Probabilistic state estimation for labeled continuous time Markov models with applications to attack detection

Dimitri Lefebvre[1], Carla Seatzu[2], Christoforos N. Hadjicostis[3], and Alessandro Giua[2]

[1]GREAH Laboratory, Normandy Univ., Le Havre, France Email: dimitri.lefebvre@univ-lehavre.fr

[2]DIEE, Univ. of Cagliari, Italy Email: carla.seatzu@unica.it, giua@unica.it

[3]Dept. of Electrical and Computer Engineering, Univ. of Cyprus, Nicosia, Cyprus, Email: chadjic@ucy.ac.cy

October 6, 2022

Abstract

This paper is about state estimation in a timed probabilistic setting. The main contribution is a general procedure to design an observer for computing the probabilities of the states for labeled continuous time Markov models as functions of time, based on a sequence of observations and their associated time stamps that have been collected thus far.

Two notions of state consistency with respect to such a timed observation sequence are introduced and related necessary and sufficient conditions are derived. The method is then applied to the detection of cyber-attacks. The plant and the possible attacks are described in terms of a labeled continuous time Markov model that includes both observable and unobservable events, and where each attack corresponds to a particular subset of states. Consequently, attack detection is reformulated as a state estimation problem.

Published as:
D. Lefebvre, C. Seatzu, C.N. Hadjicostis, A. Giua, "Probabilistic state estimation for labeled continuous time Markov models with applications to attack detection", *Discrete Event Dynamic Systems*, Vol. 32, pp. 65-88, 2022. DOI: 10.1007/s10626-021-00348-y

A correction to this paper has also been published:
D. Lefebvre, C. Seatzu, C.N. Hadjicostis, A. Giua, "Corrections to «Probabilistic state estimation for labeled continuous time Markov models with applications to attack detection»", *Discrete Event Dynamic Systems*, Vol. 32, pp. 539-544, 2022.

In this version, the corrections have been incorporated in the manuscript and are shown in blue.

1 Introduction

Due to their heterogenous and often distributed nature, cyber-physical systems are exposed to attacks from malicious intruders. Therefore, there is an emerging need for developing tools that evaluate the risk of attacks in a quantitative way. Cyber-security in dynamical systems has been studied in the framework of continuous time systems and discrete event systems [6,20,35]. As far as continuous time models are used, attack scenarios depend mainly on replay, zero dynamics, and bias injection [35]. When discrete event models are considered, attacks depend on: (i) the communication channel where the attack happens, (ii) the attack impact on the transmitted data, and (iii) the mechanism to prevent damage [26]. Attacks may occur in the observation channel (known as sensor attacks), in the control channel (known as actuator attacks), or in both the observation and control channels (as in most realistic cases) [4]. For example, weaknesses in the address resolution protocol may be exploited by malicious hosts in a local area network to implement attacks [13]. Deletion, insertion, and replacement are typical examples of the ways an attack can alter the transmitted information [3]. In particular, there are several results concerning sensor attacks that drive a controlled DES to unsafe or undesirable states by manipulating observation sequences [10, 22, 34]. The majority of previous works aims to investigate one special type of cyber attacks, where an attacker can intercept and arbitrarily alter sensor readings in order to trick the controller and drive the system to the targeted undesirable state. In the same context, the approach in [38] includes observations that are corrupted by an intruder who can insert and erase some sensor readings. The authors of [38] construct a stealthy attack structure which aims to make the operator think that the plant is in a safe state whereas it actually reaches an unsafe state. This is also the context of the present work where the attacker manipulates the output labels. In order to prevent the consequences of cyber-attacks, two main approaches have been presented in the literature: detection and prevention on the one hand, and synthesis of a resilient supervisor on the other hand. Detection approaches place an intrusion detection module in the system to detect an attack and prevent it before it causes damage to the system [4,8]. Exploiting supervisory control approaches, a supervisor is synthesized which is resilient to attacks [26].

The problem considered in this paper concerns the first approach where attack detection is formulated in a timed probabilistic setting. The considered systems are modeled by labeled continuous-time Markov models (LCTMM) defined as a subclass of nondeterministic finite automata with possibly multiple initial states, where each arc is associated with a nonnegative real number, representing the firing rate of the transition. Such stochastic models behave basically as continuous-time Markov models (CTMM) [7, 14, 23] and describe sequences of possible events in which the probability of each event depends only on the state attained after the previous event, and the next state is a function of the current state and the event that is selected. The Markovian property of CTMM also implies that the interarrival times between events are distributed exponentially.

CTMM are used in various domains. In particular, Poisson processes, birth and death processes, and parallel queuing systems are examples of uses of continuous-time Markov models in the domain of computer science and networked systems where cyber-attacks may occur [7]. With usual CTMM, the events from one state to the next one are assumed to be undetectable and the best one can do is to compute the probability of the states. In this work, on the contrary, we are interested in the case where some (but not necessarily all) events are observable [36]. Each time an observable event occurs, the label of the event is collected as well as the time when the event occurs. The observation of these timed events (and corresponding time stamps) is helpful for refining the computation of the probabilities of the various states or to even disqualify certain states. Such an LCTMM is different from a hidden Markov model (HMM) [25] which is used to model a system with a Markov model where the parameters and consequently the state probabilities are unknown. Unlike a usual Markov model, in a hidden Markov model, it is assumed that there exists a complete probabilistic mapping from the set of states to a given set of observations. On the contrary, with an LCTMM it is assumed that there is a partial deterministic mapping from the set of transitions to a given set of observations. Observe, however, that the state estimation problem has been considered in the HMM setting. For example, in [27] the authors use discrete-time hidden Markov chains, whose outputs are observable conditions that depend on the current state. In addition, to reduce the bandwidth of the output measurements, they assume outputs are not produced at each time instant.

The state estimation problem in the setting of discrete event systems (DES) has been intensively studied during the last decades [12]. This has also led to the study of various properties of interest, such as diagnosability, opacity and detectability, as well as ways to verify them. Of particular relevance to this work is the property of detectability (i.e., the ability to eventually determine exactly the state of a given system).

In a certain sense, the notions of state consistency introduced in this work can be viewed as condition-based notions of detectability (conditioned on the observation of a given timed sequence).

Most pertinent existing contributions concern logical DES where probabilistic and timing aspects are ignored. In particular, different notions of detectability have been introduced to characterize system properties: strong, weak, periodically strong and periodically weak detectability [28]; (k_1, k_2)-detectability [32]; K-delayed strong detectability [39], D-detectability [21], and so on. In the aforementioned works, the authors focus on the conditions to be satisfied in order to ensure that a given system is detectable. The standard approach relies on observer design of exponential complexity but, for some notions of detectability, algorithms with polynomial complexity exist [11]. There is also interest about initial state estimation [31] and, depending on the considered application, about dynamic event observation (i.e., situations where the occurrences of certain events may or may not be observable, based on the state of the system) [30], [33], as well as state estimation in systems with partially observable outputs (i.e., Moore automata) [37].

Detectability has been also studied in a probabilistic setting with probabilistic finite automata where events occur according to a given set of probabilities [29]. The notions of A-detectability [15] and AA-detectability [15] have been introduced for that purpose. On the one hand, with

A-detectability, one can maintain a logical decision formulation (i.e., one can insist on obtaining a binary decision regarding knowledge of the exact system state following a certain number of observations) and use the probabilistic information provided by the model to assess performance indicators of interest. On the other hand, with AA-detectability, one can relax the logical requirement on the decision (that the system state is known with absolute certainty) by using the probabilistic information to determine the posterior likelihood of this state, conditioned on the specific sequence of observations. In order to quantify the detectability of a given system, some authors have also proposed as a global metric the λ-detectability measure [40]. This measure is defined as the limit of the sum of probabilities of all detectable sequences when the length of the sequences goes to infinity, which can be viewed as a quantitative indicator of goodness of state estimation. Note that non-deterministic or probabilistic aspects can also be added in the observations (apart from the probabilistic occurrence of events) [41].

While the above methods do incorporate probabilistic information, they do not incorporate continuous timing information into the DES. On the other hand, prior studies of state estimation [17], [9] based on certain subclasses of timed automata [1] are not probabilistic and thus do not assume, as we do in this paper, that the interarrival times between events are exponentially distributed. To the best of our knowledge, adding timing aspects in a probabilistic setting was considered in only few contributions. More specifically, [36] has considered the diagnosability problem for a given chemical system. In [18] a global evaluation of attack detectability has been proposed but the approach was developed with a logical observer. Consequently, there is a need to study the state estimation problem in a timed probabilistic setting, which is the aim of this paper.

The paper is organized as follows. Section II introduces labeled continuous-time Markov models (LCTMM) and points out differences with usual CTMM. Section III formulates the considered problem as a state estimation problem and Section IV is devoted to probabilistic state estimation. In particular, two notions of state consistency are introduced and related necessary and sufficient conditions are derived. Section V is about the application to cyber-attack detection. Section VI concludes the paper.

2 Labeled Continuous-Time Markov Models

In this section we define labeled continuous-time Markov models (LCTMM) as nondeterministic finite automata (NFA) with multiple possible initial states, where each arc is associated with a nonnegative real number, representing the firing rate of the transition.

Definition 1 (**Nondeterministic finite automaton**)*:* A *nondeterministic finite automaton* (NFA) is a 4-tuple $A = (X, E, \Delta, X_0)$, where:

- $X = \{x_1, x_2, \ldots, x_n\}$ is a finite set of n *states*;
- E is an alphabet of observable labels;

- $\Delta \subseteq X \times E_\varepsilon \times X$ is the *transition relation*, with $E_\varepsilon = E \cup \{\varepsilon\}$ and ε being the empty string (word);
- $X_0 \subseteq X$ is a *subset of possible initial states.* ▲

The transition relation Δ specifies the dynamics of the automaton. If $(x, e, x') \in \Delta$, then a transition from state x to state x', which we call e-jump, may occur. An e-jump generates an observation e when $e \in E$ while when $e = \varepsilon$, no observation is generated (silent transition).

Definition 2 (**Labeled continuous-time Markov model**)*:* A (finite) *labeled continuous-time Markov model* (LCTMM) is a 4-tuple $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$, where:

- $X = \{x_1, x_2, \ldots, x_n\}$ is a finite set of n *states*;
- E is an alphabet of observable labels;
- $\Lambda \subseteq X \times E_\varepsilon \times \mathbb{R}_{>0} \times X$ is the *transition relation*;
- $\boldsymbol{\pi}_0 \in [0,1]^{1 \times n}$ is an *initial probability vector* (with $\sum_{i=1}^{n} \pi_{0,i} = 1$) where $\pi_{0,i}$ (the i-th entry of vector $\boldsymbol{\pi}_0$) refers to the initial probability of state x_i. ▲

The transition relation Λ specifies the dynamics of the LCTMM: if $(x, e, \mu, x') \in \Lambda$, then from state x an e-jump yielding state x' occurs with rate μ. The time d required to jump from state x to state x' is exponentially distributed and satisfies $Pr(d \leq t) = 1 - e^{-\mu t}$, where t is the sojourn time in state x. Let us define $Out(x_i) = \{(x_i, e, \mu, x) \in \Lambda\}$ as the set of jumps that may occur from state x_i and $Post(x_i) = \{x \in X \text{ such that } (\exists e \in E), (\exists \mu \in \mathbb{R}_{>0}) \text{ with } (x_i, e, \mu, x) \in Out(x_i)\}$ as the set of states reachable from x_i with the occurrence of a single jump. The state probabilities $\pi_i(t \mid \boldsymbol{\pi}_0)$ that the system is in state $x_i \in X$ at time t, given that the vector of initial probabilities is $\boldsymbol{\pi}_0$, form an $1 \times n$ vector $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0)$ whose i-th entry is $\pi_i(t \mid \boldsymbol{\pi}_0)$.

Given an LCTMM G, the *G-associated NFA A* is defined next. For this purpose, let us first define the support $X(t)$ of a given vector of probabilities $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0)$.

Definition 3 (**Support and support vector**)*:* Given a vector of state probabilities $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0)$, the support $X(t)$ of $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0)$ is the subset of states such that:

$$X(t) = \{x_i \in X \text{ such that } \pi_i(t \mid \boldsymbol{\pi}_0) > 0\}. \tag{1}$$

In addition, given any subset of states $X' \subseteq X$, the *support vector* of X' is defined as an n-dimensional binary vector $\boldsymbol{v}_{X'}$ such that $v_{X',i} = 1$ if $x_i \in X'$, otherwise $v_{X',i} = 0$. ▲

Then, the *G-associated NFA A* is defined as $A = (X, E, \Delta_G, X_0)$ where Δ_G is such that $(x, e, x') \in \Delta_G$ if and only if there exists $\mu \in \mathbb{R}_{>0}$ with $(x, e, \mu, x') \in \Lambda$ and X_0 is the support of $\boldsymbol{\pi}_0$. In simple words, A is obtained from G, disregarding the firing rates in the transition

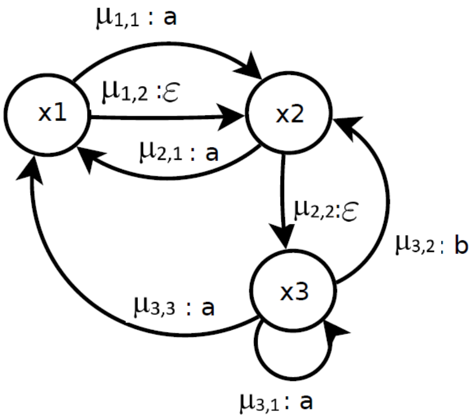

Figure 1: A labeled continuous-time Markov model.

relation as well as the initial probabilities associated with the initial states.

Example 1: Figure 1 shows a graphical representation of the LCTMM with $X = \{x_1, x_2, x_3\}$, alphabet $E = \{a, b\}$, $\boldsymbol{\pi}_0 = [1\ 0\ 0]$ and transition relation:

$$\begin{aligned}\Lambda = \{ \quad & (x_1, a, \mu_{1,1}, x_2), (x_1, \varepsilon, \mu_{1,2}, x_2), (x_2, a, \mu_{2,1}, x_1), \\ & (x_2, \varepsilon, \mu_{2,2}, x_3), (x_3, a, \mu_{3,1}, x_3), (x_3, b, \mu_{3,2}, x_2), (x_3, a, \mu_{3,3}, x_1) \quad \}.\end{aligned}$$

In this example, we have, for instance, $Out(x_1) = \{(x_1, a, \mu_{1,1}, x_2), (x_1, \varepsilon, \mu_{1,2}, x_2)\}$ and $Post(x_1) = \{x_2\}$.

◇

Remark 1: An alternative way of defining a labeled CTMM is that of starting from a CTMM and then associating labels to transitions. However in a CTMM we cannot have two primitives that are possible in an NFA.

- Two transitions in parallel from state x to state x', e.g., transitions $(x_1, \varepsilon, \mu_{1,2}, x_2)$ and $(x_1, a, \mu_{1,1}, x_2)$ in Fig. 1. This case is possible in an NFA provided the parallel transitions have different labels.

  Each transition corresponds to an event that can be observable or unobservable. In the first case, the transition is labeled with a symbol in E and in the second case, the transition is labeled with ε. Observe that, considering the set of parallel transitions relative to a certain pair of states, at most one of them can be labeled with ε, and there can not exist two transitions sharing the same symbol in E.

- Self-loops, i.e., transitions whose starting and final state are the same. In this case, we assume that self-loops are not labeled by the empty string (if this is not the case, the self-loops can be simply removed), but multiple selfloops may be labeled according to two or more label in E. Observe that in a standard Markov model this makes no sense because such a model only describes the rate of change between states (and not the frequency of event occurrences).

For the above reasons, introducing LCTMMs by adding firing rates to NFAs is more general than adding labels to the usual definition of CTMMs [14], [7], [23]. $\diamond$

In order to detail the dynamic evolution of an LCTMM, we further assume that each state $x_i \in X$ is associated with a set of $n_i = |Out(x_i)|$ independent alarm clocks with rates $\mu_{i,k} > 0, k = 1, ..., n_i$. As previously explained, the delays associated to the firing of the output transitions and the sojourn times in states are exponentially distributed. The rates $\mu_{i,k} > 0, k = 1, ..., n_i$ are structural parameters assumed to be known. We define

$$\mu(x_i, x_j) = \sum_{(x_i,e,\mu,x_j)\in Out(x_i)} \mu \tag{2}$$

to be the sum of the rates of the transitions from state x_i to state x_j, and let

$$\mu(x_i) = \sum_{x_j \in Post(x_i)\setminus\{x_i\}} \mu(x_i, x_j).$$

.

$$\mu'(x_i) = \sum_{x_j \in Post(x_i)} \mu(x_i, x_j).$$

When the process enters state x_i, two times of interest can be computed.

- The average time d_i that the process spends at state x_i (including possible jumps from x_i to itself) is defined by

$$d_i = \begin{cases} \infty & \text{if } \mu(x_i) = 0, \\ (\mu(x_i))^{-1} & \text{otherwise.} \end{cases} \tag{3}$$

- The average time d'_i it spends at state x_i before the next jump is defined by

$$d'_i = \begin{cases} \infty & \text{if } \mu'(x_i) = 0 \\ (\mu'(x_i))^{-1} & \text{otherwise,} \end{cases} \tag{4}$$

From state x_i, the probability of jumping to state $x_j \in Post(x_i) \setminus \{x_i\}$ is given by $\mu(x_i, x_j) \cdot d_i$, whereas the probability that the next jump will be $(x_i, e, \mu, x_j) \in \Lambda$ is given by $\mu \cdot d'_i$. The vector $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0)$ can be computed as

$$\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0) = \boldsymbol{\pi}_0 \cdot e^{Qt} \tag{5}$$

where the matrix $Q = \{q_{i,j}\}$ is the *transition rate matrix* (also known as the generator matrix): for all i, $q_{i,i} = -\mu(x_i)$ (diagonal entry) and $q_{i,j} = \mu(x_i, x_j)$ for $j \neq i$.

Note that if $E = \emptyset$ (or equivalently $\Delta \subseteq X \times \{\varepsilon\} \times \mu \times X$) the LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ given in Definition 2 reduces to a standard (i.e., unlabeled) CTMM. In this case, one can define its structure as $(X, Q, \boldsymbol{\pi}_0)$. Such a process generates no observation at all.

Remark 2: From the perspective of the state jumps, an LCTMM behaves as an CTMM (the generator matrix Q of an LCTMM ignores the selfloops and abstracts the parallel transitions in a single transition rate). In particular, regarding the long run, a LCTMM has a single limiting distribution $\boldsymbol{\pi_L} = \lim_{t\to+\infty} \boldsymbol{\pi}(t)$ (that does not depend on the initial distribution) if it is irreducible but it has one or more stationary distributions $\boldsymbol{\pi_S}(\boldsymbol{\pi}_0) = \lim_{t\to+\infty} \boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0)$ that depend on the initial distribution. The number of stationary distributions depends on the number of strongly connected components in the graph of the LCTMM [19].

3 Probabilistic estimation

3.1 Problem statement

A sequence of K consecutive jumps is considered for a given LCTMM within the time interval $[0, t]$: $s = (e_1, \tau_1)(e_2, \tau_2) \ldots(e_K, \tau_K)$, $e_h \in E_\varepsilon, h = 1, \ldots, K$ and $\tau_1, \tau_2, \ldots, \tau_K$ are the time stamps of the jumps that satisfy $0 \leq \tau_1 \leq \tau_2 \leq \ldots \leq \tau_K \leq t$. The observation of s leads to a sequence of observations $\sigma = P(s)$ that can be formally defined by introducing λ as the empty string in $(E_\varepsilon \times \mathbb{R}_{\geq 0})^*$ and the *projection* P as follows:

$$P : (E_\varepsilon \times \mathbb{R}_{\geq 0})^* \to (E \times \mathbb{R}_{\geq 0})^*$$

where

$$\begin{aligned}
&P(\lambda) = \lambda,\\
&P((e, \tau)) = (e, \tau) \text{ for } e \in E \text{ and } P((\varepsilon, \tau)) = \lambda,\\
&P(s(e, \tau)) = P(s)P((e, \tau)) \text{ for } s \in (E_\varepsilon \times \mathbb{R}_{\geq 0})^* \text{ and } (e, \tau) \in E_\varepsilon \times \mathbb{R}_{\geq 0}.
\end{aligned}$$

We assume that an LCTMM is observed within the time interval $[0, t]$ and a sequence of k, $k \leq K$ successive observations $\sigma = P(s) = (e_1, t_1)(e_2, t_2)\ldots(e_k, t_k)$, $e_h \in E, h = 1, \ldots, k$ is collected where $t_1, t_2, \ldots, t_k$ are the time stamps of the observations $e_1, e_2, \ldots, e_k$ that satisfy $0 \leq t_1 \leq t_2 \leq \ldots \leq t_k \leq t$. At time t_h^-, $h = 1, \ldots, k$, event e_h has not yet occurred (and, consequently, has not been observed), but at time t_h the event e_h has already (just) occurred (and has been observed).

The problem we are interested in is how to compute the conditional probability $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma) = [\pi_1(t \mid \boldsymbol{\pi}_0, \sigma) \ldots \pi_n(t \mid \boldsymbol{\pi}_0, \sigma)]$, where $\pi_i(t \mid \boldsymbol{\pi}_0, \sigma)$ denotes the probability that the current state of the plant is x_i at time t, given the observed sequence σ and the initial distribution $\boldsymbol{\pi}_0$. Note that the time stamps of any silent jumps are unknown.

3.2 Extended ε sub-chain

Consider an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ as in Definition 2. The first problem we want to address is to compute $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \lambda)$ i.e., the probabilities of the states when $s = (\varepsilon, \tau_1)(\varepsilon, \tau_2)...(\varepsilon, \tau_k)$ and no observation occurs in the time interval $[0, t]$: $\sigma = P(s) = \lambda$. This problem is a particular case of the general problem described in the problem statement. To solve it, we associate to a given LCTMM a particular CTMM referred to as the extended ε sub-chain of G .

Definition 4 (**Extended ε sub-chain**)*:* Given an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ its *extended ε sub-chain* (EESC) is a CTMM defined by $G_\varepsilon = (X_\varepsilon, \{\varepsilon\}, \Lambda_\varepsilon, \boldsymbol{\pi}_{\varepsilon,0})$, where

- $X_\varepsilon = X \cup \{x_{n+1}\}$ where $n =\mid X \mid$ and x_{n+1} is an additional absorbing state;
- $\Lambda_\varepsilon = \Lambda'_\varepsilon \cup \Lambda''_\varepsilon$ where $\Lambda'_\varepsilon = \{(\bullet, \varepsilon, \bullet, \bullet) \in \Lambda\}$ (i.e., the subset of ε-transitions of Λ), and $\Lambda''_\varepsilon = \{(x_i, \varepsilon, \mu, x_{n+1}) \mid \mu = \sum_{(x_i,e,\mu',x_j) \in Out(x_i), e \in E, x_j \in X} \mu'\}$,
- $\boldsymbol{\pi}_{\varepsilon,0} = [\ \boldsymbol{\pi}_0\ 0\ ]$ is the $(n+1)$-dimensional initial probability vector. ▲

In other words, the EESC of a given LCTMM is constructed by: (a) adding a new state x_{n+1}; (b) keeping all ε-transitions; (c) adding from each state x_i (with $i \leq n$) an ε-transition to state x_{n+1} with rate equal to the sum of all rates of e-transitions (for $e \in E$) exiting state x_i; (d) removing all e-transitions (for $e \in E$).

Note that, as previously remarked, the alphabet of G_ε is by construction the empty set and thus G_ε is a CTMM that can also be represented by the triplet $(X_\varepsilon, Q_\varepsilon, \boldsymbol{\pi}_{\varepsilon,0})$ with the transition rate matrix $Q_\varepsilon \in \mathbb{R}_{\geq 0}^{(n+1)\times(n+1)}$. Note also that the observable transitions in selfloops are considered in the construction of Q_ε (see the a-transition from x_3 to itself in the next example).

Example 2: Consider again the LCTMM in Figure 1, which was discussed in Example 1. Its EESC, shown in Figure 2, is the continuous-time Markov model $(X_\varepsilon, Q_\varepsilon, \boldsymbol{\pi}_{\varepsilon,0})$ where

$$Q_\varepsilon = \begin{bmatrix} -\mu_{1,1} - \mu_{1,2} & \mu_{1,2} & 0 & \mu_{1,1} \\ 0 & -\mu_{2,1} - \mu_{2,2} & \mu_{2,2} & \mu_{2,1} \\ 0 & 0 & -\mu_{3,1} - \mu_{3,2} - \mu_{3,3} & \mu_{3,1} + \mu_{3,2} + \mu_{3,3} \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

◇

The following result shows how the EESC can be used to compute $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \lambda)$.

Lemma 1: Consider an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ and its unobservable extended sub-chain $(X_\varepsilon, Q_\varepsilon, \boldsymbol{\pi}_{\varepsilon,0})$ as defined in Definition 4. Let $\boldsymbol{\pi}_\varepsilon(t|\boldsymbol{\pi}_{\varepsilon,0}) = \boldsymbol{\pi}_{\varepsilon,0} \cdot e^{Q_\varepsilon t}$ be the probability vector of the EESC at time t. Then, the probability vector of the LCTMM at time t given a null

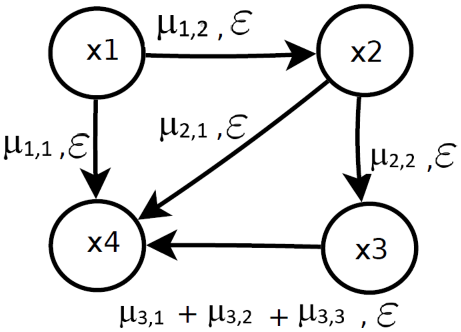
$\mu_{1,2}$, $\mathcal{E}$
x1
x2
$\mu_{1,1}$,$\mathcal{E}$
$\mu_{2,1}$,$\mathcal{E}$
$\mu_{2,2}$,$\mathcal{E}$
x4
x3
$\mu_{3,1}$ + $\mu_{3,2}$ + $\mu_{3,3}$, $\mathcal{E}$

Figure 2: The ε extended sub-chain of the LCTMM in Figure 1.

observation λ is:

$$\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \lambda) = \frac{\boldsymbol{\pi}_\varepsilon(t \mid \boldsymbol{\pi}_{\varepsilon,0}) \cdot [I_{n\times n} \,\vdots\, \mathbf{0}_{n\times 1}]^T}{1 - \boldsymbol{\pi}_\varepsilon(t \mid \boldsymbol{\pi}_{\varepsilon,0}) \cdot [\mathbf{0}_{1\times n} \,\vdots\, 1]^T}, \tag{6}$$

where $I_{n\times n}$ is the identity matrix of dimension $n \times n$, $\mathbf{0}_{n\times 1}$ is the column vector of zeros of length n and $\mathbf{0}_{1\times n}$ is the row vector of zeros of length n.

Proof. Given an initial distribution $\boldsymbol{\pi}_0$, let $x(t)$ and $x_\varepsilon(t)$ denote the current state at time t of, respectively, the LCTMM G and its EESC G_ε.

For each state x_i of the LCTMM, it holds that

$$\begin{aligned} \pi_i(t \mid \boldsymbol{\pi}_0, \lambda) &= Pr(x(t) = x_i \mid \sigma = \lambda) = \frac{Pr((x(t) = x_i) \cap (\sigma = \lambda))}{Pr(\sigma = \lambda)} \\ &= \frac{Pr((x_\varepsilon(t) = x_i) \cap (x_\varepsilon(t) \neq x_{n+1}))}{Pr(x_\varepsilon(t) \neq x_{n+1})} = \frac{Pr(x_\varepsilon(t) = x_i)}{Pr(x_\varepsilon(t) \neq x_{n+1})} \\ &= \frac{\pi_{\varepsilon,i}(t \mid \boldsymbol{\pi}_0)}{1 - \pi_{\varepsilon,n+1}(t \mid \boldsymbol{\pi}_0)}. \end{aligned}$$

Consequently,

$$\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \lambda) = \frac{1}{1 - \pi_{\varepsilon,n+1}(t \mid \boldsymbol{\pi}_{\varepsilon,0})} \; [\; \pi_{\varepsilon,1}(t \mid \boldsymbol{\pi}_{\varepsilon,0}) \; \pi_{\varepsilon,2}(t \mid, \boldsymbol{\pi}_{\varepsilon,0}) \; \cdots \pi_{\varepsilon,n}(t \mid \boldsymbol{\pi}_{\varepsilon,0}) \;]$$

which can be rewritten in a compact way as in Eq. (6). □

3.3 e-transition probability matrix

Consider now an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ as in Definition 2 and a given time $t > 0$. Suppose that $\boldsymbol{\pi}(t^- \mid \boldsymbol{\pi}_0)$ is known and $\sigma = (e, t)$ is observed with $e \in E$, the second problem we want to address is how to compute the probability vector $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma)$. To address this problem, we define for each event $e \in E$ a suitable transition probability matrix.

Definition 5 (*e*-**transition probability matrix**)*:* Given an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ and an event $e \in E$, the *e-transition probability matrix* $Q_e = (q_{e,i,j})$, has element $q_{e,i,j}$ (for $x_i, x_j \in X$) equal to the sum of the firing rates of all e-transitions from state x_i to x_j or equal to zero if no e-transition from state x_i to x_j exists. ▲

Note that the observable transitions in selfloops are considered in the construction of Q_e (see the a-transition from x_3 to itself in the next example).

Example 3: Consider again the LCTMM in Figure 1 and discussed in Example 1, whose alphabet is $E = \{a, b\}$. To this LCTMM, we can associate the a-transition and b-transition probability matrices

$$Q_a = \begin{bmatrix} 0 & \mu_{1,1} & 0 \\ \mu_{2,1} & 0 & 0 \\ \mu_{3,3} & 0 & \mu_{3,1} \end{bmatrix}, \qquad Q_b = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \mu_{3,2} & 0 \end{bmatrix}.$$

◇

The following result shows how the e-transition probability matrices can be used to compute $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma)$ with $\sigma = (e, t)$ from $\boldsymbol{\pi}(t^- \mid \boldsymbol{\pi}_0)$.

Lemma 2: Consider an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ and its e-transition probability matrices as in Definition 5. Given an observation $\sigma = (e, t)$ with $e \in E$, it holds that:

$$\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma) = \frac{\boldsymbol{\pi}(t^- \mid \boldsymbol{\pi}_0) \cdot Q_e}{\boldsymbol{\pi}(t^- \mid \boldsymbol{\pi}_0) \cdot Q_e \cdot \mathbf{1}_{n\times 1}}, \tag{7}$$

where $\mathbf{1}_{n\times 1}$ is the column vector of ones of length n.

Proof. For each state x_j of the LCTMM it holds that

$$\begin{aligned} \pi_j(t \mid \boldsymbol{\pi}_0, (e,t)) &= \lim_{dt\to 0} Pr(x(t) = x_j \mid (e, (t-dt, t])) \\ &= \lim_{dt\to 0} \frac{Pr(x(t) = x_j \cap (e, (t-dt, t]))}{Pr((e, (t-dt, t]))} \\ &= \lim_{dt\to 0} \sum_{i=1}^{n} \frac{Pr((x(t) = x_j \cap (e, (t-dt, t])) \mid x(t-dt) = x_i) \cdot Pr(x(t-dt) = x_i)}{Pr((e, (t-dt, t]))} \end{aligned}$$

The numerator and denominator of the previous expression are reformulated.

- Given an infinitesimal interval dt, the quantity $q_{e,i,j} \cdot dt$ represents the probability that a transition to $x(t) = x_j$ occurs when event e is observed in interval $(t-dt, t]$ given that $x(t-dt) = x_i$. More formally, $Pr(x(t) = x_j \cap (e, (t-dt, t]) \mid x(t-dt) = x_i) = q_{e,i,j} \cdot dt$.

- On the other hand,

$$\begin{aligned} Pr((e,(t-dt,t])) &= \sum_{i=1}^{n} Pr((e,(t-dt,t]) \mid x(t-dt)=x_i)\cdot Pr(x(t-dt)=x_i) \\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n} q_{e,i,j}.dt\right)\cdot Pr(x(t-dt)=x_i) \end{aligned}$$

Considering that $\lim_{dt\to 0} Pr(x(t-dt)=x_i) = \pi_i(t^- \mid \boldsymbol{\pi}_0)$, we have

$$\pi_j(t \mid \boldsymbol{\pi}_0,(e,t)) \;=\; \frac{\sum_{i=1}^{n} q_{e,i,j}\cdot \pi_i(t^- \mid \boldsymbol{\pi}_0)}{\sum_{j=1}^{n}\left(\sum_{i=1}^{n} q_{e,i,j}\cdot \pi_i(t^- \mid \boldsymbol{\pi}_0)\right)}$$

or equation (7) in matrix form. Observe that the denominator in equation (7) is nonzero because the event e has been observed at time t, i.e., there must exist a state x_i from which a transition labeled e may occur and such that $\pi_i(t- \mid \boldsymbol{\pi}_0) > 0$. □

3.4 State estimation

From Lemmas 1 and 2, one can compute iteratively the probability $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0,\sigma)$ at time $t \geq t_k$ when one knows the initial ditribution $\boldsymbol{\pi}_0$ and the sequence of observations σ.

Proposition 1: Consider an LCTMM, and assume that its initial probability distribution $\boldsymbol{\pi}(0)$ is known and that the sequence $\sigma = (e_1,t_1)(e_2,t_2)\ldots(e_k,t_k)$ is observed within $[0,t]$ with $t \geq t_k$. Then, the state probability vector $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0,\sigma)$ at time t can be computed with Eq. (8)

$$\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0,\sigma) = \frac{\boldsymbol{\pi}_\varepsilon(t-t_k \mid \boldsymbol{\pi}_{\varepsilon,k})\cdot [I_{n\times n} \,\vdots\, \mathbf{0}_{n\times 1}]^T}{1-\boldsymbol{\pi}_\varepsilon(t-t_k \mid \boldsymbol{\pi}_{\varepsilon,k})\cdot [\;\mathbf{0}_{1\times n} \,\vdots\, 1]^T}, \tag{8}$$

where the probability distributions $\boldsymbol{\pi}_{\varepsilon,h} = \boldsymbol{\pi}'_{\varepsilon,h}\cdot(\boldsymbol{\pi}'_{\varepsilon,h}\cdot(\mathbf{1})_n)^{-1}$, for $h = 1,\ldots,k$ are iteratively updated with

$$\boldsymbol{\pi}'_{\varepsilon,h} = \frac{\boldsymbol{\pi}_\varepsilon(t_h-t_{h-1} \mid \boldsymbol{\pi}_{\varepsilon,h-1})\cdot [I_{n\times n} \,\vdots\, \mathbf{0}_{n\times 1}]^T}{1-\boldsymbol{\pi}_\varepsilon(t_h-t_{h-1} \mid \boldsymbol{\pi}_{\varepsilon,h-1})\cdot [\;\mathbf{0}_{1\times n} \,\vdots\, 1]^T} Q_{e_h},\;\; h = 2,\ldots,k,$$

and

$$\boldsymbol{\pi}'_{\varepsilon,1} = \frac{\boldsymbol{\pi}_\varepsilon(t_1 \mid \boldsymbol{\pi}_{\varepsilon,0})\cdot [I_{n\times n} \,\vdots\, \mathbf{0}_{n\times 1}]^T}{1-\boldsymbol{\pi}_\varepsilon(t_1 \mid \boldsymbol{\pi}_{\varepsilon,0})\cdot [\;\mathbf{0}_{1\times n} \,\vdots\, 1]^T} Q_{e_1}.$$

Proof : The proof results from the iterative application of Lemmas 1 and 2. From a given LCTMM and the initial probability distribution $\boldsymbol{\pi}_0$, one can compute the initial probability distribution $\boldsymbol{\pi}_{\varepsilon,0}$ of its EESC. Applying Lemma 1, one can compute with Eq. (6) the probability distribution $\boldsymbol{\pi}(t_1^- \mid \boldsymbol{\pi}_0,\lambda)$ at time t_1^- (i.e., just before the first observation e_1 occurs)

$$\boldsymbol{\pi}(t_1^- \mid \boldsymbol{\pi}_0,\lambda) = \frac{\boldsymbol{\pi}_\varepsilon(t_1 \mid \boldsymbol{\pi}_{\varepsilon,0})\cdot [I_{n\times n} \,\vdots\, \mathbf{0}_{n\times 1}]^T}{1-\boldsymbol{\pi}_\varepsilon(t_1 \mid \boldsymbol{\pi}_{\varepsilon,0})\cdot [\;\mathbf{0}_{1\times n} \,\vdots\, 1]^T},$$

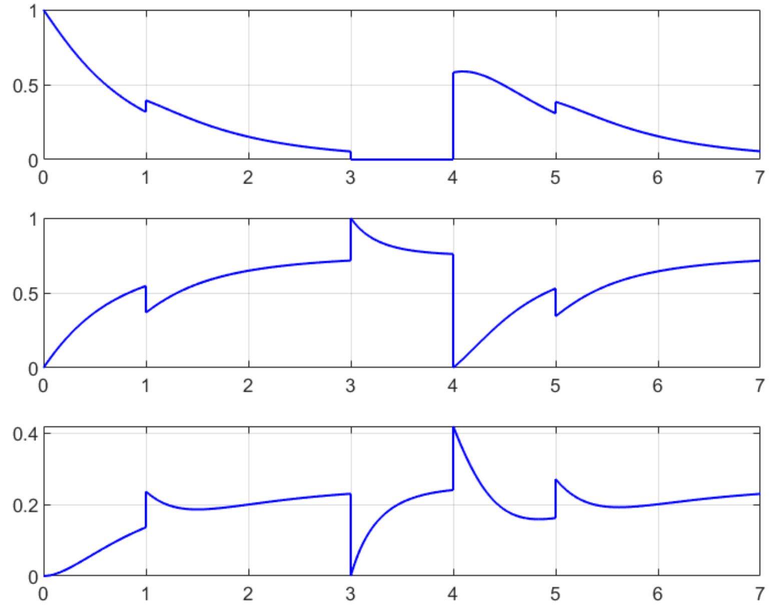

Figure 3: State probabilities with respect to $\sigma = (a,1)(b,3)(a,4)(a,5)$ x_1: top; x_2: center; x_3: bottom.

and also the probability $\boldsymbol{\pi}(t_1 \mid \boldsymbol{\pi}_0, (e_1, t_1))$ at time t_1 (just after e_1 occurs) as $\boldsymbol{\pi}(t_1 \mid \boldsymbol{\pi}_0, (e_1, t_1)) = \boldsymbol{\pi}'_{\varepsilon,1} \cdot (\boldsymbol{\pi}'_{\varepsilon,1} \cdot \mathbf{1}_{n\times 1})^{-1}$ with

$$\boldsymbol{\pi}'_{\varepsilon,1} = \frac{\boldsymbol{\pi}_\varepsilon(t_1 \mid \boldsymbol{\pi}_{\varepsilon,0}) \cdot [I_{n\times n} \mid \mathbf{0}_{n\times 1}]^T}{1 - \boldsymbol{\pi}_\varepsilon(t_1 \mid \boldsymbol{\pi}_{\varepsilon,0}) \cdot [\ \mathbf{0}_{1\times n} \mid 1]^T} Q_{e_1}.$$

Iterating the same computation for each observation, the probability distribution is updated at times $t_2, ..., t_k$ and finally from the initial probability distribution of the EESC $\boldsymbol{\pi}_{\varepsilon,k}$ at time t_k one can compute the probability distribution at time t with Eq. (8). □

Note that the same approach is also useful to evaluate the probability of an arbitrary property that depends on the LCTMM states. We assume that each state $x_i \in X$ may or may not satisfy the property. Thus, $\mathcal{P}$ may be defined as the subset of states in X that satisfy the property of interest. Let us define $\boldsymbol{v}_\mathcal{P}$ as the support vector of the set $\mathcal{P}$. $Pr(\mathcal{P}, t \mid \boldsymbol{\pi}(0), \sigma) = \boldsymbol{\pi}(t \mid \boldsymbol{\pi}(0), \sigma) \cdot \boldsymbol{v}_\mathcal{P}$ is the probability that the property $\mathcal{P}$ is satisfied at a given time t when the plant starts with an initial distribution of states $\boldsymbol{\pi}(0)$ and the sequence σ is observed within $[0, t]$.

Example 4: Consider the LCTMM in Figure 1 with sequence $\sigma = (a,1)(b,3)(a,4)(a,5)$ observed during the time interval $[0, 7]$. The state probabilities are reported in Figure 3.

In order to illustrate that the time stamps of the observation influence the probabilities of the states, consider also the sequence of observations $\sigma = (a, t_1)$ with several values of t_1 within

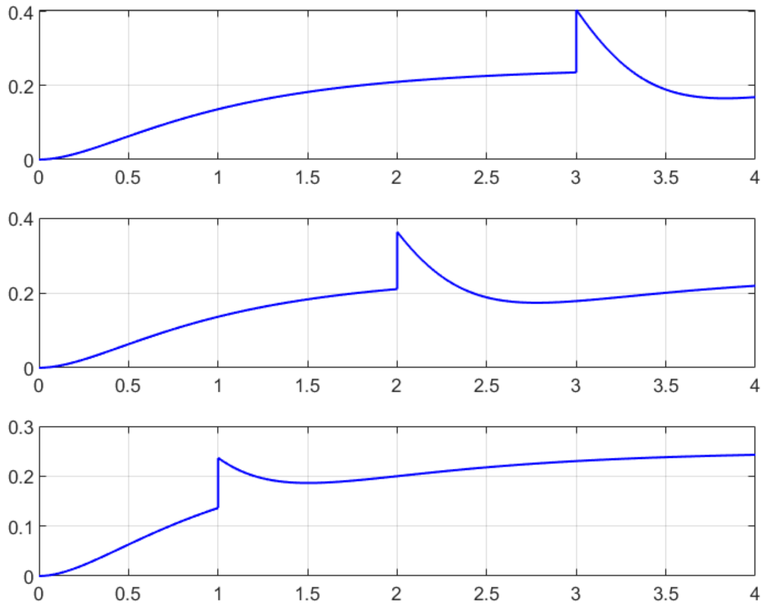

Figure 4: Probability of state x_3 corresponding to $\sigma = (a, t_1)$ with $t_1 = 3$, (top) $t_1 = 2$ (center) and $t_1 = 1$ (bottom).

the time interval $[0, 4]$. Observe in Figure 4 that the probability of x_3 at time $t = 4$ changes depending on the value of t_1.

3.5 State consistency properties based on probabilistic aspects

In this section we are interested in state consistency properties based on the probability vector $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma)$.

Let us first introduce some notation and some preliminary results. Let us refer to the support of $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma)$ as $X_{\boldsymbol{\pi}_0,\sigma}(t)$. By extension, we also define $X_{\boldsymbol{\pi}_0,\sigma}(\infty) = \{x_i \in X \text{ such that } \lim_{t\to+\infty} \pi_i(t \mid \boldsymbol{\pi}_0, \sigma) > 0\}$ (according to Remark 2, such a limit obviously exists).

Lemma 3: Consider an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ and a sequence of k observations $\sigma = (e_1, t_1)(e_2, t_2)...(e_k, t_k)$. Then, it holds that $X_{\boldsymbol{\pi}_0,\sigma}(t_k) \subseteq X_{\boldsymbol{\pi}_0,\sigma}(t)$ for $t > t_k$, and $X_{\boldsymbol{\pi}_0,\sigma}(\infty) \subseteq X_{\boldsymbol{\pi}_0,\sigma}(t)$.

Proof. According to Lemma 2, for each new observation, the state probabilities may switch to new values. Some of these values are zero at t_k and will remain zero as far as nothing more is observed in the system; some of them are also zero at t_k but then increase with respect to t;

and some of them are nonzero at t_k and will vary with respect to time without reaching zero. Consequently, $X_{\boldsymbol{\pi}_0,\sigma}(t_k) \subseteq X_{\boldsymbol{\pi}_0,\sigma}(t)$ if $t > t_k$. In addition, when t tends to ∞ the probabilities of some states may decrease to zero; these states will not be included in $X_{\boldsymbol{\pi}_0,\sigma}(\infty)$ whereas they are included in $X_{\boldsymbol{\pi}_0,\sigma}(t)$. Consequently, $X_{\boldsymbol{\pi}_0,\sigma}(\infty) \subseteq X_{\boldsymbol{\pi}_0,\sigma}(t)$. □

Note that for $\sigma = (e_1,t_1)(e_2,t_2)...(e_k,t_k)$: (i) $X_{\boldsymbol{\pi}_0,\sigma}(t)$ does not depend on t as far as $t_h < t < t_{h+1}$, $h = 1,...,k-1$, or $t > t_k$, i.e., $X_{\boldsymbol{\pi}_0,\sigma}(t) = X_{\boldsymbol{\pi}_0,\sigma}(t')$ if $t_h < t \leq t' < t_{h+1}$, or $t_k < t \leq t' < +\infty$. Consequently, $X_{\boldsymbol{\pi}_0,\sigma}(t)$ with $t_h < t < t_{h+1}$, $h = 1,...,k-1$ or $t > t_k$ will be referred to as $X_{\boldsymbol{\pi}_0,\sigma}(t_h^+)$ or $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$ in the following; (ii) there is no particular inclusion property between $X_{\boldsymbol{\pi}_0,\sigma}(t_k)$ and $X_{\boldsymbol{\pi}_0,\sigma}(\infty)$. In simple words, $X_{\boldsymbol{\pi}_0,\sigma}(t_k)$ is the set of possible states at time t_k when σ is observed, $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$ is the set of possible states for any time $t > t_k$ as far as no new observation occurs, and $X_{\boldsymbol{\pi}_0,\sigma}(\infty)$ is the set of possible states whose probabilities do not tend to 0 when t tends to ∞ (still assuming that no new observation occurs).

Next, we introduce the notions of (σ, t_k^+)-consistent and (σ,∞)-consistent subsets of states.

Definition 6 (**(σ, t_k^+)-consistent and (σ,∞)-consistent subsets of states)***:* Given an LCTMM G and a sequence of observations $\sigma = (e_1,t_1)(e_2,t_2)...(e_k,t_k)$, the subset of states $X' \subseteq X$ is said to be (σ, t_k^+)-consistent if $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+) \subseteq X'$. Similarly, the subset of states $X' \subseteq X$ is said to be (σ,∞)-consistent if $X_{\boldsymbol{\pi}_0,\sigma}(\infty) \subseteq X'$. ▲

In simple words, X' is (σ, t_k^+)-consistent when, after observing sequence σ, one can deduce that the system state belongs to X' as far as no new observations occurs. In addition, X' is (σ,∞)-consistent when the probability of the system state to be in X' converges to 1 as the time after σ has been observed goes to infinity and no new observation occurs. Note that the previous definitions are applicable for a particular state $x_i \in X$ or for a state property $\mathcal{P}$. Observe also that such properties depend on the initial distribution $\boldsymbol{\pi}_0$. Given an LCTMM $G = (X, E, \Lambda, \pi_{\mathbf{0}})$ and its G-associated NFA $A = (X, E, \Delta_G, X_0)$ (A being defined as in Section 2), timing aspects are ignored and we can use this logical model to define the logical observer of A. This observer is obtained by extending the standard method [5], that transforms an NFA into a deterministic finite automaton when several possible initial states exist (see the proof of Theorem 1 below for details). Let $OBS = (X_L, E, \Delta_L, x_{L0})$ be the logical observer where X_L is the set of observer states (each state $x_L \in X_L$ is a subset of X), Δ_L is the transition function of OBS, and x_{L0} is the observer initial state. The complexity in space of OBS is $O(2^{|X|})$. In addition, let us define the logical sequence $H(\sigma) = e_1\ e_2\ ...\ e_k$, for any sequence of observations $\sigma = (e_1,t_1)(e_2,t_2)...(e_k,t_k)$ and $H(\lambda) = \lambda$ (i.e., H filters out the logical sequence of events of σ). Finally, $x_L(H(\sigma)) \in X_L$ is the observer state (i.e., the subset of system states that are consistent with the sequence of observations σ when timing information is ignored).

Proposition 2: Let us consider a given LCTMM G, and a sequence of observations $\sigma = (e_1,t_1)(e_2,t_2)...(e_k,t_k)$. Given $X' \subseteq X$ a subset of system states, X' is (σ, t_k^+)-consistent if and only if $x_L(H(\sigma)) \subseteq X'$.

Proof : Observe first that the design of the usual logical observer [5] can be trivially extended to the case where the LDFA A has several possible initial states, and define the set of possible initial states of A as X_0 where X_0 is the support of $\boldsymbol{\pi}_0$. Let us consider a sequence of k observations $\sigma = (e_1, t_1)...(e_k, t_k)$ and $H(\sigma) = e_1 \ ... \ e_k$. The result of Theorem 1 is obtained by considering sequences of observations σ of increasing length and by showing that $x_L(H(\sigma)) = X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$.

1. Let $\sigma_0 = \lambda$ and $x_L(\lambda)$ be the set of states reachable from X_0 by executing 0 or more ε-jumps in A. Each state $x_i \in x_L(\lambda)$ is also reachable with 0 or more ε-jumps in G from X_0 and $\pi_i(t \mid \boldsymbol{\pi}_0, \lambda) > 0$. The states $x_i \in X \setminus x_L(\lambda)$ are not reachable with ε-jumps, thus $\pi_i(t \mid \boldsymbol{\pi}_0, \lambda) = 0$. Consequently $X_\lambda(0^+) = x_L(\lambda)$. According to Definition 6, a subset of states $X' \subseteq X$ is $(\lambda, 0^+)$-consistent if and only if $x_L(\lambda) \subseteq X'$.

2. Consider now $\sigma_1 = (e_1, t_1)$. For each $x \in x_L(\lambda)$ one can compute first the subset of states $X(x, e_1)$ that are reachable from x executing exactly one e_1-jump in A and then the subset of states $x_L(x, e_1)$ reachable from any of the states previously obtained in $X(x, e_1)$ by executing 0 or more ε-jumps in A. $x_L(e_1) = \cup_{x \in x_L(\lambda)} x_L(x, e_1)$ is the subset of states consistent with e_1. Each state $x_i \in x_L(e_1)$ is also reachable with 0 or more ε-jumps in G from $X(\sigma_1)$ and $\pi_i(t \mid \boldsymbol{\pi}_0, \sigma_1) > 0$. The states $x_i \in X \setminus x_L(e_1)$ are not reachable with ε-jumps and $\pi_i(t \mid \boldsymbol{\pi}_0, \sigma_1) = 0$. Consequently, $X_{\boldsymbol{\pi}_0,\sigma_1}(t_1^+) = x_L(e_1)$ and a subset of states $X' \subseteq X$ is (e_1, t_1^+)-consistent if and only if $x_L(e_1) \subseteq X'$. The same reasoning can be repeated for sequences of observations of length 2 to $k-1$.

3. Consider finally $\sigma_{k-1} = (e_1, t_1)..(e_{k-1}, t_{k-1})$ and $\sigma = \sigma_{k-1}(e_k, t_k)$. For each $x \in x_L(H(\sigma_{k-1}))$ one can compute $x_L(H(\sigma)) = \cup_{x \in x_L(H(\sigma_{k-1}))} x_L(x, \ H(\sigma))$, and $x_L(H(\sigma))$ is the subset of system states consistent with the logical sequence of observations $e_1 \ ... \ e_k$. Each state $x_i \in x_L(H(\sigma))$ is also reachable with 0 or more ε-jumps in G from $X(\sigma)$ and $\pi_i(t \mid \boldsymbol{\pi}_0, \sigma) > 0$. The states $x_i \in X \setminus x_L(H(\sigma))$ are not reachable with ε-jumps and $\pi_i(t \mid \boldsymbol{\pi}_0, \sigma) = 0$. We have $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+) = x_L(H(\sigma))$. Consequently, $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+) = x_L(H(\sigma))$ and a subset of states $X' \subseteq X$ is (σ, t_k^+)-consistent if and only if $x_L(H(\sigma)) \subseteq X'$. □

As a corollary of Theorem 1 it follows that $X_{\boldsymbol{\pi}_0,\sigma}(\infty) \subseteq x_L(H(\sigma))$. Consequently, the probability vector $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma)$ may be used to refine the state estimation in a probabilistic sense when time goes to infinity and no new observation occurs (since we assume a probability is zero if smaller than an arbitrarily fixed small value). Theorem 2 provides a characterisation of (σ, ∞)-consistent subsets of states. For this purpose, let us first introduce the notion of reduced (σ, ε) sub-chain for a given LCTMM.

Definition 7 (**Reduced** (σ, ε) **sub-chain**)*:* Given an LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ and a sequence of observations $\sigma = (e_1, t_1)...(e_k, t_k)$, the *reduced* (σ, ε) *sub-chain* (RESC) of G is a CTMM defined by $G_\sigma = (X_{\boldsymbol{\pi}_0,\sigma}(t_k^+), \{\varepsilon\}, \Lambda_{\boldsymbol{\pi}_0,\sigma}(t_k^+), \boldsymbol{\pi}_{\boldsymbol{\pi}_0,\sigma}(t_k))$, where

- $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$ is the support of $\boldsymbol{\pi}(t \mid \boldsymbol{\pi}_0, \sigma)$ for $t > t_k$,
- $\Lambda_{\boldsymbol{\pi}_0,\sigma}(t_k^+) = \{(x_i, \varepsilon, \mu, x_j) \in \Lambda\}$ with $x_i, x_j \in X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$ (i.e., the subset of ε-transitions of Λ within $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$),
- $\boldsymbol{\pi}_{\boldsymbol{\pi}_0,\sigma}(t_k)$ is the vector of size $1\times|X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)|$ with the probabilities of the states in $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$ at time t_k. ▲

In other words, the RESC of a given LCTMM is constructed by: (a) keeping all states in $X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$; (b) keeping all ε-transitions within these states with their rate; (c) removing all other ε-transitions and all e-transitions (for $e \in E$).

The graph of G_σ contains a transient component and h_σ ($h_\sigma \geq 1$) *Absorbing Strongly Connected Components* (ASCC) $\Omega_{\sigma,i}$, $i = 1, ..., h_\sigma$, some of which are reachable from a given initial distribution $\boldsymbol{\pi}_0$ whereas the others are not. Several methods of linear complexity exist to compute the ASCCs of a given graph, some of them based on the Tarjan or Gabow algorithms [2]. Let us introduce $\Omega_\sigma = (\cup_{i=1,...,h_\sigma} \Omega_{\sigma,i}) \cap X_{\boldsymbol{\pi}_0,\sigma}(t_k^+)$. The aim of Theorem 2 is to provide a necessary and sufficient condition for (σ, ∞)-consistency in terms of absorbing strongly connected components of the graph associated to the LCTMM.

Proposition 3: Let us consider a given LCTMM G, a sequence of observations $\sigma = (e_1, t_1)(e_2, t_2)...(e_k, t_k)$, and $X' \subseteq X$ a subset of states. X' is (σ, ∞)-consistent if and only if $\Omega_\sigma \subseteq X'$.

Proof : To prove Theorem 2, we prove that $\Omega_\sigma = X_{\boldsymbol{\pi}_0,\sigma}(\infty)$. According to Definition 6, a (σ, ∞)-consistent state x_i has a nonzero probability in the long run and belongs necessarily to Ω_σ (otherwise $\pi_i(t|\boldsymbol{\pi}_0, \sigma)$ will tend to 0 when t tends to ∞). Consequently $\sum_{x_i \in \Omega_\sigma}(\pi_i(\infty|\boldsymbol{\pi}_0, \sigma)) = 1$. If $\Omega_\sigma \subseteq X'$ then $\boldsymbol{\pi}_{X'}(\infty|\boldsymbol{\pi}_0, \sigma)) = 1$ and X' is (σ, ∞)-consistent. Otherwise there exists $x_i \in \Omega_\sigma$, $x_i \notin X'$, $\boldsymbol{\pi}_{X'}(\infty|\boldsymbol{\pi}_0, \sigma)) < 1$, and X' is not (σ, ∞)-consistent. As a conclusion, $\Omega_\sigma = X_{\boldsymbol{\pi}_0,\sigma}(\infty)$ and X' is (σ, ∞)-consistent if and only if $\Omega_\sigma \subseteq X'$. □

Example 5: Consider the LCTMM in Figure 1 with the sequence of observations $\sigma = (a, 1)(b, 3)(a, 4)(a, 5)$ within the time interval $[0, 7]$. The supports of the probability vectors are computed as follows: $X_\sigma(0) = \{x_1\}$, $X_\sigma(0^+) = \{x_1, x_2, x_3\}$, $X_{\boldsymbol{\pi}_0,\sigma}(1) = X_{\boldsymbol{\pi}_0,\sigma}(1^+) = \{x_1, x_2, x_3\}$, $X_{\boldsymbol{\pi}_0,\sigma}(3) = \{x_2\}$ and $X_{\boldsymbol{\pi}_0,\sigma}(3^+) = \{x_2, x_3\}$, and so on. When the whole time sequence σ is considered, $X_{\boldsymbol{\pi}_0,\sigma}(5) = X_{\boldsymbol{\pi}_0,\sigma}(5^+) = \{x_1, x_2, x_3\}$ and this estimation holds up to $t \leq 7$. In addition, $X_{\boldsymbol{\pi}_0,\sigma}(\infty) = \{x_2, x_3\}$ if one assumes that no additional observation is collected after time 5. Consequently, $\{x_2, x_3\}$ is (σ, ∞)-consistent. The same set is $(\sigma, 3^+)$-consistent but not $(\sigma, 5^+)$-consistent.

4 Application to cyber security

4.1 Model of cyber-attacks

In this section we consider a plant that is partially observed through a labeling function and that may be corrupted by a particular type of cyber-attacks that manipulate the output symbols. The following assumptions are considered for simplicity:

1. the attacks are not permanent,
2. only one attack affects the system at a time,
3. the plant is not attacked at time 0 and the initial state and initial time are assumed to be known.

We assume that the normal behaviour of the plant when no attack is present is described by an LCTMM $G_0 = (X_0, E, \Lambda_0, \boldsymbol{\pi}_{0,0})$. The plant can be subject to K different types of attacks. The behaviour of the system under attack of type A_k (for $k = 1, \ldots, K$) can also be described by LCTMM $G_k = (X_k, E, \Lambda_k, \boldsymbol{\pi}_{0,k})$ with $\boldsymbol{\pi}_{0,k}(0) = \mathbf{0}_{1\times|X_k|}$ (Assumption 2). It is important to note that the sets X_k, $k = 1, ..., k$ are copies of the set X and do not correspond to any new set of states. Indeed, the plant model is replicated to describe the different observations that the plant can produce due to the attacks when it evolves. Such a representation corresponds more or less to the composition of the plant by the attack mode and will be helpful for probabilistic detection. Assuming the switching between the different modes is also a Markovian process, one can define the sets of transition relations

- $\Lambda_{0,k} = \{(x_i, \varepsilon, \mu, x_j)$, with $x_i \in X_0$, and $x_j \in X_k\}$, $k = 1, ..., K$, that describes how the attack A_k starts from normal behaviour,
- $\Lambda_{k,0} = \{(x_i, \varepsilon, \mu, x_j)$, with $x_i \in X_k$, and $x_j \in X_0\}$, $k = 1, ..., K$, that describes how the attack A_k ends when the system returns to normal behavior,
- $\Lambda_{k,m} = \{(x_i, \varepsilon, \mu, x_j)$, with $x_i \in X_k$, and $x_j \in X_m\}$, $k = 1, ..., K$, $m = 1, ..., K$, that describes how attack A_k switches to attack A_m.

We assume that attack starting, ending and switching correspond to silent events. Other events may be silent or observable. Then, the plant under possible attacks can be described by a global LCTMM $G = (X, E, \Lambda, \boldsymbol{\pi}_0)$ with

- $X = \bigcup_{k=0}^{K} X_k$
- $\Lambda = \left(\bigcup_{k=0}^{K} \Lambda_k\right) \cup \left(\bigcup_{k=0}^{K} \bigcup_{m=0}^{K} \Lambda_{k,m}\right)$
- $\boldsymbol{\pi}_0 = [\boldsymbol{\pi}_{0,0} \ \boldsymbol{\pi}_{0,1} \ \cdots \ \boldsymbol{\pi}_{0,K}]$

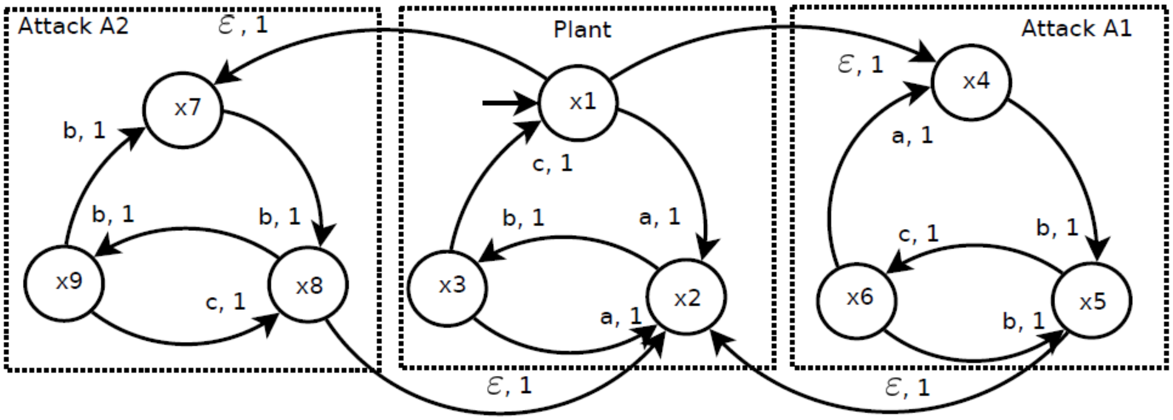

Figure 5: LCTMM model of a plant subject to two attacks.

Note that the underlying graph described by the generator matrix of G is strongly connected (Assumption 1). Each mode (the normal behaviour and the attack modes) is considered as a property to be detected and the probability of detection will be computed.

Example 6: Consider the example of a plant affected by two different attacks A_1 and A_2, depicted in Fig. 5. The set of states is $X = X_0 \cup X_1 \cup X_2$ with $X_0 = \{x_1, x_2, x_3\}$, $X_1 = \{x_4, x_5, x_6\}$ and $X_2 = \{x_7, x_8, x_9\}$ where the sets $\{x_4, x_5, x_6\}$ and $\{x_7, x_8, x_9\}$ are copies of the set $\{x_1, x_2, x_3\}$. The events that correspond to the starting or ending of an attack are unobservable. The other events generate symbols a, b or c and $E = \{a, b, c\}$. Attack A_1 permutes the labels and transforms a into b, b into c and c into a. Attack A_1 starts from state x_1 and ends at state x_2. Attack A_2 replaces a and c by b except the label a from state x_3 to state x_2 that is replaced by c. Attack A_2 also starts from state x_1 and ends at state x_2. For simplicity, all events in this system are assumed to be exponentially distributed with time parameters that are equal to 1. The initial state is assumed to be state x_1. In Fig. 5, the labels resulting from the observation function and the time parameters are reported.

4.2 Attack detection strategy

In this section we use the probabilistic estimation of the states, detailed in previous section, in order to estimate the mode of the system and to detect the attacks. For this purpose, let us introduce the $K+1$ properties: $\mathcal{N} = X_0$ and $\mathcal{A}_k = X_k$, $k = 1, ..., K$. We assume a simple detection strategy where we select the most likely among the different modes of operation. Consequently, we define $Pr(\mathcal{N}, t \mid \boldsymbol{\pi}(0), \sigma) = \boldsymbol{\pi}(t \mid \boldsymbol{\pi}(0), \sigma) \cdot \boldsymbol{v}_{|X_0|}$ as the probability that the plant is in normal mode at a given time t when it starts with an initial distribution of states $\boldsymbol{\pi}(0)$ and the sequence σ is observed within $[0, t]$. Similarly, $Pr(\mathcal{A}_k, t \mid \boldsymbol{\pi}(0), \sigma) = \boldsymbol{\pi}(t \mid \boldsymbol{\pi}(0), \sigma) \cdot \boldsymbol{v}_{|X_k|}$ is the probability that the plant is in attack mode A_k at t.

The estimated mode $M^*(t \mid \boldsymbol{\pi}(0), \sigma)$ at a given time t with respect to the sequence of observations σ is then obtained as

$$M^*(t \mid \boldsymbol{\pi}(0), \sigma) = \text{argmax}_{\mathcal{M} \in \{\mathcal{N}, \mathcal{A}_k, k=1,\ldots,K\}} \{Pr(\mathcal{M}, t \mid \boldsymbol{\pi}(0), \sigma)\}. \tag{9}$$

Observe that the proposed detection strategy may be affected by detection errors. A confidence index $CI(t \mid \boldsymbol{\pi}(0), \sigma)$ is introduced with equation (10) in order to quantify the risk of detection error.

$$CI(t \mid \boldsymbol{\pi}(0), \sigma) = \left(\left(\frac{K+1}{K} \right) Pr(M^*(t \mid \boldsymbol{\pi}(0), \sigma)) - \frac{1}{K} \right)^2, \tag{10}$$

where $Pr(M^*(t \mid \boldsymbol{\pi}(0), \sigma)) = \max_{\mathcal{M} \in \{\mathcal{N}, \mathcal{A}_k, k=1,\ldots,K\}} \{Pr(\mathcal{M}, t \mid \boldsymbol{\pi}(0), \sigma)\}$.

Note that $CI(t \mid \boldsymbol{\pi}(0), \sigma) = 1$ when $Pr(M^*(t \mid \boldsymbol{\pi}(0), \sigma)) = 1$ (i.e., no detection error) and $CI(t \mid \boldsymbol{\pi}(0), \sigma) = 0$ when $Pr(M^*(t \mid \boldsymbol{\pi}(0), \sigma)) = \frac{1}{K+1}$ (i.e., maximal uncertainty since all modes are equally probable).

Example 7: Consider a scenario where the system in Fig. 5 behaves as represented in Fig. 6 (the time is reported in X axis and the states are reported in Y axis). Several periods can be distinguished in this scenario. During period [0 3.2) the plant is safe, then it is attacked by A_2 during period [3.2 10.5), returns to safe operation during the interval [10.5, 12.4), and is attacked by A_1 during period [10.5 19.5). After time 19.5 the plant is safe again. The sequence of observations generated with this scenario is as follows

$$\begin{aligned} \sigma = \; & (a, 1.16)(b, 2.47)(a, 2.50)(b, 2.96)(c, 3.01)(b, 3.55)(b, 4.20) \\ & (c, 5.98)(b, 6.39)(b, 6.96)(b, 10.41)(b, 10.55)(c, 10.61)(a, 10.86)(b, 11.49) \\ & (c, 11.63)(b, 13.32)(c, 13.82)(b, 14.25)(c, 15.41)(a, 18.03)(b, 19.32)(b, 19.60) \\ & (c, 19.66)(a, 20.16)(b, 22.03)(c, 22.75). \end{aligned}$$

Three properties are defined here: $\mathcal{N} = \{x_1, x_2, x_3\}$, $\mathcal{A}_1 = \{x_4, x_5, x_6\}$ and $\mathcal{A}_2 = \{x_7, x_8, x_9\}$. The probabilities for normal mode and for each attack mode are computed with respect to the sequence of observations and reported in Fig. 7 with full blue lines (the true modes are also reported in red dashed line).

Applying the detection strategy defined by equation (9), results of the probabilistic mode estimation are reported in Fig. 9. In this figure, "1" stands for the normal mode, "2" stands for attack A_1 and "3" stands for attack A_2. From Fig. 7 and Fig. 9 (top), one can notice that both

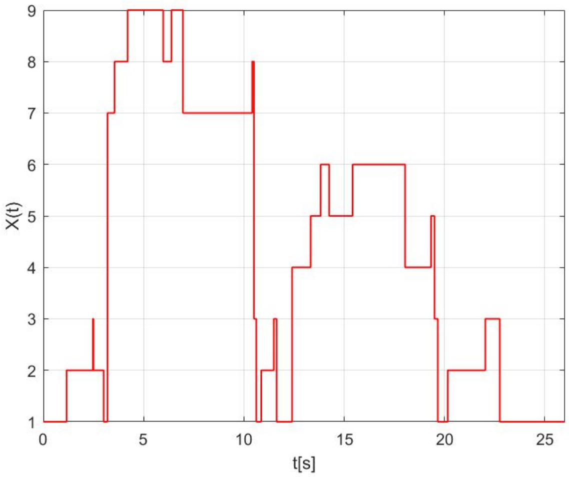

Figure 6: An example of attack scenario: $X(t) = i$ denotes the current state x_i at time t.

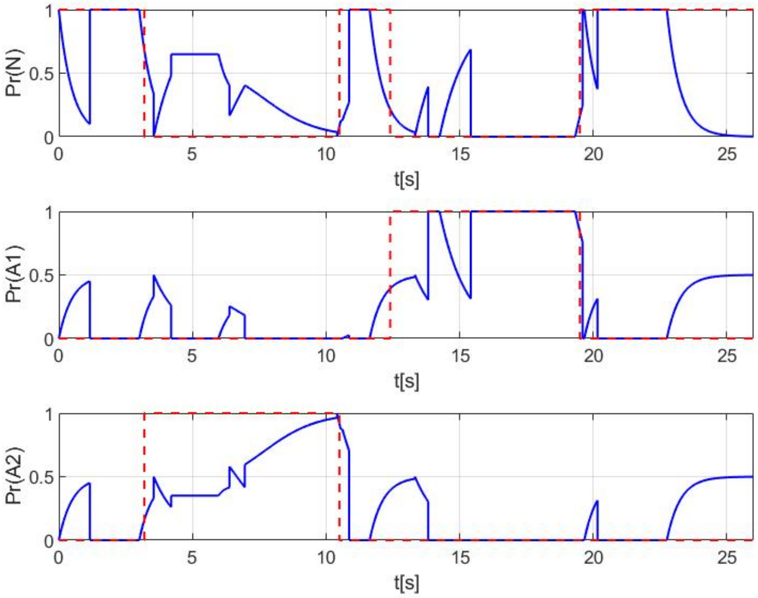

Figure 7: Probability to be in normal mode (top), attack A_1 (center) and attack A_2 (bottom).

attacks are detected with a probability higher than 0.5, but with some small delays. Attack A_1 is better detected than Attack A_2, at least for the proposed observation sequence. Observe that the confidence index in Fig. 8 decreases significantly within the interval of time [3, 8].

The logical observer of this system is computed for comparison purposes and reported in Fig. 10. With this observer, one can compute, for each new observation, the subset s_j, $j = 1, ..., 19$ of plant states x_i, $i = 1, ..., 9$, that are consistent with the sequence of untimed observations seen

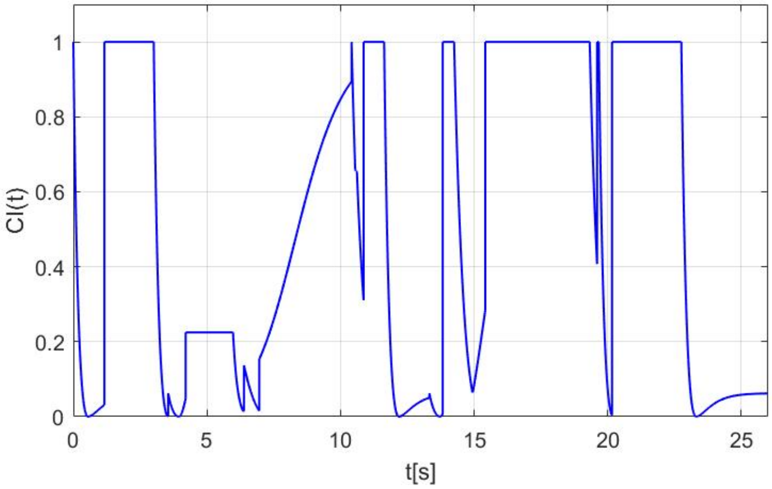

Figure 8: Confidence index.

thus far. Consequently, an estimation of the current mode is also possible with this observer (see Fig. 9 (center)). The logical observer detects the current mode $\mathcal{M}(t)$, when the subset s_j of plant states consistent with the observation of the system within $[0,t]$ satifies $s_j \subseteq \mathcal{M}(t)$ (here $\mathcal{M}(t)$ is considered as a property, and consequently as a subset of plant states). Otherwise, the logical observer returns a non detection (reported as "0" in Fig. 9 (center)). In particular, for the considered observation sequence, the logical observer is unable to detect attack A_2. To conclude, the logical observer experiences situations where it is unable to estimate the current mode, but does not lead to detection errors.

On the contrary, the detection strategy based on equation (9), always provides an estimation $M^*(t)$ of the current mode associated to a confidence index $CI(t)$. The estimation $M^*(t)$ is certainly correct (i.e., $M^*(t) = \mathcal{M}(t)$) as far as $Pr(M^*(t \mid \boldsymbol{\pi}(0), \sigma)) = 1$ (and these situations occur when the logical observer detects the current mode) but this estimation is no longer certain when $Pr(M^*(t \mid \boldsymbol{\pi}(0), \sigma)) < 1$ (and these situations occur when the logical observer returns a non detection of the mode). To conclude, the confidence index may be used to moderate the decisions of the probabilistic detection strategy and to reduce the detection error rate.

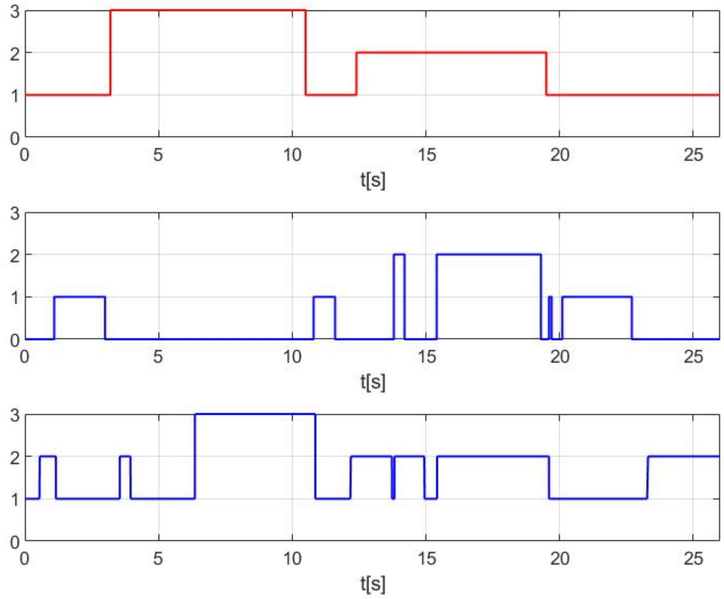

Figure 9: Mode detection with respect to time: true mode (top), with logical observer (center), with probabilistic detection (bottom). Here, "0" stands for not detected, "1" stands for $\mathcal{N}$, "2" stands for $\mathcal{A}_1$ and "3" stands for $\mathcal{A}_2$

5 Conclusion

This paper has proposed an approach to compute the probability vector of the states of a given LCTMM with respect to a sequence of observations. In a certain sense, such a vector can be viewed as a "probabilistic observer" that benefits from the timed observations generated by the plant and from the exponential dynamics of the LCTMM probabilities. At each instant, it provides not only the set of states consistent with a given sequence of observations but also the probability of each state in this set. The method has been applied to evaluate the probability, as a function of the time, that a given system is under cyber-attacks.

Future research directions for our work are twofold. From a methodological point of view, timed properties of the probabilistic observer will be used to investigate weak notions of detectability for labeled continuous-time Markov models in a formal way. From a practical point of view, we will be interested in establishing some average indicators for cyber-security performance characterization and in considering more general attack scenarios.

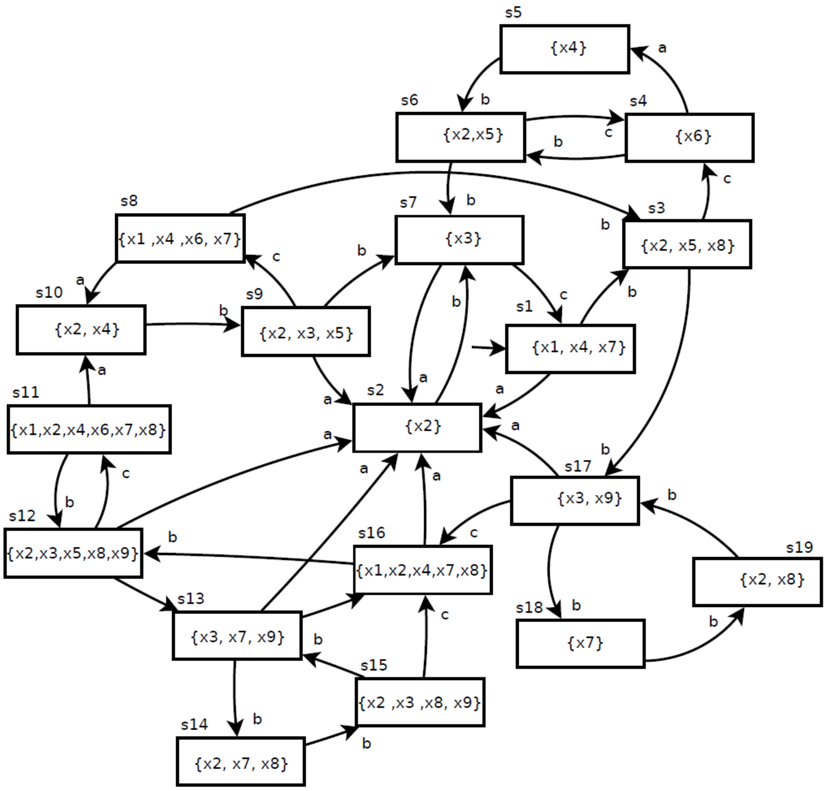

Figure 10: Logical observer for the system in Fig. 5.

References

[1] R. Alur and D. L. Dill, A theory of timed automata, *Theoretical Computer Science*, 126, pp. 183–235, 1994.

[2] B. Aspvall, M. F. Plass and R. E. Tarjan, A linear-time algorithm for testing the truth of certain quantified Boolean formulas, Information Processing Letters, vol. 8, no. 3, pp. 121–123,1979.

[3] A. A. Cardenas, S. Amin, and S. Sastry, Secure control: Towards survivable cyber-physical systems, Proc. IEEE Int. Conf. on Distributed Computing Systems, pp. 495–500, Beijing, P.R. China, 2008.

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

[5] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, Springer, 2008.

[6] D. Ding, Q. L. Han, Y. Xiang, X. Ge, and X. M. Zhang, A survey on security control and attack detection for industrial cyber-physical systems, Neurocomputing, 275, pp. 1674–1683, 2018.

[7] P. A. Gagniuc, *Markov Chains: From Theory to Implementation and Experimentation*, USA, NJ: John Wiley and Sons, 2017.

[8] C. Gao, C. Seatzu, Z. Li, and A. Giua, Multiple attacks detection on discrete event systems, Proc. IEEE International Conference on Systems, Man, and Cybernetics, pp. 2352–2357, Bari, Italy, 2019.

[9] 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, Proc. 25th IEEE Annual Conference on Emerging Technologies and Factory Automation, pp. 799–804, Vienna, Austria, 2020.

[10] R. Meira-Góes, E. Kang, R. Kwong and S. Lafortune, Stealthy deception attacks for cyber-physical systems, Proc. 56th IEEE Conference on Decision and Control, pp. 4224–4230, Melbourne, VIC, Australia, 2017.

[11] C. N. Hadjicostis and C. Seatzu, K-detectability in discrete event systems, Proc. 55th IEEE Conference on Decision and Control, pp. 420–425, Las Vegas, NV, 2016.

[12] C. N. Hadjicostis, *Estimation and Inference in Discrete Event Systems: A Model-Based Approach with Finite Automata*, Springer Nature, 2020.

[13] N. Hubballi, S. Biswas, S. Roopa, R. Ratti, and S. Nandi, LAN attack detection using discrete event systems, ISA Transactions, 50, pp. 119–130, 2011.

[14] S. Karlin and H. E. Taylor, *A First Course in Stochastic Processes*, Academic Press, 2012.

[15] C. Keroglou and C. N. Hadjicostis, Detectability in stochastic discrete event systems, Systems & Control Letters, 84, pp. 21–26, 2015.

[16] C. Keroglou and C. N. Hadjicostis, Verification of detectability in probabilistic finite automata, Automatica, 86, pp. 192–198, 2017.

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

[18] D. Lefebvre C. Seatzu, C. N. Hadjicostis, and A. Giua, Probabilistic verification of attack detection using logical observer, Proc. IFAC-WODES, Rio de Janeiro, Brazil, 2020.

[19] D. Lefebvre, C. N. Hadjicostis, Privacy and safety analysis of timed stochastic discrete event systems using Markovian trajectory-observers, Journal of Discrete Event Systems, 30(3), pp. 413–440, 2020.

[20] Y. Z. Lun, A. D'Innocenzo, F. Smarra, I. Malavolta, and M. D. Di Benedetto, State of the art of cyber-physical systems security: An automatic control perspective, The Journal of Systems and Software, 149, pp. 174–216, 2019.

[21] M. V. S. Alves and J. C. Basilio, State estimation and detectability of networked discrete event systems with multi-channel communication networks, Proc. American Control Conference, pp. 5602–5607, Philadelphia, PA, USA, 2019.

[22] R. Meira-Góes, R. Kwong and S. Lafortune, Synthesis of sensor deception attacks for systems modeled as probabilistic automata, Proc. American Control Conference, pp. 5620-5626, Philadelphia, PA, USA, 2019.

[23] J. R. Norris, *Markov Chains*, Cambridge Press, 1997.

[24] C. Perkinsa and G. Mullera, Using discrete event simulation to model attacker interactions with cyber and physical security systems, Procedia Computer Science, 61, pp. 221–226, 2015.

[25] L. R. Rabiner, A tutorial on Hidden Markov Models and selected applications in speech recognition, Proceedings of the IEEE, 77(2), pp. 257–286,1989.

[26] A. Rashidinejad, L. Y. Lin, B. Wetzels, Y. Zhu, M. Reniers, and R. Su, Supervisory control of discrete-event systems under attacks: An overview and outlook, Proc. European Control Conf., pp. 1732–1739, Naples, Italy, 2019.

[27] D. Shi, R. J. Elliott, T. Chen, Event-based state estimation of discrete-state hidden Markov models, Automatica, 65, pp. 12–26, 2016.

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

[29] S. Shu, F. Lin, H. Ying, and X. Chen, State estimation and detectability of probabilistic discrete event systems, Automatica, 44, pp. 3054–3060, 2008.

[30] S. Shu and F. Lin, Detectability of discrete event systems with dynamic event observation, Proc. Joint 48th IEEE Conference on Decision and Control and 28th Chinese Control Conference, pp. 187–192, Shanghai, P.R. China, 2009.

[31] S. Shu and F. Lin, I-detectability of discrete-event systems, IEEE Transactions on Automation Science and Engineering, 10(1), pp. 187–196, 2013.

[32] S. Shu, Delayed detectability of discrete event systems, IEEE Transactions on Automatic Control, 58(4), pp. 862–875, 2013.

[33] S. Shu, Z. Huang, and F. Lin, Online sensor activation for detectability of discrete event systems, IEEE Transactions on Automation Science and Engineering, 10(2), pp. 457–461, 2013.

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

[35] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, Attack models and scenarios for networked control systems, Proc. Int. Conf. on High Confidence Networked Systems, pp. 55–64, Beijing, P.R. China, 2012.

[36] D. Thorsley, Diagnosability of stochastic chemical kinetic systems: a discrete event systems approach, Proc. American Control Conference, pp. 2623–2630, Baltimore, Maryland, USA, 2010.

[37] D. Wang X. Wang, and Z. Li, State-based fault diagnosis of discrete-event systems with partially observable outputs Information Sciences, 529, pp. 87–100, 2020.

[38] Q. Zhang, Z. Li, C. Seatzu, and A. Giua, Stealthy attacks for partially-observed Discrete Event Systems, Proc. IEEE 23rd International Conference on Emerging Technologies and Factory Automation, pp. 1161–1164, Turin, Italy, 2018.

[39] K. Zhang and A. Giua, K-delayed strong detectability of discrete-event systems, Proc. 58th IEEE Conference on Decision and Control, pp. 7647–7652, Nice, France, 2019.

[40] P. Zhao, S. Shu, F. Lin, and B. Zhang, Detectability measure for state estimation of discrete event systems, IEEE Transactions on Automatic Control, 64(1), pp. 433–439, 2019.

[41] L. Zhou, S. Shu, and F. Lin, Detectability of discrete-event systems under nondeterministic observations, IEEE Transactions on Automation Science and Engineering, 18 (3), pp. 1315-1327, 2021.