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. Algorithm for Constructing a DIS

By following the existing algorithms for constructing insertion structures in [16]–[18], Algorithm 1 is proposed to formally build a DIS. Based on a given attacker estimator and a bad state set, we construct a safe estimator 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. We prune away all inadmissible insertion cases that lead to deadlock at Z-states in steps 13–17. 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 [17].

References

[1] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-cps: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Syst.J.*, vol. 11, no. 1, pp. 88–95, Mar. 2017.

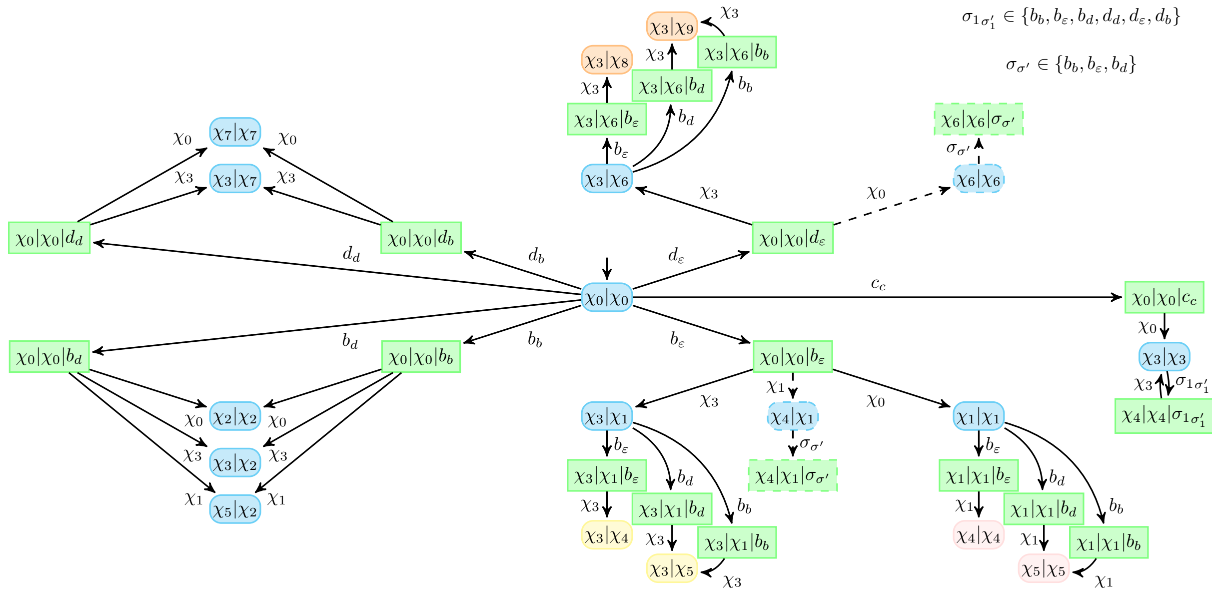

Fig. 1. A DIS w.r.t. $E_{S/G}$ and BS_s in Example 5.

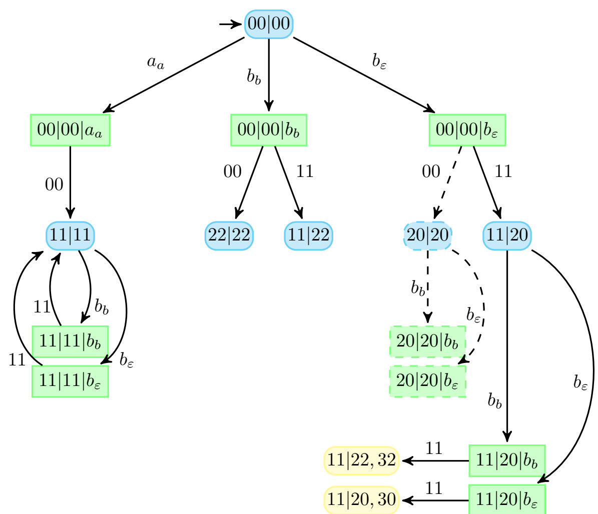

Fig. 2. A DIS w.r.t. $E_{S/G}$ and $BS_s \cup BS_w$ in Example 6.

[2] P. J. Ramadge and W. M. Wonham, "Supervisory control of a class of discrete event processes," *SIAM J. Control Optim.*, vol. 25, no. 1, pp. 206–230, Jan. 1987.

[3] A. Rashidinejad, B. Wetzels, M. Reniers, L. Lin, Y. Zhu, and R. Su, "Supervisory control of discrete-event systems under attacks: An overview and outlook," in *Proc. 18th Eur. Control Conf. (ECC)*, Naples, Italy, Jun. 2019, pp. 1732–1739.

[4] Q. Zhang, C. Seatzu, Z. Li, and A. Giua, "Selection of a stealthy and harmful attack function in discrete event systems," *Sci. Rep.*, vol. 12, no. 1, p. 16302, Sep. 2022.

[5] Y. Li, C. N. Hadjicostis, N. Wu, and Z. Li, "Error- and tamper-tolerant state estimation for discrete event systems under cost constraints," *IEEE Trans. Autom. Control*, pp. 1–8, Feb. 2023, doi: 10.1109/TAC.2023.3239590.

[6] R. Meira-Góes, E. Kang, R. H. Kwong, and S. Lafortune, "Stealthy deception attacks for cyber-physical systems," in *Proc. 56th IEEE Conf. Decis. Control (CDC)*, Melbourne, Australia, Dec. 2017, pp. 4224–4230.

[7] ——, "Synthesis of sensor deception attacks at the supervisory layer of cyber–physical systems," *Automatica*, vol. 121, p. 109172, Nov. 2020.

[8] C. N. Hadjicostis, S. Lafortune, F. Lin, and R. Su, "Cybersecurity and supervisory control: A tutorial on robust state estimation, attack synthesis, and resilient control," in *Proc. 61st IEEE Conf. Decis. Control (CDC)*, Cancun, Mexico, Dec. 2022, pp. 3020–3040.

[9] D. You, S. Wang, and C. Seatzu, "A liveness-enforcing supervisor tolerant to sensor-reading modification attacks," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 52, no. 4, pp. 2398–2411, Apr. 2021.

[10] M. Wakaiki, P. Tabuada, and J. P. Hespanha, "Supervisory control of discrete-event systems under attacks," *Dyn. Games Appl.*, vol. 9, no. 4, pp. 965–983, Dec. 2019.

[11] L. K. Carvalho, Y.-C. Wu, R. Kwong, and S. Lafortune, "Detection and mitigation of classes of attacks in supervisory control systems," *Automatica*, vol. 97, pp. 121–133, Nov. 2018.

[12] R. Su, "Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations," *Automatica*, vol. 94, pp. 35–44, Aug. 2018.

[13] R. Meira-Góes, S. Lafortune, and H. Marchand, "Synthesis of supervisors robust against sensor deception attacks," *IEEE Trans. Autom. Control*, vol. 66, no. 10, pp. 4990–4997, Jan. 2021.

[14] R. Meira-Góes, H. Marchand, and S. Lafortune, "Dealing with sensor and actuator deception attacks in supervisory control," *Automatica*, vol. 147, p. 110736, Nov. 2023.

[15] Y. Zhu, L. Lin, and R. Su, "Supervisor obfuscation against actuator enablement attack," in *Proc. 18th European Control Conference (ECC)*, Napoli, Italy, Jun. 2019, pp. 1760–1765.

[16] 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.

Algorithm 1: 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    $f_{yz}(i_y, \sigma_{\sigma'}) := (i_y, \sigma_{\sigma'})$;

7    $I_z := I_z \cup \{f_{yz}(i_y, \sigma_{\sigma'})\}$;

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    $f_{zy}(i_z, b'_{o1}) := (f_e^{BS}(b'_{o1}, \sigma_{\sigma'}), f_e(b_{o2}, \sigma_{\sigma'}))$;

12    $I_y := I_y \cup \{f_{zy}(i_z, b'_{o1})\}$;

13 Go back to step 2, repeat until all accessible part has been built, and build an automaton as $\Upsilon = (I_y \cup I_z, \Xi \cup B_o^{BS}, f_{yz}, f_{zy}, y_0)$;

14 Mark all the Y-states in Υ;

15 Let Ξ be uncontrollable and B_o^{BS} be controllable;

16 Trim Υ and let Υ_{trim} be the specification automaton;

17 Construct DIS Υ^{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 [21];

18 **return** DIS as $\Upsilon^{BS} = (I_y, I_z, \Xi, B_o^{BS}, f_{yz}, f_{zy}, y_0)$;

[17] 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.

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

[19] L. Lin and R. Su, "Synthesis of covert actuator and sensor attackers," *Automatica*, vol. 130, p. 109714, Aug. 2021.

[20] D. You, S. Wang, M. Zhou, and C. Seatzu, "Supervisory control of petri nets in the presence of replacement attacks," *IEEE Trans. Autom. Control*, vol. 67, no. 3, pp. 1466–1473, Mar. 2021.

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

[22] L. Lin, Y. Zhu, and R. Su, "Synthesis of covert actuator attackers for free," *Discrete Event Dyn. Syst.*, vol. 30, pp. 561–577, Dec. 2020.

[23] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2351–2383, Aug. 2021.

[24] G. K. Edwin, S. V. Ewards, G. J. W. Kathrine, G. M. Palmer, A. Bertia, and S. Vijay, "Honeypot based intrusion detection system for cyber physical system," in *Proc. Int. Conf. Augmented Intell. Sustain. Syst. (ICAISS)*, Trichy, India, Nov. 2022, pp. 958–962.