Opacity Enforcing Supervisory Control using Non-deterministic Supervisors

Yifan Xie & Xiang Yin & Shaoyuan Li

Department of Automation, Shanghai Jiao Tong University

xyfan1234@sjtu.edu.cn

21st IFAC World Congress

July 11-17, 2020, Germany

上海交通大學

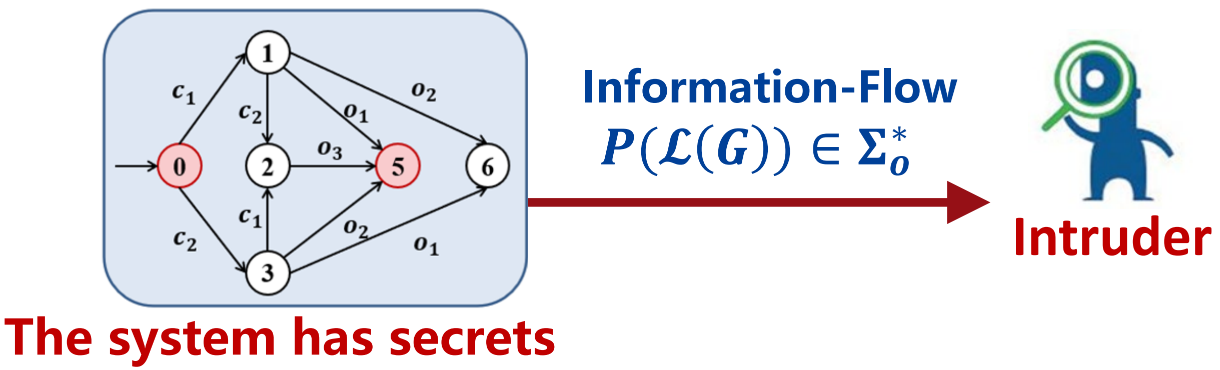
SHANGHAI JIAO TONG UNIVERSITY

Introduction

Motivation

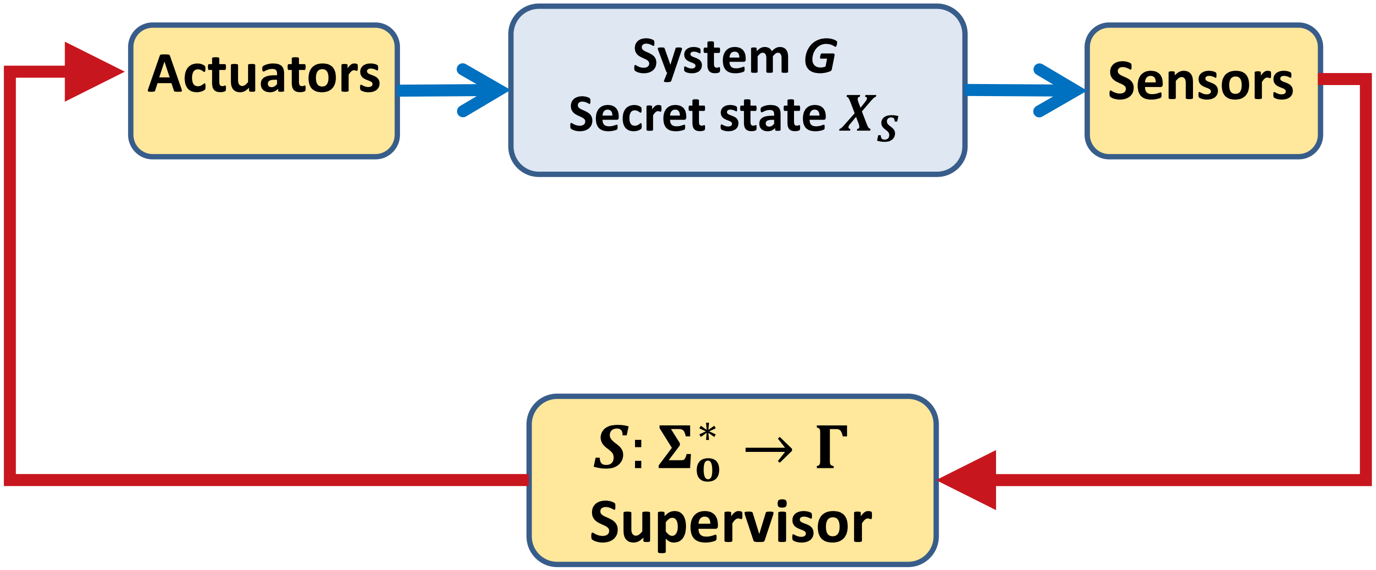
- **Security and privacy concerns in Cyber-Physical Systems**
- **Opacity: An information-flow property**
- **Application: Web services, Location-based services…**

System Model and the Intruder



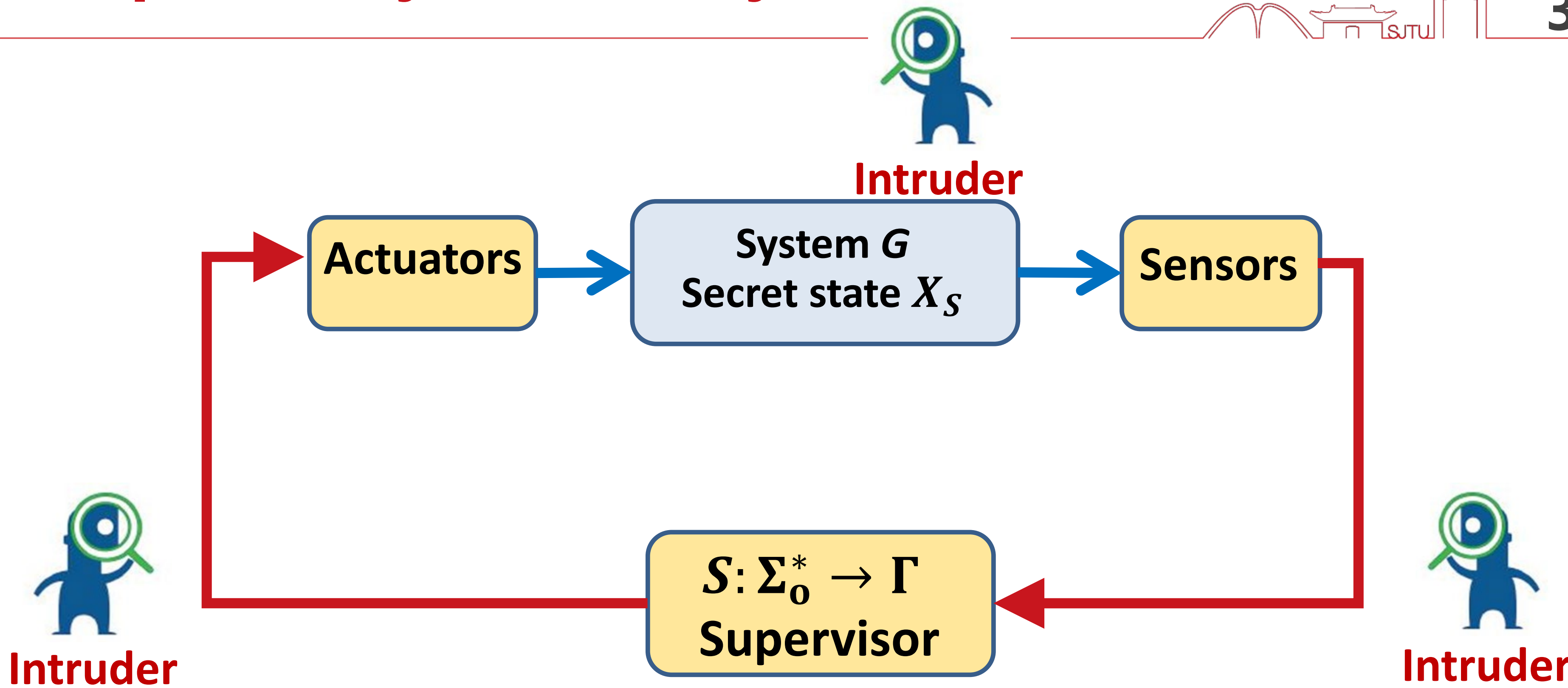
- The system is modeled as a FSA $G = (X, \Sigma, \delta, x_0)$
- The system has secrets, modeled a set of states $X_s \subseteq X$
- $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$, $P: \Sigma^* \to \Sigma_o^*$ is the natural projection
- The intruder is a passive observer seeing $P(\mathcal{L}(G))$

Supervisory Control Systems



- **Sensors:** $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ **and** $P: \Sigma^* \to \Sigma_o^*$
- **Actuators:** $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc}$ **and** $\Gamma := \{\gamma \in 2^{\Sigma}: \Sigma_{uc} \subseteq \gamma\}$
- **Supervisor:** $S: P(L(G)) \to \Gamma$ **updates decisions dynamically**

Supervisory Control Systems

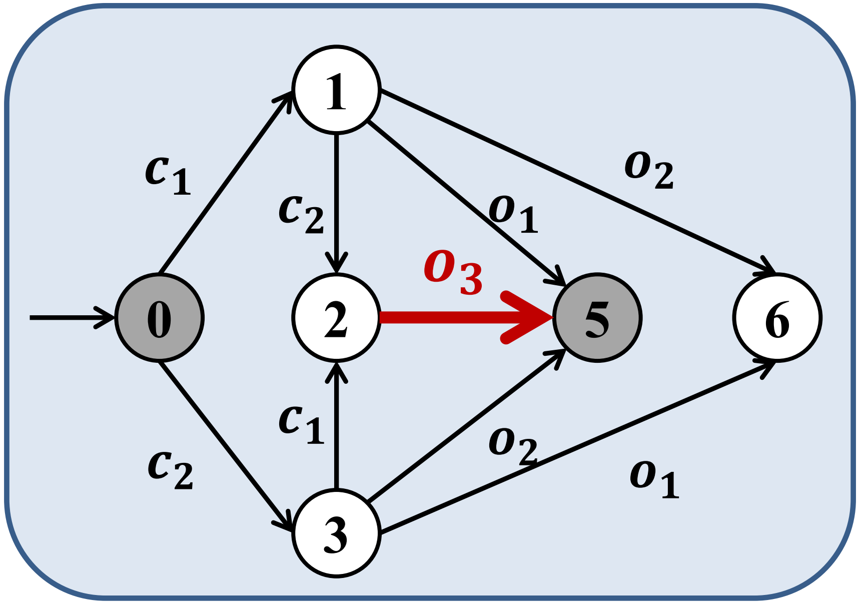


- **Sensors:** $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ and $P: \Sigma^* \rightarrow \Sigma_o^*$
- **Actuators:** $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc}$ and $\Gamma \coloneqq \{\gamma \in 2^{\Sigma}: \Sigma_{uc} \subseteq \gamma\}$
- **Supervisor:** $S: P(L(G)) \rightarrow \Gamma$ updates decisions dynamically
- **Intruder:** System model G, Observable events Σ_o^* , Control policy Γ

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

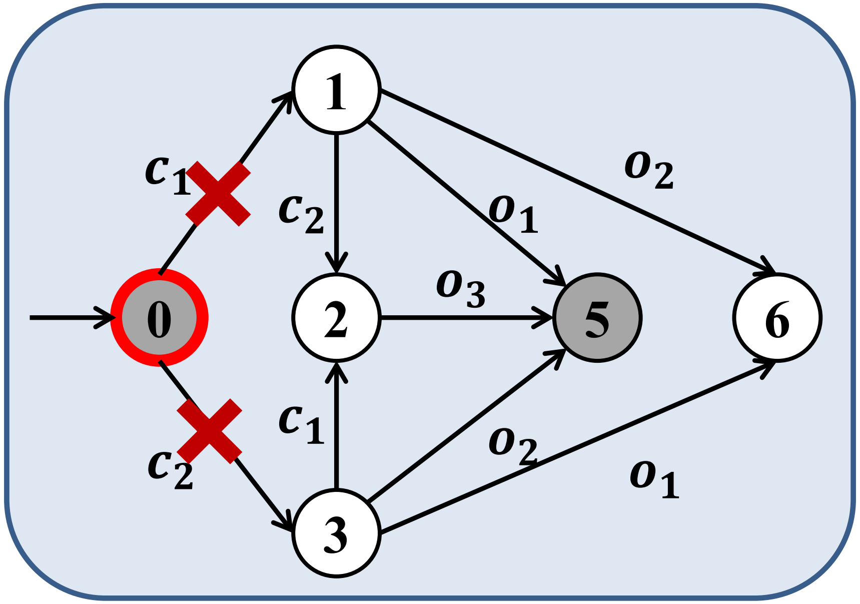
$$\Gamma = \left\{\begin{matrix} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{matrix}\right\}$$



Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{matrix} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{matrix} \right\}$$

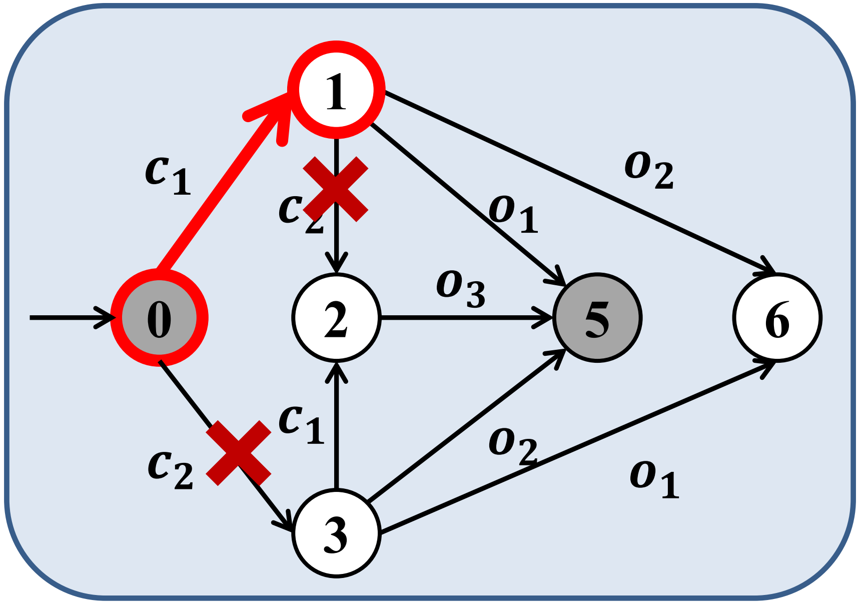


- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{array}{c} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{array} \right\}$$

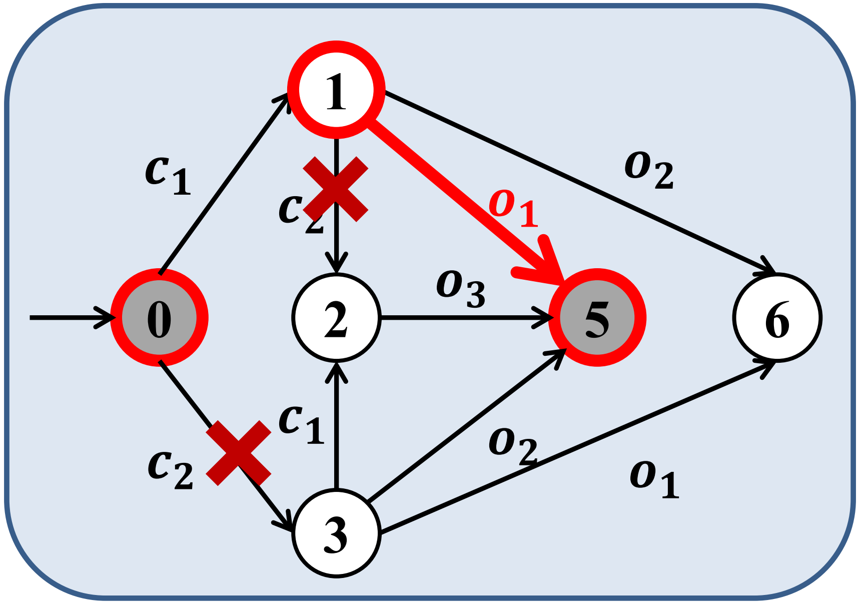


- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque
- $\{0\} \xrightarrow{\{c_1\}} \{0, 1\}$

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{matrix} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{matrix} \right\}$$

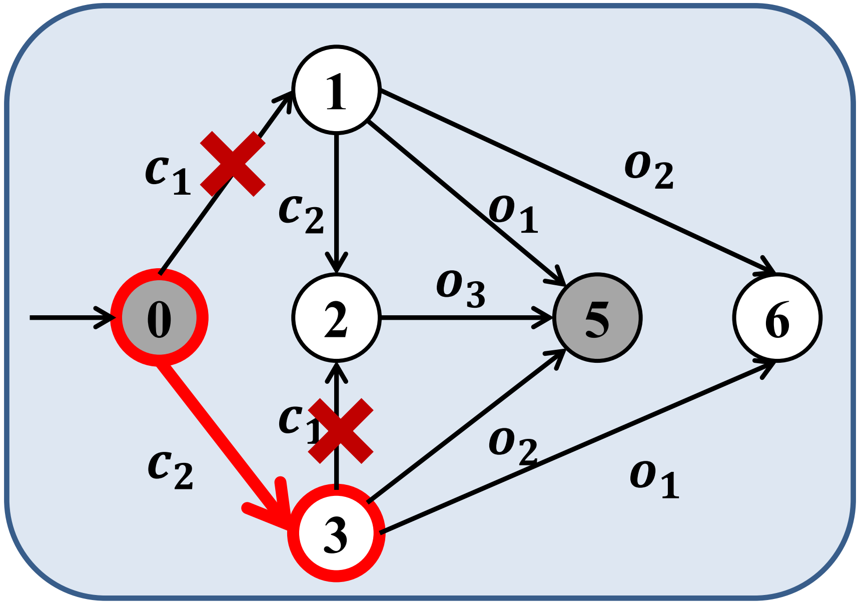


- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque
- $\{0\} \xrightarrow{\{c_1\}} \{0, 1\} \xrightarrow{o_1} \{5\}$, not opaque

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{array}{c} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{array} \right\}$$

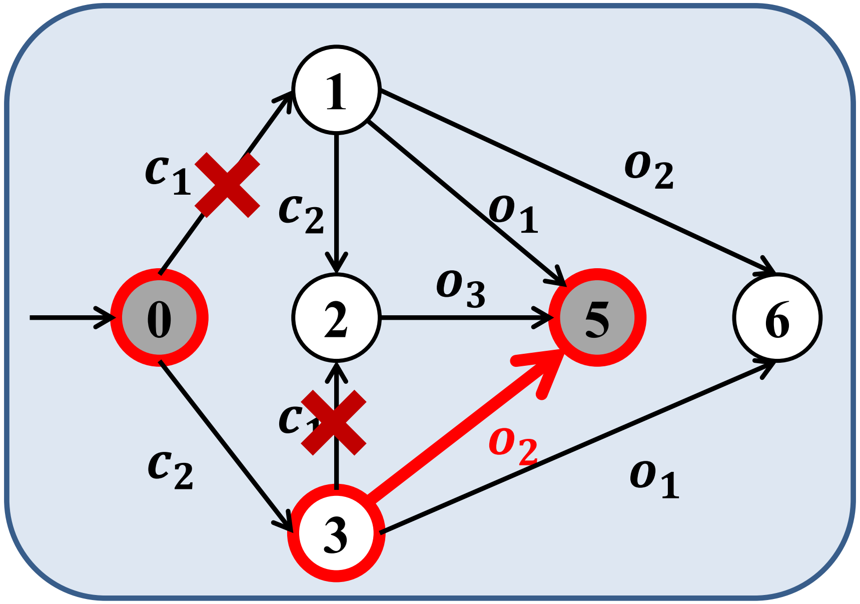


- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque
- $\{0\} \xrightarrow{\{c_1\}} \{0, 1\} \xrightarrow{o_1} \{5\}$, not opaque
- $\{0\} \xrightarrow{\{c_2\}} \{0, 3\}$

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{matrix} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{matrix} \right\}$$

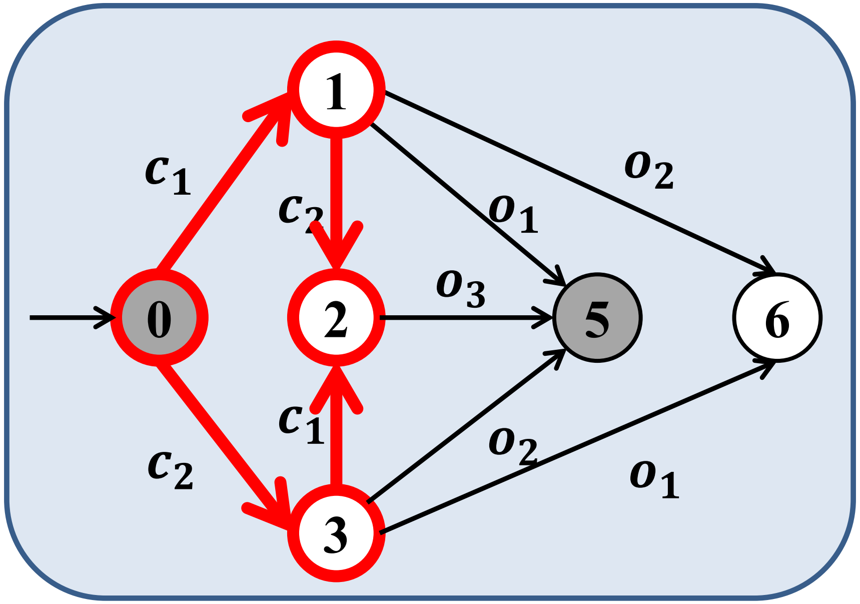


- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque
- $\{0\} \xrightarrow{\{c_1\}} \{0, 1\} \xrightarrow{o_1} \{5\}$, not opaque
- $\{0\} \xrightarrow{\{c_2\}} \{0, 3\} \xrightarrow{o_2} \{5\}$, not opaque

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{matrix} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{matrix} \right\}$$

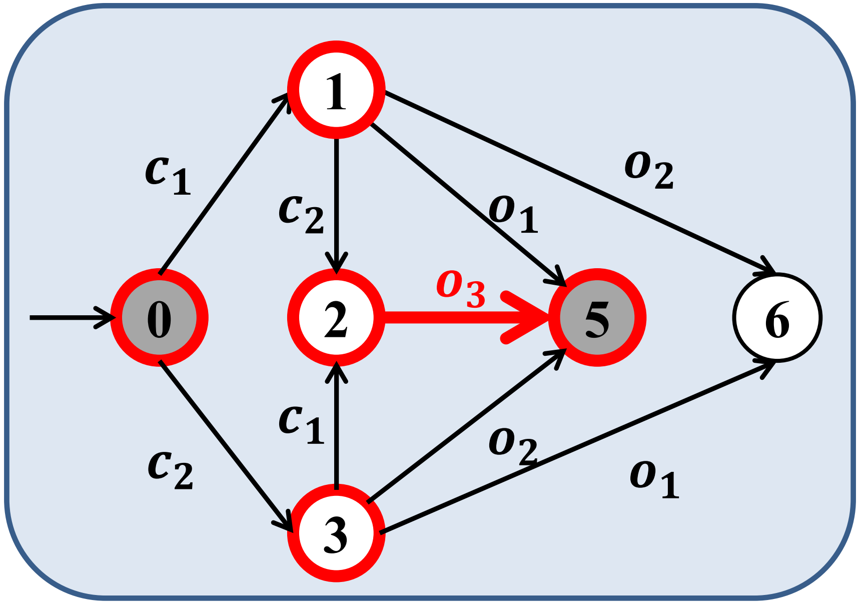


- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque
- $\{0\} \xrightarrow{\{c_1\}} \{0, 1\} \xrightarrow{o_1} \{5\}$, not opaque
- $\{0\} \xrightarrow{\{c_2\}} \{0, 3\} \xrightarrow{o_2} \{5\}$, not opaque
- $\{0\} \xrightarrow{\{c_1, c_2\}} \{0, 1, 2, 3\}$

Motivating Example

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

$$\Gamma = \left\{ \begin{matrix} \emptyset \\ \{c_1\} \\ \{c_2\} \\ \{c_1, c_2\} \end{matrix} \right\}$$



- $\{0\} \xrightarrow{\emptyset} \{0\}$, not opaque
- $\{0\} \xrightarrow{\{c_1\}} \{0, 1\} \xrightarrow{o_1} \{5\}$, not opaque
- $\{0\} \xrightarrow{\{c_2\}} \{0, 3\} \xrightarrow{o_2} \{5\}$, not opaque
- $\{0\} \xrightarrow{\{c_1, c_2\}} \{0, 1, 2, 3\} \xrightarrow{o_3} \{5\}$, not opaque

Non-deterministic Supervisor

A set of possible control decisions $\Longrightarrow$ A specific control decision

The non-deterministic supervisor is defined as a function

$$S_N\colon\ (\Gamma\Sigma_o)^* \to 2^{\Gamma}$$

that maps a decision history to a set of possible control decision.

Non-deterministic Supervisor

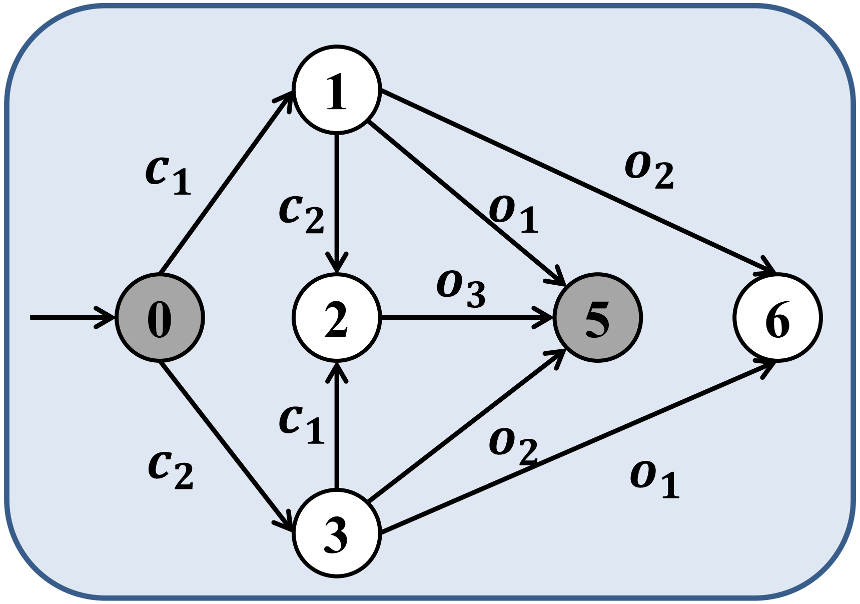
A set of possible control decisions $\Longrightarrow$ A specific control decision

The non-deterministic supervisor is defined as a function

$$S_N\colon (\Gamma\Sigma_o)^* \rightarrow 2^{\Gamma}$$

that maps a decision history to a set of possible control decision.

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$



Non-deterministic Supervisor

A set of possible control decisions $\Longrightarrow$ A specific control decision

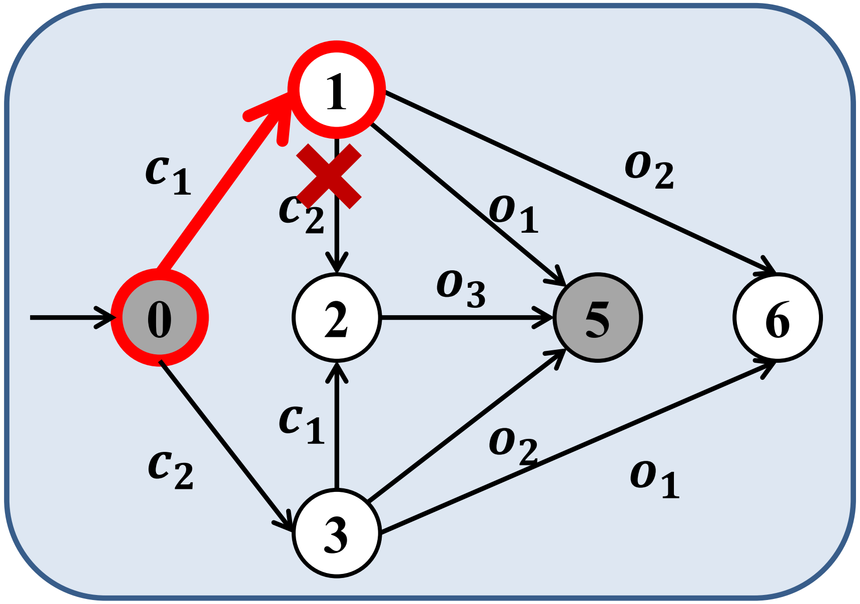
The non-deterministic supervisor is defined as a function

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

that maps a decision history to a set of possible control decision.

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

- Non-deterministic control mechanism, e.g, $\{\{c_1\}, \{c_2\}\}$
- $\{0\} \xrightarrow{\{\{c_1\},\{c_2\}\}} \begin{cases}\{0,1\} \\ \{0,3\}\end{cases}$



Non-deterministic Supervisor

A set of possible control decisions $\Longrightarrow$ A specific control decision

The non-deterministic supervisor is defined as a function

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

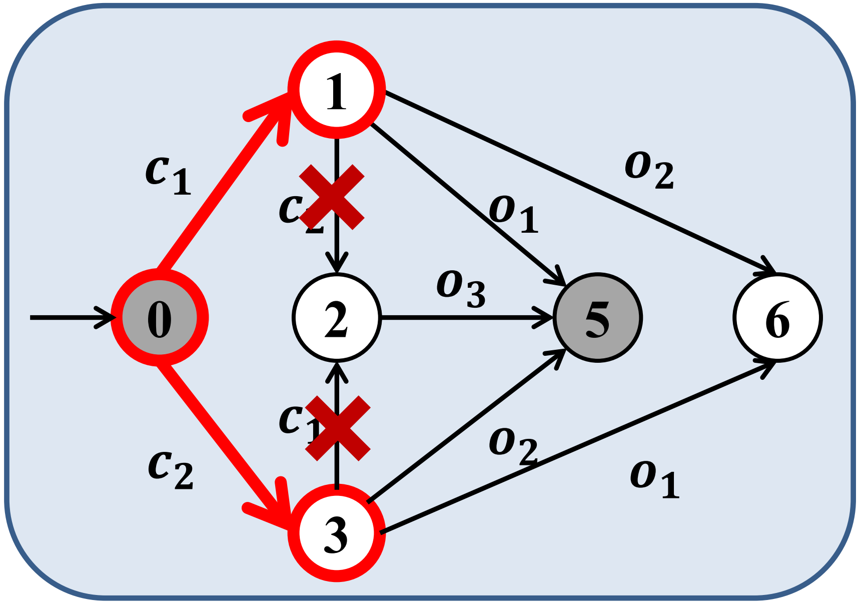
that maps a decision history to a set of possible control decision.

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

- Non-deterministic control mechanism,

  e.g, $\{\{c_1\}, \{c_2\}\}$

- $\{0\} \xrightarrow{\{\{c_1\},\{c_2\}\}} \begin{Bmatrix} \{0, 1\} \\ \{0, 3\} \end{Bmatrix}$



Non-deterministic Supervisor

A set of possible control decisions $\Longrightarrow$ A specific control decision

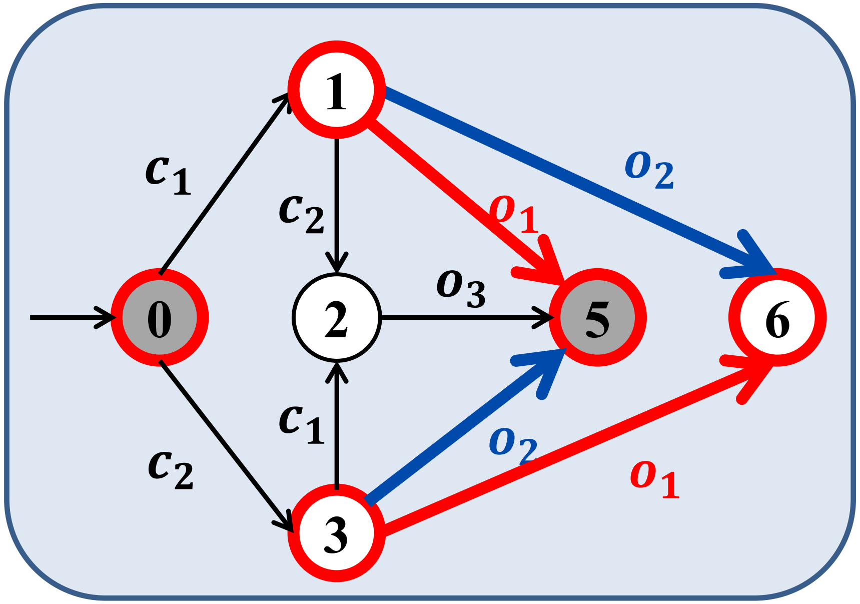
The non-deterministic supervisor is defined as a function

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

that maps a decision history to a set of possible control decision.

$$\Sigma_o = \{o_1, o_2, o_3\}$$
$$\Sigma_c = \{c_1, c_2\}$$

- Non-deterministic control mechanism, e.g, $\{\{c_1\},\{c_2\}\}$
- $\{0\} \xrightarrow{\{\{c_1\},\{c_2\}\}} \begin{Bmatrix}\{0,1\} \\ \{0,3\}\end{Bmatrix} \begin{matrix} \xrightarrow{o_1} \{\{5\},\{6\}\} \\ \xrightarrow{o_2} \{\{5\},\{6\}\} \end{matrix}$, opaque



Non-deterministic Supervisor

A set of possible control decisions $\Longrightarrow$ A specific control decision

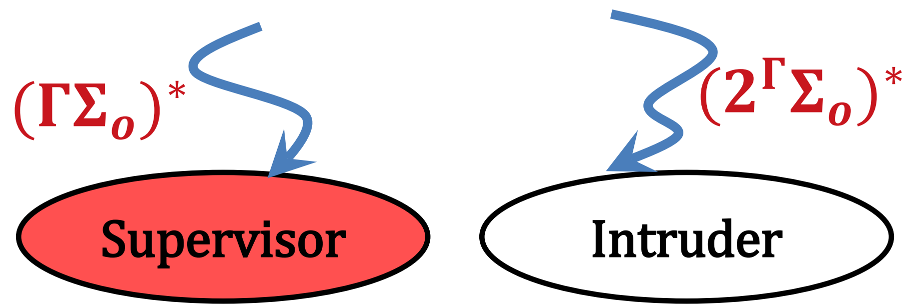
The non-deterministic supervisor is defined as a function

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

that maps a decision history to a set of possible control decision.

Supervisor: specific control decision

Intruder: the set of all possible control decisions



Non-deterministic Supervisor

A set of possible control decisions $\Longrightarrow$ A specific control decision

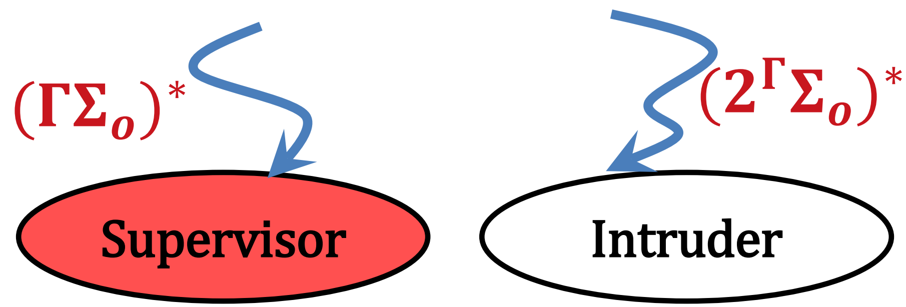
The non-deterministic supervisor is defined as a function

$$S_N \colon (\Gamma\Sigma_o)^* \rightarrow 2^{\Gamma}$$

that maps a decision history to a set of possible control decision.

Supervisor: specific control decision

Intruder: the set of all possible control decisions



Opacity under Non-deterministic Supervisor

Let $S_N \colon (\Gamma\Sigma_o)^* \rightarrow 2^{\Gamma}$ be a non-deterministic supervisor. We say the closed-loop system S_N/G is opaque (w.r.t. Σ_o and X_S) if $\forall s \in P(\mathcal{L}(S_N/G)) \colon X_I(s) \nsubseteq X_S$.

Information State and its Flow

Information State

We propose the following information-state space

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

to separate the observation of the supervisor and the intruder.

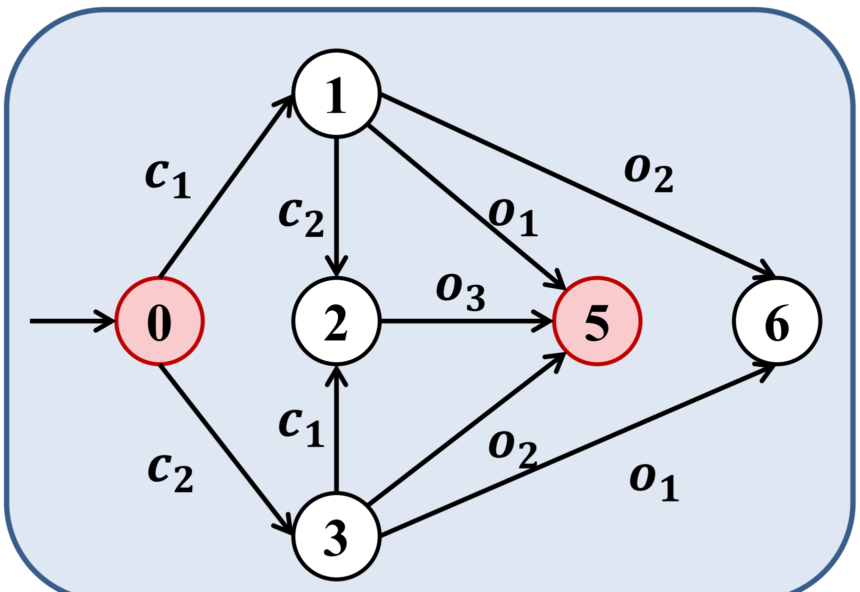
Information State and its Flow

Information State

We propose the following information-state space

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

to separate the observation of the supervisor and the intruder.



$$0 \xrightarrow{\{\{c_1\},\{c_2\}\}} \xrightarrow{\{c_1\}}$$

- **From supervisor's point of view**

$$\{0, 1\} \Rightarrow 2^X$$

- **From the intruder's point of view**

$$\begin{Bmatrix} \{0, 1\} \\ \{0, 3\} \end{Bmatrix} \Rightarrow 2^{2^X}$$

Information State and its Flow

Information State

We propose the following information-state space

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

to separate the observation of the supervisor and the intruder.

Information State Non-deterministic Supervisor

$$S_N : I \to 2^\Gamma$$

which makes control decision based on the proposed information state.

Information State and its Flow

- Micro-state: $m \in 2^X$
- Augmented micro-state:

$$m^+ = (m, \gamma) \in 2^X \times \Gamma$$

Information State and its Flow

- Micro-state: $m \in 2^X$
- Augmented micro-state:

$$m^+ = (m, \gamma) \in 2^X \times \Gamma$$

- Macro-state:

$$\mathbf{m} = \{m_1, m_2, \cdots, m_n\} \subseteq 2^X$$

- Augmented macro-state:

$$\mathbf{m}^+ = \{(m_1, \gamma_1), (m_2, \gamma_2), \cdots, (m_n, \gamma_n)\} \subseteq 2^X \times \Gamma$$

Information State and its Flow

- Micro-state: $m \in 2^X$
- Augmented micro-state:

$$m^+ = (m, \gamma) \in 2^X \times \Gamma$$

- Macro-state:

$$\mathbf{m} = \{m_1, m_2, \cdots, m_n\} \subseteq 2^X$$

- Augmented macro-state:

$$\mathbf{m}^+ = \{(m_1, \gamma_1), (m_2, \gamma_2), \cdots, (m_n, \gamma_n)\} \subseteq 2^X \times \Gamma$$

- Macro-control-decision:

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

d is compatible with **m** if *d* essentially assigns each micro-state a non-deterministic control decision.

Information State and its Flow

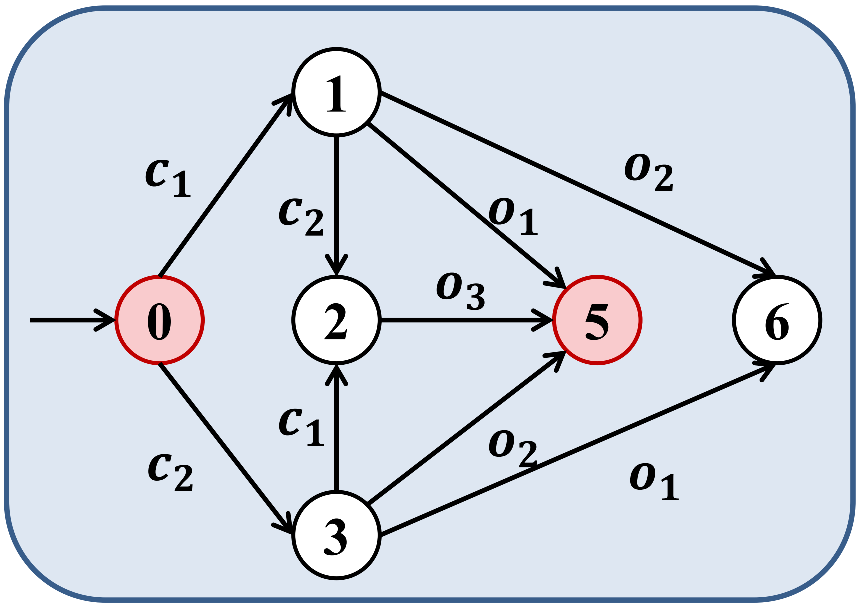
Information State Flow

Suppose that the intruder observes $\sigma_1 \cdots \sigma_n \in P(\mathcal{L}(S_N/G))$ and by knowing the fact that S_N is an IS-based supervisor

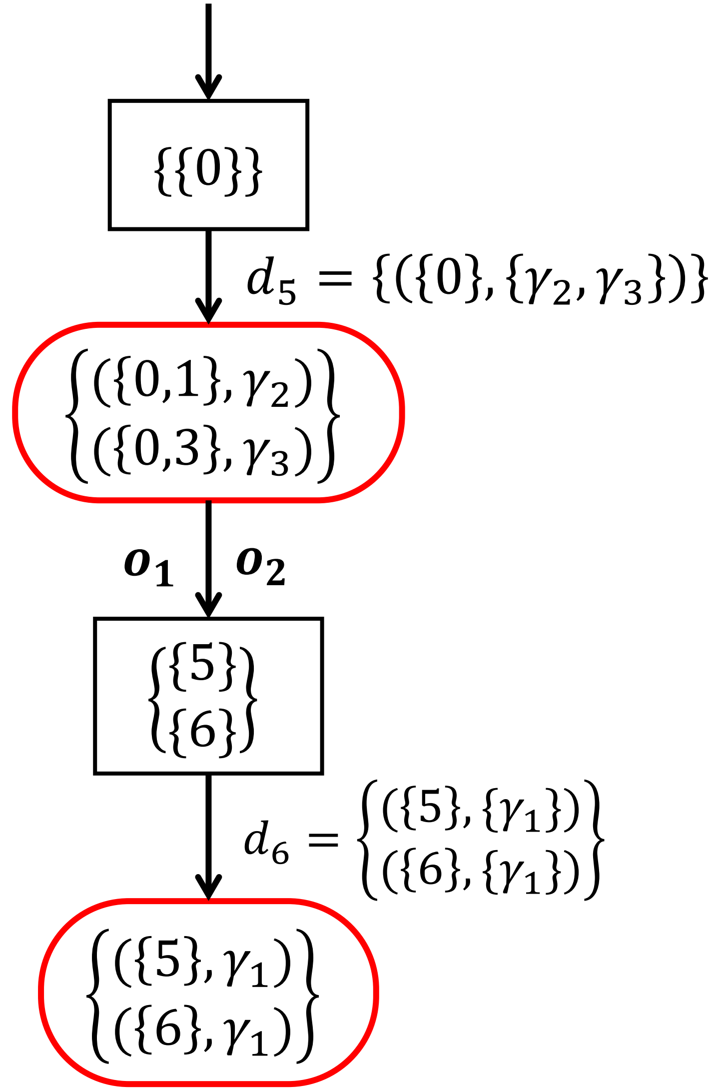
$$\mathbf{m}_0 \xrightarrow{d_0} \mathbf{m}_0^+ \xrightarrow{\sigma_1} \mathbf{m}_1 \xrightarrow{d_1} \cdots \xrightarrow{\sigma_n} \mathbf{m}_n \xrightarrow{d_n} \mathbf{m}_n^+$$

where $\mathbf{m}_0 = \{\{x_0\}\}$, $d_i = d_{S_N}(\mathbf{m}_i)$, $\mathbf{m}_i^+ = \odot(d_i)$ and $m_{i+1} = \widehat{NX}_{\sigma_{i+1}}(\mathbf{m}_i^+)$

Information State and its Flow



$$\gamma_1 = \{o_1, o_2, o_3\}$$
$$\gamma_2 = \{o_1, o_2, o_3, c_1\}$$
$$\gamma_3 = \{o_1, o_2, o_3, c_2\}$$



Supervisor Synthesis Procedure

1. Enumerates all feasible transitions

new macro-control-decision & new observation

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

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

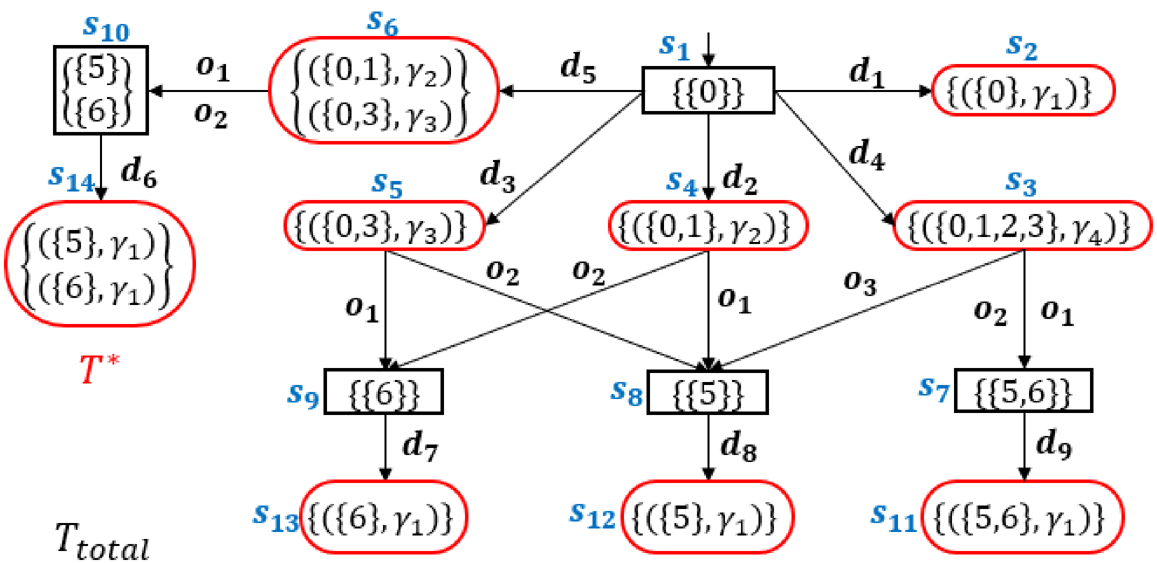
Supervisor Synthesis Procedure

1. Enumerates all feasible transitions

new macro-control-decision & new observation

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

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



Supervisor Synthesis Procedure

2. Delete all secret-revealing states and inconsistent states

Secret-revealing Z-states

$$Q_{reveal} = \{z \in \mathbb{M}^+ : \cup\, \Xi(z) \subseteq X_s\} \qquad \cup\, \Xi(z) = X_I(s)$$

Supervisor Synthesis Procedure

2. Delete all secret-revealing states and inconsistent states

Secret-revealing Z-states

$$Q_{reveal} = \{z \in \mathbb{M}^{+} : \cup\, \Xi(z) \subseteq X_s\} \qquad \cup\, \Xi(z) = X_I(s)$$

Inconsistent states

- A Y-state is consistent if at least one macro-control-decision is defined.
- A Z-state is consistent if all feasible events are defined.

Supervisor Synthesis Procedure

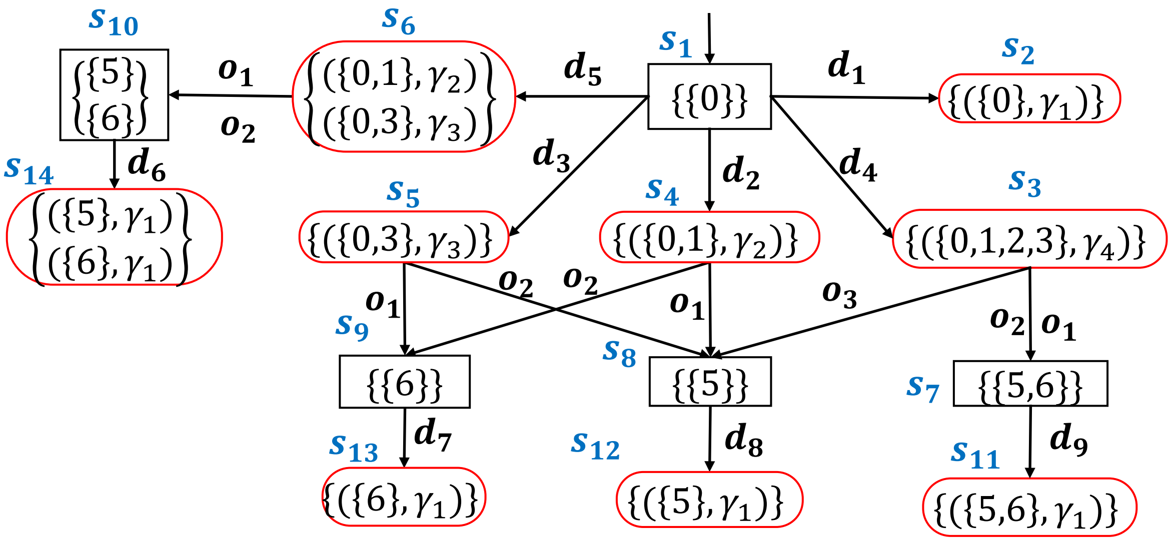
2. Delete all secret-revealing states and inconsistent states

Secret-revealing Z-states

$$Q_{reveal} = \{z \in \mathbb{M}^{+} : \cup\, \Xi(z) \subseteq X_s\} \qquad \cup\, \Xi(z) = X_I(s)$$

Inconsistent states

- **A Y-state is consistent if at least one macro-control-decision is defined.**
- **A Z-state is consistent if all feasible events are defined.**



Supervisor Synthesis Procedure

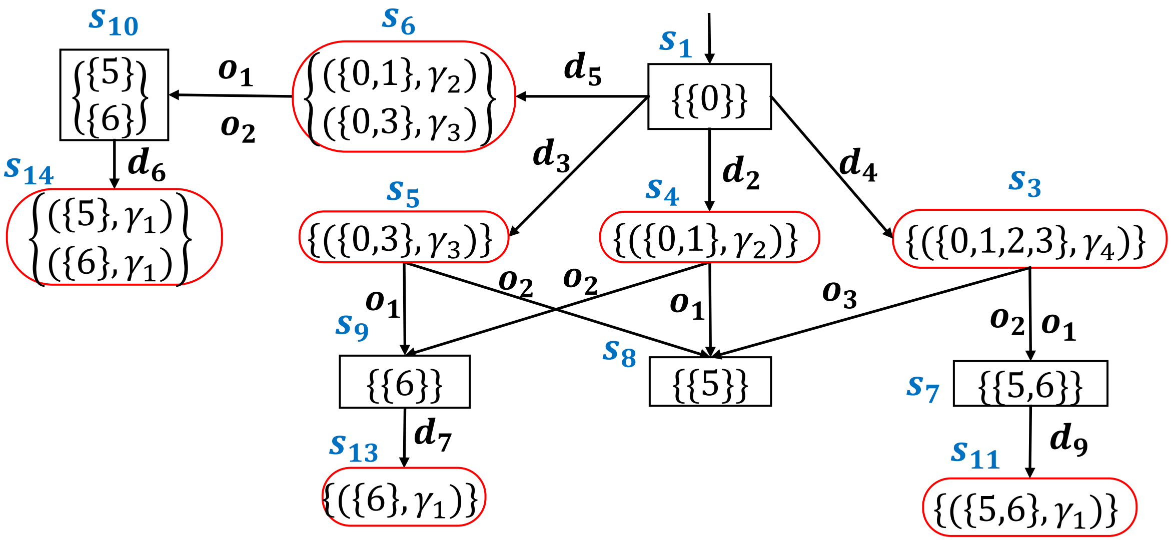
2. Delete all secret-revealing states and inconsistent states

Secret-revealing Z-states

$$Q_{reveal} = \{z \in \mathbb{M}^{+} : \cup\, \Xi(z) \subseteq X_s\} \qquad \cup\, \Xi(z) = X_I(s)$$

Inconsistent states

- **A Y-state is consistent if at least one macro-control-decision is defined.**
- **A Z-state is consistent if all feasible events are defined.**



Supervisor Synthesis Procedure

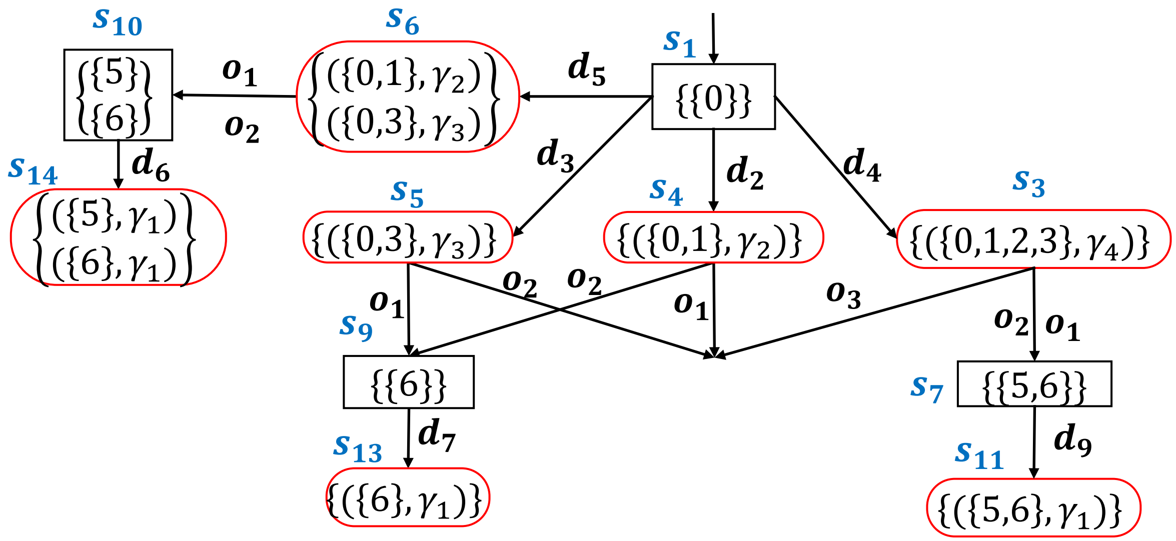
2. Delete all secret-revealing states and inconsistent states

Secret-revealing Z-states

$$Q_{reveal} = \{z \in \mathbb{M}^{+} : \cup\, \Xi(z) \subseteq X_s\} \qquad \cup\, \Xi(z) = X_I(s)$$

Inconsistent states

- **A Y-state is consistent if at least one macro-control-decision is defined.**
- **A Z-state is consistent if all feasible events are defined.**



Supervisor Synthesis Procedure

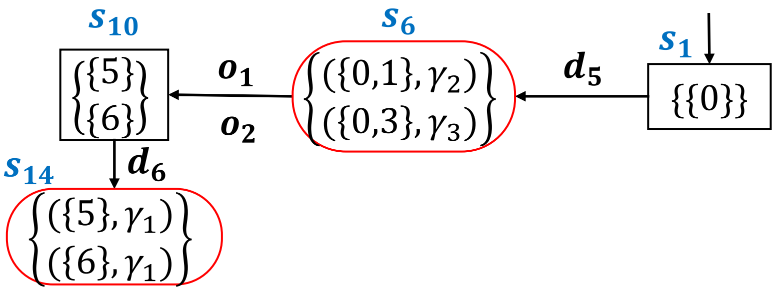
2. Delete all secret-revealing states and inconsistent states

Secret-revealing Z-states

$$Q_{reveal} = \{z \in \mathbb{M}^+ : \cup\, \Xi(z) \subseteq X_s\} \qquad \cup\, \Xi(z) = X_I(s)$$

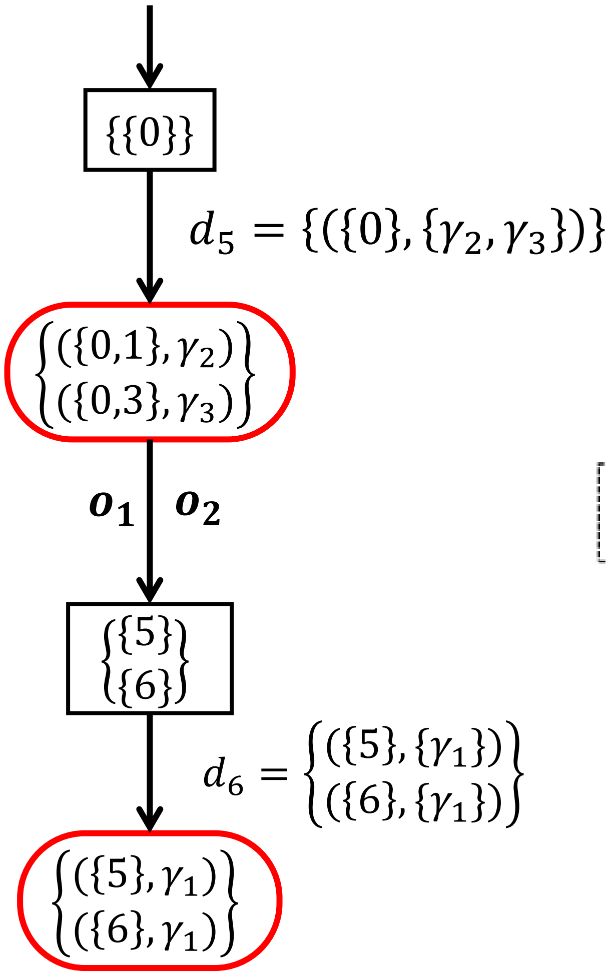
Inconsistent states

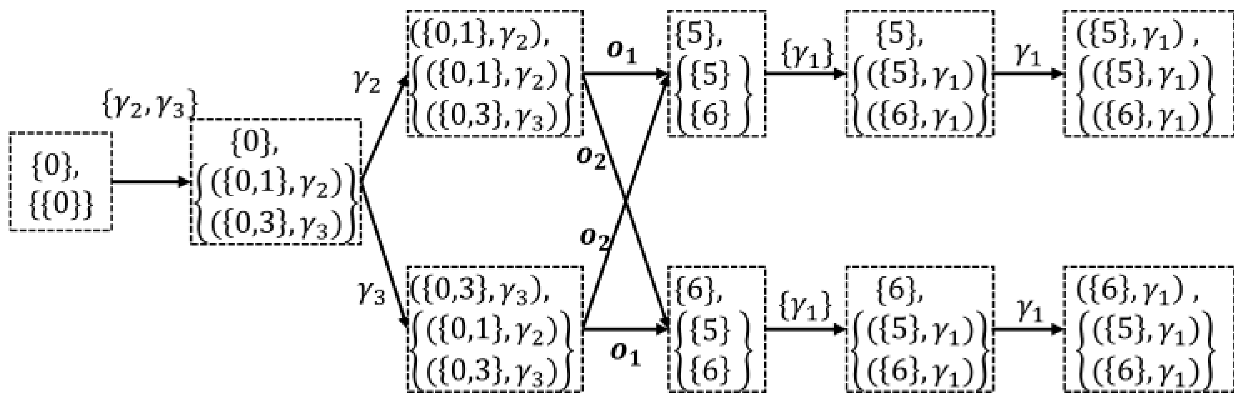
- A Y-state is consistent if at least one macro-control-decision is defined.
- A Z-state is consistent if all feasible events are defined.



Supervisor Synthesis Procedure

3. Arbitrarily pick a macro-control decision for each Y-state





Conclusion

- Propose non-deterministic control mechanism to enforce opacity
- Synthesize a non-deterministic supervisor based on the new information state
- Non-deterministic supervisors are strictly more powerful than deterministic supervisor

Conclusion

- Propose non-deterministic control mechanism to enforce opacity
- Synthesize a non-deterministic supervisor based on the new information state
- Non-deterministic supervisors are strictly more powerful than deterministic supervisor

Thank You!