State estimation of timed automata under partial observation

Chao Gao, Dimitri Lefebvre, Carla Seatzu, Zhiwu Li, and Alessandro Giua

Abstract

In this paper, we consider partially observable timed automata endowed with a single clock. A time interval is associated with each transition specifying at which clock values it may occur. In addition, a resetting condition associated to a transition specifies how the clock value is updated upon its occurrence. This work deals with the estimation of the current state given a timed observation, i.e., a succession of pairs of an observable event and the time instant at which the event has occurred. The problem of state estimation for a timed automaton is reduced to the reachability analysis of an associated zone automaton, which provides a purely discrete event description of the behaviour of the timed automaton. An algorithm is formulated to provide an approach for state estimation of a timed automaton based on the assumption that the clock is reset upon the occurrence of each observable transition.

Key words: Discrete event system, timed automaton, state estimation.

Published as:
C. Gao, D. Lefebvre, C. Seatzu, Z.W. Li, A. Giua, "State estimation of timed automata under partial observation," IEEE Trans. on Automatic Control, Vol. 70, no. 3, pp. 1981-1987, 2025. DOI: 10.1109/TAC.2024.3492955

This work is partially supported by the National Key R&D Program under Grant 2018YFB700104, National Natural Science Foundation of China under Grant 61873342, partially supported by PRIN project MOTOWN: Motown: Smart Production Planning and Control for Manufacturing of Electric Vehicle Powertrain in Industry 4.0 Environment, Call 2022 Prot. 20228XEHRE, and partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU. *(Corresponding author: Zhiwu Li)*.

Chao Gao is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China; DIEE, University of Cagliari, Cagliari 09124, Italy, E-mail: gaochao@stu.xidian.edu.cn.

Dimitri Lefebvre is with GREAH Laboratory, Université Le Havre Normandie, Le Havre 76600, France, E-mail: dimitri.lefebvre@univ-lehavre.fr.

Carla Seatzu is with DIEE, University of Cagliari, Cagliari 09124, Italy, E-mail: carla.seatzu@unica.it.

Zhiwu Li is with the School of Electro-Mechanical Engineering, Xidian University, Xi'an 710071, China; the Institute of Systems Engineering, Macau University of Science and Technology, Macau 999078, China, E-mail: zwli@must.edu.mo.

Alessandro Giua is with DIEE, University of Cagliari, Cagliari 09124, Italy, E-mail: giua@unica.it.

I. Introduction

In the area of *discrete event systems* (DES), a large body of literature considers logical DES, where time is abstracted and only the order of occurrences of the events is taken into account. The problem of state estimation has received a lot of attention considering different observation structures in different formalisms, in particular automata [1] and Petri nets [2]. Significant contributions have also been provided in the framework of timed DES. As an example, [3], proposes a state estimation approach for a particular class of weighted automata, where the time information of transition firability is given to weights. References [4], [5], [6], and [7] address the problem of state estimation of a class of timed automata under a rather restrictive scenario where the endowed single clock is reset to zero after each event occurrence. The state estimation of timed DES has also been considered in [8] and [9], but no general approach concerning state estimation for a general class of timed DES exists.

Another active area of research is that of *hybrid systems* (HS) [10], [11], characterized by the interplay between discrete event and time-driven dynamics. These systems can be modeled by *hybrid automata*, and in particular by *timed automata* [12] concerning time elapsing as time-driven dynamics. State estimation of timed automata has also been studied. In [12], the reachability of locations can be analysed by searching the finite quotient of a timed automaton with respect to the region equivalence defined over the set of all clock interpretations. However, the reachability is analyzed regardless of any observations. Tripakis proposes an online diagnoser in [13] that keeps track of all the possible discrete states. Thereby, state estimation problem is theoretically solvable. In [14] and [15], timed markings are used for representing the closure under silent transitions. Observe that in [13]–[15], only online estimators have been proposed. In particular the model we consider in this paper, that we call *timed finite automaton* can be either seen as a finite state automaton endowed with a clock or as a timed automaton [12] whose edges are labeled.

A related problem in a decentralized setting is studied in [16], where the asynchronous polling of distributed sub-systems is called *synchronization*. Concerning timed automata, references [17], [18], and [19] discuss how to define concurrent composition for timed automata, which can be used to construct complex models.

This paper considers a partially observable timed finite automaton (TFA) endowed with a single clock. The logical structure specifies the set of *discrete states* of a TFA, the sequences of events that the TFA can generate and the observations they produce. The timed structure specifies the set of clock values that allow an event to occur and how the clock is reset upon the event occurrence. A timed state of a TFA consists of a discrete state and a clock value. Our objective is that of estimating the current discrete state of the automaton as a function of the current observation and of the current time. The notion of T-reachability is proposed to describe which discrete states can be reached with a given timed observation of duration T. We show that the problem of T-reachability for a TFA can be reduced to the reachability analysis of a nondeterministic finite state automaton, called *zone automaton*.

Thus, the discrete state estimation problem for the TFA can be studied by the determinization of the zone automaton.

The proposed state estimation approach consists of two steps. When no observation occurs and time elapses, the state estimation is given by a finite set of extended states of the zone automaton, which depends on the current time. When a timed observation occurs, we update the discrete state estimation and reset the clock value to a finite set of zones according to the reinitialized observation (RO) assumption. We prove that the set of all possible state estimates is finite (see Remark 1). This means that in principle, a finite observer [20] could be constructed with an offline procedure, paving the way to the verification of a large set of dynamical properties, such as detectability [21], opacity [22] and resilience to cyber-attack [23], which depend on the overall behavior of the system. This is left for future work.

The rest of the paper is organized as follows. Section II introduces the background of DES, timed automata and time semantics. Section III formally state the problem of state estimation. Section IV illustrates the approaches to compute zones and to construct the zone automaton. Section V provides necessary and sufficient conditions for the reachability of a state of the timed automaton in terms of reachability analysis in the zone automaton. Section VI solves the problem of updating the state estimation according to the latest received *timed observation*. Finally, Section VII concludes this paper.

II. Background

A nondeterministic finite automaton (NFA) is a four-tuple $G = (X, E, \Delta, X_0)$, where X is a finite set of states, E is a finite set of events, $\Delta \subseteq X \times E \times X$ is the transition relation and $X_0 \subseteq X$ is the set of initial states. The set of events E can be partitioned as $E = E_o \dot{\cup} E_{uo}$, where E_o is the set of observable events, and E_{uo} is the set of unobservable events. We denote by E^* the set of all finite strings on E, including the empty word ε. The *concatenation* $s_1 \cdot s_2$ of two strings $s_1 \in E^*$ and $s_2 \in E^*$ is a string consisting of s_1 immediately followed by s_2. The empty string ε is an identity element of concatenation, i.e., for any string $s \in E^*$, it holds that $\varepsilon \cdot s = s = s \cdot \varepsilon$. Given a string in E^*, the observation is defined via the observation projection $P_l : E^* \longrightarrow E_o^*$ defined as: $P_l(\varepsilon) = \varepsilon$, and for all $s \in E^*$ and $e \in E$, it is $P_l(s \cdot e) = P_l(s) \cdot e$ if $e \in E_o$, or $P_l(s \cdot e) = P_l(s)$ if $e \in E_{uo}$.

Let $\mathbb{R}_{\geq 0}$ be the set of non-negative real numbers and $\mathbb{N}$ be the set of natural numbers. A closed interval, i.e., closed on both sides, is denoted as $[m, n]$, while open or semi-open intervals are denoted as (m, n), $[m, n)$ or $(m, n]$. We denote the set of all time intervals and the set of all closed time intervals as $\mathbb{I}$ and $\mathbb{I}_c$, respectively, where $\mathbb{I}_c \subseteq \mathbb{I}$. The *addition*[1] of I_1 and I_2 is defined as $I_1 \bigoplus I_2 = \{t_1 + t_2 \in \mathbb{R}_{\geq 0} \mid t_1 \in I_1, t_2 \in I_2\}$ and the *distance range* between them as $D(I_1, I_2) = \{|t_1 - t_2| \mid t_1 \in I_1, t_2 \in I_2\}$.

[1]The addition operation is associative and commutative and can be extended to $n > 2$ time intervals $\bigoplus_{i=1}^{n} I_i = I_1 \bigoplus \cdots \bigoplus I_n$.

Definition 1: A *timed finite automaton* (TFA) is a six-tuple $G = (X, E, \Delta, \Gamma, Reset, X_0)$ that operates under a single clock, where X is a finite set of discrete states, E is an alphabet, $\Delta \subseteq X \times E \times X$ is a transition relation, $\Gamma : \Delta \to \mathbb{I}_c$ is a timing function, $Reset : \Delta \to \mathbb{I}_c \cup \{id\}$ is a clock resetting function such that for $\delta \in \Delta$, the clock is reset to be an integer value in a time interval $I \in \mathbb{I}_c$ ($Reset(\delta) = I$), or the clock is not reset ($Reset(\delta) = id$), and $X_0 \subseteq X$ is the set of initial discrete states. □

For the sake of simplicity, we assume that the clock is set to be 0 initially. A transition $(x, e, x') \in \Delta$ denotes that the occurrence of event $e \in E$ leads to $x' \in X$ when the TFA is at $x \in X$. The time interval $\Gamma((x, e, x'))$ specifies a range of clock values at which the event e may occur, while $Reset((x, e, x')) \in \mathbb{I}_c$ denotes the range of the clock values that are reset to be and $Reset((x, e, x')) = id$ implies that the clock is not reset. The *set of output transitions at* x is defined as $O(x) = \{(x, e, x') \in \Delta \mid e \in E, x' \in X\}$, and *the set of input transitions at* x is defined as $I(x) = \{(x', e, x) \in \Delta \mid e \in E, x' \in X\}$.

A *timed state* is defined as a pair $(x, \theta) \in X \times \mathbb{R}_{\geq 0}$, where θ is the current value of the clock. In other words, a timed state (x, θ) keeps track of the current clock assignment θ while G stays at state x. The behaviour of a TFA is described via its timed runs. A *timed run* ρ of length $k \geq 0$ from $t_0 \in \mathbb{R}_{\geq 0}$ to $t_k \in \mathbb{R}_{\geq 0}$ is a sequence of $k+1$ timed states $(x_{(i)}, \theta_{(i)}) \in X \times \mathbb{R}_{\geq 0}$ ($i = 0, \cdots, k$), and k pairs $(e_i, t_i) \in E \times \mathbb{R}_{\geq 0}$ ($i = 1, \cdots, k$), represented as $\rho : (x_{(0)}, \theta_{(0)}) \xrightarrow{(e_1,t_1)} \cdots (x_{(k-1)}, \theta_{(k-1)}) \xrightarrow{(e_k,t_k)} (x_{(k)}, \theta_{(k)})$ such that $(x_{(i-1)}, e_i, x_{(i)}) \in \Delta$, and the following conditions hold for all $i = 1, \cdots, k$:

- $\theta_{(i)} \in Reset((x_{(i-1)}, e_i, x_{(i)}))$ and $\theta_{(i-1)} + t_i - t_{i-1} \in \Gamma((x_{(i-1)}, e_i, x_{(i)}))$, if $Reset((x_{(i-1)}, e_i, x_{(i)})) \neq id$;
- $\theta_{(i)} = \theta_{(i-1)} + t_i - t_{i-1} \in \Gamma((x_{(i-1)}, e_i, x_{(i)}))$, if $Reset((x_{(i-1)}, e_i, x_{(i)})) = id$.

We define the *timed word generated by* ρ as $\sigma(\rho) = (e_1, t_1)(e_2, t_2) \cdots (e_k, t_k) \in (E \times \mathbb{R}_{\geq 0})^*$. We also define the *logical word generated by* ρ as $S(\sigma(\rho)) = e_1 e_2 \cdots e_k$ via a function defined as $S : (E \times \mathbb{R}_{\geq 0})^* \to E^*$. For the timed run of length 0 as $\rho : (x_{(0)}, \theta_{(0)})$, we have $S(\sigma(\rho)) = \varepsilon$ and $\sigma(\rho) = \lambda$, where λ denotes the *empty timed word* in $E \times \mathbb{R}_{\geq 0}$. For the timed word $\sigma(\rho)$ generated from an arbitrary timed run ρ, it is $\lambda \cdot \sigma(\rho) = \sigma(\rho) = \sigma(\rho) \cdot \lambda$. The *starting discrete state* and the *ending discrete state* of a timed run ρ are denoted by $x_{st}(\rho) = x_{(0)}$ and $x_{en}(\rho) = x_{(k)}$, respectively. The *starting time* and the *ending time* of ρ are denoted by $t_{st}(\rho) = t_0$ and $t_{en}(\rho) = t_k$, respectively. In addition, the *duration of* ρ is denoted as $T(\rho) = t_k - t_0$. The set of timed runs generated by G is denoted as $\mathcal{R}(G)$.

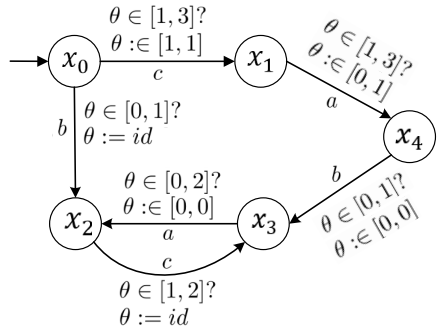
A *timed evolution* of G from $t_0 \in \mathbb{R}_{\geq 0}$ to $t \in \mathbb{R}_{\geq 0}$ is defined by a pair $(\sigma(\rho), t) \in (E \times \mathbb{R}_{\geq 0})^* \times \mathbb{R}_{\geq 0}$, where $t_{st}(\rho) = t_0$ and $t_{en}(\rho) \leq t$. Note that $t - t_{en}(\rho)$ is the time that the system stays at the ending discrete state $x_{en}(\rho)$. Furthermore, we denote as $\mathcal{E}(G, t) = \{(\sigma(\rho), t) \mid (\exists \rho \in \mathcal{R}(G))\ x_{st}(\rho) \in X_0, t_{st}(\rho) = 0, t_{en}(\rho) \leq t\}$ the *timed language of* G *from* 0 *to* $t \in \mathbb{R}_{\geq 0}$, that contains all possible timed evolutions of G from 0 to t.

Definition 2: Given a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ and a time instant $T \in \mathbb{R}_{\geq 0}$, a

discrete state $x' \in X$ is said to be *T-reachable* from $x \in X$ if there exists a timed evolution $(\sigma(\rho), t) \in (E \times \mathbb{R}_{\geq 0})^* \times \mathbb{R}_{\geq 0}$ of G such that $t - t_{st}(\rho) = T$, $x_{st}(\rho) = x$, and $x_{en}(\rho) = x'$. In addition, x' is said to be *unobservably T-reachable* from x if x' is T-reachable from x with a timed evolution $(\sigma(\rho), t)$ such that $S(\sigma(\rho)) \in E_{uo}^*$. □

In simple words, x' is T-reachable from x if a timed evolution leads the system from x to x' with an elapsed time T. If there exists such a timed evolution that produces no observation, x' is unobservably T-reachable from x.

Example 1: Given a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ in Fig. 1(a) with $X = \{x_0, x_1, x_2, x_3, x_4\}$, $E = \{a, b, c\}$, $\Delta = \{(x_0, c, x_1), (x_0, b, x_2), (x_1, a, x_4), (x_2, c, x_3), (x_3, a, x_2), (x_4, b, x_3)\}$, the initial state in $X_0 = \{x_0\}$ is marked by an input arrow. The information given by the timing function Γ and the clock resetting function $Reset$ defined in Fig. 1(b) is presented on the edges. Given an edge denoting a transition $\delta \in \Delta$, the label $\theta \in \Gamma(\delta)?$ on the edge specifies if δ is enabled with respect to θ; the label $\theta :\in Reset(\delta)$ (resp., $\theta := id$) on the edge specifies to which range θ belongs (resp., specifies that the clock is not reset) after the transition is fired. Consider a timed run $\rho : (x_0, 0) \xrightarrow{(b,0.5)} (x_2, 0.5) \xrightarrow{(c,2)} (x_3, 2) \xrightarrow{(a,2)} (x_2, 0)$ that starts from $x_{st}(\rho) = x_0$ at $t_{st}(\rho) = 0$ and terminates in $x_{en}(\rho) = x_2$ at $t_{en}(\rho) = 2$. Three transitions (x_0, b, x_2), (x_2, c, x_3), and (x_3, a, x_2) occur at time instants $t_1 = 0.5$, $t_2 = 2$ and $t_3 = 2$, respectively. The transitions (x_0, b, x_2) and (x_2, c, x_3) do not lead the clock to be reset, while (x_3, a, x_2) resets the clock to 0. Given a timed evolution $(\sigma(\rho), 2)$, it follows that x_2 and x_3 are 2-reachable from x_0. □



(a) A TFA G.

$\delta \in \Delta$	$\Gamma(\delta)$	$Reset(\delta)$
(x_0, c, x_1)	$[1, 3]$	$[1, 1]$
(x_0, b, x_2)	$[0, 1]$	id
(x_1, a, x_4)	$[1, 3]$	$[0, 1]$
(x_2, c, x_3)	$[1, 2]$	id
(x_3, a, x_2)	$[0, 2]$	$[0, 0]$
(x_4, b, x_3)	$[0, 1]$	$[0, 0]$

(b) Timing function and clock resetting function.

Fig. 1: A TFA G w.r.t. the given timing function and clock resetting function.

III. Problem Statement

In this work we model a partially observed timed plant as a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ with a partition of the alphabet into observable and unobservable events: $E = E_o \dot{\cup} E_{uo}$. Next we preliminarily define a *projection function* on timed words.

Definition 3: Given a TFA G with $E = E_o \dot{\cup} E_{uo}$, a *projection function* $P : (E \times \mathbb{R}_{\geq 0})^* \longrightarrow (E_o \times \mathbb{R}_{\geq 0})^*$ is defined as $P(\lambda) = \lambda$, and $P(\sigma(\rho) \cdot (e, t)) = P(\sigma(\rho))$ if $e \in E_{uo}$, or $P(\sigma(\rho) \cdot$

$(e,t)) = P(\sigma(\rho)) \cdot (e,t)$ if $e \in E_o$, for the timed word $\sigma(\rho) \in (E \times \mathbb{R}_{\geq 0})^*$ generated from any timed run $\rho \in \mathcal{R}(G)$ and for all $(e,t) \in E \times \mathbb{R}_{\geq 0}$. Given a timed evolution $(\sigma(\rho),t)$, the pair $(\sigma_o,t) = (P(\sigma(\rho)),t)$ is said to be the *timed observation*. □

Definition 4: Given a TFA G with $E = E_o \dot{\cup} E_{uo}$, and a *timed observation* (σ_o,t), $\mathcal{S}(\sigma_o,t) = \{(\sigma(\rho),t) \in \mathcal{E}(G,t) | P(\sigma(\rho)) = \sigma_o\}$ is said to be the *set of timed evolutions consistent with* (σ_o,t), i.e., the set of timed evolutions that can be generated by G from 0 to t producing the timed observation (σ_o,t); meanwhile $\mathcal{X}(\sigma_o,t) = \{x_{en}(\rho) \in X | (\sigma(\rho),t) \in \mathcal{S}(\sigma_o,t)\}$ is said to be *the set of discrete states consistent with* (σ_o,t), i.e., the set of discrete states in which G may be, after (σ_o,t) is observed. □

This work aims at calculating the set $\mathcal{X}(\sigma_o,t)$, which includes the discrete states reached by each timed evolution $(\sigma(\rho),t)$ consistent with (σ_o,t). In addition, this work also provides a range of the possible clock values associated with each timed evolution $(\sigma(\rho),t)$.

IV. Zone automaton

In [6] a zone automaton is defined to provide a purely discrete event description of the behaviour of a given timed automaton endowed with a single clock reset at each event occurrence. In this paper, we consider a more general setting, where the clock is not required to be reset at each occurrence of an event. The resulting zone automaton differs from other similar structures, such as the one originally introduced in [24] or that in [25]. The zones associated with a discrete state x partition the clock values at x. The timed automaton in [6] can be seen as a particular case of the TFA in this paper. In this section, a new algorithm is provided to compute the zones associated with a given discrete state. After that, we illustrate how to construct the zone automaton based on the zone automaton in [6]. We first introduce the following definitions.

Definition 5: The *set of regions* of a discrete state $x \in X$ is defined as $R(x) = \{[m_x,m_x],(m_x,m_x+1),[m_x+1,m_x+1],(m_x+1,m_x+2),\cdots,[M_x,M_x]\}$, where m_x (resp., M_x) is the minimal (resp., maximal) integer in $\{\Gamma(\delta) | \delta \in O(x) \vee (\delta \in I(x), Reset(\delta) = id)\} \cup \{Reset(\delta) \neq id | \delta \in I(x)\}$. □

The integer m_x (resp., M_x) represents the minimal (resp., maximal) clock value that can enable an output transition at x and that can reach x by an input transition. Note that for a transition δ inputting state x, we search minimal (resp., maximal) value in $\Gamma(\delta)$ if δ does not reset the clock or $Reset(\delta)$ if δ resets the clock. The regions of x include the integers from m_x to M_x and the open segments between the integers. Given $r = [k,k] \in R(x)$ (resp., $r = (k,k+1) \in R(x)$), where $k = m_x,\cdots,M_x - 1$, its successive region is denoted as $succ(r) = (k,k+1)$ (resp., $succ(r) = [k+1,k+1]$). For instance, given the discrete state x_0 of the TFA G in Fig. 1, we have $m_{x_0} = 0$, $M_{x_0} = 3$, and $R(x_0) = \{[0,0],(0,1),[1,1],\cdots,[3,3]\}$.

Definition 6: Given a TFA $G = (X,\ E,\ \Delta,\ \Gamma,\ Reset,\ X_0)$, *the set of output transitions at* $(x,r) \in X \times \bigcup_{x \in X} R(x)$ is defined as $O(x,r) = \{(x,e,x') \in \Delta | e \in E, x' \in X, r \subseteq$

$\Gamma((x,e,x'))\}$, and *the set of input transitions at* (x,r) is defined as $I(x,r) = \{(x',e,x) \in \Delta \mid e \in E, (r \subseteq Reset((x',e,x)) \neq id) \vee (Reset((x',e,x)) = id, r \subseteq \Gamma((x',e,x)))\}$. Obviously, $O(x) = \bigcup_{r \in R(x)} O(x,r)$ and $I(x) = \bigcup_{r \in R(x)} I(x,r)$. □

The set of output (resp., input) transitions at (x,r) includes all the transitions that can fire from x (resp. reach x) with a clock value in r. Based on this definition, Algorithm 1 merges the regions $r_k, r_{k+1}, \cdots, r_{k'} \in R(x)$ into a zone if the following conditions hold for $i = k+1, \cdots, k'$: (a) $r_i = succ(r_{i-1})$; (b) $I(x,r_k) = I(x,r_i)$, $O(x,r_k) = O(x,r_i)$; (c) $Reset(\delta) \neq id$ for all $\delta \in I(x,r_i) \cup O(x,r_i)$. For a region $r \in R(x)$ and a transition $\delta \in I(x,r) \cup O(x,r)$ such that $Reset(\delta) = id$, the region r is included in $Z(x)$ and no merge is done with other regions. Note that the partition of zones according to Algorithm 1 is not optimal, while one can find a more compact partition by further merging the zones associated with δ, where $Reset(\delta) = id$. In the worst case, the maximum number of zones at x equals the number of regions at x, namely $2(M_x - m_x) + 2$.

Algorithm 1: Computation of the set of zones $Z(x)$

Input: A TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$, a discrete state $x \in X$
Output: The set of zones $Z(x)$

1 Initialization: let $m = m_x$, $M = M_x$, $r = [m,m]$, $z = r$, $Z(x) = \emptyset$
2 **while** $r \neq [M,M]$ **do**
3 let $r' = succ(r)$
4 **if** $[O(x,r) = O(x,r')] \wedge [I(x,r) = I(x,r')] \wedge [(\forall \delta \in O(x,r') \cup I(x,r'))Reset(\delta) \neq id]$ **then**
5 let $z = z \cup r'$
6 **else**
7 let $Z(x) = Z(x) \cup \{z\}$ and $z = r'$
8 let $r = r'$
9 let $Z(x) = Z(x) \cup \{z\} \cup \{(M, +\infty)\}$

Example 2: Consider the TFA G in Fig. 1. Algorithm 1 provides the set of zones $Z(x_0) = \{[0,0], (0,1), [1,1], (1,3], (3,+\infty)\}$. In detail, the regions $[0,0], (0,1), [1,1]$ remain in $Z(x_0)$ and do not merge with other regions due to $Reset((x_0,b,x_2)) = id$. The zone $(1,3]$ is obtained by merging the regions $(1,2)$, $[2,2]$, $(2,3)$ and $[3,3]$, which satisfy the *if* condition in line 4 of Algorithm 1. □

Definition 7 ([6]): Consider a TFA $G = (X, E, \Delta, \Gamma, X_0)$[2] with a single clock that is reset at each event occurrence. The *zone automaton* of G is an NFA $ZA(G) = (V, E_\tau, \Delta_z, V_0)$, where

- $V \subseteq X \times \bigcup_{x \in X} Z(x)$ is the finite set of extended states,

[2]The work [6] assumes that timed automata are associated with a clock that is reset at each event occurrence; consequently, there is no clock resetting function to be considered.

- $E_\tau \subseteq E \cup \{\tau\}$ is the alphabet, where the event τ implies time elapsing from any clock value $\theta \in z$ to any $\theta' \in succ(z)$ when G stays at $x \in X$;
- $\Delta_z \subseteq V \times E_\tau \times V$ is the transition relation,
- $V_0 = \{(x, [0, 0]) \mid x \in X_0\} \subseteq V$ is the set of initial extended states. □

The work in [6] corresponds to the particular case with $Reset(\delta) = [0, 0]$ for each transition $\delta \in \Delta$ and a maximal dwell time for each discrete state. The zone automaton is a finite state automaton that provides a purely discrete event description of the behaviour of a given timed automaton. Each state of a zone automaton is called an *extended state*, which is a pair (x, z) whose first element is a discrete state $x \in X$ and whose second element is a zone $z \in Z(x)$ specifying the range of the clock values. The extended state evolves either because of the elapsed time τ or because of the occurrence of a discrete event. In the former, a transition $((x, z), \tau, (x, succ(z))) \in \Delta_z$ corresponds to a time-driven evolution of G from a clock value in z to another clock value in $succ(z) \in Z(x)$. In the latter, an event-driven evolution caused by an event $e \in E$ from (x, z) leads to (x', z') indicating that the occurrence of event e yields x' with a clock value in z'.

In this paper, the zone automaton associated with a TFA can be constructed by implementing the event-driven evolution according to both the timing function and the clock resetting function. In detail, for each transition $(x, e, x') \in \Delta$, we first determine whether $z \subseteq \Gamma((x, e, x'))$; if so, for each zone $z' \in Z(x')$, a transition $((x, z), e, (x', z'))$ is defined if (a) $Reset((x, e, x')) \neq id$ and $z' \subseteq Reset((x, e, x'))$ (the clock is reset after (x, e, x') occurs), or if (b) $Reset((x, e, x')) = id$ and $z = z'$ (the clock is not reset after (x, e, x') occurs). We further define the function $f_x : V \to X$ (resp., $f_z : V \to \bigcup_{x \in X} Z(x)$) mapping an extended state in V to a discrete state in X (resp., a zone of the associated discrete state).

Example 3: Consider the TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ in Fig. 1. The zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$ is shown in Fig. 2. For instance, transition $((x_0, [0, 0]), \tau, (x_0, (0, 1)))$ implies that the clock may evolve from 0 to any value in $(0, 1)$ if G is at x_0. Three transitions labeled with b go from $(x_0, [0, 0])$ to $(x_2, [0, 0])$, from $(x_0, (0, 1))$ to $(x_2, (0, 1))$, and from $(x_0, [1, 1])$ to $(x_2, [1, 1])$, respectively. Each transition implies an event-driven evolution from x_0 to x_2 under the occurrence of a transition (x_0, b, x_2). □

V. Dynamics of a zone automaton

In this section, we explore the dynamics of a zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$ associated with a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ and discuss how the timed evolutions of G are related to the evolutions of zone automaton G_z.

Definition 8: Given a zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$ and a discrete state x of a TFA G, a *τ-run at x* of length k $(1 \leq k \leq n)$ is defined as a sequence of k extended states $(x, z_{(i)}) \in V$ $(i = 1, \cdots, k)$, and event $\tau \in E_\tau$, represented as $\rho_\tau(x) : (x, z_{(1)}) \xrightarrow{\tau} \cdots \xrightarrow{\tau} (x, z_{(k)})$ such that $((x, z_{(i)}), \tau, (x, z_{(i+1)})) \in \Delta_z$ holds for $i = 1, \cdots, k - 1$. The *starting and ending*

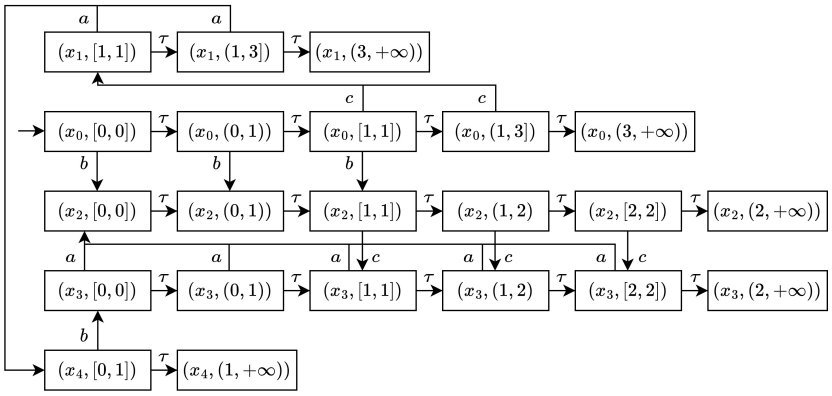


Fig. 2: Zone automaton G_z of the TFA G in Fig. 1.

extended states of $\rho_\tau(x)$ are denoted as $v_{st}(\rho_\tau(x)) = (x, z_{(1)})$ and $v_{en}(\rho_\tau(x)) = (x, z_{(k)})$, respectively. The *duration range* of $\rho_\tau(x)$ is the time distance of $z_{(1)}$ and $z_{(k)}$, denoted as $d(\rho_\tau(x)) = D(z_{(1)}, z_{(k)})$. □

Definition 9: Given a zone automaton $G_z = (V,\ E_\tau,\ \Delta_z,\ V_0)$ of a TFA G, a run of length $k \geq 0$ is a sequence of $k+1$ τ-runs $\rho_\tau(x_{(i)})$ $(i = 0, \cdots, k)$ at $x_{(i)} \in X$, and k events $e_i \in E$ $(i = 1, \cdots, k)$, denoted $\bar{\rho} : \rho_\tau(x_{(0)}) \xrightarrow{e_1} \rho_\tau(x_{(1)}) \cdots \xrightarrow{e_k} \rho_\tau(x_{(k)})$ $(k \geq 0)$, such that $(v_{en}(\rho_\tau(x_{(i-1)})), e_i, v_{st}(\rho_\tau(x_{(i)}))) \in \Delta_z$ holds for $i = 1, \cdots, k$. Consider $\rho \in \mathcal{R}(G)$ starting from t_0 and a time instant $t \geq t_0$, where $\rho : (x_{(0)}, \theta_{(0)}) \xrightarrow{(e_1,t_1)} \cdots \xrightarrow{(e_k,t_k)} (x_{(k)}, \theta_{(k)})$ $(k \geq 0)$, and $t - t_k$ denotes the time that G stays at $x_{(k)}$. The run $\bar{\rho}$ is *consistent* with ρ and t, denoted $\bar{\rho} \sim (\rho, t)$, if $\theta_{(i)} \in f_z(v_{st}(\rho_\tau(x_{(i)})))$ for $i = 0, \cdots, k$, $t_i - t_{i-1} \in d(\rho_\tau(x_{(i-1)}))$ for $i = 1, \cdots, k$, and $t - t_k \in d(\rho_\tau(x_{(k)}))$. The *starting and ending extended states* of $\bar{\rho}$ are $v_{st}(\bar{\rho}) = v_{st}(\rho_\tau(x_{(0)}))$ and $v_{en}(\bar{\rho}) = v_{en}(\rho_\tau(x_{(k)}))$, respectively. The *duration range* of $\bar{\rho}$ is $d(\bar{\rho}) = \bigoplus_{i=1}^{k} d(\rho_\tau(x_i))$. The logical word generated by $\bar{\rho}$ is $s(\bar{\rho}) = e_1 \cdots e_k$ with $s : E_\tau^* \to E^*$. The set of runs generated by G_z is $\mathcal{R}_z(G_z)$. □

The dynamics of a zone automaton G_z can be represented by its runs, each of which is a sequence of τ-runs, which implies the time elapses discretely at discrete states, connected by an evolution caused by an event $e_i \in E$. We now provide a sufficient and necessary condition for the reachability of a discrete state in a TFA and explain the correlation of the dynamics of a TFA and that of zone automaton.

Theorem 1: Given a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$, zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$ and a time instant $t \in \mathbb{R}_{\geq 0}$, $x' \in X$ is $(t - t_0)$-reachable from $x \in X$ by $(\sigma(\rho), t)$ from $t_0 \in \mathbb{R}_{\geq 0}$if and only if there exists a run $\bar{\rho}$ in G_z such that $\bar{\rho} \sim (\rho, t)$,$v_{st}(\bar{\rho}) = (x, z)$, and $v_{en}(\bar{\rho}) = (x', z')$, where $z \in Z(x)$ and $z' \in Z(x')$.

Proof: (if) Let $x = x_{(0)}$, $x' = x_{(k)}$, $t_0, t_1, \cdots, t_k \in \mathbb{R}_{\geq 0}$ and $\bar{\rho} : \rho_\tau(x_{(0)}) \xrightarrow{e_1} \cdots \xrightarrow{e_k} \rho_\tau(x_{(k)})$ be a run such that $e_i \in E$, $t_i - t_{i-1} \in d(\rho_\tau(x_{(i-1)}))$ for $i = 1, \cdots, k$, $t - t_k \in d(\rho_\tau(x_{(k)}))$, and $t - t_0 \in d(\bar{\rho})$. It can be inferred that $(v_{en}(\rho_\tau(x_{(i-1)}))$, e_i, $v_{st}(\rho_\tau(x_{(i)})))$ $\in \Delta_z$ holds for

$i = 1, \cdots, k$. Accordingly, for $i = 1, \cdots, k$, there exist $\theta_{(i-1)} + t_i - t_{i-1} \in f_z(v_{en}(\rho_\tau(x_{(i-1)})))$ and $\theta_{(i)} \in f_z(v_{st}(\rho_\tau(x_{(i)})))$ such that $(x_{(i-1)}, e_i, x_{(i)}) \in O(x_{(i-1)}, f_z(v_{st}(\rho_\tau(x_{(i-1)}))))$ and $(x_{(i-1)}, e_i, x_{(i)}) \in I(x_{(i)}, f_z(v_{st}(\rho_\tau(x_{(i)}))))$. It is obvious that there exists a timed evolution $(\sigma(\rho), t)$, where the timed run ρ: $(x_{(0)}, \theta_{(0)}) \xrightarrow{(e_1,t_1)} \cdots \xrightarrow{(e_k,t_k)} (x_{(k)}, \theta_{(k)})$ satisfies the condition $\bar{\rho} \sim (\rho, t)$. If no event in E occurs in $\bar{\rho} : \rho_\tau(x)$ with $t - t_0 \in d(\bar{\rho})$, then $\bar{\rho} \sim (\rho, t)$, where $\sigma(\rho) = \lambda$. Thus, x' is T-reachable from x.

(only if) Let $(\sigma(\rho), t) \in (E \times \mathbb{R}_{\geq 0})^* \times \mathbb{R}_{\geq 0}$ be a timed evolution from t_0 such that $x_{st}(\rho) = x$ and $x_{en}(\rho) = x'$. The proof is made by induction on the length k of the timed run ρ. The base case is for ρ of length 0 that involves only the discrete state x and no transition in G. It is $\sigma(\rho) = \lambda$ and $x_{st}(\rho) = x_{en}(\rho) = x = x'$. There exists a run $\bar{\rho} : (x, \bar{z}) \xrightarrow{\tau} \cdots \xrightarrow{\tau} (x, z)$ in G_z, where $\bar{\rho} \sim (\rho, t)$. Thus the base case holds. By denoting $x = x_{(0)}$ and $x' = x_{(k)}$, the induction hypothesis is that the existence of a timed evolution $(\sigma(\rho), t)$ generating from t_0, where $\rho : (x_{(0)}, \theta_{(0)}) \xrightarrow{(e_1,t_1)} \cdots \xrightarrow{(e_k,t_k)} (x_{(k)}, \theta_{(k)})$ of length $k \geq 1$ with $x_{(i)} \in X$ and $e_i \in E$ for all $i = 1, \cdots, k$, implies the existence of a run $\bar{\rho} : \rho_\tau(x_{(0)}) \xrightarrow{e_1} \cdots \xrightarrow{e_k} \rho_\tau(x_{(k)})$ in G_z such that $t - t_0 \in d(\bar{\rho})$, $t - t_k \in d(\rho_\tau(x_{(k)}))$, $t_i - t_{i-1} \in d(\rho_\tau(x_{(i-1)}))$ for $i = 1, \cdots, k$, $v_{st}(\bar{\rho}) = (x_{(0)}, z)$ and $v_{en}(\bar{\rho}) = (x_{(k)}, \bar{z})$, where $z \in Z(x_{(0)})$, and $\bar{z} \in Z(x_{(k)})$. We now prove that the same implication holds for $(\sigma(\rho'), t')$, where ρ': $\rho \xrightarrow{(e_{k+1},t)} (x_{(k+1)}, \theta_{(k+1)})$. According to ρ', it is $\theta_{(k+1)} \in Reset((x_{(k)}, e_{k+1}, x_{(k+1)}))$ if $Reset((x_{(k)}, e_{k+1}, x_{(k+1)})) \neq id$, or $\theta_{(k+1)} \in \Gamma((x_{(k)}, e_{k+1}, x_{(k+1)}))$ if $Reset((x_{(k)}, e_{k+1}, x_{(k+1)})) = id$. In addition, $\theta_{(k)} + t - t_k \in \Gamma((x_{(k)}, e_{k+1}, x_{(k+1)}))$. It implies that there exists a run $\bar{\rho}' : \bar{\rho} \xrightarrow{e_{k+1}} \rho_\tau(x_{(k+1)})$ in G_z such that $\theta_{(k+1)} \in f_z(v_{st}(\rho_\tau(x_{(k+1)})))$ and $\theta_{(k+1)} + t' - t \in f_z(v_{en}(\rho_\tau(x_{(k+1)})))$. Therefore, it is $\bar{\rho}' \sim (\rho', t')$ according to $t' - t \in d(\rho_\tau(x_{(k+1)})))$ and $t - t_0 \in d(\bar{\rho})$. ■

By Theorem 1, if x' is $(t - t_0)$-reachable from x via $(\sigma(\rho), t)$ starting at t_0, then in G_z there exists a run $\bar{\rho} \sim (\rho, t)$ that originates from (x, z) and reaches (x', z'), where $z \in Z(x)$ and $z' \in Z(x')$. In turn, given a run $\bar{\rho} \sim (\rho, t)$ in G_z, where $(\sigma(\rho), t)$ starting from t_0, it can be concluded that $f_x(v_{en}(\bar{\rho}))$ is $(t - t_0)$-reachable from $f_x(v_{st}(\bar{\rho}))$. In simple words, the reachability of x' from x within time $t - t_0$ can be analyzed by exploring an appropriate run in the zone automaton.

Example 4: Consider the TFA G in Fig. 1 and zone automaton G_z in Fig. 2. A timed evolution $((c, 1.5)(a, 3), 4)$ of G from 0 to 4 implies that x_4 is 4-reachable from x_0, which can be concluded from a run in G_z as $\bar{\rho} : \rho_\tau(x_0) \xrightarrow{c} \rho_\tau(x_1) \xrightarrow{a} \rho_\tau(x_4)$, where $\rho_\tau(x_0) : (x_0, [0, 0]) \xrightarrow{\tau} (x_0, (0, 1)) \xrightarrow{\tau} (x_0, [1, 1]) \xrightarrow{\tau} (x_0, (1, 3])$, $\rho_\tau(x_1) : (x_1, [1, 1]) \xrightarrow{\tau} (x_1, (1, 3])$ and $\rho_\tau(x_4) : (x_4, [0, 1])$. □

VI. State estimation of TFA

Given a partially observed TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ with $E = E_o \dot{\cup} E_{uo}$, in this section we develop an approach for state estimation based on the zone automaton G_z, given a timed observation $(\sigma_o, t) \in (E_o \times \mathbb{R}_{\geq 0})^* \times \mathbb{R}_{\geq 0}$. We partition this section into two

subsections. In the first subsection, we consider the case where G produces no observation, which is an intermediate step towards the solution of the state estimation problem under partial observation. In the second subsection, we take into account the information coming from the observation of new events at certain time instants, and prove that the discrete states consistent with a timed observation (σ_o, t) and the range of clock value associated with each estimated discrete state can be inferred following a finite number of runs in the zone automaton G_z. We make the following assumption.

Assumption 1 (RO: Reinitialized observations): The clock is reset upon the occurrence of any observable event, i.e.,

$$(x, e, x') \in \Delta,\ e \in E_o \quad \Longrightarrow \quad Reset(x, e, x') \neq id.$$

This assumption is necessary to ensure that the defined zone automaton contains all relevant information to estimate the discrete state. Consider a scenario where an observable event occurs without resetting the clock. In such a case, for future estimations one may need to keep track of this exact value adding new extended states to the zone automaton: thus, the state space of the zone automaton could grow indefinitely as new events are observed. However, it is reasonable to propose the RO assumption considering typical scenarios where a timer is used to record the start and completion of an operation indicated by observable events; the timer is reset whenever such an operation starts or completes.

A. State estimation under no observation

Definition 10: Given a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ with set of unobservable events E_{uo} and zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$, the following set of extended states $V_\lambda(x, z, t) = \{v_{en}(\bar{\rho}) \in V \mid (\exists \bar{\rho} \in \mathcal{R}_z(G_z))t \in d(\bar{\rho}), v_{st}(\bar{\rho}) = (x, z), s(\bar{\rho}) \in E_{uo}^*\}$ is said to be *λ-estimation from $(x, z) \in V$ within $t \in \mathbb{R}_{\geq 0}$*. □

Given a zone automaton, the λ-estimation from $(x, z) \in V$ within $t \in \mathbb{R}_{\geq 0}$ is the set of extended states of G_z that can be reached following a run of duration t, originating at (x, z) and producing no observation. If $(x', z') \in V_\lambda(x, z, t)$, it basically reveals that x' is unobservably T-reachable from x with a clock value $\theta \in z$ according to Theorem 1. In addition, the zone z' associated with x' specifies the range of the value of the clock. The λ-estimation from (x, z) within t can be obtained by enumerating the runs starting from (x, z) with a duration associated with t. By denoting the maximum number of zones for $x \in X$ as Q_x, the complexity for computing the λ-estimation is $\mathcal{O}(q^3|X|)$ with $q = \max_{x \in X} |Q_x|$.

Proposition 1: Given a TFA with a set of discrete states X, the set of unobservable events E_{uo}, and zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$, $x' \in X$ is unobservably T-reachable from $x \in X$, where $T \in \mathbb{R}_{\geq 0}$, if and only if there exist $z \in Z(x)$ and $z' \in Z(x')$ such that $(x', z') \in V_\lambda(x, z, T)$.

Proof: (if) Suppose that there exist $z \in Z(x)$ and $z' \in Z(x')$ such that $(x', z') \in$

TABLE I: State estimation of the TFA G in Fig. 1 under no observation for $t \in [0, 2]$.

k	Time interval I_k	λ-estimation $V_\lambda(x_0, [0,0], t)$, where $t \in I_k$	$\mathcal{X}(\lambda, t), t \in I_k$
0	[0,0]	$\{(x_0, [0,0]), (x_2, [0,0])\}$	$\{x_0, x_2\}$
1	(0,1)	$\{(x_0, (0,1)), (x_2, (0,1))\}$	$\{x_0, x_2\}$
2	[1,1]	$\{(x_0, [1,1]), (x_1, [1,1]), (x_2, [1,1]), (x_3, [1,1])\}$	$\{x_0, x_1, x_2, x_3\}$
3	(1,2)	$\{(x_0, (1,3]), (x_1, [1,1]), (x_1, (1,3]), (x_2, (1,2)), (x_3, (1,2))\}$	$\{x_0, x_1, x_2, x_3\}$
4	[2,2]	$\{(x_0, (1,3]), (x_1, [1,1]), (x_1, (1,3]), (x_2, [2,2]), (x_3, [2,2])\}$	$\{x_0, x_1, x_2, x_3\}$

$V_\lambda(x, z, T)$. There exists a run $\bar{\rho}$ in G_z such that $v_{st}(\bar{\rho}) = (x, z)$, $v_{en}(\bar{\rho}) = (x', z')$, and $\bar{\rho} \sim (\rho, t)$, where $(\sigma(\rho), t)$ begins at $t_0 = t - T$ and $S(\sigma(\rho)) \in E^*_{uo}$. By Theorem 1, x' is unobservably T-reachable from x.

(only if) Let x' be unobservably T-reachable from x. Then, there exists a timed evolution $(\sigma(\rho), t)$ from t_0 such that $x_{st}(\rho) = x$, $x_{en}(\rho) = x'$. Accordingly, there exists a run $\bar{\rho} \sim (\rho, t)$ in G_z such that $v_{st}(\bar{\rho}) = (x, z)$, $v_{en}(\bar{\rho}) = (x', z')$, $s(\bar{\rho}) \in E^*_{uo}$, and $T = t - t_0 \in d(\bar{\rho})$, where $z \in Z(x)$ and $z' \in Z(x')$. Thus, $(x', z') \in V_\lambda(x, z, T)$. ■

Proposition 1 implies that the λ-estimation $V_\lambda(x, z, t)$ provides the set of extended states of G_z that are consistent with no observation at time t starting from x with a clock in z.

Remark 1: According to Proposition 1, $V_\lambda(x, z, t) \subseteq 2^V$, i.e., it is a subset of the states of the zone automaton, and thus it can only take a finite number of values. In addition, the RO assumption implies that, each time a new observation occurs, the set of consistent states is a subset of the extended states of the zone automaton. Therefore, the set of all possible state estimations is finite.

Example 5: Consider the TFA G in Fig. 1, where $E_o = \{a\}$, $E_{uo} = \{b, c\}$, and zone automaton G_z in Fig. 2. Given the following runs in G_z of duration 1 starting from $(x_0, [0,0])$ and involving no observable events: (1) $\bar{\rho}_1 : \rho_\tau(x_0)$; (2) $\bar{\rho}_2 : \rho_\tau(x_0) \xrightarrow{c} \rho_\tau(x_1)$; (3) $\bar{\rho}_3 : \rho_\tau(x_0) \xrightarrow{b} \rho_\tau(x_2)$; and (4) $\bar{\rho}_4 : \rho_\tau(x_0) \xrightarrow{b} \rho_\tau(x_2) \xrightarrow{c} \rho_\tau(x_3)$, where $\rho_\tau(x_0) : (x_0, [0,0]) \xrightarrow{\tau} (x_0, (0,1)) \xrightarrow{\tau} (x_0, [1,1])$, $\rho_\tau(x_1) : (x_1, [1,1])$, $\rho_\tau(x_2) : (x_2, [1,1])$, and $\rho_\tau(x_3) : (x_3, [1,1])$, it can be inferred that $V_\lambda(x_0, [0,0], 1) = \{(x_0, [1,1]), (x_1, [1,1]), (x_2, [1,1]), (x_3, [1,1])\}$. Table I summarizes the λ-estimation and the set of discrete states consistent with (λ, t), where t belongs to a region of $[0, 2]$. □

B. State estimation under partial observation

In this subsection we focus on the most general state estimation problem when a timed observation is received as a pair of a non-empty timed word and a time instant. We first propose a general result that characterizes the set of discrete states of a TFA consistent with a given timed observation, by means of the extended states reachable in zone automaton.

Theorem 2: Consider a TFA $G = (X, E, \Delta, \Gamma, Reset, X_0)$ with set of observable events E_o. Given a timed observation $(\sigma_o, t) \in (E_o \times \mathbb{R}_{\geq 0})^* \times \mathbb{R}_{\geq 0}$, it is $x \in \mathcal{X}(\sigma_o, t)$ if and

only if there exists a run $\bar{\rho} \sim (\rho, t)$ in G_z such that $f_x(v_{st}(\bar{\rho})) \in X_0$, $f_x(v_{en}(\bar{\rho})) = x$, and $(\sigma(\rho), t) \in \mathcal{S}(\sigma_o, t)$.

Proof: (if) In the case that no observation is contained in σ_o, let $\bar{\rho}$ be a run in G_z, where $t \in d(\bar{\rho})$, $f_x(v_{st}(\bar{\rho})) \in X_0$, $f_x(v_{en}(\bar{\rho})) = x$, and $s(\bar{\rho}) \in E_{uo}^*$. In this case there exists $(\sigma(\rho), t)$ such that $\bar{\rho} \sim (\rho, t)$ and $x \in \mathcal{X}(\lambda, t)$. In the case that there exist one or more event measurements, let us suppose that $x_{(0)} \in X_0$, $x_{(k)} = x$, and a run in G_z as $\bar{\rho} : \rho_\tau(x_{(0)}) \xrightarrow{e_1} \cdots \xrightarrow{e_k} \rho_\tau(x_{(k)})$ such that $P_l(s(\bar{\rho})) = S(\sigma_o)$, $t_{i+1} - t_i \in d(\rho_\tau(x_{(i)}))$ with $0 < t_i < t$, $x_{(i)} \in X$ and $e_i \in E$ for $i = 0, \cdots, k$, denoting $t = t_k$. It can be inferred that there exists a timed evolution $(\sigma(\rho), t)$ such that $\bar{\rho} \sim (\rho, t)$ and $x_{(k)}$ is t-reachable from $x_{(0)}$, where the timed run $\rho : (x_{(0)}, \theta_{(0)}) \xrightarrow{(e_1,t_1)} \cdots \xrightarrow{(e_k,t_k)} (x_{(k)}, \theta_{(k)})$ satisfies for $i = 1, \cdots, k$ that $t - t_k \in d(\rho_\tau(x_{(k)}))$, $t_i - t_{i-1} \in d(\rho_\tau(x_{(i-1)}))$, $\theta_{(i-1)} + t_i - t_{i-1} \in \Gamma((x_{(i-1)}, e_i, x_{(i)}))$, $\theta_{(i)} \in Reset((x_{(i-1)}, e_i, x_{(i)}))$ if $Reset((x_{(i-1)}, e_i, x_{(i)})) \neq id$, and $\theta_{(i)} \in \Gamma((x_{(i-1)}, e_i, x_{(i)}))$ if $Reset((x_{(i-1)}, e_i, x_{(i)})) = id$. According to $(\sigma(\rho), t) \in \mathcal{S}(\sigma_o, t)$, $x \in \mathcal{X}(\sigma_o, t)$ holds.

(only if) In the case that $\sigma_o = \lambda$, $x \in \mathcal{X}(\lambda, t)$ holds. There exists a run $\bar{\rho} \sim (\rho, t)$ in G_z such that x is unobservably t-reachable from $x_0 \in X_0$ via $(\sigma(\rho), t)$, where $P(\sigma(\rho)) = \lambda$. Consequently, $f_x(v_{en}(\bar{\rho})) = x$ and $(\sigma(\rho), t) \in \mathcal{S}(\lambda, t)$ hold. In the case that $\sigma_o = (e_{o1}, t_1) \cdots (e_{ok}, t_k)$, where $k \geq 1$, $0 \leq t_1 \leq \cdots \leq t_k \leq t$ and $e_{oi} \in E_o$ $(i = 1, \cdots, k)$, it is $x \in \mathcal{X}(\sigma_o, t)$, implying that x is t-reachable from $x_0 \in X_0$ at time 0 via $(\sigma(\rho), t)$ such that $P(\sigma(\rho)) = \sigma_o$. Consequently, there exists a run $\bar{\rho} \sim (\rho, t)$ in G_z such that $f_x(v_{st}(\bar{\rho})) = x_0$ and $f_x(v_{en}(\bar{\rho})) = x$. Let $\bar{\rho}$ be a sequence of k runs $\bar{\rho}_i$ and k observable events e_{oi}, where $i = 1, \cdots, k$, as $\bar{\rho} : \bar{\rho}_0 \xrightarrow{e_{o1}} \cdots \xrightarrow{e_{ok}} \bar{\rho}_k$ with $s(\bar{\rho}_i) = \varepsilon$. Obviously, $t - t_k \in d(\bar{\rho}_k)$, $t_i - t_{i-1} \in d(\bar{\rho}_{i-1})$ hold for each $i = 1, \cdots, k$. ■

Theorem 2 establishes that checking whether $x \in \mathcal{X}(\sigma_o, t)$ can be done by searching for runs in G_z.

Proposition 2: Consider a TFA G with set of observable events E_o that produces two timed observations $(\sigma_o, t_i), (\sigma_o, t) \in (E_o \times \mathbb{R}_{\geq 0})^* \times \mathbb{R}_{\geq 0}$, where $\sigma_o = (e_{o1}, t_1) \cdots (e_{oi}, t_i)$ and $t_1 \leq \cdots \leq t_i \leq t$ for $i \geq 1$. For each timed state (x, θ) reached by a timed evolution in $\mathcal{S}(\sigma_o, t_i)$, and for each $v \in V_\lambda(x, z, t - t_i)$, where $z \in Z(x)$ and $\theta \in z$, it holds $f_x(v) \in \mathcal{X}(\sigma_o, t)$ if Assumption RO holds.

Proof: Let a timed run $\rho : (x_0, 0) \xrightarrow{(e_1,t_1)} (x_{(1)}, \theta_{(1)}) \cdots \xrightarrow{(e_k,t_k)} (x_{(k)}, \theta_{(k)}) \xrightarrow{(e_{oi},t_i)} (x, \theta)$, where $x_{(1)}, \cdots, x_{(k)} \in X$, $e_1, \cdots, e_k \in E$, and $P(\sigma(\rho)) = \sigma_o$, the timed state (x, θ) is reached by the timed evolution $(\sigma(\rho), t_i) \in \mathcal{S}(\sigma_o, t_i)$. According to Theorem 1, it can be inferred that there exists a run in G_z as $\bar{\rho} : (x_0, [0, 0]) \to \cdots \to (x, z)$, where $\theta \in z$. If Assumption RO holds, it implies that there exists $z \in Z(x)$ such that $\theta \in z$ and $z \subseteq Reset((x_{(k)}, e_{oi}, x))$. Given $v \in V_\lambda(x, z, t - t_i)$, there exists a run $\bar{\rho}' : (x, z) \to \cdots \to v$ such that $t - t_i \in d(\bar{\rho}')$ and $P_l(s(\bar{\rho}')) = \varepsilon$. Given $\bar{\rho}$ and $\bar{\rho}'$, it can be inferred that $f_x(v) \in \mathcal{X}(\sigma_o, t)$ according to Theorem 2. ■

This proposition shows that the state estimation with no observation can be updated by

Algorithm 2: State estimation of a TFA

Input: A TFA G with a set of initial discrete states X_0, a set of observable events $E_o \subseteq E$, a zone automaton $G_z = (V, E_\tau, \Delta_z, V_0)$, and a timed observation (σ_o, t) from 0 to $t \in \mathbb{R}_{\geq 0}$, where $\sigma_o = (e_{o1}, t_1) \cdots (e_{on}, t_n)$ $(n \geq 1)$ and $t_1, \cdots, t_n \in \mathbb{R}_{\geq 0}$

Output: A set of discrete states $\mathcal{X}(\sigma_o, t)$

1 let $\bar{V}_0 = V_0$, $t_0 = 0$ and $X_\lambda = \emptyset$
2 **for** *each* $i \in \{1, \cdots, n\}$ **do**
3 let $e = e_{oi}$, $\bar{V}_i = \emptyset$ and $V_\lambda = \emptyset$
4 **for** *each* $(\bar{x}, \bar{z}) \in \bar{V}_{i-1}$ **do**
5 compute $V_\lambda(\bar{x}, \bar{z}, t_i - t_{i-1})$
6 let $V_\lambda = V_\lambda \cup V_\lambda(\bar{x}, \bar{z}, t_i - t_{i-1})$
7 **for** *each* $v \in V_\lambda$ **do**
8 let $x = f_x(v)$ and $z = f_z(v)$
9 **if** $\exists x' \in X$ *s.t.* $z \subseteq \Gamma((x, e, x'))$ **then**
10 **for** *each* $z' \in Z(x')$ *s.t.* $z' \subseteq Reset((x, e, x'))$ **do**
11 let $\bar{V}_i = \bar{V}_i \cup \{(x', z')\}$
12 let $V_\lambda = \emptyset$
13 **for** *each* $(\bar{x}, \bar{z}) \in \bar{V}_n$ **do**
14 compute $V_\lambda(\bar{x}, \bar{z}, t - t_n)$
15 let $V_\lambda = V_\lambda \cup V_\lambda(\bar{x}, \bar{z}, t - t_n)$
16 **return** $\mathcal{X}(\sigma_o, t) = \{x \in X \mid (\exists z \in Z(x))(x, z) \in V_\lambda\}$

computing associated λ-estimations under RO assumption. Based on the previous results, Algorithm 2 summarizes the proposed approach to compute $\mathcal{X}(\sigma_o, t)$. Consider a timed observation (σ_o, t) with $\sigma_o = (e_{o1}, t_1) \cdots (e_{on}, t_n)$ $(n \geq 1)$, where $e_{o1}, \cdots, e_{on} \in E_o$. The timed observation (σ_o, t) is updated whenever an observable event e_{oi} occurs at a time instant t_i, where $i = 1, \cdots, n$. The algorithm provides the estimated states via a set of extended states $V_\lambda \subseteq V$ while time elapses in $[t_{i-1}, t_i]$ with no event being observed, in addition to a set of extended states $\bar{V}_i \subseteq V$ of G_z consistent with each new observation (e_{oi}, t_i), where $i = 1, \cdots, n$ and $t_0 = 0$. Initially, it is imposed $\bar{V}_0 = V_0$ and $\bar{V}_i = \emptyset$ for all $i = 1, \cdots, n$. Then, for any $i = 1, \cdots, n$, the algorithm computes the λ-estimation from an extended state $(\bar{x}, \bar{z}) \in \bar{V}_{i-1}$ within $t_i - t_{i-1}$ implying the discrete states unobservably $(t_i - t_{i-1})$-reachable from $\bar{x}$ with a clock value in $\bar{z}$, and the set $\bar{V}_i$ is updated with the extended states reached by transitions labeled with e_{oi} from the extended states in V_λ. After the set $\bar{V}_n$ is determined, we initialize V_λ to be empty and update V_λ by including the λ-estimation for each $(\bar{x}, \bar{z}) \in \bar{V}_n$ within $t - t_n$. Finally, we return the set of discrete states of G associated with V_λ as the set of discrete states consistent with (σ_o, t).

The complexity of Algorithm 2 depends on the size n of the timed observation. For each pair (e_{oi}, t_i), two *for* loops are executed: (1) the first *for* loop at Step 4 is executed at most $|V|$ times, computing λ-estimation whose complexity is $\mathcal{O}(q^3|X|)$, where $q = \max_{x \in X} |Q_x|$ denotes

the maximum number of zones for all discrete states, the complexity of this loop is $\mathcal{O}(q^4|X|^2)$; (2) the second *for* loop at Step 7 is executed at most $|V|$ times, and the *for* loop at Step 10 is executed at most $2q+1$ times; hence its complexity is $\mathcal{O}(q^2|X|)$. Finally, the *for* loop at Step 13, analogously to the *for* loop at Step 4, has complexity $\mathcal{O}(q^4|X|^2)$. Overall, the complexity of Algorithm 2 is $\mathcal{O}(n(q^4|X|^2 + q^2|X|) + q^4|X|^2) = \mathcal{O}(nq^4|X|^2)$.

TABLE II: State estimation of the TFA G in Fig. 1 with $\bar{X}_0 = X_0$, $t_0 = 0$ and $(\sigma_o, t), t \in [0, 4]$.

k	σ_o	Time interval I ($t \in I$)	$V_\lambda = \bigcup_{v \in \bar{V}_{k-1}} V_\lambda(f_x(v), f_z(v), t - t_{k-1}), t \in I$	$\mathcal{X}(\sigma_o, t)$	$\bar{V}_k$
1	λ	[0,0]	$\{(x_0, [0,0]), (x_2, [0,0])\}$	$\{x_0, x_2\}$	$\{(x_2, [0,0]), (x_4, [0,1])\}$
		(0,1)	$\{(x_0, (0,1)), (x_2, (0,1))\}$	$\{x_0, x_2\}$	
		[1,1]	$\{(x_0, [1,1]), (x_1, [1,1]), (x_2, [1,1]), (x_3, [1,1])\}$	$\{x_0, x_1, x_2, x_3\}$	
2	$(a, 1)$	[1,1]	$\{(x_2, [0,0]), (x_3, [0,0]), (x_4, [0,1])\}$	$\{x_2, x_3, x_4\}$	$\{(x_2, [0,0])\}$
		(1,2)	$\{(x_2, (0,1)), (x_3, [0,0]), (x_3, (0,1)), (x_4, [0,1])\}$	$\{x_2, x_3, x_4\}$	
		[2,2]	$\{(x_2, [1,1]), (x_3, [0,0]), (x_3, (0,1)), (x_3, [1,1]), (x_4, [0,1])\}$	$\{x_2, x_3, x_4\}$	
		(2,3)	$\{(x_2, (1,2)), (x_3, (0,1)), (x_3, [1,1]), (x_3, (1,2)), (x_4, (1, +\infty))\}$	$\{x_2, x_3, x_4\}$	
		[3,3]	$\{(x_2, [2,2]), (x_3, [1,1]), (x_3, (1,2)), (x_3, [2,2]), (x_4, (1, +\infty))\}$	$\{x_2, x_3, x_4\}$	
3	$(a, 1)(a, 3)$	[3,3]	$\{(x_2, [0,0])\}$	$\{x_2\}$	-
		(3,4)	$\{(x_2, (0,1))\}$	$\{x_2\}$	
		[4,4]	$\{(x_2, [1,1]), (x_3, [1,1])\}$	$\{x_2, x_3\}$	

Example 6: Consider a timed observation $(\sigma_o, 4)$, where $\sigma_o = (a, 1)(a, 3)$, produced by G in Fig. 1 with $E_o = \{a\}$ and $E_{uo} = \{b, c\}$. It implies that the observable event a has been measured twice at $t_1 = 1$ and $t_2 = 3$, respectively, while the current time instant is $t = 4$. Table II shows how the state estimation is updated while time elapses in the time interval $[0, 4]$ taking into account the two observations of event a. □

VII. Conclusions and Future Work

In this paper, we consider timed automata with a single clock. Assuming that certain events are unobservable, we deal with the problem of estimating the current discrete state of the system as a function of the measured timed observations. By constructing a zone automaton that provides a purely discrete description of the considered TFA, the problem of investigating the reachability of a discrete state in the TFA is reduced to the reachability analysis of an extended state in the associated zone automaton. Assuming that the clock is reset upon each occurrence of observable transitions, we present a formal approach that can provide the set of discrete states consistent with a given timed observation and a range of the possible clock values. The proposed approach paves the way for the development of an offline observer, reserved for future work. Additionally, the example provided in this paper is intentionally simplified to illustrate the approach, with real case studies to be explored in the future. Finally, it is worth exploring the extension of the presented approach to timed automata with multiple clocks.

ACKNOWLEDGMENT

The authors would like to thank Julian Klein for his insightful comments on a preliminary version of this manuscript.

REFERENCES

[1] C. Hadjicostis. *Estimation and Inference in Discrete Event Systems*. Springer, 2020.

[2] M. Cabasino, A. Giua, and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica*, 46(9):1531–1539, 2010.

[3] A. Lai, S. Lahaye, and A. Giua. State estimation of max-plus automata with unobservable events. *Automatica*, 105:36–42, 2019.

[4] J. Li, D. Lefebvre, C. Hadjicostis, and Z. Li. Observers for a class of timed automata based on elapsed time graphs. *IEEE Transactions on Automatic Control*, 67(2):767–779, 2022.

[5] C. Gao, D. Lefebvre, C. Seatzu, Z. Li, and A. Giua. A region-based approach for state estimation of timed automata under no event observation. In *Proceedings of IEEE International Conference on Emerging Technologies and Factory Automation*, 1:799–804. IEEE, 2020.

[6] C. Gao, D. Lefebvre, C. Seatzu, Z. Li, and A. Giua. Fault Diagnosis of Timed Discrete Event Systems. *IFAC-PapersOnLine*, 56(2): 9612-9617. 2023.

[7] D. Lefebvre, Z. Li, and Y. Liang. Diagnosis of timed patterns for discrete event systems by means of state isolation. *Automatica*, 153:111045, 2023.

[8] F. Basile, M. P. Cabasino, and C. Seatzu. Diagnosability analysis of labeled Time Petri net systems. *IEEE Transactions on Automatic Control*, 62(3):1384–1396, 2017.

[9] Z. He, Z. Li, A. Giua, F. Basile, and C. Seatzu. Some remarks on "state estimation and fault diagnosis of labeled time Petri net systems with unobservable transitions". *IEEE Transactions on Automatic Control*, 64(12):5253–5259, 2019.

[10] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(1):3–34, 1995.

[11] T. Henzinger. The theory of hybrid automata. In *Verification of Digital and Hybrid Systems*, pages 265–292. Springer, 2000.

[12] R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science*, 126(2):183–235, 1994.

[13] S. Tripakis. Fault diagnosis for timed automata. In *Proceedings of the 7th International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems: Co-sponsored by IFIP WG 2.2*, pages 205–224, 2002.

[14] P. Bouyer, S. Jaziri, and N. Markey. Efficient timed diagnosis using automata with timed domains. In *Proceedings of the 18th Workshop on Runtime Verification (RV'18)*, 11237: 205–221, 2018.

[15] P. Bouyer, L. Henry, S. Jaziri, T. Jéron and N. Markey. Diagnosing timed automata using timed markings. *International Journal on Software Tools for Technology Transfer*, 23: 229–253, 2021.

[16] A. Giua, C. Mahulea, and C. Seatzu. Decentralized observability of discrete event systems with synchronizations. *Automatica*, 85:468–476, 2017.

[17] D. D´Souza and P. Thiagarajan. Product interval automata: a subclass of timed automata. In *Proceedings of Foundations of Software Technology and Theoretical Computer Science(FSTTCS)*, pages 60–71, 2000.

[18] J. Komenda, S. Lahaye, and J. Boimond. Synchronous composition of interval weighted automata using tensor algebra of product semirings. In *IFAC Proceedings Volumes*, 43(12): 318–323, 2010.

[19] L. Lin, R. Su, B. Brandin, S. Ware, Y. Zhu, and Y. Sun. Synchronous composition of finite interval automata. In *Proceedings of IEEE 15th International Conference on Control and Automation (ICCA)*, pages 578–583, 2019.

[20] C. G. Cassandras and S. Lafortune. *Introduction to discrete event systems*. Springer, 2009.

[21] S. Shu, F. Lin, and H. Ying. Detectability of discrete event systems. *IEEE Transactions on Automatic Control*, 52(12):2356–2359, 2007.

[22] F. Lin. Opacity of discrete event systems and its applications. *Automatica*, 47(3):496–503, 2011.

[23] L. Carvalho, Y. Wu, R. Kwong, and S. Lafortune. Detection and mitigation of classes of attacks in supervisory control systems. *Automatica*, 97:121–133, 2018.

[24] C. Daws and S. Tripakis. Model checking of real-time reachability properties using abstractions. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 1998)*, 1384: 313–329. 1998.

[25] P. Bouyer, U. Fahrenberg, K.G. Larsen, N. Markey, J. Ouaknine, and J. Worrell. Model Checking Real-Time Systems. *Handbook of model checking*, pages 1001-1046. 2018.