Supplement Material for the Paper "Over-Approximation State Estimation for Networked Timed Discrete Event Systems with Communication Delays and Losses"

I. Proof of Proposition 1

Proposition 1: Let $\mathfrak{N} = (G, oc, cc)$ be an NTDES and $G_e = (Q_e, \Sigma_e, \delta_e, q_{0_e})$ be the augmented plant for $\mathfrak{N}$. Then, the state set Q_e of G_e is finite.

Proof: We start by considering Assumption 1, given in Eq. (1), which states that from any state in the state set Q of the original plant G, prior to the occurrence of a $tick$ event, no more than $|Q|-1$ events can be sent to an observation channel oc_i, for $i \in I_o$. Here, $|Q|$ denotes the cardinality of Q.

Importantly, any event transmitted through oc_i may experience a delay of up to $N_{d,i}$ occurrences of the $tick$ event. Consequently, at any given time, there can be at most $N_{d,i} \cdot (|Q| - 1)$ events delayed in oc_i. Let φ represent the maximum delay bound across all observation channels, defined as $\varphi = \max\{N_{d,i} | i \in I_o\}$.

Since only the events in Σ_{on} can be delayed in an observation channel, we can deduce that there are at most

$$\frac{1 - (|\Sigma_{on}| \cdot (\varphi + 1))^{\varphi \cdot (|Q|-1)}}{1 - (|\Sigma_{on}| \cdot (\varphi + 1))}$$

possible observation channel configurations for each individual channel in $\mathfrak{N}$. This, in turn, implies that the total number of possible global observation channel configurations for $\mathfrak{N}$ is bounded by

$$\left(\frac{1 - (|\Sigma_{on}| \cdot (\varphi + 1))^{\varphi \cdot (|Q|-1)}}{1 - (|\Sigma_{on}| \cdot (\varphi + 1))}\right)^k$$

where k is the number of observation channels in $\mathfrak{N}$.

Recall that each state of the extended system G_e consists of a state from Q and a configuration of A_Θ. Hence, the total number of possible states in G_e is at most

$$|Q| \cdot \left(\frac{1 - (|\Sigma_{on}| \cdot (\varphi + 1))^{\varphi \cdot (|Q|-1)}}{1 - (|\Sigma_{on}| \cdot (\varphi + 1))}\right)^k$$

Since G is a finite system, it follows that the state set Q_e of G_e is also finite. This concludes the proof. ■

II. Proof of Theorem 1

Theorem 1: Consider an NTDES $\mathfrak{N} = (G, oc, cc)$ and its augmented plant $G_e = (Q_e, \Sigma_e, \delta_e, q_{0_e})$. Let Γ_S be the augmented supervisor w.r.t. a supervisor S, as defined in Eq. (7). For any observation string $\alpha \in P_{e,o}(\mathcal{L}(\Gamma_S/\mathfrak{N}))$ generated by the compensated system $\Gamma_S/\mathfrak{N}$, $W(\alpha) = (x, \tilde{\gamma}) \in I$ is an information state satisfying:

1) $x = E_{\Gamma_S}(\alpha)$;
2) $\tilde{\gamma} = \Gamma_S(\alpha)$.

Proof: We prove the theorem by induction on the length of strings $\alpha \in P_{e,o}(\mathcal{L}(\Gamma_S/\mathfrak{N}))$.

Base case: Let $|\alpha| = 0$, i.e., $\alpha = \varepsilon$. In this case, the state estimate of $\Gamma_S/\mathfrak{N}$ upon observing the empty string ε is $\{q_{0_e}\}$. Due to Eq. (15), it holds $W(\varepsilon) = U_r(\hat{W}(\varepsilon), \Gamma_S(\varepsilon)) = (x, \tilde{\gamma})$ with $x \in 2^{Q_e}$ and $\tilde{\gamma} \in 2^{\Gamma_{net}}$.

First, by Eq. (10), we have $\tilde{\gamma} = \Gamma_S(\varepsilon)$, satisfying Statement (2). Next, we determine x. Due to Eq. (9), x comprises all states reachable from $\{q_{0_e}\}$ via unobservable events enabled by $\Gamma_S(\varepsilon)$. By Definition 5, x is the state estimate of $\Gamma_S/\mathfrak{N}$ upon observing the empty string ε. Formally,

$$x = \{q_e \in Q_e | \exists s \in \mathcal{L}(\Gamma_S/\mathfrak{N}) \cap \Sigma_{n,uo}^* : q_e = \delta_e(q_{0_e}, s)\}.$$

Due to Eq. (8), $x = E_{\Gamma_S}(\varepsilon)$ follows, satisfying Statement (1). The base case holds.

Induction hypothesis: Assume that for any $\alpha \in P_{e,o}(\mathcal{L}(\Gamma_S/\mathfrak{N}))$ such that $|\alpha| \leq j$, Statements (1) and (2) hold.

Induction step: Consider $\alpha\sigma \in P_{e,o}(\mathcal{L}(\Gamma_S/\mathfrak{N}))$ such that $|\alpha| = j$ and $\sigma \in \Sigma_{n,o}$. Write $W(\alpha\sigma) = (x, \tilde{\gamma})$ again.

First, by Eq. (15), $W(\alpha\sigma) = U_r(\hat{W}(\alpha\sigma), \Gamma_S(\alpha\sigma)) = U_r(O_r(W(\alpha), \sigma), \Gamma_S(\alpha\sigma))$ holds. It follows $\Gamma_S(\alpha\sigma) = \tilde{\gamma}$, satisfying Statement (2).

Next, to determine x, write $W(\alpha) = (x', \Gamma_S(\alpha))$ and $\hat{W}(\alpha\sigma) = x''$. By the induction hypothesis,

$$x' = \{q_e \in Q_e | \exists s \in \mathcal{L}(\Gamma_S/\mathfrak{N}) : P_{e,o}(s) = \alpha \wedge q_e = \delta_e(q_{0_e}, s)\}.$$

That it, x' is the state estimate of $\Gamma_S/\mathfrak{N}$ upon observing the string α. Based on x', we determine x'' using Eqs. (12)–(14). We deduce that x'' comprises all states reachable from a subset of x' via σ under the control of $\Gamma_S(\alpha\sigma)$. As a result, in accordance with Definition 5, x'' is the state estimate of $\Gamma_S/\mathfrak{N}$ immediately after observing the string $\alpha\sigma$. Formally,

$$x'' = \{q_e \in Q_e | \exists s \in \mathcal{L}(\Gamma_S/\mathfrak{N}) \cap \Sigma_e^* \Sigma_{n,o} : P_{e,o}(s) = \alpha\sigma \wedge q_e = \delta_e(q_{0_e}, s)\}.$$

Finally, due to Eq. (9), x comprises all states reachable from x'' via unobservable events enabled by $\Gamma_S(\alpha\sigma)$. Hence, by Definition 5, x is the state estimate of $\Gamma_S/\mathfrak{N}$ upon observing the string $\alpha\sigma$. We have

$$x = \{q_e \in Q_e | \exists s \in \mathcal{L}(\Gamma_S/\mathfrak{N}) : P_{e,o}(s) = \alpha\sigma \wedge q_e = \delta_e(q_{0_e}, s)\}.$$

Statement (1) holds. This completes the proof. ■

III. Proof of Proposition 2

Proposition 2: Consider an NTDES $\mathfrak{N} = (G, oc, cc)$, the augmented plant G_e for $\mathfrak{N}$, and a supervisor S. Let Γ_S be the augmented supervisor w.r.t. S, as defined in Eq. (7). For any observation string $\alpha \in P_{e,o}(\mathcal{L}(G_e))$, we have

$$\Gamma_S(\alpha) = \{\gamma \in \Gamma_{net} \mid \exists l \in [0, cc] : (\gamma, l) \in \Lambda_S(\alpha)\}$$

Proof: ($\subseteq$) Consider any $\gamma \in \Gamma_S(\alpha)$. Due to Eq. (7), there must exist observation strings $\alpha', \alpha'' \in \Sigma_{n,o}^*$ such that $\alpha = \alpha'\alpha''$, $\#_t(\alpha'') \leq cc$, and $\gamma = S(\alpha')$. According to Eq. (16), upon observing α', the decision γ paired with the maximum delay tolerance cc is sent to the configuration $\Lambda_S(\alpha')$, i.e., $(\gamma, cc) \in \Lambda_S(\alpha')$.

Now, as each $tick$ event in α'' is observed, the delay tolerance decreases by one. Since there are $\#_t(\alpha'')$ such events and $\#_t(\alpha'') \leq cc$, it follows that after observing all of α'', the remaining delay tolerance is $cc - \#_t(\alpha'')$. Therefore, $(\gamma, cc - \#_t(\alpha'')) \in \Lambda_S(\alpha'\alpha'') = \Lambda_S(\alpha)$. Because $cc - \#_t(\alpha'') \in [0, cc]$, we can conclude that

$$\gamma \in \{\gamma \in \Gamma_{net} \mid \exists l \in [0, cc] : (\gamma, l) \in \Lambda_S(\alpha)\}$$

($\supseteq$) Conversely, suppose $\gamma \in \{\gamma \in \Gamma_{net} | \exists l \in [0, cc] : (\gamma, l) \in \Lambda_S(\alpha)\}$. Then, there exists some $l \in [0, cc]$ such that $(\gamma, l) \in \Lambda_S(\alpha)$. By the recursive definition of Λ_S, this means that in the process of observing α, decision γ must have been added to the configuration at some point, and its delay tolerance was subsequently reduced to l. In particular, there exists a prefix α' of α such that $\gamma = S(\alpha')$ and the pair (γ, cc) is added to the configuration after observing α'. The remaining string α'' must contain exactly $cc - l$ events of $tick$ in order to reduce the delay tolerance from cc to l. Therefore, $\#_t(\alpha'') = cc - l \leq cc$, satisfying the definition of augmented control decisions. So, we can conclude that $\gamma \in \Gamma_S(\alpha)$. ■

IV. Proof of Proposition 3

Proposition 3: Let $\mathfrak{N} = (G, oc, cc)$ be an NTDES, $G_e = (Q_e, \Sigma_e, \delta_e, q_{0_e})$ be the augmented plant for $\mathfrak{N}$, and S be a supervisor. The complexity of Algorithm 1 per execution is polynomial in the number of states in Q_e but exponential in the number of events in Σ_e.

Proof: Assuming that a string $\alpha \in P_{e,o}(\mathcal{L}(\Gamma_S/\mathfrak{N}))$ has been observed so far, and the current information state is $W(\alpha)$. Whenever a new event $\sigma \in \Sigma_{n,o}$ is observed, computing $\hat{W}(\alpha\sigma)$ involves distinguishing whether σ is the $tick$ event. If $\sigma \neq tick$, the operator $\hat{W}(\alpha\sigma)$ requires at most $O(|Q_e|)$ time, where $|Q_e|$ denotes the cardinality of Q_e. However, if $\sigma = tick$, the time complexity of the operator $\hat{W}(\alpha\sigma)$ is $n_1 = O(2^{|\Sigma| + |\Sigma_{n,for}|} \cdot (cc+1) \cdot (|Q_e| \cdot |\Sigma| + 1))$.

Subsequently, computing $W(\alpha\sigma)$ in the worst case takes $n_2 = O(|Q_e| \cdot |\Sigma_{n,uo}|)$ time. Thus, for each iteration of the while-loop, the algorithm has a time complexity of $O(n_1 + n_2)$ for computing the current over-approximation state estimate of the NTDES $\mathfrak{N}$.

In summary, the algorithm's complexity per execution is polynomial in the number of states in Q_e but exponential in the number of events in Σ_e. In practice, the number of events in Σ_e is typically much smaller than the number of states in Q_e [1]. This ensures that the algorithm can process data rapidly, making it suitable for networked engineering applications. ■