Comments on "A new approach for the verification of infinite-step and K-step opacity using two-way observers" [Automatica, 2017(80)162-171] ⋆

Hao Lan [a,b], Yin Tong [a], Jin Guo [a], Alessandro Giua [b]

[a] *School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China*

[b] *Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari 09123, Italy*

Abstract

In this note, we point out that the observer of a given discrete event system and the observer of the reversed system can be used together to verify both infinite-step opacity and K-step opacity rather than constructing the two-way observer in [1]. In this way, the complexity of checking the two opacity properties can be reduced.

Key words: Discrete event system; Infinite-step opacity; K-step opacity.

Published as:

Hao Lan, Yin Tong, Jin Guo, Alessandro Giua, Comments on "A new approach for the verification of infinite-step and K-step opacity using two-way observers" [Automatica 80 (2017) 162C171], Automatica, Volume 122, article 109290, 2020. DOI: 10.1016/j.automatica.2020.109290

⋆ This work has been partially supported by the National Natural Science Foundation of China under Grant No. 61803317, and the Fundamental Research Funds for the Central Universities under Grant No. 2682018CX24. This paper was not presented at any IFAC meeting. Corresponding author Yin Tong.

Email addresses: haolan@my.swjtu.edu.cn (Hao Lan), yintong@swjtu.edu.cn (Yin Tong), jguo_scce@swjtu.edu.cn (Jin Guo), giua@unica.it (Alessandro Giua).

1 Main results

In [1], a structure called *two-way observer* (TW-observer) is proposed to verify *infinite-step opacity* and *K-step opacity* in a discrete event system G described by a partially observable automaton. This structure is constructed by the composition of two automata:
- $Obs(G) = (Q_{obs}, E_o, f_{obs}, q_{obs,0})$, i.e., the observer of system G;
- $Obs(G_R) = (Q_{obs,R}, E_o, f_{obs,R}, X)$, i.e., the observer of the reversed automaton of system G.

In this note, we prove that infinite-step opacity and K-step opacity can be verified more efficiently by simply checking the intersections between pairs of states of the two observers without constructing the TW-observer. The following technical result will be used in this note.

Proposition 1 *Given a system G, it holds that $s \in P(\mathcal{L}(G)) \wedge t_R \in P(\mathcal{L}(G_R)) \wedge f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) \neq \emptyset \Leftrightarrow st \in P(\mathcal{L}(G))$.*

Proof. As shown in [1], the state set of the TW-observer is $Q_{TW} = Q_{obs} \times Q_{obs,R}$. Thus the result follows from Lemmata 3 and 4 in [1] replacing Q_{TW} with $Q_{obs} \times Q_{obs,R}$. □

In other words, if the intersection between $f_{obs}(q_{obs,0}, s)$ and $f_{obs,R}(X, t_R)$ is not empty, then concatenation of s and t is an observation that can be generated by the system, and vice versa.

1.1 Infinite-step Opacity

Theorem 2 *Let G be a system, E_o a set of observable events, and X_s a set of secret states. System G is infinite-step opaque w.r.t. X_s and E_o if and only if $\nexists (q_1, q_2) \in Q_{obs} \times Q_{obs,R}$ such that*

$$\emptyset \neq (q_1 \cap q_2) \subseteq X_s. \tag{1}$$

Proof. (If) Assume that there exist $q_1 \in Q_{obs}$ and $q_2 \in Q_{obs,R}$ such that $\emptyset \neq (q_1 \cap q_2) \subseteq X_s$. Since system G is accessible, there must exist a string $s \in P(\mathcal{L}(G))$ and a string $t_R \in P(\mathcal{L}(G_R))$ such that $q_1 = f_{obs}(q_{obs,0}, s)$ and $q_2 = f_{obs,R}(X, t_R)$. Thus, $f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) \neq \emptyset$. By Theorem 2 in [1] and Proposition 1, we have that $st \in P(\mathcal{L}(G))$ and $\hat{X}_{|s|}(st) = f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) = q_1 \cap q_2 \subseteq X_s$. By Proposition 1 in [1], system G is not infinite-step opaque.
(Only if) Assume that system G is not infinite-step opaque. By Proposition 1 in [1], there exists $st \in P(\mathcal{L}(G))$ such that $\hat{X}_{|s|}(st) \subseteq X_s$. By Theorem 2 in [1] and Proposition 1, we have that $s \in P(\mathcal{L}(G))$, $t_R \in P(\mathcal{L}(G_R))$, $f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) \neq \emptyset$ and $f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) = \hat{X}_{|s|}(st) \subseteq X_s$. Let $q_1 = f_{obs}(q_{obs,0}, s) \in Q_{obs}$ and $q_2 = f_{obs,R}(X, t_R) \in Q_{obs,R}$. Thus, $\emptyset \neq (q_1 \cap q_2) \subseteq X_s$. □

In other words, a system G is not infinite-step opaque w.r.t. X_s and E_o if and only if there exist a state q_1 in $Obs(G)$ and a state q_2 in $Obs(G_R)$ such that the intersection of the two states is not empty and it belongs to the set of secret states. By Theorem 2, we need to check the intersections between pairs of states in $Obs(G)$ and $Obs(G_R)$. Given a state $q_1 \in Q_{obs}$ and a state $q_2 \in Q_{obs,R}$, the complexity of testing condition (1) is $\mathcal{O}(|X|)$. Therefore, the complexity of verifying infinite-step opaque is $\mathcal{O}(|Q_{obs}| \times |Q_{obs,R}| \times |X|)$. In the worst case, there are $2^{|X|}$ states in both $Obs(G)$ and $Obs(G_R)$. Thus, in the worst case, the complexity of our approach to verifying infinite-step opacity is $\mathcal{O}(2^{|X|} \times 2^{|X|} \times |X|)$. Compared with the complexity [1] $\mathcal{O}((|E_o| + |X|) \times 2^{|X|} \times 2^{|X|})$ of the method in [1], our approach is more efficient especially when $|E_o|$ and $|X|$ are large.

1.2 K-step Opacity

Proposition 3 *System G is K-step opaque w.r.t. X_s and E_o if and only if*

$$\nexists st \in P(\mathcal{L}(G)) \text{ with } |t| \leq K : \hat{X}_{|s|}(st) \subseteq X_s.$$

[1] The complexity was originally stated as $\mathcal{O}(|E_o| \times 2^{|X|} \times 2^{|X|})$ in [1] since only the complexity of constructing the TW-observer is considered. However, after the TW-observer is constructed, it is also required to test condition (1) for all the states in the TW-observer.

Proof. (If) Assume that $\exists st \in P(\mathcal{L}(G))$ with $|t| \leq K$ such that $\hat{X}_{|s|}(st) \subseteq X_s$. This implies that $\forall x_0 \in X_0, \forall wv \in \mathcal{L}(G, x_0)$ with $P(w) = s$, $P(v) = t$ and $|P(v)| \leq K$, it holds that $f(x_0, w) \in X_s$. Thus, by Definition 3.1 in [1], system G is not K-step opaque.
(Only if) Assume that system G is not K-step opaque, which means that there exists $st \in P(\mathcal{L}(G))$ such that $|t| \leq K$ and $f(x_0, w) \in X_s$ for any $x_0 \in X_0$ and any $wv \in \mathcal{L}(G, x_0)$ with $P(w) = s$ and $P(v) = t$. By the definition of $\hat{X}_{|s|}(st)$ in [1], $\forall x \in \hat{X}_{|s|}(st)$, $x \in X_s$. Therefore, $\hat{X}_{|s|}(st) \subseteq X_s$ with $|t| \leq K$. □

According to the previous proposition, a system is K-step opaque w.r.t. the set of secret states if and only if for any string $st \in P(\mathcal{L}(G))$ with $|t| \leq K$, the set of states, that the system could have been in $|t|$ steps earlier after observing st, is not included in the set of secret states.

We define the K-reduced set of $Q_{obs,R}$ as

$$Q_{R,K} = \{q \in Q_{obs,R} | \exists t_R \in P(\mathcal{L}(G_R)), |t_R| \leq K : \\ q = f_{obs,R}(X, t_R)\}. \tag{2}$$

Namely, $Q_{R,K}$ is the set of states that can be reached from the initial state of $Obs(G_R)$ within K steps. Note that the complexity of computing $Q_{R,K}$ is linear in K and the number of states of $Obs(G_R)$.

Theorem 4 *Let G be a system, E_o a set of observable events, and X_s a set of secret states. System G is K-step opaque w.r.t. X_s and E_o if and only if $\nexists (q_1, q_2) \in Q_{obs} \times Q_{R,K}$ such that*

$$\emptyset \neq (q_1 \cap q_2) \subseteq X_s.$$

Proof. (If) Assume that there exist $q_1 \in Q_{obs}$ and $q_2 \in Q_{R,K}$ such that $\emptyset \neq (q_1 \cap q_2) \subseteq X_s$. Since system G is accessible, there must exist a string $s \in P(\mathcal{L}(G))$ and a string $t_R \in P(\mathcal{L}(G_R))$ with $|t_R| \leq K$ such that $q_1 = f_{obs}(q_{obs,0}, s)$ and $q_2 = f_{obs,R}(X, t_R)$. Thus, $f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) \neq \emptyset$. By Theorem 2 in [1] and Proposition 1, we have that $st \in P(\mathcal{L}(G))$ and $\hat{X}_{|s|}(st) = f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) = q_1 \cap q_2 \subseteq X_s$. Since $|t| = |t_R| \leq K$, by Proposition 3, system G is not K-step opaque.
(Only if) Assume that system G is not K-step opaque. By Proposition 3, there exists $st \in P(\mathcal{L}(G))$ with $|t| \leq K$ such that $\hat{X}_{|s|}(st) \subseteq X_s$. By Theorem 2 in [1] and Proposition 1, we have that $s \in P(\mathcal{L}(G))$, $t_R \in P(\mathcal{L}(G_R))$, $f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) \neq \emptyset$ and $f_{obs}(q_{obs,0}, s) \cap f_{obs,R}(X, t_R) = \hat{X}_{|s|}(st) \subseteq X_s$. Let $q_1 = f_{obs}(q_{obs,0}, s) \in Q_{obs}$ and $q_2 = f_{obs,R}(X, t_R) \in Q_{obs,R}$. It holds that $\emptyset \neq (q_1 \cap q_2) \subseteq X_s$, and $q_2 \in Q_{R,K}$ as $|t_R| = |t| \leq K$. □

In simple words, K-step opacity can be verified by checking whether the intersection of pairs of states in Q_{obs} and $Q_{R,K}$ is a subset of X_s and is nonempty. Clearly, compared with the improved method of verifying K-step opacity in [1] using the K-reduced TW-observer, the proposed approach is still more efficient. More precisely, the complexity of verifying K-step opacity is $\mathcal{O}(|Q_{obs}| \times |Q_{R,K}| \times |X|)$, By Eq. (2), the number of states in $Q_{R,K}$ is bounded by $min\{|E_o|^K, 2^{|X|}\}$. In the worst case, the complexity of the proposed approach is $\mathcal{O}(min\{|E_o|^K, 2^{|X|}\} \times 2^{|X|} \times |X|)$, which is smaller than the complexity $\mathcal{O}(min\{|E_o|^K, 2^{|X|}\} \times 2^{|X|} \times (|E_o| + |X|))$ of the method in [1].

References

[1] X. Yin and S. Lafortune. A new approach for the verification of infinite-step and K-step opacity using two-way observers. *Automatica*, 80:162–171, 2017.