2015 IEEE 54th Annual Conference on Decision and Control (CDC)
December 15-18, 2015. Osaka, Japan

A General Approach for Solving Dynamic Sensor Activation Problems for a Class of Properties

Xiang Yin and Stéphane Lafortune

Abstract— **We study the problem of dynamic sensor activation for centralized partially-observed discrete event systems. The sensors can be turned on/off online dynamically according to a sensor activation policy in order to satisfy some observation property. In this paper, we consider a general class of properties, called Information-State-based (or IS-based) properties, which include, but are not limited to, observability, K-diagnosability, predictability, and opacity. We define a new Most Permissive Observer (MPO) that generalizes previous versions of this structure. The MPO that we define embeds all sensor activation policies for an IS-based property. An optimal sensor activation policy can then be synthesized based on the MPO. Our results generalize the previous works on dynamic sensor activation for enforcing the properties of observability, K-diagnosability, and opacity. Moreover, our MPO is applicable to solving dynamic sensor activation problems for a wide class of user-defined properties that can be formulated as IS-based properties. As a special case, we show that the problem of minimal sensor activation for enforcing predictability, which has not been considered in the literature, is solvable by our new approach.**

I. Introduction

The problem under consideration in this paper is that of dynamic sensor activation in partially-observed Discrete Event Systems (DES). The objective in this problem is to synthesize a sensor activation policy that dynamically turns sensors on/off online in order to achieve a given objective, e.g., to control the system or to diagnose faults.

Dynamic sensor activation has been studied extensively in the DES literature; see, e.g., [1]–[10] for a sample of this work and the recent survey paper [11] for an extensive bibliography. In [1], [2], the problem of dynamic sensor activation for the purpose of fault diagnosis was studied; the optimal synthesis problems considered therein were solved according to numerical cost criteria. In [4], [5], both centralized and decentralized sensor activation problems for the purposes of control and diagnosis, respectively, were studied. The features of these works are: (i) the properties of interest to be enforced are (co)observability or (co)diagnosability; (ii) the optimality criterion is logical; and (iii) the solutions are only sub-optimal in the sense that by enlarging the solution space, better solutions could be obtained in principle.

In [2], a structure called the *Most Permissive Observer* (MPO) was proposed for solving the problem of dynamic sensor activation for the purpose of fault diagnosis. Roughly speaking, the MPO is a finite structure that embeds all valid sensor activation policies, i.e., all policies that enforce the property of K-diagnosability. Therefore, the MPO can serve as a basis for finding one optimal solution w.r.t. some cost criterion. This approach was extended to timed systems in [12] and to the problem of opacity in [6]. Recently, an information-state-based characterization of the MPO structure was proposed in [10]; this work showed that the size complexity of the MPO could be reduced, as compared with the original MPO from [2], by appropriately defining the notion of information state in the context of enforcement of K-diagnosability.

In this paper, we use the MPO approach to investigate the sensor activation problem for centralized partially-observed DES. However, instead of investigating the enforcement of a particular property, e.g., observability, diagnosability, or opacity, as was done in previous works, we study a general class of properties called Information-State-based (IS-based) properties, that captures all properties previously considered, and more. Specifically, as will be demonstrated in the paper, our contributions are as follows.

(1) We formulate the problem of dynamic sensor activation for any property that can be expressed as an IS-based property. We show that this problem formulation is more general than both the state disambiguation problem and the opacity problem that have been studied previously in the literature. To solve this problem, we define a generalized version of the most permissive observer, which embeds all valid solutions to the enforcement of an IS-based property in its finite structure. Based on the MPO, we present an algorithm for the synthesis of optimal sensor activation policies under a logical performance objective.

(2) Compared with prior works where the MPO was employed [2], [6], [10], our contributions are twofold. First, we define the MPO directly from the new notion of bipartite dynamic observer without using the recursive definition used in [10]. Second, the MPO defined in this paper is more general since we consider a general class of properties and we show that the most permissive observer for K-diagnosability studied by [2], [10] and the most permissive dynamic mask for opacity studied by [6] are essentially special cases of the generalized MPO. Moreover, the problem of optimal sensor activation for predictability, which to the best of our knowledge has not been considered in the literature, can also be solved by our approach. Similarly, our approach can be employed to solve sensor activation problems for the enforcement of a wide class of *user-defined* properties that can be expressed as IS-based properties; see, e.g., [13].

(3) Compared with other solution approaches for dynamic

This work was partially supported by NSF grants CCF-1138860 (Expeditions in Computing project ExCAPE: Expeditions in Computer Augmented Program Engineering), CNS-1421122, and CNS-1446298.

Xiang Yin and Stéphane Lafortune are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA. {xiangyin,stephane}@umich.edu.

978-1-4799-7885-4/15/$31.00 ©2015 IEEE

sensor activation problems, our methodology has the following features. First, the optimal solution that we obtain is language-based. Recall that the solutions obtained by [4], [5] are optimal only w.r.t. finite (restricted) solution spaces, based on the state space of the system model. Moreover, the generalized MPO that we define embeds *all* solutions in its *single* finite structure. Therefore, it can serve as a basis for optimization w.r.t. a numerical cost criterion, which cannot be done by the online approaches described in [3], [8].

Due to space constraints, all proofs have been omitted.

II. Preliminary and Problem Formulation

A. System Model

The system under consideration is modeled by a deterministic finite state automaton $G=(Q,\Sigma,\delta,q_0)$, where Q is the finite set of states, Σ is the finite set of events, $\delta: Q\times\Sigma\to Q$ is the partial transition function and q_0 is the initial state. The transition function δ is extended to $Q\times\Sigma^*$ in the usual manner (see, e.g., [14]). The language generated by G from state q is defined by $\mathcal{L}(G,q)=\{s\in\Sigma^*:\delta(q,s)!\}$, where ! means "is defined". We write $\mathcal{L}(G,q)$ as $\mathcal{L}(G)$ if $q=q_0$. We denote by $\overline{L}$ the prefix-closure of a language L. We denote by L/s the post-language of L after s. We say a language L is live if $\forall s\in L,\exists\sigma\in\Sigma: s\sigma\in L$.

In dynamic sensor activation problems, the sensors are turned on/off dynamically based on the observation history. When the sensor corresponding to an event $\sigma\in\Sigma$ is turned "on", we say that the event is being *monitored*. While an event is monitored, any occurrence of it will be *observed* by the supervisor, diagnoser, predictor, or external observer, according to the problem under consideration (e.g., control, diagnosis, prediction, or opacification). At any point in the execution of the system, the set of events $\theta\in 2^\Sigma$ that we decide to monitor, is called a *sensing decision*.

We assume that Σ is partitioned into three disjoint sets, $\Sigma=\Sigma_o\dot{\cup}\Sigma_s\dot{\cup}\Sigma_{uo}$, where: (i) Σ_o is the set of events whose occurrences are always observed (ii) Σ_s is the set of events that we can choose to monitor or not and (iii) Σ_{uo} is the set of events that are always unobservable We say that a sensing decision $\theta\in 2^\Sigma$ is *admissible* if $\Sigma_o\subseteq\theta\subseteq\Sigma_o\cup\Sigma_s$ and we let Θ denote the set of all admissible sensing decisions.

Under dynamic sensing decisions, the observations of the system behavior are specified by an *information mapping* $\omega:\mathcal{L}(G)\to\Theta$, where for any $s\in\mathcal{L}(G)$, $\omega(s)$ is the set of events that are monitored after the occurrence of s. Given an information mapping ω, we define the projection $P_\omega:\mathcal{L}(G)\to\Sigma^*$ in the usual manner (see, e.g., [14]). We also define the *state estimator function* (or simply "state estimator") $\mathcal{E}_\omega^G:\mathcal{L}(G)\to 2^Q$ by: for any $s\in\mathcal{L}(G)$, $\mathcal{E}_\omega^G(s) := \{q\in Q:\exists t\in\mathcal{L}(G) \text{ s.t. } P_\omega(s)=P_\omega(t)\wedge\delta(q_0,t)=q\}$.

For the purpose of implementation, we require that the information mapping ω satisfy $\forall s,t\in\mathcal{L}(G): P_\omega(s)=P_\omega(t)\Rightarrow\omega(s)=\omega(t)$. This condition is referred to as the *feasibility* condition in [4], [5]. We say that ω is a *sensor activation policy* if it is feasible and for any $s\in\mathcal{L}(G)$, $\omega(s)$ is admissible, i.e., $\omega(s)\in\Theta$. We use notation Ω to denote the set of all sensor activation policies. Given two sensor activation policies $\omega,\omega'\in\Omega$, we say that ω is *smaller* than ω', denoted by $\omega<\omega'$, if 1) $\forall s\in\mathcal{L}(G):\omega(s)\subseteq\omega'(s)$; and 2) $\exists s\in\mathcal{L}(G):\omega(s)\subset\omega'(s)$.

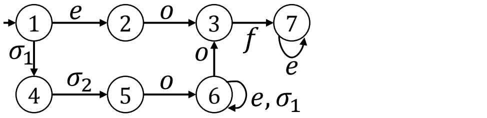


Fig. 1. System G with $\Sigma_o=\{o\}$, $\Sigma_s=\{\sigma_1,\sigma_2\}$, and $\Sigma_{uo}=\{e,f\}$

B. Problem Formulation

As was explained in the introduction, in a given problem domain (control, diagnosis, and so forth), the sensor activation policy must satisfy some problem-dependent *property* (observability, diagnosability, and so forth). For the sake of generality, we define a property φ as a function $\varphi:\Omega\to\{0,1\}$ and for any sensor activation policy $\omega\in\Omega$, we write $\varphi(\omega)=1$ to mean that ω satisfies property φ. The properties of interest are typically defined in a language-based manner. Hereafter, we consider a special class of properties called *information-state-based (IS-based) properties*. These are properties whose verification can be performed over information states of the system state space.

We define an *information state* to be a subset of states in Q and denote by $I=2^Q$ the set of information states. Roughly speaking, an IS-based property is a property that only depends on the *current* knowledge of the system, as provided by the state estimator function $\mathcal{E}_\omega^G$ under a given sensor activation policy ω. In particular, the property should not depend on information about the *future* behavior of the system. We will show later that most of the important properties in the DES literature can be formulated as IS-based properties, possibly after suitable state space refinements of the original model G. First, we present the formal definition of the IS-based property.

Definition 1: (IS-based Property). Let $G=(Q,\Sigma,\delta,q_0)$ be the system automaton and $\omega:\mathcal{L}(G)\to\Theta$ be a sensor activation policy. An IS-based property w.r.t. G is a function $\varphi:2^Q\to\{0,1\}$. We say that ω satisfies φ w.r.t. G, denoted by $\omega\models_G\varphi$, if $\forall s\in\mathcal{L}(G):\varphi(\mathcal{E}_\omega^G(s))=1$.

Example 1: Consider the system G in Fig. 1. Let $\varphi: 2^Q\to\{0,1\}$ be an IS-based property defined as follows:

$$\forall i\in 2^Q:[\varphi(i)=1]\Leftrightarrow[\nexists q\in\{1,4,5,6\}:\{3,q\}\subseteq i] \quad (1)$$

This IS-based property φ requires that we should never confuse state 3 with any state in $\{1,4,5,6\}$.

Let us consider the information mapping ω defined by $\forall s\in\mathcal{L}(G):\omega(s)=\{o\}$. By taking $eo\in\mathcal{L}(G)$, we know that $\mathcal{E}_\omega^G(eo)=\{3,6\}$. Therefore, $\omega\not\models_G\varphi$. ■

As was mentioned earlier, the objective of this paper is to synthesize a sensor activation policy such that some given property provably holds. Since turning sensors on/off can be costly, we define the *Minimal Sensor Activation Problem for IS-Based Properties* as follows.

Problem 1: (Minimal Sensor Activation Problem for IS-Based Properties). Let $G=(Q,\Sigma,\delta,q_0)$ be the system automaton and $\varphi:2^Q\to\{0,1\}$ be an IS-based property w.r.t. G. Find a sensor activation policy $\omega\in\Omega$ such that:

(i) $\omega \models_G \varphi$;

(ii) $\nexists \omega' \in \Omega$ such that $\omega' \models_G \varphi$ and $\omega' < \omega$.

In some contexts, we may be interested in the dual version of the Minimal Sensor Activation Problem, the *Maximal Sensor Activation Problem for IS-Based Properties*. Its definition is analogous, with "<" replaced by ">" in condition (ii).

Remark 1: In [15], the *state disambiguation problem* is defined. Formally, $T_{spec} \subseteq Q \times Q$ is the set of state pairs that need to be distinguished and the goal is to find a minimal $\omega \in \Omega$ such that $(\forall s \in \mathcal{L}(G))(\forall q_1, q_2 \in \mathcal{E}_\omega^G(s))[(q_1, q_2) \notin T_{spec}]$. Clearly, this problem is a special case of the minimal sensor activation problem for IS-based properties, since given T_{spec}, we can always define an IS-based property $\varphi_{spec} : 2^Q \to \{0,1\}$ by: $\forall i \in 2^Q : [\varphi_{spec}(i) = 0] \Leftrightarrow [\exists q_1, q_2 \in i : (q_1, q_2) \in T_{spec}]$. Therefore, the problem we consider here is more general than the state disambiguation problem.

Remark 2: In many cases, the system is not only monitored by its internal controller, but it may also be monitored by an *external* observer that is potentially malicious. Therefore, instead of disambiguating states, the objective is to *confuse* the external observer so that it may not infer a given secret about the system. In such a scenario, the "disablement" of sensors can be costly, since we need to spend some additional effort, e.g., adding a dynamic mask, to hide the occurrences of the corresponding events. In this regard, the optimal dynamic mask synthesis problem investigated in the literature (see, e.g., [6]) is essentially the maximal sensor activation problem defined above.

III. A General Most Permissive Observer

A. Information State Dynamics

A sensor activation policy ω works dynamically as follows. Initially, a sensing decision θ_0 is issued. Then, upon the occurrence of (monitored) event $\sigma_1 \in \theta_0$, a new decision θ_1 is made and so forth. We call such a sequence in the form of $\theta_0\sigma_1\theta_1\sigma_2\ldots$, where $\theta_i \in \Theta, \sigma_{i+1} \in \theta_i, \forall i \geq 0$, a *run*. For any $s \in \mathcal{L}(G)$, suppose that $s = \xi_0\sigma_1\xi_1\sigma_2\ldots\xi_{n-1}\sigma_n\xi_n$, where $\xi_i \in (\Sigma \setminus w(\xi_0\sigma_1\ldots\xi_{i-1}\sigma_i))^*, \forall i \geq 0$ and $\sigma_i \in w(\xi_0\sigma_1\ldots\sigma_{i-1}\xi_{i-1}), \forall i \geq 1$. Then the information available to the sensor activation module upon the occurrence of s is, in fact, the run $\mathcal{R}_\omega(s) := \theta_0\sigma_1\theta_1\ldots\theta_{n-1}\sigma_n\theta_n$, where $\theta_i = \omega(\xi_0\sigma_1\ldots\xi_{i-1}\sigma_i\xi_i), \forall i \geq 0$.

To capture the alternating nature of sensing decisions and observations of monitored events, we define two kinds of states, termed Y-states and Z-states, respectively. A Y-state y is an information state from which a sensing decision is made and $Y \subseteq I$ denotes the set of Y-states. A Z-state z is an information state augmented with a sensing decision from which observations of monitored events occur. $Z \subseteq I \times \Theta$ denotes the set of Z-states and we write $z = (I(z), \Theta(z))$ for any $z \in Z$. Next, we define the transition function from Y-states to Z-states, $h_{YZ} : Y \times \Theta \to Z$, and the transition function from Z-states to Y-states, $h_{ZY} : Z \times \Sigma \to Y$. For any $y \in I, z \in I \times \Theta, \sigma \in \Sigma$ and $\theta \in \Theta$,

- $z = h_{YZ}(y, \theta)$ if and only if
  $I(z) = \{q \in Q : \exists q' \in y, \exists s \in (\Sigma \setminus \theta)^* \text{ s.t. } \delta(q', s) = q\}$
  and $\Theta(z) = \theta$
- $y = h_{ZY}(z, \sigma)$ if and only if
  $\sigma \in \Theta(z)$ and $y = \{q \in Q : \exists q' \in I(z) \text{ s.t. } \delta(q', \sigma) = q\}$

For simplicity hereafter, we write $y \xrightarrow{\theta} z$ if $z = h_{YZ}(y, \theta)$ and $z \xrightarrow{\sigma} y$ if $z = h_{ZY}(z, \sigma)$.

Now, let $s \in \mathcal{L}(G)$ be a string and $\mathcal{R}_\omega(s) = \theta_0\sigma_1\theta_1\ldots\theta_{n-1}\sigma_n\theta_n$ be the corresponding run defined earlier. Let $y_0 = \{q_0\}$ be the initial Y-state. Then occurrence of the run $\theta_0\sigma_1\theta_1\ldots\theta_{n-1}\sigma_n\theta_n$ will reach an alternating sequence of Y- and Z-states

$$y_0 \xrightarrow{\theta_0} z_0 \xrightarrow{\sigma_1} y_1 \xrightarrow{\theta_1} \ldots \xrightarrow{\theta_{n-1}} z_{n-1} \xrightarrow{\sigma_n} y_n \xrightarrow{\theta_n} z_n \quad (2)$$

We denote by $\mathcal{I}_\omega^Y(s)$ and $\mathcal{I}_\omega^Z(s)$, the last Y-state and Z-state in $y_0z_0y_1z_2\ldots z_{n-1}y_nz_n$, respectively, i.e., $\mathcal{I}_\omega^Y(s) = y_n$ and $\mathcal{I}_\omega^Z(s) = z_n$. By induction on the length of $P_\omega(s)$, we have $I(\mathcal{I}_\omega^Z(s)) = \mathcal{E}_\omega^G(s)$, which says that the information state component of $\mathcal{I}_\omega^Z(s)$ is the state estimator of s.

Example 2: Let us return to the system G in Fig. 1. Consider the sensor activation policy ω defined by:

$$\omega(s) = \begin{cases} \{o, \sigma_1\}, & \text{if } s \in \{\epsilon, e\} \\ \{o\}, & \text{otherwise} \end{cases} \quad (3)$$

Let us consider the string $s = \sigma_1\sigma_2$. The corresponding run of s is $\mathcal{R}_\omega(\sigma_1\sigma_2) = \{o, \sigma_1\}\sigma_1\{o\}$ and the corresponding sequence of Y- and Z-states is $\{1\}\xrightarrow{\{o,\sigma_1\}}(\{1,2\},\{o,\sigma_1\})\xrightarrow{\sigma_1}\{4\}\xrightarrow{\{o\}}(\{4,5\},\{o\})$. So we have that $\mathcal{I}_\omega^Y(\sigma_1\sigma_2) = \{4\}$, $\mathcal{I}_\omega^Z(\sigma_1\sigma_2) = (\{4,5\},\{o\})$ and $\mathcal{E}_\omega^G(\sigma_1\sigma_2) = \{4,5\}$. ■

B. Bipartite Dynamic Observer

Recall that the sensor activation policy ω is a function defined over a language domain. For implementation purposes, we need to build a finite representation of the function ω. To this end, we define the bipartite dynamic observer (BDO) that realizes a (set of) sensor activation policy(ies).

Definition 2: A bipartite dynamic observer $\mathcal{O}$ is a 7-tuple

$$\mathcal{O} = (Q_Y^{\mathcal{O}}, Q_Z^{\mathcal{O}}, h_{YZ}^{\mathcal{O}}, h_{ZY}^{\mathcal{O}}, \Sigma, \Theta, y_0) \quad (4)$$

where, $Q_Y^{\mathcal{O}} \subseteq I$ is a set of Y-states, $Q_Z^{\mathcal{O}} \subseteq I \times \Theta$ is a set of Z-states, $h_{YZ}^{\mathcal{O}} : Q_Y^{\mathcal{O}} \times \Theta \to Q_Z^{\mathcal{O}}$ and $h_{ZY}^{\mathcal{O}} : Q_Z^{\mathcal{O}} \times E \to Q_Y^{\mathcal{O}}$ are partial transition functions such that for any $z \in Q_Z^{\mathcal{O}}, y \in Q_Y^{\mathcal{O}}, \theta \in \Theta$ and $\sigma \in \Sigma$, the following conditions hold

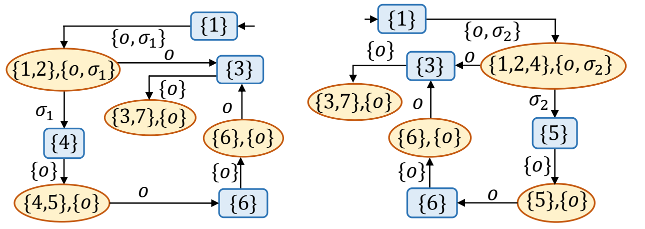
C1. $h_{ZY}^{\mathcal{O}}(z, \sigma) = y \Leftrightarrow h_{ZY}(z, \sigma) = y$;

C2. $h_{YZ}^{\mathcal{O}}(y, \theta) = z \Rightarrow h_{YZ}(y, \theta) = z$;

C3. $\forall y \in Q_Y^{\mathcal{O}}, \exists \theta \in \Theta : h_{YZ}^{\mathcal{O}}(y, \theta)!$.

Σ is the set of events of G, Θ is the set of admissible sensing decisions, and $y_0 = \{q_0\}$ is the initial Y-state. For brevity, we only consider the accessible part of a BDO.

Condition C1 says that the transition function $h_{ZY}^{\mathcal{O}}$ in $\mathcal{O}$ is identical to h_{ZY}. Therefore, for any $z \in Q_Z^{\mathcal{O}}$, $h_{ZY}^{\mathcal{O}}(z, \sigma)$ is defined for any possible observation $\sigma \in \Theta(z)$ by the definition of h_{ZY}. This is due to the fact that we cannot decide which monitored event will occur once we make a sensing decision. Conditions C2 says that for the transition function $h_{YZ}^{\mathcal{O}}$, we have either $h_{YZ}^{\mathcal{O}}(y, \theta) = h_{YZ}(y, \theta)$ or it is undefined. Condition C3 requires that for any Y-state $y \in Q_Y^{\mathcal{O}}$, there exists at least one $\theta \in \Theta$ such that $h_{YZ}^{\mathcal{O}}(y, \theta)$ is



(a) Solution $\mathcal{O}_1$ (b) Solution $\mathcal{O}_2$

Fig. 2. Examples of BDOs that represent two incomparable minimal solutions; [blue] rectangular states and [yellow] oval states represent, respectively, Y-states and Z-states.

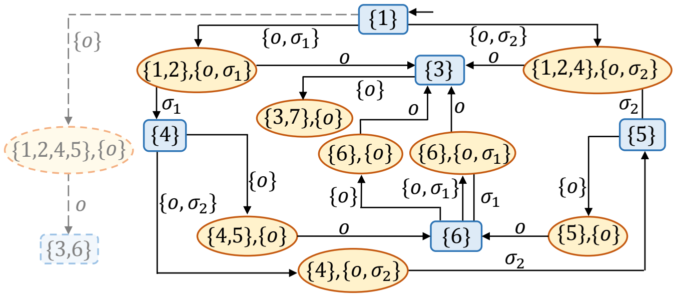


Fig. 3. Example of MPO

defined. This is because a sensor activation policy is defined for all strings in $\mathcal{L}(G)$.

Definition 3: Given a BDO $\mathcal{O}$, we say that a sensor activation policy ω is *allowed* by $\mathcal{O}$ if $\forall s\in\mathcal{L}(G)$: $h_{YZ}^{\mathcal{O}}(\mathcal{I}_\omega^Y(s),\omega(s))!$. With a slight abuse of notation, we write that $\omega\in\mathcal{O}$ whenever ω is allowed by $\mathcal{O}$.

We say that a BDO $\mathcal{O}$ is *deterministic* if, for any $y\in Q_Y^{\mathcal{O}}$, there exists only one $\theta\in\Theta$ such that $h_{YZ}^{\mathcal{O}}(y,\theta)!$. It is clear that a deterministic BDO $\mathcal{O}$ allows a unique sensor activation policy; we denote it by $\omega_{\mathcal{O}}$. In this case, the deterministic BDO $\mathcal{O}$ is essentially a *finite representation* of $\omega_{\mathcal{O}}$.

Example 3: Consider again the system G in Fig. 1. Fig. 2(a) provides an example of a deterministic BDO. For the initial Y-state $y_0=\{1\}$, by making sensing decision $\theta=\{o,\sigma_1\}$, we will reach Z-state $z=(\{1,2\},\{o,\sigma_1\})$. From z, only monitored events o and σ_1 can be observed. If σ_1 is observed, then the next Y-state is $y_1=\{4\}$. We can verify that the sensor activation policy ω defined in Eqn. (3) is allowed by $\mathcal{O}_1$; moreover, it is the only one allowed by $\mathcal{O}_1$ since this BDO is deterministic. Similarly, the BDO $\mathcal{O}_2$ shown in Fig. 2(b) is also deterministic. However, the BDO shown in Fig. 3 is not a deterministic BDO, since there are two sensing decisions defined at Y-state $\{1\}$. ■

C. Generalized MPO and its Properties

We return to the sensor activation problem for IS-based properties, Problem 1, formulation in Section II-B. By condition (i) in Problem 1, we must find an ω such that $\forall s\in\mathcal{L}(G):\varphi(\mathcal{E}_\omega^G(s))=1$. However, for any BDO, we know that $\forall s\in\mathcal{L}(G):I(\mathcal{I}_\omega^Z(s))=\mathcal{E}_\omega^G(s)$ and $\mathcal{I}_\omega^Z(s)$ is indeed the Z-state reached by the run $\mathcal{R}_\omega(s)$ in the BDO. Therefore, if we construct a BDO $\mathcal{O}$ such that $\forall z\in Q_Z^{\mathcal{O}}:\varphi(I(z))=1$ and such that $\mathcal{O}$ is "as large as possible", then the resulting structure will contain all sensor activation policies that satisfy φ. The property of such a BDO being as large as possible is actually well defined: if $\mathcal{O}_1$ and $\mathcal{O}_2$ are two BDOs that both satisfy the above requirement, then their union, in the sense of graph merger, is a BDO that satisfies the above requirement. This observation leads to the definition of the most permissive observer.

```
Data: $G$ and $\varphi$
Result: $\mathcal{MPO}_\varphi$
$Q_Y^{MPO}\leftarrow y_0=\{q_0\}$ and $Q_Z^{MPO}\leftarrow\emptyset$;
DoDFS($y_0,\mathcal{MPO}_\varphi,\varphi$);
while $\exists y\in Q_Y^{MPO}:\nexists\theta\in\Theta$ s.t. $h_{YZ}^{MPO}(y,\theta)!$ do
    $Q_Y^{MPO}\leftarrow Q_Y^{MPO}\setminus\{y\}$;
    remove all $Z$-states $z\in Q_Z^{MPO}$ such that
    $h_{ZY}^{MPO}(z,\sigma)=y$ for some $\sigma\in\Theta(z)$;
    take the accessible part of $\mathcal{MPO}_\varphi$;
procedure DoDFS($y,\mathcal{MPO}_\varphi,\varphi$);
    for $\theta\in\Theta$ do
        $z\leftarrow h_{YZ}(y,\theta)$;
        if $\varphi(I(z))=1$ then
            add transition $y\xrightarrow{\theta}z$ to $h_{YZ}^{MPO}$;
            if $z\notin Q_Z^{MPO}$ then
                $Q_Z^{MPO}\leftarrow Q_Z^{MPO}\cup\{z\}$;
                for $\sigma\in\Sigma$ s.t. $h_{ZY}(z,\sigma)!$ do
                    $y'\leftarrow h_{ZY}(z,\sigma)$;
                    add transition $z\xrightarrow{\sigma}y'$ to $h_{ZY}^{MPO}$;
                    if $y'\notin Q_Y^{MPO}$ then
                        $Q_Y^{MPO}\leftarrow Q_Y^{MPO}\cup\{y'\}$;
                        DoDFS($y',\mathcal{MPO}_\varphi,\varphi$);
```

Algorithm 1: The construction of the MPO

Definition 4: (Most Permissive Observer). Let $G=(Q,\Sigma,\delta,q_0)$ be the system and let $\varphi:2^Q\to\{0,1\}$ be the IS-based property under consideration. The Most Permissive Observer for φ is the BDO

$$\mathcal{MPO}_\varphi=(Q_Y^{MPO},Q_Z^{MPO},h_{YZ}^{MPO},h_{ZY}^{MPO},\Sigma,\Theta,y_0)$$

defined as the largest BDO such that $\forall z\in Q_Z^{MPO}:\varphi(I(z))=1$.

The following theorem reveals the correctness of the MPO defined above, namely, the MPO embeds all sensor activation policies satisfying φ in its structure.

Theorem 1: $\omega\models_G\varphi$ if and only if $\omega\in\mathcal{MPO}_\varphi$.

Algorithm 1 provides a procedure for the construction of the MPO. The steps of Algorithm 1 follow direction from the definition of the MPO. First, we search through the state space of Y-states and Z-states until a Z-state that violates the IS-based property φ is encountered. Then we need to go back to prune such a Y-state and the corresponding Z-states that lead to this state, until the structure converge. The worst-case time complexity of the construction of the MPO is exponential in both $|Q|$ and $|\Sigma_s|$.

Example 4: We return to system G in Fig. 1 and IS-based property φ defined by Equation (1). The corresponding MPO is shown in Fig. 3. At initial Y-state $\{1\}$, if we make sensing decision $\{o\}$, then Y-state $\{3,6\}$ will be reached upon the occurrence of monitored event o (see the dashed lines). However, at state $\{3,6\}$, no matter what sensing decision we make, a Z-state that contains both state 3 and 6 will be reached, which violates the IS-based property φ. Therefore, we need to go back to prune Y-state $\{3,6\}$ and its predecessor Z-state $(\{1,2,4,5\},\{o\})$. This is why we cannot make sensing decision $\{o\}$ at the initial state. ■

Remark 3: In Fig. 3, we can also make sensing decision $\{o,\sigma_1,\sigma_2\}$ at the initial Y-state. However, σ_2 cannot be observed before the next sensing decision is issued, which will occur when either o or σ_1 is observed. Therefore, σ_2 is a "redundant" event in the sensing decision, since it has no effect on future states in the MPO. In this paper, we adopt the following convention. We *remove* all redundant events from sensing decisions in the MPO when solving the *minimal* sensor activation problem. Similarly, we *include* all redundant events to the sensing decisions in the MPO when solving the *maximal* sensor activation problem. Clearly, these conventions will not affect the properties of the MPO.

IV. Synthesis of Optimal Sensor Activation Policies

In this section, we show how to synthesize from the MPO an optimal sensor activation policy ω that solves Problem 1. Specifically, we require that ω satisfy the minimality criterion (ii) of Problem 1 (or the maximality criterion for the dual version of Problem 1). Moreover, we shall also require that ω be defined over a finite domain, so that it can be effectively implemented. To this end, we define a special class of sensor activation policies that are represented by subgraphs of the MPO and thus have finite realizations.

Definition 5: (IS-based Sensor Activation Policy). A sensor activation policy ω is said to be Information-State-based (or IS-based) if $\forall s,t\in\mathcal{L}(G):\mathcal{I}^Y_\omega(s)=\mathcal{I}^Y_\omega(t)\Rightarrow\omega(s)=\omega(t)$.

Clearly, if ω is IS-based, then ω can always be represented by a deterministic BDO that is a subgraph of the MPO.

Definition 6: (Greedy Optimal Sensor Activation Policy). Suppose that ω is a sensor activation policy such that $\omega \models_G \varphi$. We say that ω is *greedy minimal* if

$$\forall s\in\mathcal{L}(G),\forall\theta\in\Theta:h^{MPO}_{YZ}(\mathcal{I}^Y_\omega(s),\theta)!\Rightarrow\theta\not\subset\omega(s) \quad (5)$$

The notion of *greedy maximality* is defined analogously.

The following theorem says that a greedy minimal (respectively, maximal) solution is a minimal (respectively, maximal) solution.

Theorem 2: Let ω be a sensor activation policy such that $\omega\models_G\varphi$. Then ω is minimal (respectively, maximal) if it is greedy minimal (respectively, greedy maximal).

By Theorem 2, it is clear that if we synthesize an IS-based greedy optimal sensor activation policy, then we will have obtained a solution to Problem 1, which was our objective. An IS-based greedy optimal sensor activation policy can be obtained by a depth-first search over the state space of the MPO that picks *one* greedy optimal sensing decision at each Y-state and then picks *all* observations for each Z-state. The resulting structure will be a deterministic BDO representing the solution. We illustrate this procedure by an example.

Example 5: We return to the MPO shown in Fig. 3. To synthesize a minimal sensor activation policy for φ, we can pick decision $\{o,\sigma_1\}$, which is greedy minimal, at the initial Y-state. Then, upon the occurrence of monitored event σ_1, the new Y-state $\{4\}$ is reached. At that state, we pick the unique greedy minimal decision $\{o\}$, and so forth. These choices result in deterministic BDO $\mathcal{O}_1$ shown in Fig. 2(a) that allows the unique sensor activation policy $\omega_{\mathcal{O}_1}$, which is provably minimal. We see that $\omega_{\mathcal{O}_1}$ is, in fact, the sensor activation policy ω defined by Equation (3).

Remark 4: In the synthesis step in th previous example, we could have selected $\{o,\sigma_2\}$ at the initial Y-state, which yields the minimal solution shown in Fig. 2(b). Interestingly, we see that the intersection of the two valid decisions $\{o,\sigma_1\}$ and $\{o,\sigma_2\}$ is not a valid decision, since $\{o\}$ is not defined at Y-state $\{1\}$ in the MPO. This illustrates that Problem 1 may not have an infimal (respectively, supremal) solution in general, but instead several incomparable minimal (respectively maximal) solutions. (This phenomenon is similar to the supervisory control problem under partial observation, in which supremal solutions do not exist in general [16].)

V. Applications of the Generalized MPO

A. Application to Control and Diagnosis

Observability and diagnosability are two key properties of interest in control and diagnosis of DES. It is shown in [15] that the problem of sensor activation for observability can be formulated as a state-disambiguation problem. Similarly, it is shown in [10] that the problem of sensor activation for K-diagnosability can be formulated as a state-disambiguation problem. Therefore, as was discussed in Remark 1, both of these sensor activation problems can be solved by the generalized MPO approach that we have presented. In fact, the most permissive observer for K-diagnosability [2], [10] is a special case of the MPO defined in this paper. Another property of interest in sensor activation is detectability [17]. By using the same approach that is used for the reformulation of K-diagnosability in [10], we can show that strong K-detectability can also be formulated as an IS-based property.

B. Application to Fault Prediction

As a specific example of how the methodology presented in this paper can be used to solve problems that have not yet been addressed in the literature, we consider the problem of sensor activation for the enforcement of *predictability*, a notion introduced in [18]. Let $f\in\Sigma$ be the fault event to be predicted. We denote by $\Psi(f):=\{sf\in\mathcal{L}(G):s\in\Sigma^*\}$ the set of strings that end with f. We write $f\in s$ if $\overline{s}\cap\Psi(f)\neq\emptyset$. We recall the definition of predictability from [18].

Definition 7: (Predictability). A live language $\mathcal{L}(G)$ is said to be predictable w.r.t. $f\in\Sigma$ and ω if

$$(\forall s\in\Psi(f))(\exists t\in\overline{\{s\}}:f\notin t)(\forall u\in\mathcal{L}(G):f\notin u\wedge P_\omega(u)=P_\omega(t))$$
$$(\exists n\in\mathbb{N})(\forall v\in\mathcal{L}(G)/u)[|v|\geq n\Rightarrow f\in v] \quad (6)$$

The above definition requires that the fault event f should be predicted unambiguously before its occurrence.

To proceed further, we assume that state space of G is partitioned into two disjoint sets $Q=Q_Y\dot{\cup}Q_N$, such that $\forall s\in\mathcal{L}(G):\delta(q_0,s)\in Q_Y\Leftrightarrow f\in s$. This assumption is also w.l.o.g., since we can always refine G by taking the parallel composition of G with an automaton with two states that captures the occurrence of f. Next, similarly to the notions of boundary strings and indicator strings in [19], we define the two following sets:

- Boundary states, $\partial_Q = \{q \in Q : \delta(q, f)!\}$; and
- Non-indicator states, $\mathcal{N}_Q = \{q \in Q_N : \forall n \in \mathbb{N}, \exists s \in \mathcal{L}(G, q) \text{ s.t. } |s| > n \wedge f \notin s\}$.

With the above notions, we define the IS-based property $\varphi_{pre} : 2^Q \to \{0, 1\}$ by:

$$\forall i \in 2^Q : [\varphi_{pre}(i) = 0] \Leftrightarrow [\exists q, q' \in i : q \in \partial_Q \wedge q' \in \mathcal{N}_Q] \quad (7)$$

The following result says that predictability is equivalent to the IS-based property φ_{pre}.

Theorem 3: Let φ_{pre} be the IS-based property defined by Equation (7). For any sensor activation policy $\omega \in \Omega$, $\mathcal{L}(G)$ is predictable w.r.t. f and ω if and only if $\omega \models_G \varphi_{pre}$.

The above theorem implies that to synthesize a minimal sensor activation policy for the purpose of prediction, it suffices to solve Problem 1 by taking φ_{pre} into account.

Example 6: Let us return to the system G in Fig. 1. Suppose that f is the fault event that we want to predict. G already satisfies the state partition assumption $Q = Q_Y \dot{\cup} Q_N$, where $Q_N = \{1, 2, 3, 4, 5, 6\}$ and $Q_Y = \{7\}$. Also, we have $\partial_Q = \{3\}$ and $\mathcal{N}_Q = \{1, 4, 5, 6\}$. In fact, we see that the IS-based property defined by Eqn. (1) is the IS-based property φ_{pre} for this example. Therefore, the solutions $\mathcal{O}_1$ and $\mathcal{O}_2$ shown in Fig. 2 that we obtained previously are two minimal sensor activation policies that guarantee predictability.

C. Application to Cyber-Security

As was discussed earlier in Remark 2, in some cases, the system may also be monitored by an *external* observer that is potentially malicious. Therefore, for security purposes, one may want the information mapping not to release some crucial information to this external observer. We recall an important security property called opacity.

Definition 8: Secret $Q_S \subseteq Q$ is current-state opaque w.r.t. G and ω if $\forall s \in \mathcal{L}(G) : \mathcal{E}^G_\omega(s) \not\subseteq Q_S$.

Current-state opacity is clearly an IS-based property. Therefore, the most permissive dynamic mask studied in [6] is also a special case of the generalized MPO and the problem of synthesizing a maximal sensor activation policy can also be solved by the approach presented in this paper.

Moreover, the same approach can be applied to other user-defined properties. For example, consider the IS-based property $\varphi : 2^Q \to \{0, 1\}$ defined by $\forall i \in 2^Q : \varphi(i) = 0 \Leftrightarrow |i| = 1$. This property is related to 1-*anonymity* studied in the computer security literature [20]. Intuitively, it requires that the observer should never determine the current-state of the system precisely. We can also synthesize a sensor activation policy for it by applying the generalized MPO approach.

VI. Conclusion

We presented a new approach to the problem of synthesizing an optimal sensor activation policy that guarantees some observation property in problems of control, diagnosis, prediction, or other types in the context of partially-observed discrete event systems. To this end, we defined a novel information structure called the generalized Most Permissive Observer that is applicable to a wide class of properties called information-state-based properties. We presented an algorithm for the construction of the MPO and a procedure for synthesizing an optimal sensor activation policy based on the MPO. Our approach generalizes the previous works on the MPO, which pertain to specific properties such as opacity or K-diagnosability. Our approach is applicable to a wide class of user-defined properties. In particular, we showed how the problem of optimal sensor activation for the purpose of fault prediction, not previously considered in the literature, can be solved by the generalized MPO.

References

[1] D. Thorsley and D. Teneketzis, "Active acquisition of information for diagnosis and supervisory control of discrete event systems," *Disc. Event Dyn. Sys.: Theory & Appl.*, vol. 17, no. 4, pp. 531–583, 2007.

[2] F. Cassez and S. Tripakis, "Fault diagnosis with static and dynamic observers," *Fund. Informa.*, vol. 88, no. 4, pp. 497–540, 2008.

[3] W. Wang, S. Lafortune, F. Lin, and A. R. Girard, "An online algorithm for minimal sensor activation in discrete event systems," in *48th IEEE Conference on Decision and Control*, 2009, pp. 2242–2247.

[4] ——, "Minimization of dynamic sensor activation in discrete event systems for the purpose of control," *IEEE TAC*, vol. 55, no. 11, pp. 2447–2461, 2010.

[5] W. Wang, S. Lafortune, A. R. Girard, and F. Lin, "Optimal sensor activation for diagnosing discrete event systems," *Automatica*, vol. 46, no. 7, pp. 1165–1175, 2010.

[6] F. Cassez, J. Dubreil, and H. Marchand, "Synthesis of opaque systems with static and dynamic masks," *Formal Methods in System Design*, vol. 40, no. 1, pp. 88–115, 2012.

[7] F. Cassez, "The complexity of codiagnosability for discrete event and timed systems," *IEEE TAC*, vol. 57, no. 7, pp. 1752–1764, 2012.

[8] S. Shu, Z. Huang, and F. Lin, "Online sensor activation for detectability of discrete event systems," *IEEE Trans. Automation Science and Engineering*, vol. 10, no. 2, pp. 457–461, 2013.

[9] D. Sears and K. Rudie, "Efficient computation of sensor activation decisions in discrete-event systems," in *52nd IEEE Conference on Decision and Control*, 2013, pp. 6966–6971.

[10] E. Dallal and S. Lafortune, "On most permissive observers in dynamic sensor activation problems," *IEEE TAC*, vol. 59, no. 4, pp. 966–981, 2014.

[11] D. Sears and K. Rudie, "Minimal sensor activation and minimal communication in discrete-event systems," *Discrete Event Dyn. Sys.: Theory & Appl.*, 2015.

[12] F. Cassez, "Dynamic observers for fault diagnosis of timed systems," in *49th IEEE Conf. Decision and Control*, 2010, pp. 4359–4364.

[13] X. Yin and S. Lafortune, "Minimization of sensor activation in decentralized fault diagnosis of discrete event systems," in *54th IEEE Conference on Decision and Control*, 2015.

[14] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, 2nd ed. Springer, 2008.

[15] W. Wang, S. Lafortune, and F. Lin, "An algorithm for calculating indistinguishable states and clusters in finite-state automata with partially observable transitions," *Systems & Control Letters*, vol. 56, no. 9, pp. 656–661, 2007.

[16] X. Yin and S. Lafortune, "Synthesis of maximally permissive nonblocking supervisors for partially observed discrete event systems," in *53rd IEEE Conf. Decision and Control*, 2014, pp. 5156–5162.

[17] S. Shu, F. Lin, and H. Ying, "Detectability of discrete event systems," *IEEE TAC*, vol. 52, no. 12, pp. 2356–2359, 2007.

[18] S. Genc and S. Lafortune, "Predictability of event occurrences in partially observed discrete-event systems," *Automatica*, vol. 45, no. 2, pp. 301–311, 2009.

[19] R. Kumar and S. Takai, "Decentralized prognosis of failures in discrete event systems," *IEEE TAC*, vol. 55, no. 1, pp. 48–59, 2010.

[20] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncert., Fuzz. Knowl.-Based Sys.*, vol. 10, no. 05, pp. 557–570, 2002.