

© 2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Local Opacity Verification for Distributed Discrete Event Systems

Sasinee Pruekprasert¹ and Kai Cai²

Abstract—This paper studies current-state opacity and initial-state opacity verification of distributed discrete event systems. The distributed system’s global model is the parallel composition of multiple local systems: each of which represents a component. We propose sufficient conditions for verifying opacity of the global system model 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 was introduced to the discrete event systems (DES) community in [2] for petri-nets, and in [3] for transition systems, and has been an active research topic in the DES community in recent years. Several notions of opacity have been proposed and studied in the literature [4], [5], [6]. Overviews, surveys on commonly used techniques and existing tools, and historical remarks on the opacity of DES are presented in [7], [8], [9].

This work studies the opacity verification of distributed DESs, 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 [10]. The monolithic approach to verify the opacity of modular systems 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. To mitigate this problem, many previous studies (e.g., [11], [12], [13]) investigated compositional opacity verification approaches. The approaches construct abstract structures of local DESs. Then, the opacity verification is performed by considering synchronizations between those abstract structures in a sound and efficient manner.

S. P. is supported by ERATO HASUO Metamathematics for Systems Design Project No. JPMJER1603, JST, and Grant-in-aid No. 21K14191, JSPS. K. C. is supported by Grant-in-aid No. 21H04875, JSPS.

¹Sasinee Pruekprasert is with the National Institute of Informatics, Hitotsubashi 2-1-2, Tokyo 101-8430, Japan. sasinee@nii.ac.jp

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

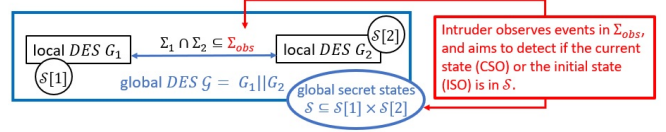


Fig. 1. An overview of our distributed architecture with two local DESs. The global DES G is the parallel composition of local DESs. The secret state set S is a subset of states of G . The intruder observes the events shared between the local DESs and some local events, then aims to detect if the current state (for the CSO) or the initial state (for the ISO) of G is in S (see Section III). Note that this architecture can be extended to n local DESs.

In this work, we propose a different approach to verify the opacity of distributed DESs, which we call *local opacity verification*. Our technique verifies the opacity of the global system of the distributed DESs by estimating the intruder’s information *based only on local DESs*. We propose sufficient conditions and their corresponding efficient verification approaches for the global DES’s opacity using local DESs’ observer automata. 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.

Reduced complexity opacity verification techniques for modular DESs by considering its local components was proposed for ISO in [14], and for CSO in [15] and [16]. However, our setting is different from the previous studies. The objective of [14] and [16] is to ensure that local secret states of all local DESs are protected confidentially. In both studies, the secret of the whole system is revealed if a secret state of any local DES is revealed. Instead, in our 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 [15], which considers one 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 setting, the intruder has only one observation map and observes the global DES’s event sequences directly. These differences make the algorithms developed in the previous studies unsuitable to solve our opacity verification problem.

The rest of this paper is organized as follows. In Section II, we propose a distributed architecture of a global DES with several local DESs. In Section III, we introduce the concept of local opacity verification. We present sufficient conditions for the global DES’s opacity in Section IV, and propose the corresponding approaches to verify the global DES using the observer automata of local DESs in Section V. 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.

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, $\delta_i : X_i \times \Sigma_i \rightarrow X_i$ 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 .

We consider a distributed system that consists of all n local DESs. The global DES of the distributed system is constructed by the parallel composition.

Definition 1 ([17]): Given two DESs G_i and G_j , their parallel composition is the DES

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

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

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

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 [17], 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, we consider indexed local DESs, so 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 $\mathcal{X} = X_1 \times \dots \times X_n$, $\Sigma_{\mathcal{G}} = \Sigma_1 \cup \dots \cup \Sigma_n$, $\mathcal{X}_{\text{in}} = X_{\text{in},1} \times \dots \times X_{\text{in},n}$, and $\Delta = \delta_{G_1 \parallel G_2 \parallel \dots \parallel G_n}$.

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 $\delta_G^* : X \times \Sigma_G^* \rightarrow X$ in the usual way. Namely, $\delta_G^*(x, \varepsilon) = x$, and for all $(\beta, \sigma) \in \Sigma_G^* \times \Sigma_G$,

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

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 event sequences $\alpha = \sigma_1 \dots \sigma_k \in \Sigma^*$. Let $\pi_G : \Sigma_G^* \rightarrow \Sigma_G^*$ 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 $\sigma \in \Sigma_G \setminus \Sigma_G$, $\pi_G(\sigma) = \sigma$ if $\sigma \in \Sigma_G$, and $\pi_G(\beta\sigma) = \pi_G(\beta)\pi_G(\sigma)$ for all $(\beta, \sigma) \in \Sigma_G^* \times \Sigma_G$. For notational convenience, we also use π_i for denoting the mapping π_{G_i} , for $i \in \{1, \dots, n\}$. Thereby, π_i maps each event sequence generated by the global DES \mathcal{G} to its corresponding sequence generated by the local DES G_i .

For a 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 $\alpha \in \Sigma^*$,

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

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

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

III. PROBLEM FORMULATION

A. Notion of Opacity

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 [4]. The study of these two types of opacity will lay a foundation for investigation of more complicated opacity notions.

Let $\Sigma_{\text{obs}} \subseteq \Sigma_{\mathcal{G}}$ be the set of observable events, and $\pi_{\text{obs}} : \Sigma_{\mathcal{G}}^* \rightarrow \Sigma_{\text{obs}}^*$ be the observation mapping from each event sequence of \mathcal{G} to the sequence observed by the intruder. Notice that the composite mappings $\pi_i \circ \pi_{\text{obs}}$ and $\pi_{\text{obs}} \circ \pi_i$ are equal. Let $G = (X, \Sigma_G, \delta_G, X_{\text{in}})$ 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 $\pi_{\text{obs}}(\alpha) = \pi_{\text{obs}}(\alpha')$.

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

The intuitions of CSO and ISO are as follows. CSO (resp. ISO) requires that for each event sequence α reaching (resp. starting from) a secret state, there exists another sequence α' with the same observable events ($\pi_{\text{obs}}(\alpha) = \pi_{\text{obs}}(\alpha')$) reaching (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 $S = S_1 \cup \dots \cup S_m$.

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

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

Lemma 2 (resp. Lemma 3) implies that if for each event sequence α reaching (resp. starting from) any secret subset S_j , there exists another sequence α' with the same observable events (resp. starting from) a non-secret state $X \setminus S$, then the DES G is opaque. These two lemmas follow from Definitions 2 and 3 and the fact that $S = S_1 \cup \dots \cup S_m$.

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 $\mathcal{S} \subseteq \mathcal{X}$ of secret states. Note that we allow the set \mathcal{S} to be any subset of the set \mathcal{X} of global states without any restrictions.

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, the opacity verification problem is to verify whether the global DES $\mathcal{G} = \parallel_{i \in \{1, \dots, n\}} G_i$ is opaque (CSO, ISO) w.r.t. the secret set \mathcal{S} .

Opacity verification for modular systems is decidable but costly [10]. The monolithic approach 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. Therefore, in this work, we consider *local opacity verification*: to verify the global DES based only on the observer automata of local DESs. We propose sufficient conditions for local opacity verification in Sections IV and corresponding efficient approaches in Section V.

IV. LOCAL OPACITY VERIFICATION

A. Shared Events

As depicted in Fig. 1, we assume that the intruder can observe events shared between local DESs. This assumption is common for DESs with modular structure [14], [18].

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 $(\Sigma_i \setminus \bigcup_{j \neq i} \Sigma_j) \cap \Sigma_{obs} = \emptyset$.

Then, we present Lemma 4, which will be used for our results in the next sections. The intuition of this lemma is that an event sequence α'_i of a local DES G_i can be projected to a sequence of the global DES \mathcal{G} (not blocked by the parallel composition) if there exists at least one sequence α of \mathcal{G} with $\pi_{obs} \circ \pi_i(\alpha) = \pi_{obs}(\alpha'_i)$.

Lemma 4: Let $\mathcal{S} \subseteq \mathcal{X}$ be a set of global secret states. We assume that Assumption 1 holds and there exists $(x, \alpha) \in \mathcal{X}_{in} \times \Sigma_{\mathcal{G}}^*$ where $\Delta^*(x, \alpha)!$, and consider any $i \in \{1, \dots, n\}$. For all $(x'_i, \alpha'_i) \in X_{in,i} \times \Sigma_i^*$ satisfying

$$\delta_i^*(x'_i, \alpha'_i)! \text{ and } \pi_{obs}(\alpha'_i) = \pi_{obs} \circ \pi_i(\alpha), \quad (5)$$

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

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

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

Proof: As the parallel composition operation is commutative and associative, we assume without loss of generality that $i = 1$ and $\mathcal{G} = G_1 \parallel \mathcal{G}_J$, where $\mathcal{G}_J = \parallel_{k \in \{2, \dots, n\}} G_k$. Let $x_J = (x[2], \dots, x[n])$. We consider any $(x'_1, \alpha'_1) \in X_{in,1} \times \Sigma_1^*$ satisfying (5), and will prove the lemma by induction on the length of α .

For the base step, let $\alpha = \varepsilon$ and $\alpha' = \alpha'_1$. By (5), we have $\pi_{obs}(\alpha') = \pi_{obs} \circ \pi_1(\alpha) = \varepsilon = \pi_{obs}(\alpha)$. By Assumption 1, $\alpha'_1 \in (\Sigma_1 \setminus \bigcup_{k \in \{1, \dots, n\}} \Sigma_k)^*$ and $(s_2, \dots, s_n) = x_J$. By Lemma 1, $\Delta^*(x'_1, x_J, \alpha'_1) = (\delta_1^*(x'_1, \alpha'_1), x_J)$, and (6) holds.

Induction hypothesis (I.H.): if $|\alpha| < k$, there exists $\alpha' \in \Sigma_{\mathcal{G}}^*$ that satisfies $\pi_{obs}(\alpha') = \pi_{obs}(\alpha)$ and (6).

For the inductive step, let $\alpha = \beta\sigma$, where $\sigma \in \Sigma_{\mathcal{G}}$ and $|\beta| < k$. Notice that, since $\Delta^*(x, \alpha)!$, we have $\delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))!$ by Lemma 1, and $\Delta^*(x, \beta)!$ and $\Delta(\Delta^*(x, \beta), \sigma)!$ by (2). 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 I.H., there exists $\beta' \in \Sigma_{\mathcal{G}}^*$ such that $\pi_{obs}(\beta') = \pi_{obs}(\beta)$ and

$$\Delta^*(x'_1, x_J, \beta') = (\delta_1^*(x'_1, \alpha'_1), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta))) \quad (7)$$

By setting $\alpha' = \beta'\sigma$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\beta'\sigma) = \pi_{obs}(\beta\sigma) = \pi_{obs}(\alpha)$. As $\sigma \notin \Sigma_1$, by (1c), (2), and (7),

$$\begin{aligned} \Delta^*(x'_1, x_J, \alpha') &= \Delta^*(x'_1, x_J, \beta'\sigma) \\ &= (\delta_1^*(x'_1, \alpha'_1), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta\sigma))) \\ &= (\delta_1^*(x'_1, \alpha'_1), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))). \end{aligned}$$

Thereby, (6) holds in this case.

- Case 2: $\sigma \in \Sigma_1 \cap \Sigma_{\mathcal{G}_J}$. By Assumption 1, $\pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)\sigma$. By (5), there exists $\beta'_1 \in \Sigma_1^*$ such that $\beta'_1\sigma = \alpha'_1$ and $\pi_{obs}(\beta'_1)\sigma = \pi_{obs}(\alpha'_1) = \pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)\sigma$. Thus, we have $\pi_{obs}(\beta'_1) = \pi_{obs} \circ \pi_1(\beta)$. By I.H., there exists β' with $\pi_{obs}(\beta') = \pi_{obs}(\beta)$ and

$$\Delta^*(x'_1, x_J, \beta') = (\delta_1^*(x'_1, \beta'_1), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta))). \quad (8)$$

By setting $\alpha' = \beta'\sigma$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\beta')\sigma = \pi_{obs}(\beta)\sigma = \pi_{obs}(\alpha)$. Then, by (1a), (2), and (8),

$$\begin{aligned} \Delta^*(x'_1, x_J, \alpha') &= \Delta^*(x'_1, x_J, \beta'\sigma) \\ &= (\delta_1^*(x'_1, \beta'_1\sigma), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta\sigma))) \\ &= (\delta_1^*(x'_1, \alpha'_1), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))). \end{aligned}$$

Thereby, (6) holds in this case.

- Case 3: $\sigma \in (\Sigma_1 \setminus \Sigma_{\mathcal{G}_J}) \cap \Sigma_{obs}$. As $\sigma \in \Sigma_1 \cap \Sigma_{obs}$, $\pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)\sigma$. 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 $\pi_{obs}(\beta') = \pi_{obs}(\beta)$. By setting $\alpha' = \beta'\sigma$, we have $\pi_{obs}(\alpha') = \pi_{obs}(\beta')\sigma = \pi_{obs}(\beta)\sigma = \pi_{obs}(\alpha)$. Moreover, we have $\pi_{\mathcal{G}_J}(\alpha) = \pi_{\mathcal{G}_J}(\beta)$ as $\sigma \notin \Sigma_{\mathcal{G}_J}$. By (1b), (2), and (8),

$$\begin{aligned} \Delta^*(x'_1, x_J, \alpha') &= \Delta^*(x'_1, x_J, \beta'\sigma) \\ &= (\delta_1^*(x'_1, \beta'_1\sigma), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\beta))) \\ &= (\delta_1^*(x'_1, \alpha'_1), \delta_{\mathcal{G}_J}^*(x_J, \pi_{\mathcal{G}_J}(\alpha))). \end{aligned}$$

Thereby, (6) holds in this case.

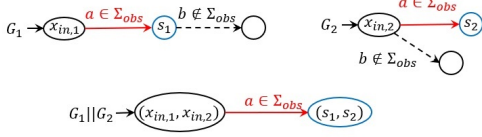


Fig. 2. Two local DESs and the accessible part of their parallel composition. The DES G_1 is CSO w.r.t $\{s_1\}$, but $G_1 \parallel G_2$ is not CSO w.r.t. $\{(s_1, s_2)\}$.

- Case 4: $\sigma \in \Sigma_1 \setminus (\Sigma_{G_J} \cup \Sigma_{obs})$. Since $\pi_{obs}(\sigma) = \varepsilon$, $\pi_{obs} \circ \pi_1(\sigma) = \varepsilon$. By (5), $\pi_{obs}(\alpha'_1) = \pi_{obs} \circ \pi_1(\alpha) = \pi_{obs} \circ \pi_1(\beta)$. By the I.H., there exists β' satisfying (7) and $\pi_{obs}(\beta') = \pi_{obs}(\beta)$. 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 $\pi_{obs}(\alpha') = \pi_{obs}(\alpha)$. Since $\sigma \in \Sigma_1 \setminus \Sigma_{G_J}$, $\delta_{G_J}^*(x_J, \pi_{G_J}(\beta\sigma)) = \delta_{G_J}^*(x_J, \pi_{G_J}(\beta))$. Then, by (1b), (7), and (2),

$$\begin{aligned} \Delta^*(x'_1, x_J, \alpha') &= \Delta^*(x'_1, x_J, \beta') \\ &= (\delta_1^*(x'_1, \alpha'_1), \delta_{G_J}^*(x_J, \pi_{G_J}(\beta))) \\ &= (\delta_1^*(x'_1, \alpha'_1), \delta_{G_J}^*(x_J, \pi_{G_J}(\alpha))). \end{aligned}$$

Thereby, (6) holds in this case.

As we have $\alpha' \in \Sigma_{\mathcal{G}}^*$ that satisfies $\pi_{obs}(\alpha') = \pi_{obs}(\alpha)$ and (6) 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 $i \in \{1, \dots, n\}$ 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

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

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

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

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

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.

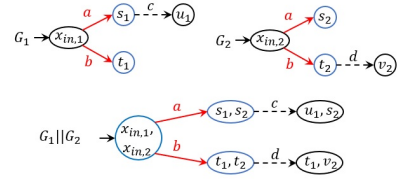


Fig. 3. Two local DESs and the accessible part of their parallel composition. $\Sigma_{obs} = \{a, b\}$. The DESs G_1 and G_2 are not CSO w.r.t. $\{s_1, t_1\}$ and $\{s_2, t_2\}$, respectively, but their composition $G_1 \parallel G_2$ is CSO w.r.t. $\{(s_1, s_2), (s_1, t_2), (t_1, s_2), (t_1, t_2)\}$.

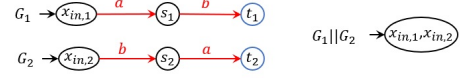


Fig. 4. Two local DESs and the accessible part of their parallel composition. All events are observable. The DESs G_1 and G_2 are not CSO w.r.t. $\{t_1\}$ and $\{t_2\}$, respectively, but $G_1 \parallel G_2$ is CSO w.r.t. $\{(t_1, t_2)\}$.

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 $\mathcal{S} = \mathcal{S}[i] \times \dots \times \mathcal{S}[n]$. 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.

Theorem 1 provides a sufficient condition for the opacity of the global DES. However, if there is no local DES G_i that is CSO w.r.t. $\mathcal{S}[i]$, \mathcal{G} can still be CSO w.r.t. \mathcal{S} . Using Lemma 2, we propose another sufficient condition for the CSO of \mathcal{G} by considering subsets of secret states.

Theorem 2: We assume Assumption 1. Consider a set of secret global states $\mathcal{S} = \mathcal{S}_1 \cup \dots \cup \mathcal{S}_m \subseteq \mathcal{X}$. 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 $j \in \{1, \dots, m\}$. Then, \mathcal{G} is CSO w.r.t. \mathcal{S} if for all $j \in \{1, \dots, m\}$, there exists $i \in \{1, \dots, n\}$ such that the following condition holds.

$$\begin{aligned} \forall (x_i, \alpha_i) \in X_{i,in} \times \Sigma_i^*, \delta_i^*(x_i, \alpha_i) \in \mathcal{S}_j[i], \\ \exists (x'_i, \alpha'_i) \in X_{i,in} \times \Sigma_i^*, \delta_i^*(x'_i, \alpha'_i) \in X_i \setminus \mathcal{S}[i] \\ \text{and } \pi_{obs}(\alpha'_i) = \pi_{obs}(\alpha_i). \end{aligned} \quad (9)$$

Proof: Let us consider a secret subset \mathcal{S}_j and let G_i be the local DES that satisfy (9). Consider any

$$(x, \alpha) \in \mathcal{X}_{in} \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha) = s \in \mathcal{S}_j. \quad (10)$$

By Lemma 1, $\delta_i^*(x[i], \pi_i(\alpha)) = s[i] \in \mathcal{S}_j[i]$. By (9), there exists $(x'_i, \alpha'_i) \in X_{i,in} \times \Sigma_i^*$ 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

$$\begin{aligned} \Delta^*(x[1], \dots, x[i-1], \delta_i^*(x'_i, \alpha'_i), x[i+1], \dots, x[n], \alpha') \\ \in \mathcal{X} \setminus \mathcal{S}. \end{aligned} \quad (11)$$

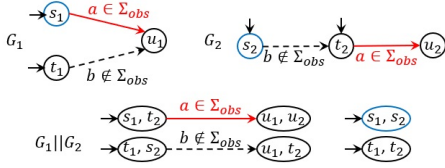


Fig. 5. Two local DESs and the accessible part of their parallel composition. Initial states of G_1 (resp. G_2) are s_1 and t_1 (resp. s_2 and t_2). The DES G_2 is ISO w.r.t. $\{s_2\}$, but $G_1 \parallel G_2$ is not ISO w.r.t. $\{(s_1, s_2)\}$.

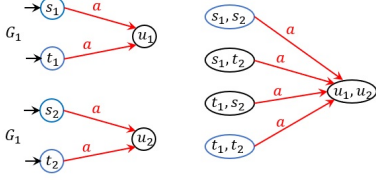


Fig. 6. Two local DESs and the accessible part of their parallel composition. Initial states of G_1 (resp. G_2) are s_1 and t_1 (resp. s_2 and t_2). The event a is observable. The DESs G_1 and G_2 are both not ISO w.r.t. $\{s_1, t_1\}$ and $\{s_2, t_2\}$, respectively, but $G_1 \parallel G_2$ is ISO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

By Lemma 2, (10) and (11), the global DES \mathcal{G} is CSO w.r.t. $\mathcal{S} = \bigcup_{j \in \{1, \dots, m\}} \mathcal{S}_j$ 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

We show that our results for CSO also hold for ISO.

Theorem 3: We assume Assumption 1. Given a secret subset $\mathcal{S} \subseteq \mathcal{X}_{in}$ of global initial states, if there exists $i \in \{1, \dots, n\}$ 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 G_i is ISO w.r.t. $\mathcal{S}[i]$. Consider any

$$(x, \alpha) \in \mathcal{S} \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha)!. \quad (12)$$

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

$$\Delta^*(x', \alpha')! \text{ and } \pi_{obs}(\alpha) = \pi_{obs}(\alpha'). \quad (13)$$

Notice that $x' \in \mathcal{X} \setminus \mathcal{S}$ because $x'_i \in X_i \setminus \mathcal{S}[i]$. Therefore, the lemma holds by (12), (13), and Definition 3. ■

Remark 3: Assumption 1 is a necessary condition for Theorem 3. In 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. $\mathcal{S}[i]$. 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. $\{(s_1, s_2), (t_1, t_2)\}$.

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 $\mathcal{S}_1, \dots, \mathcal{S}_m \in \mathcal{S}$ where $\mathcal{S} = \mathcal{S}_1 \cup \dots \cup \mathcal{S}_m$.

Theorem 4: We assume Assumption 1. Consider a set of secret global initial states $\mathcal{S} = \mathcal{S}_1 \cup \dots \cup \mathcal{S}_m \subseteq \mathcal{X}_{in}$. 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 $j \in \{1, \dots, m\}$. Then, \mathcal{G} is ISO w.r.t. \mathcal{S} if for all $j \in \{1, \dots, m\}$, there exist $i \in \{1, \dots, n\}$ satisfying the following condition.

$$\begin{aligned} \forall (x_i, \alpha_i) \in \mathcal{S}_j[i] \times \Sigma_i^*, \delta_i(x_i, \alpha_i)!, \\ \exists (x'_i, \alpha'_i) \in (X_i \setminus \mathcal{S}[i]) \times \Sigma_i^*, \delta_i(x'_i, \alpha'_i)! \\ \text{and } \pi_{obs}(\alpha'_i) = \pi_{obs}(\alpha_i). \end{aligned} \quad (14)$$

Proof: Consider any secret subset \mathcal{S}_j and let G_i be the local DES that satisfy (14). Consider any

$$(x, \alpha) \in \mathcal{S}_j \times \Sigma_{\mathcal{G}}^* \text{ such that } \Delta^*(x, \alpha)! \quad (15)$$

By Lemma 1, $\delta_i^*(x[i], \pi_i(\alpha))!$ and $x[i] \in \mathcal{S}_j[i]$. By (14), 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 $x' = x[1], \dots, x[i-1], x'_i, x[i+1], \dots, x[n]$. By Lemma 4, there exists α' such that

$$\Delta^*(x', \alpha')! \text{ and } \pi_{obs}(\alpha) = \pi_{obs}(\alpha'). \quad (16)$$

Notice that $x' \in \mathcal{X} \setminus \mathcal{S}$ because $x'_i \in X_i \setminus \mathcal{S}[i]$. By Lemma 3, (15) and (16), \mathcal{G} is ISO w.r.t. $\mathcal{S} = \bigcup_{j \in \{1, \dots, m\}} \mathcal{S}_j$. ■

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

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 , $i \in \{1, \dots, n\}$. Hence, we can use Theorems 1 and 3 to verify each local DES using existing opacity verification algorithms (e.g. [19], [20], [21], [22]). 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 [17] 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 $Agent1 \parallel Agent2 \parallel Resource$ of the DESs in Fig. 7. Suppose that $(1wait, 2use, 2)$ is the only secret state. By considering the observer automaton in Fig. 8 (a), we know that $Agent1$ is CSO (resp. ISO) w.r.t. $\{1wait\}$. By Theorem 1, the global DES is also CSO (resp. ISO) w.r.t. $\{(1wait, 2use, 2)\}$.

As discussed in Remarks 2 and 4, Theorems 1 and 3 provide only sufficient conditions for the opacity of the global DES \mathcal{G} . Let us consider the DESs in Fig. 7 and $\mathcal{S} = \{(1wait, 2use, 2), (1use, 2wait, 1), (1end, 2end, free)\}$. For this case, we cannot verify the global DES by verifying local DESs w.r.t. their corresponding local secret sets, e.g., $Agent1$ is not opaque w.r.t. $\{1wait, 1use, 1end\}$. However, 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 $s \in \mathcal{S}$.

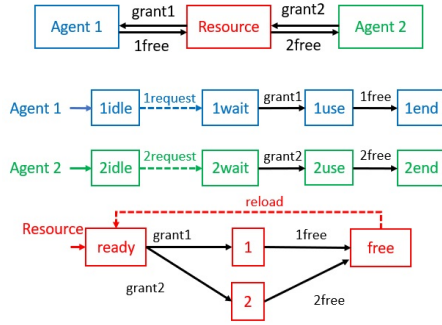


Fig. 7. Two agents sharing one resource. The events “1request”, “2request”, and “reload” are not observable by the intruder.

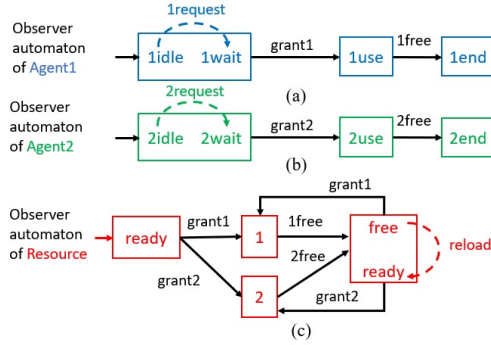


Fig. 8. Intruder's CSO observer automata for local DESs in Fig. 7.

Let $S_1 = \{(1wait, 2use, 2)\}$, $S_2 = \{(1use, 2wait, 1)\}$, and $S_3 = \{(1end, 2end, free)\}$. Let G_1 , G_2 , and G_3 be *Agent1*, *Agent2*, and *Resource*, respectively. Using the observer automata in Fig. 8, we have the following properties.

- 1) $S_1[1] = \{1wait\}$. For the event sequence $1request$ with $\delta_1(1idle, 1request) = 1wait \in S_1[1]$, we have $\delta_1(1idle, \varepsilon) = 1idle \notin S[1] = \{1wait, 1use, 1end\}$ and $\pi_{obs}(1request) = \pi_{obs}(\varepsilon) = \varepsilon$.
- 2) $S_2[2] = \{2wait\}$. For the event sequence $2request$ with $\delta_2(2idle, 2request) = 2wait \in S_2[2]$, we have $\delta_2(2idle, \varepsilon) = 2idle \notin S[2] = \{2wait, 2use, 2end\}$ and $\pi_{obs}(2request) = \pi_{obs}(\varepsilon) = \varepsilon$.
- 3) $S_3[3] = \{free\}$. For all $\alpha \in \Sigma_3^*$ such that $\delta_3(ready, \alpha) = free \in S_3[3]$, we have $\alpha' = \alpha reload$ where $\delta_3(ready, \alpha') = ready \notin S[3] = \{1, 2, free\}$ and $\pi_{obs}(\alpha) = \pi_{obs}(\alpha')$.

By Theorem 2, the global DES is CSO w.r.t S . We can use Theorem 4 to verify that the global DES is also ISO w.r.t S in the same way. Thus, for this example, we can verify the global DES using the observer automata of the local DESs.

VI. CONCLUSIONS

We studied current-state opacity (CSO) and 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 conditions, we introduced efficient methodologies to verify the global DES's opacity using observer automata of the local DESs. 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] 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.
- [5] 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.
- [6] 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.
- [7] 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.
- [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] 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.
- [10] T. Masopust and X. Yin, “Complexity of detectability, opacity and a-diagnosability for modular discrete event systems,” *Automatica*, vol. 101, pp. 290–295, 2019.
- [11] S. Mohajerani, Y. Ji, and S. Lafortune, “Compositional and abstraction-based approach for synthesis of edit functions for opacity enforcement,” *IEEE Transactions on Automatic Control*, vol. 65, no. 8, pp. 3349–3364, 2019.
- [12] M. Noori-Hosseini, B. Lennartson, and C. Hadjicostis, “Compositional visible bisimulation abstraction applied to opacity verification,” *IFAC-PapersOnLine*, vol. 51, no. 7, pp. 434–441, 2018.
- [13] S. Mohajerani and S. Lafortune, “Transforming opacity verification to nonblocking verification in modular systems,” *IEEE Transactions on Automatic Control*, vol. 65, no. 4, pp. 1739–1746, 2019.
- [14] 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.
- [15] 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.
- [16] G. Zinck, L. Ricker, H. Marchand, and L. Hérouët, “Enforcing opacity in modular systems,” in *Ifac world Congress*, 2020.
- [17] C. G. Cassandras and S. Lafortune, *Introduction to discrete event systems*. Springer Science & Business Media, 2009.
- [18] 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.
- [19] 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.
- [20] J. Dubreil, P. Darondeau, and H. Marchand, “Supervisory control for opacity,” *IEEE Transactions on Automatic Control*, vol. 55, no. 5, pp. 1089–1100, 2010.
- [21] A. Saboori and C. N. Hadjicostis, “Opacity-enforcing supervisory strategies via state estimator constructions,” *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1155–1165, 2011.
- [22] X. Yin and S. Lafortune, “A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems,” *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2140–2154, 2015.