Local Opacity Verification for Distributed Discrete Event Systems

Sasinee Pruekprasert[1] and Kai Cai[2]

***Abstract*— This paper studies the current-state opacity and the initial-state opacity verification of distributed discrete event systems. The distributed system's global system is the parallel composition of multiple local systems: each of which represents a sub-component. We propose sufficient conditions for the global system's opacity based only on the opacity of the local systems. We also present efficient approaches for the opacity verification problem that only rely on the intruder's observer automata of the local DESs.**

I. Introduction

Security is a crucial issue in many applications, especially for distributed systems with multiple components that communicate across a network. As a result, methodologies to protect data privacy from malicious intruders are needed. In this work, we consider the concept of system opacity: a property that indicates whether or not a given "secret" about the system is detectable by the intruder based on the observed system's behaviors. Opacity was proposed for analyzing security protocols in [1]. This concept is introduced to the discrete event systems (DES) community in [2] for petri-nets, and in [3] for transition systems, and has been a hot research topic in the DES community in recent year. Several notions of opacity have been proposed and studied in the literature [4], [5], [6], [7], [8].

This work studies the opacity verification of distributed discrete event systems, which are systems with modular structure as illustrated in Fig. 1. Opacity verification for modular systems is known to be decidable but computationally expensive: its complexity has shown to be in EXPSPACE-complete for general cases, and PSPACE-complete if all events shared by any local DESs are observable [9]. The common technique for modular systems opacity verification is to construct data structures that estimate the intruder's global DES information based on observed event sequences. These data structures can be large, especially for distributed DESs with several local components. Motivated by this problem, we study *local opacity verification*: to verify the global DES by estimating the intruder's information based only on local DESs. We propose sufficient conditions and their corresponding efficient approaches for the global DES's opacity without constructing an observer automaton of the global DES. We focus on current-state opacity (CSO) and initial-state opacity (ISO) verification. Our results for these two types of opacity will establish a foundation for studying other opacity notions in the future.

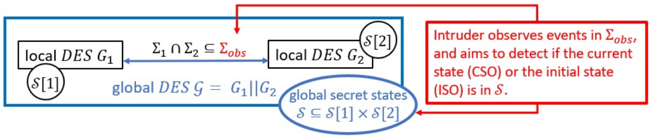
local DES G_1
$\mathcal{S}[1]$
$\Sigma_1 \cap \Sigma_2 \subseteq \Sigma_{obs}$
local DES G_2
$\mathcal{S}[2]$
global DES $\mathcal{G} = G_1||G_2$
global secret states
$\mathcal{S} \subseteq \mathcal{S}[1] \times \mathcal{S}[2]$
Intruder observes events in Σ_{obs}, and aims to detect if the current state (CSO) or the initial state (ISO) is in $\mathcal{S}$.

Fig. 1. An overview of our distributed architecture with two local DESs. The global DES $\mathcal{G}$ is the parallel composition of local DESs. The secret state set $\mathcal{S}$ is a set of states of $\mathcal{G}$. We assume that the events shared by the local DESs are observable by the intruder ($\Sigma_1 \cap \Sigma_2 \subseteq \Sigma_{obs}$). The objective of the intruder is to detect if the current state (for the CSO problem) or the initial state (for the ISO problem) of $\mathcal{G}$ is in $\mathcal{S}$ (see Section III). Note that this architecture can be extended to n local DESs.

Reduced complexity opacity verification techniques for modular DESs by considering its local components was proposed for ISO in [10], and for CSO in [11] and [12]. However, our setting is different from the previous works. The objective of [10] and [12] is to ensure that local secret states of all local DESs are protected confidentially. In both works, the secret of the whole system is revealed if a secret state of any local DES is revealed. Instead, in this work, we consider the secret of the global system defined as a subset of the global system's states, as depicted in Fig. 1. Our work is also different from [11], which considers each observation map for each local DES. Using these maps, the intruder observes the global DES through the event sequences of all local DESs. In our work, the intruder has only one observation map and observes the global DES's event sequences directly. These differences are significant, as one cannot straightforwardly generalize our setting to those in the previous works.

The rest of this paper is organized as follows. In Section II, we proposed a distributed architecture of a global DES with several local DESs as its components. In Section III, we present the notions of CSO and ISO, and introduce the concept of local opacity verification. Then, in Section IV, we present sufficient conditions for the opacity of the global DES based only on the local DESs. Using the sufficient conditions in Section IV, we propose approaches to verify the global DES using the intruder's observer automata for local DESs. Finally, Section VI presents the conclusion.

II. Distributed Discrete Event Systems

We study a distributed discrete event system (DES), which we call the global DES, consisting of n local DESs. Fig. 1 depicts an overview of the architecture with two local DESs.

This work was supported by ERATO HASUO Metamathematics for Systems Design Project No. JPMJER1603, JST

[1] Sasinee Pruekprasert is with National Institute of Informatics, Tokyo 100-0003, Japan. sasinee@nii.ac.jp

[2] Kai Cai is with Department of Electrical and Information Engineering, Osaka City University, Osaka 558-8585, Japan. kai.cai@eng.osaka-cu.ac.jp

A. Local and Global Systems

For each $i \in \{1, \dots, n\}$, we model the local DES G_i as

$$G_i = (X_i, \Sigma_i, \delta_i, X_{\text{in},i}),$$

where X_i is the set of states, Σ_i is the set of events, $\delta_i : X_i \times \Sigma_i \rightharpoonup X_i$ is a partial transition function, and $X_{\text{in},i} \subseteq X_i$ is the set of initial states. We use the notation $\delta_i(x, \sigma)!$ for "$\delta_i(x, \sigma)$ is defined". We also write Σ_{G_i} (*resp.* δ_{G_i}) for Σ_i (*resp.* δ_i) when we specifically refer to it as the event set (*resp.* the transition function) of the DES G_i.

The global DES is a distributed system that consists of all n local DESs as its components, constructed by the parallel composition of their local DESs.

Definition 1 ([13]): Given two DESs G_i and G_j, their parallel composition is the DES

$$G_i \parallel G_j = (X_i \times X_j, \Sigma_{G_i \| G_j}, \delta_{G_i \| G_j}, X_{\text{in},i} \times X_{\text{in},j}),$$

where $\Sigma_{G_i \| G_j} = \Sigma_{G_i} \cup \Sigma_{G_j}$ and the transition function $\delta_{G_i \| G_j} : X_i \times X_j \times \Sigma_{G_i \| G_j} \rightharpoonup X_i \times X_j$ is defined as follows.

$$\delta_{G_i \| G_j}(x_i, x_j, \sigma) = \begin{cases} (\delta_{G_i}(x_i, \sigma), \delta_{G_j}(x_j, \sigma)) & \text{(1a)} \\ \qquad \text{if } \delta_{G_i}(x_i, \sigma)! \text{ and } \delta_{G_j}(x_j, \sigma)! & \\ (\delta_{G_i}(x_i, \sigma), x_j) & \text{(1b)} \\ \qquad \text{if } \delta_{G_i}(x_i, \sigma)! \text{ and } \sigma \notin \Sigma_{G_j} & \\ (x_i, \delta_{G_j}(x_j, \sigma)) & \text{(1c)} \\ \qquad \text{if } \delta_{G_j}(x_j, \sigma)! \text{ and } \sigma \notin \Sigma_{G_i} & \\ \text{undefined otherwise.} & \text{(1d)} \end{cases}$$

Let $G_i \parallel G_j \parallel G_k = G_i \parallel (G_j \parallel G_k)$. From Definition 1, the parallel composition of two DESs is also a DES. Moreover, the composition is associative and commutative up to a reordering of the state components in composed states [13], i.e., $G_i \parallel (G_j \parallel G_k) = (G_i \parallel G_j) \parallel G_k$, and $G_i \parallel G_j$ can be obtained from $G_j \parallel G_i$ by reordering the state components. In this work, as we consider indexed local DESs, we can treat $G_i \parallel G_j$ and $G_j \parallel G_i$ as equivalent.

The global DES is the parallel composition

$$\mathcal{G} = (\mathcal{X}, \Sigma_{\mathcal{G}}, \Delta, \mathcal{X}_{\text{in}}) = G_1 \parallel \dots \parallel G_n,$$

where $\mathcal{X} = X_1 \times \cdots \times X_n$, $\Sigma_{\mathcal{G}} = \Sigma_1 \cup \cdots \cup \Sigma_n$, $\mathcal{X}_{\text{in}} = X_{\text{in},1} \times \cdots \times X_{\text{in},n}$, and $\Delta = \delta_{G_1 \| G_2 \| \dots \| G_n}$.

B. Extended Transition Functions and Event Sequences

For any DES $G = (X, \Sigma_G, \delta_G, X_{\text{in}})$, which can either be a local DES or a composition of local DESs, we extend its transition function δ_G to $\delta_G^* : X \times (\Sigma_G)^* \rightharpoonup X$ in the usual way. Namely, $\delta_G^*(x, \varepsilon) = x$ and for all $(\beta, \sigma) \in \Sigma_G^* \times \Sigma_G$,

$$\delta_G^*(x, \beta\sigma) = \begin{cases} \delta_G(\delta_G^*(x, \beta), \sigma) & \text{if } \delta_G^*(x, \beta)! \text{ and} \\ & \qquad \delta_G(\delta_G^*(x, \beta), \sigma)! \\ \text{undefined} & \text{otherwise.} \end{cases} \tag{2}$$

An event sequence α is generated by G if there exists $x \in X_{\text{in}}$ such that $\delta_G^*(x, \alpha)!$. Let $|\alpha| = k$ denote the length of the even sequences $\alpha = \sigma_1 \dots \sigma_k \in \Sigma^*$. As $\Sigma_G \subseteq \Sigma_{\mathcal{G}}$, let $\pi_G : \Sigma_{\mathcal{G}}^* \to \Sigma_G^*$ be the natural mapping from event sequences generated by the global DES $\mathcal{G}$ to those generated by the DES G. More precisely, $\pi_G(\sigma) = \varepsilon$ if $\sigma = \varepsilon$ or $\sigma \in \Sigma_{\mathcal{G}} \setminus \Sigma_G$, $\pi_G(\sigma) = \sigma$ if $\sigma \in \Sigma_G$, and $\pi_G(\beta\sigma) = \pi_G(\beta)\pi_G(\sigma)$ for all $(\beta, \sigma) \in \Sigma_{\mathcal{G}}^* \times \Sigma_{\mathcal{G}}$. For notational convenience, we also use π_i for denoting the mapping π_{G_i}, for $i \in \{1, \dots, n\}$. Thereby, we can use π_i to map each event sequence generated by the global DES $\mathcal{G}$ to its corresponding sequence generated by the local DES G_i. For all global state $x = (x_1, \dots, x_n) \in \mathcal{X}$, let $x[i]$ denote the local state $x_i \in X_i$.

From Definition 1, we have the following Lemma.

Lemma 1: For any $x \in \mathcal{X}_{\text{in}}$ and any $\alpha \in \Sigma^*$,

$$\Delta^*(x, \alpha)! \text{ if and only if } (\delta_i^*(x[i], \pi_i(\alpha))!, \forall i \in \{1, \dots n\}). \tag{3}$$

Moreover, if $\Delta^*(x, \alpha)!$,

$$\Delta^*(x, \alpha) = (\delta_1^*(x[1], \pi_1(\alpha)), \dots, \delta_n^*(x[n], \pi_n(\alpha))) \tag{4}$$

III. Problem formulation

A. Notion of Opacity

Let $\Sigma_{obs} \subseteq \Sigma_{\mathcal{G}}$ be the set of of observable events, and $\pi_{obs} : \Sigma_{\mathcal{G}}^* \to \Sigma_{obs}^*$ be the observation map from each event sequence generated by the global DES $\mathcal{G}$ to the event sequence observed by the intruder. Notice that $\pi_i \circ \pi_{obs}(\alpha) = \pi_{obs} \circ \pi_i(\alpha)$, for all $\alpha \in \Sigma_{\mathcal{G}}^*$ and all $i \in \{1, \dots, n\}$.

In this paper, we consider two notions of opacity: current-state opacity (CSO) and initial-state opacity (ISO), which are two basic types of opacity properties in the literature [5]. The study of these two types of opacity will lay a foundation for investigation of more complicated opacity notions. Consider $G = (X, \Sigma_G, \delta_G, X_{\text{in}})$, which can either be a local DES or a composition of local DESs.

Definition 2 (CSO): Given a set $S \subseteq X$ of secret states, the DES G is *current-state opaque (CSO)* w.r.t. S if, for all $(x, \alpha) \in X_{\text{in}} \times \Sigma_G^*$ such that $\delta_G^*(x, \alpha) \in S$, there exists $(x', \alpha') \in X_{\text{in}} \times \Sigma_G^*$ such that $\delta_G^*(x', \alpha') \in X \setminus S$ and $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$.

Definition 3 (ISO): Given a set $S \subseteq X_{\text{in}}$ of secret initial states, the DES G is *initial-state opaque (ISO)* w.r.t. S if for all $(x, \alpha) \in S \times \Sigma_G^*$ with $\delta_G^*(x, \alpha)!$, there exists $(x', \alpha') \in (X \setminus S) \times \Sigma_G^*$ with $\delta_G^*(x', \alpha')!$ and $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$.

The intuitions of the two notions of opacity are as follows. CSO (*resp.* ISO) requires that for each even sequence α going to (*resp.* starting from) a secret state, there must exists another sequence α' with the same observation ($\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$) going to (*resp.* starting from) a non-secret state.

By Definitions 2 and 3, we have Lemmas 2 and 3, which state that we can verify the opacity w.r.t. a set S by considering its subsets $S_1, \dots, S_m$ such that $S = S_1 \cup \cdots \cup S_m$.

Lemma 2: Suppose that for all $i \in \{1, \dots, m\}$ and all $(x, \alpha) \in X_{\text{in}} \times \Sigma_G^*$ such that $\delta_G^*(x, \alpha) \in S_i$, there exists $(x', \alpha') \in X_{\text{in}} \times \Sigma_G^*$ with $\delta_G^*(x', \alpha') \in X \setminus S$ and $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$. Then, G is CSO w.r.t. S

Lemma 3: Suppose that for all $i \in \{1, \dots, m\}$ and all $(x, \alpha) \in S_i \times \Sigma_G^*$ such that $\delta_G^*(x, \alpha)!$, there exists $(x', \alpha') \in (X_{\text{in}} \setminus S) \times \Sigma_G^*$ with $\delta_G^*(x', \alpha')!$ and $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$. Then, G is ISO w.r.t. S

Lemma 2 (*resp.* Lemma 3) implies that: if for all even sequence α going to (*resp.* starting from) a secret subset S_i, there exists another sequence α' with the same observation going to (*resp.* starting from) a non-secret state $X \setminus S$, then the DES G is opaque. These two lemmas follows from Definitions 2 and 3 and the fact that $S = S_1 \cup \cdots \cup S_m$.

B. Opacity Verification Problem

The goal of this work is to verify whether or not the global DES $\mathcal{G}$ is opaque (CSO, ISO) w.r.t. a given set $\mathcal{S}$.

Definition 4 (Opacity verification problem): Given local DESs $G_1, \dots, G_n$, an observation map π_{obs}, and a secret subset $\mathcal{S} \subseteq \mathcal{X}$ of global states, verify whether the global DES $\mathcal{G} =\|_{i\in\{1,\dots,n\}} G_i$ is opaque (CSO, ISO) w.r.t. $\mathcal{S}$.

Opacity verification for modular systems is decidable but costly [9]. One technique for modular systems opacity verification is to construct an observer automaton that estimate the intruder's information of the global DES based on observed event sequences, which can be large, especially for the system with many local DESs. Therefore, in this work, we consider *local opacity verification*: to verify the global DES without constructing an observer automaton for the global DES. In Sections IV and V, we propose sufficient conditions and corresponding efficient approaches for the opacity verification problem based only on the observer automata of local DESs.

IV. Local Opacity Verification

A. Assumption on Shared Events

We first introduce an assumption on shared event, which is necessary for our results. We assume that events shared by at least two local DESs are observable by the intruder, as depicted in Fig. 1. This assumption is common for DESs with modular structure [10], [14].

Assumption 1: For all $\sigma \in \Sigma_{\mathcal{G}}$, we have $\sigma \in \Sigma_{obs}$ if there exist $i, j \in \{1, \dots, n\}$ such that $i \neq j$ and $\sigma \in \Sigma_i \cap \Sigma_j$.

Note that we allow internal events of local DESs to be observable, i.e., we do not require $(\Sigma_i \setminus \bigcup_{j\neq i} \Sigma_j) \cap \Sigma_{obs} = \emptyset$.

Assumption 1 is a necessary condition for local opacity verification. We will discuss this matter in details later on in Remarks 1 and 3. Under this assumption, we have Lemma 4, which is crucial for our results in the next sections. The intuition of this lemma is that: an event sequence α_i' generated by a local DES G_i can be projected to a sequence of the global DES (not blocked by the parallel composition) if there exists at least one sequence α generated by the global DES with $\pi_{obs} \circ \pi_i(\alpha) = \pi_{obs}(\alpha_i')$.

Lemma 4: Given a secret subset $\mathcal{S} \subseteq \mathcal{X}$ of global states, we assume that Assumption 1 holds and there exists $(x, \alpha) \in \mathcal{X}_{\text{in}} \times \Sigma_{\mathcal{G}}^*$ such that $\Delta^*(x, \alpha)!$. Then, for any $(x_i', \alpha_i') \in X_{\text{in},i} \times \Sigma_i^*$ satisfying

$$\delta_i^*(x_i', \alpha_i')! \text{ and } \pi_{obs}(\alpha_i') = \pi_{obs} \circ \pi_i(\alpha), \tag{5}$$

there exists $\alpha' \in \Sigma_{\mathcal{G}}^*$ such that $\pi_{obs}(\alpha') = \pi_{obs}(\alpha)$ and

$$\begin{aligned} &\Delta^*(x[1], \dots, x[i-1], x_i', x[i+1], \dots, x[n], \alpha') \\ &\quad = (s_1, \dots, s_{i-1}, \delta_i^*(x_i', \alpha_i'), s_{i+1}, \dots, s_n), \end{aligned} \tag{6}$$

where $s_j = \delta_j^*(x[j], \pi_j(\alpha))$ for all $j \in \{1, \dots, n\}$.

Proof: Since the parallel composition operation is commutative and associative, we assume without loss of generality that $G_i = G_1$ and $\mathcal{G} = G_1 \parallel \mathcal{G}_J$, where $\mathcal{G}_J =\|_{k\in\{2,\dots,n\}} G_k$. Therefore, we can write $x = (x[1], x_J)$, where $x_J = (x[2], \dots, x[n])$. We will prove the lemma by induction on the length of α.

For the base step, we consider the case where $\alpha = \varepsilon$. For any $(x_1', \alpha_1') \in X_{\text{in},1} \times \Sigma_1^*$ such that

$$\delta_1^*(x_1', \alpha_1')! \text{ and } \pi_{obs}(\alpha_1') = \pi_{obs} \circ \pi_1(\alpha) = \varepsilon,$$

we have $\alpha_1' \in (\Sigma_1 \setminus \bigcup_{k\in\{1,\dots,n\}} \Sigma_k)^*$ by Assumption 1. By (1b) and Lemma 1,

$$\Delta^*(x_1', x_J, \alpha_1') = (\delta_1^*(x_1', \alpha_1'), s_2, \dots, s_n),$$

which implies (6).

For the induction hypothesis, we assume that if $|\alpha| < k$, then, for all $(x_1', \alpha_1') \in X_{\text{in},1} \times \Sigma_1^*$ satisfying (5), there exists $\alpha' \in \Sigma_{\mathcal{G}}^*$ satisfying $\pi_{obs}(\alpha') = \pi_{obs}(\alpha)$ and (6).

For the inductive step, let $\alpha = \beta\sigma$, where $\sigma \in \Sigma_{\mathcal{G}}$ and $|\beta| < k$. Since $\Delta^*(x, \alpha)!$, we have $\delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))!$ by Lemma 1. Furthermore, $\Delta^*(x, \beta)!$ and $\Delta(\Delta^*(x, \beta), \sigma)!$ by (2). Let us consider any $(x_1', \alpha_1') \in X_{\text{in},1} \times \Sigma_1^*$ that satisfies (5). To show (6), we consider the following cases.

- Case 1: $\sigma \in \Sigma_{\mathcal{G}_J} \setminus \Sigma_1$. In this case, $\pi_{obs}(\alpha_1') = \pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)$. By the induction hypothesis, there exists $\beta' \in \Sigma_{\mathcal{G}}^*$ such that $\pi_{obs}(\beta') = \pi_{obs}(\beta)$ and

  $$\Delta^*(x_1', x_J, \beta') = (\delta_1^*(x_1', \alpha_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta))) \tag{7}$$

  By setting $\alpha' = \beta'\sigma$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\beta'\sigma) = \pi_{obs}(\beta\sigma) = \pi_{obs}(\alpha)$. Moreover, since $\sigma \notin \Sigma_1$, by (1c), (7), and Lemma 1,

  $$\begin{aligned} \Delta^*(x_1', x_J, \alpha') &= \Delta^*(x_1', x_J, \beta'\sigma) \\ &= (\delta_1^*(x_1', \alpha_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta\sigma))) \\ &= (\delta_1^*(x_1', \alpha_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))) \\ &= (\delta_1^*(x_1', \alpha_1'), s_2, \dots, s_n). \end{aligned}$$

  Thus, (6) holds in this case.
- Case 2: $\sigma \in \Sigma_1 \cap \Sigma_{\mathcal{G}_J}$. By Assumption 1, $\pi_{obs} \circ \pi_1(\sigma) = \sigma$ and $\pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)\sigma$. By (5), there exists $\beta_1' \in \Sigma_1^*$ such that $\beta_1'\sigma = \alpha_1'$ and

  $$\pi_{obs}(\beta_1')\sigma = \pi_{obs}(\alpha_1') = \pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)\sigma.$$

  Therefore, $\pi_{obs}(\beta_1') = \pi_{obs} \circ \pi_1(\beta)$. By the induction hypothesis, there exists β' with $\pi_{obs}(\beta') = \pi_{obs}(\beta)$ and

  $$\Delta^*(x_1', x_J, \beta') = (\delta_1^*(x_1', \beta_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta))). \tag{8}$$

  By setting $\alpha' = \beta'\sigma$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\beta')\sigma = \pi_{obs}(\beta)\sigma = \pi_{obs}(\alpha)$. By (1a), (8), and Lemma 1,

  $$\begin{aligned} \Delta^*(x_1', x_J, \alpha') &= \Delta^*(x_1', x_J, \beta'\sigma) \\ &= (\delta_1^*(x_1', \beta_1'\sigma), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))) \\ &= (\delta_1^*(x_1', \alpha_1'), s_2, \dots, s_n), \end{aligned}$$

  which implies (6).
- Case 3: $\sigma \in (\Sigma_1 \setminus \Sigma_{\mathcal{G}_J}) \cap \Sigma_{obs}$. As $\sigma \in \Sigma_1 \cap \Sigma_{obs}$, we have $\pi_{obs} \circ \pi_1(\sigma) = \sigma$ and $\pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)\sigma$.

It can be shown in the same way as in Case 2 that there exist $\beta_1' \in \Sigma_1^*$ and $\beta' \in \Sigma_{\mathcal{G}}^*$ satisfying (8), $\alpha_1' = \beta_1'\sigma$, and $\pi_{obs}(\beta') = \pi_{obs}(\beta)$. Moreover, since $\sigma \notin \Sigma_{\mathcal{G}_J}$, we have $\pi_{\mathcal{G}_J}(\alpha) = \pi_{\mathcal{G}_J}(\beta)$.

By setting $\alpha' = \beta'\sigma$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\beta)\sigma = \pi_{obs}(\alpha)$. Then, by (1b), (8), and Lemma 1,

$$\begin{aligned}\Delta^*(x_1', x_J, \alpha') &= (\delta_1^*(x_1', \beta_1'\sigma), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta)))\\ &= (\delta_1^*(x_1', \alpha_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha)))\\ &= (\delta_1^*(x_1', \alpha_1'), s_2, \ldots, s_n),\end{aligned}$$

which implies (6).

- Case 4: $\sigma \in \Sigma_1 \setminus (\Sigma_{\mathcal{G}_J} \cup \Sigma_{obs})$. In this case, we have $\pi_{obs}(\sigma) = \varepsilon$, which implies that $\pi_{obs} \circ \pi_1(\sigma) = \varepsilon$ and $\pi_{obs}(\alpha_1') = \pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)$. By the induction hypothesis, there exists β' satisfying (7) and $\pi_{obs}(\beta') = \pi_{obs}(\beta)$. Since $\sigma \in \Sigma_1 \setminus \Sigma_{\mathcal{G}_J}$, we have

$$\begin{aligned}\delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha)) &= \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta\sigma))\\ &= \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta)).\end{aligned} \tag{9}$$

Since $\pi_{obs}(\sigma) = \varepsilon$, we have

$$\pi_{obs}(\beta') = \pi_{obs}(\beta')\pi_{obs}(\sigma) = \pi_{obs}(\beta\sigma) = \pi_{obs}(\alpha).$$

By setting $\alpha' = \beta'$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\alpha)$. Then, by (1b), (7), (9), and Lemma 1,

$$\begin{aligned}\Delta^*(x_1', x_J, \alpha') &= \Delta^*(x_1', x_J, \beta')\\ &= (\delta_1^*(x_1', \alpha_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta)))\\ &= (\delta_1^*(x_1', \alpha_1'), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha)))\\ &= (\delta_1^*(x_1', \alpha_1'), s_2, \ldots, s_n),\end{aligned}$$

which implies (6).

As (6) holds for all cases, the induction is concluded. ■

B. Local Current-state Opacity

This section introduces sufficient conditions for the CSO of the global DES, based on the local DESs. For a set $\mathcal{S}$ of global secret states, let $\mathcal{S}[i] = \{s[i] \mid s \in \mathcal{S}\}$ be the set of its corresponding local secret states in the local DES G_i.

Theorem 1: We assume Assumption 1. Given a secret subset $\mathcal{S} \subseteq \mathcal{X}$ of global states, if there exists $i \in \{1, \ldots, n\}$ where G_i is CSO w.r.t. $\mathcal{S}[i]$, then $\mathcal{G}$ is also CSO w.r.t. $\mathcal{S}$.

Proof: We assume that G_i is CSO w.r.t. $\mathcal{S}[i]$ and will show that $\mathcal{G}$ is CSO w.r.t. $\mathcal{S}$. Let us consider any

$$(x, \alpha) \in \mathcal{X}_{\text{in}} \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha) = s \in \mathcal{S}.$$

By Lemma 1, $\delta_i^*(x[i], \pi_i(\alpha)) = s[i] \in \mathcal{S}[i]$. Since G_i is CSO w.r.t. $\mathcal{S}[i]$, by Definition 2, there exists $(x_i', \alpha_i') \in X_i \times \Sigma_i^*$ such that

$$\pi_{obs}(\alpha_i') = \pi_{obs} \circ \pi_i(\alpha) \text{ and } \delta_i^*(x_i', \alpha_i') \in X_i \setminus \mathcal{S}[i].$$

By Lemma 4, there exists α' with $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$ and

$$\begin{aligned}&\Delta^*(x[1], \ldots, x[i-1], x_i', x[i+1], \ldots, x[n], \alpha')\\ &\quad = (s[1], \ldots, s[i-1], \delta_i^*(x_i', \alpha_i'), s[i+1], \ldots, s[n])\\ &\quad \in \mathcal{X} \setminus \mathcal{S}.\end{aligned}$$

Thereby, $\mathcal{G}$ is CSO w.r.t. $\mathcal{S}$ and the theorem holds. ■

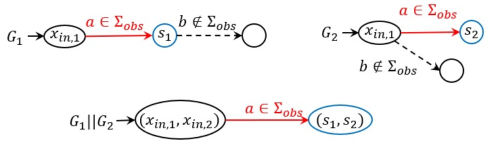

Fig. 2. Two local DESs and the accessible part of their parallel composition. The DES G_1 is CSO w.r.t $\{s_1\}$, but $G_1 \parallel G_2$ is not CSO w.r.t. $\{(s_1, s_2)\}$.

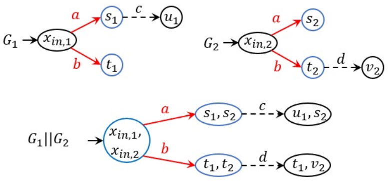

Fig. 3. Two local DESs and the accessible part of their parallel composition. $\Sigma_{obs} = \{a, b\}$. The DESs G_1 and G_2 are not CSO w.r.t. $\{s_1, t_1\}$ and $\{s_2, t_2\}$, respectively, but their composition $G_1 \parallel G_2$ is CSO w.r.t. $\{(s_1, s_2), (s_1, t_2), (t_1, s_2), (t_1, t_2)\}$.

Remark 1: Assumption 1 is a necessary condition for Theorem 1. In the example DES in Fig. 2, in which the shared event b is not observable, G_1 is CSO w.r.t. $\{s_1\}$ but $G_1 \parallel G_2$ is not CSO w.r.t. $\{s_1, s_2\}$. In this example, the shared event b is blocked by the parallel composition. Such an event blocking is generally difficult to detect without constructing any part of $\mathcal{G}$, which we aim to avoid.

Remark 2: The inverse of the implication in Theorem 1 does not hold. In other words, the global DES $\mathcal{G}$ being CSO w.r.t. $\mathcal{S}$ does not imply the existence of a local DES G_i that is CSO w.r.t. $\mathcal{S}[i] = \{s[i] \mid s \in \mathcal{S}\}$. We provide two counter examples in Fig. 3 and Fig. 4. In both examples, each local DES G_i, $i \in \{1, 2\}$, is not CSO w.r.t. $\mathcal{S}[i]$, but the global DES $\mathcal{G}$ is CSO w.r.t. $\mathcal{S}$. From both examples, we can see that the inverse of the implication in Theorem 1 does not hold even if $\mathcal{S} = \mathcal{S}[i] \times \ldots \times \mathcal{S}[n]$. Notice that, in Fig. 3, the global DES becomes CSO thanks to unobservable local events c and d. In Fig. 4, the event sequence reaching the secret state (t_1, t_2) is blocked by the parallel composition. As discussed in Remark 1, detecting such a blocked event sequence is difficult without constructing any part of $\mathcal{G}$.

As presented above, Theorem 1 provides a sufficient condition for the opacity of the global DES. If there is no local DES G_i that is CSO w.r.t. $\mathcal{S}[i]$, it is still possible that $\mathcal{G}$ is CSO w.r.t. $\mathcal{S}$. Using Lemma 2, we propose another sufficient condition for the CSO of $\mathcal{G}$ by considering its secret subsets $\mathcal{S}_1, \ldots, \mathcal{S}_m \in \mathcal{S}$ where $\mathcal{S} = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_m$.

Theorem 2: We assume Assumption 1. Consider a set of secret global states $\mathcal{S} = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_m \subseteq \mathcal{X}$. Let $\mathcal{S}[i] = \{s[i] \mid s \in \mathcal{S}\}$ and $\mathcal{S}_j[i] = \{s[i] \mid s \in \mathcal{S}_j\}$ for all $j \in \{1, \ldots, m\}$. Suppose that, for all global secret subset $\mathcal{S}_{j \in \{1,\ldots,m\}}$, there exists a local DES $G_{i \in \{1,\ldots,n\}}$ such that:

$$\begin{aligned}&\forall (x_i, \alpha_i) \in X_{i,\text{in}} \times \Sigma_i^*, \delta_i^*(x_i, \alpha_i) \in \mathcal{S}_j[i],\\ &\quad \exists (x_i', \alpha_i') \in X_{i,\text{in}} \times \Sigma_i^*, \delta_i^*(x_i', \alpha_i') \in X_i \setminus \mathcal{S}[i]\\ &\qquad\qquad \text{and } \pi_{obs}(\alpha_i') = \pi_{obs}(\alpha_i).\end{aligned} \tag{10}$$

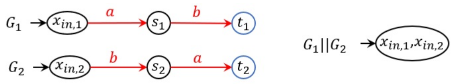

Fig. 4. Two local DESs and the accessible part of their parallel composition. All events are observable. The DESs G_1 and G_2 are not CSO w.r.t. $\{t_1\}$ and $\{t_2\}$, respectively, but $G_1 \parallel G_2$ is CSO w.r.t. $\{(t_1, t_2)\}$.

Then, $\mathcal{G}$ is CSO w.r.t. $\mathcal{S}$.

Proof: Let us consider each secret subset $\mathcal{S}_{j\in\{1,\ldots,m\}}$ and let $G_{i\in\{1,\ldots,n\}}$ be the local DES that satisfy (10). Consider any

$$(x, \alpha) \in \mathcal{X}_{\text{in}} \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha) = s \in \mathcal{S}_j. \tag{11}$$

By Lemma 1, $\delta_i^*(x[i], \pi_i(\alpha)) = s[i] \in \mathcal{S}_j[i]$. By (10), there exists $(x_i', \alpha_i') \in X_i \times \Sigma_i^*$ such that

$$\pi_{obs}(\alpha_i') = \pi_{obs} \circ \pi_i(\alpha) \text{ and } \delta_i^*(x_i', \alpha_i') \in X_i \setminus \mathcal{S}[i].$$

By Lemma 4, there exists α' with $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$ and

$$\Delta^*(x[1], \ldots, x[i-1], \delta_i^*(x_i', \alpha_i'), x[i+1], \ldots, x[n], \alpha') \\ \in \mathcal{X} \setminus \mathcal{S}. \tag{12}$$

By Lemma 2, (11) and (12), the global DES $\mathcal{G}$ is CSO w.r.t. $\mathcal{S}$ and the theorem holds. ■

Theorem 2 also provides a sufficient condition. Its inverse of the implication does not hold, as shown in the counter example in Fig. 4. However, we show in Section V that we can use this theorem to verify the global DES in some cases.

C. Local Initial-state Opacity

In this section, we show that the presented results for CSO also hold for ISO.

Theorem 3: We assume Assumption 1. Given a secret subset $\mathcal{S} \subseteq \mathcal{X}_{\text{in}}$ of global initial states, if there exists $i \in \{1, \ldots, n\}$ such that G_i is ISO w.r.t. $\mathcal{S}[i] = \{s[i] \mid s \in \mathcal{S}\}$, then $\mathcal{G}$ is also ISO w.r.t. $\mathcal{S}$.

Proof: Suppose that Assumption 1 holds and G_i is ISO w.r.t. $\mathcal{S}[i]$. Consider any pair

$$(x, \alpha) \in \mathcal{S} \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha)!. \tag{13}$$

By Lemma 1, $\delta^*(x[i], \pi_i(\alpha))!$. Since $x[i] \in \mathcal{S}[i]$ and G_i is ISO w.r.t. $\mathcal{S}[i]$, there exists $(x_i', \alpha_i') \in (X_i \setminus \mathcal{S}[i]) \times \Sigma_i^*$ with

$$\delta^*(x_i', \alpha_i')! \text{ and } \pi_{obs}(\alpha_i') = \pi_{obs} \circ \pi_i(\alpha).$$

Let $x' = x[1], \ldots, x[i-1], x_i', x[i+1], \ldots, x[n]$. By Lemma 4, there exists α' such that

$$\Delta^*(x', \alpha')! \text{ and } \pi_{obs}(\alpha) = \pi_{obs}(\alpha'). \tag{14}$$

Notice that $x' \in \mathcal{X} \setminus \mathcal{S}$ because $x_i' \in X_i \setminus \mathcal{S}[i]$. Therefore, the lemma holds by (13), (14), and Definition 3. ■

Remark 3: Assumption 1 is a necessary condition for Theorem 3. From the example in Fig. 5, G_2 is ISO w.r.t $\{s_2\}$, but $G_1 \parallel G_2$ is not ISO w.r.t. $\{(s_1, s_2)\}$.

Remark 4: The inverse of the implication in Theorem 3 also does not hold. The global DES $\mathcal{G}$ being ISO w.r.t. $\mathcal{S}$ does not imply the existence of a local DES G_i that is ISO w.r.t. $\mathcal{S}[i] = \{s[i] \mid s \in \mathcal{S}\}$. Fig. 6 provides a counter example. Both local DESs G_1 and G_2 are not ISO w.r.t $\{s_1, t_1\}$ and $\{s_2, t_2\}$, respectively, but $G_1 \parallel G_2$ is ISO w.r.t. $\{(s_1, s_2), (t_1, t_2)\}$.

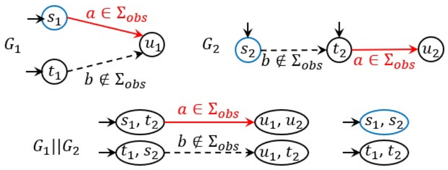

Fig. 5. Two local DESs and the accessible part of their parallel composition. Initial states of G_1 (*resp.* G_2) are s_1 and t_1 (*resp.* s_2 and t_2). The DES G_2 is ISO w.r.t $\{s_2\}$, but $G_1 \parallel G_2$ is not ISO w.r.t. $\{(s_1, s_2)\}$.

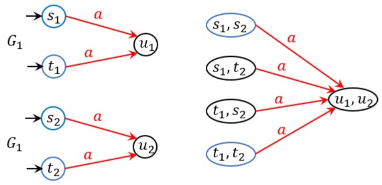

Fig. 6. Two local DESs and the accessible part of their parallel composition. Initial states of G_1 (*resp.* G_2) are s_1 and t_1 (*resp.* s_2 and t_2). The event a is observable. The DESs G_1 and G_2 are both not ISO w.r.t $\{s_1, t_1\}$ and $\{s_2, t_2\}$, respectively, but $G_1 \parallel G_2$ is ISO w.r.t. $\{(s_1, s_2), (t_1, t_2)\}$.

In the same way as in Theorem 2, we propose another sufficient condition in for the ISO of $\mathcal{G}$ by considering its secret subsets $\mathcal{S}_1, \ldots, \mathcal{S}_m \in \mathcal{S}$ where $\mathcal{S} = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_m$.

Theorem 4: We assume Assumption 1. Consider a set of secret global initial states $\mathcal{S} = \mathcal{S}_1 \cup \ldots \cup \mathcal{S}_m \subseteq \mathcal{X}_{\text{in}}$. Let $\mathcal{S}[i] = \{s[i] \mid s \in \mathcal{S}\}$ and $\mathcal{S}_j[i] = \{s[i] \mid s \in \mathcal{S}_j\}$ for all $j \in \{1, \ldots, m\}$. Suppose that for all global secret subset $\mathcal{S}_{j\in\{1,\ldots,m\}}$, there exists a local DES $G_{i\in\{1,\ldots,n\}}$ such that:

$$\forall (x_i, \alpha_i) \in \mathcal{S}_j[i] \times \Sigma_i^*, \delta_i(x_i, \alpha_i)!, \\ \exists (x_i', \alpha_i') \in (X_i \backslash \mathcal{S}[i]) \times \Sigma_i^*, \delta_i(x_i', \alpha_i')! \\ \text{and } \pi_{obs}(\alpha_i') = \pi_{obs}(\alpha_i). \tag{15}$$

Then, $\mathcal{G}$ is ISO w.r.t. $\mathcal{S}$.

Proof: Consider any secret subset $\mathcal{S}_{j\in\{1,\ldots,m\}}$ and let $G_{i\in\{1,\ldots,n\}}$ be the local DES that satisfy (15). Consider any

$$(x, \alpha) \in \mathcal{S}_j \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha)! \tag{16}$$

By Lemma 1, $\delta_i^*(x[i], \pi_i(\alpha))!$ and $x[i] \in \mathcal{S}_j[i]$. By (15), there exists $(x_i', \alpha_i') \in (X_i \setminus \mathcal{S}[i]) \times \Sigma_i^*$ such that

$$\pi_{obs}(\alpha_i') = \pi_{obs} \circ \pi_i(\alpha) \text{ and } \delta_i^*(x_i', \alpha_i')!$$

Let $x' = x[1], \ldots, x[i-1], x_i', x[i+1], \ldots, x[n]$. By Lemma 4, there exists α' such that

$$\Delta^*(x', \alpha')! \text{ and } \pi_{obs}(\alpha) = \pi_{obs}(\alpha'). \tag{17}$$

Notice that $x' \in \mathcal{X} \setminus \mathcal{S}$ because $x_i' \in X_i \setminus \mathcal{S}[i]$. By Lemma 3, (16) and (17), the global DES $\mathcal{G}$ is ISO w.r.t. $\mathcal{S}$. ■

The inverse of the implication in Theorem 3 also does not hold, as it can be shown using the counter example in Fig. 6.

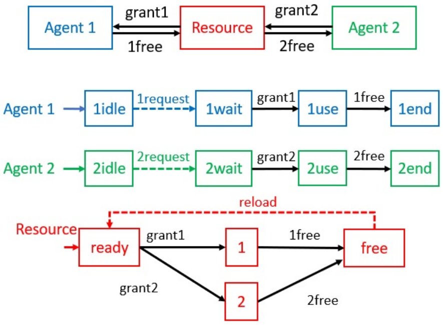

Fig. 7. Two agents sharing one resource. The events "1request", "2request", and "reload" are not observable by the intruder.

V. Opacity Verification of Global System

In section IV, we presented the sufficient conditions of the opacity (CSO and ISO) of the global system $\mathcal{G}$, by only considering the local DESs G_i, $i \in \{1, \dots, n\}$. The straightforward way to use Theorems 1 and 3 is to verify each local DES using existing opacity verification algorithms (e.g. [15]). Then, if there exists a local DES G_i that is opaque w.r.t. $\mathcal{S}[i]$, the global DES $\mathcal{G}$ is also opaque w.r.t. $\mathcal{S}$ thanks to Theorems 1 and 3. By using this technique, we only need to construct the intruder's observer automata [13] for each local DES G_i, not the global DES $\mathcal{G}$. As a result, we can reduce the size of the intruder's observer automata from $\mathcal{O}(2^{|X_1| \times \dots \times |X_n|})$ (for $\mathcal{G}$) to $\mathcal{O}(2^{|X_1|} + \dots + 2^{|X_n|})$.

For example, let us consider the global DES $\mathit{Agent1} \parallel \mathit{Agent2} \parallel \mathit{Resource}$ of the DESs in Fig. 7. Suppose that $(\mathit{1wait}, \mathit{2use}, \mathit{2})$ is the only secret state. By the observer automaton in Fig. 8 (a), we know that $\mathit{Agent1}$ is CSO w.r.t. $\{\mathit{1wait}\}$. Thus, by Theorem 1, the global system is also CSO.

As discussed in Remarks 2 and 4, Theorems 1 and 3 provide only sufficient conditions for the opacity of the global DES. If there is no local DES G_i that is opaque w.r.t. $\mathcal{S}[i]$, it is still possible that $\mathcal{G}$ is opaque w.r.t. $\mathcal{S}$. By Theorems 2 and 4, we can try to verify the opacity of $\mathcal{G}$ by verifying the opacity of each G_i w.r.t. $\{s\}$, for all secret state $s \in \mathcal{S}$. Let us again consider the global DES of the DESs in Fig. 7, but this time let the secret set be $\mathcal{S} = \{(\mathit{1wait}, \mathit{2use}, \mathit{2}), (\mathit{1use}, \mathit{2wait}, \mathit{1})(\mathit{1end}, \mathit{2end}, \mathit{free})\}$. For this case, we cannot simply verify the global DES by verifying local DESs w.r.t. theirs corresponding local secret sets, e.g., $\mathit{Agent1}$ is not CSO w.r.t. $\{\mathit{1wait}, \mathit{1use}, \mathit{1end}\}$. Let $\mathcal{S}_1 = \{(\mathit{1wait}, \mathit{2use}, \mathit{2})\}$, $\mathcal{S}_2 = \{(\mathit{1use}, \mathit{2wait}, \mathit{1})\}$, and $\mathcal{S}_3 = \{(\mathit{1end}, \mathit{2end}, \mathit{free})\}$. Let G_1, G_2, and G_3 be the local DESs $\mathit{Agent1}$, $\mathit{Agent2}$, and $\mathit{Resource}$, respectively. Using the observer automata in Fig. 8, we have the following properties.

1) $\mathcal{S}_1[1] = \{\mathit{1wait}\}$. For the event sequence $\mathit{1request}$ with $\delta_1(\mathit{1idle}, \mathit{1request}) = \mathit{1wait} \in \mathcal{S}_1[1]$, we have $\delta_1(\mathit{1idle}, \varepsilon) = \mathit{1idle} \notin \mathcal{S}[1] = \{\mathit{1wait}, \mathit{1use}, \mathit{1end}\}$ and $\pi_{obs}(1request) = \pi_{obs}(\varepsilon) = \varepsilon$.
2) $\mathcal{S}_2[2] = \{\mathit{2wait}\}$. For the event sequence $\mathit{2request}$ with $\delta_2(\mathit{2idle}, \mathit{2request}) = \mathit{2wait} \in \mathcal{S}_2[2]$, we have $\delta_2(\mathit{2idle}, \varepsilon) = \mathit{2idle} \notin \mathcal{S}[2] = \{\mathit{2wait}, \mathit{2use}, \mathit{2end}\}$ and $\pi_{obs}(2request) = \pi_{obs}(\varepsilon) = \varepsilon$.

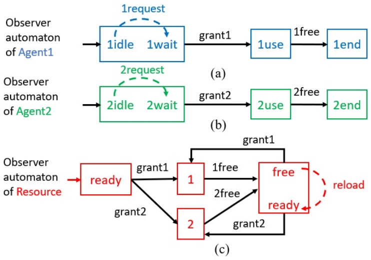

Fig. 8. Intruder's CSO observer automata for local DESs in Fig. 7.

3) $\mathcal{S}_3[3] = \{\mathit{free}\}$. For all $\alpha \in \Sigma_3^*$ such that $\delta_3(\mathit{ready}, \alpha) = \mathit{free} \in \mathcal{S}_3[3]$, we have $\alpha' = \alpha\,\mathit{reload}$ where $\delta_3(\mathit{ready}, \alpha') = \mathit{ready} \notin \mathcal{S}[3] = \{1, 2, \mathit{free}\}$ and $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$.

Therefore, by Theorem 2, the global DES is CSO w.r.t $\mathcal{S}$. Thus, for this case, we can verify the global DES using the observer automata of the local DESs.

VI. Conclusions

We study the current-state opacity (CSO) and the initial-state opacity (ISO) verification of a distributed DES. The distributed DES, which we call the global DES, is the parallel composition of n local DESs. By assuming that the intruder observes the events shared between local DESs, we proposed sufficient conditions for the opacity (CSO and ISO) of the global DES, by considering only the opacity of local DESs. Using these sufficient conditions, we introduced efficient methodologies to verify the global DES's opacity without constructing the intruder's observer automaton of the global DES. For future work, we will study the verification of other system opacity concepts and the opacity enforcement of distributed DESs.

References

[1] L. Mazaré, "Using unification for opacity properties," *Proceedings of the 4th IFIP WG1*, vol. 7, pp. 165–176, 2004.

[2] J. W. Bryans, M. Koutny, and P. Y. Ryan, "Modelling opacity using petri nets," *Electronic Notes in Theoretical Computer Science*, vol. 121, pp. 101–115, 2005.

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

[4] R. Jacob, J.-J. Lesage, and J.-M. Faure, "Overview of discrete event systems opacity: Models, validation, and quantification," *Annual reviews in control*, vol. 41, pp. 135–146, 2016.

[5] Y. C. Wu and S. Lafortune, "Comparative analysis of related notions of opacity in centralized and coordinated architectures," *Discrete Event Dynamic Systems*, vol. 23, no. 3, pp. 307–339, 2013.

[6] 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.

[7] Y. Falcone and H. Marchand, "Enforcement and validation (at runtime) of various notions of opacity," *Discrete Event Dynamic Systems*, vol. 25, no. 4, pp. 531–570, 2015.

[8] Y. Guo, X. Jiang, C. Guo, S. Wang, and O. Karoui, "Overview of opacity in discrete event systems," *IEEE Access*, vol. 8, pp. 48 731–48 741, 2020.

[9] T. Masopust and X. Yin, "Complexity of detectability, opacity and a-diagnosability for modular discrete event systems," *Automatica*, vol. 101, pp. 290–295, 2019.

[10] A. Saboori and C. N. Hadjicostis, "Reduced-complexity verification for initial-state opacity in modular discrete event systems," *IFAC Proceedings Volumes*, vol. 43, no. 12, pp. 78–83, 2010.

[11] Y. Tong and H. Lan, "Current-state opacity verification in modular discrete event systems," in *2019 IEEE 58th Conference on Decision and Control (CDC)*. IEEE, 2019, pp. 7665–7670.

[12] G. Zinck, L. Ricker, H. Marchand, and L. Hélouët, "Enforcing opacity in modular systems," in *Ifac world Congress*, 2020.

[13] C. G. Cassandras and S. Lafortune, *Introduction to discrete event systems*. Springer Science & Business Media, 2009.

[14] O. Contant, S. Lafortune, and D. Teneketzis, "Diagnosability of discrete event systems with modular structure," *Discrete Event Dynamic Systems*, vol. 16, no. 1, pp. 9–37, 2006.

[15] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Current-state opacity enforcement in discrete event systems under incomparable observations," *Discrete Event Dynamic Systems*, vol. 28, no. 2, pp. 161–182, 2018.