Modular verification of opacity for interconnected control systems via barrier certificates

Shadi Tasdighi Kalat, Siyuan Liu, and Majid Zamani

***Abstract*—In this paper, we consider the problem of verifying *initial-state opacity* for networks of discrete-time control systems. We formulate the opacity property as a safety one over an appropriately constructed *augmented system*, and aim to verify this latter property by finding suitable barrier certificates. To reduce the computational complexity associated with computing barrier certificates for large networks, we propose a compositional approach to construct such barrier certificates for large-scale interconnected systems. This is achieved by introducing *local barrier certificates* for subsystems in the network and imposing some small-gain type conditions on the gains of those local barrier certificates. We also provide sufficient conditions for verifying the lack of opacity in large-scale networks by constructing barrier certificates ensuring some reachability properties over the augmented systems. To illustrate the effectiveness of our results, we consider the problem of tracking a target using a team of vehicles and verify if its initial position is secret from possible outside intruders.**

***Index Terms*—Discrete event systems, Large-scale systems, Network analysis and control**

I. Introduction

In the last two decades, there has been a significant interest in formal verification and synthesis against safety properties for cyber-physical systems (CPSs) which are resulting from intricate interaction of digital devices with the physical plants. However, security and privacy properties, including *opacity*, have not been investigated thoroughly for CPSs till very recently. Roughly speaking, opacity is a confidentiality property that characterizes whether or not some "secret" information about the system can be inferred by outside observers with potentially malicious intentions (e.g., intruders). Many of the CPS applications are security-critical with some vulnerability to (cyber) attacks and opacity can provide some formal guarantee for the plausible deniability of the system's "secret" in the presence of malicious observer. We refer the interested readers to the seminal work in [1] explaining different notions of opacity in detail.

Related work. Opacity was initially introduced in [2] to analyze cryptographic protocols. The results in [3], [4], [5], [6], [7], [8], [9], among many others, consider the formulation and verification of different notions of opacity in the context of *finite state automata*, including: (i) state-based opacity, where the secret is a set of states; and (ii) language-based opacity, where the secret is a subset of the set of system behaviors. The study of opacity was later extended to other classes of systems with potentially infinite sets of states, including real-time automata [10], Petri nets [11], pushdown systems [12], probabilistic automata [13], and partially-observable Markov decision processes (POMDPs) [14]. More recently, there have been some attempts on verifying opacity properties for continuous-space systems including the results in [15] which formulate opacity as an output reachability property. However, it is limited to discrete-time linear systems. The results in [16] use barrier certificate to verify *approximate* initial-state opacity for discrete time control systems. The idea of approximate opacity was first introduced in [17], which accommodates for the intruders' measurement precision, defined as a parameter δ. This concept is also studied in the domain of continuous-space stochastic control systems using opacity-preserving simulation functions and by constructing their finite abstractions (i.e. finite Markov decision processes) in [18].

Our contribution. This paper focuses on the verification of *approximate* initial-state opacity for networks of discrete-time control systems. Unlike the methodologies proposed in [17], [18] which are based on abstraction-based techniques, we propose a discretization-free approach for formal verification of approximate initial-state opacity based on barrier certificates. We tackle the opacity verification by formulating it as a safety verification over an augmented system, and verify it by finding suitable barrier certificates. To this end, we define an *augmented system* by taking the product of an interconnected system with itself. Then, we construct barrier certificates for this augmented system *compositionally* by leveraging so-called local barrier certificates of augmented versions of subsystems. The barrier certificate for the interconnected system is then constructed by composing those easier-to-compute local barrier certificates under some small-gain type conditions [19], [20]. We show that the existence of such barrier certificates is sufficient to ensure approximate initial-state opacity of the interconnected 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 an interconnected system by defining a reachability-type property over its augmented version. Finding a barrier certificate verifying this reachability property for the augmented system will prove the lack of opacity for the original interconnected system. Here, we also propose a similar compositional framework for computing those barrier certificates based on those of subsystems. Although the results in [16] also use barrier certificates to verify opacity, they treat large-scale interconnected systems monolithically. Consequently, they suffer severely from the computational complexity in searching for those barrier certificates while

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.

confronted with large-scale interconnected systems.

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 $\emptyset$. Given functions $f : X \to Y$ and $g : A \to B$, we define $f \times g : X \times A \to Y \times B$. We define $\mathcal{K} = \{\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, such that α is continuous, strictly increasing, and, $\alpha(0) = 0\}$, and $\mathcal{K}_\infty = \{\alpha \in \mathcal{K}$, such that $\lim_{r\to\infty} \alpha(r) = \infty\}$. We use id $\in \mathcal{K}_\infty$ to denote the identity function. Let us first introduce the class of discrete-time control subsystems studied in this paper.

Definition 1. ***(Control subsystem)*** *A discrete-time control subsystem S_i is defined as a tuple*

$$S_i = (X_i, X_{0i}, X_{si}, U_i, W_i, f_i, Y_i, h_i),\ i \in [1; N],$$

where X_i, $X_{0i} \subseteq X_i$, U_i, W_i, and Y_i are the sets of state, initial state, external input, internal input, and output, respectively. Set $X_{si} \subseteq X_i$ denotes the set of secret states. f_i and h_i are the transition and output functions, respectively. A discrete-time control system S_i is described by the following difference equations:

$$S_i : \begin{cases} \mathbf{x}_i(t+1) = f_i(\mathbf{x}_i(t), \mathbf{u}_i(t), \mathbf{w}_i(t)), \\ \mathbf{y}_i(t) = h_i(\mathbf{x}_i(t)), \end{cases}$$

where $\mathbf{x}_i : \mathbb{N} \to X_i$, $\mathbf{y}_i : \mathbb{N} \to Y_i$, $\mathbf{u}_i : \mathbb{N} \to U_i$, and $\mathbf{w}_i : \mathbb{N} \to W_i$ denote the the state, output, external input and internal input signals, respectively.

Consider $N \geq 1$ subsystems S_i as in Definition 1, $i \in [1; N]$, with their internal inputs and outputs partitioned as

$$w_i = [w_{i1}; \dots; w_{i(i-1)}; w_{i(i+1)}; \dots; w_{iN}], \tag{1}$$

$$h_i(x_i) = [h_{i1}(x_i); \dots; h_{iN}(x_i)], \tag{2}$$

with $W_i = \prod_{j=1, j\neq i}^{N} W_{ij}$ and $Y_i = \prod_{j=1}^{N} Y_{ij}$, $w_{ij} \in W_{ij}$, $y_{ij} = h_{ij}(x_i) \in Y_{ij}$. The outputs y_{ii} are considered *external*, and y_{ij} with $i \neq j$ are *internal*. We assume $w_{ij} = y_{ji}$, if there is a connection from system S_j to S_i, otherwise, we set $h_{ji} \equiv 0$. Next, we define a discrete-time control system that is formed by the interconnection of subsystems.

Definition 2. ***(Interconnected control system)*** *An interconnected control system $S = \mathcal{I}(S_1, \dots, S_N)$, $N \in \mathbb{N}_{\geq 1}$, is a tuple*

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

where $X = \prod_{i=1}^{N} X_i$, $U = \prod_{i=1}^{N} U_i$, $Y = \prod_{i=1}^{N} Y_i$, and sets X_0 and X_s denote sets of initial and secret states, respectively. The input-output structure of S_i, $i \in [1; N]$, is given as in (1)-(2), subject to $w_{ij} = y_{ji}$, $Y_{ji} \subseteq W_{ij}, \forall i, j \in [1; N], i \neq j$. 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 $x = [x_1; \dots; x_N] \in X$, $u = [u_1; \dots; u_N] \in U$, and $f(x, u) = [f_1(x_1, u_1, w_1); \dots; f_N(x_N, u_N, w_N)]$.

We use $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \dots, x_n\}$ to denote a finite state sequence under the input sequence $\mathbf{u}$. Our focus is to verify whether the system defined in Definition 2 is able to conceal its secret from the outside intruder. This property is described in [18] as the following.

Definition 3. ***(Approximate initial-state opacity)*** *Given $\delta \in \mathbb{R}_{\geq 0}$, an interconnected system S in Definition 2 is δ-approximate initial-state opaque if for any $x_0 \in X_0 \cap X_s$ and any finite state sequence $\mathbf{x}_{x_0,\mathbf{u}} = \{x_0, \dots, x_T\}$, there exists $\hat{x}_0 \in X_0 \setminus X_s$ and a finite state sequence $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}} = \{\hat{x}_0, \dots, \hat{x}_T\}$ such that*

$$\max_{t\in[0;T]} ||h(x_t) - h(\hat{x}_t)|| \leq \delta.$$

Without loss of generality, we assume $\forall x_0 \in X_0 \cap X_s$, $\{x \in X_0 |\ ||h(x) - h(x_0)|| \leq \delta\} \not\subset X_s$, which indicates that the system does not start from an initial state which violates the approximate initial-state opacity.

III. Verifying approximate Initial-state opacity for interconnected systems

In this section, we present an approach for the verification of approximate initial-state opacity for an interconnected system S. This is achieved by computing barrier certificates defined over a so-called augmented system as described below.

Definition 4. ***(Augmented system)*** *Consider an interconnected control system S as in Definition 2. 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 $(x_0, \hat{x}_0)$ and under input sequence $(\mathbf{u}, \hat{\mathbf{u}})$. Additionally, we denote the augmented state set by $\mathcal{X} = X \times X$. Similarly, the augmented system associated with a subsystem S_i is defined as $S_i \times S_i = (X_i \times X_i, X_{0i} \times X_{0i}, X_{si} \times X_{si}, U_i \times U_i, W_i \times W_i, f_i \times f_i, Y_i \times Y_i, h_i \times h_i)$. Next, we introduce barrier certificates for the augmented systems defined in Definition 4.

Definition 5. ***(Barrier certificate for augmented systems)*** *Consider an augmented system $S \times S$ as in Definition 4, 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*

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

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

$$\forall (x, \hat{x}) \in \mathcal{X}, \forall u \in U, \exists \hat{u} \in U,$$

$$B(f(x, u), f(\hat{x}, \hat{u})) - B(x, \hat{x}) \leq 0,$$

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

In order to leverage the proposed barrier certificate to verify approximate initial-state opacity for an interconnected system S, we define the sets of initial conditions $\mathcal{X}_0$ and unsafe states $\mathcal{X}_u$ as:

$$\mathcal{X}_0 = \{(x,\hat{x}) \in (X_0 \cap X_s) \times (X_0 \backslash X_s) \mid \|h(x) - h(\hat{x})\| \leq \delta\}, \quad (3)$$

$$\mathcal{X}_u = \{(x,\hat{x}) \in X \times X \mid \|h(x) - h(\hat{x})\| > \delta\}, \quad (4)$$

where $\delta \in \mathbb{R}_{\geq 0}$ captures the measurement precision of the outside intruder as introduced in Definition 3. Notice that the regions of interest are defined in specific forms which incorporate the secret and initial information of the original interconnected system S. Now, we are ready to introduce the next proposition, which states the usefulness of the above-defined barrier certificate for verifying opacity of an interconnected system.

Proposition 1. *Consider an interconnected control system S and the associated augmented system $S \times S$. Suppose that there exists a function $B : X \times X \to \mathbb{R}_{\geq 0}$ satisfying the conditions in Definition 5 with sets $\mathcal{X}_0$ and $\mathcal{X}_u$ given in* (3) *and* (4)*. Then, system S is δ-approximate initial-state opaque.*

Proof. Consider a secret initial state x_0, an input sequence $\mathbf{u}$, and the corresponding state sequence $\mathbf{x}_{x_0,\mathbf{u}}$ in S. Since $\{x \in X_0 \mid ||h(x) - h(x_0)|| \leq \delta\} \not\subseteq X_s$, there exists an initial state $\hat{x}_0 \in X_0 \backslash X_s$ such that $||h(\hat{x}_0) - h(x_0)|| \leq \delta$. Now, notice that the existence of a barrier certificate B as in Definition 5 guarantees that for any $(x_0, \hat{x}_0) \in \mathcal{X}_0$, there exists a control sequence $\hat{\mathbf{u}}$ such that any state sequence of $S \times S$ starting from $\mathcal{X}_0$ never reaches the unsafe region $\mathcal{X}_u$. This implies the satisfaction of $||h(\mathbf{x}_{x_0,\mathbf{u}}(t)) - h(\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(t))|| \leq \delta, \forall t \in \mathbb{N}$. Since x_0 and $\mathbf{x}_{x_0,\mathbf{u}}$ are arbitrarily chosen, we conclude that S is δ-approximate initial-state opaque. □

A. Compositional construction of barrier certificates

In this subsection, we provide a compositional approach for the construction of barrier certificates to alleviate the computational cost encountered while dealing with large-scale interconnected systems. We show that by employing a small-gain type condition, a barrier certificate B for $S \times S$ as in Definition 5 can be constructed by composing so-called local barrier certificates of subsystems as defined next.

Definition 6. ***(Local barrier certificate for verifying opacity)*** *Consider a control subsystem S_i. A function $\hat{B}_i : X_i \times X_i \to \mathbb{R}_{\geq 0}$ is called a local barrier certificate for the augmented subsystem $S_i \times S_i$ if it satisfies the following conditions*

$$\forall (x_i, \hat{x}_i) \in \mathcal{X}_i, \quad \hat{B}_i(x_i, \hat{x}_i) \geq \alpha_i(||h_i(x_i, \hat{x}_i)||^2), \quad (6)$$

$$\forall (x_i, \hat{x}_i) \in \mathcal{X}_{0i}, \quad \hat{B}_i(x_i, \hat{x}_i) \leq \overline{\epsilon}_i, \quad (7)$$

$$\forall (x_i, \hat{x}_i) \in \mathcal{X}_{ui}, \quad \hat{B}_i(x_i, \hat{x}_i) > \underline{\epsilon}_i, \quad (8)$$

$$\forall (x_i, \hat{x}_i) \in \mathcal{X}_i, \forall u_i \in U_i, \exists \hat{u}_i \in U_i,$$
$$\hat{B}_i(f_i(x_i, w_i, u_i)) \leq \kappa_i(\hat{B}_i(x_i, \hat{x}_i)) + \gamma_{wi}(||w_i||^2), \quad (9)$$

where sets $\mathcal{X}_{0i}$ and $\mathcal{X}_{ui}$ are the projections of sets $\mathcal{X}_0$ and $\mathcal{X}_u$ on the augmented subsystem $S_i \times S_i$, and α_i, γ_{wi}, $\kappa_i \in \mathcal{K}_\infty$, $\kappa_i \leq \mathrm{id}$, $\overline{\epsilon}_i, \underline{\epsilon}_i \in \mathbb{R}_{\geq 0}$.

Note that local barrier certificates of subsystems are mainly defined for constructing an overall barrier certificate for the interconnected system, and they are not useful on their own to verify opacity property. We now introduce the following lemma which will be used later in proving our main result.

Lemma 1. *For $a, b \in \mathbb{R}_{\geq 0}$, $\forall \lambda \in \mathcal{K}_\infty$, we have*

$$a + b \leq \max\{(\mathrm{id} + \lambda)(a), (\mathrm{id} + \lambda^{-1})(b)\}. \quad (10)$$

Proof. Define $c := \lambda^{-1}(b)$, we get the following

$$a + b = \begin{cases} a + \lambda(c) \leq c + \lambda(c) = (\mathrm{id} + \lambda^{-1})(b) & \text{if } a \leq c, \\ a + \lambda(c) < a + \lambda(a) = (\mathrm{id} + \lambda)(a) & \text{if } a > c, \end{cases}$$

which implies (10). □

For functions α_i, γ_{wi}, and κ_i associated with $\hat{B}_i$ as in Definition 6, we define, $\forall i, j \in [1; N]$,

$$\gamma_{ij} = \begin{cases} (\mathrm{id} + \lambda) \circ \kappa_i & \text{if } i = j, \\ (\mathrm{id} + \lambda^{-1}) \circ \gamma_{wi} \circ \alpha_j^{-1} & \text{if } i \neq j, \end{cases} \quad (11)$$

for some arbitrarily chosen $\lambda \in \mathcal{K}_\infty$.

Before stating our main compositionality result, we pose the following small-gain type assumption on the composition of gains γ_{ij}.

Assumption 1. *Assume functions γ_{ij} defined in* (11) *satisfy the following inequality*

$$\gamma_{i_1 i_2} \circ \gamma_{i_2 i_3} \circ \cdots \circ \gamma_{i_r i_1} < \mathrm{id}, \quad (12)$$

$\forall (i_1, \ldots, i_r) \in \{1, \ldots, N\}^r$, where $r \in \{1, \ldots, N\}$.

Note that by leveraging Theorem 5.2 in [19], the small gain condition in (12) *implies that there exists $\phi_i \in \mathcal{K}_\infty$, $\forall i \in [1; N]$, satisfying*

$$\max_{j \in [1;N]} \{\phi_i^{-1} \circ \gamma_{ij} \circ \phi_j\} < \mathrm{id}. \quad (13)$$

The following results show that a barrier certificate B for the augmented interconnected system $S \times S$ can be obtained by composing local barrier certificates $\hat{B}_i$ computed for subsystems.

Theorem 1. *Consider an interconnected system $S = \mathcal{I}(S_1, \ldots, S_N)$, and the associated augmented system $S \times S$ composed of augmented subsystems $S_i \times S_i$. Assume each $S_i \times S_i$ admits a local barrier certificate $\hat{B}_i$ as in Definition 6. Let Assumption 1 hold, and $\max_{i \in [1;N]}\{\phi_i^{-1}(\overline{\epsilon}_i)\} \leq \max_{i \in [1;N]}\{\phi_i^{-1}(\underline{\epsilon}_i)\}$. Then, function $B : X \times X \to \mathbb{R}_{\geq 0}$ defined as*

$$B(x, \hat{x}) = \max_{i \in [1;N]} \{\phi_i^{-1} \circ \hat{B}_i(x_i, \hat{x}_i)\}, \quad (14)$$

is a barrier certificate for $S \times S$ as in Definition 5.

Proof. First, by Definition 6, we have

$$B(x, \hat{x}) = \max_{i \in [1;N]} \{\phi_i^{-1} \circ B_i(x_i, \hat{x}_i)\} \overset{(7)}{\leq} \max_{i \in [1;N]} \{\phi_i^{-1}(\overline{\epsilon}_i)\},$$

$$B(x, \hat{x}) = \max_{i \in [1;N]} \{\phi_i^{-1} \circ B_i(x_i, \hat{x}_i)\} \overset{(8)}{>} \max_{i \in [1;N]} \{\phi_i^{-1}(\underline{\epsilon}_i)\},$$

which satisfies the first two conditions in Definition 5 by taking $\overline{\epsilon} = \max_{i \in [1;N]}\{\phi_i^{-1}(\overline{\epsilon}_i)\}$ and $\underline{\epsilon} = \max_{i \in [1;N]}\{\phi_i^{-1}(\underline{\epsilon}_i)\}$.

$$\begin{aligned}
&B(f(x,u), f(\hat{x},\hat{u})) = \max_i\{\phi_i^{-1} \circ \hat{B}_i(f_i(x_i,u_i,w_i), f_i(\hat{x}_i,\hat{u}_i,w_i))\} \overset{(9)}{\leq} \max_i \Big\{\phi_i^{-1}\big(\kappa_i(\hat{B}_i(x_i,\hat{x}_i)) + \gamma_{wi}(||w_i||^2)\big)\Big\}\\
&\overset{(10)}{\leq} \max_i \Big\{\phi_i^{-1}\big(\max\{(\mathrm{id}+\lambda)(\kappa_i(\hat{B}_i(x_i,\hat{x}_i))), (\mathrm{id}+\lambda^{-1})(\gamma_{wi}(||w_i||^2))\}\big)\Big\}\\
&= \max_i \Big\{\phi_i^{-1}\big(\max\{(\mathrm{id}+\lambda)(\kappa_i(\hat{B}_i(x_i,\hat{x}_i))), (\mathrm{id}+\lambda^{-1})(\gamma_{wi}(\max_{j,j\neq i}\{||w_{ij}||^2\}))\}\big)\Big\}\\
&= \max_i \Big\{\phi_i^{-1}\big(\max\{(\mathrm{id}+\lambda)(\kappa_i(\hat{B}_i(x_i,\hat{x}_i))), (\mathrm{id}+\lambda^{-1})(\gamma_{wi}(\max_{j,j\neq i}\{||y_{ij}||^2\}))\}\big)\Big\}\\
&= \max_i \Big\{\phi_i^{-1}\big(\max\{(\mathrm{id}+\lambda)(\kappa_i(\hat{B}_i(x_i,\hat{x}_i))), (\mathrm{id}+\lambda^{-1})(\gamma_{wi}(\max_{j,j\neq i}\{||h_{ji}(x_j,\hat{x}_j)||^2\}))\}\big)\Big\}\\
&\leq \max_i \Big\{\phi_i^{-1}\big(\max\{(\mathrm{id}+\lambda)(\kappa_i(\hat{B}_i(x_i,\hat{x}_i))), (\mathrm{id}+\lambda^{-1})(\gamma_{wi}(\max_{j,j\neq i}\{||h_j(x_j,\hat{x}_j)||^2\}))\}\big)\Big\}\\
&\overset{(6)}{\leq} \max_i \Big\{\phi_i^{-1}\big(\max\{(\mathrm{id}+\lambda)(\kappa_i(\hat{B}_i(x_i,\hat{x}_i))), (\mathrm{id}+\lambda^{-1})(\gamma_{wi}(\max_{j,j\neq i}\{\alpha_j^{-1} \circ \hat{B}_j(x_j,\hat{x}_j)\}))\}\big)\Big\} \overset{(11)}{\leq} \max_{i,j}\Big\{\phi_i^{-1} \circ \gamma_{ij} \circ \hat{B}_j(x_j,\hat{x}_j)\Big\}\\
&\leq \max_{i,j,k}\Big\{\phi_i^{-1} \circ \gamma_{ij} \circ \phi_j \circ \phi_k^{-1} \circ B_k(x_k,\hat{x}_k)\Big\} \overset{(14)}{\leq} \max_{i,j}\Big\{\phi_i^{-1} \circ \gamma_{ij} \circ \phi_j \circ B(x,\hat{x})\Big\} \overset{(13)}{\leq} B(x,\hat{x}). \qquad (5)
\end{aligned}$$

Next, by condition (9) of Definition 6, for all $(x,\hat{x}) \in \mathcal{X}$ and $u \in U$, there exists $\hat{u} \in U$ such that the chain of inequalities in (5) holds. Recall that we set $w_{ij} = y_{ji} = h_{ji}(x_j,\hat{x}_j)$ in Definitions 1 and 2. This gives us the identities in lines 4 and 5. The inequality in (5) satisfies the last condition in Definition 5. Therefore function B defined in (14) is a barrier certificate for the augmented interconnected system $S \times S$. □

IV. Verifying Lack of Approximate Initial-State Opacity for Interconnected Systems

In the previous section, we presented sufficient conditions for verifying approximate initial-state opacity of the interconnected system by constructing a barrier certificate for it. However, failing to find the local barrier certificate, and consequently, not being able to compute a barrier certificate for the interconnected system does not imply the lack of opacity. This section studies the lack of opacity for interconnected systems by considering reachability as the dual of safety (i.e. having opacity). Therefore, the existence of a feasible solution to this dual problem guarantees the lack of opacity for the interconnected system.

The following proposition provides a sufficient condition for a reachability property of the augmented interconnected system $S \times S$.

Proposition 2. *Consider an interconnected control system S and the associated augmented system $S \times S$. Suppose the state set X of S is bounded, and there exists a continuous function $V : X \times X \to \mathbb{R}$ which satisfies*

$$\forall (x,\hat{x}) \in \mathcal{X}_0, \quad V(x,\hat{x}) \leq 0, \qquad (15)$$

$$\forall (x,\hat{x}) \in \partial\mathcal{X} \setminus \partial\mathcal{X}_u, \quad V(x,\hat{x}) > 0, \qquad (16)$$

$$\begin{aligned}&\forall (x,\hat{x}) \in \overline{\mathcal{X} \setminus \mathcal{X}_u}, \exists u \in U, \text{ s.t. } \forall \hat{u} \in U,\\ &\quad V(f(x,u), f(\hat{x},\hat{u})) - V(x,\hat{x}) \leq 0, \qquad (17)\end{aligned}$$

for some $\mathcal{X}_0, \mathcal{X}_u \subseteq \mathcal{X}$. Then, for any initial condition $(x_0,\hat{x}_0) \in \mathcal{X}_0$, there exists an input sequence $\mathbf{u}$ such that $(\mathbf{x}_{x_0,\mathbf{u}}(T), \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(T)) \in \mathcal{X}_u$ for any input sequence $\hat{\mathbf{u}}$ and some $T \geq 0$, and additionally $(\mathbf{x}_{x_0,\mathbf{u}}(t), \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(t)) \in \mathcal{X}$, $\forall t \in [0,T]$.

Proof. Consider an initial state $(x_0,\hat{x}_0) \in \mathcal{X}_0$, with $V(x_0,\hat{x}_0) \leq 0$. Consider an input sequence $\mathbf{u}$. The continuous function $V(x,\hat{x})$ is bounded below on the compact set $\overline{\mathcal{X} \setminus \mathcal{X}_u}$, and is strictly decreasing along the sequence $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ on this set. Therefore, sequence $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ must leave $\overline{\mathcal{X} \setminus \mathcal{X}_u}$ in finite time. If $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ leaves $\overline{\mathcal{X} \setminus \mathcal{X}_u}$ and does not enter $\mathcal{X}_u$, we get $(\mathbf{x}_{x_0,\mathbf{u}}(T+\epsilon), \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(T+\epsilon)) \notin \mathcal{X}$, $\forall \epsilon > 0$. This results in $V(\mathbf{x}_{x_0,\mathbf{u}}(T), \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(T)) \leq 0$, which is a contradiction. □

The next result proves the lack of initial-state opacity for interconnected systems.

Proposition 3. *Consider an interconnected control system S and the associated augmented system $S \times S$. Suppose there exists a continuous function $V : X \times X \to \mathbb{R}$ satisfying the conditions in Proposition 2 with sets $\mathcal{X}_0$, $\mathcal{X}_u$ as in (3) and (4). Then, the system S is not δ-approximate initial-state opaque.*

Proof. Consider the function $V : X \times X \to \mathbb{R}$ and an input sequence $\mathbf{u}$ satisfying (17). By Proposition 2 and the structure of sets $\mathcal{X}_0$ and $\mathcal{X}_u$ as in (3) and (4), there must exist a secret state $x_0 \in X_0 \cap X_s$ such that for any state sequence $\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}$ starting from a non-secret initial condition $\hat{x}_0 \in X_0 \setminus X_s$, the state sequences $(\mathbf{x}_{x_0,\mathbf{u}}, \mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}})$ will eventually reach $\mathcal{X}_u$ in finite time t, i.e. $||h(\mathbf{x}_{x_0,\mathbf{u}}(t) - h(\mathbf{x}_{\hat{x}_0,\hat{\mathbf{u}}}(t))|| > \delta$. Therefore, given the state sequence $\mathbf{x}_{x_0,\mathbf{u}}$, there is no other state sequence starting from a non-secret initial state while having δ-close observation. This implies that the interconnected system is not δ-approximate initial-state opaque. □

By applying the compositionality result proposed in Theorem 1, the described barrier certificate V for verifying the lack of opacity of an augmented system $S \times S$ can be computed by composing local barrier certificates $\hat{V}_i$ of subsystems as defined below.

Definition 7. ***(Local barrier certificates for verifying lack of opacity)*** *Consider a control subsystem S_i. A function $\hat{V}_i : X_i \times X_i \to \mathbb{R}_{\geq 0}$ is called a local barrier certificate for* *the augmented subsystem $S_i \times S_i$ if it satisfies the following conditions*

$$\forall (x_i, \hat{x}_i) \in \mathcal{X}_i, \quad \hat{V}_i(x_i, \hat{x}_i) \geq \alpha_i(||h_i(x_i, \hat{x}_i)||^2), \tag{18}$$

$$\forall (x_i, \hat{x}_i) \in \mathcal{X}_{0i}, \quad \hat{V}_i(x_i, \hat{x}_i) \leq 0, \tag{19}$$

$$\forall (x_i, \hat{x}_i) \in \partial\mathcal{X}_i \setminus \partial\mathcal{X}_{ui}, \quad \hat{V}_i(x_i, \hat{x}_i) > 0, \tag{20}$$

$$\begin{aligned} &\forall (x_i, \hat{x}_i) \in \overline{\mathcal{X}_i \setminus \mathcal{X}_{ui}}, \forall u_i \in U_i, \exists \hat{u}_i \in U_i, \\ &\quad \hat{V}_i(f_i(x_i, w_i, u_i)) \leq \kappa_i(\hat{V}_i(x_i, \hat{x}_i)) + \gamma_{wi}(||w_i||^2), \end{aligned} \tag{21}$$

where the sets $\mathcal{X}_i$, $\mathcal{X}_{0i}$, $\partial\mathcal{X}_i \setminus \partial\mathcal{X}_{ui}$ and $\overline{\mathcal{X}_i \setminus \mathcal{X}_{ui}}$ are, respectively, the projections of sets $\mathcal{X}$, $\mathcal{X}_0$, $\partial\mathcal{X} \setminus \partial\mathcal{X}_u$ and $\overline{\mathcal{X} \setminus \mathcal{X}_u}$ on the augmented subsystem $S_i \times S_i$, and α_i, γ_{wi}, $\kappa_i \in \mathcal{K}_\infty$, $\kappa_i \leq \mathrm{id}$, $\overline{\epsilon}_i, \underline{\epsilon}_i \in \mathbb{R}_{\geq 0}$.

Using the results of Theorem 1, one can construct a barrier certificate V for an augmented interconnected system $S \times S$, from the local barrier certificates V_i as in Definition 7.

V. Implementation

For systems with polynomial transition functions and semi-algebraic sets X_{0i}, X_{si}, and X_i, we can use sum-of-squares (SOS) programming to search for polynomial local barrier certificates. We follow the same strategy as in [16, Sec. IV], and use SOSTOOLS [21] together with a semidefinite programming solver SeDuMi [22] to compute local barrier certificates for subsystems in the following case study. Consider a team of vehicles that are assigned to track a moving target. For the sake of simplicity, we constrain the target to move in a line, with bounded arbitrary acceleration. We also assume the vehicles are connected to each other in a line topology, and the distance between the first vehicle and the target is negligible. An intruder with δ measurement precision is trying to gain information about the initial position of the target. It has full knowledge of the system dynamics, but can only observe the position of the last vehicle in the team. Our aim is to verify whether the system is able to conceal its secret (defined as the initial position of the target) from the intruder. Figure. 1 presents the experimental results of implementing our methodology for a team of $N = 100$ vehicles. The evolution of the states for the interconnected system is governed by

$$\begin{cases} \boldsymbol{\xi}_1(t+1) = A\boldsymbol{\xi}_1(t) + C\mathbf{u}(t) + \boldsymbol{\xi}_2(t) \\ \boldsymbol{\xi}_2(t+1) = \mathbf{u}(t) + \boldsymbol{\xi}_2(t) \end{cases} \tag{22}$$

where $\boldsymbol{\xi}_1(t) = [\xi_{11}, \ldots, \xi_{1N}]^T \in \mathbb{R}^N$ and $\boldsymbol{\xi}_2(t) = [\xi_{21}, \ldots, \xi_{2N}]^T \in \mathbb{R}^N$ are the position and velocity vectors, respectively, and $\mathbf{u}(t) \in \mathbb{R}^N$ contains the external input values of all the vehicles in the team. Taking $\mathbf{x}_i = [\xi_{1i}, \xi_{2i}]^T$, the following set of difference equations describe the dynamics of each subsystem S_i, $\forall i \in [1; N]$:

$$S_i : \begin{cases} \mathbf{x}_i(t+1) = \begin{bmatrix} 1-a & 1 \\ 0 & 1 \end{bmatrix} \mathbf{x}_i(t) + \mathbf{u}_i(t) \begin{bmatrix} 0.5 \\ 1 \end{bmatrix} + \mathbf{w}_i(t), \\ \mathbf{y}_i(t) = [0, \ldots, \mathbf{w}_{(i+1)i}(t), 0, \ldots, 0] \end{cases}$$

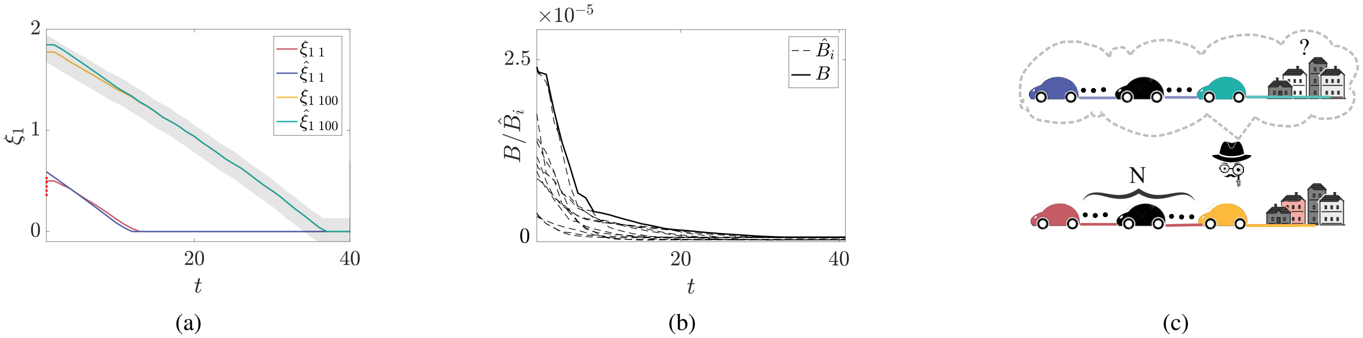
where $\mathbf{x}_0(t)$ is the state of the target at time t. In vector $\mathbf{w}_i(t)$, we have $\mathbf{w}_{i(i-1)}(t) = \mathbf{y}_{(i-1)i}(t) = \begin{bmatrix} a & 0 \end{bmatrix} \mathbf{x}_{i-1}(t)$, and all other entries are 0.

Matrix $A_{N\times N}$ in (22) represents the effects of internal input, as well as capturing the constant-acceleration motion of the vehicle i during the time interval $(t, t+1]$. Therefore, the entries A_{ij} are defined as $A_{ij} = \begin{cases} 1-a & \forall i = j, \\ a & \forall j = i-1, \end{cases}$ and zero else where. We set the constant $a = 0.01$ in this example. Matrix $C_{N\times N}$ is diagonal with $C_{i,i} = 0.5$, $\forall i \in [1; N]$. The output of the interconnected system is the position of the last vehicle, i.e., $\mathbf{y}(t) = [0, \ldots, 0, \xi_{1N}(t), 0]^T$, $N = 100$. The state set and initial set are $X = X_0 = \prod_{i=1}^{N} X_i$ where $X_i = X_{0i} = [0, 2]$. The secret set for the interconnected system is set to $X_s = \prod_{i=1}^{N} X_{si}$, where $X_{s1} = [0, 0.5]$, and X_{si} for all $i \in [2; 100]$ is a singleton containing a random number between $[0, 2]$. The measurement precision of the intruder is set to $\delta = 0.1$.

For finding local barrier certificates, we used $\overline{\epsilon}_i = 1, \underline{\epsilon}_i = 1.5$, for all $i \in [1; 100]$, $\alpha_j(r) = r$, $\kappa_i(r) = a\,r$, and $\gamma_{wi}(r) = a\,r$, $\forall r \in \mathbb{R}_{\geq 0}$. With the help of SOSTOOLS [21] and SeDuMi [22], we computed local barrier certificates together with their corresponding control policy $\hat{u}_i(\mathbf{x}_i, \hat{\mathbf{x}}_i, u_i) = \begin{bmatrix} 0.6 & -0.6 \end{bmatrix} \mathbf{x}_i + \begin{bmatrix} 1.2 & -1.2 \end{bmatrix} \hat{\mathbf{x}}_i + u_i$. One can readily verify that the small-gain assumption in (12) holds with $\gamma_{ij} < \mathrm{id}$, $\forall i, j \in [1; N]$. Then, by applying the results in Theorem 1, and taking $\phi_i = \mathrm{id}, \forall i \in [1; N]$, a barrier certificate for the interconnected system can be obtained as $B(x, \hat{x}) = \max_{i\in[1;N]}\{\hat{B}_i(x_i, \hat{x}_i)\}$. Figure 1b shows 10 of the computed local barrier certificates $\hat{B}_i$ for subsystems and the obtained overall barrier certificate B. The existence of the overall barrier certificate guarantees that for every state sequence of the interconnected system starting from a secret state, there exists at least another state sequence starting from a non-secret state such that the two sequences are indistinguishable in the eyes of the intruder with measurement precision δ. This is shown in Figure 1a, where position sequences of the first and last vehicles (i.e. $\xi_{1\,1}$ and $\xi_{1\,100}$), are plotted with their corresponding $\hat{\xi}_{1\,1}$ and $\hat{\xi}_{1\,100}$, starting from non-secret initial states. One can readily see that the interconnected system is able to conceal its secret from possible intruders.

VI. Conclusions and Future Directions

We studied the problem of verifying approximate initial-state opacity for discrete-time interconnected systems. We posed opacity as a safety property over an augmented system, and aimed to verify it by finding a barrier certificate. For large-scale interconnected systems, searching for these functions using optimization-based techniques is computationally expensive. Therefore, we proposed a compositional approach to construct these functions from so-called local barrier certificates defined over subsystems. The existence of local barrier certificates does not verify any property over the subsystems. However, our main result shows that by posing a small-gain type condition, we can construct a barrier certificate ensuring approximate initial-opacity of the interconnect system by composing the local ones. Failure to find such



(a) (b) (c)

Figure 1: Results of simulating a system of 100 vehicles tracking a target. Target (red), and last vehicle (yellow) trajectories are plotted together with their corresponding non-secret pairs (blue and green lines). The shaded grey area indicates the region where the distance from the observed trajectory (yellow) is less than $\delta = 0.1$. The red dashed line on the x axis indicates the secret set for the target. b) The local barrier certificates computed for augmented subsystems (dashed lines), and their $\max$ in time, which is a barrier certificate for the interconnected system. c) The vehicles are connected together in a line topology, where vehicle i receives the position of $i-1$ as internal input. The intruder measures the location of the yellow vehicle, and tries to uncover the initial location of the target (red vehicle).

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 interconnected system. For networks which do not satisfy the small gain condition (cf. Assumption 1), the methodology in [16] can be used to search for a barrier certificate for the entire network. Unfortunately, due to the computational complexity, one may not be able to find a barrier certificate using SOS programming within a reasonable computation time (e.g. in the target tracking scenario with 2 subsystems, the computation does not terminate within 24 hours). Our future plan is to extend our approach to verification of k-step, and infinite-step opacity for interconnected systems. Finally, formal synthesis of controllers to enforce opacity is another future direction which we are considering.

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] L. Mazaré, "Using unification for opacity properties," *Verimag Technical Report*, 2004.

[3] A. Saboori and C. N. Hadjicostis, "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] 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.

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

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

[7] 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.

[8] 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.

[9] 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.

[10] L. Wang, N. Zhan, and J. An, "The opacity of real-time automata," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 11, pp. 2845–2856, 2018.

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

[12] K. Kobayashi and K. Hiraishi, "Verification of opacity and diagnosability for pushdown systems," *Journal of Applied Mathematics*, vol. 2013, 2013.

[13] A. Saboori and C. Hadjicostis, "Current-state opacity formulations in probabilistic finite automata," *IEEE Transactions on Automatic Control*, vol. 59, no. 1, pp. 120–133, 2014.

[14] 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.

[15] 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.

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

[17] 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.

[18] 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.

[19] S. N. Dashkovskiy, B. S. Rüffer, and F. R. Wirth, "Small gain theorems for large scale systems and construction of ISS Lyapunov functions," *SIAM Journal on Control and Optimization*, vol. 48, no. 6, pp. 4089–4118, 2010.

[20] P. Jagtap, A. Swikir, and M. Zamani, "Compositional construction of control barrier functions for interconnected control systems," in *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, 2020, pp. 1–11.

[21] 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.

[22] 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.