Error- and Tamper-Tolerant State Estimation for Discrete Event Systems under Cost Constraints

Yuting Li, Christoforos N. Hadjicostis, *Fellow, IEEE*, Naiqi Wu, *Fellow, IEEE,* and Zhiwu Li, *Fellow, IEEE*

The F-verifier is an NFA $V_F = AC(Q^{V_F}, \Sigma, \delta_{V_F}, q_0^{V_F})$ (refer to Fig. 3), where

$Q^{V_F} := X_{mn} \times \Delta \times X_{mn} \times \Delta$,

$q_0^{V_F} := \cup_{x_{mn}, y_{mn} \in X_{mn0}} \{(x_{mn}, N, y_{mn}, N)\} \subseteq Q^{V_F}$.

For $x_{mni}, x_{mnj} \in X_{mn}$ and $l_i, l_j \in \Delta$, the (nondeterministic) transition function δ_{V_F} is defined as follows.

For $\sigma \in \Sigma_o$, $\delta_{V_F}((x_{mni}, l_i, x_{mnj}, l_j), \sigma) = \delta_{mn}(x_{mni}, \sigma) \times \{l_i\} \times \delta_{mn}(x_{mnj}, \sigma) \times \{l_j\}$.

For $\sigma \in \Sigma_{uo} \setminus \Sigma_f$, $\delta_{V_F}((x_{mni}, l_i, x_{mnj}, l_j), \sigma) =$

$$\begin{cases} \delta_{mn}(x_{mni}, \sigma) \times \{l_i\} \times \{x_{mnj}\} \times \{l_j\} \\ \{x_{mni}\} \times \{l_i\} \times \delta_{mn}(x_{mnj}, \sigma) \times \{l_j\} \\ \delta_{mn}(x_{mni}, \sigma) \times \{l_i\} \times \delta_{mn}(x_{mnj}, \sigma) \times \{l_j\}. \end{cases}$$

For $\sigma \in \Sigma_f$, $\delta_{V_F}((x_{mni}, l_i, x_{mnj}, l_j), \sigma) =$

$$\begin{cases} \delta_{mn}(x_{mni}, \sigma) \times \{F\} \times \{x_{mnj}\} \times \{l_j\} \\ \{x_{mni}\} \times \{l_i\} \times \delta_{mn}(x_{mnj}, \sigma) \times \{F\} \\ \delta_{mn}(x_{mni}, \sigma) \times \{F\} \times \delta_{mn}(x_{mnj}, \sigma) \times \{F\}. \end{cases}$$

Note that for $\sigma \in \Sigma_o$, $\delta_{V_F}((x_{mni}, l_i, x_{mnj}, l_j), \sigma)$ is empty if $\delta_{mn}(x_{mni}, \sigma) = \emptyset$ or $\delta_{mn}(x_{mnj}, \sigma) = \emptyset$; for $\sigma \in \Sigma_{uo} \setminus \Sigma_f$ or $\sigma \in \Sigma_f$, three types of transitions are feasible if $\delta_{mn}(x_{mni}, \sigma) \neq \emptyset$ and $\delta_{mn}(x_{mnj}, \sigma) \neq \emptyset$ whereas only one type of transition is feasible if only one of $\delta_{mn}(x_{mni}, \sigma)$ or $\delta_{mn}(x_{mnj}, \sigma)$ is non-empty. For example, in Fig. 2, event γ is feasible at state $((1,0), F, (0,0), N)$ since $\delta_{mn}((1,0), \gamma)$ and $\delta_{mn}((0,0), \gamma)$ are both non-empty. In Fig. 3, note that $\delta_{V_F}(((1,0), F, (0,0), N), \sigma_f) = \{(1,0)\} \times \{F\} \times \delta_{mn}((0,0), \sigma_f) \times \{F\}$ is also non-empty and leads to state $((1,0), F, (1,0), F)$.

A path in the verifier $V_F = AC(Q^{V_F}, \Sigma, \delta_{V_F}, q_0^{V_F})$ is a sequence of states and transitions $\langle q_1^{V_F}, \sigma_1, q_2^{V_F}, ..., \sigma_{n-1}, q_n^{V_F} \rangle$ such that for each $i \in \{1, 2, ..., n-1\}$, $q_{i+1}^{V_F} \in \delta_{V_F}(q_i^{V_F}, \sigma_i)$; this path is a cycle if $q_n^{V_F} = q_1^{V_F}$ and at least one transition is contained along the path.

The NFA V_F is said to be F-*confused* if there is a cycle, $\langle q_1^{V_F}, \sigma_1, q_2^{V_F}, ..., \sigma_{n-1}, q_n^{V_F} \rangle$, such that for all $q_i^{V_F} = (x_{mn} = (x, c), l, x'_{mn} = (x', c'), l')$, $i \in \{1, 2, ..., n-1\}$, we have $c, c' \leq C$, $l = N$ and $l' = F$ or vice versa. If there are no such cycles, we say that V_F is F-*confusion free*.

Theorem 1. An NFA G_{nd} is C-constrained tamper-tolerant diagnosable w.r.t. Σ, Σ_o, Σ_f, and AT if and only if the corresponding V_F is F-confusion free.

Proof. ($\Rightarrow$) Assume that $\mathcal{L}(G_{nd})$ is C-constrained tamper-tolerant diagnosable w.r.t. Σ, Σ_o and Σ_f. By contradiction, suppose that V_F has an F-confused cycle $\langle q_1^{V_F}, \sigma_1, q_2^{V_F}, ..., \sigma_{n-1}, q_n^{V_F} \rangle$. Let $q_1^{V_F} = (x_{mni}, N, x_{mnj}, F)$. There exist $s, s' \in \mathcal{L}(G_{mnd}(C+1))$, and $x_{mn}, y_{mn} \in X_{mn0}$ such that $P(s) = P(s')$, $x_{mni} \in \delta_{mn}(x_{mn}, s)$, $x_{mnj} \in \delta_{mn}(y_{mn}, s')$, $\Sigma_f \in s$, and $\Sigma_f \notin s'$. Now, we have $s(\sigma_1\sigma_2...\sigma_{n-1})^k$, $s'(\sigma_1\sigma_2...\sigma_{n-1})^k \in \mathcal{L}(G_{mnd}(C+1))$ with the same projection for $k \geq 0$. It is obvious that fault events in s are not diagnosable since k can be arbitrarily large. The definition of C-constrained tamper-tolerant diagnosability is violated.

($\Leftarrow$) By contrapositive, suppose that $\mathcal{L}(G_{nd})$ is not C-constrained tamper-tolerant diagnosable w.r.t. Σ, Σ_o, Σ_f and AT. This means that for any nonnegative integer n, we can find $s \in (\Sigma \backslash \Sigma_f)^*, \sigma_f \in \Sigma_f$, such that $s\sigma_f \in \mathcal{L}(G_{mnd}(C+1))$ and the following is true:

$(\exists t \in \mathcal{L}(G_{mnd}(C+1))/(s\sigma_f))$ $(\exists s' \in P^{-1}[P(s\sigma_f t)] \cap \mathcal{L}(G_{mnd}(C+1)))$ $(|t| \geq n) \implies \sigma_f \notin s'$.

Let $l \in \overline{s'}$ and $P(l) = P(s\sigma_f)$. It is obvious that $\Sigma_f \notin l$. Let $x_{s\sigma_f} \in \delta_{mn}(x_{mn}, s\sigma_f)$, $x_l \in \delta_{mn}(y_{mn}, l)$, $x_{s\sigma_f t} \in \delta_{mn}(x_{s\sigma_f}, t)$, and $x_{s'} \in \delta_{mn}(x_l, \{s'\}/l)$. We obtain reachable states $(x_{s\sigma_f}, F, x_l, N), (x_{s\sigma_f t}, F, x_{s'}, N) \in Q^{V_F}$ in V_F. Since n can be arbitrarily large, choose $n' \geq (2|X|(C+2))^2$. There exists a path, denoted by $\langle q_{k1}^{V_F}, \sigma_{k1}, q_{k2}^{V_F}, ..., \sigma_{k(n'-1)}, q_{kn'}^{V_F} \rangle$, where $q_{k1}^{V_F} = (x_{s\sigma_f}, F, x_l, N)$ and $q_{kn'}^{V_F} = (x_{s\sigma_f t}, F, x_{s'}, N)$. Then, it is certain that there exist i, j satisfying $1 \leq i < j \leq n'$ such that $q_{ki}^{V_F} = q_{kj}^{V_F}$ since $n' \geq (2|X|(C+2))^2$ is greater than the maximum possible number of distinct states in the verifier construction. Therefore we have identified an F-confused cycle. □

Example 1. We construct part of the F-verifier of the modified NFA in Fig. 2, as shown in Fig. 3. The verifier in Fig. 3 is F-confused. Hence, Σ_f is not C-constrained tamper-tolerant diagnosable for the NFA in Fig. 1. For the system in Fig. 1, if the attacker successfully corrupts $\alpha\beta$ to $\gamma\alpha$, σ_f cannot be diagnosed regardless of how long we wait for additional observations.

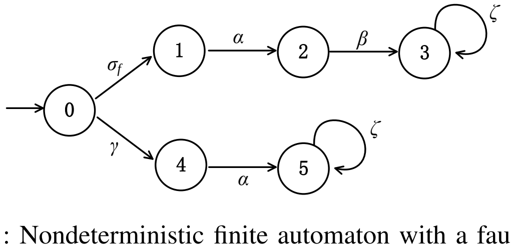

Fig. 1: Nondeterministic finite automaton with a fault event.

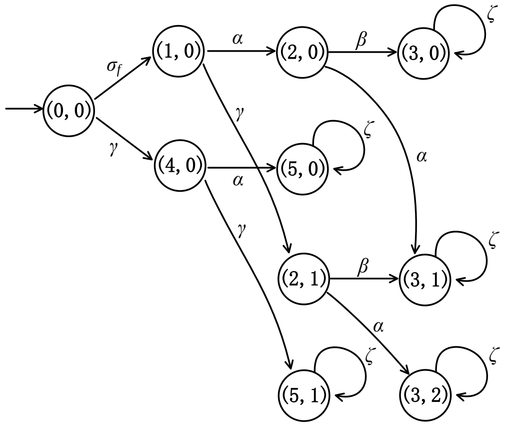

Fig. 2: Modified NFA for the system in Fig. 1.

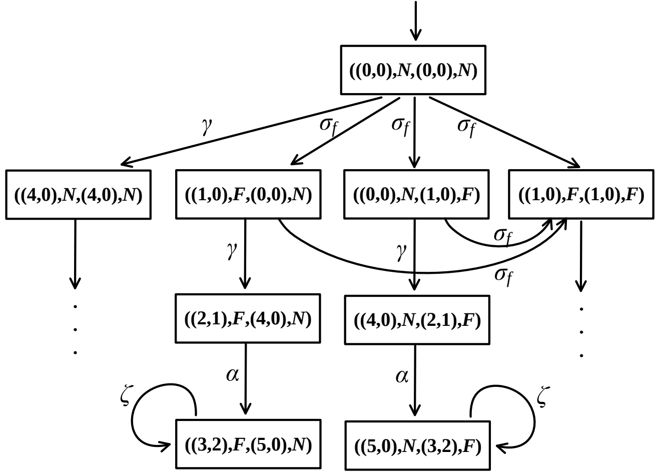

Fig. 3: Part of the verifier for the modified NFA in Fig. 2 (continuations not shown cannot lead to F-confused cycles).