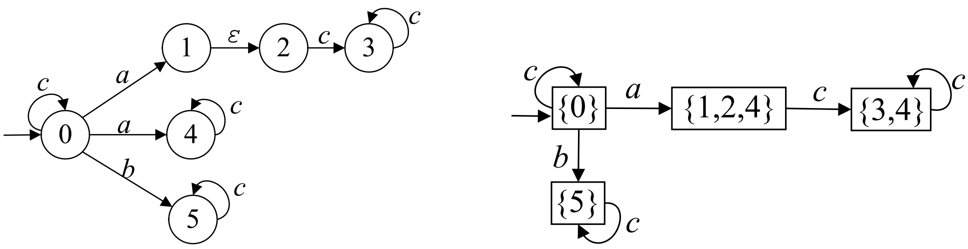
Stealthy Sensor Attacks for Violating Detectability of Discrete Event Systems

Yuling Zhang, Tenglong Kang, Abdulrahman Al-Ahmari, and Zhiwu Li, *Fellow, IEEE*

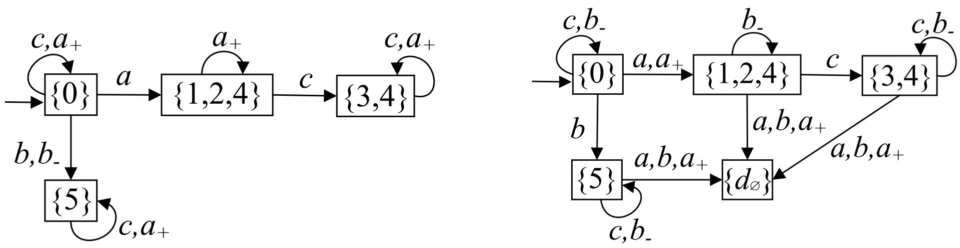
1 All examples in the manuscript

Example 1.1. Consider the plant G_{nd} in Fig. 1(a), where $X = \{0, 1, 2, 3, 4, 5\}$, $X_0 = \{0\}$, and $\Sigma = \Sigma_o = \{a, b, c\}$. The observer of G_{nd} is depicted in Fig. 1(b). Assume that $\Sigma_{ins} = \{a\}$ and $\Sigma_{era} = \{b\}$. The attacker observer G^{att}_{obs} and the operator observer G^{opr}_{obs} are shown in Fig. 2. ⋄



(a) G_{nd} (b) G_{obs}

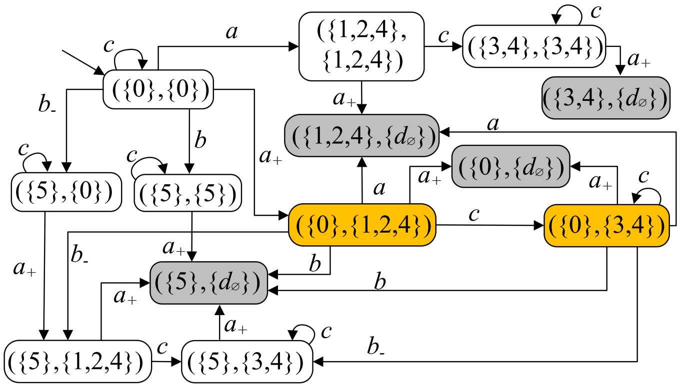
Figure 1: (a) A plant G_{nd} and (b) its observer G_{obs}.



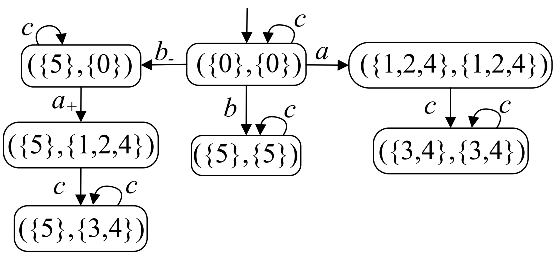
(a) G^{att}_{obs} (b) G^{opr}_{obs}

Figure 2: (a) Attacker observer G^{att}_{obs} and (b) Operator observer G^{opr}_{obs}.

The joint observer G^{J}_{obs} for G_{nd} in Fig. 1(a) and stealthy joint observer G^{SJ}_{obs} w.r.t. $\Sigma_{era} = \{b\}$ and $\Sigma_{ins} = \{a\}$ are portrayed in Fig. 3.



(a) Joint observer G^J_{obs}



(b) Stealthy joint observer G^{SJ}_{obs}

Figure 3: (a) Joint observer and (b) Stealthy joint observer w.r.t. $E_{era} = \{b\}$ and $E_{ins} = \{a\}$.

Note: The initial state of an NFA is numbered starting from 1 in programs, whereas in figures, the initial state is labeled as 0.

Input:

```
% NFA for the figure (G_nd)
n = 6;
E = {'a','b','c'};   % a=1, b=2, c=3 ; epsilon=0
T = [
1, 3, 1;   % 0 --c--> 0 (self-loop)
1, 1, 2;   % 0 --a--> 1
1, 1, 5;   % 0 --a--> 4
1, 2, 6;   % 0 --b--> 5
2, 0, 3;   % 1 --epsilon--> 2
3, 3, 4;   % 2 --c--> 3
4, 3, 4;   % 3 --c--> 3 (self-loop)
5, 3, 5;   % 4 --c--> 4
6, 3, 6;   % 5 --c--> 5
];
X0 = [1];   % initial state is 0 in the figure
Xm = [];    % no marked states shown
Gn = {n, E, T, X0, Xm};
Sigma_o   = {'a','b','c'};  % e.g., all observable
```

```
Sigma_ins = {'a'};              % insertable events
Sigma_era = {'b'};              % erasable events
```

Output:

```
===== Joint Observer (G_J) Statistics =====
G_J states count       : 13
G_J transitions count  : 27

===== Stealthy Joint Observer (SJ) Statistics =====
SJ states count       : 7
SJ transitions count  : 11

===== SJ states mapped to y-sets =====
( 0) ({1} , {1})
( 1) ({2  3  5} , {2  3  5})
( 2) ({6} , {6})
( 3) ({6} , {1})
( 4) ({4  5} , {4  5})
( 5) ({6} , {2  3  5})
( 6) ({6} , {4  5})

===== SJ transitions with y-sets =====
({1} , {1}) -- a --> ({2  3  5} , {2  3  5})
({1} , {1}) -- b --> ({6} , {6})
({1} , {1}) -- c --> ({1} , {1})
({1} , {1}) -- b_- --> ({6} , {1})
({2  3  5} , {2  3  5}) -- c --> ({4  5} , {4  5})
({6} , {6}) -- c --> ({6} , {6})
({6} , {1}) -- c --> ({6} , {1})
({6} , {1}) -- a_+ --> ({6} , {2  3  5})
({4  5} , {4  5}) -- c --> ({4  5} , {4  5})
({6} , {2  3  5}) -- c --> ({6} , {4  5})
({6} , {4  5}) -- c --> ({6} , {4  5})
```

Example 1.2. Consider the plant on the left of Fig. 4 with its observer depicted on the middle. Assume that $\Sigma_{era} = \{d, e\}$ and $\Sigma_{ins} = \emptyset$. The stealthy joint observer for the plant is shown on the right of Fig. 4.

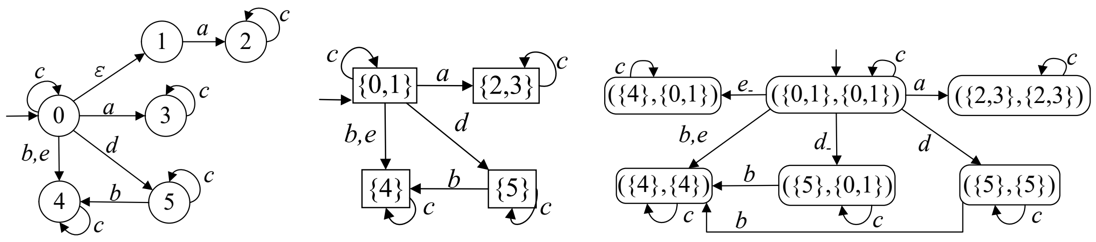


Figure 4: Plant (left), its observer (middle), and stealthy joint observer (right).

Input:

```
n = 6;
E = {'a','b','c','d','e'};   % a=1, b=2, c=3, d=4, e=5;  epsilon=0
T = [
1, 3, 1;   % 0 --c--> 0
1, 0, 2;   % 0 --epsilon--> 1
1, 1, 4;   % 0 --a--> 3
1, 4, 6;   % 0 --d--> 5
1, 2, 5;   % 0 --b--> 4
1, 5, 5;   % 0 --e--> 4
2, 1, 3;   % 1 --a--> 2
3, 3, 3;   % 2 --c--> 2
4, 3, 4;   % 3 --c--> 3
6, 2, 5;   % 5 --b--> 4
6, 3, 6;   % 5 --c--> 5
5, 3, 5;   % 4 --c--> 4
];
X0 = [1];     % initial state is node 0 in the figure
Xm = [];      % (no marked states in the figure)
Gn = {n, E, T, X0, Xm};
Sigma_o   = {'a','b','c','d','e'};
Sigma_ins = {};
Sigma_era = {'d','e'};
```

Output:

```
===== Joint Observer (G_J) Statistics =====
G_J states count       : 6
G_J transitions count  : 14
```

```
===== Stealthy Joint Observer (SJ) Statistics =====
SJ states count       : 6
SJ transitions count  : 14

===== Stealthy Trimmed Observers =====
GSJ1_A states count       : 0
GSJ1_A transitions count  : 0
GSJ1_B states count       : 0
GSJ1_B transitions count  : 0

===== SJ states mapped to y-sets =====
( 0) ({1  2} , {1  2})
( 1) ({3  4} , {3  4})
( 2) ({5} , {5})
( 3) ({6} , {6})
( 4) ({6} , {1  2})
( 5) ({5} , {1  2})

===== SJ transitions with y-sets =====
({1  2} , {1  2}) -- a --> ({3  4} , {3  4})
({1  2} , {1  2}) -- b --> ({5} , {5})
({1  2} , {1  2}) -- c --> ({1  2} , {1  2})
({1  2} , {1  2}) -- d --> ({6} , {6})
({1  2} , {1  2}) -- e --> ({5} , {5})
({1  2} , {1  2}) -- d_- --> ({6} , {1  2})
({1  2} , {1  2}) -- e_- --> ({5} , {1  2})
({3  4} , {3  4}) -- c --> ({3  4} , {3  4})
({5} , {5}) -- c --> ({5} , {5})
({6} , {6}) -- b --> ({5} , {5})
({6} , {6}) -- c --> ({6} , {6})
({6} , {1  2}) -- b --> ({5} , {5})
({6} , {1  2}) -- c --> ({6} , {1  2})
({5} , {1  2}) -- c --> ({5} , {1  2})
```

Example 1.3. Let us reconsider the plant G_{nd} in Fig. 1(a). Suppose that $\Sigma_{ins} = \{a\}$ and $\Sigma_{era} = \{a, b\}$. The stealthy joint observer G^{SJ}_{obs} is shown in Fig. 5, while the structure in the orange dotted box is $G^{SJ,1}_{obs}$. On the other hand, $G^{SJ,2}_{obs}$ is obtained by removing the portion from the initial state to $(\{5\}, \{5\})$ from G^{SJ}_{obs}.

In the observer of G_{nd}, there are two detectable cycles ($cl_1 = \{0\} \xrightarrow{c} \{0\}$ and $cl_2 = \{5\} \xrightarrow{c} \{5\}$) and one undetectable cycle ($cl = \{3, 4\} \xrightarrow{c} \{3, 4\}$). It is verified that each detectable cycle has an ambiguity-inducing cycle, and each undetectable cycle has a determinacy-inducing cycle (see Example 4.6 in the manuscript for more details). Therefore, condition C1 or C2 in Theorem 4.5 is satisfied, indicating the existence of a successful attacker.

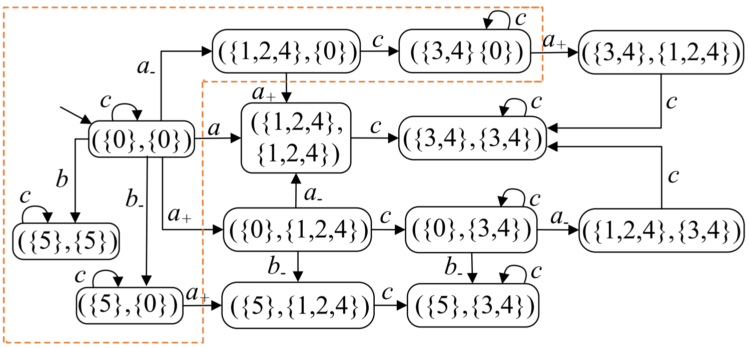


Figure 5: Stealthy joint observer G^{SJ}_{obs} for $E_{era} = \{a, b\}$ and $E_{ins} = \{a\}$.

◇

Output:

```
===== GSJ1_A =====
GSJ1_A states count       : 5
GSJ1_A transitions count  : 8

===== GSJ1_B =====
GSJ1_B states count       : 12
GSJ1_B transitions count  : 23

===== GSJ1_B states with y-sets =====
( 0) ({1} , {1})
( 1) ({2  3  5} , {2  3  5})
( 2) ({1} , {2  3  5})
( 3) ({2  3  5} , {1})
( 4) ({6} , {1})
( 5) ({4  5} , {4  5})
( 6) ({1} , {4  5})
( 7) ({6} , {2  3  5})
( 8) ({4  5} , {1})
( 9) ({2  3  5} , {4  5})
```

```
(10) ({6} , {4  5})
(11) ({4  5} , {2  3  5})

===== GSJ1_B transitions with y-sets =====
({1} , {1}) -- a --> ({2  3  5} , {2  3  5})
({1} , {1}) -- c --> ({1} , {1})
({1} , {1}) -- a_+ --> ({1} , {2  3  5})
({1} , {1}) -- a_- --> ({2  3  5} , {1})
({1} , {1}) -- b_- --> ({6} , {1})
({2  3  5} , {2  3  5}) -- c --> ({4  5} , {4  5})
({1} , {2  3  5}) -- c --> ({1} , {4  5})
({1} , {2  3  5}) -- a_- --> ({2  3  5} , {2  3  5})
({1} , {2  3  5}) -- b_- --> ({6} , {2  3  5})
({2  3  5} , {1}) -- c --> ({4  5} , {1})
({2  3  5} , {1}) -- a_+ --> ({2  3  5} , {2  3  5})
({6} , {1}) -- c --> ({6} , {1})
({6} , {1}) -- a_+ --> ({6} , {2  3  5})
({4  5} , {4  5}) -- c --> ({4  5} , {4  5})
({1} , {4  5}) -- c --> ({1} , {4  5})
({1} , {4  5}) -- a_- --> ({2  3  5} , {4  5})
({1} , {4  5}) -- b_- --> ({6} , {4  5})
({6} , {2  3  5}) -- c --> ({6} , {4  5})
({4  5} , {1}) -- c --> ({4  5} , {1})
({4  5} , {1}) -- a_+ --> ({4  5} , {2  3  5})
({2  3  5} , {4  5}) -- c --> ({4  5} , {4  5})
({6} , {4  5}) -- c --> ({6} , {4  5})
({4  5} , {2  3  5}) -- c --> ({4  5} , {4  5})
Qp (idx 0-based): 0 4 8
0 : ({1} , {1})
4 : ({6} , {1})
8 : ({4 5} , {1})
===== SUMMARY =====
Detected 3 obs-cycles; detectable=2, undetectable=1
GSJ1 cycles: 4, GSJ2 cycles: 6
C1 (determinacy for undetectable cycles) => 1
C2 (ambiguity for detectable cycles) => 1
=> At least one of C1 or C2 holds -> a successful attacker exists
C1_all_true: 1
C2_all_true: 1
exists_attack: 1
```

2 The case study in the manuscript

As depicted in Fig. 6, the set of states is $X = \{1, 2, \ldots, 9\}$, the set of events is $\Sigma = \{a, b, c, d\}$. We assume that there is an attacker who can insert and erase events b and d, i.e., $\Sigma_{ins} = \Sigma_{era} = \{b, d\}$. Fig. 7 is the stealthy joint observer G^{SJ}_{obs} for the plant. It is computed that $G^{SJ,1}_{obs} = \emptyset$ and $G^{SJ,2}_{obs} = G^{SJ}_{obs}$. There is only one detectable cycle $cl = \{5\} \xrightarrow{a} \{4\} \xrightarrow{b} \{7\} \xrightarrow{c} \{5\}$ in the observer of the plant. It is seen that $cl' = (\{5\}, \{2, 9\}) \xrightarrow{a} (\{4\}, \{6, 8\}) \xrightarrow{b_-} (\{7\}, \{6, 8\}) \xrightarrow{c} (\{5\}, \{2, 9\})$ is an ambiguity-inducing cycle of cl in $G^{SJ,2}_{obs}$. Therefore, a stealthy attacker exists that can violate the detectability of the plant.

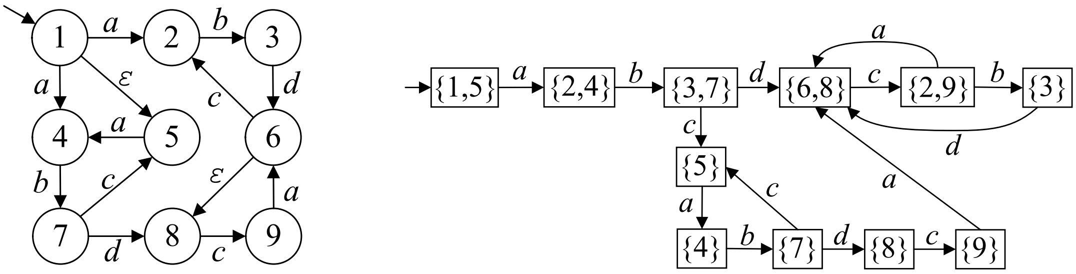


Figure 6: Plant and its observer for the case study in the manuscript.

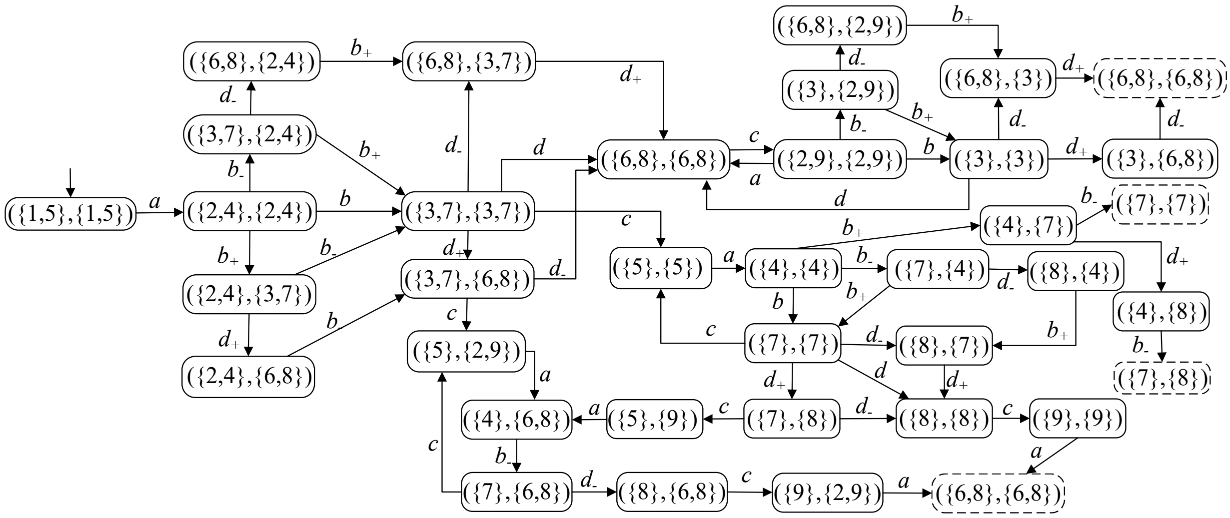


Figure 7: Stealthy joint observer for the plant.

Output:

```
===== Joint Observer (G_J) Statistics =====
G_J states count       : 60
G_J transitions count  : 183

===== Stealthy Joint Observer (SJ) Statistics =====
SJ states count       : 33
SJ transitions count  : 55
```

```
===== Stealthy Trimmed Observers =====
GSJ1_A states count       : 0
GSJ1_A transitions count  : 0
GSJ1_B states count       : 33
GSJ1_B transitions count  : 55

===== SUMMARY =====
Detected 3 obs-cycles; detectable=1, undetectable=2
GSJ1 cycles: 0, GSJ2 cycles: 12
C1 (determinacy for undetectable cycles) => 0
C2 (ambiguity for detectable cycles) => 1
=> At least one of C1 or C2 holds -> a successful attacker exists
```