

# Opacity Enforcing Supervisory Control using Non-deterministic Supervisors

Yifan Xie, *Student Member, IEEE*, Xiang Yin, *Member, IEEE*, Shaoyuan Li, *Senior Member, IEEE*

**Abstract**—In this paper, we investigate the enforcement of opacity via supervisory control in the context of discrete-event systems. A system is said to be opaque if the intruder, which is modeled as a passive observer, can never infer confidentially that the system is at a secret state. The design objective is to synthesize a supervisor such that the closed-loop system is opaque even when the control policy is publicly known. In this paper, we propose a new approach for enforcing opacity using *non-deterministic supervisors*. A non-deterministic supervisor is a decision mechanism that provides a set of control decisions at each instant, and randomly picks a specific control decision from the decision set to actually control the plant. Compared with the standard deterministic control mechanism, such a non-deterministic control mechanism can enhance the plausible deniability of the controlled system as the online control decision is a random realization and cannot be implicitly inferred from the control policy. We provide a sound and complete algorithm for synthesizing a non-deterministic opacity-enforcing supervisor. Furthermore, we show that non-deterministic supervisors are strictly more powerful than deterministic supervisors in the sense that there may exist a non-deterministic opacity-enforcing supervisor even when deterministic supervisors cannot enforce opacity.

**Index Terms**—Opacity, Supervisory Control, Discrete Event Systems.

## I. INTRODUCTION

INFORMATION security and privacy have been becoming increasingly important issues in the analysis and design of modern engineering systems due to potential malicious attacks and information leakages in networks. In this paper, we investigate an important information-flow security property called *opacity* in the context of Discrete-Event Systems (DES). In the framework, a dynamic system is modeled as a DES and an intruder is modeled as a passive observer that monitors the behavior of the dynamic system via observable events. A system is said to be opaque if the intruder can never know for sure that the system is visiting a secret state. Essentially, opacity is a confidential property capturing whether or not the system can always *plausibly deny* the execution of a secret behavior even when it may be true.

Due to the increasing demands for security certification in safety-critical systems, the notion of opacity has drawn considerable attention in the past years in the literature; see,

e.g., [2], [5], [28]. In particular, in the context of DES, different notions of opacity have been studied, including, e.g., current-state opacity [24], initial-state opacity [35],  $K$ -step and infinite-step opacity [47]. The verification of opacity has also been studied for different DES models including Petri nets [23], [33], [39], stochastic DES [8], [19], [43], [48], real-time systems [41] and networked DES [25], [45]. More recently, the notion of opacity has been extended to linear/nonlinear systems with infinite-states and continuous dynamics [1], [32], [49]. Compositional approaches have also been applied for the verification and synthesis of opacity for large-scale systems [27], [29]–[31]. The reader is referred to the comprehensive surveys [17], [22] and the textbook [15] for recent advances on this active research area.

Given an open-loop system that is verified to be non-opaque, one important problem is to *enforce* opacity via some enforcement mechanisms. This is also referred to as the *synthesis problem*, which is a very active research topic in the literature and many different enforcement mechanisms have been proposed. For example, [4], [7], [50] consider the enforcement of opacity via dynamic masks that change the output information dynamically. The idea of changing the output information has also been leveraged by using insertion functions [18], [20], [26], [42] and event shuffles [3]. In addition, event delays is also used to enforce opacity in [12].

One of the most widely investigated opacity enforcement mechanism is via the *supervisory control theory*. In this framework, a supervisor is used to restrict the behavior of the system such that the closed-loop system is opaque [9], [34], [52]. For example, in [38] a formula for controllable and opaque sublanguage is provided. In [10], the authors solve the opacity control problem by assuming that all controllable events are observable and the observation of the intruder is included in the observation of the supervisor. In [46], a uniform approach is provided to solve the opacity-enforcing control problem without the assumption that controllable events are observable; however, it assumes that the observations of the supervisor and the intruder are equivalent. Recently in [40], the authors provide an algorithm for synthesizing an opacity enforcing supervisor without any assumption on event sets. However, it needs to assume that the control policy is not publicly known, which reduces the problem to the computation a maximal controllable and observable sublanguage of the supremal opaque sublanguage.

Note that all existing works on opacity-enforcing supervisory control considers deterministic supervisors, which issue a specific control decision at each instant. However, such a deterministic decision mechanism may decrease the plausible

This work was supported by the National Natural Science Foundation of China (61803259, 61833012) and by Shanghai Jiao Tong University Scientific and Technological Innovation Funds.

Yifan Xie, Xiang Yin and Shaoyuan Li are with Department of Automation and Key Laboratory of System Control and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China. {xyfan1234, yinxiang, syli}@sjtu.edu.cn. (Corresponding Author: Xiang Yin)

deniability of the system. This is because, by knowing the control policy and by observing the occurrences of observable events, the intruder can recover the control decision made by the supervisor and, therefore, obtain a better state-estimate of the system.

In this paper, we propose to use *non-deterministic supervisors*, for the first time, to enforce opacity. Unlike a deterministic supervisor that issues a specific control decision at each instant, a non-deterministic supervisor provides a *set of control decisions* at each instant and the specific control decision applied is chosen randomly via a “coin toss” manner. In other words, even if the intruder knows the control policy, it still does not know the specific control decision applied as it is decided randomly on-the-fly. Compared with the deterministic control mechanism, the non-deterministic control mechanism can significantly enhance the plausible deniability of the system, and, therefore, is more likely to enforce opacity.

The main contribution of this paper is that we provide an algorithmic correct-by-construction procedure for synthesizing a non-deterministic supervisor that enforces opacity. This problem is fundamentally more challenging than the deterministic case as the observation of the supervisor and the intruder are *incomparable*. Specifically, although the specific control decision applied is unknown *a priori*, the supervisor will know this online choice after it is chosen. This information, however, is not available to the intruder. Hence, the supervisor’s knowledge is strictly more than that of the intruder. In the standard opacity-enforcing control problem, it is sufficient to know the state-estimate of the system, which is not sufficient in our setting due to the issue of incomparable information. To address this issue, we propose a new information-state that not only contains the state-estimate from the supervisor’s point of view, but also contains the estimate of the supervisor’s estimate from the intruder’s point of view. In other words, the control decision should be made not only based on what the supervisor thinks about the plant, but also based on what the intruder thinks about the supervisor. Based on the proposed new information-state, we provide a sound and complete approach that synthesizes a non-deterministic supervisor enforcing opacity. In particular, we show that using non-deterministic supervisors is strictly more powerful than using deterministic supervisors, in the sense that, there may exist a non-deterministic opacity-enforcing supervisor even when deterministic supervisors cannot enforce opacity.

We note that the notion of non-deterministic supervisors was originally proposed in [16] to solve the standard supervisory control problem for safety and non-blockingness under partial observation. This approach was extended by [21]. Non-deterministic control mechanism has also been used for (bi)similarity enforcing supervisory control problems with non-deterministic models and specifications [11], [13], [36], [37], [51]. However, to the best of our knowledge, non-deterministic supervisors have never been applied to the opacity-enforcement problem. More importantly, the essence why we use non-deterministic supervisors here is to enhance the plausible deniability of the system, which is fundamentally different from the essence of the existing works.

The rest of this paper is organized as follows. In Section II,

we introduce some necessary preliminaries. In Section III, we first provide a motivating example to illustrate the advantage of non-deterministic supervisors. Then we formally present the non-deterministic control mechanism and formulate the corresponding opacity enforcement control problem. In Section IV, we propose a new type of information state (IS) that captures both the knowledge of the supervisor and the knowledge of the intruder and analyze the underlying information-flow. Then we restrict our attention to the class of information-state-based supervisors and discuss how an IS-based supervisor can be encoded as or be decoded from an IS-mapping. In Section V, we propose an algorithm to synthesize an IS-based non-deterministic opacity-enforcing supervisor based on the structure of the generalized bipartite transition system. In Section VI, we prove the correctness of the synthesis procedure proposed in Section V by showing that restricting our attention to IS-based supervisors is without loss of generality. Finally, we conclude the paper in Section VII. Preliminary and partial versions of some of the results in this paper are presented in [44]. First, all definitions, notations and theorems in [44] have been reformulated in a more uniform manner. More importantly, the result in [44] is only sound as it restricts the solution space to a finite space a priori. In this work, we show that restricting to IS-based supervisor is without loss of generality using new techniques developed based on IS-mappings. This new result establishes both the soundness and the completeness of the synthesis algorithm, i.e., the non-deterministic synthesis problem is completely solved.

## II. PRELIMINARIES

### A. System Model

Let  $\Sigma$  be a finite set of events. A string over  $\Sigma$  is a finite sequence  $s = \sigma_1 \cdots \sigma_n, \sigma_i \in \Sigma$ . We denote by  $\Sigma^*$  the set of all strings over  $\Sigma$  including the empty string  $\epsilon$ . A language  $L \subseteq \Sigma^*$  is a set of strings. For two languages  $L_1$  and  $L_2$ , their concatenation is  $L_1 L_2 = \{s_1 s_2 \in \Sigma^* : s_1 \in L_1, s_2 \in L_2\}$ . The prefix-closure of language  $L$  is define a  $\bar{L} = \{v \in \Sigma^* : \exists u \in \Sigma^* \text{ s.t. } vu \in L\}$ .

We assume basic knowledge of DES and use common notations; see, e.g., [6]. A DES is modeled as a deterministic finite-state automaton

$$G = (X, \Sigma, \delta, x_0),$$

where  $X$  is the finite set of states,  $\Sigma$  is the finite set of events,  $\delta : X \times \Sigma \rightarrow X$  is the partial transition function, where  $\delta(x, \sigma) = y$  means that there is a transition labeled by event  $\sigma$  from state  $x$  to  $y$ , and  $x_0 \in X$  is the initial state. The transition function is also be extended to  $\delta : X \times \Sigma^* \rightarrow X$  in the usual manner [6]. For simplicity, we write  $\delta(x, s)$  as  $\delta(s)$  when  $x = x_0$ . The language generated by  $G$  is defined by  $\mathcal{L}(G) := \{s \in \Sigma^* : \delta(x_0, s)!\}$ , where  $!$  means “is defined”.

When the system is partially observed,  $\Sigma$  is partitioned into two disjoint sets:  $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ , where  $\Sigma_o$  is the set of observable events and  $\Sigma_{uo}$  is the set of unobservable events. The natural projection  $P : \Sigma^* \rightarrow \Sigma_o^*$  is defined by

$$P(\epsilon) = \epsilon \text{ and } P(s\sigma) = \begin{cases} P(s)\sigma & \text{if } \sigma \in \Sigma_o \\ P(s) & \text{if } \sigma \in \Sigma_{uo} \end{cases}$$

The natural projection is also extended to  $P : 2^{\Sigma^*} \rightarrow 2^{\Sigma_o^*}$  by  $P(L) = \{P(s) : s \in L\}$ .

### B. Deterministic Supervisory Control

In the framework of supervisory control, a supervisor dynamically enables/disables controllable events based on its observation. Formally, we assume that the events set is further partitioned as  $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc}$ , where  $\Sigma_c$  is the set of controllable events and  $\Sigma_{uc}$  is the set of uncontrollable events. A control decision  $\gamma \in 2^\Sigma$  is a set of events such that  $\Sigma_{uc} \subseteq \gamma$ , i.e., uncontrollable events can never be disabled. We define  $\Gamma = \{\gamma \in 2^\Sigma : \Sigma_{uc} \subseteq \gamma\}$  as the set of control decisions or control patterns. A *deterministic supervisor* is a function  $S : P(\mathcal{L}(G)) \rightarrow \Gamma$ . The language generated by the controlled system, denoted by  $\mathcal{L}(S/G)$ , is defined recursively by

- $\epsilon \in \mathcal{L}(S/G)$ ; and
- For any  $s \in \Sigma^*$ ,  $\sigma \in \Sigma$ , we have  $s\sigma \in \mathcal{L}(S/G)$  iff  $s\sigma \in \mathcal{L}(G)$ ,  $s \in \mathcal{L}(S/G)$  and  $\sigma \in S(P(s))$ .

### C. Opacity

We assume that system  $G$  has a “secret”, which is modeled as a set of secret states  $X_S \subseteq X$ . Furthermore, we consider a passive *intruder* having the following capabilities:

- A1 The intruder knows the system model;
- A2 The intruder can observe the occurrences of observable events.

Such an intruder is essentially an outside observer or an “eavesdropper”. We say that system  $G$  is *opaque* w.r.t.  $X_S$  and  $\Sigma_o$  if

$$(\forall s \in \mathcal{L}(G) : \delta(s) \in X_S) (\exists t \in \mathcal{L}(G) : \delta(t) \notin X_S [P(s) = P(t)]).$$

That is, the intruder cannot infer for sure that the system is in a secret state based on the information flow.

When the original system is not opaque, one approach is to design a supervisor  $S$  such that the closed-loop system  $S/G$  is opaque; this is referred to as the *opacity-enforcing control problem*. In this setting, however, the implementation of such a supervisor may become a public information. To capture this severe scenario, we assume:

- A3 The intruder knows the functionality of the supervisor, i.e., the control policy.

Note that this knowledge together with the assumption that the intruder and the observer both observe  $\Sigma_o$  imply that the intruder knows precisely the control decision applied at each instant. Therefore, to define opacity of the controlled system, we should only consider strings in  $\mathcal{L}(S/G)$  rather than all strings in  $\mathcal{L}(G)$ . Formally, we say that a deterministic supervisor  $S : P(\mathcal{L}(G)) \rightarrow \Gamma$  enforces opacity on  $G$ , or the closed-loop system  $S/G$  is opaque, if for any string  $s \in \mathcal{L}(S/G)$  such that  $\delta(s) \in X_S$ , there exists a string  $t \in \mathcal{L}(S/G)$  such that  $\delta(t) \notin X_S$  and  $P(s) = P(t)$ .

Finally, we introduce some operators that will be used in this paper. Given a set of states  $m \in 2^X$ , we denote by  $UR_\gamma(m)$  the *unobservable reach* of  $m$  under control decision  $\gamma \in \Gamma$ , i.e.,

$$UR_\gamma(m) = \{\delta(x, w) \in X : x \in m, w \in (\Sigma_{uc} \cap \gamma)^*\}. \quad (1)$$

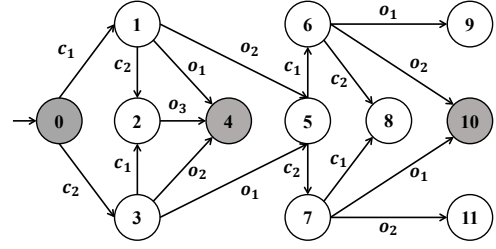


Fig. 1. System  $G$  with  $\Sigma_c = \{c_1, c_2\}$ ,  $\Sigma_o = \{o_1, o_2, o_3\}$  and  $X_S = \{0, 4, 10\}$ .

We also denote by  $NX_\sigma(m)$  the *observable reach* of  $m$  upon the occurrence of an observable event  $\sigma \in \Sigma_o$ , i.e.,

$$NX_\sigma(m) = \{\delta(x, \sigma) \in X : x \in m\}. \quad (2)$$

## III. ENFORCING OPACITY USING NON-DETERMINISTIC SUPERVISORS

In this section, we propose to use non-deterministic supervisors to enforce opacity. First, we illustrate the advantage of using non-deterministic supervisors by a motivating example. Then we formally define the functionality of the non-deterministic supervisor and opacity of non-deterministic control systems. We formulate the corresponding opacity-enforcing supervisory control problem that we want to solve in this paper.

### A. Motivating Example

**Example 1.** Let us consider system  $G$  shown in Fig. 1 with  $\Sigma_o = \Sigma_{uc} = \{o_1, o_2, o_3\}$  and  $X_S = \{0, 4, 10\}$ . String  $c_2 o_1 c_2 o_1$  leads to secret state 10 and its observation is  $P(c_2 o_1 c_2 o_1) = o_1 o_1$ . By observing  $o_1 o_1$ , the intruder cannot infer for sure that the system is in state 10 since  $P(c_2 o_1 c_1 o_1) = o_1 o_1$  and  $\delta(c_2 o_1 c_1 o_1) = 9 \notin X_S$ . However, by observing  $o_3$ , the intruder knows for sure that the system is at secret state 4 since for any string  $s$  such that  $P(s) = o_3$ , we have  $\delta(s) = 4 \in X_S$ . Therefore, the system is not opaque and we need to synthesize a supervisor to protect the system from revealing secret 4.

For this system, however, we cannot even synthesize a deterministic supervisor to enforce opacity. To see this clearly, let us evaluate what the supervisor can do initially. We have  $\Gamma = \{\emptyset, \{c_1\}, \{c_2\}, \{c_1, c_2\}\}$ .<sup>1</sup> Clearly, the supervisor cannot choose  $\emptyset$  as the initial control decision; otherwise secret state 0 will be the only reachable state. Also, the supervisor cannot make  $\{c_1\}$  initially. This is because, under this control decision and by observing event  $o_1$ , the intruder knows for sure that the system is at state 4 which is reached via  $0 \xrightarrow{c_1} 1 \xrightarrow{o_1} 4$ . Note that transitions  $0 \xrightarrow{c_2} 3 \xrightarrow{o_1} 5$  cannot provide the plausible deniability since  $c_2$  is disabled initially. For the same reason, making  $\{c_2\}$  initially will also reveal the secret. Finally, decision  $\{c_1, c_2\}$  is also problematic initially as it makes state 2 reachable from which transition  $2 \xrightarrow{o_3} 4$  will also reveal the

<sup>1</sup>For the sake of simplicity, uncontrollable events are omitted in each control decision, i.e.,  $\emptyset$  stands for  $\{o_1, o_2, o_3\}$  in this example.

secret. Therefore, we cannot enforce opacity for this system using a deterministic supervisor.

However, one can enforce opacity using the following control mechanism. Initially, the supervisor randomly chooses to either enable  $c_1$  or enable  $c_2$ , but not enable both simultaneously. In other words, the control policy initially is a set  $\{\{c_1\}, \{c_2\}\}$  and the specific choice is made randomly on-the-fly. Therefore, upon the occurrence of  $o_1$  or  $o_2$ , the intruder does not know whether this event is from state 1 or from state 3 since it does not know whether or not the initial online control decision is  $\{c_1\}$  or  $\{c_2\}$  by just knowing the control policy  $\{\{c_1\}, \{c_2\}\}$ . On the other hand, since  $c_1$  and  $c_2$  will not be enabled simultaneously, state 2 is not reachable; hence, event  $o_3$ , which reveals the secret, will also not occur. Then after observing  $o_1$  or  $o_2$ , the supervisor can make decision  $\{c_1, c_2\}$  deterministically, which prevents the system from revealing secret state 10.

The above example shows that using non-deterministic control mechanism is more powerful than the deterministic one for the purpose of enforcing opacity. This result is intuitive as opacity is essentially a confidentiality property. Using a non-deterministic decision framework will, on the one hand, enhance the plausible deniability of the secret behavior of the system, and, on the other hand, decrease the confidentiality of the intruder's knowledge about the system. Hence, the system is more likely to be opaque under the non-deterministic mechanism.

### B. Non-deterministic Supervisor

Now, we formally define the non-deterministic supervisor and the corresponding opacity enforcement problem.

Compared with a deterministic supervisor that issues a specific control decision at each instant, a non-deterministic supervisor works as follows. At each instant, the non-deterministic supervisor provides a *set of possible control decisions*. Then it non-deterministically picks a specific control decision from this set in a “coin-toss” manner. In other words, the control policy only determines a set of allowed decisions, but the specific control decision chosen is unknown *a priori*, which is a *random realization* under the control policy. Therefore, the supervisor makes decision not only based on observable events, but also depends on the specific control decisions chosen along the trajectory.

To define the “history” of the supervisor, we introduce the notion of the *extended string* which is an alternating sequence of control decisions and events either ending up with a control decision in the form of

$$\rho = \gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n \in \Gamma(\Sigma\Gamma)^* \quad (3)$$

or ending up with an event in the form of

$$\rho = \gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \in (\Gamma\Sigma)^* \quad (4)$$

Then the set of all extended strings is  $\Gamma(\Sigma\Gamma)^* \cup (\Gamma\Sigma)^* = (\Gamma\Sigma)^*(\Gamma \cup \{\epsilon\})$ . For any extended string  $\rho \in (\Gamma\Sigma)^*(\Gamma \cup \{\epsilon\})$ , we denote by  $\rho|_\Sigma$  the projection to  $\Sigma^*$ , i.e.,  $\rho|_\Sigma = \sigma_1 \dots \sigma_n$ .

Since some events are unobservable for the supervisor and the supervisor cannot update its decision upon the occurrence

of an unobservable event, similar to the natural projection, we define a new projection mapping

$$\mathcal{O} : (\Gamma\Sigma)^*(\Gamma \cup \{\epsilon\}) \rightarrow (\Gamma\Sigma_o)^*(\Gamma \cup \{\epsilon\}) \quad (5)$$

such that, for any extended string, projection  $\mathcal{O}$  erases each unobservable event together with its successor control decision (if there exists one). Formally, for extended string  $\rho$  in the form of Equation (3), let  $1 \leq i_1 < i_2 < \dots < i_k \leq n$  be all indices such that  $\sigma_{i_j} \in \Sigma_o$ . Then we have

$$\mathcal{O}(\rho) = \gamma_0(\sigma_{i_1}\gamma_{i_1})(\sigma_{i_2}\gamma_{i_2}) \cdots (\sigma_{i_k}\gamma_{i_k}) \quad (6)$$

and for extended string  $\rho$  in the form of Equation (4), we have

$$\mathcal{O}(\rho) = \gamma_0(\sigma_{i_1}\gamma_{i_1})(\sigma_{i_2}\gamma_{i_2}) \cdots (\sigma_{i_{k-1}}\gamma_{i_{k-1}})\sigma_{i_k}. \quad (7)$$

From the supervisor's point of view, each decision is made immediately (by first providing a set of decisions and then picking one from the set) after observing an event. Therefore, the supervisor should make decision based on alternating sequences that end up with observable events. Hence, the non-deterministic supervisor is defined as a function

$$S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$$

that maps an extended string  $\rho = \gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \in (\Gamma\Sigma_o)^*$ , which is referred to a *decision history*, to a set of possible control decisions. This definition essentially says that, although the control policy is non-deterministic, the supervisor knows the *realization*, i.e., which specific decision was picked at each previous instant. This is a reasonable setting as the supervisor always knows what it actually picks. Now, we define the language generated by a non-deterministic supervisor.

**Definition 1.** Let  $S_N$  be a non-deterministic supervisor. The set of extended strings generated by the closed-loop system, denoted by  $\mathcal{L}_e(S_N/G)$ , is defined recursively by:

- $\epsilon \in \mathcal{L}_e(S_N/G)$ ;
- $\gamma_0 \in \mathcal{L}_e(S_N/G)$  if  $\gamma_0 \in S_N(\epsilon)$ ;
- For any  $\rho = \gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n \sigma_{n+1} \in (\Gamma\Sigma)^*$ , we have  $\rho \in \mathcal{L}_e(S_N/G)$ , if and only if
  - $\gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n \in \mathcal{L}_e(S_N/G)$ ; and
  - $\sigma_1 \cdots \sigma_n \sigma_{n+1} \in \mathcal{L}(G)$ ;
  - $\sigma_{n+1} \in \gamma_n$ .
- For any  $\rho = \gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n \sigma_{n+1} \gamma_{n+1} \in \Gamma(\Sigma\Gamma)^*$ , we have  $\rho \in \mathcal{L}_e(S_N/G)$ , if and only if
  - $\gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n \sigma_{n+1} \in \mathcal{L}_e(S_N/G)$ ; and
  - $\gamma_{n+1} \in \begin{cases} \{\gamma_n\} & \text{if } \sigma_{n+1} \in \Sigma_{uo} \\ S_N(\mathcal{O}(\gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n \sigma_{n+1})) & \text{if } \sigma_{n+1} \in \Sigma_o \end{cases}$

Then a string  $s \in \Sigma^*$  is said to be *generated* by  $S_N/G$  if there exists an extended string  $\rho \in \mathcal{L}_e(S_N/G)$  such that  $\rho|_\Sigma = s$ . We define  $\mathcal{L}(S_N/G) = \{s \in \Sigma^* : \rho \in \mathcal{L}_e(S_N/G) \text{ such that } \rho|_\Sigma = s\}$  as the language generated by the closed-loop system.

The intuition of the above definition is as follows. Initially, the first control decision should be included in the initial set of control decisions provided by  $S_N$ . When extended string  $\gamma_0 \sigma_1 \gamma_1 \cdots \sigma_n \gamma_n$  is executed, the next event  $\sigma_{n+1}$  should be both feasible in the plant and enabled by the control decision applied currently, i.e.,  $\gamma_n$ . Furthermore, if  $\sigma_{n+1}$

is unobservable, then the supervisor should not change the control decision, i.e.,  $\gamma_{n+1} = \gamma_n$ . On the other hand, if  $\sigma_{n+1}$  is observable, then the supervisor may choose a specific control decision from the new set of all possible control decisions provided by  $S_N$ , i.e.,  $\gamma_{n+1} \in S_N(\mathcal{O}(\gamma_0\sigma_1\gamma_1\ldots\sigma_n\gamma_n\sigma_{n+1}))$ . We denote by  $\mathcal{L}_e^o(S_N/G)$  the set of extended strings that end up with observable events including the empty string, i.e.,

$$\mathcal{L}_e^o(S_N/G) = \mathcal{L}_e(S_N/G) \cap (\{\epsilon\} \cup (\Gamma\Sigma)^*(\Gamma\Sigma_o)).$$

We also denote by  $\mathcal{L}_e^d(S_N/G)$  the set of extended strings that end up with control decisions, i.e.,

$$\mathcal{L}_e^d(S_N/G) = \mathcal{L}_e(S_N/G) \cap \Gamma(\Sigma\Gamma)^*.$$

The supervisor always issues a decision (first generates a set of control decisions and then randomly picks one) when an extended string  $\rho$  in  $\mathcal{L}_e^o(S_N/G)$  is generated. Then for any observable extended string  $\rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G))$ , we define

$$\hat{\mathcal{E}}_S(\rho) = \{\delta(\rho'|_\Sigma) \in X : \exists \rho' \in \mathcal{L}_e^o(S_N/G) \text{ s.t. } \mathcal{O}(\rho') = \rho\} \quad (8)$$

as the set of all possible states that can be reached immediately after observing the last event from the supervisor's point of view, i.e., the state estimate of the supervisor without the unobservable tail.

Once the supervisor issues the last control decision, the set of states that can be reached unobservably can be determined. Formally, for any extended string  $\rho \in \mathcal{O}(\mathcal{L}_e^d(S_N/G))$ , we define

$$\mathcal{E}_S(\rho) = \{\delta(\rho'|_\Sigma) \in X : \exists \rho' \in \mathcal{L}_e(S_N/G) \text{ s.t. } \mathcal{O}(\rho') = \rho\} \quad (9)$$

as the state-estimate of the supervisor with the unobservable tail included. These two state estimates can be computed recursively as follows [46]:

- $\hat{\mathcal{E}}_S(\epsilon) = \{x_0\}$ ;
- $\mathcal{E}_S(\rho') = UR_{\gamma}(\hat{\mathcal{E}}_S(\rho))$  for  $\rho' = \rho\gamma \in \mathcal{O}(\mathcal{L}_e^d(S_N/G))$ ;
- $\hat{\mathcal{E}}_S(\rho'') = NX_{\sigma}(\mathcal{E}_S(\rho'))$  for  $\rho'' = \rho'\sigma \in \mathcal{O}(\mathcal{L}_e^o(S_N/G))$ .

Here we use subscript “S” to emphasize that these state-estimates are from the supervisor's point of view.

**Example 2.** Still consider system  $G$  in Fig. 1 with  $\Sigma_c = \{c_1, c_2\}$  and  $\Sigma_o = \{o_1, o_2, o_3\}$ . Suppose that the initial non-deterministic decision set is  $S_N(\epsilon) = \{\gamma_1, \gamma_2, \gamma_3, \gamma_4\}$ , where  $\gamma_1 = \emptyset, \gamma_2 = \{c_1\}, \gamma_3 = \{c_2\}$  and  $\gamma_4 = \{c_1, c_2\}$ . Then we have  $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathcal{L}_e(S_N/G)$ . Suppose that the supervisor chooses  $\gamma_2$  initially. Then we have  $\gamma_2 c_1 \in \mathcal{L}_e(S_N/G)$  and since  $c_1$  is unobservable, we have  $\gamma_2 c_1 \gamma_2 \in \mathcal{L}_e(S_N/G)$ . When  $o_2$  occurs,  $\rho = \gamma_2 c_1 \gamma_2 o_2 \in \mathcal{L}_e^o(S_N/G)$  becomes the first extended string that ends up with an observable event. Then the information available to the supervisor is  $\mathcal{O}(\rho) = \gamma_2 o_2$ . The state estimate of the supervisor is  $\hat{\mathcal{E}}_S(\gamma_2 o_2) = NX_{o_2}(UR_{\gamma_2}(\hat{\mathcal{E}}(\epsilon))) = NX_{o_2}(\{0, 1\}) = \{5\}$ , i.e., the supervisor knows for sure that system is at state 5 by first choosing  $\gamma_2$  and then observing  $o_2$ .

Suppose that the supervisor then issues  $\gamma_4$  deterministically, i.e.,  $S_N(\gamma_2 o_2) = \{\gamma_4\}$  and the supervisor can only choose  $\gamma_4$ ; this yields extended string  $\rho' = \gamma_2 c_1 \gamma_2 o_2 \gamma_4 \in \mathcal{L}_e^d(S_N/G)$

With the last control decision information attached, the information available to the supervisor is  $\mathcal{O}(\rho') = \gamma_2 o_2 \gamma_4$ . Then the state estimate of the supervisor is  $\mathcal{E}_S(\gamma_2 o_2 \gamma_4) = UR_{\gamma_4}(\hat{\mathcal{E}}_S(\gamma_2 o_2)) = \{5, 6, 7, 8\}$ .

Again, extended string  $\rho'' = \gamma_2 c_1 \gamma_2 o_2 \gamma_4 c_1 \gamma_4 o_1 \in \mathcal{L}_e^o(S_N/G)$  can be generated with  $\mathcal{O}(\rho'') = \gamma_2 o_2 \gamma_4 o_1$ . Then the state estimate of the supervisor becomes  $\hat{\mathcal{E}}_S(\gamma_2 o_2 \gamma_4 o_1) = NX_{o_1}(\mathcal{E}_S(\gamma_2 o_2 \gamma_4)) = \{9, 10\}$ .

**Remark 1.** Finally, we note that some non-deterministic control decision sets may contain redundancy, i.e., for  $\{\gamma_1, \dots, \gamma_n\} \in 2^\Gamma$ ,  $\gamma_i \subset \gamma_j$  for some  $i, j = 1, \dots, n$ . In this case, removing  $\gamma_i$  from the non-deterministic control decision set does not change the behavior of the closed-loop system. Formally, we say that a non-deterministic control decision set  $\{\gamma_1, \dots, \gamma_n\} \in 2^\Gamma$  is *irredundant* if its elements are incomparable, i.e.,  $\forall i, j = 1, \dots, n : \gamma_i \not\subset \gamma_j$ . For the sake of simplicity and without loss of generality, hereafter, we only consider irredundant non-deterministic control decision sets.

### C. Opacity of Non-deterministic Control Systems

In the definition of opacity for the standard deterministic setting, the intruder model has been specified by A1-A3. Here, we still consider the same intruder model, but we explain A3 more clearly in the non-deterministic setting:

A3' The intruder knows the functionality of the supervisor. That is, the intruder knows the set of all possible control decisions the supervisor may pick according to the control policy. However, it does not know which specific control decision the supervisor picks online.

This assumption is reasonable in many applications as long as the communication channel between supervisor and the actuator is reliable. Then under this setting, when the supervisor observes  $\rho \in \mathcal{O}(\mathcal{L}_e(S_N/G))$ , the intruder can only observe  $\rho|_\Sigma \in P(\mathcal{L}(S_N/G))$ . Therefore, the state estimate of the intruder essentially is more uncertainty, which needs to estimate all possible realizations consistent with the control policy and the observation. Formally, for any observable string  $s \in P(\mathcal{L}(S_N/G))$ , we define  $X_I(s)$  as the state estimate of the intruder, i.e.,

$$X_I(s) = \{\delta(s') \in X : \exists s' \in \mathcal{L}(S_N/G) \text{ s.t. } P(s') = s\}. \quad (10)$$

Then opacity of control systems under non-deterministic supervisors is defined as follows.

**Definition 2.** Let  $S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  be a non-deterministic supervisor. We say the closed-loop system  $S_N/G$  is opaque (w.r.t.  $\Sigma_o$  and  $X_S$ ) if  $\forall s \in P(\mathcal{L}(S_N/G)) : X_I(s) \not\subseteq X_S$ .

The state estimate of the supervisor and the state estimate of the intruder can be related as follows. Since the intruder observes strictly less than the supervisor, its estimate of the system is essentially the union of its estimate of all possible supervisor's knowledge about the system. To see this more

clearly, for any observable string  $s \in P(\mathcal{L}(S_N/G))$ , we also define

$$\hat{\mathcal{E}}_I(s) = \{\hat{\mathcal{E}}_S(\rho) \in 2^X : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\} \quad (11)$$

$$\mathcal{E}_I(s) = \{\mathcal{E}_S(\rho) \in 2^X : \rho \in \mathcal{O}(\mathcal{L}_e^d(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\} \quad (12)$$

as the intruder's estimates of the state-estimations of the supervisor. Note that  $\hat{\mathcal{E}}_I(s)$  and  $\mathcal{E}_I(s)$  are respectively the state estimate immediately after observing an observable event and the state-estimate with the unobservable tail included. Note that we use subscript "I" to emphasize that the estimates are from the intruder's point of view. Then we have the following result that connects  $\mathcal{E}_I$  and  $X_I$ .

**Proposition 1.** *For any  $s \in P(\mathcal{L}(S_N/G))$ , we have*

$$X_I(s) = \bigcup \mathcal{E}_I(s).$$

*Proof.* By the definitions of  $\mathcal{E}_I(s)$ ,  $\mathcal{E}_S(\rho)$ ,  $\mathcal{L}(S_N/G)$  and mapping  $\mathcal{O}$ , we have

$$\begin{aligned} & \bigcup \mathcal{E}_I(s) \\ &= \bigcup \{\mathcal{E}_S(\rho) \in 2^X : \rho \in \mathcal{O}(\mathcal{L}_e^d(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\} \\ &= \{x \in \mathcal{E}_S(\rho) : \rho \in \mathcal{O}(\mathcal{L}_e^d(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\} \\ &= \{\delta(\rho'|_\Sigma) : \rho' \in \mathcal{L}_e(S_N/G) \text{ s.t. } \mathcal{O}(\rho')|_\Sigma = s\} \\ &= \{\delta(s') : s' \in \mathcal{L}(S_N/G) \text{ s.t. } P(s') = s\} \\ &= X_I(s) \end{aligned}$$

This completes the proof.  $\square$

Given a non-opaque system, our goal is to synthesize a non-deterministic supervisor that restricts the system behavior such that opacity is satisfied for the closed-loop system. The opacity enforcement synthesis problem is formulated as follows.

**Problem 1. (Opacity Enforcement Problem)** *Given system  $G$  and secret states  $X_S \subseteq X$ , synthesize a partial observation non-deterministic supervisor  $S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$ , such that  $S_N/G$  is opaque w.r.t.  $X_S$  and  $\Sigma_o$ .*

#### IV. INFORMATION STATE AND ITS FLOW

In the formulation of the opacity enforcement problem, the domain of the supervisor is defined over languages. Therefore, the solution space is infinite in general and there is no prior knowledge to bound the memory of the supervisor. To effectively solve the synthesis problem, in this section, we restrict our attention to a class of *information-state-based supervisors*, where the space of information states is finite. We first define the information state in the non-deterministic control problem and then discuss how the selected information state evolves. Besides, we define a IS-mapping that can encode an IS-based supervisor. Our method for synthesizing a non-deterministic supervisor is to first synthesize a IS-mapping and then encode a supervisor from it. To this end, we finally put forward an algorithm that decodes a non-deterministic supervisor from IS-mapping.

##### A. Proposed Information Structure

In the deterministic control problem, it is known that  $2^X$  is sufficient to realize an opacity-enforcing supervisor. That is, a deterministic supervisor can be encoded as a state-based mapping  $S : 2^X \rightarrow \Gamma$ , which can be decoded by recursively estimating the state of the system and making decision based on the state-estimate (information-state).

In the non-deterministic control problem, the supervisor and the intruder observe different information. Hence, the supervisor needs to make decision based on both the state estimates of itself and that of the intruder. To separate the observation of the supervisor and the intruder, we propose the following information-state space

$$I := 2^X \times 2^{2^X}.$$

Each information state  $\iota \in I$  is in the form of  $\iota = (m, \mathbf{m})$ . Intuitively, the first component aims to represent the state estimate of supervisor, while the second component aims to represent intruder's knowledge of the supervisor.

Formally, given a non-deterministic supervisor  $S_N$  and let  $\rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G))$  be a decision history observed by the supervisor. We define

$$\mathcal{I}_{S_N}(\rho) = (\hat{\mathcal{E}}_S(\rho), \hat{\mathcal{E}}_I(\rho|_\Sigma)) \in 2^X \times 2^{2^X}$$

as the information-state reached by  $\rho$  under  $S_N$ . Clearly, we have  $\hat{\mathcal{E}}_S(\rho) \in \hat{\mathcal{E}}_I(\rho|_\Sigma)$  for any  $\rho$  by definition. We also define

$$\mathcal{I}_{S_N} := \{\mathcal{I}_{S_N}(\rho) : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G))\}$$

the set of all information-states reached by  $S_N$ .

**Definition 3.** A non-deterministic supervisor  $S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  is said to be *information-state-based (IS-based)* if

$$\forall \rho, \rho' \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) : \mathcal{I}_{S_N}(\rho) = \mathcal{I}_{S_N}(\rho') \Rightarrow S_N(\rho) = S_N(\rho'). \quad (13)$$

An IS-based supervisor only makes decisions based on its current information-state rather than the entire history. Therefore, we can encode an IS-based supervisor as a partial IS-mapping.

**Definition 4.** We say a partial IS-mapping  $\Theta : I \rightarrow 2^\Gamma$  encodes supervisor  $S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  if

$$\forall \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) : \Theta(\mathcal{I}_{S_N}(\rho)) = S_N(\rho).$$

Our general approach for synthesizing a non-deterministic supervisor is to synthesize its IS-mapping encoding. Clearly, given an IS-based supervisor  $S_N$ , we can easily encode it as an IS-mapping  $\Theta : I \rightarrow 2^\Gamma$ , which is defined at each state in  $\mathcal{I}_{S_N}$ . On the other hand, however, given a partial IS-mapping  $\Theta : I \rightarrow 2^\Gamma$ , it is not straightforward how to *decode* an IS-based supervisor from it. In fact, not every partial IS-mapping  $\Theta : I \rightarrow 2^\Gamma$  actually encodes an IS-based supervisor. As a necessary requirement, the partial IS-mapping should be defined at state  $\iota_0 = (\{x_0\}, \{\{x_0\}\})$ , which is the initial information-state of any IS-based supervisor. Then one can argue inductively that, for any information-state reachable, the partial IS-mapping should be defined, which suggests that the domain of the partial IS-mapping should contain the

“reachability closure” from the initial-state  $\iota_0$ ; otherwise, the decoded supervisor will “get stuck” at those states where the IS-mapping is undefined.

To compute such an “reachability closure”, we need to investigate how the information-state evolves. As we discussed earlier, the first component of the information-state can be computed recursively based on  $\rho$ . However, the question is how to compute the second component. To this end, we should not only know the control decision for history  $\rho$ , but should also know the control decisions for those  $\rho'$  such that  $\rho|_{\Sigma} = \rho'|_{\Sigma}$ . In the remaining part of this section, we will elaborate on how  $\hat{\mathcal{E}}_I(\rho|_{\Sigma})$  can be computed recursively and by what information.

### B. Micro/Macro States and Decisions

Before we proceed further, we define some necessary concepts. First, we introduce the notion of micro-state, which is used to represent the knowledge of supervisor.

**Definition 5. (Micro-State)** A micro-state  $m \in 2^X$  is a set of states and we define  $M = 2^X$  as the set of micro-states. An augmented micro-state  $m^+ = (m, \gamma) \in 2^X \times \Gamma$  is a micro-state augmented with a control decision and we define  $M^+ = 2^X \times \Gamma$  as the set of augmented micro-states.

Then, we define the notion of macro-state, which is used to represent the knowledge of intruder about the supervisor.

**Definition 6. (Macro-State)** A macro-state  $\mathbf{m} = \{m_1, m_2, \dots, m_n\} \subseteq 2^X$  is a set of micro-states and we define  $\mathbb{M} = 2^{2^X}$  as the set of macro-states. An augmented macro-state  $\mathbf{m}^+ = \{(m_1, \gamma_1), (m_2, \gamma_2), \dots, (m_n, \gamma_n)\} \subseteq 2^X \times \Gamma$  is a set of augmented micro-states and we define  $\mathbb{M}^+ = 2^{2^X \times \Gamma}$  as the set of augmented macro-states.

In order to estimate the knowledge of the intruder, we should not only know the decision of the supervisor at a specific micro-state, but also should know the decisions at other micro-states in the same macro-state, which means that these micro-states are indistinguishable from the intruder’s point of view. This leads to the notion of macro-control-decision.

**Definition 7. (Macro-Control-Decision)** A macro-control-decision is a set in the form of

$$d = \{(m_1, \Gamma_1), (m_2, \Gamma_2), \dots, (m_n, \Gamma_n)\} \subseteq 2^X \times 2^\Gamma,$$

where each  $(m_i, \Gamma_i)$  is a pair of micro-state and a non-deterministic control decision (a set of control decisions). We denote by  $D = 2^{2^X \times 2^\Gamma}$  the set of macro-control-decisions.

Let  $\mathbf{m} = \{m_1, m_2, \dots, m_n\} \in \mathbb{M}$  be a macro-state and  $d \in D$  be a macro-control-decision. We say that  $d$  is compatible with  $\mathbf{m}$  if it is in the form of

$$d = \{(m_1, \Gamma_1), (m_2, \Gamma_2), \dots, (m_n, \Gamma_n)\} \subseteq 2^X \times 2^\Gamma,$$

i.e.,  $d$  essentially assigns each micro-state  $m_i \in \mathbf{m}$  a non-deterministic control decision  $\Gamma_i \in 2^\Gamma$ .

The unobservable reach of a macro-control-decision  $d \in D$  is defined by

$$\odot(d) = \{(m', \gamma) : \exists(m, \Gamma) \in d, \gamma \in \Gamma \text{ s.t. } m' = UR_\gamma(m)\}.$$

Let  $\mathbf{m}^+$  be an augmented macro-state and  $\sigma \in \Sigma_o$  be an observable event. Then the observable reach of  $\mathbf{m}^+$  upon the occurrence of  $\sigma$  is defined as

$$\widehat{NX}_\sigma(\mathbf{m}^+) = \{m' : \exists(m, \gamma) \in \mathbf{m}^+ \text{ s.t. } m' = NX_\sigma(m) \wedge \sigma \in \gamma\}.$$

### C. Information-Flow Analysis

Now, suppose that an IS-mapping  $\Theta : I \rightarrow 2^\Gamma$  that encodes an IS-based supervisor  $S_N$  is given. Let  $\mathbf{m} = \{m_1, \dots, m_k\}$  be a macro-state representing the intruder’s estimate of the supervisor’s knowledge. We define

$$d_\Theta(\mathbf{m}) = \{(m_1, \Theta(m_1, \mathbf{m})), \dots, (m_k, \Theta(m_k, \mathbf{m}))\}$$

as the macro-control-decision made by IS-based supervisor at macro-state  $\mathbf{m}$ .

Initially, the state-estimate of the supervisor is  $m_0 = \{x_0\}$  and the intruder believes that this is the unique estimate of the system with estimate  $\mathbf{m}_0 = \{m_0\}$ , which forms the initial information-state  $\iota_0 = (m_0, \mathbf{m}_0)$ .

Then the supervisor issues a non-deterministic decision set  $\Gamma_0 = S_N(\epsilon) = \Theta(m_0, \mathbf{m}_0)$ . Note that, we have pre-specified that the supervisor is IS-based. Therefore, we denote the control decision information at this instant by a macro-control-decision  $d_\Theta(\mathbf{m}_0) = \{(m_0, \Theta(m_0, \mathbf{m}_0))\}$ , which means that “the supervisor will make control decision if its state-estimate is  $m_0$ ”. Note that, at this instant,  $d_\Theta(\mathbf{m}_0)$  is a singleton as the intruder does not yet have ambiguity about the supervisor, i.e.,  $\mathbf{m}_0 = \{m_0\}$ .

Once the allowed decision set  $\Gamma_0$  is specified, the supervisor will pick a concrete control decision in it. The intruder does not know which decision is chosen while the supervisor knows. Suppose that  $\Gamma_0 = \{\gamma_0^1, \dots, \gamma_0^k\}$  contains  $k$  control decisions. Then the intruder’s knowledge about the supervisor becomes

$$\begin{aligned} \mathbf{m}_0^+ &= \odot(d_\Theta(\mathbf{m}_0)) \\ &= \{(UR_{\gamma_0^1}(m_0), \gamma_0^1), \dots, (UR_{\gamma_0^k}(m_0), \gamma_0^k)\} \\ &= \{(m_0^1, \gamma_0^1), \dots, (m_0^k, \gamma_0^k)\}, \end{aligned} \quad (14)$$

which means that the supervisor’s estimate (with the unobservable tail) is possibly  $UR_{\gamma_0^i}(m_0)$  and the control decision applied is  $\gamma_0^i$ . Note that, the supervisor knows precisely which augmented micro-state  $(m_0^i, \gamma_0^i)$  it is at.

Then when a new observable event  $\sigma \in \Sigma_o$  occurs, and the intruder updates its knowledge to

$$\mathbf{m}_1 = \widehat{NX}_\sigma(\mathbf{m}_0^+) = \{m_1^1, \dots, m_1^p\}. \quad (15)$$

which is a macro-state containing at most  $k$  micro-states, i.e.  $p \leq k$ .

Now, let us assume that, after some steps, the intruder’s knowledge about the supervisor (immediately after the occurrence of an observable event) is

$$\mathbf{m}_n = \{m_n^1, \dots, m_n^k\}, \quad (16)$$

Note that the supervisor knows the exact state estimate, i.e.,  $m_n^i \in \mathbf{m}_n$ , and for each  $m_n^i$ , it allows non-deterministic decision set  $\Gamma_i = \Theta(m_n^i, \mathbf{m}_n)$  as we assume the supervisor is IS-based and is encoded by  $\Theta$ . Therefore, the corresponding macro-control-decision is

$$d_\Theta(\mathbf{m}_n) = \{(m_n^1, \Theta(m_n^1, \mathbf{m}_n)), \dots, (m_n^k, \Theta(m_n^k, \mathbf{m}_n))\}. \quad (17)$$

Then the intruder's knowledge about the supervisor by adding this control information becomes

$$\mathbf{m}_n^+ = \odot(d_\Theta(\mathbf{m}_n)), \quad (18)$$

which is an augmented marco-state containing at most  $\sum_{i=1}^k |\Theta(m_n^i, \mathbf{m}_n)|$  augmented micro-states.

Based on the above discussion, suppose that the intruder observes  $\sigma_1 \dots \sigma_n \in P(\mathcal{L}(S_N/G))$  and by assuming the fact that  $S_N$  is an IS-based supervisor encoded by  $\Theta$ , it induces the following sequence

$$\mathbf{m}_0 \xrightarrow{d_0} \mathbf{m}_0^+ \xrightarrow{\sigma_1} \mathbf{m}_1 \xrightarrow{d_1} \dots \xrightarrow{\sigma_n} \mathbf{m}_n \xrightarrow{d_n} \mathbf{m}_n^+, \quad (19)$$

where  $\mathbf{m}_0 = \{\{x_0\}\}$ ,  $d_i = d_\Theta(\mathbf{m}_i)$ ,  $\mathbf{m}_i^+ = \odot(d_i)$  and  $\mathbf{m}_{i+1} = \widehat{NX}_{\sigma_{i+1}}(\mathbf{m}_i^+)$ . We note that  $\sigma_{i+1}$  is defined at  $\mathbf{m}_i^+$  iff there exist  $(m, \gamma) \in \mathbf{m}_i^+$  and  $x \in m$  such that  $\delta(x, \sigma_{i+1})!$  and  $\sigma_{i+1} \in \gamma$ . Therefore, the sequence in Equation (19) is uniquely defined when  $\sigma_1 \dots \sigma_n$  and  $\Theta$  are fixed; it is independent from the actual online choice of the supervisor at each instant.

Now we are ready to specify the reachability closure of an IS-mapping. Formally let  $\Theta : I \rightarrow 2^\Gamma$  be a partial IS-mapping and  $\iota = (m, \mathbf{m}) \in I$  be an information-state. Then the *reachability closure* of  $\iota$  under  $\Theta$ , denoted by  $\text{REACH}_\Theta(\iota) \subseteq I$ , is defined recursively as follows:

- $\iota \in \text{REACH}_\Theta(\iota)$ ;
- $\iota' = (m', \mathbf{m}') \in \text{REACH}_\Theta(\iota)$  if
  - $m' \in \mathbf{m}'$ ; and
  - there exists  $\iota'' = (m'', \mathbf{m}'') \in \text{REACH}_\Theta(\iota)$  such that  $\mathbf{m}'' \xrightarrow{d_\Theta(\mathbf{m}'')} \mathbf{m}''^+ \xrightarrow{\sigma} \mathbf{m}'$  for some  $\sigma \in \Sigma_o$ .

#### D. Property of the Information-State

The above analysis of information-flow is heuristic. In this subsection, we formally show that the proposed information updating rule indeed yields the state estimate of the intruder in the controlled system.

**Theorem 1.** *Let  $\Theta$  be an IS-mapping that encodes an IS-based supervisor  $S_N$  and  $s = \sigma_1 \dots \sigma_k \in P(\mathcal{L}(S_N/G))$  be an observable string available to the intruder. Let  $\mathbf{m}_k$  and  $\mathbf{m}_k^+$  be states induced by  $s$  and  $\Theta$  according to Equation (19). Then we have*

- (i)  $\mathbf{m}_k = \hat{\mathcal{E}}_I(s)$ ; and
- (ii)

$$\mathbf{m}_k^+ = \left\{ (\mathcal{E}_S(\rho\gamma), \gamma) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t.} \\ \rho|_\Sigma = s \text{ and } \gamma \in S_N(\rho) \end{array} \right\}.$$

*Proof.* We prove by induction on the length of  $s$ .

*Induction Basis:* For  $|s| = 0$ , i.e.  $s = \epsilon$ , from the definition of  $\hat{\mathcal{E}}_I(s)$ , we know that

$$\begin{aligned} \hat{\mathcal{E}}_I(\epsilon) &= \{\hat{\mathcal{E}}_S(\rho) \in 2^X : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t. } \rho|_\Sigma = \epsilon\} \\ &= \{\hat{\mathcal{E}}_S(\epsilon)\} \\ &= \{\{\delta(\epsilon)\}\} \\ &= \{\{x_0\}\} \\ &= \mathbf{m}_0 \end{aligned}$$

Since  $\mathbf{m}_0^+ = \odot(d_\Theta(\mathbf{m}_0))$  and  $d_\Theta(\mathbf{m}_0) = \{(m_0, S_N(\epsilon))\}$ , we have

$$\begin{aligned} \mathbf{m}_0^+ &= \odot(d_\Theta(\mathbf{m}_0)) \\ &= \{(UR_\gamma(m_0), \gamma) : \gamma \in S_N(\epsilon)\} \\ &= \{(UR_\gamma(\hat{\mathcal{E}}_S(\epsilon)), \gamma) : \gamma \in S_N(\epsilon)\} \\ &= \{(\mathcal{E}_S(\gamma), \gamma) : \gamma \in S_N(\epsilon)\} \end{aligned}$$

Note that  $\rho = \epsilon$  is the only extended string in  $\mathcal{O}(\mathcal{L}_e^o(S_N/G))$  such that  $\rho|_\Sigma = s$ . This completes the induction basis.

*Induction Step:* Let us assume that Theorem 1 holds for  $|s| = k$ . Then we want to prove the case of  $s\sigma_{k+1} \in P(\mathcal{L}(S_N/G))$ . By the induction hypothesis, we know that

$$\mathbf{m}_k^+ = \left\{ (\mathcal{E}_S(\rho\gamma), \gamma) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t.} \\ \rho|_\Sigma = s \text{ and } \gamma \in S_N(\rho) \end{array} \right\}.$$

Then, we have

$$\begin{aligned} \mathbf{m}_{k+1} &= \widehat{NX}_{\sigma_{k+1}}(\mathbf{m}_k^+) \\ &= \{NX_{\sigma_{k+1}}(m) : (m, \gamma) \in \mathbf{m}_k^+, \sigma_{k+1} \in \gamma\} \\ &= \left\{ NX_{\sigma_{k+1}}(\mathcal{E}_S(\rho\gamma)) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t.} \\ \rho|_\Sigma = s, \gamma \in S_N(\rho) \text{ and } \sigma_{k+1} \in \gamma \end{array} \right\} \\ &= \{\hat{\mathcal{E}}_S(\rho\gamma\sigma_{k+1}) : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\} \\ &= \{\hat{\mathcal{E}}_S(\rho') : \rho' \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t. } \rho'|_\Sigma = s\sigma_{k+1}\} \\ &= \hat{\mathcal{E}}_I(s\sigma_{k+1}). \end{aligned}$$

For  $\mathbf{m}_{k+1}^+ = \odot(d_\Theta(\mathbf{m}_{k+1}))$ . Suppose that  $d_\Theta(\mathbf{m}_{k+1}) = \{(m_{k+1}^1, \Theta(m_{k+1}^1, \mathbf{m}_{k+1})), \dots, (m_{k+1}^n, \Theta(m_{k+1}^n, \mathbf{m}_{k+1}))\}$ . Note that we have

$$\begin{aligned} \mathbf{m}_{k+1} &= \{\hat{\mathcal{E}}_S(\rho) : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\sigma_{k+1}\} \\ &= \{m_{k+1}^1, \dots, m_{k+1}^n\} \end{aligned}$$

For each  $\rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G))$  such that  $\rho|_\Sigma = s\sigma_{k+1}$ , since  $S_N$  is IS-based, we have  $S_N(\rho) = \Theta(\hat{\mathcal{E}}_S(\rho), \mathbf{m}_{k+1})$ . Then we have the followings

$$\begin{aligned} \mathbf{m}_{k+1}^+ &= \odot(d_\Theta(\mathbf{m}_{k+1})) \\ &= \{(UR_\gamma(m), \gamma) : \exists(m, \Gamma) \in d_\Theta(\mathbf{m}_{k+1}) \text{ s.t. } \gamma \in \Gamma\} \\ &= \left\{ (UR_\gamma(\hat{\mathcal{E}}_S(\rho)), \gamma) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t.} \\ \gamma \in S_N(\rho) \text{ and } \rho|_\Sigma = s\sigma_{k+1} \end{array} \right\} \\ &= \left\{ (\mathcal{E}_S(\rho\gamma), \gamma) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)), \text{ s.t.} \\ \gamma \in S_N(\rho) \text{ and } \rho|_\Sigma = s\sigma_{k+1} \end{array} \right\} \end{aligned}$$

This completes the induction step, i.e. (ii) holds.  $\square$



For any augmented macro-state  $\mathbf{m}^+$ , we define

$$M(\mathbf{m}^+) = \{m \in M : (m, \gamma) \in \mathbf{m}^+\}$$

as the macro-state obtained by removing the control decision components from  $\mathbf{m}^+$ . Then the following result reveals that the above defined states  $M(\mathbf{m}_k^+)$  are indeed the state estimate of the intruder  $\mathcal{E}_I(s)$ .

**Corollary 1.** *Let  $\Theta$  be an IS-mapping that encodes an IS-based supervisor  $S_N$  and  $s = \sigma_1 \dots \sigma_k \in P(\mathcal{L}(S_N/G))$  be an observable string available to the intruder. Let  $\mathbf{m}_k^+$  be the state reached according to the information-flow. Then we have*

$$M(\mathbf{m}_k^+) = \mathcal{E}_I(s)$$

*Proof.* By Theorem 1, we have

$$\mathbf{m}_k^+ = \left\{ (\mathcal{E}_S(\rho\gamma), \gamma) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t.} \\ \rho|_\Sigma = s \text{ and } \gamma \in S_N(\rho) \end{array} \right\}.$$

Therefore,

$$\begin{aligned} M(\mathbf{m}_k^+) &= \left\{ \mathcal{E}_S(\rho\gamma) : \begin{array}{l} \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)) \text{ s.t.} \\ \rho|_\Sigma = s \text{ and } \gamma \in S_N(\rho) \end{array} \right\} \\ &= \{\mathcal{E}_S(\rho') : \rho' \in \mathcal{O}(\mathcal{L}_e^d(S_N/G)) \text{ s.t. } \rho'|_\Sigma = s\} \\ &= \mathcal{E}_I(s) \end{aligned}$$

This completes the proof.  $\square$

We explain the above concepts by the following example.

**Example 3.** Let us still consider system  $G$  in Figure 1. We consider a non-deterministic supervisor  $S_N$  defined by

$$\forall \rho \in (\Gamma\Sigma_o)^* : S_N(\rho) = \{\{c_1\}, \{c_2\}\}.$$

Clearly, this supervisor is IS-based and it can be encoded by IS-mapping  $\Theta : I \rightarrow 2^\Gamma$  such that  $\forall \iota \in I : \Theta(\iota) = \{\{c_1\}, \{c_2\}\}$ .

Initially, the supervisor's estimate is  $m_0 = \{0\}$  and the intruder's estimate of supervisor's estimation is  $\mathbf{m}_0 = \{\{0\}\}$ , where the macro-control-decision induced by  $\Theta$  is

$$d_\Theta(\mathbf{m}_0) = \{(\{0\}, \Theta(\{0\}, \{\{0\}\}))\} = \{(\{0\}, \{\{c_1\}, \{c_2\}\})\}.$$

Then the intruder's knowledge is updated to

$$\begin{aligned} \mathbf{m}_0^+ &= \odot(d_\Theta(\mathbf{m}_0)) \\ &= \{(UR_{\{c_1\}}(\{0\}), \{c_1\}), (UR_{\{c_2\}}(\{0\}), \{c_2\})\} \\ &= \{(\{0, 1\}, \{c_1\}), (\{0, 3\}, \{c_2\})\} \end{aligned}$$

When event  $o_1$  is observed, the intruder updates its knowledge to

$$\begin{aligned} \mathbf{m}_1 &= \widehat{NX}_{o_1}(\mathbf{m}_0^+) = \{NX_{o_1}(\{0, 1\}), NX_{o_1}(\{0, 3\})\} \\ &= \{\{4\}, \{5\}\} \end{aligned}$$

which means that the intruder guesses that the supervisor's state-estimate is either  $\{4\}$  or  $\{5\}$  based on the information available. Again, the macro-control-decision at  $\mathbf{m}_1$  is

$$\begin{aligned} d_\Theta(\mathbf{m}_1) &= \{(\{4\}, \Theta(\{4\}, \mathbf{m}_1)), (\{5\}, \Theta(\{5\}, \mathbf{m}_1))\} \\ &= \{(\{4\}, \{\{c_1\}, \{c_2\}\}), (\{5\}, \{\{c_1\}, \{c_2\}\})\} \end{aligned}$$

which leads to

$$\begin{aligned} \mathbf{m}_1^+ &= \odot(d_\Theta(\mathbf{m}_1)) \\ &= \left\{ \begin{array}{l} (UR_{\{c_1\}}(\{4\}), \{c_1\}), (UR_{\{c_2\}}(\{4\}), \{c_2\}), \\ (UR_{\{c_1\}}(\{5\}), \{c_1\}), (UR_{\{c_2\}}(\{5\}), \{c_2\}) \end{array} \right\} \\ &= \{(\{4\}, \{c_1\}), (\{4\}, \{c_2\}), (\{5, 6\}, \{c_1\}), (\{5, 7\}, \{c_2\})\} \end{aligned}$$

Similarly, from  $\mathbf{m}_1^+$ , observations can be made and so forth.

### E. Decode Supervisor from IS-Mapping

Finally, we are ready to discuss how to *decode* an IS-based non-deterministic supervisor from an IS-mapping  $\Theta : I \rightarrow \Gamma$ ; the decoded non-deterministic supervisor is denoted by  $S_\Theta$ . Let  $\text{DOM}(\Theta) = \{\iota \in I : \Theta(\iota) \neq \emptyset\}$  be the domain of  $\Theta$ . We say that IS-mapping  $\Theta$  is *reachability-closed* if

$$\text{REACH}_\Theta(\iota_0) \subseteq \text{DOM}(\Theta),$$

where  $\iota_0 = (\{x_0\}, \{\{x_0\}\})$  is the initial information-state. Clearly,  $\Theta$  is necessarily to be reachability-closed; otherwise, the supervisor cannot make decision after some executions. Without loss of generality, we can further assume that  $\text{REACH}_\Theta(\iota_0) = \text{DOM}(\Theta)$  as the mapping information of those unreachable states are not used.

When IS-mapping  $\Theta$  is reachability-closed, we can decode a supervisor  $S_\Theta$  as follows. For any decision history  $\rho = \gamma_0\sigma_1\gamma_1 \dots \gamma_{n-1}\sigma_n$ , we have

$$S_\Theta(\rho) = \Theta(\hat{\mathcal{E}}_S(\rho), \hat{\mathcal{E}}_I(\rho|_\Sigma)). \quad (20)$$

Note that, based on the previous discussion, both  $\hat{\mathcal{E}}_S(\rho)$  and  $\hat{\mathcal{E}}_I(\rho|_\Sigma)$  can be computed recursively based on  $\Theta$ . Therefore, in practice,  $S_\Theta(\rho)$  can be executed online according to Algorithm 1. Specifically, we use parameters  $m, m^+, \mathbf{m}$  and  $\mathbf{m}^+$  to represent  $\hat{\mathcal{E}}_S(\rho), \mathcal{E}_S(\rho), \hat{\mathcal{E}}_I(\rho|_\Sigma)$  and  $\mathcal{E}_I(\rho|_\Sigma)$ , respectively. Note that the updates of  $\mathbf{m}$  and  $\mathbf{m}^+$  use the online observation  $\sigma$  and the IS-mapping  $\Theta$  to generate a non-deterministic control decision set  $\Gamma$ , in which an actual control decision applied  $\gamma \in \Gamma$  is chosen randomly. However, the updates of  $m$  and  $m^+$  only use the online observation  $\sigma$  and the actual decision  $\gamma$  applied.

---

#### Algorithm 1: Online Decoding of IS-Mapping $\Theta$

---

```

1   $m \leftarrow \{x_0\}$  and  $\mathbf{m} \leftarrow \{\{x_0\}\}$  and  $\rho \leftarrow \epsilon$ ;
2  while  $\rho = \epsilon$  or a new event  $\sigma \in \Sigma_o$  is observed do
3      if a new event  $\sigma \in \Sigma_o \cap \gamma$  is observed then
4           $m \leftarrow NX_\sigma(m^+)$  and  $\mathbf{m} \leftarrow \widehat{NX}_\sigma(\mathbf{m}^+)$ ;
5           $\rho \leftarrow \rho\sigma$ ;
6      Define  $S_\Theta(\rho) \leftarrow \Theta(m, \mathbf{m})$  as the current
7      non-deterministic control decision;
8      Randomly pick  $\gamma \in S_\Theta(\rho)$  and apply this
9      control decision online;
10      $m^+ \leftarrow UR_\gamma(m)$  and  $\mathbf{m}^+ \leftarrow \odot(d_\Theta(\mathbf{m}))$ ;
11      $\rho \leftarrow \rho\gamma$ ;

```

---

By understanding how an IS-mapping  $\Theta$  can be decoded as an IS-based supervisor, hereafter, we will also refer to a

reachability-closed IS-mapping  $\Theta$  as an IS-based supervisor directly. In order to solve the general opacity enforcement problem as formulated in Problem 1, our approach is to restrict our solution space to IS-based supervisors and solve the following IS-mapping synthesis problem.

**Problem 2.** (*Information-State-Based Opacity Enforcement Problem*) Given system  $G$  and secret states  $X_S \subseteq X$ , synthesize an IS-based supervisor  $S_\Theta : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  decoded from IS-mapping  $\Theta : I \rightarrow 2^\Gamma$ , such that  $S_\Theta/G$  is opaque w.r.t.  $X_S$  and  $\Sigma_o$ .

**Remark 2.** Problem 2 essentially restricts the solution space of Problem 1 to a finite domain. Clearly, if there exists an IS-based supervisor that enforces opacity, then there exists a non-deterministic opacity-enforcing supervisor. However, the following question arise immediately: *whether or not the non-existence of an IS-based supervisor also implies the non-existence of a general supervisor?* We will show later in Section VI that there exists a non-deterministic opacity enforcing supervisor *if and only if* there exists an IS-based one. In other words, restricting our attention to Problem 2 is without loss of generality for the solvability of Problem 1.

## V. SYNTHESIS OF IS-BASED SUPERVISORS

In this section, we discuss how to synthesize an IS-based supervisor that enforces opacity. We first introduced the structure of the generalized bipartite transition system. Then we present a synthesis algorithm that returns a solution to Problem 2.

### A. Bipartite Transition System

By the analysis in the previous section, we see that the update of the intruder's knowledge consists of two steps: one is when the supervisor picks a macro-control-decision and the other is when a new observable event occurs. To separate these two steps, we adopt the idea of the bipartite transition systems (BTS) proposed in [46]. Here, we call the proposed structure *generalized* BTS (G-BTS) as it captures, in a more general manner, both the supervisor's estimate and the intruder's knowledge about the supervisor, while the original BTS in [46] only captures the supervisor's estimate.

**Definition 8.** A *generalized bipartite transition system* (G-BTS)  $T$  w.r.t.  $G$  is a 7-tuple

$$T = (Q_Y, Q_Z, h_{YZ}, h_{ZY}, \Sigma_o, D, y_0).$$

where

- $Q_Y \subseteq \mathbb{M}$  is a set of macro-states;
- $Q_Z \subseteq \mathbb{M}^+$  is the set of augmented macro-states;
- $h_{YZ} : Q_Y \times D \rightarrow Q_Z$  is the transition function from  $Y$ -states to  $Z$ -states satisfying: for any  $h_{YZ}(\mathbf{m}, d) = \mathbf{m}^+$ , we have
  - $d$  is compatible with  $\mathbf{m}$ ; and
  - $\mathbf{m}^+ = \odot(d)$ .
- $h_{ZY} : Q_Z \times \Sigma_o \rightarrow Q_Y$  is the transition function from  $Z$ -states to  $Y$ -states satisfying: for any  $h_{ZY}(\mathbf{m}^+, \sigma) = \mathbf{m}$ ,  $\sigma \in \Sigma_o$ , we have
  - $\mathbf{m} = \widehat{NX}_\sigma(\mathbf{m}^+)$ .

- $D$  is the set of macro-control-decisions;
- $\Sigma_o$  is the set of observable events of system  $G$ ;
- $y_0 = \{\{x_0\}\} \in Q_Y$  is the initial  $Y$ -state.

The G-BTS essentially captures the information-flow analyzed in Section IV. Specifically, at each  $Y$ -state, the IS-based supervisor makes a macro-control-decision  $d$  and then moves to a  $Z$ -state by updating of the intruder knowledge via unobservable reaches under the issued macro-control-decision  $d$ . When a new observable event  $\sigma \in \Sigma_o$  occurs at a  $Z$ -state, we move to a  $Y$ -state by computing the observable reach, and so forth.

**Example 4.** Again, we consider system  $G$  in Figure 1. An example of the G-BTS is shown in Figure 2(a), in which rectangular states represent  $Y$ -states and oval states represent  $Z$ -states. Some states are omitted in Figure 2(a) for simplicity. States are named by  $s_1, \dots, s_{32}$ . The initial  $Y$ -state is  $s_1 = \{\{0\}\}$ , from which macro-control-decisions  $d_1, \dots, d_5$  that are compatible with  $s_1$  can be made. For example, if the macro-control-decision made is  $d_5 = \{\{0\}, \{c_1\}, \{c_2\}\}$ , then we move to  $Z$ -state  $s_{10} = \odot(d_5)$ . From this state, observable events  $o_1$  and  $o_2$  can occur, and both lead to the same  $Y$ -state  $s_{18}$ . From  $Y$ -state  $s_{18}$ , macro-control-decisions  $d_9, \dots, d_{13}$  that are compatible with  $s_{18}$  can be made. If the macro-control-decision made is  $d_{11}$ , then we move to  $s_{23} = \odot(d_{11})$  and so forth.

### B. Synthesis of IS-Based Supervisors

Now, we present how to synthesize IS-based non-deterministic opacity-enforcing supervisors represented by an IS-mapping. Given a G-BTS  $T$ , for any  $Y$ -state  $y \in Q_Y$ , we define

$$C_T(y) := \{d \in D : h_{YZ}(y, d)!\}$$

as the set of macro-control-decisions defined at  $y$  in  $T$ . Also, we say that a  $Y$ -state  $y$  is *consistent* if  $C_T(y) \neq \emptyset$ ; and a  $Z$ -state  $z$  is *consistent* if, for any  $\sigma \in \Sigma_o$ , we have

$$h_{ZY}(z, \sigma)! \Leftrightarrow (\exists(m, \gamma) \in z)[NX_\sigma(m) \neq \emptyset \wedge \sigma \in \gamma].$$

Intuitively, a  $Y$ -state is consistent if at least one macro-control-decision is defined and a  $Z$ -state is consistent if all feasible events are defined. Consistency is required for the purpose of control as the supervisor should be able to provide a control decision for any observation. We denote by  $Q_{const}^T$  the set of consistent states in  $T$  and we say that  $T$  is consistent if all reachable states are consistent.

As discussed earlier, we restrict our attention to IS-based supervisors. Our approach for synthesizing non-deterministic opacity-enforcing supervisors consists of the following two steps:

- (i) construct the largest consistent G-BTS in which all states are not secret-revealing;
- (ii) extract one IS-based supervisor in the form of an IS-mapping from this largest G-BTS.

Since such an IS-based supervisor is extracted from  $T$ , by Theorem 1 and Corollary 1, we know that, upon the occurrence of any decision history, the  $Z$ -state  $z \in \mathbb{M}^+$  reached is essentially the set of all possible state-estimates of the supervisor.

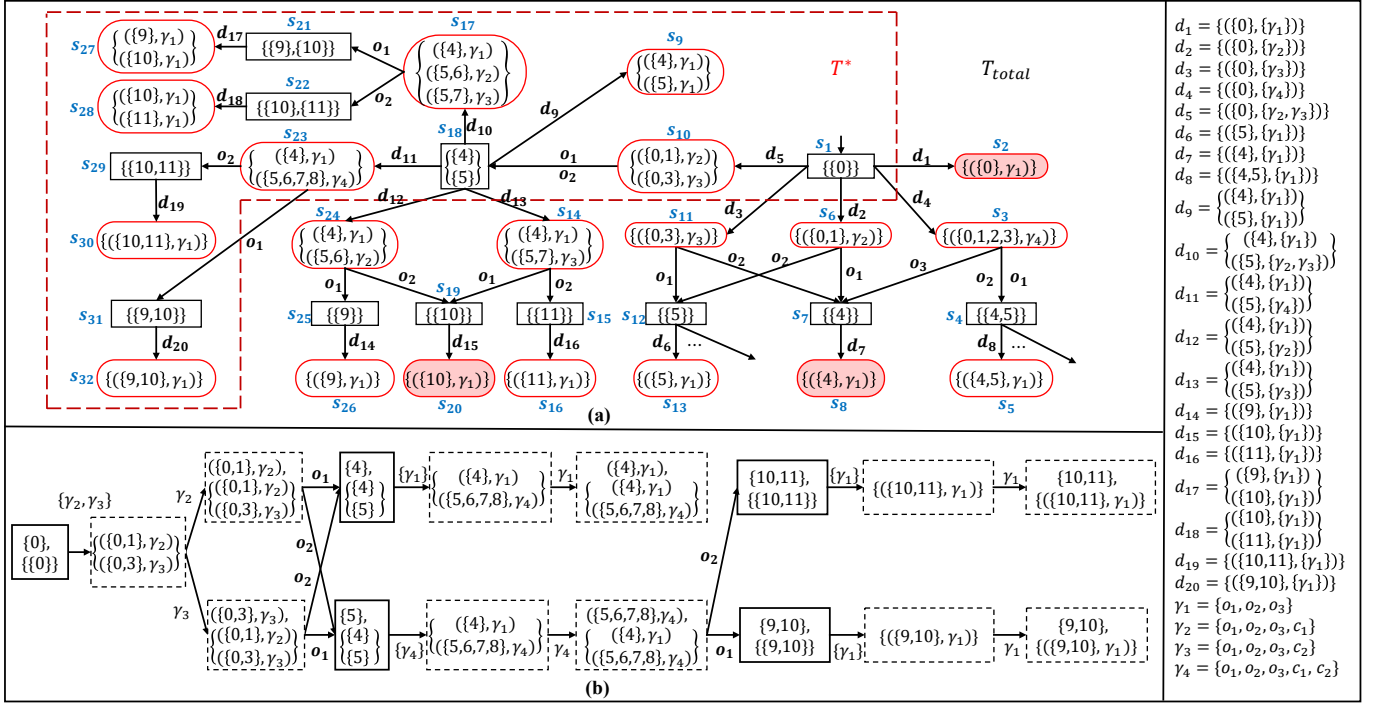


Fig. 2. (a) An Example of the G-BTS, where rectangular states represent Y-states and oval states represent Z-states. (b) Decision diagram of the synthesized non-deterministic supervisor.

Moreover, by Proposition 1, we know that  $\bigcup M(z) = X_I(s)$ , where  $s$  is the observation leading to the Z-state. Therefore, to make sure that the closed-loop system  $S_\Theta/G$  is opaque, it suffices to guarantee that, for any Z-state  $z \in \mathbb{M}^+$  reached, we have

$$\bigcup M(z) \not\subseteq X_S.$$

To this end, we define

$$Q_{\text{reveal}} = \{z \in \mathbb{M}^+ : \bigcup M(z) \subseteq X_S\}$$

as the set of *secret-revealing* Z-states.

In order to synthesize an IS-based supervisor, first, we construct the largest G-BTS w.r.t.  $G$  that enumerates all the feasible transitions satisfying the constraints of  $h_{YZ}$  and  $h_{ZY}$ . We denote such an all-feasible G-BTS by  $T_{\text{total}}$ . Then, we need to delete all secret-revealing Z-states in  $T_{\text{total}}$  and obtain a new G-BTS

$$T_0 = T_{\text{total}} \upharpoonright_{(Q_Y \cup Q_Z) \setminus Q_{\text{reveal}}},$$

where  $T \upharpoonright_Q$  denotes the G-BTS obtained by restricting the state-space of  $T$  to  $Q \subseteq Q_Y \cup Q_Z$ .

However, by deleting secret-revealing states, the resulting G-BTS may become inconsistent. Hence, we also need to delete inconsistent states recursively. Specifically, we define an operator  $F$  that maps a G-BTS to a new G-BTS by:

$$F : T \mapsto T \upharpoonright_{Q_{\text{const}}^T},$$

and we define

$$T^* = \lim_{k \rightarrow \infty} F^k(T_0)$$

as the largest consistent G-BTS in which there is no secret-revealing state. The existence of the supremal fixed-point as

well as the finite-convergence of iteration follow directly from the computation of winning region in two-player games [14] or the well-known supremal controllable sub-language [6]. We illustrate this procedure by the following example.

**Example 5.** Consider again system  $G$  in Figure 1. First, we construct the largest G-BTS  $T_{\text{total}}$  by enumerating all possible transitions, which is in fact the structure shown in Figure 2(a). For sake of simplicity, as we discussed earlier, redundant macro-control-decisions are omitted in  $T_{\text{total}}$ . For example,  $d = \{(\{0\}, \gamma_1, \gamma_2)\}$  is not listed at state  $s_1$ , since  $\gamma_1 \subset \gamma_2$  and macro-control-decision  $d_2$  is sufficient enough to carry this information.

Note that Z-states  $s_2$ ,  $s_8$  and  $s_{20}$  are secret-revealing states since  $\bigcup M(s_2) = \{0\} \subseteq X_S$ ,  $\bigcup M(s_8) = \{4\} \subseteq X_S$  and  $\bigcup M(s_{20}) = \{10\} \subseteq X_S$ . Therefore, we need to delete states  $s_2$ ,  $s_8$  and  $s_{20}$  to obtain  $T_0$ . However, this creates inconsistent states  $s_7$  and  $s_{19}$  as no macro-control-decision is defined. Therefore, these two states are removed when applying operator  $F$  for the first time. Again, this further creates inconsistent states  $s_3$ ,  $s_6$ ,  $s_{11}$ ,  $s_{14}$  and  $s_{24}$  since some feasible observations are not defined. Therefore, these states and the associated transitions are again deleted when applying operator  $F$  for the second time. This yields the final structure  $T^*$  including states  $s_1, s_9, s_{10}, s_{17}, s_{18}, s_{21}, s_{22}, s_{23}, s_{27}, \dots, s_{32}$ , which is the largest consistent G-BTS having no secret-revealing state.

Based on  $T^*$ , Algorithm 2 is provided to synthesize an IS-based non-deterministic supervisor in the form of an IS-mapping via a depth-first search. Specifically, we start from the initial Y-state and pick a macro-control-decision  $d$  from

**Algorithm 2:** Synthesis of IS-Based Supervisor  $\Theta^*$ 


---

**input :**  $T^*$   
**output:**  $\Theta^*$

```

1   $y_0 \leftarrow \{\{x_0\}\}$ , VISITED  $\leftarrow \{y_0\}$ ,  $\text{DOM}(\Theta^*) \leftarrow \emptyset$ ;
2  if  $y_0$  is not in  $T^*$  then
3  |   return “no solution”;
4  DoDFS( $\Theta^*$ ,  $y_0$ );
5  return  $\Theta^*$ ;

procedure DoDFS( $\Theta^*$ ,  $y$ );
6  choose a macro-control-decision  $d \in C_{T^*}(y)$ ;
7  for  $m \in y$  do
8  |    $\text{DOM}(\Theta^*) \leftarrow \text{DOM}(\Theta^*) \cup \{(m, y)\}$ ;
9  |    $\Theta^*(m, y) \leftarrow \Gamma_{m,d}$ , where  $\Gamma_{m,d}$  is the unique
   |   decision such that  $(m, \Gamma_{m,d}) \in d$ ;
10 for  $\sigma \in \Sigma_o$  such that  $h_{ZY}(h_{YZ}(y, d), \sigma) = y'$  do
   |   if  $y' \notin \text{VISITED}$  then
11 |   |   VISITED  $\leftarrow \text{VISITED} \cup \{y'\}$ ;
12 |   |   DoDFS( $\Theta^*$ ,  $y'$ );
```

---

the set of all macro-control-decisions defined at  $y$ . Then for each pair  $(m, y)$ , where  $m \in y$ , we use  $d$  to define the mapping value for information-state  $(m, y)$ , which is the unique non-deterministic decision set associated with  $m$  in  $d$ . Then we move to the unique  $Z$ -state reached under macro-control-decision  $d$  and consider all successor  $Y$ -states by considering all possible observable events. If the new  $Y$ -state has not yet been visited, then we repeat the selection procedure by making a recursive call of procedure DoDFS until all reachable information-states are traversed. The computed IS-mapping  $\Theta^*$  is reachability-closed by construction; hence can be used to decode a corresponding IS-based supervisor  $S_{\Theta^*}$  according to Algorithm 1.

We show the computation procedure in Algorithm 2 by the following example.

**Example 6.** We still consider our running example with  $T^*$  shown in Figure 2 and we use Algorithm 2 to synthesize an IS-mapping from  $T^*$ . The algorithm starts from the initial  $Y$ -state  $s_1 = \{\{0\}\}$ , at which the macro-control-decision in  $T^*$  is unique. Therefore, the supervisor will pick  $d_5$  which induces partial mapping value  $\Theta^*(\{0\}, \{\{0\}\}) = \{\gamma_2, \gamma_3\}$ . By choosing  $d_5$ , we move to  $Z$ -state  $s_{10}$  and we need to consider all possible successor  $Y$ -state of  $s_{10}$ . Here, both  $o_1$  and  $o_1$  from  $s_{10}$  leads to  $Y$ -state  $s_{18} = \{\{4\}, \{5\}\}$ , where three macro-control-decisions  $d_9, d_{10}$  and  $d_{11}$  are defined. Suppose that the supervisor chooses  $d_{11} = \{(\{4\}, \{\gamma_1\}), (\{5\}, \{\gamma_4\})\}$ . This again induces partial mapping values  $\Theta^*(\{4\}, \{\{4\}, \{5\}\}) = \{\gamma_1\}$  and  $\Theta^*(\{5\}, \{\{4\}, \{5\}\}) = \{\gamma_4\}$ . If observable event  $o_2$  occurs,  $Y$ -state  $s_{29}$  is reachable and the macro-control-decision defined is unique. Therefore, by choosing  $d_{19}$  at  $s_{29} = \{\{10, 11\}\}$ , partial mapping value  $\Theta^*(\{10, 11\}, \{\{10, 11\}\}) = \{\gamma_1\}$  is induced. If observable event  $o_1$  occurs,  $Y$ -state  $s_{31}$  is reachable and the macro-control-decision defined is  $d_{20}$ . Partial mapping value

$\Theta^*(\{9, 10\}, \{\{9, 10\}\}) = \{\gamma_1\}$  is induced. This completes the construction of reachability-closed IS-mapping  $\Theta^*$ , which can also be represented as the decision diagram shown in Figure 2(b).

**Remark 3.** The main purpose of this paper is to synthesize a non-deterministic supervisor that guarantees opacity. Our focus is the solvability of this problem and whether or not the synthesized solution is maximally-permissive is out of the main scope of this work. Here, we provide a heuristic approach to improve the permissiveness of this solution. In line 6 of Algorithm 2, we do not put specific criterion for which macro-control-decision to choose from  $C_{T^*}(y)$ . To enhance the permissiveness of the supervisor, we can pick a *locally maximal* macro-control-decision at each  $Y$ -state. Formally, given two non-deterministic decision sets  $\Gamma_1$  and  $\Gamma_2$ , we denote

- by  $\Gamma_1 \leq \Gamma_2$  if  $\forall \gamma \in \Gamma_1, \exists \gamma' \in \Gamma_2 : \gamma \subseteq \gamma'$ ; and
- by  $\Gamma_1 < \Gamma_2$  if  $\Gamma_1 \leq \Gamma_2$  and  $\exists \gamma \in \Gamma_1, \exists \gamma' \in \Gamma_2 : \gamma \subset \gamma'$ .

Then for each  $Y$ -state  $y = \{m_1, \dots, m_k\}$  in  $T^*$  and two macro-control-decisions  $d_1$  and  $d_2$  defined at  $y$ , where  $d_1 = \{(m_1, \Gamma_1), \dots, (m_k, \Gamma_k)\}$ ,  $d_2 = \{(m_1, \Gamma'_1), \dots, (m_k, \Gamma'_k)\}$ , we say  $d_2$  is more permissive than  $d_1$ , denoted by  $d_1 < d_2$  if

- $\forall i \in \{1, \dots, k\}, \Gamma_i \leq \Gamma'_i$ ; and
- $\exists i \in \{1, \dots, k\}, \Gamma_i < \Gamma'_i$ .

Therefore, in line 6 of Algorithm 2, one can choose a locally maximal macro-control-decision  $d \in C_{T^*}(y)$  in the sense of

$$\forall d' \in C_{T^*}(y) : d \not< d'.$$

For example, for  $T^*$  in Figure 2(a), there are three macro-control-decisions  $d_9 = \{(\{4\}, \{\gamma_1\}), (\{5\}, \{\gamma_1\})\}$ ,  $d_{10} = \{(\{4\}, \{\gamma_1\}), (\{5\}, \{\gamma_2, \gamma_3\})\}$  and  $d_{11} = \{(\{4\}, \{\gamma_1\}), (\{5\}, \{\gamma_4\})\}$  defined at  $s_{10}$ . Then  $d_{11}$  is a locally maximally macro-control-decision among these three. For example, we have  $d_{10} < d_{11}$  since  $\gamma_2 \subset \gamma_4$  and  $\gamma_3 \subset \gamma_4$ . Therefore, for the sake of permissiveness, the IS-mapping synthesis procedure can pick  $d_{11}$  instead of  $s_9$  or  $s_{10}$ .

## VI. PROPERTIES OF THE SYNTHESIS PROCEDURE

In this section, we formally prove the correctness of the synthesis procedure proposed in Section V. Note that in the formulation of Problem 1, supervisors make control decision based on the decision histories and can be non-IS-based in general. However, our algorithm in Section V solves a restricted version of Problem 1 by only considering IS-based supervisors as formulated in Problem 2. Therefore, to show the correctness of the proposed synthesis procedure in the context of Problem 1, our arguments consist of the following two steps:

- first, we show that our solution to the IS-based synthesis problem, i.e., Problem 2, is sound and complete;
- then we show that restricting Problem 1 to Problem 2 is without loss of generality, i.e., Problem 1 is solvable if and only if Problem 2 is solvable.

Throughout this section, we denote by  $S_{\Theta^*}$  the IS-based supervisor synthesized by Algorithm 2.

### A. Correctness of the IS-Based Synthesis Algorithm

In this subsection, we show that Algorithm 2 indeed solves Problem 2. First, we show that Algorithm 2 is sound in the sense that the synthesized supervisor  $S_{\Theta^*}$  is opacity-enforcing.

**Theorem 2.** *IS-based non-deterministic supervisor  $S_{\Theta^*} : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  encoded from  $\Theta^*$  enforces opacity.*

*Proof.* Let  $s = \sigma_1 \cdots \sigma_n \in P(\mathcal{L}(S_{\Theta^*}/G))$  be any observable string in closed-loop system  $S_{\Theta^*}/G$ . Let  $\mathbf{m}_n^+$  be state induced by  $s$  and IS-mapping  $\Theta^*$  according to Equation (19). By Corollary 1, we know that  $\bigcup M(\mathbf{m}_n^+) = X_I(s)$ . According to Algorithm 2,  $\mathbf{m}_n^+$  is a reachable  $Z$ -state in  $T^*$  by construction. Furthermore, since  $T^*$  is obtained from  $T_0$  where all  $Z$ -states in  $Q_{\text{reveal}}$  are removed. Therefore, we conclude that

$$X_I(s) = \bigcup M(\mathbf{m}^+) \not\subseteq X_S,$$

which means that  $\Theta^*$  enforces opacity.  $\square$

Note that Algorithm 2 returns “no solution” when  $y_0$  is not included in  $T^*$ . Next, we show that Algorithm 2 is also complete in the sense that there is indeed no solution to Problem 2 when  $y_0$  is removed by operator  $F$  during the construction of  $T^*$ .

**Theorem 3.** *If there exists a non-deterministic IS-based supervisor that enforces opacity, then  $y_0$  must be included in  $T^*$ , i.e., Algorithm 2 will not return “no solution” when a solution to Problem 2 exists.*

*Proof.* Suppose that there exists a reachability-closed IS-mapping  $\Theta : I \rightarrow 2^\Gamma$  such that the encoded non-deterministic supervisor  $S_\Theta$  enforces opacity. We construct a consistent G-BTS  $T = (Q_Y, Q_Z, h_{YZ}, h_{ZY}, \Sigma_o, D, y_0)$  as follows:  $Q_Y = \mathcal{I}_{S_\Theta}$  and for any  $y \in Q_Y$ ,  $d = \{(m, \Theta(m, y)) : m \in y\}$  is the unique macro-control-decision defined at  $y$  and  $Q_Z = \{\odot(d) : \exists y \in Q_Y \text{ s.t. } h_{YZ}(y, d)!\}$ . Since  $S_\Theta$  enforces opacity, we have  $\forall s \in P(\mathcal{L}(S_\Theta/G)) : X_I(s) \not\subseteq X_S$ . Let  $\mathbf{m}_n^+$  be state induced by  $s$  and IS-mapping  $\Theta$  according to Equation (19). By the construction of  $T$ , we have  $\mathbf{m}_n^+ \in Q_Z$ . By Corollary 1, we know that  $\bigcup M(\mathbf{m}_n^+) = X_I(s)$ . Therefore, we have  $Q_Z \cap Q_{\text{reveal}} = \emptyset$ . Since  $T$  is included in  $T_0$  and  $T$  itself is consistent, no states in  $T$  can be removed when iteratively applying operator  $F$ , which means that all states in  $T$  are also included in  $T^*$ . Therefore, the initial  $Y$ -state  $y_0$  is included in  $T^*$  and Algorithm 2 will not return “no solution”.  $\square$

### B. From Non-IS-Based Supervisors to IS-Based Supervisors

So far, we have shown that Algorithm 2 correctly solves Problem 2, which is a restrictive version of Problem 1. Clearly, Algorithm 2 is also sound for Problem 1 because an IS-based solution is also a solution to Problem 1. Then it remains to show the completeness of Algorithm 2 in terms of Problem 1. To this end, it suffices to show that Problem 2 always has a solution when Problem 1 has one. Here, we provide a constructive procedure that always construct an IS-based opacity-enforcing supervisor that solves Problem 2 when a non-IS-based one that solves Problem 1 exists.

Suppose that there exists a (possibly non-IS-based) non-deterministic supervisor  $S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  that enforces opacity. We construct an IS-mapping  $\Theta$  according to Algorithm 3. The idea is similar to the information-flow analysis for IS-mapping, which expands the information-state space from the initial information state. We still use  $y$  to denote state-estimates immediately after an observable event and use  $z$  to denote state-estimates with the unobservable tail included. However, since the supervisor needs not to be IS-based, simply remembering the current information-state is not sufficient and we also need to remember the history leading to each state estimate. Therefore, for each micro-state  $m_i$  in a  $Y$ -state, we add an additional information  $\rho_i$  to track how this micro-state is visited. Note that for each micro-state  $m$  in a  $Y$ -state, the decision history may not be unique since there may have multiple  $\rho$  associated with the same  $m$ . Similarly, each augmented micro-state in a  $Z$ -state is also attached with a decision history information. Then procedure DoDSF implements a depth-first search to generate the domain of the IS-mapping. Note that, since  $S_N$  is not IS-based in general, it may take different actions for different histories visiting the same information-state. Our approach is to fix the control decision for each information-state as the union of the decisions for all its visits; the constructed mapping is, therefore, forced to be IS-based. Algorithm 3 clearly terminates in a finite number of states since it will stop when all possible macro-states are visited.

The following result shows that Algorithm 3 indeed converts a non-IS-based opacity-enforcing supervisor into an IS-based opacity-enforcing supervisor.

**Theorem 4.** *Let  $S_N : (\Gamma\Sigma_o)^* \rightarrow 2^\Gamma$  be a non-deterministic supervisor enforcing opacity and  $\Theta : I \rightarrow 2^\Gamma$  be the partial IS-mapping constructed by Algorithm 3. Then IS-based supervisor  $S_\Theta$  also enforces opacity.*

*Proof.* First, by construction, for each macro-state ( $Y$ -state without the extended strings components) visited by IS-mapping  $\Theta$ , i.e.,  $\mathbf{m} = \{m_1, \dots, m_k\} \in \text{VISITED}$ , IS-mapping  $\Theta$  defines a non-deterministic control decision for each micro-state  $m_i \in \mathbf{m}$  (lines 9-10). Also, for each  $Z$ -state reached by  $S_\Theta$ , every possible observable events are defined (line 14). Therefore, for every information-state  $(m, \mathbf{m}) \in \text{REACH}_\Theta(\{\{x_0\}, \{\{x_0\}\}\})$ ,  $\Theta(m, \mathbf{m})$  is always well-defined, i.e., IS-mapping  $\Theta$  is reachability-closed. Therefore, its decoded IS-based supervisor  $S_\Theta$  is well-defined and we have

$$\mathcal{I}_{S_\Theta} = \text{REACH}_\Theta(v_0) = \text{DOM}(\Theta),$$

where  $v_0 = (\{x_0\}, \{\{x_0\}\})$ .

By Corollary 1 and Proposition 1, to show that  $S_\Theta$  enforces opacity, it suffices to show that

$$\forall (m, \mathbf{m}) \in \text{DOM}(\Theta) : \bigcup M(\odot(d_\Theta(\mathbf{m}))) \not\subseteq X_S.$$

To this end, we consider how  $\mathbf{m}$  is added. Suppose  $y_0 y_1 \dots y_n$  is the sequence of  $Y$ -states in the depth-first search such that  $y_n$  contributes  $\mathbf{m}$  to  $\text{VISITED}$ , and let  $s = \sigma_1 \dots \sigma_n$  be the observable events along this sequence. More clearly,

**Algorithm 3:** Construction of IS-Mapping  $\Theta$  from  $S_N$ 


---

**input :**  $S_N$   
**output:**  $\Theta$

```

1   $\rho \leftarrow \epsilon, m \leftarrow \{x_0\}, \text{VISITED} \leftarrow \{\{m\}\};$ 
2   $y \leftarrow \{(m, \epsilon)\};$ 
3  DoDFS( $y, \text{VISITED}$ );
4  return  $\Theta$ ;

procedure DoDFS( $y, \text{VISITED}$ );
5   $z \leftarrow \emptyset$ ;
6  Suppose  $y = \{(m_1, \rho_1), \dots, (m_k, \rho_k)\};$ 
7   $\mathbf{m} \leftarrow \{m_1, \dots, m_k\};$ 
8  for  $i = 1, \dots, k$  do
9     $\text{DOM}(\Theta) \leftarrow \text{DOM}(\Theta) \cup \{(m_i, \mathbf{m})\};$ 
10    $\Theta(m_i, \mathbf{m}) \leftarrow \bigcup \{S_N(\rho) : (m_i, \rho) \in Y\};$ 
11   for  $\gamma \in S_N(\rho_i)$  do
12      $z \leftarrow z \cup \{(UR_\gamma(m_i), \rho_i \gamma, \gamma)\};$ 

13  Suppose  $z = \{(m_1, \rho_1, \gamma_1), \dots, (m_p, \rho_p, \gamma_p)\};$ 
14  for  $\sigma \in \Sigma_o$  do
15     $y' \leftarrow \emptyset$ ;
16    for  $i = 1, \dots, p$  do
17       $y' \leftarrow y' \cup \{(NX_\sigma(m_i), \rho_i \sigma)\};$ 
18    if  $\{m : (m, \rho) \in y'\} \notin \text{VISITED}$  then
19       $\text{VISITED} \leftarrow \text{VISITED} \cup \{m : (m, \rho) \in y'\};$ 
20      DoDFS( $y'$ );
```

---

suppose that  $y_n = \{(m_1, \rho_1), \dots, (m_k, \rho_k)\}$  and we have  $\{m_1, \dots, m_k\} = \mathbf{m}$ . We claim that for  $y_n$ , we have

$$y_n = \{(\hat{\mathcal{E}}_S(\rho), \rho) : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)), \rho|_\Sigma = s\}$$

This claim can be seen inductively by the length of  $s$ . For  $|s| = 0$ , we have  $y_0 = \{(\{x_0\}, \epsilon)\}$ , where  $\epsilon$  is the unique string in  $\mathcal{O}(\mathcal{L}_e^o(S_N/G))$  whose projection is also  $\epsilon$  and  $\hat{\mathcal{E}}_S(\rho) = \{x_0\}$ . Assume that this claim holds for  $|s| = k$ , then for the case of  $s\sigma_{k+1}$ , according to lines 11-12 and lines 16-17, we have

$$\begin{aligned} y_{k+1} &= \left\{ \begin{array}{l} (NX_{\sigma_{k+1}}(UR_\gamma(m)), \rho\gamma\sigma_{k+1}) : \\ (m, \rho) \in y_k, \gamma \in S_N(\rho), \sigma_{k+1} \in \gamma \end{array} \right\} \\ &= \left\{ \begin{array}{l} (\hat{\mathcal{E}}_S(\rho'), \rho') : \\ \rho' \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)), \rho'|_\Sigma = \sigma_1 \dots \sigma_k \sigma_{k+1} \end{array} \right\} \end{aligned}$$

Now, still for the same  $\mathbf{m}$  and string  $s$  leading to it. We have

$$\begin{aligned} &M(\odot(d_\Theta(\mathbf{m}))) \\ &= \{UR_\gamma(m) \in 2^X : (m, \Gamma) \in d_\Theta(\mathbf{m}), \gamma \in \Gamma\} \\ &= \{UR_\gamma(\hat{\mathcal{E}}_S(\rho)) \in 2^X : \rho \in \mathcal{O}(\mathcal{L}_e^o(S_N/G)), \rho|_\Sigma = s, \gamma \in S_N(\rho)\} \\ &= \{\mathcal{E}_S(\rho) \in 2^X : \rho \in \mathcal{O}(\mathcal{L}_e^d(S_N/G)) \text{ s.t. } \rho|_\Sigma = s\} \\ &= \mathcal{E}_I(s) \end{aligned}$$

Since  $S_N$  enforces opacity, we have  $\bigcup \mathcal{E}_I(s) = X_I(s) \not\subseteq X_S$ , which means that  $\bigcup M(\odot(d_\Theta(\mathbf{m}))) \not\subseteq X_S$ . This completes the proof.  $\square$

By combining Theorems 2-4, we have the following result immediately that finally establishes the correctness of the synthesis procedure.

**Corollary 2.** *Algorithm 2 also correctly solves Problem 1, i.e., it is both sound and complete.*

## VII. CONCLUSION

In this paper, we proposed to use non-deterministic control mechanism to enforce opacity. The essence is to leverage the non-deterministic mechanism to enhance the plausible deniability of the system. To this end, we formally defined the non-deterministic supervisor and formulated the corresponding opacity enforcement problem. Effective approach was provided to synthesize a non-deterministic opacity-enforcing supervisor based on both the information of the supervisor and the information of the intruder. We showed that the proposed algorithm is both sound and complete in the sense that it will correctly return a non-deterministic opacity-enforcing supervisor when one exists. In particular, we showed that nondeterministic supervisors are more powerful in terms of opacity enforcement since they may successfully enforce opacity even when deterministic supervisors fail to do so.

## REFERENCES

- [1] L. An and G.-H. Yang. Opacity enforcement for confidential robust control in linear cyber-physical systems. *IEEE Transactions on Automatic Control*, 65(3):1234–1241, 2020.
- [2] E. Badouel, M. Bednarczyk, A. Borzyszkowski, B. Caillaud, and P. Darondeau. Concurrent secrets. *Discrete Event Dynamic Systems*, 17(4):425–446, 2007.
- [3] R.J. Barcelos and J.C. Basilio. Enforcing current-state opacity through shuffle in event observations. *IFAC-PapersOnLine*, 51(7):100–105, 2018.
- [4] B. Behinaein, F. Lin, and K. Rudie. Optimal information release for mixed opacity in discrete-event systems. *IEEE Transactions on Automation Science and Engineering*, 16(4):1960–1970, 2019.
- [5] J.W. Bryans, M. Koutny, L. Mazaré, and P. Ryan. Opacity generalised to transition systems. *International Journal of Information Security*, 7(6):421–435, 2008.
- [6] C.G. Cassandras and S. Lafortune. *Introduction to Discrete Event Systems*. Springer, 2nd edition, 2008.
- [7] F. Cassez, J. Dubreil, and H. Marchand. Synthesis of opaque systems with static and dynamic masks. *Formal Methods in System Design*, 40(1):88–115, 2012.
- [8] J. Chen, M. Ibrahim, and R. Kumar. Quantification of secrecy in partially observed stochastic discrete event systems. *IEEE Trans. Automation Science and Engineering*, 14(1):185–195, 2017.
- [9] P. Darondeau, H. Marchand, and L. Ricker. Enforcing opacity of regular predicates on modal transition systems. *Discrete Event Dynamic Systems*, 25(1-2):251–270, 2014.
- [10] J. Dubreil, P. Darondeau, and H. Marchand. Supervisory control for opacity. *IEEE Trans. Automatic Control*, 55(5):1089–1100, 2010.
- [11] M. Fabian and B. Lennartson. On non-deterministic supervisory control. In *35th IEEE Conference on Decision and Control*.
- [12] Y. Falcone and H. Marchand. Enforcement and validation (at runtime) of various notions of opacity. *Discrete Event Dynamic Systems*, 25(4):531–570, 2015.
- [13] H. Farhat. Control of nondeterministic systems for bisimulation equivalence under partial information. *IEEE Transactions on Automatic Control*, 2020.
- [14] E. Gradel and W. Thomas. *Automata, logics, and infinite games: a guide to current research*, volume 2500. Springer Science & Business Media, 2002.
- [15] C.N. Hadjicostis. *Estimation and Inference in Discrete Event Systems*. Springer, 2020.
- [16] K. Inan. Nondeterministic supervision under partial observations. In *11th Int. Conf. Analysis and Optim. Systems Discrete Event Systems*, pages 39–48, 1994.
- [17] R. Jacob, J.-J. Lesage, and J.-M. Faure. Overview of discrete event systems opacity: Models, validation, and quantification. *Annual Rev. Control*, 41:135–146, 2016.
- [18] Y. Ji, Y.-C. Wu, and S. Lafortune. Enforcement of opacity by public and private insertion functions. *Automatica*, 93:369–378, 2018.

- [19] C. Keroglou and C.N. Hadjicostis. Probabilistic system opacity in discrete event systems. *Discrete Event Dynamic Systems*, pages 1–26, 2017.
- [20] C. Keroglou, L. Ricker, and S. Lafortune. Insertion functions with memory for opacity enforcement. *IFAC-PapersOnLine*, 51(7):394–399, 2018.
- [21] R. Kumar, S. Jiang, C. Zhou, and W. Qiu. Polynomial synthesis of supervisor for partially observed discrete-event systems by allowing nondeterminism in control. *IEEE Trans. Automatic Control*, 50(4):463–475, 2005.
- [22] S. Lafortune, F. Lin, and C.N. Hadjicostis. On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control*, 45:257–266, 2018.
- [23] D. Lefebvre and C.N. Hadjicostis. Exposure time as a measure of opacity in timed discrete event systems. In *18th European Control Conference (ECC)*, pages 1740–1745, 2019.
- [24] F. Lin. Opacity of discrete event systems and its applications. *Automatica*, 47(3):496–503, 2011.
- [25] F. Lin, W. Chen, W. Wang, and F. Wang. Information control in networked discrete event systems and its application to battery management systems. *Discrete Event Dynamic Systems*, pages 1–26, 2020.
- [26] R. Liu, L. Mei, and J. Lu.  $K$ -memory-embedded insertion mechanism for opacity enforcement. *Systems & Control Letters*, 145:104785, 2020.
- [27] S. Liu and M. Zamani. Compositional synthesis of opacity-preserving finite abstractions for interconnected systems. *arXiv preprint:2004.00131*, 2020.
- [28] L. Mazaré. Using unification for opacity properties. In *Workshop on Issues in the Theory of Security*, volume 4, pages 165–176, 2004.
- [29] 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*, 65(8):3349–3364, 2020.
- [30] S. Mohajerani and S. Lafortune. Transforming opacity verification to nonblocking verification in modular systems. *IEEE Transactions on Automatic Control*, 65(4):1739–1746, 2020.
- [31] M. Noori-Hosseini, B. Lennartson, and C.N. Hadjicostis. Compositional visible bisimulation abstraction applied to opacity verification. *IFAC-PapersOnLine*, 51(7):434–441, 2018.
- [32] B. Ramasubramanian, W.R. Cleaveland, and S. Marcus. Notions of centralized and decentralized opacity in linear systems. *IEEE Transactions on Automatic Control*, 265(4):1442–1455, 2020.
- [33] I. Saadaoui, Z. Li, and N. Wu. Current-state opacity modelling and verification in partially observed petri nets. *Automatica*, 116:108907, 2020.
- [34] A. Saboori and C.N. Hadjicostis. Opacity-enforcing supervisory strategies via state estimator constructions. *IEEE Trans. Automatic Control*, 57(5):1155–1165, 2011.
- [45] Y. Yao, Y. Tong, and H. Lan. Initial-state estimation of multi-channel networked discrete event systems. *IEEE Control Systems Letters*, 2020.
- [35] A. Saboori and C.N. Hadjicostis. Verification of initial-state opacity in security applications of discrete event systems. *Information Sciences*, 246:115–132, 2013.
- [36] S. Takai. Bisimilarity enforcing supervisory control of nondeterministic discrete event systems with nondeterministic specifications. *Automatica*, 108:108470, 2019.
- [37] S. Takai. Synthesis of maximally permissive supervisors for nondeterministic discrete event systems with nondeterministic specifications. *IEEE Transactions on Automatic Control*, 2020.
- [38] S. Takai and Y. Oka. A formula for the supremal controllable and opaque sublanguage arising in supervisory control. *SICE J. Control, Measu. & Syst. Integration*, 1(4):307–311, 2008.
- [39] Y. Tong, Z. Li, C. Seatzu, and A. Giua. Verification of state-based opacity using Petri nets. *IEEE Trans. Automatic Control*, 62(6):2823–2837, 2017.
- [40] Y. Tong, Z. Li, C. Seatzu, and A. Giua. Current-state opacity enforcement in discrete event systems under incomparable observations. *Discrete Event Dynamic Systems*, 28(2):161–182, 2018.
- [41] L. Wang, N. Zhan, and J. An. The opacity of real-time automata. *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, 37(11):2845–2856, 2018.
- [42] B. Wu, J. Dai, and H. Lin. Synthesis of insertion functions to enforce decentralized and joint opacity properties of discrete-event systems. In *American Control Conference (ACC)*, pages 3026–3031. IEEE, 2018.
- [43] B. Wu and H. Lin. Privacy verification and enforcement via belief abstraction. *IEEE Control Systems Letters*, 2(4):815–820, 2018.
- [44] Y. Xie, X. Yin, and S. Li. Opacity enforcing supervisory control using non-deterministic supervisors. In *21st IFAC World Congress*, 2020.
- [46] X. Yin and S. Lafortune. A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems. *IEEE Transactions on Automatic Control*, 61(8):2140–2154, 2016.
- [47] X. Yin and S. Lafortune. A new approach for the verification of infinite-step and  $k$ -step opacity using two-way observers. *Automatica*, 80:162–171, 2017.
- [48] X. Yin, Z. Li, W. Wang, and S. Li. Infinite-step opacity and  $K$ -step opacity of stochastic discrete-event systems. *Automatica*, 99:266–274, 2019.
- [49] X. Yin, M. Zamani, and S. Liu. On approximate opacity of cyber-physical system. *IEEE Transactions on Automatic Control*, 2020.
- [50] B. Zhang, S. Shu, and F. Lin. Maximum information release while ensuring opacity in discrete event systems. *IEEE Trans. Automation Science and Engineering*, 12(4):1067–1079, 2015.
- [51] C. Zhou, R. Kumar, and S. Jiang. Control of nondeterministic discrete-event systems for bisimulation equivalence. *IEEE Transactions on Automatic Control*, 51(5):754–765, 2006.
- [52] G. Zinck, L. Ricker, H. Marchand, and L. Héluët. Enforcing opacity in modular systems. In *IFAC World Congress*, 2020.