Supplementary material concerning the paper "Estimation and Prevention of Sensor Replacement Attacks in Supervisory Control Systems"

I. Proof of Theorem 1

Theorem 1: A closed-loop system S/G is strongly SR-estimable w.r.t. P_o^a, Σ_a, and X_u iff there exists a state b_o in $E_{S/G}$ such that $Fir(b_o) \subseteq X_u$.

Proof: ($\Leftarrow$) Suppose that there exists a state b_o in $E_{S/G}$ such that $Fir(b_o) \subseteq X_u$. For all states (x, q) in b_o, we have $x \in X_u$. According to the construction of $E_{S/G}$, for any decision string $\phi \in \Sigma_o \times (\Sigma_o \cup \{\varepsilon\})$ such that $f_e(b_{0,o}, \phi) = b_o$, we have that for all decision strings $\omega' \in P_o^{a-1}(\phi) \cap L(M_a)$, $f(x_0, \alpha(\omega')) \in X_u$. Then, there exists $\omega \in L(M_a)$ with $P_o^a(\omega) = P_o^a(\omega') = \phi$ such that the condition in Definition 1 holds, i.e., S/G is strongly SR-estimable w.r.t. P_o^a, Σ_a, and X_u.

($\Rightarrow$) Suppose that S/G is strongly SR-estimable w.r.t. P_o^a, Σ_a, and X_u. Then, there exists a decision string $\omega \in L(M_a)$ such that the condition in Definition 1 hold. Let $\phi = P_o^a(\omega)$. By Definition 3, it holds $\phi \in L(E_{S/G})$, i.e., there exists a state b_o such that $f_e(b_{0,o}, \phi) = b_o$. For any state (x, q) in b_o, there exists a decision string $\omega' \in P_o^{a-1}(\phi) \cap L(M_a)$ such that $f_a((x_0, q_0), \omega') = (x, q)$ and $x \in X_u$, i.e., $Fir(b_o) \subseteq X_u$. Thus, Theorem 1 holds. ■

II. Proof of Theorem 2

Theorem 2: A closed-loop system S/G is weakly SR-estimable w.r.t. P_o, Σ_a, and X_u iff the following two conditions hold: (1) There exists a state b_o in $E_{S/G}$ such that $Fir(b_o) \cap X_u \neq \emptyset$; and (2) For all states b'_o in $E_{S/G}$, $Fir(b'_o) \cap (X \setminus X_u) \neq \emptyset$.

Proof: ($\Leftarrow$) Suppose that there exists a state b_o in $E_{S/G}$ such that $Fir(b_o) \cap X_u \neq \emptyset$. Then, there exists a state (x, q) in b_o such that $x \in X_u$. According to the construction of $E_{S/G}$, given a decision string $\phi \in \Sigma_o \times (\Sigma_o \cup \{\varepsilon\})$ such that $f_e(b_{0,o}, \phi) = b_o$, there exists a decision string $\omega \in P_o^{a-1}(\phi) \cap L(M_a)$ such that $f(x_0, \alpha(\omega)) \in X_u$, i.e., condition (1) in Definition 2 hold. Suppose that for all states b'_o in $E_{S/G}$, $Fir(b'_o) \cap (X \setminus X_u) \neq \emptyset$, i.e., there exists a state (x', q') in b'_o such that $x' \notin X_u$. According to Theorem 1, S/G is not strongly SR-estimable w.r.t. P_o^a, Σ_a, and X_u. By Definition 2, we conclude that S/G is weakly SR-estimable w.r.t. P_o^a, Σ_a, and X_u.

($\Rightarrow$) Suppose that S/G is weakly SR-estimable w.r.t. P_o^a, Σ_a, and X_u. Then, there exists a decision string $\omega \in L(M_a)$ such that $f(x_0, \alpha(\omega)) \in X_u$, and S/G is not strongly SR-estimable w.r.t. P_o^a, Σ_a, and X_u. Due to $P_o^a(\omega) \in L(E_{S/G})$, there exists a state (b_o, d_o) such that $f_e(b_{0,o}, P_o^a(\omega)) = b_o$. By $f(x_0, \alpha(\omega)) \in X_u$, there exists a state (x, q) in b_o such that $x \in X_u$ (i.e., $Fir(b_o) \cap X_u \neq \emptyset$). By Theorem 1, for any state b'_o in $E_{S/G}$, there exists (x', q') in b'_o such that $x' \notin X_u$, i.e., $Fir(b'_o) \cap (X \setminus X_u) \neq \emptyset$. This completes the proof. ■

III. Proof of Theorem 3

Theorem 3: Given an attacker estimator $E_{S/G}$ w.r.t. a closed-loop system S/G, (1) let $L_{sb} \neq \emptyset$ and $BS = BS_s$. An SSR-safe DI-function D exists if and only if the DIS Υ^{BS} w.r.t. $E_{S/G}$ and BS is not an empty automaton; (2) let $L_{sb} \cup L_{wb} \neq \emptyset$ and $BS = BS_s \cup BS_w$. An SR-safe DI-function D exists if and only if the DIS Υ^{BS} w.r.t. $E_{S/G}$ and BS is not an empty automaton.

Proof: (1) ($\Leftarrow$) If the DIS Υ^{BS} is not the empty automaton, there exists an SSR-safe DI-function D that can be synthesized from Υ^{BS} according to Proposition 1.

($\Rightarrow$) If an SSR-safe DI-function D exists, it holds that D can be synthesized from the DIS based on Proposition 1. Then, the DIS is not an empty automaton. Thus, this theorem holds.

(2) It can be proved in the same way as (1). ■

IV. Construction of a DIS

We briefly review the construction of an "All insertion structure" in [1]. Let $\mathscr{D} = (M_1, \Sigma, \delta_1, m_{0,1})$ and $\mathscr{A} = (M_2, \Sigma, \delta_2, m_{0,2})$ be two automata.

In [1], the set of all information states is denoted by $\mathcal{Q} = M_1 \times M_2$, and the AIS is the tuple:

$$\mathrm{AIS} = (Y, Z, \Sigma, M_1, f_{\mathrm{AIS},yz}, f_{\mathrm{AIS},zy}, y_0)$$

where Σ is the set of events in $\mathscr{A}$. M_1 is the set of states in $\mathscr{D}$. $Y \subseteq \mathcal{Q}$ is the set of Y-states. $Z \subseteq \mathcal{Q} \times \Sigma$ is the set of Z-states. Let $\mathcal{Q}(z)$, $\mathcal{E}(z)$ denote the information state component and event component of $z \in Z$ respectively, so that $z = (\mathcal{Q}(z), \mathcal{E}(z))$. $f_{\mathrm{AIS},yz} : Y \times \Sigma \to Z$ is the transition function from Y-state to Z-state. For $y = (m_1, m_2) \in Y$, $\sigma \in \Sigma$, we have: $f_{\mathrm{AIS},yz}(y, \sigma) = z \Rightarrow [\delta_2(m_2, \sigma)!] \wedge [\mathcal{Q}(z) = y] \wedge [\mathcal{E}(z) = \sigma]$. $f_{\mathrm{AIS},zy} : Z \times M_1 \to Y$ is the transition function from

Z-state to Y-state. For $z = ((m_1, m_2), \sigma) \in Z$, $m_1' \in M_1$, we have: $f_{\text{AIS},zy}(z, m_1') = y \Rightarrow [\exists s \in \Sigma^* \text{s.t.} \delta_1(m_1, s) = m_1'] \wedge [\delta_1(m_1', \sigma)!] \wedge [y = (\delta_1(m_1', \sigma), \delta_2(m_2, \sigma))]$. $y_0 \in Y$ is the unique initial Y-state, where $y_0 = (m_{0,1}, m_{0,2})$.

Given two automata $\mathscr{D} = (M_1, \Sigma, \delta_1, m_{0,1})$ and $\mathscr{A} = (M_2, \Sigma, \delta_2, m_{0,2})$, the construction procedure for the AIS consist of two steps: (1) obtaining the AIS$_{pre}$; and (2) obtaining the AIS. Based on $\mathscr{D}$ and $\mathscr{A}$, the game-like structure AIS$_{pre}$ can be obtained in Algorithm 1. In Algorithm 2, the AIS can be obtained by pruning away all the inappropriate insertion choices in the AIS$_{pre}$.

Algorithm 1: Construction AIS$_{pre}$ in [1]

```
   Input: $\mathscr{D} = (M_1, \Sigma, \delta_1, m_{0,1})$ and $\mathscr{A} = (M_2, \Sigma, \delta_2, m_{0,2})$
   Output: AIS$_{pre} = (Y, Z, \Sigma, M_1, f_{\text{AIS}_{pre},yz}, f_{\text{AIS}_{pre},zy}, y_0)$
1  $y_0 := (m_{0,1}, m_{0,2})$, $Y := \{y_0\}$, $Z := \emptyset$;
2  for all $y = (m_1, m_2) \in Y$ that have not been examined do
3      for $\sigma \in \Sigma$ do
4          if $\delta_2(m_2, \sigma)$ is defined then
5              $f_{\text{AIS}_{pre},yz}(y, \sigma) := (y, \sigma)$;
6              $Z := Z \cup \{f_{\text{AIS}_{pre},yz}(y, \sigma)\}$;
7  for all $z = (y, \sigma) = ((m_1, m_2), \sigma) \in Z$ that have not been examined do
8      for $m' \in M_1$ do
9          if $\delta_1(m', \sigma)$ is defined and $\exists t \in \Sigma^*$ such that $m' = \delta_1(m', t)$ then
10             $f_{\text{AIS}_{pre},zy}(z, m') := (\delta_1(m', \sigma), \delta_2(m_2, \sigma))$;
11             $Y := Y \cup \{f_{\text{AIS}_{pre},zy}(z, m')\}$;
12 Go back to step 2, repeat until all accessible part has been built;
```

Algorithm 2: Construct AIS in [1]

```
   Input: AIS$_{pre} = (Y, Z, \Sigma, M_1, f_{\text{AIS}_{pre},yz}, f_{\text{AIS}_{pre},zy}, y_0)$
   Output: AIS $= (Y, Z, \Sigma, M_1, f_{\text{AIS},yz}, f_{\text{AIS},zy}, y_0)$
1  Obtain an automaton as
     $A = (Y \cup Z, \Sigma \cup M_1, f_{\text{AIS}_{pre},yz} \cup f_{\text{AIS}_{pre},zy}, y_0)$;
2  Mark all the $Y$-states in $A$;
3  Let $\Sigma$ be uncontrollable and $M_1$ be controllable;
4  Trim $A$ and let $A_{trim}$ be the specification automaton;
5  Obtain the AIS as the automaton obtained from
     $[L_m(A_{trim})]^{\uparrow C}$ w.r.t. $L(A)$ by following the standard
     $\uparrow C$ algorithm in [2];
6  return the AIS as
     AIS $= (Y, Z, \Sigma, M_1, f_{\text{AIS},yz}, f_{\text{AIS},zy}, y_0)$;
```

Algorithm 3: Construction of DIS

```
   Input: An attacker estimator $E_{S/G} = (B_o, \Sigma_o \times (\Sigma_o \cup \{\varepsilon\}), f_e, b_{0,o})$ and a bad state set $BS \in \{BS_s, BS_s \cup BS_w\}$
   Output: A DIS $\Upsilon^{BS} = (I_y, I_z, \Xi, B_o^{BS}, f_{yz}, f_{zy}, y_0)$
1  Construct a safe estimator
     $E_{S/G}^{BS} = (B_o^{BS}, \Sigma_o \times (\Sigma_o \cup \{\varepsilon\}), f_e^{BS}, b_{0,o})$ by
     removing all the sets in $BS$ from $E_{S/G}$ and keeping
     the accessible part;
2  $I_y := \{y_0\} = \{(b_{0,o}, b_{0,o})\}$, $I_z := \emptyset$;
3  for all $i_y = (b_{o1}, b_{o2}) \in I_y$ that have not been examined do
4      for $\sigma_{\sigma'} \in \Xi$ do
5          if $f_e(b_{o2}, \sigma_{\sigma'})!$ then
6              $f_{pre,yz}(i_y, \sigma_{\sigma'}) := (i_y, \sigma_{\sigma'})$;
7              $I_z := I_z \cup \{f_{pre,yz}(i_y, \sigma_{\sigma'})\}$;
8  for all $i_z = (i_y, \sigma_{\sigma'}) = ((b_{o1}, b_{o2}), \sigma_{\sigma'}) \in I_z$ that have not been examined do
9      for $b_{o1}' \in B_o^{BS}$ do
10         if $f_e^{BS}(b_{o1}', \sigma_{\sigma'})!$ and there exists $\omega \in \Xi^*$ such that $b_{o1}' = f_e^{BS}(b_{o1}, \omega)$ then
11             $f_{pre,zy}(i_z, b_{o1}') :=$
                 $(f_e^{BS}(b_{o1}', \sigma_{\sigma'}), f_e(b_{o2}, \sigma_{\sigma'}))$;
12             $I_y := I_y \cup \{f_{pre,zy}(i_z, b_{o1}')\}$;
13 Go back to step 2, repeat until all accessible part has
     been built, and build an automaton as
     $\Upsilon = (I_y \cup I_z, \Xi \cup B_o^{BS}, f_{pre,yz}, f_{pre,zy}, y_0)$;
14 Mark all the $Y$-states in $\Upsilon$;
15 Let $\Xi$ be uncontrollable and $B_o^{BS}$ be controllable;
16 Trim $\Upsilon$ and let $\Upsilon_{trim}$ be the specification automaton;
17 Construct DIS $\Upsilon^{BS}$ as the automaton obtained from
     $[L_m(\Upsilon_{trim})]^{\uparrow C}$ w.r.t. $L(\Upsilon)$ by using the standard
     $\uparrow C$ algorithm in [2];
18 return DIS as $\Upsilon^{BS} = (I_y, I_z, \Xi, B_o^{BS}, f_{yz}, f_{zy}, y_0)$;
```

Next, we integrate these two algorithms and transform them into one algorithm (Algorithm 3 in the supplementary material) to build a DIS in our work. Given an attacker estimator $E_{S/G}$ and a bad state set $BS \in \{BS_s, BS_s \cup BS_w\}$, we first obtain a safe estimator $E_{S/G}^{BS}$ w.r.t. S/G and BS by removing all the states in BS from $E_{S/G}$ and keeping the accessible part in step 1. Step 2 initializes the sets I_y and I_z. Steps 3–7 and 8–12 define the transitions from Y-states to Z-states and the transitions from Z-states to Y-states, respectively. In step 13, we built an automaton $\Upsilon = (I_y \cup I_z, \Xi \cup B_o^{BS}, f_{pre,yz}, f_{pre,zy}, y_0)$. We prune away all inadmissible insertion cases that lead to deadlock at Z-states in Υ by steps 14–17. In step 18, a DIS is constructed. Given an estimator with $|B_o|$ states and the set of observable decision events Ξ, an obtained DIS has at most $(|\Xi| + 1)|B_o|^2$ states, and the computational complexity for constructing the DIS is $\mathcal{O}(|B_o|^6)$ by referring to [4].

Algorithm 3 is an integrated version of Algorithms 1 and 2 in [1]. Intuitively, we first take the automata $E_{S/G}^{BS}$ and $E_{S/G}$ as the input of Algorithm 1, i.e., substituting the automata $E_{S/G}^{BS}$ and $E_{S/G}$ for the automata $\mathscr{D}$ and $\mathscr{A}$, respectively. Then, we go directly to the step 1 of Algorithm 2 to obtain an automaton $\Upsilon = (I_y \cup I_z, \Xi \cup B_o^{BS}, f_{pre,yz}, f_{pre,zy}, y_0)$. Finally, we build a DIS Υ^{BS} by pruning away all inadmissible insertion cases that lead to deadlock at Z-states in Υ.

V. Figure of Example 5

We build an automaton Υ based on $E_{S/G}$ and $BS = BS_s$ as shown in Fig. 1 of this supplementary material. All dashed states and arcs should be pruned since they correspond to inadmissible insertion cases, and a DIS Υ^{BS} is obtained. We use $\sigma_{\sigma'}$ and $\sigma_{1\sigma_1'}$ to represent any event in decision event sets $\{b_b, b_\varepsilon, b_d\}$ and $\{b_b, b_\varepsilon, b_d, d_d, d_\varepsilon, d_b\}$, respectively. For instance, we use a transition $f_{yz}(\chi_6\chi_6, \sigma_{\sigma'}) = (\chi_6\chi_6, \sigma_{\sigma'})$ to briefly represent the transitions $f_{yz}(\chi_6\chi_6, b_b) = (\chi_6\chi_6, b_b)$, $f_{yz}(\chi_6\chi_6, b_\varepsilon) = (\chi_6\chi_6, b_\varepsilon)$, and $f_{yz}(\chi_6\chi_6, b_d) = (\chi_6\chi_6, b_d)$.

VI. Figure of Example 6

In Fig. 2 of this supplementary material, an automaton Υ is constructed based on $E_{S/G}$ and $BS = BS_s \cup BS_w$, and a DIS Υ^{BS} is obtained by removing all the dashed states and arcs in Υ.

References

[1] R. Liu and J. Lu, “Enforcement for infinite-step opacity and k-step opacity via insertion mechanism,” *Automatica*, vol. 140, p. 110212, Jun. 2022.

[2] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Springer Science & Business Media, 2009.

[3] Y.-C. Wu and S. Lafortune, “Synthesis of insertion functions for enforcement of opacity security properties,” *Automatica*, vol. 50, no. 5, pp. 1336–1348, May 2014.

[4] Y. Ji, Y.-C. Wu, and S. Lafortune, “Enforcement of opacity by public and private insertion functions,” *Automatica*, vol. 93, pp. 369–378, Jul. 2018.

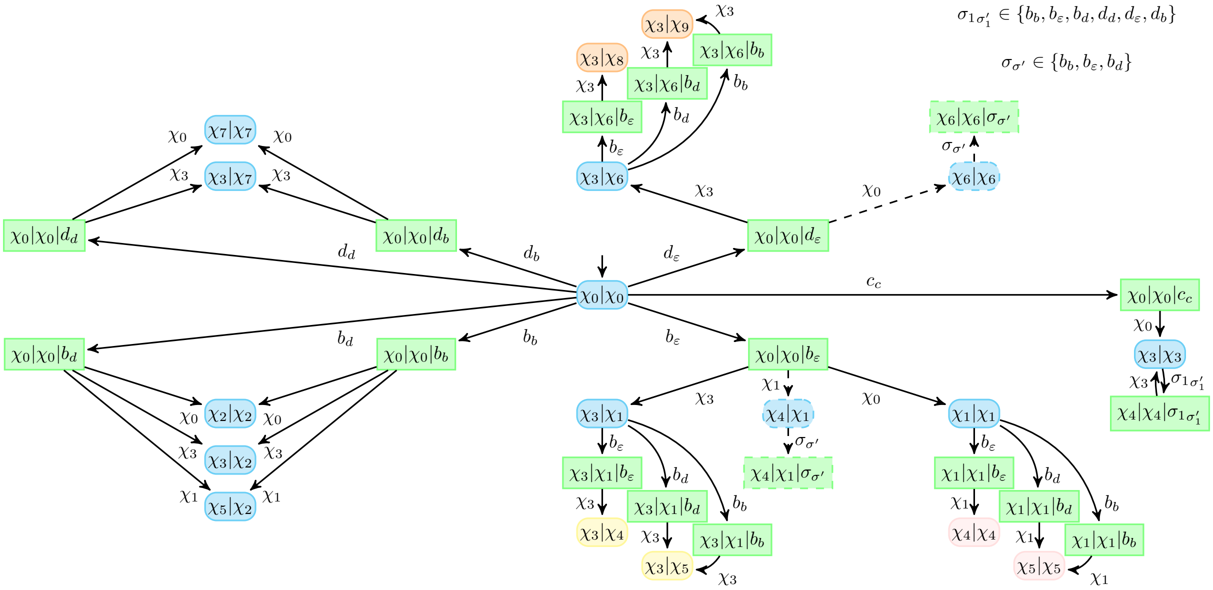

Fig. 1. A DIS w.r.t. $\boldsymbol{E_{S/G}}$ and $\boldsymbol{BS_s}$ in Example 5.

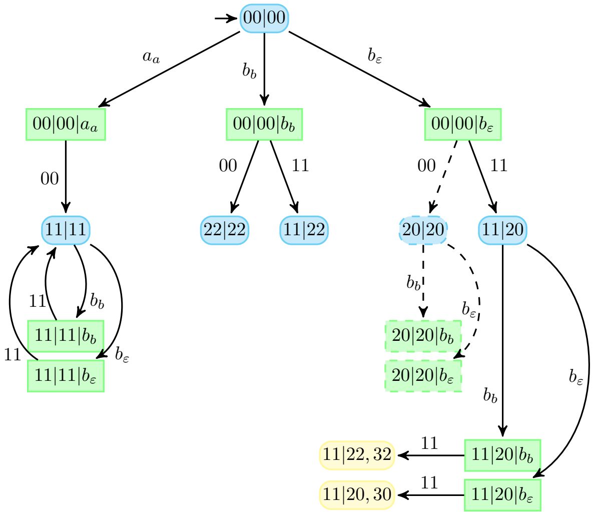

Fig. 2. A DIS w.r.t. $\boldsymbol{E_{S/G}}$ and $\boldsymbol{BS_s} \cup \boldsymbol{BS_w}$ in Example 6.