2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

A data-driven approach to approximate opacity verification

Vishnu Murali, Shadi Tasdighi Kalat, and Majid Zamani

Abstract— **Recent results in the verification of cyber-physical systems have focused not just in giving guarantees of properties such as safety, but also in ensuring that these systems are *secure*. One such notion of security is that of initial-state opacity, where one seeks to ensure that an outside intruder is not able to determine some sensitive information about the initial-state of the system by observing the output traces. An existing approach to verify the initial-state opacity of a system relies on finding a barrier certificate over an appropriately constructed augmented system. However this search for a barrier certificate relies on the dynamics of the system being known. Unfortunately, in many scenarios, it may be difficult or infeasible to determine the dynamics of a given system.**

We thus consider the problem of determining whether a system is opaque when its dynamics are *unknown*. To do so, we recast the conditions of opacity on the augmented system as a robust program with uncountably many constraints. By collecting data from the system's trajectories, we construct a corresponding scenario program. We show that if a feasible solution of the scenario program satisfies some conditions, then the original system with unknown dynamics is opaque under reasonable assumptions. We show the effectiveness of the proposed approach by demonstrating the opacity of a room-temperature model.

I. Introduction

Broad deployment, and access to sensitive data makes many of the cyber-physical systems (CPS) vulnerable to attacks and information leaks. CPS has traditionally been verified against temporal logic specifications [1], [2], [3], [4], [5], which stipulate properties on the set of system executions. While these properties can express a wide range of requirements that take individual CPS execution traces into account, they are unable to capture other properties concerned with information-flow features and planning objectives that require relating different execution traces. These properties that rely on relations between traces have been collectively called hyperproperties [6]. A key hyperproperty is that of *opacity* [7]. Opacity is a security property that is concerned with the system's information flow. It refers to a system's secret's plausible deniability in the presence of an outside intruder. Different concepts of information flow properties are discussed in [8], [9], [10], and different notions of opacity have been discussed in [11], however in all cases these information flow properties are not defined over individual traces but rather depend on the relation between traces of a system. Another key challenge faced in the verification of CPS is knowing the system model. In many cases finding or determining such a closed form expression may be difficult or infeasible, either practically (when identifying the model may be difficult) or to preserve intellectual property information. We thus consider the problem of verifying approximate opacity for unknown systems and provide a sound guarantee.

We observe that one faces challenges when verifying opacity even when one has an exact model of a system. While there exist complete decision procedures to verify notions of opacity for finite state While systems [12], [10], the problem is undecidable for infinite state systems. This follows from the fact that verifying simple trace properties such as safety are undecidable. Thus verifying properties such as even reachability for CPS with uncountable state spaces turn out to be undecidable [13], and these challenges carry over for opacity verification. Secondly, one may no longer use standard abstraction based approaches as they do not preserve hyperproperties [12]. Lastly, unlike in the case of finite programs, the output observations for CPS tend to be real values over an uncountable set. In many cases, it is unrealistic to expect an intruder to be able to precisely measure these observations. Thus the authors of [14] proposed a notion of *approximate opacity*. This definition takes into account the intruder's measurement precision, which is specified by a parameter δ. Here, any pair of observations separated by a distance that is less than δ are indistinguishable to the intruder.

Recent results in [15] provide guarantees for opacity by recasting the problem to that of synthesizing a controller to ensure the safety of an "augmented" system. To do so, the authors provide a sound guarantee through the use of barrier certificates [16]. This allows for one to make use of optimization approaches such as semidefinite programming to automatically search for barrier certificates that act as proofs of opacity. These approaches have since been extended for interconnected systems [17], as well as in designing controllers to ensure opacity [18].

However these approaches are inapplicable when the system dynamics are *unknown*. Recent results [19], [20] on data-driven approaches to compute barrier certificates, rely on the scenario approach [21], [22] to verify safety based on the connection between robust convex programs, chance-constrained programs and scenario convex programs [23]. Unfortunately, these approaches can not be extended to search for a controller to ensure the opacity of a system as the problem is no longer convex. While results exist in the nonconvex case [24], all of the above rely on relating solutions of scenario programs to robust ones via chance-constrained programs. All of the above mentioned results provide a confidence while giving a guarantee of safety.

This work was supported by the NSF under Grant ECCS-2015403.

V. Murali, S. Tasdighi Kalat and M. Zamani are with the Department of Computer Science at the University of Colorado, Boulder, USA. Emails: {vishnu.murali, shadi.tasdighi.kalat, majid.zamani}@colorado.edu

To consider a data-driven approach for opacity, we provide a direct relation between the scenario and robust programs and so our approach provides a sure (100%) guarantee. To do so, we partition the state-set of an "augmented" system into finitely many regions. We then select representative points from these regions and construct a scenario program. If the solution for the scenario program satisfies some conditions, under reasonable assumptions, then we can formally verify that the system is approximately opaque.

II. Problem Definition

We let $\mathbb{R}$, $\mathbb{Z}$, and $\mathbb{N}$ to denote the set of real numbers, integers, and non-negative integers respectively. For $a \in \mathbb{R}$, we write $\mathbb{R}_{\geq a}$ and $\mathbb{R}_{>a}$ for the intervals $[a, \infty[$ and $]a, \infty[$, respectively. We write $\mathbb{Z}_{\geq n}$ and $\mathbb{N}_{\geq n}$ for the set of integers and non-negative integers greater than or equal to $n \in \mathbb{Z}$. We denote an infinite sequence using the angular bracket notation $\langle a_1, a_2, \ldots \rangle$ and a finite sequence as $(a_1, a_2, \ldots a_n)$. For sets A,B, we write $|A|$ for the cardinality and A^n for its n-ary Cartesian power. The Cartesian product of A and B is defined by $A \times B = \{(x, y) | x \in A, y \in B\}$. Given sets A, B, and a function $f : A \to B$, we define the product of the function f with itself as the function $(f \times f) : A \times A \to B \times B$, where for all $a_1, a_2 \in A$, $(f \times f)(a_1, a_2) = (f(a_1), f(a_2))$. As usual, we use $\wedge$, $\vee$, and $\implies$ to denote logical conjunction, disjunction, and implication, respectively. Given a vector $v \in \mathbb{R}^n$, we use $||v||$, and $|v|_\infty$, to denote its 2-norm, and ∞-norm, respectively. A ball of radius $r \in \mathbb{R}_{>0}$ centered at point $p \in \mathbb{R}^n$ with respect to a distance metric $\zeta : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ is the set $\{x \in \mathbb{R}^n \mid \zeta(p, x) \leq r\}$.

A. Optimization Programs

Given an action or decision space $D \subseteq R^l$, an infinite set Q, and a measurable function $g : D \times Q \to \mathbb{R}$ we consider the following two optimization problems.

(1) **Robust Programs (RP)** An optimization problem is a RP, with a parameter if it is of the form:

$$\text{RP}_\xi : \begin{cases} \min\limits_{d} & c^T d \\ \text{subject to} & g(d, q) \leq 0 \quad \text{for all } q \in Q. \end{cases}$$

We abbreviate this as RP when the parameter ξ is set to 0.

(2) **Scenario Program (SP)** An optimization problem is a scenario program if it of the form:

$$\text{SP} : \begin{cases} \min\limits_{d} & c^T d \\ \text{subject to} & g(d, q_i) \leq 0 \quad \text{for } q_1, \ldots, q_N \in Q. \end{cases}$$

We refer to the function $c^T d$ as the objective or the cost function. A value $d \in D$ is a feasible solution for a robust (scenario) program if it satisfies the constraints of the problem. We say a value $d_{opt} \in D$ is an optimal solution if $c^T d_{opt} \leq c^T d$ for all $d \in D$.

B. Discrete-time Control Systems

A discrete-time control system $\mathfrak{S}$ is a tuple (X, X_0, U, f, Y, h), where $X \subseteq \mathbb{R}^n$ denotes the state set of the system, $X_0 \subseteq X$ is the set of initial states, $U = \{u_1, \ldots, u_m\}$ denotes the set of finite control inputs, $Y \subseteq R^p$ denotes the set of outputs, and functions $f : X \times U \to X$, and $h : X \to Y$ are the state transition function and output function, respectively. The state evolution of the system $\mathfrak{S}$ is described by the following difference equations:

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

A *trace* or *state sequence* is an infinite sequence $\mathbf{x}_{x_0, \mathbf{u}} = \langle x_0, x_1, \ldots \rangle$ of the system starting from a state x_0 under an input sequence $\mathbf{u} = \langle u_0, u_1, \ldots \rangle$, such that $x_{i+1} = f(x_i, u_i)$ for all $i \in \mathbb{N}$. We denote the corresponding output of this trace as $\mathbf{y} = \langle y_0, y_1, \ldots \rangle$, such that $y_i = h(x_i)$ for all $i \in \mathbb{N}$. Throughout the rest of the paper we assume the state set X to be uncountable but compact.

C. Approximate Opacity Verification via Barrier Certificates

We first define the notion of δ-approximate opacity for a system $\mathfrak{S}$ with respect to a parameter $\delta \in \mathbb{R}_{>0}$, and set of secret states $X_s \subseteq X$ as follows.

Definition 2.1: A discrete-time control system $\mathfrak{S}$ is said to be δ-approximate initial-state opaque for some $\delta \in \mathbb{R}_{>0}$ and a secret set of states $X_s \subseteq X$, if: for any state run $\mathbf{x}_{x_0, \mathbf{u}} = \langle x_0, \ldots, \rangle$, that starts from some secret state $x_0 \in X_s$, there exists some state run $\mathbf{x}_{\hat{x}_0, \hat{\mathbf{u}}} = \langle x'_0, \ldots, \rangle$ starting from a non-secret state $x'_0 \in X_0 \setminus X_s$ such that: $||h(x_i) - h(x'_i)|| \leq \delta$, for all $i \in \mathbb{N}$.

Intuitively, the definition of approximate initial-state 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 initially. We assume without loss of generality that for all $x_s \in X_0 \cap X_S$, there exists $x_{ns} \in X_0 \setminus X_S$, such that $\|h(x_s) - h(x_{ns})\| \leq \delta$; otherwise, initial-state opacity is trivially violated. To study the opacity for the system $\mathfrak{S}$, we construct the augmented system as the following.

Definition 2.2: Consider a control system $\mathfrak{S}$. We define its associated augmented system as the product of $\mathfrak{S}$ with itself:

$$\mathfrak{S} \times \mathfrak{S} = (\tilde{X}, \tilde{X}_0, \tilde{U}, \tilde{f}, \tilde{Y}, \tilde{h}),$$

where $\tilde{X} = X \times X$ is the state set, the set $\tilde{X}_0 = (X_0 \cap X_s) \times (X_0 \setminus X_s)$ is the initial set of states, $\tilde{U} = U \times U$ is the input set, and $\tilde{Y} = Y \times Y$ is the output set. We define the state transition function as $\tilde{f} = (f \times f)$ and the output function as $\tilde{h} = (h \times h)$. We use the notation $\tilde{x} = (x, x') \in \tilde{X}$ to denote a state, $\tilde{u} = (u, u') \in \tilde{U}$ a control input, and $\tilde{y} = (y, y') \in \tilde{Y}$ an output of $\mathfrak{S} \times \mathfrak{S}$. Let $(\mathbf{x}_{x_0, \mathbf{u}}, \mathbf{x}_{\hat{x}_0, \hat{\mathbf{u}}})$ denote the trace of $\mathfrak{S} \times \mathfrak{S}$ starting from $\tilde{x}_0 = (x_0, x'_0)$ under input sequence $(\mathbf{u}, \mathbf{u}')$, and define the set $\tilde{X}_u = \{(x, x') \mid \|h(x) - h(x')\| > \delta\}$, *i.e.*, the set of all pairs of states such that the distance

between their outputs is greater than δ. Now we define the notion of augmented barrier certificates.

Definition 2.3: We say a function $\mathcal{B} : \tilde{X} \to \mathbb{R}$ is an *augmented barrier certificate* for a system $\mathfrak{S} \times \mathfrak{S}$ with initial states $\tilde{X}_0$ and unsafe states $\tilde{X}_u$ if there exists $\gamma < \lambda$ satisfying:

$$\mathcal{B}(\tilde{x}) \leq \gamma, \quad \text{for all } \tilde{x} \in \tilde{X}_0, \tag{2}$$

$$\mathcal{B}(\tilde{x}) \geq \lambda, \quad \text{for all } \tilde{x} \in \tilde{X}_u, \text{ and} \tag{3}$$

$$\text{for all } \tilde{x} \in \tilde{X} \setminus \tilde{X}_u, \text{for all } u \in U, \text{there exists } u' \in U,$$

$$\mathcal{B}\big(\tilde{f}(\tilde{x}, \tilde{u})\big) - \mathcal{B}(\tilde{x}) \leq 0. \tag{4}$$

A system $\mathfrak{S}$ is initial-state opaque if there exists an augmented barrier certificate $\mathcal{B} : \tilde{X} \to \mathbb{R}$ as in Definition 2.3. This follows from [15, Theorem 5], by ensuring that for any trace starting from a secret state, there exists another trace starting from a non-secret state such that the difference in their observations are not more than δ far apart. When the control input set $U = \{u_1, \ldots, u_m\}$ is finite, we can rewrite condition (4) as:

$$\text{for all } \tilde{x} \in \tilde{X},$$

$$\bigwedge_{(1\leq i\leq m)} \bigvee_{(1\leq j\leq m)} \Big(\mathcal{B}\big(\tilde{f}(\tilde{x}, \tilde{u}_{i,j})\big) - \mathcal{B}(\tilde{x}) \leq 0\Big), \tag{5}$$

where $\tilde{u}_{i,j} = (u_i, u_j)$. For easier readability, we use $\phi(\tilde{x}, \tilde{u}_{i,j})$ to denote $\Big(\mathcal{B}\big(\tilde{f}(\tilde{x}, \tilde{u}_{i,j})\big) - \mathcal{B}(\tilde{x}) \leq 0\Big)$, and abbreviate condition (5) as $\bigwedge_{(1\leq i\leq m)} \bigvee_{(1\leq j\leq m)} \phi(\tilde{x}, \tilde{u}_{i,j})$.

D. Opacity Verification for Unknown Systems

To reason about opacity for "unknown" systems, we rely on the following assumptions. We consider the system $\mathfrak{S}$ to be "unknown", in the sense that the only way to acquire knowledge about its transition function f is through samples.

Assumption 1: We assume that we can initialize the system at any state $x \in X$, and simulate it to collect the points $\mathcal{D}_x = \{x, f(x, u_1), \ldots, f(x, u_m)\}$.

We consider augmented barrier certificates to be continuous functions that are weighted sums of z user-defined basis functions $p_1(\tilde{x}), \ldots, p_z(\tilde{x})$, *i.e.*, $\mathcal{B}(\tilde{x}) = \sum_{j=1}^{z} b_j p_j(\tilde{x})$. In a specific case, where the barrier certificates are polynomials, functions p_j are monomials. As a result, the search for barrier certificates as in Definition 2.3, reduces to a search for the values $b_1, \ldots, b_z$ such that the function $\mathcal{B}(b, \tilde{x})$that satisfies conditions (2) to (4).

The key problem we study in this paper is as follows:

Problem 1 (Opacity verification for Unknown Systems): Given a system $\mathfrak{S}$, where the state transition function f is unknown, parameter $\delta \in \mathbb{R}_{\geq 0}$, and a set of secret states $X_s \subseteq X$, verify whether $\mathfrak{S}$ is δ-approximate initial-state opaque.

III. A Scenario-Based Approach to Verify Opacity

We present a data-driven approach to solve Problem 1, and thus verify δ-approximate initial state opacity for an unknown system $\mathfrak{S}$. To do so, we frame the search for a barrier certificate over the augmented system as in Definition 2.3 as an optimization problem. Conditions (2) and (3) can easily be framed as constraints of an optimization problem, however to frame disjunction and quantification in condition (4), we first assume that the system has finitely many inputs, and so we instead consider equation (5). Observe that this conjunction can be split into m different constraints each of the form $c_i = \bigvee_{(1\leq j\leq m)} \phi(\tilde{x}, \tilde{u}_{i,j})$ for each $1 \leq i \leq m$. We now replace each of these disjunctions with a different constraint that provides a sufficient condition via the S-procedure [25].

Lemma 1: The existence of values $\tau_{i,0}, \ldots, \tau_{i,m-1} \in \mathbb{R}_{\geq 0}$ satisfying the following condition:

$$\begin{aligned}&(\mathcal{B}(\tilde{x}) - \mathcal{B}(\tilde{f}(\tilde{x}, \tilde{u}_{i,m})))\\ &- \sum_{j=1}^{m-1} \tau_{i,j}(\mathcal{B}(\tilde{f}(\tilde{x}, \tilde{u}_{i,j})) - \mathcal{B}(\tilde{x})) \geq 0\end{aligned} \tag{6}$$

implies the satisfaction of $\bigvee_{(1\leq j\leq m)} \phi(\tilde{x}, \tilde{u}_{i,j})$ for each $1 \leq i \leq m$.

Finally, we consider the decision variables of the optimization problem to be elements of a vector containing a "deflation parameter" η, γ, and λ from conditions (2) and (3), weights b of the non-linear basis functions, and the variables introduced by S-procedure $\tau_{i,j}$ for every $1 \leq i \leq m$ and $1 \leq j < m$ collected as a vector τ. We consider three sets $\tilde{X}_0$, $\tilde{X}$, and $\tilde{X}_u$, and denote elements of these sets as $\tilde{x}_0$, $\tilde{x}$, and $\tilde{x}_u$, respectively.

This allows us to reformulate the search for a barrier certificate as in Definition 2.3 as the following RP.

$$\text{RP} : \begin{cases} \min\limits_{d} \quad \eta \\ \text{s.t.} \quad g_1(d, \tilde{x}_0) \leq 0, \text{ for all } \tilde{x}_0 \in \tilde{X}_0 \\ \quad\; g_2(d, \tilde{x}_u) \leq 0, \text{ for all } \tilde{x}_u \in \tilde{X}_u \\ \quad\; \max\limits_{1\leq i\leq m} \{g_{i+2}(d, \tilde{x})\} \leq 0, \text{ for all } \tilde{x} \in \tilde{X} \setminus \tilde{X}_0 \\ \quad\; d = [\eta; \gamma; \lambda; \tau; b], \eta, \gamma, \lambda \in \mathbb{R}, \\ \quad\; \tau_{i,j} \in \mathbb{R}_{\geq 0}, \text{ for all } 0 \leq i \leq m, b \in \mathbb{R}^z, \end{cases}$$

where,

$$g_1(d, \tilde{x}) = (\mathcal{B}(b, \tilde{x}_0) - \gamma) - \eta, \tag{7}$$

$$g_2(d, \tilde{x}) = (-\mathcal{B}(b, \tilde{x}_u) + \lambda) - \eta, \tag{8}$$

$$\begin{aligned} g_3(d, \tilde{x}) = &(\mathcal{B}(b, \tilde{f}(\tilde{x}, \tilde{u}_{1,m})) - \mathcal{B}(b, \tilde{x})) \\ &+ \sum_{j=1}^{m-1} \tau_{1,j}(\mathcal{B}(b, \tilde{f}(\tilde{x}, \tilde{u}_{1,j}))\mathcal{B}(b, \tilde{x})) - \eta, \end{aligned} \tag{9}$$

$$\vdots$$

$$\begin{aligned} g_{m+1}(d, \tilde{x}) = &(\mathcal{B}(b, \tilde{f}(\tilde{x}, \tilde{u}_{(m-1),m})) - \mathcal{B}(b, \tilde{x})) \\ &+ \sum_{j=1}^{m-1} \tau_{(m-1),j}(\mathcal{B}(b, \tilde{f}(\tilde{x}, \tilde{u}_{(m-1),j})) \\ &- \mathcal{B}(b, \tilde{x})) - \eta, \end{aligned} \tag{10}$$

$$g_{m+2}(d, \tilde{x}) = \gamma + \epsilon - \lambda - \eta, \tag{11}$$

and $\epsilon \in \mathbb{R}_{>0}$ is a small positive value.

Let the optimal solution of RP be η^*_{rp}. If $\eta^*_{rp} \leq 0$, then conditions (7)-(8) imply the satisfaction of conditions (2)-(3), while condition condition (11) ensures that $\gamma < \lambda$. Conditions (9)-(10) imply the condition (5). Thus a solution to RP with $\eta^*_{rp} \leq 0$ gives us an augmented barrier certificate and acts as a proof of opacity. The value η acts as a deflation parameter as decreasing it makes the conditions of the barrier certificate more difficult to satisfy and hence "deflates" the set of points where these conditions hold. Unfortunately, the above RP has uncountably many constraints as the sets $\tilde{X}$, $\tilde{X}_0$, and $\tilde{X}_u$ are uncountable. A further challenge is that we cannot leverage techniques such as sum-of-squares programming or semidefinite programming as these approaches rely on the knowledge of the function $\tilde{f}$. We observe that conditions (4)-(10) contain terms $\tilde{f}(\tilde{x}, \tilde{u}_{i,j})$ for every point $\tilde{x} \in \tilde{X}$ and every input pair (u_i, u_j), for all $1 \leq i \leq m$ and $1 \leq j \leq m$.

To adopt a data-driven technique, we construct a SP by collecting a finite set of samples $\mathcal{S} = \{\hat{\tilde{x}}_1, \ldots, \hat{\tilde{x}}_N\}$ from the augmented system as follows. First, we pick a discretization parameter $\zeta \in \mathbb{R}_{>0}$, and cover the state set $\tilde{X}$ of the augmented system by finitely many sets $\tilde{X}_1, \ldots, \tilde{X}_N$ such that $\tilde{X} \subseteq \bigcup_{1 \leq i \leq N} \tilde{X}_i$. We then pick the points $\hat{\tilde{x}}_i$ for every cover element $1 \leq i \leq N$ such that for every $\tilde{x} \in \tilde{X}$, there exists some point $\hat{\tilde{x}}_j \in \tilde{X}_j$ with $||\hat{\tilde{x}}_j - \tilde{x}|| \leq \zeta$ for some $1 \leq j \leq N$. One way to do this is to cover the state set of the augmented system by finitely many balls each with radius ζ and select the centers of these balls as sample points.

Observe that $\hat{\tilde{x}}_i$ consists of a pair of points $(\hat{x}, \hat{x}')$. From Assumption 1, we can construct the sets $\mathcal{D}_{\hat{x}} = \{\hat{x}, f(\hat{x}, u_1), \ldots, f(\hat{x}, u_m)\}$, and $\mathcal{D}_{\hat{x}'} = \{\hat{x}', f(\hat{x}', u_1), \ldots, f(\hat{x}', u_m)\}$. We can use the elements from these sets to thus construct the set $\mathcal{D}_{\hat{\tilde{x}}} = \{\hat{\tilde{x}}_i, \tilde{f}(\hat{\tilde{x}}, \tilde{u}_{1,1}), \ldots, \tilde{f}(\hat{\tilde{x}}, \tilde{u}_{m,m})\}$, where $\tilde{u}_{i,j} = (u_i, u_j)$ for all $1 \leq i \leq m$ and $1 \leq j \leq m$.

This allows us to construct the scenario program SP as follows:

$$\text{SP}: \begin{cases} \min\limits_{d} \quad \eta \\ \text{s.t.} \quad g_1(d, \tilde{x}_0) \leq 0, \text{ for all } \tilde{x}_0 \in \mathcal{S} \cap \tilde{X}_0 \\ \quad\quad g_2(d, \tilde{x}_u) \leq 0, \text{ for all } \tilde{x}_u \in \mathcal{S} \cap \tilde{X}_u \\ \quad\quad \max\limits_{1 \leq i \leq m} \{g_{i+2}(d, \tilde{x})\} \leq 0, \text{ for all } \tilde{x} \in \mathcal{S} \cap \tilde{X} \setminus \tilde{X}_0 \\ \quad\quad d = [\eta; \gamma; \lambda; \tau; b], \eta, \gamma, \lambda \in \mathbb{R}, \\ \quad\quad \tau_{i,j} \in \mathbb{R}_{\geq 0}, \text{ for all } 0 \leq i \leq m, b \in \mathbb{R}^z, \end{cases}$$

where functions g_j are the same as in conditions (7)-(11) for all $1 \leq j \leq m+2$. Observe that the set $\mathcal{S}$ has finitely many points and so one can determine whether each point is in the set $\tilde{X}_0$, $\tilde{X}_u$, or $\tilde{X} \setminus \tilde{X}_u$, respectively. Furthermore, the above program has finitely many constraints.

Assumption 2: We assume that functions $g_3(d, \tilde{x}), \ldots, g_{m+1}(d, \tilde{x})$ to Lipschitz-continuous in $\tilde{X} \setminus \tilde{X}_u$ with Lipschitz constants $\mathcal{L}_{g_3}, \ldots, \mathcal{L}_{g_{m+1}}$ with respect to the 2-norm. Let the maximum of these be denoted as $\mathcal{L}'$.

The following theorem indicates when a solution for SP can be used as an augmented barrier certificate to verify that a system is δ-approximate initial-state opaque.

Theorem 1: Consider an unknown system $\mathfrak{S} = (X, X_0, X_s, U, f, Y, h)$, value $\delta \in \mathbb{R}_{>0}$ to specify the parameter for approximate opacity, and $X_s \subseteq X$ to indicate a secret set of states. Let the augmented state set of the system be partitioned into N finite covers. Construct SP by selecting representative points for each cover element, such that for every state $\tilde{x} \in \tilde{X}$, there exists some cover element $\hat{\tilde{x}}$ whose distance is at most ζ. Let the values of the decision variables for the sub-optimal solution of SP be $d^*_{sp} = [\eta^*; \gamma^*; \lambda^*; \tau^*; b^*]$. If $\eta^* + \mathcal{L}'\zeta \leq 0$, and conditions (2) and (3) hold, then the system is δ-approximate initial-state opaque.

Proof: First, observe that conditions (2) and (3) can be checked by substituting the values of b^*, λ^*, and γ^* in the candidate certificate $\mathcal{B}(b, \tilde{x})$ as they do not depend on the transition function of the system. Thus, one can exactly check if the above conditions are satisfied or not. We now need to show that condition (9) holds, or equivalently that conditions (9) to (10) hold for every state $\tilde{x} \in \tilde{X}$. We observe that any point $\tilde{x} \in \tilde{X}$, there exists some sample point $\tilde{x}_i \in \mathcal{S}$, such that $||\tilde{x} - \tilde{x}_i|| \leq \zeta$. Since functions $g_1, \ldots, g_{m+1}$ are Lipschitz-continuous, one has $||g_j(d^*, \tilde{x}) - g_j(d^*, \tilde{x}_i)|| \leq \mathcal{L}'||\tilde{x} - \tilde{x}_i||$. From reverse triangle inequality, one obtains $g_j(d^*, \tilde{x}) \leq g_j(d^*, \tilde{x}_i) + \mathcal{L}'||\tilde{x} - \tilde{x}_i||$. Thus, for every $\tilde{x} \in \tilde{X}$, one has $g_j(d^*, \tilde{x}) \leq g_j(d^*, \tilde{x}_i) + \mathcal{L}'\zeta$ for all $2 \leq j \leq m+1$. If $\eta^* + \mathcal{L}'\zeta \leq 0$, then we have $g_j(d^*, \tilde{x}) \leq 0$ for all $\tilde{x} \in \tilde{X}$. This concludes that the function $\mathcal{B}(b^*, x)$ is an augmented barrier certificate and, hence, the system is δ-approximate initial-state opaque. ■

We should add that we proved Theorem 1 by assuming the functions g_j to be Lipschitz-continuous with respect to the 2-norm for all $2 \leq j \leq m+1$. We can equivalently, consider the theorem for other norms as well. Now, we discuss techniques to solve the scenario program SP and determine the Lipschitz constants of the constraints to verify the δ-approximate initial-state opacity of a system.

A. Computation of Barrier Certificates and Lipschitz-constants

To construct the scenario program SP, we first partition the augmented state space $\tilde{X}$ into finitely many balls, with respect to a norm. We then take the centers of these balls to denote the sample points, and then simulate the system for one unit of time from these points by applying every possible input. We consider the template for the augmented barrier certificate as a polynomial of a fixed degree d. Therefore, its basis functions p_j are monomials. We substitute the values of the sample points in conditions (7) to (11) to construct SP. Now, we search for an augmented barrier certificate by solving SP. As the above program is bilinear, we make use of V-K iteration [26]. We take an initial guess for the values of variables $\tau_{0,0}, \ldots, \tau_{(m-1),(m-1)}$ and substitute them in SP. We then use a linear programming solver such as Gurobi [27]

Algorithm 1 Algorithm to estimate Lipschitz Constants adapted from [28]

procedure LIPSCHITZ ESTIMATION(g_i, $\mathcal{N}$, M, α)
Input: function g_i, number of samples $\mathcal{N}$
number of rounds M, measure of closeness α
Initialize SL to an empty set
for $j \leftarrow 1$ to M **do**
set max to 0
for $i \leftarrow 1$ to $\mathcal{N}$ **do**
Sample points $\hat{\tilde{x}}_{i,1}$ and $\hat{\tilde{x}}_{i,2}$
such that $||\hat{\tilde{x}}_{i,1} - \hat{\tilde{x}}_{i,2}|| \leq \alpha$
Set $sl_i \leftarrow \dfrac{||g_i(d^*, \hat{\tilde{x}}_{i,1}) - g_i(d^*, \hat{\tilde{x}}_{i,2})||}{||\hat{\tilde{x}}_{i,1} - \hat{\tilde{x}}_{i,2}||}$
if $sl_i > max$ **then**
Set max to sl_i
end if
end for
$SL \leftarrow SL \cup \{max\}$
end for
Consider $SL = \{sl'_1, \ldots, sl'_M\}$.
Fit the points of SL to a reverse Weibull Distribution [28] with three parameters: its shape, scale, and location.
Set $\mathcal{L}_i$ to the location parameter of the above reverse Weibull Distribution.
Return $\mathcal{L}_i$
end procedure

to find the values of the other decision variables (η, γ, λ and b). Now, we fix the values of these variables, and solve SP to optimize over the values τ. We iterate between these until the difference in the optimal values is negligible, and consider the values of the decision variables at this point to be the sub-optimal values. Let this be denoted as $d^* = [\eta^*, \gamma^*, \lambda^*, \tau^*, b^*]$. If $\eta^* + \mathcal{L}'\zeta \leq 0$, then the values of b^* correspond to the coefficients of an augmented barrier certificate, and we have $\mathcal{B}(\tilde{x}) = \sum_{j=1}^{m} b_j^* p_j(\tilde{x})$.

To determine the Lipschitz-constants of the functions $g_j(d^*, x)$, we make use of the technique proposed in [28] as illustrated in Algorithm 1. We run the above algorithm for the functions $g_3, \ldots, g_{m+1}$ to get the values $\mathcal{L}_{g_3}, \ldots, \mathcal{L}_{g_{m+1}}$. We define the maximum of these as $\mathcal{L}' = \max\{\mathcal{L}_{g_3}, \ldots, \mathcal{L}_{g_{m+1}}\}$. We then determine if $\eta^* + \mathcal{L}'\zeta \leq 0$. If so, we conclude that the system is δ-approximate initial-state opaque, and otherwise our approach is inconclusive. We consider the estimation technique for the Lipschitz constants to be accurate and neglect the confidence involved in their calculations. Following [28, Proposition 1], our estimate for the constant approaches the true value of the Lipschitz constant as the values N, M tend to ∞, and the value α tends to 0.

IV. CASE STUDIES

As a case study, we consider the problem of demonstrating the opacity of a room temperature model. The dynamics of the system are described as follows and are adapted from [29].

$$\mathfrak{S}: \begin{cases} T(t+1) = T(t) + t_s\alpha_e(T_e - T(t)) \\ \qquad\qquad +\alpha_h(T_h - T(t)))u(t), \\ h(T) = \frac{T}{15}, \end{cases} \tag{12}$$

where $T(t)$ indicates the temperature at time t, $t_s = 5$ minutes indicates the sampling time, $T_e = -1$C is the ambient temperature, $T_h = 35$C is the heater temperature, $\alpha_e = 0.01$ and $\alpha_h = 0.02$ are the heat exchange coefficients, $U = \{0, 1\}$ are the two control inputs indicating whether the heater is off or on, and $u(t) \in U$ is the control input applied at time t. We consider the state space of the system $X = [-1, 35]$, with the initial states $X_0 = [21, 22]$, and the secret set of states $X_s = [21, 21.5)$, and construct the augmented system as in Definition 2.2, with $\tilde{X}_0 = \{(x_0, x'_0) \in (X_0 \cap X_S) \times (X_0 \setminus X_S) \mid ||h(x_0) - h(x')|| \leq \delta - 0.02\}$ and $\tilde{X}_u = \{(x_u, x'_u) \mid ||h(x) - h(x')|| \geq \delta\}$, and $\delta = 2$. We then draw cover the augmented state-space $\tilde{X}$ by with the size of their edges $\zeta = 0.0025$. We select the centers of these hyperrectangles as the sample points for SP and then simulate the system for one unit of time under all possible inputs. Note that we only use the closed-form expression for the function f to simulate the system for one unit of time from the sample points. We do not use equation (12) to find the barrier certificate.

We assume the barrier certificate to be of degree three and of the form $\mathcal{B}((x, x')) = b_1 + b_2x + b_3x' + b_4x^2 + b_5x'^2 + b_6x \cdot x' + b_7x^3 + b_8x'^3 + b_9x^2x' + b_{10}xx'^2$. We construct SP, set the initial guess of the values of $\tau_{0,0} = 0$, $\tau_{0,1} = 0.01$, and then solve the linear program using Gurobi. Now, we fix the values of all the decision variables except η and τ, and solve a linear program to determine their values. We repeat the above $V - K$ iteration until the difference in optimal values is less than 10^{-4}. The overall time taken is around 4.5 hours on a machine running MacOS 11.2 (Intel i9-9980HK with 64 GB of RAM). We then find the values of $\eta^* = -0.0204$, $\gamma^* = 9.979$, $\lambda = 10$, and the coefficients of the barrier to be

$$\begin{aligned} b^* = &[-10; -0.0072; 3.6408; 0.0026; -0.2445; \\ &-0.0137; 0.0009; 0.0105; -0.0083; 0.0028]. \end{aligned}$$

We estimate the maximum Lipschitz-constant to be 5.2, and find the value of $\eta^* + \mathcal{L}'\zeta = -0.0074$. As this is less than 0, we conclude that the above system is opaque from Theorem 1.

V. CONCLUSION

We presented a data-driven approach for approximate opacity verification of discrete-time dynamical systems. Our approach relied on relating the optimal solutions of a robust program with that of a scenario program to find an appropriate augmented barrier certificate to guarantee opacity. We demonstrated its use on a room-temperature model and

verified the system to be opaque. As future work, we plan on investigating data-driven approaches for opacity verification when the set of controls are uncountable. We also plan on investigating approaches to reduce the conservatism of current approaches for opacity verification.

REFERENCES

[1] M. Mazo Jr, A. Davitian, and P. Tabuada, "Pessoa: A tool for embedded controller synthesis," in *Computer Aided Verification: 22nd International Conference, CAV 2010, Edinburgh, UK, July 15-19, 2010. Proceedings*. Springer, 2010, pp. 566–569.

[2] T. Wongpiromsarn, U. Topcu, and A. Lamperski, "Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems," *IEEE Transactions on Automatic Control*, 2015.

[3] M. Rungger and M. Zamani, "Scots: A tool for the synthesis of symbolic controllers," in *Proceedings of the 19th international conference on hybrid systems: Computation and control*, 2016, pp. 99–104.

[4] P. Jagtap, S. Soudjani, and M. Zamani, "Temporal logic verification of stochastic systems using barrier certificates," in *ATVA*, 2018, pp. 177–193.

[5] M. Khaled and M. Zamani, "Omegathreads: symbolic controller design for ω-regular objectives," in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, 2021, pp. 1–7.

[6] M. R. Clarkson and F. B. Schneider, "Hyperproperties," *Journal of Computer Security*, vol. 18, no. 6, pp. 1157–1210, 2010.

[7] J. W. Bryans, M. Koutny, L. Mazaré, and P. Y. A. Ryan, "Opacity generalised to transition systems," in *Formal Aspects in Security and Trust*, 2006.

[8] R. Alur, P. Černỳ, and S. Zdancewic, "Preserving secrecy under refinement," in *Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33*. Springer, 2006, pp. 107–118.

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

[10] B. Finkbeiner, "Model checking algorithms for hyperproperties," in *International Conference on Verification, Model Checking, and Abstract Interpretation*. Springer, 2021, pp. 3–16.

[11] 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.

[12] K. Zhang, X. Yin, and M. Zamani, "Opacity of nondeterministic transition systems: A (bi) simulation relation approach," *IEEE Transactions on Automatic Control*, vol. 64, no. 12, pp. 5116–5123, 2019.

[13] E. Asarin, O. Maler, and A. Pnueli, "Reachability analysis of dynamical systems having piecewise-constant derivatives," *Theoretical computer science*, vol. 138, no. 1, pp. 35–65, 1995.

[14] 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.

[15] S. Liu and M. Zamani, "Verification of approximate opacity via barrier certificates," *IEEE Control Systems Letters*, vol. 5, no. 4, pp. 1369–1374, 2020.

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

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

[18] B. Zhong, S. Liu, M. Caccamo, and M. Zamani, "Secure-by-construction synthesis for control systems," *arXiv preprint arXiv:2307.02564*, 2023.

[19] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates," *IFAC-PapersOnLine*, pp. 7–12, 2021.

[20] A. Salamati and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach," *The 4th Annual Learning for Dynamics and Control Conference*, 2022.

[21] R. Tempo, G. Calafiore, and F. Dabbene, *Randomized algorithms for analysis and control of uncertain systems*. Springer, 2013.

[22] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE TAC*, pp. 742–753, 2006.

[23] P. M. Esfahani, T. Sutter, and J. Lygeros, "Performance bounds for the scenario approach and an extension to a class of non-convex programs," *IEEE Transactions on Automatic Control*, pp. 46–58, 2014.

[24] V. Murali, A. Trivedi, and M. Zamani, "A scenario approach for synthesizing k-inductive barrier certificates," *IEEE Control Systems Letters*, vol. 6, pp. 3247–3252, 2022.

[25] S. V. Gusev and A. L. Likhtarnikov, "Kalman-popov-yakubovich lemma and the s-procedure: A historical essay," *Automation and Remote Control*, 2006.

[26] A. Hassibi, S. Boyd, and J. How, "Control of asynchronous dynamical systems with rate constraints on events," in *38th IEEE Conference on Decision and Control*, 1999, pp. 1345–1351.

[27] Gurobi Optimization, LLC, "Gurobi Optimizer Reference Manual," 2021. [Online]. Available: https://www.gurobi.com

[28] G. Wood and B. Zhang, "Estimation of the lipschitz constant of a function," *Journal of Global Optimization*, pp. 91–103, 1996.

[29] P. Jagtap, S. Soudjani, and M. Zamani, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Transactions on Automatic Control*, vol. 66, no. 7, pp. 3097–3110, 2020.