Synthesis of Maximally-Permissive Supervisors for the Range Control Problem

Xiang Yin and Stéphane Lafortune

EECS Department, University of Michigan

ExCAPE Annual Meeting, May 09-10, 2016
Introduction

Control Engineering Perspective

- \( E = E_c \cup E_{uc} = E_o \cup E_{uo} \)
- Supervisor: \( S: E^*_o \rightarrow 2^E; \) Disable events in \( E_c \) based on its observations
- Closed-loop Behavior: \( \mathcal{L}(S/G) \) and \( \mathcal{L}_m(S/G) \)
Discrete Event Systems: Logical Properties

- Safety: Regular sublanguage $L_{am} \subseteq \mathcal{L}(G)$
Discrete Event Systems: Logical Properties

- Safety: Regular sublanguage $L_{am} \subseteq \mathcal{L}(G)$

- Non-blockingness: no deadlocks or livelocks
Discrete Event Systems: Logical Properties

- Safety: Regular sublanguage $L_{am} \subseteq \mathcal{L}(G)$
- Non-blockingness: no deadlocks or livelocks

Maximal Permissiveness: Optimality criterion is set inclusion. Only disable an event if absolutely necessary to guarantee safety and non-blockingness.
Non-Uniqueness of Locally Maximal Solutions

- Non-Uniqueness of Locally Maximal Solutions

\[ E_c = \{c\}, E_o = \{o\} \]

- Two incomparable solutions
Non-Uniqueness of Locally Maximal Solutions

- Non-Uniqueness of Locally Maximal Solutions

\[ E_c = \{c\}, E_o = \{o\} \]

- Two incomparable solutions

- How to choose among locally maximal solutions?
Range Control Problem

- Using Lower Bound Language as a Criterion

\[ \mathcal{L}(G) \]

\[ L_{am} \]

\[ Max_1 \]

\[ L_r \]

\[ Max_2 \]

Problem (Range Control Problem for Safety and Maximal-Permissiveness)

Let \( G \) be the plant and \( L_r \) and \( L_{am} \) be two prefix-closed languages. Find a supervisor \( S : E_o^* \rightarrow \Gamma \) such that

C1. \( L_r \subseteq \mathcal{L}(S/G) \subseteq L_{am} \)

C2. For any \( S' \) satisfying C1, we have \( \mathcal{L}(S/G) \nsubseteq \mathcal{L}(S'/G) \)
Current Status

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Safe+Max</th>
<th>Safe+NB</th>
<th>Safe+NB+Max</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized Upper Bound</strong></td>
<td>[1],[2],[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>OPEN</td>
</tr>
<tr>
<td><strong>Centralized Range</strong></td>
<td>[1],[2],[3]</td>
<td>OPEN</td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
</tbody>
</table>

[1] [Lin and Wonham, 1988]
[2] [Cieslak et al., 1988]
[3] [Rudie and Wonham, 1990]
[4] [Ben Hadj-Alouane et al., 1996]
[5] [Yoo and Lafortune, 2006]

Table: Summary of Problems in Partially-Observed DES literature
## Current Status

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Safe+Max</th>
<th>Safe+NB</th>
<th>Safe+NB+Max</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized</strong></td>
<td>[1],[2],[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>OPEN</td>
</tr>
<tr>
<td><strong>Upper Bound</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Centralized</strong></td>
<td>[1],[2],[3]</td>
<td>OPEN</td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Upper Bound</strong></td>
<td></td>
<td></td>
<td>[7],[8]</td>
<td></td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[1] [Lin and Wonham, 1988]  
[2] [Cieslak et al., 1988]  
[3] [Rudie and Wonham, 1990]  
[4] [Ben Hadj-Alouane et al., 1996]  
[5] [Yoo and Lafortune, 2006]  
[6] [Rudie and Wonham, 1992]  
[7] [Tripakis, 2004]  
[8] [Thistle, 2005]

**Table:** Summary of Problems in Partially-Observed DES literature
### Current Status

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Safe+Max</th>
<th>Safe+NB</th>
<th>Safe+NB+Max</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized Upper Bound</strong></td>
<td>[1],[2],[3]</td>
<td>[4]</td>
<td>[5]</td>
<td><strong>Last Year’s Talk [9]</strong></td>
</tr>
<tr>
<td><strong>Centralized Range</strong></td>
<td>[1],[2],[3]</td>
<td>OPEN</td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
<tr>
<td><strong>Decentralized Upper Bound</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable [7],[8]</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Decentralized Range</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
</tbody>
</table>

[1] [Lin and Wonham, 1988]  
[2] [Cieslak et al., 1988]  
[3][Rudie and Wonham, 1990]  
[4][Ben Hadj-Alouane et al., 1996]  
[5][Yoo and Lafortune, 2006]  
[6][Rudie and Wonham, 1992]  
[7][Tripakis, 2004]  
[8][Thistle, 2005]  
[9][Yin and Lafortune, 2016a]

**Table:** Summary of Problems in Partially-Observed DES literature
## Current Status

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Safe+Max</th>
<th>Safe+NB</th>
<th>Safe+NB+Max</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>Last Year’s Talk</strong></td>
</tr>
<tr>
<td>Upper Bound</td>
<td>[1],[2],[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[9]</td>
</tr>
<tr>
<td><strong>Centralized</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>OPEN</strong></td>
</tr>
<tr>
<td>Range</td>
<td>[1],[2],[3]</td>
<td>This Talk</td>
<td>OPEN</td>
<td><strong>OPEN</strong></td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>Undecidable</strong></td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>Undecidable</strong></td>
</tr>
<tr>
<td>Range</td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
</tbody>
</table>

[1] [Lin and Wonham, 1988]
[2] [Cieslak et al., 1988]
[3] [Rudie and Wonham, 1990]
[4] [Ben Hadj-Alouane et al., 1996]
[5] [Yoo and Lafortune, 2006]

[6] [Rudie and Wonham, 1992]
[7] [Tripakis, 2004]
[8] [Thistle, 2005]
[9] [Yin and Lafortune, 2016a]
[10] [Yin and Lafortune, 2016b]

### Table: Summary of Problems in Partially-Observed DES literature
Difficulties in the Range Control Problem

• The verification of maximal-permissiveness was still open (solved in [Yin and Lafortune, WODES, 2016])
The verification of maximal-permissiveness was still open (solved in [Yin and Lafortune, WODES, 2016])

Enabling less now may result in a larger future behavior

\[
E_c = \{c\}, \quad E_o = \{o\}
\]
• The verification of maximal-permissiveness was still open
  (solved in [Yin and Lafortune, WODES, 2016])

• Enabling less now may result in a larger future behavior

\[ E_c = \{c\}, E_o = \{o\} \]
The verification of maximal-permissiveness was still open (solved in [Yin and LaFortune, WODES, 2016])

Enabling less now may result in a larger future behavior

$E_C = \{c\}, E_O = \{o\}$
Difficulties in the Range Control Problem

- The verification of maximal-permissiveness was still open (solved in [Yin and Lafortune, WODES, 2016])

- Enabling less now may result in a larger future behavior

\[ E_c = \{c\}, E_o = \{o\} \]

- The effect of enabling an event depends on future information

\[ E_c = \{c\}, E_o = \{o\} \]
The verification of maximal-permissiveness was still open (solved in [Yin and Lafortune, WODES, 2016])

Enabling less now may result in a larger future behavior

The effect of enabling an event depends on future information

\[ E_c = \{c\}, E_o = \{o\} \]
Difficulties in the Range Control Problem

- The verification of maximal-permissiveness was still open (solved in [Yin and Lafortune, WODES, 2016])

- Enabling less now may result in a larger future behavior

\[ E_c = \{c\}, E_o = \{o\} \]

- The effect of enabling an event depends on future information

\[ E_c = \{c\}, E_o = \{o\} \]
Definition. (BTS).
A bipartite transition system $T$ w.r.t. $G$ is a 7-tuple
$$T = (Q_Y, Q_Z, h_{YZ}, h_{ZY}, E, \Gamma, y_0)$$
where
- $Q_Y \subseteq I$ is the set of $Y$-states;
- $Q_Z \subseteq I \times \Gamma$ is the set of $Z$-states so that $z = (I(z), \Gamma(z))$;
- $h_{YZ}: Q_Y \times \Gamma \rightarrow Q_Z$ represents the unobservable reach;
- $h_{ZY}: Q_Z \times E \rightarrow Q_Y$ represents the observation transition;
Definition. (AIC).

The All Inclusive Controller

\[ \mathcal{AIC}(G) = (Q_{Y}^{AIC}, Q_{Z}^{AIC}, h_{YZ}^{AIC}, h_{ZY}^{AIC}, E, \Gamma, y_0), \]

is defined as the largest BTS such

1. For any \( y \in Q_{Y}^{AIC} \), there exists at least one control decision
2. For any \( z \in Q_{Z}^{AIC} \), we have
   2.1. all feasible observable event are defined
   2.2. \( I(z) \) only contains legal states
The Infimal Supervisor

- If there exists a supervisor such that $L_r \subseteq \mathcal{L}(S/G) \subseteq L_{am}$, then there exists an infimal one.
- The infimal supervisor can be realized by a BTS.
Definition. (Control Simulation Relation)

Let \( T_1 \) and \( T_2 \) between BTSs. A relation \( \Phi = \Phi_Y \cup \Phi_Z \subseteq (Q^T_Y \times Q^T_Y) \times (Q^T_Z \times Q^T_Z) \) is said to be a control simulation relation from \( T_1 \) to \( T_2 \) if the following conditions hold:

1. \((y_0, y_0) \in \Phi_Y;\)
2. For every \((y_1, y_2) \in \Phi_Y, \) we have that: for any \( y_1 \overset{\gamma_1}{\rightarrow} z_1 \) in \( T_1, \) there exists \( y_2 \overset{\gamma_2}{\rightarrow} z_2 \) such that \((z_1, z_2) \in \Phi_Z \) and \( \gamma_1 \subseteq \gamma_2. \)
3. For every \((z_1, z_2) \in \Phi_Z, \) we have that: for any \( z_1 \overset{\sigma}{\rightarrow} y_1 \) in \( T_1, \) there exists \( z_2 \overset{\sigma}{\rightarrow} y_2 \) such that \((y_1, y_2) \in \Phi_Y. \)
Synthesis Steps:

1. Construct $\mathcal{AJC}(G)$ that contains all safe supervisors
2. Construct BTS $T_R$ that realizes the \textit{infimal} supervisor achieving $L_r$
3. Compute the maximal CSR $\Phi^*$ from $T_R$ to $\mathcal{AJC}(G)$
4. Construct BTS $T^*$ that realizes the \textit{maximal} supervisor achieving $L_r$ by using $T_R$, $\mathcal{AJC}(G)$ and $\Phi^*$
   - For each Y-state, enable as many events as possible without violating $\Phi^*$
Example

Graph $G$ and $R$ with labeled vertices and edges.
Step 1: Construct $\mathcal{AIC}(G)$
Example

Step 2: Construct the infimal BTS $T_R$
Step 3: Compute the maximal CSR $\Phi^*$
Example

Step 4: Construct the maximal BTS $T^*$
Step 4: Construct the maximal BTS $T^*$
Step 4: Construct the maximal BTS $T^*$
Step 4: Construct the maximal BTS $T^*$
Step 4: Construct the maximal BTS $T^*$
Step 4: Construct the maximal BTS $T^*$
## Summary

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Safe+Max</th>
<th>Safe+NB</th>
<th>Safe+NB+Max</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized</strong></td>
<td>[1],[2],[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[9]</td>
</tr>
<tr>
<td><strong>Upper Bound</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Centralized</strong></td>
<td>[1],[2],[3]</td>
<td><strong>This Talk</strong></td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Upper Bound</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[1] [Lin and Wonham, 1988]  
[2] [Cieslak et al., 1988]  
[3][Rudie and Wonham, 1990]  
[4][Ben Hadj-Alouane et al., 1996]  
[5][Yoo and Lafortune, 2006]  
[6][Rudie and Wonham, 1992]  
[7][Tripakis, 2004]  
[8][Thistle, 2005]  
[9][Yin and Lafortune, 2016a]  
[10][Yin and Lafortune, 2016b]
## Summary

<table>
<thead>
<tr>
<th></th>
<th>Safety</th>
<th>Safe+Max</th>
<th>Safe+NB</th>
<th>Safe+NB+Max</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centralized</strong></td>
<td>[1],[2],[3]</td>
<td>[4]</td>
<td>[5]</td>
<td>[9]</td>
</tr>
<tr>
<td><strong>Range</strong></td>
<td>[1],[2],[3]</td>
<td><strong>This Talk [10]</strong></td>
<td>OPEN</td>
<td>OPEN</td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable [7],[8]</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Upper Bound</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
<tr>
<td><strong>Decentralized</strong></td>
<td>[2],[6]</td>
<td>OPEN</td>
<td>Undecidable</td>
<td>Undecidable</td>
</tr>
</tbody>
</table>

[1] [Lin and Wonham, 1988]  
[2] [Cieslak et al., 1988]  
[3][Rudie and Wonham, 1990]  
[4][Ben Hadj-Alouane et al., 1996]  
[5][Yoo and LaFortune, 2006]  
[6][Rudie and Wonham, 1992]  
[7][Tripakis, 2004]  
[8][Thistle, 2005]  
[9][Yin and LaFortune, 2016a]  
[10][Yin and LaFortune, 2016b]  

- **Future Work**