2022 European Control Conference (ECC)
July 12-15, 2022. London, United Kingdom

Verification of approximate infinite-step opacity using barrier certificates

Shadi Tasdighi Kalat, Siyuan Liu, and Majid Zamani

***Abstract*— In this paper, we consider the verification of approximate infinite-step opacity for discrete-time control systems. Relying on finite abstraction techniques for solving this problem requires discretization of the state and input sets, which requires significant computational resources. Here, we propose a discretization-free approach in which we formulate opacity as a safety property over an appropriately constructed *augmented system*, and seek to verify it by finding suitable barrier certificates. Within our proposed scheme, lack of opacity is also verified by posing it as a reachability property over the augmented system. The main result of this paper offers a discretization-free approach to verify (lack of) infinite-step opacity in discrete-time control systems. We also discuss other notions of opacity, and their relations to one another. We particularly study the conditions under which verifying one form of opacity for a system also implies other forms. Finally, we illustrate our theoretical results on two numerical examples, where we utilize sum-of-squares programming to search for polynomial barrier certificates. In these examples, we verify the infinite-step, and current-step opacity for a vehicle by checking whether its position is concealed from possible outside intruders.**

I. Introduction

Many of the cyber-physical systems (CPS) are vulnerable to attacks and information leaks, as they have been broadly deployed and access to sensitive data. The presence of cyber and physical components in such systems introduces a suit of challenges in detecting security vulnerabilities. *Opacity* is a security property which is concerned with the information-flow of the system. In other words, opacity characterizes the plausible deniability of a system's secret in the presence of an outside intruder. Depending on whether the system secret is modeled as a set of states, or a set of behaviors, opacity can be formulated as state-based, or language-based, respectively. State-based opacity has different notions that are expounded in [1]. Among these notions, initial-state opacity prevents the intruder from realizing, at any step, whether the system started from a secret state, and current-state opacity prevents the intruder from knowing whether the current state of the system is secret. However, this does not prevent the intruder from realizing that the system was in a secret state at a previous time step. This issue led to the introduction of K-step opacity [2], [3]. The notion of K-step opacity requires that the intruder cannot discover the secret in the last K consecutive steps. Two special cases for $K = 0$ and $K = \infty$ are known as current-state opacity and infinite-step opacity, respectively.

A growing body of work has considered opacity in different systems. Although studying opacity for continuous-space systems became the subject of many studies recently, the majority of the existing works on opacity pertain to discrete event systems (DESs), including those modeled by bounded Petri nets [4], or finite state automata with discrete state sets [3], [5], [6], [7], [8], [9], [10].

Properties such as safety and reachability have been leveraged recently in studying opacity. The approach presented in [11] formulates the notion of opacity as an output reachability property, and verifies it by approximating the reachable states of the system. However, the proposed framework is limited to discrete-time linear systems. Although the results in [12] are limited to systems with finite state sets modeled by partially-observable Markov decision processes, they also study opacity by checking a safety property of the intruder's belief dynamics using barrier certificates. (Control) barrier functions are a common approach to verify or enforce safety and reachability properties. Results in [13] introduce notions of *barrier certificates* as tools for safety verification of a class of hybrid systems. They study safety and reachability as a dual pair, by searching for such barrier certificates using optimization techniques [14]. The results in [15] use barrier certificate to verify *approximate* initial-state opacity for discrete time control systems. *Approximate opacity* is introduced in [16], which allows us to quantitatively evaluate the security level of control systems whose output are physical signals. This definition accommodates for the intruder's measurement precision, defined as a parameter δ. In other words, any pair of observations whose distance is less than δ are indistinguishable to the eyes of an intruder with imperfect measurement precision. This concept is also studied in the domain of continuous-space stochastic control systems using opacity-preserving simulation functions and their finite abstractions (finite Markov decision processes) in [17].

Our contribution. We consider the problem of verifying *approximate* infinite-step opacity for discrete-time control systems. Unlike the methodologies proposed in [16], [17] which are based on abstraction-based techniques, we propose a discretization-free approach for formal verification of approximate infinite-step opacity based on a notion of barrier certificates. We tackle the verification of opacity by formulating it as a safety verification over an augmented

This work was supported in part by the NSF under grant ECCS-2015403 and the German Research Foundation (DFG) under grant ZA 873/7-1.

S. Tasdighi Kalat and M. Zamani are with the Computer Science Department, University of Colorado Boulder, USA. S. Liu is with the Department of Electrical and Computer Engineering, Technical University of Munich, Germany. M. Zamani is also with the Computer Science Department, Ludwig Maximilian University of Munich, Germany. Emails: shadi.tasdighikalat@colorado.edu, sy.liu@tum.de, majid.zamani@colorado.edu.

system, and verify it by finding suitable barrier certificates. Similar to the methodology presented in [15], [18], we define an *augmented system* by taking the product of a system with itself, and we find barrier certificates for this augmented system. It is known that the existence of a barrier certificate ensures that no trajectory originated from a predefined initial region will reach the unsafe region. We show that, by properly defining the initial and unsafe sets which capture the initial, and secret states of the system, the existence of such barrier certificates for the augmented system is sufficient to ensure approximate infinite-step opacity of the original system. However, failure in finding such barrier certificates does not imply the lack of opacity. Due to the duality between *safety* and *reachability*, we show the lack of opacity for a system by defining a reachability-type property over its augmented version. Finding a barrier certificate verifying this reachability property for the augmented system will show the lack of infinite-step opacity for the original system. Compared with the results in [15], [18] which are focused on initial-state opacity only, our results here propose for the first time a verification procedure tailored to infinite-step opacity. We further investigate relationships between different notions of state-based opacity, i.e., initial-state, current-state, and K-step opacity, and study conditions under which one property may imply another one.

II. Notation and Preliminaries

Notation: We use $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, and $\mathbb{N}$ to denote the set of real numbers, non-negative real numbers, and natural numbers, respectively. A closed interval from a to b, where $a \leq b$, in $\mathbb{R}$ is represented as $[a, b]$. If $a, b \in \mathbb{N}$, this interval is denoted by $[a; b]$. Given a vector x, we denote its Euclidean norm by $||x||$. For sets X and Y with $X \subset Y$, the complement of X with respect to Y is defined as $Y \setminus X = \{x \in Y | x \notin X\}$. The Cartesian product of X and Y is defined by $X \times Y = \{(x, y) | x \in X, y \in Y\}$. For any set $Z \subseteq \mathbb{R}^n$, ∂Z and $\overline{Z}$, denote its boundary and topological closure, respectively. The empty set is represented by $\emptyset$.

Let us first introduce the class of discrete-time control systems studied in this paper.

Definition 1: **(Control system)** A discrete-time control system S is defined as a tuple

$$S = (X, X_0, X_s, U, f, Y, h),$$

where X, $X_0 \subseteq X$, U, and Y are the sets of state, initial state, input, and output, respectively. Set $X_s \subseteq X$ denotes the set of secret states. The functions $f : X \times U \to X$ and $h : X \to Y$ are the state transition function and output functions, respectively. A discrete-time control system S is described by the following difference equations:

$$S : \begin{cases} \mathbf{x}(t+1) = f(\mathbf{x}(t), \mathbf{u}(t)), \\ \mathbf{y}(t) = h(\mathbf{x}(t)), \end{cases}$$

where $\mathbf{x} : \mathbb{N} \to X$, $\mathbf{y} : \mathbb{N} \to Y$, and $\mathbf{u} : \mathbb{N} \to U$ denote the the state, output, and input signals, respectively. We use $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$ to denote a finite state run of S starting from initial state x_0 under input run $\mathbf{u}$.

In this paper, we mainly focus on a state-based opacity property, called *approximate infinite-step opacity*, which is originally proposed in [16] and recalled next.

Definition 2: **(Approximate infinite-step opacity)** Given $\delta \in \mathbb{R}^+$, a system S as in Definition 1 is said to be δ-approximate infinite-step opaque if for any $x_0 \in X_0$, any finite state run $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$, and any $k \in \{0, \ldots n\}$ such that $x_k \in X_s$, there exists $\hat{x}_0 \in X_0$ and a finite state run $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}} = \{\hat{x}_0, \ldots, \hat{x}_n\}$ such that $\hat{x}_k \in X \setminus X_s$ and

$$\max_{i \in [0,n]} ||h(x_i) - h(\hat{x}_i)|| \leq \delta.$$

Intuitively, the definition of approximate infinite-step opacity requires that an intruder with imperfect measurement precision (captured by the parameter δ) should never know for sure that the system was at a secret state for any specific instant. Note that throughout the paper, we assume without loss of generality that for all $x_0 \in X_0$, $\{x \in X_0 : \|h(x) - h(x_0)\| \leq \delta\} \not\subseteq X_s$; otherwise, infinite-step opacity is trivially violated.

III. Verifying Approximate Infinite-step Opacity

In this section, we present a method to verify approximate infinite-step opacity for discrete-time control systems S as in Definition 1. Our approach is based on finding a barrier certificate for the augmented system of S as defined next.

Definition 3: **(Augmented system)** Consider a control system S as in Definition 1. The associated augmented system for S is defined as the product of S with itself:

$$S \times S = (X \times X, X_0 \times X_0, X_s \times X_s, U \times U, f \times f, Y \times Y, h \times h).$$

We use notation $(x, \hat{x}) \in X \times X$ to denote a state in $S \times S$ and $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ to denote the state sequence of $S \times S$ starting from $(x_0, \hat{x}_0)$ under input sequence $(\mathbf{u}, \hat{\mathbf{u}})$. Additionally, we denote the augmented state set by $\mathcal{X} = X \times X$.

A. Verifying Approximate Infinite-Step Opacity

Our verification approach seeks to find a so-called barrier certificate for the augmented system defined in Definition 3 to ensure approximate infinite-step opacity of the original system. Such a barrier certificate is defined as the following.

Definition 4: **(Barrier certificate for augmented system)** Consider an augmented system $S \times S$ as in Definition 3, and sets $\mathcal{X}_0, \mathcal{X}_u \subseteq \mathcal{X}$. A function $B : X \times X \to \mathbb{R}_{\geq 0}$ is a barrier certificate for $S \times S$, if it satisfies the following conditions:

$$\forall (x, \hat{x}) \in \mathcal{X}_0, \quad B(x, \hat{x}) \leq \bar{\epsilon}, \tag{1}$$

$$\forall (x, \hat{x}) \in \mathcal{X}_u, \quad B(x, \hat{x}) > \underline{\epsilon}, \tag{2}$$

$$\forall (x, \hat{x}) \in \mathcal{X}, \forall u \in U, \exists \hat{u} \in U, \quad B(f(x, u), f(\hat{x}, \hat{u})) - B(x, \hat{x}) \leq 0, \tag{3}$$

where $\bar{\epsilon}$, $\underline{\epsilon} \in \mathbb{R}_{\geq 0}$ and $\underline{\epsilon} \geq \bar{\epsilon}$.

To verify infinite-step opacity of system S using the above-defined barrier certificate, the sets of interest appeared in Definition 4 need to be defined in a specific way to capture

the initial and secret information of system S. In particular, we define sets of initial states $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$ as:

$$\begin{aligned}\mathcal{X}_0 &= \{(x,\hat{x}) \in X_0 \times X_0 : x \notin X_s, ||h(x) - h(\hat{x})|| \leq \delta\} \cup \\ &\quad \{(x,\hat{x}) \in X_0 \times X_0 : x \in X_s, \hat{x} \notin X_s, ||h(x) – h(\hat{x})|| \leq \delta\}, \\ \mathcal{X}_u &= \{(x,\hat{x}) \in X \times X : x \in X_s, \hat{x} \in X_s\} \cup \\ &\quad \{(x,\hat{x}) \in X \times X : x \in X_s, \hat{x} \notin X_s, ||h(x) – h(\hat{x})|| > \delta\} \cup \\ &\quad \{(x,\hat{x}) \in X \times X : x \notin X_s, \hat{x} \in X, ||h(x) – h(\hat{x})|| > \delta\},\end{aligned} \tag{4}$$

where $\delta \in \mathbb{R}_{\geq 0}$ denotes the measurement precision of the outside intruder as introduced in Definition 2.

Remark 1: The intuitions of the above definition for sets $\mathcal{X}_0$ and $\mathcal{X}_u$ are explained as follows. The unsafe set $\mathcal{X}_u$ as in (4) is defined as the union of three sets, where each set captures a certain scenario which violates approximate infinite-step opacity. The first case happens when both x and $\hat{x}$ belong to the set X_s. When the system's state x belongs to the secret set, opacity requires that $\hat{x}$ is not in this set, so that the desired alternative trajectory exists. Second case happens if x belongs to X_s, and $\hat{x}$ belongs to $X \setminus X_s$, but they are not δ close. This makes the two system's trajectories distinguishable from the intruder point of view. Third case happens if x belongs to $X \setminus X_s$, and $\hat{x}$ belongs to X, and they are not δ-close. In this case, since x does not belong to the secret set, we do not require $\hat{x}$ to belong to a certain subset of X. However, if the distance between the two trajectories exceeds δ, they would be distinguished by the intruder. Similarly, to define the initial set, we also consider possible initial conditions which the system can start from. First case is when x_0 belongs to $X_0 \setminus X_s$, $\hat{x}_0$ belongs to X_0, and they are δ close. This conveys if the system's initial condition is not secret, all we need for ensuring opacity of the system is to keep the trajectories δ-close. However, if the initial condition is secret, we require the alternative trajectory $\hat{x}$ to remain δ-close. This means x belongs to X_s, $\hat{x}$ belongs to $X_0 \setminus X_s$, and they are δ-close. Finally, we note that the sets defined to form $\mathcal{X}_0$ and $\mathcal{X}_u$ do not intersect.

Now, we are ready to introduce the next theorem, which states the usefulness of the above-defined barrier certificate for verifying approximate infinite-step opacity of system S.

Theorem 1: Consider a control system S as in Definition 1 and its associated augmented system $S \times S$ as in Definition 3. Suppose that there exists a function $B : X \times X \to \mathbb{R}_{\geq 0}$ satisfying conditions (1)-(3) in Definition 4 with sets $\mathcal{X}_0$ and $\mathcal{X}_u$ defined as in (4). Then, system S is δ-approximate infinite-step opaque.

Proof: Let us first mention that, by applying the result from [15, Proposition 1], the existence of a barrier certificate B as in Definition 4 ensures a safety property for the augmented system $S \times S$. That is, for any initial condition $(x_0, \hat{x}_0) \in \mathcal{X}_0$, and any input run $\mathbf{u}$, there exists an input run $\hat{\mathbf{u}}$ such that $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}) \cap \mathcal{X}_u = \emptyset$.

Now, let the set of initial conditions $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$ be as defined in (4). Consider an arbitrary initial state x_0, an input sequence $\mathbf{u}$ and the corresponding state run $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$ in S such that $x_k \in X_s$ for some $k \in \{0, \ldots, n\}$. We consider the following two cases:

If $k = 0$, then we have $x_0 \in X_s$. By the assumption that $\{x \in X_0 : \|h(x) - h(x_0)\| \leq \delta\} \not\subseteq X_s$ for any $x_0 \in X_0$, we know that there exists $\hat{x}_0 \in X \setminus X_s$ such that $\|h(x_0) - h(\hat{x}_0)\| \leq \delta$. Consider the augmented initial state $(x_0, \hat{x}_0)$, it can be readily verified that $(x_0, \hat{x}_0) \in \mathcal{X}_0$, where set $\mathcal{X}_0$ is as defined in (4). Then, as a consequence of the safety property of $S \times S$ (which is guaranteed from the existence of a barrier certificate B), we get that there exists an input run $\hat{\mathbf{u}}$ such that the state run $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ of the augmented system $S \times S$ never reaches the unsafe set $\mathcal{X}_u$, i.e., $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}) \cap \mathcal{X}_u = \emptyset$. By the structure of $\mathcal{X}_u$, this implies the satisfaction of $\|h(\mathbf{x}_{x_0,\mathbf{u}}(t)) - h(\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(t))\| \leq \delta$, for all $t \in \mathbb{N}$ (cf. Remark 1 for more intuitions on the structure of set $\mathcal{X}_u$).

If $k \geq 1$, then we have $x_0 \in X_0 \setminus X_s$. Again, we get by assumption that there exists $\hat{x}_0 \in X \setminus X_s$ such that $\|h(x_0) - h(\hat{x}_0)\| \leq \delta$. One can verify that the augmented initial state $(x_0, \hat{x}_0)$ also belongs to the set $\mathcal{X}_0$ as defined in (4). Again, by utilizing the safety property of $S \times S$, there exists an input run $\hat{\mathbf{u}}$ such that the state run $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ of the augmented system $S \times S$ never reaches the unsafe set $\mathcal{X}_u$. Given that $x_k \in X_s$ and by further leveraging the structure of $\mathcal{X}_u$, it follows that $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(k) \in X \setminus X_s$ and $\|h(\mathbf{x}_{x_0,\mathbf{u}}(t)) - h(\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(t))\| \leq \delta$, for all $t \in \mathbb{N}$ (cf. Remark 1 for more intuitions on the structure of set $\mathcal{X}_u$).

Since the state run $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$ in S and index k are arbitrary, we can conclude that system S is δ-approximate infinite-step opaque. ■

B. Verifying Lack of Approximate Infinite-Step Opacity

In the last subsection, we developed a sufficient condition for verifying approximate infinite-step opacity based on a notion of barrier certificates. In particular, if one can find a barrier certificate satisfying conditions (1)-(4), which ensures a safety property for the augmented system $S \times S$, then system S is shown to be approximate infinite-step opaque. Note that failure in finding such a barrier certificate does not imply the lack of opacity. Inspired by the duality between safety and reachability, we introduce by the following proposition a sufficient condition for the the lack of approximate infinite-step opacity of S by searching for a barrier certificate which ensures a reachability property for the augmented system $S \times S$.

Proposition 1: Consider a control system S as in Definition 1 and its associated augmented system $S \times S$ as in Definition 3. Suppose the state set X of S is bounded, and there exists a continuous function $V : X \times X \to \mathbb{R}$ which satisfies

$$\forall (x,\hat{x}) \in \mathcal{X}_0, \quad V(x,\hat{x}) \leq 0, \tag{5}$$

$$\forall (x,\hat{x}) \in \partial\mathcal{X} \setminus \partial\mathcal{X}_u, \quad V(x,\hat{x}) > 0, \tag{6}$$

$$\begin{aligned}&\forall (x,\hat{x}) \in \overline{\mathcal{X} \setminus \mathcal{X}_u}, \exists u \in U, \text{ s.t. } \forall \hat{u} \in U, \\ &\quad V(f(x,u), f(\hat{x},\hat{u})) - V(x,\hat{x}) \leq 0,\end{aligned} \tag{7}$$

where sets $\mathcal{X}_0, \mathcal{X}_u \subseteq \mathcal{X}$ are defined as in (4). Then, system S is not δ-approximate infinite-step opacity.

Proof: The proof of this proposition follows by combining the result of Proposition 2 and Theorem 2 in [15].

However, we should note that the definitions of the sets $\mathcal{X}_0$ and $\mathcal{X}_u$ are different in order to capture different notions of opacity. ■

IV. Verifying Other Notions of Approximate Opacity

In the previous section, we presented a methodology to verify approximate infinite-step opacity by searching for a certain type of barrier certificates. There are other notions of state-based opacity, including initial-state opacity, current-state opacity, and K-step opacity, which can be used to capture different types of privacy requirements in real-world applications [2]. In the sequel, we make some remarks regarding relationships between these notions of state-based opacity in the context of verification. Specifically, we first show approximate infinite-step opacity implies approximate initial-state, current-state, and K-step opacity. We should note that similar results does not hold for the lack of opacity. Then, we further show that for a class of so-called invertible systems, the problem of verifying current-state opacity can be solved by the verification of initial-state opacity of its time-reversed system.

Let us first recall from [16] the formal definitions of approximate initial-state, current-state and K-step opacity.

Definition 5: **(Approximate initial-state, current-state and K-step opacity)** Given $\delta \in \mathbb{R}^+$, a system S as in Definition 1 is said to be

- δ-approximate *initial-state* opaque if for any $x_0 \in X_0 \cap X_s$ and any finite state run $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$, there exists $\hat{x}_0 \in X_0 \setminus X_s$ and a finite state run $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}} = \{\hat{x}_0, \ldots, \hat{x}_n\}$ such that $\max_{i\in[0;n]} ||h(x_i) - h(\hat{x}_i)|| \leq \delta$.
- δ-approximate *current-state* opaque if for any $x_0 \in X_0$ and any finite state run $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$ such that $x_n \in X_s$, there exists $\hat{x}_0 \in X_0$ and a finite state run $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}} = \{\hat{x}_0, \ldots, \hat{x}_n\}$ such that $\hat{x}_n \in X \setminus X_s$ and $\max_{i\in[0;n]} ||h(x_i) - h(\hat{x}_i)|| \leq \delta$.
- δ-approximate K-*step* opaque for a given positive integer K if for any $x_0 \in X_0$ and any finite state run $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$ such that $x_i \in X_s$, $i \in \{n-K, n\}$, there exists $\hat{x}_0 \in X_0$ and a finite state run $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}$ such that $\hat{x}_i \in X \setminus X_s$ and $\max_{i\in[0;n]} ||h(x_i) - h(\hat{x}_i)|| \leq \delta$.

Intuitively speaking, if a system is approximate initial-state opaque (resp. current-state opaque or K-step opaque), then an intruder with imperfect measurement precision cannot make sure whether the initial state (resp. the current state or any state within K steps prior to the current state) is secret or not.

Lemma 1: If a control system S as in Definition 1 is δ-approximate infinite-step opaque, it is also δ-approximate initial-state opaque (resp. current-state opaque and K-step opaque).

Proof: Let us note that the other notions of approximate opacity as in Definition 5 can be regarded as special cases of approximate infinite-step opacity. Specifically, as can be seen from Definition 2, δ-approximate infinite-step opacity requires that the intruder should never know for sure that the system is/was at a secret state for any specific time instant $k \in \{0, \ldots n\}$. When $k = 0$, the notion of approximate infinite-step opacity reduces to approximate initial-state opacity; when $k = n$, infinite-step boils down to current-state opacity. Moreover, note that the notion of K-step opacity requires that the secret should not be revealed within K steps prior to the current instant, while infinite-step opacity captures the entire observation trajectory from initial point up to the current time, which is again stronger then K-step opacity. Therefore, if one can verify that a system S is δ-approximate infinite-step opaque, it suffices to claim that S is also δ-approximate initial-state opaque (resp. current-state opaque and K-step opaque). ■

Based on the relationships between different notions of opacity as in Lemma 1, one can solve the verification problem for other notions of approximate opacity by searching for a barrier certificate as in Definition 4.

Next, we further show that if the dynamics of system S are *invertible* [19], the verification of current-state opacity can be formulated as an initial-state opacity verification problem for the system that starts at the current state, and evolves backwards in time. Let us recall the definition of invertible systems from [19].

Definition 6: **(Invertible system)** Consider a discrete-time control system $S = (X, X_0, X_s, U, f, Y, h)$ as in Definition 1, and let $\forall u \in U$, $f_u = f(\cdot, u) : X \to X$. System S is said to be invertible if for each u in an open neighborhood of U the map f_u is a global diffeomorphism of X.

For an invertible system S as in Definition 6, let us define a discrete-time control system $S^- = (X, X, X_s, U, f^-, Y, h)$ as the time-reversed system of S, where f^- denotes the inverse map of f. We also denote by $\bar{\mathbf{x}}_{\bar{x}_0,\bar{\mathbf{u}}} = \{\bar{x}_0, \ldots, \bar{x}_n\}$ a finite state run of the time-reversed system S^-. The following lemma will be used later in the main result of this section.

Lemma 2: Consider an invertible system S and its associated time-reversed system S^-. Let $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \ldots, x_n\}$ be a finite state run of S, then, there exists an input sequence $\bar{\mathbf{u}}$ in S^- such that $\bar{\mathbf{x}}_{x_n,\bar{\mathbf{u}}} = \{x_n, \ldots, x_0\}$ is a state run of the time-reversed system S^-, and vice versa.

The next proposition shows that the current-state opacity of an invertible system can be verified by showing initial-state opacity of its time-reversed system.

Proposition 2: Consider an invertible system S as in Definition 6. If the time-reversed system S^- is δ-approximate initial-state opaque, then the original system S is δ-approximate current-state opaque.

Proof: Consider an arbitrary finite state run $\{x_0, \ldots, x_n\}$ of system S, where $x_n \in X_s$. Note that from Lemma 2, there exists an input sequence $\bar{\mathbf{u}}$ in S^- such that $\bar{\mathbf{x}}_{x_n,\bar{\mathbf{u}}} = \{x_n, \ldots, x_0\}$ is a state run of the time-reversed system S^-. Since S^- is δ-approximate initial-state opaque, we have from Definition 5 that for the state run $\bar{\mathbf{x}}_{x_n,\bar{\mathbf{u}}} = \{x_n, \ldots, x_0\}$ which starts from secret initial state $x_n \in X_s$, there exists another state run $\{\bar{x}_n, \ldots, \bar{x}_0\}$ starting from a nonsecret initial state $\bar{x}_n \in X \setminus X_s$ such that $\max_{i\in[0;n]} ||h(\bar{x}_i) - h(x_i)|| \leq \delta$.

Again by leveraging Lemma 2, for the state run $\{\bar{x}_n, \ldots, \bar{x}_0\}$ in S^-, there exists an input run $\mathbf{u}$ in S such that $\mathbf{x}_{\bar{x}_0,\mathbf{u}} = \{\bar{x}_0, \ldots, \bar{x}_n\}$ is a state run in S. Note that since $\bar{x}_n \in X \setminus X_s$, and $\max_{i\in[0;n]} ||h(\bar{x}_i) - h(x_i)|| \leq \delta$ holds, we can conclude that the original system is δ-approximate current-state opaque. ■

Based on the results provided in Proposition 2, the problem of verifying current-state opacity for an invertible system can be solved by the verification of initial-state opacity for its time-reversed system. In this context, one can readily resort to the results developed in [15] to search for a barrier certificate tailored to approximate initial-state opacity for the time-reversed system, and then carry back the result to show approximate current-state opacity of the original system.

Remark 2: Note that for a discrete-time control system as in Definition 1 to be invertible, the *Inverse Function Theorem* [20] asks function $f : X \times U \to X$ to be continuously differentiable, and the Jacobian determinant to be nonzero at every point (x, u) in its domain. This can be a strong assumption for a system. However, global invertibility of f might be granted under some circumstances. If a discrete-time system is obtained by sampling continuous-time solutions of a set of finite-dimensional differential equations over a time interval with control input u, the discrete-time system is invertible [19]. Assume we have an Ordinary Differential Equation (ODE) in the form

$$\begin{aligned} \dot{x} &= g\big(x(t), t, u(t)\big), \\ x(0) &= x_0. \end{aligned}$$

Consider the state of the above ODE at an arbitrary time T. Since t is always increasing, we define $y(t) = x(T - t)$ to represent the state sequence of this system backwards in time. The evolution of y is described by

$$\begin{aligned} \dot{y} &= -\dot{x}(T-t) = -g\big(x(T-t), T-t, u(T-t)\big) \\ &= -g\big(y(t), T-t, u(T-t)\big), \\ y(0) &= x(T). \end{aligned}$$

Therefore, such systems are always invertible, and the inverse is achieved by switching the sign of g.

V. Case Study

A. SOS Programming

For systems with polynomial transition functions f and semi-algebraic sets X_0, X_s, and X, we can use sum-of-squares (SOS) programming to search for polynomial barrier certificates. We showed previously in [15] that each of the sets as in (4) is a semi-algebraic set which can be defined using polynomial inequalities. Since basic semi-algebraic sets are closed under finite union and intersection [21], sets $\mathcal{X}_u$ and $\mathcal{X}_0$ are also semi-algebraic.

We follow the same strategy as in [15, Sec. IV], and use SOSTOOLS [22] together with a semidefinite programming solver SeDuMi [23] to compute barrier certificates in the following case study.

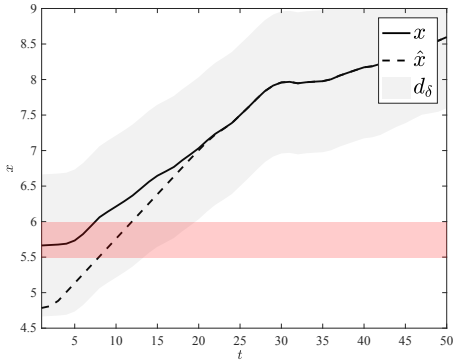

Fig. 1: State run $\mathbf{x}_{x_0,\mathbf{u}}$ of an infinite-step opaque system along with an alternative trajectory $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}$ which does not enter the secret set. The shaded area in grey d_δ is within $\delta = 1$ distance from the actual trajectory of the system, and the red region specifies the unsafe set.

B. Infinite-step opacity

Consider an autonomous vehicle moving on a single lane road, whose state variable is defined as $x = [x_1; x_2]$, with x_1 being its absolute position (in the road frame) and x_2 being its absolute velocity. The discrete-time dynamics of the vehicle is modeled as:

$$\begin{aligned} \begin{bmatrix} x_1(t+1) \\ x_2(t+1) \end{bmatrix} &= \begin{bmatrix} 1 & \Delta\tau \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \begin{bmatrix} \Delta\tau^2/2 \\ \Delta\tau \end{bmatrix} u(t), \\ y(t) &= \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}, \end{aligned} \tag{8}$$

where u is the control input, and $\Delta\tau$ is the sampling time. The system output is the position of the vehicle on the road. Assume there is an intruder with δ measurement precision trying to gain information on the position of the vehicle. We first want to answer whether the system is able to conceal its position in every time step. Applying our theoretical results, we formulate this problem as a δ-approximate infinite-step opacity verification problem. Let $X = X_0 = [0, 10]$, $X_s = [5.5, 6]$, $U = [-0.05, 0.05]$, $\delta = 1$, and $\Delta\tau = 1s$. By considering the augmented system and constructing the regions of interest as in (4), we found a barrier certificate by solving SOS programming with the help of SOSTOOLS. By Theorem 1, we conclude that the system is 1-approximate infinite-step opaque. Figure 1 presents the simulation results of this scenario. As we observe from this figure, for every time step which the location of the vehicle belongs to the secret set, the alternative trajectory passes through a position that does not belong to the secret set, and is within δ distance from it.

C. Current-state opacity

In the last subsection, we showed that the system in (8) is 1-approximate infinite-step opaque. Note that by the relationships between different notions of approxiamte opacity as in Lemma 1, we can readily conclude that the system is also 1-approximate current-state opaque. In this subsection, we aim to verify the current-state opacity for the vehicle model by following the strategy discussed in Proposition

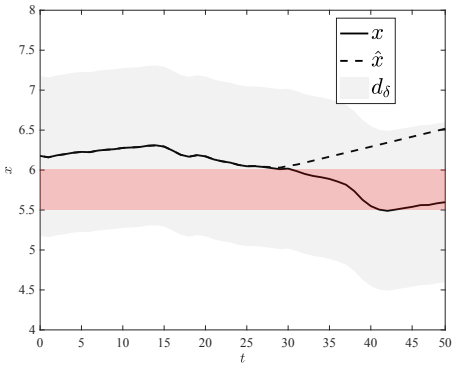

Fig. 2: State run $\mathbf{x}_{x_0,\mathbf{u}}$ of an infinite-step opaque system along with an alternative trajectory $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}$ which does not enter the secret set. The shaded area in grey d_δ is within $\delta = 1$ distance from the actual trajectory of the system, and the red region specifies the unsafe set.

2. In particular, we show the current-state opacity of the original vehicle model by verifying initial-state opacity of its associated reverse dynamic model, which can be described as

$$\begin{aligned} \begin{bmatrix} x_1(t+1) \\ x_2(t+1) \end{bmatrix} &= \begin{bmatrix} 1 & -\Delta\tau \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \begin{bmatrix} \Delta\tau^2/2 \\ -\Delta\tau \end{bmatrix} u(t), \\ y(t) &= \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix}. \end{aligned} \tag{9}$$

Using the same strategy as in [15], we aim to verify initial-state opacity for the system as in (9). A barrier certificate is found for the associated augmented system of the reverse model by solving an SOS programming problem with the help of SOSTOOLS. Note that by [15, Theorem 1], we can conclude that the reverse system in (9) is 1-approximate initial-state opaque. By further leveraging the results in Proposition 2, this implies 1-approximate current-state opacity for the original system in (8). Figure 2 presents the results of our simulation, which illustrates 1-approximate initial-state opacity for the system in (9).

VI. Conclusions and Future Directions

We studied the problem of verifying approximate infinite-step opacity for discrete-time control systems. We posed opacity as a safety property over an augmented system, and aimed to verify it by finding a barrier certificate. Failure to find such barrier certificate does not imply lack of opacity of the system. To ensure the lack of opacity, we formulated a reachability verification problem on the augmented system, where finding a barrier certificate guarantees the lack of opacity of the system. We made brief remarks on the connection between different notions of approximate opacity, and study the conditions under which one form of opacity implies another. Finally, we demonstrated the effectiveness of our approach through two numerical examples. The first example presents the verification of approximate infinite-step opacity for a vehicle. In the second example, we present an example of an invertible system, where verifying current-state opacity can be posed as an initial-state opacity verification problem. Our plan for future research directions is to synthesize controllers to enforce opacity in systems that do not originally satisfy the requirements for opacity.

References

[1] S. Lafortune, F. Lin, and C. N. Hadjicostis, "On the history of diagnosability and opacity in discrete event systems," *Annual Reviews in Control*, vol. 45, pp. 257–266, 2018.

[2] A. Saboori and C. N. Hadjicostis, "Notions of security and opacity in discrete event systems," in *2007 46th IEEE Conference on Decision and Control*. IEEE, 2007, pp. 5056–5061.

[3] ——, "Verification of K-step opacity and analysis of its complexity," *IEEE Transactions on Automation Science and Engineering*, vol. 8, no. 3, pp. 549–559, July 2011.

[4] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using petri nets," *IEEE Transactions on Automatic Control*, 2017.

[5] J. Bryans, M. Koutny, L. Mazaré, and P. Ryan, "Opacity generalised to transition systems," *International Journal of Information Security*, vol. 7, no. 6, pp. 421–435, 2008.

[6] F. Lin, "Opacity of discrete event systems and its applications," *Automatica*, vol. 47, no. 3, pp. 496–503, 2011.

[7] J. Dubreil, P. Darondeau, and H. Marchand, "Supervisory control for opacity," *IEEE Transactions on Automatic Control*, vol. 55, no. 5, pp. 1089–1100, 2010.

[8] A. Saboori and C. N. Hadjicostis, "Verification of infinite-step opacity and complexity considerations," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1265–1269, 2012.

[9] 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.

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

[11] B. Ramasubramanian, R. Cleaveland, and S. I. Marcus, "Notions of centralized and decentralized opacity in linear systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 4, pp. 1442–1455, 2019.

[12] M. Ahmadi, B. Wu, H. Lin, and U. Topcu, "Privacy verification in POMDPs via barrier certificates," in *2018 IEEE Conference on Decision and Control*, 2018, pp. 5610–5615.

[13] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2004, pp. 477–492.

[14] S. Prajna and A. Rantzer, "Primal–dual tests for safety and reachability," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2005, pp. 542–556.

[15] S. Liu and M. Zamani, "Verification of approximate opacity via barrier certificates," *IEEE Control Systems Letters*, vol. 5, no. 4, pp. 1369–1374, 2021.

[16] X. Yin, M. Zamani, and S. Liu, "On approximate opacity of cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 4, pp. 1630–1645, 2021.

[17] S. Liu, X. Yin, and M. Zamani, "On a notion of approximate opacity for discrete-time stochastic control systems," in *American Control Conference*, 2020, pp. 5413–5418.

[18] S. T. Kalat, S. Liu, and M. Zamani, "Modular verification of opacity for interconnected control systems via barrier certificates," *IEEE Control Systems Letters*, 2021.

[19] B. Jakubczyk and E. D. Sontag, "Controllability of nonlinear discrete-time systems: A lie-algebraic approach," *SIAM Journal on Control and Optimization*, vol. 28, no. 1, pp. 1–33, 1990.

[20] F. Clarke, "On the inverse function theorem," *Pacific Journal of Mathematics*, vol. 64, no. 1, pp. 97–102, 1976.

[21] J. Harris, *Algebraic geometry: a first course*. Springer Science & Business Media, 2013, vol. 133.

[22] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, and P. Parrilo, "SOSTOOLS version 3.00 sum of squares optimization toolbox for MATLAB," *arXiv preprint arXiv:1310.4716*, 2013.

[23] J. F. Sturm, "Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones," *Optimization methods and software*, vol. 11, no. 1-4, pp. 625–653, 1999.