_n} x_n$ are arbitrary, we conclude that S_a is $(\delta + 2\varepsilon)$-approximate K-step pre-opaque. ■

We should mention that, essentially, Theorem 1 provides us with a sufficient but not necessary condition for verifying pre-opacity of control systems using abstraction-based techniques. In particular, when encountered with a complex control system S_a (possibly with infinite state set), one can build a finite abstraction S_b for S_a through the proposed ε-AKP simulation relation. Then, one can verify pre-opacity of the finite abstraction S_b leveraging existing algorithms in DES literature, and then carry back the verification result to the concrete system S_a by employing the result obtained in Theorem 1. Note that such δ and ε are parameters that specify two different types of precision. The parameter δ is used to specify the intruder's measurement precision under which one can guarantee pre-opacity of a single system, whereas ε appeared in the proposed ε-AKP simulation relation is used to describe the "distance" between two systems in terms of preserving pre-opacity.

Remark 1: In order to verify δ-approximate K-step pre-opacity for finite systems, one can combine techniques in [16] and [17]. Specifically, one can first construct the δ-approximate current-state estimator as defined in [17], and then use the reachability analysis provided in [16] to check pre-opacity. The reader is referred to [4, Sec. III] for more details about how these two techniques can be combined.

We illustrate the newly proposed ε-AKP simulation relation and the preservation of pre-opacity between two related finite systems by the following example.

Example 2: Consider systems S_a and S_b shown in Figures 2(a) and 2(b), respectively. All secret states are marked by red and the output of each state is specified by the value associated to it. Let us consider the following relation $R = \{(A, L), (B, I), (C, I), (D, I), (E, J), (F, J), (G, J), (H, K)\}$. We claim



(a) S_a (b) S_b

Fig. 2. Example of ε-approximate 0-step pre-opacity preserving simulation relation.

that R is an ε-approximate K-step pre-opacity preserving simulation relation from S_a to S_b when $\varepsilon = 0.1$. First, for both initial states A and H in S_a, we have $L, K \in X_{b0}$ in S_b such that $(A, L) \in R$ and $(H, K) \in R$. Thus, condition 1) in Definition 3 holds. Also, one can check that $\mathbf{d}(H_a(x_a), H_b(x_b)) \leq 0.1$ for any $(x_a, x_b) \in R$. Therefore, condition 2) in Definition 3 holds. Moreover, one can check that conditions 3)-a) and 3)-b) in Definition 3 hold as well. For example, for $(B, I) \in R$ and $B \xrightarrow[a]{u} C$, we can choose $I \xrightarrow[b]{u} I$ such that $(C, I) \in R$. Finally, condition 3)-c) in Definition 3 is also satisfied. As an example, for $(H, K) \in R$ and the transition $K \xrightarrow[b]{u} J \in X_b \backslash X_{bS}$ in S_b, there exists a transition $H \xrightarrow[b]{u} G \in X_a \backslash X_{aS}$ in S_a such that $(G, J) \in R$. Therefore, one can conclude that R is an ε-AKP simulation relation from S_a to S_b, i.e., $S_a \preceq^{0.1}_A S_b$. Furthermore, it can be seen that S_b is δ-approximate 0-step pre-opaque with $\delta = 0.2$. Therefore, according to Theorem 1, we can readily conclude that S_a is 0.4-approximate 0-step pre-opaque, where $0.4 = \delta + 2\varepsilon$, without applying any verification algorithm to S_a directly.

IV. Pre-Opacity of Control Systems

In this section, we proceed to investigate how to construct pre-opacity preserving finite abstractions for control systems. In particular, we show that for a class of discrete-time control systems under certain stability assumptions, one can build finite abstractions which preserve pre-opacity of the concrete control systems under the proposed ε-AKP simulation relation.

A. Discrete-Time Control Systems

In this section, we consider a class of discrete-time control systems of the following form.

Definition 4: A discrete-time control system Σ is defined by the tuple $\Sigma = (\mathbb{X}, \mathbb{S}, \mathbb{U}, f, \mathbb{Y}, h)$, where $\mathbb{X}$, $\mathbb{S} \subseteq \mathbb{X}$, $\mathbb{U}$, and $\mathbb{Y}$ are the state, secret state, input, and output sets, respectively. The map $f : \mathbb{X} \times \mathbb{U} \to \mathbb{X}$ is the state transition function, and $h : \mathbb{X} \to \mathbb{Y}$ is the output map. The dynamics of Σ is described by difference equations of the form

$$\Sigma : \begin{cases} \xi(k+1) = f(\xi(k), \upsilon(k)), \\ \zeta(k) = h(\xi(k)), \end{cases} \tag{5}$$

where $\xi : \mathbb{N} \to \mathbb{X}$, $\zeta : \mathbb{N} \to \mathbb{Y}$, and $\upsilon : \mathbb{N} \to \mathbb{U}$ represent the state, output, and input signals, respectively. We write $\xi_{x\upsilon}(k)$ to denote the point reached at time k under the input signal υ from initial condition $x = \xi_{x\upsilon}(0)$, and $\zeta_{x\upsilon}(k)$ to denote the output corresponding to state $\xi_{x\upsilon}(k)$, i.e., $\zeta_{x\upsilon}(k) = h(\xi_{x\upsilon}(k))$. Throughout this section, we assume that

the output map satisfies the following Lipschitz condition: $\|h(x) - h(x')\| \leq \alpha(\|x - x'\|)$ for some $\alpha \in \mathcal{K}_\infty$, for all $x, x' \in \mathbb{X}$.

B. Construction of Finite Abstractions

Next, we present how to construct finite abstractions which preserve pre-opacity for a class of discrete-time control systems. Specifically, the finite abstraction is built under the assumption that the concrete control system is incrementally input-to-state stable [14] as defined next.

Definition 5: System $\Sigma = (\mathbb{X}, \mathbb{S}, \mathbb{U}, f, \mathbb{Y}, h)$ is called incrementally input-to-state stable (δ-ISS) if there exist functions $\beta \in \mathcal{KL}$ and $\gamma \in \mathcal{K}_\infty$ such that $\forall x, x' \in \mathbb{X}$ and $\forall \upsilon, \upsilon' \in \mathbb{N} \to \mathbb{U}$, the following inequality holds for any $k \in \mathbb{N}$:

$$\|\xi_{x\upsilon}(k) - \xi_{x'\upsilon'}(k)\| \leq \beta(\|x - x'\|, k) + \gamma(\|\upsilon - \upsilon'\|_\infty). \quad (6)$$

Next, in order to construct pre-opacity preserving finite abstractions for a control system $\Sigma = (\mathbb{X}, \mathbb{S}, \mathbb{U}, f, \mathbb{Y}, h)$ in Definition 4, we define an associated metric system $S(\Sigma) = (X, X_0, X_S, U, \longrightarrow, Y, H)$, where $X = \mathbb{X}$, $X_0 = \mathbb{X}$, $X_S = \mathbb{S}$, $U = \mathbb{U}$, Y[1] $= \mathbb{Y}$, $H = h$, and $x \xrightarrow{u} x'$ if and only if $x' = f(x, u)$. In the sequel, we will use $S(\Sigma)$ to denote the concrete control systems interchangeably. Now, we are ready to introduce a finite abstraction for a control system Σ. To do so, we assume that sets $\mathbb{X}$, $\mathbb{S}$ and $\mathbb{U}$ are of the form of finite union of boxes. Consider a tuple $\mathsf{q} = (\eta, \mu, \theta)$ of parameters, where $0 < \eta \leq \min\{span(\mathbb{S}), span(\mathbb{X}\backslash\mathbb{S})\}$ is the state set quantization, $0 < \mu \leq span(\mathbb{U})$ is the input set quantization, and θ is the designed inflation parameter. A finite abstraction of Σ is defined as

$$S_{\mathsf{q}}(\Sigma) = (X_{\mathsf{q}}, X_{\mathsf{q}0}, X_{\mathsf{q}S}, U_{\mathsf{q}}, \underset{\mathsf{q}}{\longrightarrow}, Y_{\mathsf{q}}, H_{\mathsf{q}}), \quad (7)$$

where $X_{\mathsf{q}} = X_{\mathsf{q}0} = [\mathbb{X}]_\eta$, $X_{\mathsf{q}S} = [\mathbb{S}^\theta]_\eta$, where $\mathbb{S}^\theta = \{x \in \mathbb{X} : \exists x' \in \mathbb{S}, \text{ s.t. } \|x - x'\| \leq \theta\}$ denotes the θ-expansion of set $\mathbb{S}$, $U_{\mathsf{q}} = [\mathbb{U}]_\mu$, $Y_{\mathsf{q}} = \{h(x_{\mathsf{q}}) \mid x_{\mathsf{q}} \in X_{\mathsf{q}}\}$, $H_{\mathsf{q}}(x_{\mathsf{q}}) = h(x_{\mathsf{q}})$, $\forall x_{\mathsf{q}} \in X_{\mathsf{q}}$, and

$$x_{\mathsf{q}} \underset{\mathsf{q}}{\xrightarrow{u_{\mathsf{q}}}} x'_{\mathsf{q}} \text{ if and only if } \|x'_{\mathsf{q}} - f(x_{\mathsf{q}}, u_{\mathsf{q}})\| \leq \eta. \quad (8)$$

Now, we are ready to present the main result of this section, which shows that under some condition over the quantization parameters η, θ and μ, the finite abstraction $S_{\mathsf{q}}(\Sigma)$ constructed in (7) indeed simulates our concrete control system $S(\Sigma)$ through approximate K-step pre-opacity preserving simulation relation as in Definition 3.

Theorem 2: Consider a δ-ISS control system $\Sigma = (\mathbb{X}, \mathbb{S}, \mathbb{U}, f, \mathbb{Y}, h)$ as in Definition 5 and its associated metric system $S(\Sigma)$. For any desired precision $\varepsilon > 0$, and any tuple $\mathsf{q} = (\eta, \mu, \theta)$ of quantization parameters satisfying

$$\beta\Big(\alpha^{-1}(\varepsilon), 1\Big) + \gamma(\mu) + \eta \leq \alpha^{-1}(\varepsilon), \quad (9)$$

$$\beta\Big(\alpha^{-1}(\varepsilon), 1\Big) + \eta \leq \theta, \quad (10)$$

we have $S(\Sigma) \preceq^\varepsilon_A S_{\mathsf{q}}(\Sigma)$.

Proof: Given a desired precision $\varepsilon > 0$ appeared in Definition 3, let us consider a relation $R \subseteq X \times X_{\mathsf{q}}$ defined by: $(x, x_{\mathsf{q}}) \in R$ if and only if $\|x - x_{\mathsf{q}}\| \leq \alpha^{-1}(\varepsilon)$. First, according to the construction of $S_{\mathsf{q}}(\Sigma)$ in (7), for any initial state $x_0 \in X_0$ in $S(\Sigma)$, there exists an initial state $x_{q0} \in X_{q0}$ in $S_{\mathsf{q}}(\Sigma)$ such that $\|x_{a0} - x_{q0}\| \leq \eta$. By (9), we further have $\eta \leq \alpha^{-1}(\varepsilon)$. Thus, we get that $(x_0, x_{q0}) \in R$ and condition 1)-a) in Definition 3 readily holds. Moreover, for any $x_{\mathsf{q}0} \in X_{\mathsf{q}0}$, there exists $x_0 = x_{\mathsf{q}0} \in X_0$ such that $\|x_0 - x_{\mathsf{q}0}\| = 0 \leq \alpha^{-1}(\varepsilon)$. Hence, $(x_0, x_{\mathsf{q}0}) \in R$ and condition 1)-b) in Definition 3 is also satisfied. Now consider any $(x, x_{\mathsf{q}}) \in R$. By the definition of R and the Lipschitz assumption, we have $\|H(x) - H_{\mathsf{q}}(x_{\mathsf{q}})\| = \|h(x) - h(x_{\mathsf{q}})\| \leq \alpha(\|x - x_{\mathsf{q}}\|) \leq \varepsilon$, which shows that condition 2) in Definition 3 is satisfied. Further, let us proceed to prove condition 3) in Definition 3. First, consider any pair $(x, x_{\mathsf{q}}) \in R$. Given any input $u \in U$ and the transition $x \xrightarrow{u} x' = f(x, u)$ in $S(\Sigma)$, let us choose an input $u_q \in U_q$ such that $\|u - u_{\mathsf{q}}\| \leq \mu$, where $\mu \leq span(\mathbb{U})$. From the δ-ISS assumption on Σ, the distance between x' and $f(x_{\mathsf{q}}, u_{\mathsf{q}})$ is bounded as:

$$\begin{aligned}\|x' - f(x_{\mathsf{q}}, u_{\mathsf{q}})\| &\overset{(6)}{\leq} \beta\big(\|x - x_{\mathsf{q}}\|, 1\big) + \gamma\big(\|u - u_{\mathsf{q}}\|\big) \\ &\leq \beta\Big(\alpha^{-1}(\varepsilon), 1\Big) + \gamma(\mu). \end{aligned} \quad (11)$$

Besides, by the structure of $S_{\mathsf{q}}(\Sigma)$ as in (8), we have

$$\|f(x_{\mathsf{q}}, u_{\mathsf{q}}) - x'_{\mathsf{q}}\| \leq \eta. \quad (12)$$

Now, combining the inequalities (9), (11), (12), and triangle inequality, we obtain:

$$\begin{aligned}\|x' - x'_{\mathsf{q}}\| &= \|x' - f(x_{\mathsf{q}}, u_{\mathsf{q}}) + f(x_{\mathsf{q}}, u_{\mathsf{q}}) - x'_{\mathsf{q}}\| \\ &\leq \|x' - f(x_{\mathsf{q}}, u_{\mathsf{q}})\| + \|f(x_{\mathsf{q}}, u_{\mathsf{q}}) - x'_{\mathsf{q}}\| \\ &\leq \beta\Big(\alpha^{-1}(\varepsilon), 1\Big) + \gamma(\mu) + \eta \leq \alpha^{-1}(\varepsilon).\end{aligned}$$

Therefore, we can conclude that $(x', x'_{\mathsf{q}}) \in R$ and condition 3)-a) in Definition 3 holds. Next, let us show that the condition 3)-b) in Definition 3 holds as well. Consider x_q and any input $u_q \in U_q$ in $S_{\mathsf{q}}(\Sigma)$. Let us choose $u = u_q$. Then, we get the unique transition $x \xrightarrow{u} x' = f(x, u)$ in $S(\Sigma)$. Be leveraging the δ-ISS assumption on Σ, we have that the distance between x' and $f(x_{\mathsf{q}}, u_{\mathsf{q}})$ is bounded as:

$$\begin{aligned}\|x' - f(x_{\mathsf{q}}, u_{\mathsf{q}})\| &\leq \beta\big(\|x - x_{\mathsf{q}}\|, 1\big) + \gamma\big(\|u - u_{\mathsf{q}}\|\big) \\ &\leq \beta\Big(\alpha^{-1}(\varepsilon), 1\Big). \end{aligned} \quad (13)$$

Based on the structure of $S_{\mathsf{q}}(\Sigma)$, there exists $x'_{\mathsf{q}} \in X_{\mathsf{q}}$ s.t.:

$$\|f(x_{\mathsf{q}}, u_{\mathsf{q}}) - x'_{\mathsf{q}}\| \leq \eta, \quad (14)$$

which, by the definition of $S_{\mathsf{q}}(\Sigma)$ in (8), implies the existence of $x_{\mathsf{q}} \underset{\mathsf{q}}{\xrightarrow{u_{\mathsf{q}}}} x'_{\mathsf{q}}$ in $S_{\mathsf{q}}(\Sigma)$. Combining inequalities (9), (13), (14), and triangle inequality, we obtain:

$$\begin{aligned}\|x' - x'_{\mathsf{q}}\| &= \|x' - f(x_{\mathsf{q}}, u_{\mathsf{q}}) + f(x_{\mathsf{q}}, u_{\mathsf{q}}) - x'_{\mathsf{q}}\| \\ &\leq \|x' - f(x_{\mathsf{q}}, u_{\mathsf{q}})\| + \|f(x_{\mathsf{q}}, u_{\mathsf{q}}) - x'_{\mathsf{q}}\| \\ &\leq \beta\Big(\alpha^{-1}(\varepsilon), 1\Big) + \eta \leq \alpha^{-1}(\varepsilon).\end{aligned}$$

Therefore, we conclude that $(x'_{\mathsf{q}}, x') \in R$ and condition 3)-b) in Definition 3 holds. Finally, let us show that condition 3)-c) in Definition 3 holds. To this end, we firstly consider an arbitrary transition $x_q \xrightarrow{u_q} x'_q$ with $x'_q \notin X_S$ in $S_q(\Sigma)$. Similar to

[1]The output set is assumed to be equipped with the infinity norm: $\mathbf{d}(y_1, y_2) = \|y_1 - y_2\|, \forall y_1, y_2 \in Y$.

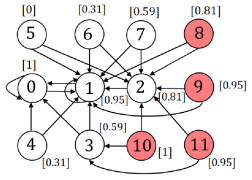


Fig. 3. A pre-opacity preserving finite abstraction of a control system.

the proof of condition 3)-b), we can show the existence of a transition $x \xrightarrow{u} x'$ in $S(\Sigma)$ where $(x', x'_{\mathsf{q}}) \in R$ holds, and the input is chosen as $u = u_{\mathsf{q}} \in U_{\mathsf{q}}$. Then by the construction of the secret set in the finite abstraction, one has $X_{\mathsf{q}S} = [\mathbb{S}^{\theta}]_{\eta}$ with the inflation parameter satisfying $\theta \geq \beta(\alpha^{-1}(\varepsilon), 1) + \eta$ and $0 < \eta \leq \min\{span(\mathbb{S}), span(\mathbb{X}\backslash\mathbb{S})\}$, which also implies that the size of the non-secret region in $S_q(\Sigma)$ is smaller than that in $S(\Sigma)$. Therefore, since $(x', x'_{\mathsf{q}}) \in R$ which implies $\|x' - x'_{\mathsf{q}}\| \leq \beta(\alpha^{-1}(\varepsilon), 1) + \eta \leq \theta$, we obtain that $x' \notin X_S$. Thus, we conclude that condition 3)-c) in Definition 3 holds, which completes the proof. ■

V. Example

Here, we provide an example to illustrate the proposed abstraction-based pre-opacity verification approach. Consider the following simple control system:

$$\Sigma : \begin{cases} \xi(k+1) = 0.2\xi(k) + v(k) \\ \zeta(k) = \|\cos(0.1\pi\xi(k))\|, \end{cases} \tag{15}$$

where the state set is $\mathbb{X} = \mathbb{X}_0 = [0, 12)$, the secret set is $\mathbb{X}_S = [11, 12)$, the input set is a singleton $\mathbb{U} = \{0.05\}$, and the output set is $\mathbb{Y} = [0, 1]$. The output function of the system satisfies the Lipschitz condition as in Definition 4 with $\alpha(r) = 0.1\pi r$. The main goal of the example is to verify approximate pre-opacity of the system using the proposed abstraction-based approach.

Next, we apply our main results to achieve this goal. First, let us construct a finite abstraction $S_{\mathsf{q}}(\Sigma)$ of Σ which preserves pre-opacity with desired precision $\varepsilon = 0.4$ as in Definition 3. Note that by Definition 5, one can readily check that this control system Σ is δ-ISS with $\beta(r, k) = 0.2^k r$ and $\gamma(r) = 2r$. Next, a tuple of quantization parameters $q = (\eta, \mu, \theta) = (1, 0, 2.3)$ are chosen such that inequalities (9)-(10) are satisfied. By Theorem 2, we have $S(\Sigma) \preceq_A^{0.4} S_{\mathsf{q}}(\Sigma)$. Given the quantization parameters $q = (\eta, \mu, \theta) = (1, 0, 2.3)$, the state set $\mathbb{X}$ is discretized into 12 discrete states as $X_q = X_{q0} = \{0, 1, 2, \ldots, 11\}$, the discrete secret set is $X_{qS} = \{8, 9, 10, 11\}$, the discrete input set is $U_q = \{0.05\}$, and the discrete output set is $Y_q = \{0, 0.31, 0.59, 0.81, 0.95, 1\}$. The obtained finite abstraction $S_{\mathsf{q}}(\Sigma)$ of Σ is shown in Fig. 3. The states marked in red represent the secret states, and the output of each state is specified by a value associated to it. Note that the system can be initiated from any state since $X_q = X_{q0}$ and the input $u = 0.05$ is omitted in the figure for the sake of better presentation. One can readily check that $S_{\mathsf{q}}(\Sigma)$ is exact 0-step pre-opaque since for any run generated from any initial state of the system and any future instant $k \geq 0$, there exists another run with exactly the same output trajectory such that it will reach a non-secret state in exactly k steps. As an example, consider a state run $11 \xrightarrow{u} 2 \xrightarrow{u} 1 \xrightarrow{u} 0 \xrightarrow{u} 1$ which generates an output run [0.95][0.81][0.95][1][0.95]. There exists another state run $9 \xrightarrow{u} 2 \xrightarrow{u} 1 \xrightarrow{u} 0 \xrightarrow{u} 1$ which generates exactly the same output behavior, and will reach non-secret states (either 0 or 1) in any future time step $k \geq 0$. Finally, by leveraging Theorem 1, we can readily conclude that the concrete system Σ is 0.8-approximate 0-step pre-opaque without directly applying verification algorithms on it.

VI. Conclusion

In this letter, we proposed an abstraction-based verification framework tailored to a security property called pre-opacity for discrete-time control systems. The concept of pre-opacity was first extended to an approximate version which is more applicable to control systems with continuous-space outputs. Then, a notion of approximate pre-opacity preserving simulation relation was proposed, based on which one can verify pre-opacity of control systems using their finite abstractions. We also investigated how to construct finite abstractions that preserve pre-opacity for a class of control systems via the proposed system relation. Finally, an example was presented to illustrate the proposed abstraction-based verification approach. For future work, an interesting problem is how to synthesize controllers to enforce pre-opacity for general control systems.

References

[1] L. An and G. Yang, "Opacity enforcement for confidential robust control in linear cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 1234–1241, Mar. 2020.
[2] J. Balun and T. Masopust, "Comparing the notions of opacity for discrete-event systems," *Discr. Event Dyn. Syst.*, vol. 31, no. 4, pp. 553–582, 2021.
[3] J. C. Basilio, C. N. Hadjicostis, and R. Su, "Analysis and control for resilience of discrete event systems: Fault diagnosis, opacity and cyber security," *Found. Trends Syst. Control.*, vol. 8, no. 4, pp. 285–443, 2021.
[4] J. Hou, S. Liu, X. Yin, and M. Zamani, "Abstraction-based verification of approximate pre-opacity for control systems," 2022, *arXiv: 2211.04098*.
[5] R. Jacob, J.-J. Lesage, and J.-M. Faure, "Overview of discrete event systems opacity: Models, validation, and quantification," *Annu. Rev. Control.*, vol. 41, pp. 135–146, Jun. 2016.
[6] S. Lafortune, F. Lin, and C. N. Hadjicostis, "On the history of diagnosability and opacity in discrete event systems," *Annu. Rev. Control.*, vol. 45, pp. 257–266, Apr. 2018.
[7] B. Lennartson, M. Noori-Hosseini, and C. N. Hadjicostis, "State-labeled safety analysis of modular observers for opacity verification," *IEEE Control Syst. Lett.*, vol. 6, pp. 2936–2941, 2022.
[8] F. Lin, "Opacity of discrete event systems and its applications," *Automatica*, vol. 47, no. 3, pp. 496–503, 2011.
[9] S. Liu, A. Trivedi, X. Yin, and M. Zamani, "Secure-by-construction synthesis of cyber-physical systems," *Annu. Rev. Control.*, vol. 53, pp. 30–50, Apr. 2022.
[10] Z. Ma, X. Yin, and Z. Li, "Verification and enforcement of strong infinite-and k-step opacity using state recognizers," *Automatica*, vol. 133, Nov. 2021, Art. no. 109838.
[11] L. Mazaré, "Using unification for opacity properties," in *Proc. Workshop Issues Theory Secururity*, vol. 4, 2004, pp. 165–176.
[12] 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.
[13] Y. Tong, H. Lan, and C. Seatzu, "Verification of K-step and infinite-step opacity of bounded labeled Petri nets," *Automatica*, vol. 140, Jun. 2022, Art. no. 110221.
[14] D. N. Tran, "Advances in stability analysis for nonlinear discrete-time dynamical systems," Ph.D. dissertation, Dept. Electr. Eng., Univ. Newcastle, Callaghan, NSW, Australia, 2018.
[15] A. Wintenberg, M. Blischke, S. Lafortune, and N. Ozay, "A general language-based framework for specifying and verifying notions of opacity," *Discr. Event Dyn. Syst.*, vol. 32, no. 2, pp. 253–289, 2022.
[16] S. Yang and X. Yin, "Secure your intention: On notions of pre-opacity in discrete-event systems," *IEEE Trans. Autom. Control*, early access, Sep. 27, 2022, doi: 10.1109/TAC.2022.3210148.
[17] X. Yin, M. Zamani, and S. Liu, "On approximate opacity of cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 66, no. 4, pp. 1630–1645, Apr. 2021.