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

Xiang Yin and Stéphane Lafortune

EECS Department, University of Michigan

54th IEEE CDC, Dec 15-18, 2015, Osaka, Japan
Introduction

- Dynamic Sensor Activation Problem

![Diagram showing a graph with states 0 to 5 and a process P, connected to an observer. The graph represents a plant G.]
• Dynamic Sensor Activation Problem
Introduction

- Dynamic Sensor Activation Problem

![Diagram showing dynamic sensor activation problem with nodes and arrows representing connections between states and a sensor activation module.]

\[ P \]

Sensor Activation Module

\[ P_\omega(s) \]

Property \( \sqrt{\text{Observer}} \)
$G = (Q, \Sigma, \delta, q_0)$ is a deterministic FSA

- $Q$ is the finite set of states;
- $\Sigma$ is the finite set of events;
- $\delta : Q \times \Sigma \rightarrow Q$ is the partial transition function;
- $q_0$ is the initial state
System Model

\( G = (Q, \Sigma, \delta, q_0) \) is a deterministic FSA

- \( Q \) is the finite set of states;
- \( \Sigma \) is the finite set of events;
- \( \delta: Q \times \Sigma \to Q \) is the partial transition function;
- \( q_0 \) is the initial state

- \( \Sigma = \Sigma_o \cup \Sigma_s \cup \Sigma_{uo} \)
- A sensing decision is a set of events \( \theta \in 2^\Sigma \) s.t. \( \Sigma_o \subseteq \theta \subseteq \Sigma_o \cup \Sigma_s \)
- \( \Theta \) denotes the set of sensing decisions
- Information mapping \( \omega: \mathcal{L}(G) \to \Theta \)
  \( P_\omega: \mathcal{L}(G) \to (\Sigma_o \cup \Sigma_s)^* \) denotes the corresponding projection
- A sensor activation policy is an information mapping \( \omega: \mathcal{L}(G) \to \Theta \) s.t.
  \( \forall s, t \in \mathcal{L}(G): P_\omega(s) = P_\omega(t) \Rightarrow \omega(s) = \omega(t) \)
Information State: a set of states, \( I := 2^Q \)

• **Information-State-Based Property**

Let \( G \) 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 \( \omega \) satisfies \( \varphi \) w.r.t. \( G \), denoted by \( \omega \models_G \varphi \), if

\[
\forall s \in \mathcal{L}(G): \varphi(\mathcal{E}_\omega(s)) = 1
\]

where

\[
\mathcal{E}_\omega(s) = \{ q \in Q: \exists t \in L \text{ s.t. } P_\omega(t) = P_\omega(s) \land \delta(q_0, t) = q \}
\]
• **Information-State-Based Properties**
  - **Opacity:** privacy applications
  - **Diagnosability:** fault detection and isolation
  - **Predictability:** fault prognosis
  - **Detectability:** state estimation
  - **Anonymity:** privacy applications
  - **Etc.**
Example 1

- IS-based Property $\varphi: 2^Q \rightarrow \{0,1\}$
  
  $\forall i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\forall q \in \{1, 4, 5, 6\}: \{3, q\} \subseteq i]$
Example 1

- IS-based Property $\varphi: 2^Q \rightarrow \{0,1\}$
  \[ \forall i \in 2^Q: [\varphi(i) = 1] \iff [\not\exists q \in \{1, 4, 5, 6\}: \{3, q\} \subseteq i] \]

- Sensor Activation Policy $\omega: \mathcal{L}(G) \rightarrow \emptyset$
  \[ \forall s \in \mathcal{L}(G): \omega(s) = \{o\} \]
Example 1

- **IS-based Property** $\varphi: 2^Q \to \{0, 1\}$
  \[
  \forall i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\not\exists q \in \{1, 4, 5, 6\}: \{3, q\} \subseteq i]
  \]

- **Sensor Activation Policy** $\omega: \mathcal{L}(G) \to \Theta$
  \[
  \forall s \in \mathcal{L}(G): \omega(s) = \{o\}
  \]

- The IS-based property is not satisfied, i.e., $\omega \not\models \varphi$
  \[
  \mathcal{E}_\omega^G(eo) = \{3, 6\}
  \]
• IS-based Property $\varphi: 2^Q \rightarrow \{0,1\}$
  $$\forall i \in 2^Q: [\varphi(i) = 1] \Leftrightarrow [\nexists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$$

• Sensor Activation Policy $\omega: \mathcal{L}(G) \rightarrow \Theta$
  $$\forall s \in \mathcal{L}(G): \omega(s) = \{o\}$$

• The IS-based property is not satisfied, i.e., $\omega \not\models \varphi$
  $$\mathcal{E}_\omega^G(\epsilon o) = \{3, 6\}$$

• State-disambiguation problem
Example 2

- IS-based Property $\varphi: 2^Q \rightarrow \{0, 1\}$
  $\forall i \in 2^Q: [\varphi(i) = 1] \iff [i \not\in X_{\text{Secret}}]$, where $X_{\text{Secret}} \subseteq X$

- Opacity problem

\[ P_\omega(s) = P_\omega(t) \]
• **Minimal Sensor Activation Problem for IS-Based Properties**

Let $G = (Q, \Sigma, \delta, q_0)$ be the system automaton and $\varphi : 2^Q \rightarrow \{0,1\}$ be an IS-based property w.r.t. $G$. Find a sensor activation policy $\omega$ such that

(i) $\omega \models_G \varphi$  

(IS-based Property)

(ii) $\not\exists \omega' \in \Omega$ such that $\omega \models_G \varphi$ and $\omega' < \omega$.  

(Minimality)

The **Maximal Sensor Activation Problem** is also defined analogously.

$\omega' < \omega$ is defined in terms of set inclusion.
Literature Review

Dynamic Sensor Activation Problem

Literature Review

Dynamic Sensor Activation Problem


- Different approaches for different properties
- The sensor activation problems for some properties have not been considered
- Need general approach
Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. $G$ is a 7-tuple $\mathcal{O} = (Q^0_Y, Q^0_Z, h^0_{YZ}, h^0_{ZY}, E, \Gamma, y_0)$

- $Q^0_Y \subseteq I$ is the set of $Y$-states;
- $Q^0_Z \subseteq I \times \Theta$ is the set of $Z$-states so that $z = (I(z), \Theta(z));$
- $h^0_{YZ}: Q^0_Y \times \Theta \rightarrow Q^0_Z$ represents the unobservable reach;
- $h^0_{ZY}: Q^0_Z \times \Sigma \rightarrow Q^0_Y$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.
Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. $G$ is a 7-tuple $\mathcal{O} = (Q_Y^\mathcal{O}, Q_Z^\mathcal{O}, h_{YZ}^\mathcal{O}, h_{ZY}^\mathcal{O}, E, \Gamma, y_0)$

- $Q_Y^\mathcal{O} \subseteq I$ is the set of Y-states;
- $Q_Z^\mathcal{O} \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^\mathcal{O}: Q_Y^\mathcal{O} \times \Theta \to Q_Z^\mathcal{O}$ represents the unobservable reach;
- $h_{ZY}^\mathcal{O}: Q_Z^\mathcal{O} \times \Sigma \to Q_Y^\mathcal{O}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.

$$\Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\}$$
Bipartite Dynamic Observer

A bipartite dynamic observer $\mathcal{O}$ w.r.t. $G$ is a 7-tuple $\mathcal{O} = (Q^O_Y, Q^O_Z, h^O_{YZ}, h^O_{ZY}, E, \Gamma, y_0)$

- $Q^O_Y \subseteq I$ is the set of Y-states;
- $Q^O_Z \subseteq I \times \Theta$ is the set of Z-states so that $z = (I(z), \Theta(z))$;
- $h^O_{YZ} : Q^O_Y \times \Theta \to Q^O_Z$ represents the unobservable reach;
- $h^O_{ZY} : Q^O_Z \times \Sigma \to Q^O_Y$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.

\[ \Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\} \]
Bipartite Dynamic Observer (BDO)

A bipartite dynamic observer $\mathcal{O}$ w.r.t. $G$ is a 7-tuple $\mathcal{O} = (Q^Y_\mathcal{O}, Q^Z_\mathcal{O}, h^Y_{YZ}, h^Z_{ZY}, E, \Gamma, y_0)$

- $Q^Y_\mathcal{O} \subseteq I$ is the set of $Y$-states;
- $Q^Z_\mathcal{O} \subseteq I \times \Theta$ is the set of $Z$-states so that $z = (I(z), \Theta(z))$;
- $h^Y_{YZ}: Q^Y_\mathcal{O} \times \Theta \rightarrow Q^Z_\mathcal{O}$ represents the unobservable reach;
- $h^Z_{ZY}: Q^Z_\mathcal{O} \times \Sigma \rightarrow Q^Y_\mathcal{O}$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.

$\Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\}$
A bipartite dynamic observer $\mathcal{O}$ w.r.t. $G$ is a 7-tuple $\mathcal{O} = (Q_Y^0, Q_Z^0, h_{YZ}^0, h_{ZY}^0, E, \Gamma, y_0)$

- $Q_Y^0 \subseteq I$ is the set of $Y$-states;
- $Q_Z^0 \subseteq I \times \Theta$ is the set of $Z$-states so that $z = (I(z), \Theta(z))$;
- $h_{YZ}^0: Q_Y^0 \times \Theta \rightarrow Q_Z^0$ represents the unobservable reach;
- $h_{ZY}^0: Q_Z^0 \times \Sigma \rightarrow Q_Y^0$ represents the observable reach;
- $y_0 = \{q_0\}$ is the initial state.

\[ \Sigma_o = \{o\}, \Sigma_s = \{\sigma_1, \sigma_2\}, \Sigma_{uo} = \{e, f\} \]
Generalized Most Permissive Observer

- **Most Permissive Observer (MPO)**

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

1. For any $y \in Q_Y^{MPO}$, there exists $\theta \in \Theta$ such that $h_{YZ}^{MPO} (y, \theta)!$
2. For any $z \in Q_Z^{MPO}$, we have
   2.1. $(\forall \sigma \in \Theta(z))[ (\exists x \in I(z): \delta(x, \sigma)! ) \Rightarrow h_{ZY}^{MPO} (z, \sigma)! ];$
   2.2. $\varphi(I(z)) = 1$
Generalized Most Permissive Observer

**Most Permissive Observer (MPO)**

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

1. For any $y \in Q_{Y}^{MPO}$, there exists $\theta \in \Theta$ such that $h_{YZ}^{MPO}(y, \theta)!$;
2. For any $z \in Q_{Z}^{MPO}$, we have
   2.1. $(\forall \sigma \in \Theta(z))[(\exists x \in I(z): \delta(x, \sigma)!) \Rightarrow h_{ZY}^{MPO}(z, \sigma)!]$;
   2.2. $\varphi(I(z)) = 1$

**MPO for Diagnosability**


**MPO for Opacity**

• Depth-first search until reach a Z-state violating \( \varphi \)
• Iteratively prune:
  - Y-state, from which all sensing decisions have been removed
  - Z-state, from which one observation has been removed
There exists a sensor activation policy $\omega$ such that $\omega \models_G \varphi$ iff $\mathcal{MPO}_\varphi$ is non-empty.
Properties of the MPO

• Theorem

There exists a sensor activation policy $\omega$ such that $\omega \models_G \varphi$ iff $\mathcal{MPO}_\varphi$ is non-empty.

• Theorem

$\omega \models_G \varphi$ iff $\omega$ is included in $\mathcal{MPO}_\varphi$. 
There exists a sensor activation policy $\omega$ such that $\omega \models^G \varphi$ iff $\mathcal{MPO}_\varphi$ is non-empty.

$\omega \models^G \varphi$ iff $\omega$ is included in $\mathcal{MPO}_\varphi$. 
• **IS-based Sensor Activation Policy**

A sensor activation policy $\omega$ is said to be *Information-State-based* (or IS-based) if

$$\forall s, t \in \mathcal{L}(G): J^Y_\omega(s) = J^Y_\omega(t) \Rightarrow \omega(s) = \omega(t)$$
• **IS-based Sensor Activation Policy**

A sensor activation policy $\omega$ is said to be *Information-State-based* (or IS-based) if

$$\forall s, t \in \mathcal{L}(G): J^Y_\omega(s) = J^Y_\omega(t) \Rightarrow \omega(s) = \omega(t)$$

• **Greedy Optimal Sensor Activation Policy**

Suppose that $\omega$ is a sensor activation policy such that policy $\omega \models_G \varphi$. We say that $\omega$ is greedy minimal if

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

The notion of *greedy maximality* is defined analogously.
Synthesis of Optimal Sensor Activation Policies

• **IS-based Sensor Activation Policy**
  A sensor activation policy $\omega$ is said to be *Information-State-based* (or IS-based) if
  \[
  \forall s, t \in \mathcal{L}(G): \mathcal{I}_\omega^Y(s) = \mathcal{I}_\omega^Y(t) \Rightarrow \omega(s) = \omega(t)
  \]

• **Greedy Optimal Sensor Activation Policy**
  Suppose that $\omega$ is a sensor activation policy such that policy $\omega \models_G \varphi$. We say that $\omega$ is greedy minimal if
  \[
  \forall s \in \mathcal{L}(G), \forall \theta \in \Theta: h_{YZ}^{MPO}(\mathcal{I}_\omega^Y(s), \theta) \Rightarrow \theta \not\in \omega(s)
  \]
  The notion of *greedy maximality* is defined analogously

• **Theorem**
  Let $\omega$ be a sensor activation policy such that policy $\omega \models_G \varphi$. Then $\omega$ is minimal (respectively, maximal) if it is greedy minimal (respectively, greedy maximal).
An Optimal $\omega$ s.t. $\omega \models_G \varphi$

Synthesis Procedure

System: $G$

Property: $\varphi$

Construct $\mathcal{MPO}_\varphi$

Find a greedy minimal IS-based Solution via a DFS

Property: $\varphi$
IS-based Formulation of Predictability

• Predictability
A live language $\mathcal{L}(G)$ is said to be **predictable** if any fault of the system can be predicted prior to its occurrence with no missed alarm and no false alarm.

• IS-based Predictability $\varphi_{\text{pre}}: \mathcal{P}(Q) \rightarrow \{0,1\}$
\[ \forall i \in \mathcal{P}(Q) : [\varphi_{\text{pre}}(i) = 0] \iff [\exists q, q' \in i : q \in \partial Q \land q' \in \mathcal{N}_Q] \]

• Theorem
Let $\varphi_{\text{pre}}$ be the IS-based predictability defined above. For ant sensor activation policy $\omega$, $\mathcal{L}(G)$ is predictable w.r.t. $f$ and $\omega$ if and only if $\omega \models_G \varphi_{\text{pre}}$.

---

**Boundary State** [Kumar & Takai, 2010]  
**Non-indicator State**
Example

- Boundary states, $\partial Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1, 4, 5, 6\}$
- $\forall i \in 2^Q: \left[ \varphi_{pre}(i) = 1 \right] \iff \left[ \forall q \in \{1, 4, 5, 6\}: \{3, q\} \subseteq i \right]$
Example

- Boundary states, $\partial_Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1, 4, 5, 6\}$
- $\forall i \in 2^Q: [\varphi_{pre}(i) = 1] \iff [\exists q \in \{1, 4, 5, 6\}: \{3, q\} \subseteq i]$
Example

- Boundary states, $\partial_Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1,4,5,6\}$
- $\forall i \in 2^Q: [\varphi_{pre}(i) = 1] \iff [\not\exists q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$
Example

- Boundary states, $\partial Q = \{3\}$
- Non-indicator states, $\mathcal{N}_Q = \{1,4,5,6\}$
- $\forall i \in 2^Q: [\phi_{pre}(i) = 1] \iff [\forall q \in \{1,4,5,6\}: \{3, q\} \subseteq i]$
Contributions:

• A general approach for solving dynamic sensor activation problems
• Information-state-based properties: A general class of properties
• Solve previous open problem, e.g., predictability
• Applicable to more *user-defined* properties
• The solution is provably *language-based* minimal