Bożena Woźna-Szcześniak
Andrzej Zbrzezny

Checking EMTLK Properties of Timed Interpreted Systems Via Bounded Model Checking

Abstract. We investigate a SAT-based bounded model checking (BMC) method for EMTLK (the existential fragment of the metric temporal logic with knowledge) that is interpreted over timed models generated by timed interpreted systems. In particular, we translate the existential model checking problem for EMTLK to the existential model checking problem for a variant of linear temporal logic (called HLTLK), and we provide a SAT-based BMC technique for HLTLK. We evaluated the performance of our BMC by means of a variant of a timed generic pipeline paradigm scenario and a timed train controller system.

Keywords: Bounded Model Checking, Timed Interpreted Systems, Metric Temporal Logic with Knowledge.

1. Introduction

The formalism of *interpreted systems* (ISs) [9] was designed to model multi-agent systems (MASs) [21], and to reason about the agents' epistemic and temporal properties. The formalism of *timed interpreted systems* (TISs) extends ISs to make possible reasoning about real-time aspects of MASs. The TIS provides a computationally grounded semantics on which it is possible to interpret time-bounded temporal modalities as well as traditional epistemic modalities.

The transition system modelling the behaviour of TISs, which we call the *timed model*, comprises two kinds of transitions: *action transitions* that are labelled with timeless joint actions and that represent the discrete evolutions of TIS, and *time transitions* that are labelled with natural numbers and that correspond to the passage of time. Due to infinity of time, there are infinitely many time transitions.

The main idea of SAT-based bounded model checking (BMC) methods [7,19] consists in translating the existential model checking problem for a

Special Issue: Logical Aspects of Multi-Agent Systems
Edited by **Nils Bulling and Wiebe van der Hoek**

Studia Logica (2016) 104: 641–678
DOI: 10.1007/s11225-015-9637-9

modal language and for a transition system to the satisfiability problem of a propositional formula, and taking advantage of the power of modern SAT-solvers. The usefulness of SAT-based BMC for error tracking and complementarity to the BDD-based model checking have already been proven in several works, e.g. [6,17].

To describe the requirements of MASs various extensions of standard temporal logics [8] with epistemic [9], doxastic [13], and deontic (to represent correct functioning behaviour) [14] modalities have been proposed. In this paper we consider MTLK which is an epistemic extension of Metric Temporal Logic (MTL) [10] that cannot be translated into LTL (because of the considered semantics), and which allows for the representation of the quantitative temporal evolution of epistemic states of the agents. We interpret MTLK over discrete *timed models* generated by TISs.

Furthermore, note that both the MTL with discrete-time semantics and the S5 logic for knowledge have decidable model checking problems, [1] and [9], respectively. Since timed interpreted systems can be shown to be as expressive as the MTL-structure in [1], and the fusion between MTL and S5 for knowledge is a proper extension of MTL (which we call MTLK), it follows that problem of model checking for the full fusion is also decidable. This implies that the model checking of the existential fragment of MTLK (EMTLK) is also decidable, and thus BMC methods are worth exploring.

The original contributions of the paper are as follows. First of all, we define timed interpreted systems as a model of MASs where agents have real-time deadlines to achieve intended goals. We assume the synchronous semantics of TISs, thus the agents over this semantics perform a joint action at a given time in a global state. Secondly, we introduce two languages: MTLK and HLTLK—the *hard reset* linear time temporal epistemic logic. Finally, we define and implement a SAT-based BMC technique for TIS and for EMTLK. This BMC method consists of the following two steps, the formal description of which is provided in Sects. 3 and 4, respectively:

(a) A translation of the existential model checking problem for EMTLK and for TISs to the existential model checking problem for HLTLK and for an *augmented timed interpreted system* (ATIS). This translation is necessary because of the EMTLK semantics, which we use. Namely, this semantics is defined with respect to the Kripke model that has been defined for components having their clocks. The values of these clocks have an influence on interpretation of intervals associated to the temporal modalities, contrary to the step semantics, in which the interpretation of intervals takes into account only action steps, and thus the existential model checking problem for EMTLK can be translated into the existential model checking problem for LTLK.

(b) A definition of a SAT-based BMC algorithm for HLTLK and for ATIS.

The proposed SAT-based BMC method for EMTLK and for TISs is based on the BMC method for MTL and for discrete timed automata (DTA)[23]. The main differences between SAT-based BMC for MTL and for DTA, and the proposed SAT-based BMC for EMTLK and for TIS are the following. Firstly, EMTLK is an epistemic extension of MTL, thus the proposed method handles a more expressive language that allows to reason about not only temporal properties of MAS but also about the epistemic properties of MAS. Next, we assume the synchronous semantics of TISs, contrary to the asynchronous semantics of DTA (only one local or shared action may be performed by automata (agents) at a given time in a global state).

The rest of the paper is organised as follows. In Sect. 2 we introduce TIS, the MTLK logic, and its subset EMTLK. In Sect. 3 we show how to translate the existential model checking problem for EMTLK to the existential model checking problem for HLTLK. In Sect. 4 we provide a BMC method for HLTLK and for ATIS. In Sect. 5 we discuss our experimental results, and finally in Sect. 6 we conclude the paper.

2. Preliminaries

Let us start by fixing some notation used through the paper. $\mathbb{N}$ is the set of non-negative integers, $\mathbb{N}_+ = \mathbb{N}\setminus\{0\}$, and X is a finite set of non-negative integer variables, called *clocks*. A *clock valuation* is a function $v : X \to \mathbb{N}$ that assigns to each clock $x \in X$ a non-negative integer value $v(x)$. $\mathbb{N}^{|X|}$ is the set of all the clock valuations. For $X' \subseteq X$, the valuation $v' = v[X' := 0]$ is defined as: $\forall x \in X', v'(x) = 0$ and $\forall x \in X \setminus X', v'(x) = v(x)$. For $\delta \in \mathbb{N}, v + \delta$ denotes the valuation v' such that $\forall x \in \mathrm{X}, v'(x) = v(x) + \delta$.

Let $x \in X, c \in \mathbb{N}$, and $\sim \in \{\leq, <, =, >, \geq\}$. The set $\mathcal{C}(X)$ of *clock constraints* over X is defined by the following grammar: $\phi := x \sim c \mid \phi \wedge \phi$. Next, let v be a clock valuation and $\phi \in \mathcal{C}(X)$. The satisfaction relation $v \models \phi$ is defined inductively with the following rules: $v \models x \sim c$ iff $v(x) \sim c, v \models \phi \wedge \phi'$ iff $v \models \phi$ and $v \models \phi'$. Finally, let v be a clock valuation. The *time successor* of v (written *succ*(v)) is defined as follows: $\forall x \in X, v'(x) = v(x) + 1$.

2.1. Timed Interpreted Systems

Let $\mathbb{A} = \{1, \ldots, n\}$ denote the non-empty and finite set of agents, $\mathcal{E}$ be a special agent that is used to model the environment in which the agents operate, and let $\mathcal{PV} = \bigcup_{\mathbf{c}\in\mathbb{A}} \mathcal{PV}_{\mathbf{c}} \cup \mathcal{PV}_{\mathcal{E}}$ be a set of propositional variables such that $\mathcal{PV}_{\mathbf{c}_1} \cap \mathcal{PV}_{\mathbf{c}_2} = \emptyset$ for all $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{A} \cup \{\mathcal{E}\}$. The set of agents $\mathbb{A}$ constitute a multi-agent system (MAS). In the paper we use the *timed interpreted system* to model MAS. In this formalism, each agent $\mathbf{c} \in \mathbb{A}$ is modelled using a non-empty and finite set $L_{\mathbf{c}}$ of *local states*, a non-empty and finite set $Act_{\mathbf{c}}$ of *possible actions* such that the special *null* action $\epsilon_{\mathbf{c}}$ belongs to $Act_{\mathbf{c}}$ (it is assumed that actions are "public"), a non-empty and finite set $X_{\mathbf{c}}$ of *clocks*, a *protocol function* $P_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{Act_{\mathbf{c}}}$ that defines rules according to which actions may be performed in each local state, a (partial) *evolution function* $t_{\mathbf{c}} : L_{\mathbf{c}} \times L_{\mathcal{E}} \times \mathcal{C}(X_{\mathbf{c}}) \times 2^{X_{\mathbf{c}}} \times Act \to L_{\mathbf{c}}$ with $Act = \prod_{\mathbf{c}\in\mathbb{A}} Act_{\mathbf{c}} \times Act_{\mathcal{E}}$ (each element of Act and of $\mathcal{C}(X_{\mathbf{c}})$ is called a *joint action* and an *enabling condition*, respectively) which defines local transitions, a *valuation function* $\mathcal{V}_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{\mathcal{PV}_{\mathbf{c}}}$ which assigns to each local state a set of propositional variables that are assumed to be true at that state, and an *invariant function* $\mathcal{I}_{\mathbf{c}} : L_{\mathbf{c}} \to \mathcal{C}(X_{\mathbf{c}})$ which specifies the amount of time agent $\mathbf{c}$ may spend in its local states. We assume that if $\epsilon_{\mathbf{c}} \in P_{\mathbf{c}}(\ell_{\mathbf{c}})$, then $t_{\mathbf{c}}(\ell_{\mathbf{c}}, \ell_{\mathcal{E}}, \phi_{\mathbf{c}}, X, (a_1, \ldots, a_n, a_{\mathcal{E}})) = \ell_{\mathbf{c}}$ for $a_{\mathbf{c}} = \epsilon_{\mathbf{c}}$, any $\phi_{\mathbf{c}} \in \mathcal{C}(X_{\mathbf{c}})$, and any $X \in 2^{X_{\mathbf{c}}}$.

Similarly to the other agents, the environment $\mathcal{E}$ is modelled by a non-empty and finite set $L_{\mathcal{E}}$ of *local states*, a non-empty and finite set $Act_{\mathcal{E}}$ of *possible actions*, a non-empty and finite set $X_{\mathcal{E}}$ of *clocks*, a protocol function $P_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act_{\mathcal{E}}}$, a (partial) *evolution function* $t_{\mathcal{E}} : L_{\mathcal{E}} \times \mathcal{C}(X_{\mathcal{E}}) \times 2^{X_{\mathcal{E}}} \times Act \to L_{\mathcal{E}}$, a *valuation function* $\mathcal{V}_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{\mathcal{PV}_{\mathcal{E}}}$, and an *invariant function* $\mathcal{I}_{\mathcal{E}} : L_{\mathcal{E}} \to \mathcal{C}(X_{\mathcal{E}})$ which specifies the amount of time agent $\mathcal{E}$ may spend in its local states. It is assumed that local states, actions and clocks for $\mathcal{E}$ are "public".

For convenience, the symbol $S = \prod_{\mathbf{c}\in\mathbb{A}\cup\mathcal{E}} L_{\mathbf{c}} \times \mathbb{N}^{|X_{\mathbf{c}}|}$ denotes the non-empty set of all *global states*. Next, given a global state $s = ((\ell_1, v_1), \ldots, (\ell_n, v_n), (\ell_{\mathcal{E}}, v_{\mathcal{E}})) \in S$, the symbols $l_{\mathbf{c}}(s) = \ell_{\mathbf{c}}$ and $v_{\mathbf{c}}(s) = v_{\mathbf{c}}$ denote, respectively, the local component and the clock valuation of agent $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$ in the global state s. Finally, given a set of initial global states $\iota \subseteq S$ such that for all $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$ and for all $x \in X_{\mathbf{c}}$ it holds $v_{\mathbf{c}}(x) = 0$, a set of agents $\mathbb{A}$ and an environment $\mathcal{E}$, a *timed interpreted system* (TIS) as a tuple $\mathbb{I} = (\{L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c}\in\mathbb{A}\cup\{\mathcal{E}\}}, \iota)$.

For a given time interpreted system $\mathbb{I}$ we define a *timed model* as a tuple $M = (\Sigma, \iota, S, T, \mathcal{V})$, where $\Sigma = Act \cup \mathbb{N}$ is the set of labels (i.e., joint actions and natural numbers), S is the set of all possible global states as defined above, $\mathcal{V} : S \to 2^{\mathcal{PV}}$ is the valuation function defined as $\mathcal{V}(s) = \bigcup_{\mathbf{c}\in\mathbb{A}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$, and $T \subseteq S \times \Sigma \times S$ is a transition relation defined by action and time transitions:

1. Action transition: for any $\overline{a} \in Act, (s, \overline{a}, s') \in T$ iff for all $\mathbf{c} \in \mathbb{A}$, there exists a local transition $t_{\mathbf{c}}(l_{\mathbf{c}}(s), l_{\mathcal{E}}(s), \phi_{\mathbf{c}}, X', \overline{a}) = l_{\mathbf{c}}(s')$ such that $v_{\mathbf{c}}(s) \models \phi_{\mathbf{c}} \wedge \mathcal{I}(l_{\mathbf{c}}(s))$ and $v'_{\mathbf{c}}(s') = v_{\mathbf{c}}(s)[X' := 0]$ and $v'_{\mathbf{c}}(s') \models \mathcal{I}(l_{\mathbf{c}}(s'))$, and there exists a local transition $t_{\mathcal{E}}(l_{\mathcal{E}}(s), \phi_{\mathcal{E}}, X', \overline{a}) = l_{\mathcal{E}}(s')$ such that $v_{\mathcal{E}}(s) \models \phi_{\mathcal{E}} \wedge \mathcal{I}(l_{\mathcal{E}}(s))$ and $v'_{\mathcal{E}}(s') = v_{\mathcal{E}}(s)[X' := 0]$ and $v'_{\mathcal{E}}(s') \models \mathcal{I}(l_{\mathcal{E}}(s'))$.
2. Time transition: let $\delta \in \mathbb{N}, (s, \delta, s') \in T$ iff for all $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}, l_{\mathbf{c}}(s) = l_{\mathbf{c}}(s')$ and $v_{\mathbf{c}}(s) \models \mathcal{I}(l_{\mathbf{c}}(s))$ and $v'_{\mathbf{c}}(s') = v_{\mathbf{c}}(s) + \delta$ and $v'_{\mathbf{c}}(s') \models \mathcal{I}(l_{\mathbf{c}}(s))$.

We assume that the relation T is total, i.e. for any $s \in S$ there exists $s' \in S$ and there exist either a non-empty joint action $\overline{a} \in Act$ or natural number $\delta \in \mathbb{N}$ such that it holds $T(s, \overline{a}, s')$ or $T(s, \delta, s')$.

Given a timed interpreted system and an agent $\mathbf{c} \in \mathbb{A}$, the *indistinguishability* relation $\sim_{\mathbf{c}} \subseteq S \times S$ is defined as follows: $s \sim_{\mathbf{c}} s'$ iff $l_{\mathbf{c}}(s') = l_{\mathbf{c}}(s)$ and $v_{\mathbf{c}}(s') = v_{\mathbf{c}}(s)$. Moreover, hereafter we assume the following definitions of epistemic relations: $\sim^E_\Gamma \overset{def}{=} \bigcup_{\mathbf{c} \in \Gamma} \sim_{\mathbf{c}}, \sim^C_\Gamma \overset{def}{=} (\sim^E_\Gamma)^+$ (the transitive closure of $\sim^E_\Gamma$), $\sim^D_\Gamma \overset{def}{=} \bigcap_{\mathbf{c} \in \Gamma} \sim_{\mathbf{c}}$, where $\Gamma \subseteq \mathbb{A}$.

2.2. Runs and Discrete Paths

Let M be a timed model generated by TIS. An infinite sequence $\rho = s_0 \overset{\delta_0, \overline{a}_0}{\longrightarrow} s_1 \overset{\delta_1, \overline{a}_1}{\longrightarrow} s_2 \overset{\delta_2, \overline{a}_2}{\longrightarrow} \ldots$ of global states is called a *run* originating at s_0 if there is a sequence of transitions from s_0 onwards such that for every $i \in \mathbb{N}, s_i \in S, \overline{a}_i \in Act, \delta_i \in \mathbb{N}_+$, and there exists $s'_i \in S$ such that $(s_i, \delta, s'_i) \in T$ and $(s'_i, \overline{a}, s_{i+1}) \in T$. Notice that the definition of the run does not permit two consecutive joint actions to be performed one after the other, i.e., between each two joint actions some time must pass; such a run is called *strongly monotonic.*

Let $\Omega_0 = [b_0, b_1), \Omega_1 = [b_1, b_2), \ldots$ be the sequence of pairwise disjoint intervals, where: $b_0 = 0$ and $b_i = b_{i-1} + \delta_{i-1}$ if $i > 0$. For each $t \in \mathbb{N}$, let $idx_\rho(t)$ denote the unique index i such that $t \in \Omega_i$. A *discrete path* (or *path*) λ_ρ *corresponding to* ρ is a mapping $\lambda_\rho : \mathbb{N} \to S$ such that $\lambda_\rho(t) = ((\ell^i_1, v^i_1 + t - b_i), \ldots, (\ell^i_n, v^i_n + t - b_i), (\ell^i_{\mathcal{E}}, v^i_{\mathcal{E}} + t - b_i)) = s_i + t - b_i$, where $i = idx_\rho(t)$. Given $t \in \mathbb{N}$, the suffix λ^t_ρ of a path λ_ρ at time t is a path defined as: $\forall i \in \mathbb{N}, \lambda^t_\rho(i) = \lambda_\rho(t + i)$.

Observe that because of the assumption that the runs are strongly monotonic, the definition of the discrete path is done in a unique way.

Example 2.1. Assume the following run: $\rho = s_0 \overset{1, \overline{a}_0}{\longrightarrow} s_1 \overset{3, \overline{a}_1}{\longrightarrow} s_2 \overset{2, \overline{a}_2}{\longrightarrow} s_3 \overset{3, \overline{a}_2}{\longrightarrow} \ldots$. Then, we have: $\Omega_0 = [0, 1), \Omega_1 = [1, 4), \Omega_2 = [4, 6), \Omega_3 = [6, 9), \ldots$. Next, we have: $idx_\rho(0) = 0$ since $0 \in \Omega_0, idx_\rho(1) = 1$ since $1 \in \Omega_1, idx_\rho(2) = 1$

since $2 \in \Omega_1, idx_\rho(3) = 1$ since $3 \in \Omega_1, idx_\rho(4) = 2$ since $4 \in \Omega_2, idx_\rho(5) = 2$ since $5 \in \Omega_2, idx_\rho(6) = 3$ since $6 \in \Omega_3, idx_\rho(7) = 3$ since $7 \in \Omega_3, idx_\rho(8) = 3$ since $8 \in \Omega_3$, etc. Finally, we get the following discrete path λ_ρ corresponding to run ρ: $\lambda_\rho(0) = s_0, \lambda_\rho(1) = s_1, \lambda_\rho(2) = s_1 + 1, \lambda_\rho(3) = s_1 + 2, \lambda_\rho(4) = s_2, \lambda_\rho(5) = s_2 + 1, \lambda_\rho(6) = s_3, \lambda_\rho(7) = s_3 + 1, \lambda_\rho(8) = s_3 + 2$, etc.

The set of all the paths originating from $s \in S$ is denoted by $\Pi(s)$. The set of all the paths originating from all initial states in S is defined as $\Pi = \bigcup_{s^0 \in \iota} \Pi(s^0)$.

2.3. Examples of MASs and Their Models

In the section we present MASs modelled by means of timed interpreted systems. We utilize the systems to assess the bounded model checking methods considered in the paper. In what follows we denote by $\overline{\epsilon}$ the joint null action, i.e., the action composed of the null actions only.

2.3.1. Timed Generic Pipeline Paradigm (TGPP). The TGPP (adapted from [18]) consists of $n + 2$ agents: Producer P that is able to produce data ($ProdReady$) within certain time interval $[a, b]$ or being inactive ($ProdSend$), Consumer C that is able to receive data ($ConsReady$) within certain time interval $[c, d]$, to consume data ($ConsFree$) within certain time interval $[g, h]$ or being inactive ($ConsStart$), a chain of n intermediate Nodes N_i which can be ready for receiving data ($Node_iReady$) within certain time interval $[c, d]$, processing data ($Node_iProc$) within certain time interval $[e, f]$, sending data ($Node_iSend$), or being inactive ($Node_iStart$), and the environment $\mathcal{E}$. The local states, the possible local actions, the local clocks, the clock constraints, invariants and the local protocol for each agent, but for the environment $\mathcal{E}$ are shown in Figure 1. Null actions are omitted in the figure. For environment $\mathcal{E}$, to simplify the presentation, we shall consider just one local state: $L_\mathcal{E} = \{\cdot\}$. The set of actions for $\mathcal{E}$ is $Act_\mathcal{E} = \{\epsilon_\mathcal{E}\}$. The local protocols of $\mathcal{E}$ is the following: $P_\mathcal{E}(\cdot) = Act_\mathcal{E}$. The set of clocks of $\mathcal{E}$ is empty, and the invariant function is $\mathcal{I}_\mathcal{E}(\cdot) = \emptyset$.

From Figure 1 we can easily deduce the local evolution functions of each agent. As an example, we show the definition of the local evolution function of Producer P. The remaining ones are equally straightforward.

Let $state$ denote a local state of Producer P, and $Act = Act_P \times \prod_{i=1}^{n} Act_{Ni} \times Act_C \times Act_\mathcal{E}$ with $Act_P = \{Produce, Send_1, \epsilon_P\}, Act_C = \{Start_{n+1}, Send_{n+1}, Consume, \epsilon_C\}, Act_{Ni} = \{Start_i, Send_i, Send_{i+1}, \epsilon_{Ni}, Proc_i\}$, and $Act_\mathcal{E} = \{\epsilon_\mathcal{E}\}$. Moreover, let $\overline{a} \in Act$, and $act_P(\overline{a}), act_{N_i}(\overline{a})$, $act_C(\overline{a})$ and $act_\mathcal{E}(\overline{a})$, respectively, denote an action of Producer P, Node

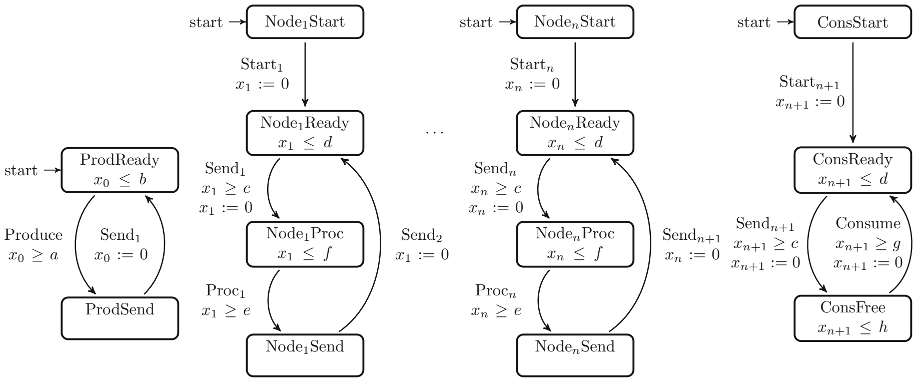

Figure 1. A TGPP scenario

N_i, Consumer C and environment $\mathcal{E}$. The local evaluation function of Producer P is the following:

- $t_P(state, \cdot, true, \emptyset, \overline{a}) = state$ if $\overline{a} \neq \overline{\epsilon}$ and $act_P(\overline{a}) = \epsilon_P$
- $t_P(ProdReady, \cdot, x_0 > a, \emptyset, \overline{a}) = ProdSend$ if $act_P(\overline{a}) = Produce$
- $t_P(ProdSend, \cdot, true, \{x_0\}, \overline{a}) = ProdReady$ if $act_P(\overline{a}) = Send_1$ and $act_{N1}(\overline{a}) = Send_1$

We can define the set of possible global states S for the scenario as the product $(L_P \times \mathbb{N}) \times \prod_{i=1}^{n}(L_{N_i} \times \mathbb{N}) \times (L_C \times \mathbb{N}) \times L_{\mathcal{E}}$, and we consider the following set of initial states $\iota = \{s^0\}$, where $s^0 = ((ProdReady, 0), (Node_1Start, 0), \ldots, (Node_nStarts, 0), (ConsStart, 0), (\cdot))$.

The example can be scaled by adding Nodes, or by changing the length of intervals (i.e., the parameters a, b, c, d, e, f, g, h) that are used to adjust the time properties of Producer P, Consumer C, and Nodes N_i $(i = 1, .., n)$.

It should be straightforward to infer the timed model that is induced by the above description of the TGPP scenario. Next, in the timed model of the scenario we assume the following set of proposition variables: $\mathcal{PV} = \{ProdSend, ConsReady, ConsFree\}$, and the following definition of valuation functions for agents the Producer and the Consumer:

- $\mathcal{V}_P(ProdSend) = ProdSend,$
- $\mathcal{V}_C(ConsReady) = ConsReady, \mathcal{V}_C(ConsFree) = ConsFree.$

2.3.2. A Timed Train Controller System (TTCS). The TTCS (adapted from [20]) consists of n (for $n \geq 2$) trains $T_1, \ldots, T_n$, each one using its own

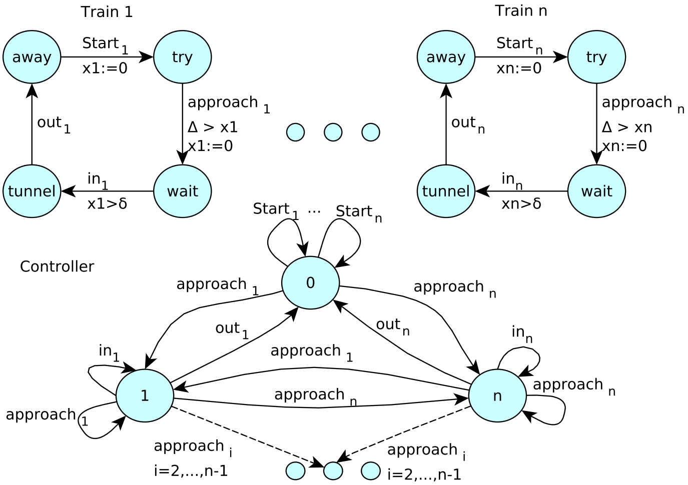

Figure 2. A timed train controller system

circular track for travelling in one direction and containing its own clock y_i, together with controller C used to coordinate the access of trains to the tunnel through all trains have to pass at certain point, and the environment $\mathcal{E}$. Because there is only one track in the tunnel, trains arriving from each direction cannot use it simultaneously. There are signals on both sides of the tunnel, which can be either red or green. All trains notify the controller when they request entry to the tunnel or when they leave the tunnel. The controller controls the colour of the displayed signal, and the behaviour of the scenario depends on the values δ and Δ ($\Delta > \delta + 3$ makes it incorrect - the mutual exclusion does not hold).

Figure 2 shows the local states, the possible local actions, the local clocks, the clock constraints, invariants, and the local protocol for each agent, but for the environment $\mathcal{E}$. Null actions are omitted in the figure. Being at state *away*, train T_i may express its will to enter the tunnel, provided that the value of controller C is zero (i.e., no other train has already done the same). It then advances to state *try*, where it delays for an arbitrary amount of time, less than Δ time units, before setting C to i. From there on, it is ready to enter the tunnel; however, a minimum amount of time δ is necessary for this. Upon leaving the tunnel, the train sets C to state 0.

Controller C has $n+1$ states, denoting that all trains are *away* (state 0), and the numbers of trains, i.e., $1, \ldots, n$. Controller C is initially at state 0. It moves to state i, if it is notified by train T_i. Being at state i, it can either move to state 0, or "jump" to state j when notified by train T_j.

The action $Start_i$ of train T_i denotes the passage from state *away* to the state where the train wishes to obtain access to the tunnel. As it has been already said, this is allowed only if controller C is in state 0. The restriction is ensured by the fact that train T_i synchronises with controller C on action $Start_i$, and the latter is enabled only from state 0 of C. Similarly, train T_i synchronizes with controller C on action $approach_i$, which denotes setting C to state i, as well as out_i, which denotes setting C to state 0. Finally, action in_i denotes the entering of train T_i into the tunnel.

For environment $\mathcal{E}$, to simplify the presentation, we shall consider just one local state: $L_{\mathcal{E}} = \{\cdot\}$. The set of actions for $\mathcal{E}$ is $Act_{\mathcal{E}} = \{\epsilon_{\mathcal{E}}\}$. The local protocol of $\mathcal{E}$ is the following: $P_{\mathcal{E}}(\cdot) = Act_{\mathcal{E}}$. The set of clocks of $\mathcal{E}$ is empty, and the invariant function is $\mathcal{I}_{\mathcal{E}}(\cdot) = \emptyset$.

From Figure 2 we can easily deduce the local evolution functions of each agent. As an example, we show the definition of the local evolution function of train T_1. The remaining ones are equally straightforward.

Let *state* denote a local state of train T_1, and $Act = \prod_{i=1}^{n} Act_{T_i} \times Act_C \times Act_{\mathcal{E}}$ with $Act_C = \{Start_i, approach_i, out_i, in_i, \epsilon_C \mid i = 1,..,n\}, Act_{T_i} = \{Start_i, approach_i, out_i, in_i, \epsilon_{Ti}\}$, and $Act_{\mathcal{E}} = \{\epsilon_{\mathcal{E}}\}$. Moreover, let $\overline{a} \in Act$, and $act_{T_i}(\overline{a}), act_C(\overline{a})$ and $act_{\mathcal{E}}(\overline{a})$, respectively, denote an action of the $i-$th train, the controller, and the environment. The local evaluation function of train T_1 is the following:

- $t_{T_1}(state, \cdot, true, \emptyset, \overline{a}) = state$, if $\overline{a} \neq \overline{\epsilon}$ and $act_{T_1}(\overline{a}) = \epsilon_{T_1}$.
- $t_{T_1}(away, \cdot, true, \{x_1\}, \overline{a}) = try$, if $act_{T_1}(\overline{a}) = act_C(\overline{a}) = Start_1$.
- $t_{T_1}(try, \cdot, x_1 < \Delta, \{x_1\}, \overline{a}) = wait$, if $act_{T_1}(\overline{a}) = act_C(\overline{a}) = approach_1$.
- $t_{T_1}(wait, \cdot, x_1 > \delta, \emptyset, \overline{a}) = tunnel$, if $act_{T_1}(\overline{a}) = act_C(\overline{a}) = in_1$.
- $t_{T_1}(tunnel, \cdot, true, \emptyset, \overline{a}) = away$, if $act_{T_1}(\overline{a}) = act_C(\overline{a}) = out_1$.

We can define the set of possible global states S for the scenario as the product $\prod_{i=1}^{n}(L_{T_i} \times \mathbb{N}) \times L_C \times L_{\mathcal{E}}$, and we consider the following set of initial states $\iota = \{s^0\}$, where $s^0 = ((away, 0), \ldots, (away, 0), 0, \cdot)$.

The example can be scaled by adding trains, or the time-delay constants δ and Δ. It should be noted that the preservation of *the mutual exclusion property* (i.e., the property ensuring that no two trains are in the tunnel at the same time) depends on the relative values of the time-delay constants δ and Δ. In particular, the following holds: *"A timed train controller system ensures mutual exclusion iff* $\Delta \leq \delta + 3$*"*.

It should be straightforward to infer the timed model that is induced by the above description of the TTCS scenario. Next, in the timed model of the scenario we assume the following set of proposition variables: $\mathcal{PV} = \{tunnel_i \mid i = 1,..,n\}$, and the following definition of valuation functions for trains: $\mathcal{V}_{T_i}(tunnel) = tunnel_i$, for $i = 1,..,n$.

2.4. MTLK

Let $p \in \mathcal{PV}, \mathbf{c} \in \mathbb{A}, \Gamma \subseteq \mathbb{A}$, and I be an interval in $\mathbb{N}$ of the form: $[a, b)$ or $[a, \infty)$, for $a, b \in \mathbb{N}$ and $a \neq b$. Metric temporal logic with knowledge (MTLK) in negation normal form is defined by the following grammar:

$$\begin{aligned}\varphi := \top \mid \bot \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \mathrm{U}_I \varphi \mid \mathrm{G}_I \varphi \\ \mid \mathrm{K}_{\mathbf{c}}\varphi \mid \overline{\mathrm{K}}_{\mathbf{c}}\varphi \mid \mathrm{E}_\Gamma\varphi \mid \overline{\mathrm{E}}_\Gamma\varphi \mid \mathrm{D}_\Gamma\varphi \mid \overline{\mathrm{D}}_\Gamma\varphi \mid \mathrm{C}_\Gamma\varphi \mid \overline{\mathrm{C}}_\Gamma\varphi\end{aligned}$$

The temporal modalities U_I and G_I are named as *bounded until* and *bounded globally*, respectively. The derived basic temporal modalities for *bounded eventually* and *bounded release* are defined as follows: $\mathrm{F}_I\varphi \overset{def}{=} \top \mathrm{U}_I \varphi$ and $\varphi \mathrm{R}_I \psi \overset{def}{=} \psi \mathrm{U}_I(\psi \wedge \varphi) \vee \mathrm{G}_I\psi$. Hereafter, if the interval I is of the form $[0, \infty)$, then we omit it for the simplicity of the presentation. The epistemic operator $\mathrm{K}_{\mathbf{c}}$ represents "agent $\mathbf{c}$ knows", while the operator $\overline{\mathrm{K}}_{\mathbf{c}}$ is the corresponding dual one representing "agent $\mathbf{c}$ considers possible". The epistemic operators D_Γ , E_Γ and C_Γ represent distributed knowledge in the group Γ, "everyone in Γ knows", and common knowledge among agents in Γ, respectively. The epistemic operators $\overline{\mathrm{D}}_\Gamma$, $\overline{\mathrm{E}}_\Gamma$ and $\overline{\mathrm{C}}_\Gamma$ are the corresponding dual ones.

EMTLK is the existential fragment of MTLK, defined as:

$$\varphi := \top \mid \bot \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \mathrm{U}_I \varphi \mid \mathrm{G}_I \varphi \mid \overline{\mathrm{K}}_{\mathbf{c}}\varphi \mid \overline{\mathrm{E}}_\Gamma\varphi \mid \overline{\mathrm{D}}_\Gamma\varphi \mid \overline{\mathrm{C}}_\Gamma\varphi$$

Observe that we assume that MTLK (and so EMTLK) formulae are given in the negation normal form, in which the negation can be only applied to propositional variables. Moreover, EMTLK is existential only w.r.t. the epistemic modalities.

Turning to semantics, MTLK formulae are interpreted on timed models. Let $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$. The *satisfiability* relation $\models$, which indicates truth of a MTLK formula in the timed model M along a path λ_ρ at time t, is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

- $M, \lambda_\rho^t \models \alpha \mathrm{U}_I \beta$ iff $(\exists i \in I)(M, \lambda_\rho^{t+i} \models \beta$ and $(\forall 0 \leq j < i)\ M, \lambda_\rho^{t+j} \models \alpha)$
- $M, \lambda_\rho^t \models \mathrm{G}_I \alpha$ iff $(\forall i \in I)(M, \lambda_\rho^{t+i} \models \alpha)$
- $M, \lambda_\rho^t \models \mathrm{K}_{\mathbf{c}} \alpha$ iff $(\forall \pi \in \Pi)(\forall i \geq 0)(\pi(i) \sim_{\mathbf{c}} \lambda_\rho(t)$ implies $M, \pi^i \models \alpha)$

- $M, \lambda_\rho^t \models \overline{\mathrm{K}}_{\mathbf{c}}\alpha$ iff $(\exists \pi \in \Pi)(\exists i \geq 0)(\pi(i) \sim_{\mathbf{c}} \lambda_\rho(t)$ and $M, \pi^i \models \alpha)$
- $M, \lambda_\rho^t \models Y_\Gamma\alpha$ iff $(\forall \pi \in \Pi)(\forall i \geq 0)(\pi(i) \sim_\Gamma^Y \lambda_\rho(t)$ implies $M, \pi^i \models \alpha)$
- $M, \lambda_\rho^t \models \overline{Y}_\Gamma\alpha$ iff $(\exists \pi \in \Pi)(\exists i \geq 0)(\pi(i) \sim_\Gamma^Y \lambda_\rho(t)$ and $M, \pi^i \models \alpha)$

The MTLK formula φ *holds* in the model M (denoted $M \models^\forall \varphi$) iff $M, \lambda_\rho^0 \models \varphi$ for all paths $\lambda_\rho \in \Pi$. The EMTLK formula φ *holds* in the timed model M (denoted $M \models \varphi$) iff $M, \lambda_\rho^0 \models \varphi$ for some path $\lambda_\rho \in \Pi$.

Example 2.2. Consider TTCS described in Sect. 2.3.2 for two trains T_1 and $T_2, \Delta = 5$ and $\delta = 1$ (the mutual exclusion does not hold), the EMTLK formula $\varphi = \mathrm{F}_{[0,9)}(tunnel_1 \wedge tunnel_2)$, and the run ρ with the following prefix:

$$((away, 0), (away, 0), 0, \cdot) \overset{1,(\epsilon_{T_1}, Start_2, Start_2, \epsilon_{\mathcal{E}})}{\longrightarrow}$$
$$((away, 1), (try, 0), 0, \cdot) \overset{1,(Start_1, \epsilon_{T_2}, Start_1, \epsilon_{\mathcal{E}})}{\longrightarrow}$$
$$((try, 0), (try, 1), 0, \cdot) \overset{1,(\epsilon_{T_1}, approach_2, approach_2, \epsilon_{\mathcal{E}})}{\longrightarrow}$$
$$((try, 1), (wait, 0), 2, \cdot) \overset{2,(\epsilon_{T_1}, in_2, in_2, \epsilon_{\mathcal{E}})}{\longrightarrow}$$
$$((try, 3), (tunnel, 2), 2, \cdot) \overset{1,(approach_1, \epsilon_{T_2}, approach_1, \epsilon_{\mathcal{E}})}{\longrightarrow}$$
$$((wait, 0), (tunnel, 3), 1, \cdot) \overset{2,(in_1, \epsilon_{T_2}, in_1, \epsilon_{\mathcal{E}})}{\longrightarrow}$$
$$((tunnel, 2), (tunnel, 5), 1, \cdot) \overset{\dots}{\longrightarrow}$$

The corresponding path λ_ρ is constructed as follows. First, we take $\Omega_0 = [0, 1), \Omega_1 = [1, 2), \Omega_2 = [2, 3), \Omega_3 = [3, 5), \Omega_4 = [5, 6), \Omega_5 = [6, 8), \dots$. Next, we have: $idx_\rho(0) = 0$ since $0 \in \Omega_0, idx_\rho(1) = 1$ since $1 \in \Omega_1, idx_\rho(2) = 2$ since $2 \in \Omega_2, idx_\rho(3) = 3$ since $3 \in \Omega_3, idx_\rho(4) = 3$ since $4 \in \Omega_3, idx_\rho(5) = 4$ since $5 \in \Omega_4, idx_\rho(6) = 5$ since $6 \in \Omega_5, idx_\rho(7) = 5$ since $7 \in \Omega_5, idx_\rho(8) = 6$ since $8 \in \Omega_6$ etc. Finally, we get the following discrete path λ_ρ corresponding to run ρ:

$$\lambda_\rho(0) = (away, 0), (away, 0), 0, \cdot), \lambda_\rho(1) = ((away, 1), (try, 0), 0, \cdot),$$
$$\lambda_\rho(2) = ((try, 0), (try, 1), 0, \cdot), \lambda_\rho(3) = ((try, 1), (wait, 0), 2, \cdot),$$
$$\lambda_\rho(4) = ((try, 2), (wait, 1), 2, \cdot), \lambda_\rho(5) = ((try, 3), (tunnel, 2), 2, \cdot),$$
$$\lambda_\rho(6) = ((wait, 0), (tunnel, 3), 1, \cdot), \lambda_\rho(7) = ((wait, 1), (tunnel, 4), 1, \cdot),$$
$$\lambda_\rho(8) = ((tunnel, 2), (tunnel, 5), 1, \cdot), etc.$$

Let M be the timed model of TTCS. Observe that the following is true: $tunnel_1 \in \mathcal{V}(\lambda_\rho(8))$ and $tunnel_2 \in \mathcal{V}(\lambda_\rho(8))$. Therefore, we have $M, \lambda_\rho^8 \models$

$tunnel_1 \wedge tunnel_2$. This implies that $M, \lambda_\rho^0 \models \mathrm{F}_{[0,9)}(tunnel_1 \wedge tunnel_2)$ is valid.

Determining whether a MTLK formula φ is existentially (resp. universally) valid in a timed model M is called an *existential* (resp. *universal*) *model checking problem*. In other words, the universal model checking problem asks whether $M \models^\forall \varphi$ and the existential model checking problem asks whether $M \models \varphi$.

To solve the universal model checking problem, one can negate the formula and demonstrate that the existential model checking problem for the negated formula has no solution. Intuitively, we are trying to discover a counterexample, and if we do not find it, then the formula is universally valid. Now, since *bounded model checking* is designed for finding a solution to an existential model checking problem, in the paper we only consider the EMTLK properties. This is because looking for a counterexample, for example, to $M \models^\forall \mathrm{F}_{[0,10)}\mathrm{K}_{\mathbf{c}}p$ corresponds to the query whether there exists a witness $M \models \mathrm{G}_{[0,10)}\overline{\mathrm{K}}_{\mathbf{c}}\neg p$.

3. From EMTLK to HLTLK

The translation of the existential model checking problem for EMTLK to the existential model checking problem for HLTLK, a language defined below and interpreted over an *abstract model* for an *augmented timed interpreted system* is based on [22], where the translation of the existential model checking problem for Metric Interval Temporal Logic (MITL) [2] with a dense-time and interleaving semantics defined over timed automata to the existential model checking problem for HLTL with an interleaving semantics defined over the region graph has been introduced.

The reason for redefining the translation of [22] in the discrete-time context, and for extending it to the full MTL with epistemic components is the following. First of all the discrete time semantics is interesting by itself. Secondly, we can take advantage of the finite-state nature of discrete time and apply techniques which cannot be applied directly to dense time. Namely, in our case we can apply the BMC technique directly to the proposed abstract model. In the case of the dense semantics this step is impossible, since we need to discretise the proposed abstract model before we can apply the BMC technique. Moreover, the discretisation process requires additional theoretical background that will show that the used discretisation preserves considered logic.

We begin the section by introducing the definitions of the augmented timed interpreted system, its abstract model, and paths in this model. Then, we define the HLTLK language. Next, we show how to translate an EMTLK formula φ into a HLTLK formula $\mathcal{H}(\varphi)$, and finally we prove the correctness and completeness of the proposed translation.

3.1. An Augmented Timed Interpreted System

Let $\mathbb{I} = (\{L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c}\in\mathbb{A}\cup\{\mathcal{E}\}}, \iota)$ be a timed interpreted system, φ an EMTLK formula, and m the number of intervals appearing in φ. An *augmented timed interpreted system* (ATIS) is defined as a tuple
$\mathbb{I}_\varphi = (\{L_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}\}_{\mathbf{c}\in\mathbb{A}\cup\{\mathcal{E}\}}, \{Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}\}_{\mathbf{c}\in\mathbb{A}}, Act'_{\mathcal{E}}, X'_{\mathcal{E}}, P'_{\mathcal{E}}, t'_{\mathcal{E}}, \iota')$ with:

- $X'_{\mathcal{E}} = X_{\mathcal{E}} \cup Y$, where $Y = \{y_1, \ldots, y_m\}$ is a set of new clocks that corresponds to all the time intervals appearing in φ; one clock y_i per one time interval. Each clock y_i measures the passage of time for the i-th interval.
- $Act'_{\mathcal{E}} = Act_{\mathcal{E}} \cup (2^Y \setminus \{\emptyset\})$.
- $P'_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act'_{\mathcal{E}}}$ is an extension of the protocol function $P_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act_{\mathcal{E}}}$ such that $(2^Y \setminus \{\emptyset\}) \subseteq P'_{\mathcal{E}}(\ell)$ for all $\ell \in L_{\mathcal{E}}$.
- $t'_{\mathcal{E}} : L_{\mathcal{E}} \times \mathcal{C}(X'_{\mathcal{E}}) \times 2^{X'_{\mathcal{E}}} \times Act' \to L_{\mathcal{E}}$ is an extension of $t_{\mathcal{E}}$ such that $Act' = \prod_{i=1}^{n} Act_i \times Act'_{\mathcal{E}}$ and $t'_{\mathcal{E}}(\ell_{\mathcal{E}}, true, B, (\epsilon_1, \ldots, \epsilon_n, B)) = \ell_{\mathcal{E}}$ for all $B \in 2^Y$ and $B \neq \emptyset$.
- $\iota' \subseteq S_\varphi$ (with $S_\varphi = \prod_{\mathbf{c}\in\mathbb{A}} L_{\mathbf{c}} \times \mathbb{N}^{|X_{\mathbf{c}}|} \times L_{\mathcal{E}} \times \mathbb{N}^{|X'_{\mathbf{c}}|}$) such that for all $\mathbf{c} \in \mathbb{A}$ and for all $x \in X_{\mathbf{c}}$ it holds $v_{\mathbf{c}}(x) = 0$, and for all $x \in X'_{\mathcal{E}}$ it holds $v_{\mathcal{E}}(x) = 0$.

Example 3.1. Consider TTCS described in Sect. 2.3.2. In the TIS model of the system the environment $\mathcal{E}$ is modelled as follows. The set of local states is $L_{\mathcal{E}} = \{\cdot\}$, the set of local action is $Act_{\mathcal{E}} = \{\epsilon_{\mathcal{E}}\}$, the set of clocks is $X_{\mathcal{E}} = \emptyset$, the local protocol is: $P_{\mathcal{E}}(\cdot) = Act_{\mathcal{E}}$, the local valuation function is: $\mathcal{V}_{\mathcal{E}}(\cdot) = \emptyset$, the invariant function is: $\mathcal{I}_{\mathcal{E}}(\cdot) = \emptyset$, and the local evolution function is: $t_{\mathcal{E}}(\cdot, true, \emptyset, \overline{a}) = \cdot$ if $act_{\mathcal{E}}(\overline{a}) = \epsilon_{\mathcal{E}}$, where $\overline{a} \in Act$.

In the ATIS model $\mathbb{I}_\varphi$ of TTCS for an EMTLK formula φ with two intervals (e.g., $G_{[0,\infty)}(\overline{\mathrm{K}}_{\mathbf{c}}p \Rightarrow \mathrm{F}_{[0,100)}\overline{\mathrm{K}}_{\mathbf{c}}q)$) the environment $\mathcal{E}$ is modelled as follows: $L_{\mathcal{E}} = \{\cdot\}, Act'_{\mathcal{E}} = \{\epsilon_{\mathcal{E}}, \{y_1\}, \{y_2\}, \{y_1, y_2\}\}, X'_{\mathcal{E}} = \{y_1, y_2\}, P_{\mathcal{E}}(\cdot) = Act'_{\mathcal{E}}, \mathcal{V}_{\mathcal{E}}(\cdot) = \emptyset, \mathcal{I}_{\mathcal{E}}(\cdot) = \emptyset$, and the local evolution function is: $t_{\mathcal{E}}(\cdot, true, \emptyset, \overline{a}) = \cdot$ if $act_{\mathcal{E}}(\overline{a}) = \epsilon_{\mathcal{E}}, t_{\mathcal{E}}(\cdot, true, \{y_1\}, \overline{a}) = \cdot$ if $act_{\mathcal{E}}(\overline{a}) = \{y_1\}, t_{\mathcal{E}}(\cdot, true, \{y_2\}, \overline{a}) = \cdot$ if $act_{\mathcal{E}}(\overline{a}) = \{y_2\}, t_{\mathcal{E}}(\cdot, true, \{y_1, y_2\}, \overline{a}) = \cdot$ if $act_{\mathcal{E}}(\overline{a}) = \{y_1, y_2\}$, where $\overline{a} \in \prod_{\mathbf{c}\in\mathbb{A}} Act_{\mathbf{c}} \times Act'_{\mathcal{E}}$.

3.2. A Model for ATIS

Let φ be an EMTLK formula, m a number of intervals appearing in $\varphi, \mathcal{PV}' = \mathcal{PV} \cup \mathcal{PV}_y$ with $\mathcal{PV}_y = \{q_{y_h \in I_h} \mid h = 1, \ldots, m\}$, and $\mathbb{I}_\varphi = (\{L_\mathbf{c}, Act_\mathbf{c}, X_\mathbf{c}, P_\mathbf{c}, t_\mathbf{c}, \mathcal{V}_\mathbf{c}, \mathcal{I}_\mathbf{c}\}_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}}, \iota)$ be an ATIS. The *abstract model* for $\mathbb{I}_\varphi$ is a tuple $M_\varphi = (\Sigma_\varphi, \iota, S_\varphi, T_\varphi, \mathcal{V}_\varphi)$, where

- $\Sigma_\varphi = Act \cup \{\tau\}$, where $Act = \prod_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} Act_\mathbf{c}$,
- $S_\varphi = \prod_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} L_\mathbf{c} \times \mathbb{N}^{|X_\mathbf{c}|}$ is the set of all possible global states,
- $\mathcal{V}_\varphi : S_\varphi \to 2^{\mathcal{PV}'}$ is the valuation function such that:
  1. $p \in \mathcal{V}_\varphi(s)$ iff $p \in \bigcup_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} \mathcal{V}_\mathbf{c}(l_\mathbf{c}(s))$ for all $p \in \mathcal{PV}$,
  2. $q_{y_h \in I_h} \in \mathcal{V}_\varphi(((\ell_1, v_1), \ldots, (\ell_n, v_n), (\ell_\mathcal{E}, v_\mathcal{E})))$ iff $v_\mathcal{E}(y_h) \in I_h$,
- $T_\varphi \subseteq S_\varphi \times \Sigma_\varphi \times S_\varphi$ is a transition relation defined by action and time transitions. Let $\overline{a} \in Act$:
  1. Action transition: $(s, \overline{a}, s') \in T_\varphi$ iff $(\forall \mathbf{c} \in \mathbb{A})$ $(\exists \phi_\mathbf{c} \in \mathcal{C}(X_\mathbf{c}))$ $(\exists X'_\mathbf{c} \subseteq X_\mathbf{c})$ $(t_\mathbf{c}(l_\mathbf{c}(s), l_\mathcal{E}(s), \phi_\mathbf{c}, X'_\mathbf{c}, \overline{a}) = l_\mathbf{c}(s')$ and $v_\mathbf{c}(s) \models \phi_\mathbf{c} \wedge \mathcal{I}(l_\mathbf{c}(s))$ and $v'_\mathbf{c}(s') = v_\mathbf{c}(s)[X'_\mathbf{c} := 0]$ and $v'_\mathbf{c}(s') \models \mathcal{I}(l_\mathbf{c}(s')))$ and $(\exists \phi_\mathcal{E} \in \mathcal{C}(X_\mathcal{E}))$ $(\exists X'_\mathcal{E} \subseteq X_\mathcal{E})$ $(t'_\mathcal{E}(l_\mathcal{E}(s), \phi_\mathcal{E}, X'_\mathcal{E}, \overline{a}) = l_\mathcal{E}(s')$ and $v_\mathcal{E}(s) \models \phi_\mathcal{E} \wedge \mathcal{I}(l_\mathcal{E}(s))$ and $v'_\mathcal{E}(s') = v_\mathcal{E}(s)[X'_\mathcal{E} := 0]$ and $v'_\mathcal{E}(s') \models \mathcal{I}(l_\mathcal{E}(s')))$
  2. Time transition: $(s, \tau, s') \in T_\varphi$ iff $(\forall \mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\})(l_\mathbf{c}(s) = l_\mathbf{c}(s')$ and $v_\mathbf{c}(s) \models \mathcal{I}(l_\mathbf{c}(s))$ and $v'_\mathbf{c}(s') = succ(v_\mathbf{c}(s))$ and $v'_\mathbf{c}(s') \models \mathcal{I}(l_\mathbf{c}(s)))$.

  Note that each transition is followed by a possible reset of new clocks. This is to ensure that the new clocks can be reset along the evolution of the system any time it is needed.

Given an ATIS one can define the indistinguishability relation $\sim_\mathbf{c} \subseteq S_\varphi \times S_\varphi$ for agent $\mathbf{c}$ as follows: $s \sim_\mathbf{c} s'$ iff $l_\mathbf{c}(s) = l_\mathbf{c}(s')$ and $v_\mathbf{c}(s) = v_\mathbf{c}(s')$.

3.3. Paths in M_φ

Let φ be an EMTLK formula, $\mathbb{I}_\varphi$ an augmented timed interpreted system, and M_φ a model for $\mathbb{I}_\varphi$.

Definition 3.2. A *path* π in M_φ is a sequence $\pi = (s_0, s_1, \ldots)$ of states such that $(s_0, \tau, s_1) \in T_\varphi$, and for each $i > 0$, either $(s_i, \overline{a}_i, s_{i+1}) \in T_\varphi$ or $(s_i, \tau, s_{i+1}) \in T_\varphi$, and if $(s_i, \overline{a}_i, s_{i+1}) \in T_\varphi$ holds, then $(s_{i+1}, \tau, s_{i+2}) \in T_\varphi$ holds, and $\overline{a}_i \in Act$ for each $i \geq 0$.

Observe that the above definition of the path ensures that the first transition is the time one, and between each two action transitions at least one time transition appears.

For a path $\pi, \pi(i)$ denotes the i-th state s_i of $\pi, \pi^i = (s_i, s_{i+1}, \ldots)$ denotes the suffix of π starting with $\pi(i), \Pi_\varphi(s)$ denotes the set of all the paths starting at $s \in S_\varphi$, and $\Pi_\varphi = \bigcup_{s^0 \in \iota} \Pi_\varphi(s^0)$ denotes the set of all the paths originating from all initial states in S_φ.

Assume that each state of M_φ has the following form: $s_i = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^i))$, for all $i \geq 0$. Then, for $t \in \mathbb{N}, y \in Y$, and a path $\pi = (s_0, s_1, \ldots)$ in M_φ, we define the (unique) path $\Upsilon_y^t(\pi) = (s'_0, s'_1, \ldots)$ as follows. $(\forall j \in \mathbb{N})$ $((\forall \mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\})$ $({\ell'}_{\mathbf{c}}^j = \ell_{\mathbf{c}}^j)$ and $(\forall \mathbf{c} \in \mathbb{A})({v'}_{\mathbf{c}}^j = v_{\mathbf{c}}^j)$ and

$$
{v'}_{\mathcal{E}}^j = \begin{cases} v_{\mathcal{E}}^j, & \text{if } 0 \leq j < t \\ v_{\mathcal{E}}^j[\{y\} := 0], & \text{if } j = t \\ succ({v'}_{\mathcal{E}}^{j-1}), & \text{if } j > t \text{ and } v_{\mathcal{E}}^j = succ(v_{\mathcal{E}}^{j-1}) \\ {v'}_{\mathcal{E}}^{j-1}[X := 0], & \text{if } j > t \text{ and } v_{\mathcal{E}}^j = v_{\mathcal{E}}^{j-1}[X := 0] \\ succ({v'}_{\mathcal{E}}^{j-1})[X := 0], & \text{if } j > t \text{ and } v_{\mathcal{E}}^j = succ(v_{\mathcal{E}}^{j-1})[X := 0]) \end{cases}
$$

Example 3.3. Consider TTCS described in Sect. 2.3.2 for two trains T_1 and $T_2, \Delta = 2$ and $\delta = 1$ (the mutual exclusion holds), and an EMTLK formula φ with one interval, and the following path π:

$$
((away, 0), (away, 0), 0, (\cdot, 0)) \xrightarrow{1} ((away, 1), (away, 1), 0, (\cdot, 1)) \overset{(Start_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow}
$$
$$
((try, 0), (away, 1), 0, (\cdot, 1)) \xrightarrow{1} ((try, 1), (away, 2), 0, (\cdot, 2)) \overset{(approach_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow}
$$
$$
((wait, 0), (away, 2), 1, (\cdot, 2)) \xrightarrow{1} ((wait, 1), (away, 3), 1, (\cdot, 3)) \xrightarrow{1}
$$
$$
((wait, 2), (away, 4), 1, (\cdot, 4)) \overset{(in_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow} ((tunnel, 2), (away, 4), 1, (\cdot, 4)) \xrightarrow{1}
$$
$$
((tunnel, 3), (away, 5), 1, (\cdot, 5)) \overset{(out_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow}
$$
$$
((away, 3), (away, 5), 0, (\cdot, 5)) \xrightarrow{1} ((away, 4), (away, 6), 0, (\cdot, 6)) \overset{\cdots}{\to} .
$$

The path $\Upsilon_y^t(\pi)$ with $t = 4$ is the following:

$$
((away, 0), (away, 0), 0, (\cdot, 0)) \xrightarrow{1} ((away, 1), (away, 1), 0, (\cdot, 1)) \overset{(Start_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow}
$$
$$
((try, 0), (away, 1), 0, (\cdot, 1)) \xrightarrow{1} ((try, 1), (away, 2), 0, (\cdot, 2)) \overset{(approach_1, \epsilon_{T_1}, \{y_1\})}{\longrightarrow}
$$
$$
((wait, 0), (away, 2), 1, (\cdot, 0)) \xrightarrow{1} ((wait, 1), (away, 3), 1, (\cdot, 1)) \xrightarrow{1}
$$
$$
((wait, 2), (away, 4), 1, (\cdot, 2)) \overset{(in_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow} ((tunnel, 2), (away, 4), 1, (\cdot, 2)) \xrightarrow{1}
$$
$$
((tunnel, 3), (away, 5), 1, (\cdot, 3)) \overset{(out_1, \epsilon_{T_1}, \epsilon_{\mathcal{E}})}{\longrightarrow}
$$
$$
((away, 3), (away, 5), 0, (\cdot, 3)) \xrightarrow{1} ((away, 4), (away, 6), 0, (\cdot, 4)) \overset{\cdots}{\to} .
$$

3.4. The HLTLK Language

Let φ be an EMTLK formula, m the number of intervals in $\varphi, h = 1, \ldots, m, p \in \mathcal{PV}', \mathbf{c} \in \mathbb{A}$, and $\Gamma \subseteq \mathbb{A}$. The HLTLK formulae in the negation normal form are given by the following grammar:

$$\phi := \top \,|\, \bot \,|\, p \,|\, \neg p \,|\, \phi \wedge \phi \,|\, \phi \vee \phi \,|\, \phi \mathrm{U}^h \phi \,|\, \mathrm{G}^h \phi \,|\, \overline{\mathrm{K}}_{\mathbf{c}} \phi \,|\, \overline{\mathrm{E}}_\Gamma \phi \,|\, \overline{\mathrm{D}}_\Gamma \phi \,|\, \overline{\mathrm{C}}_\Gamma \phi$$

The symbols U^h and G^h denote the *indexed until* and *indexed globally* modalities, respectively. The meaning of until and globally is standard. The index h denotes the number of a clock that will be set to zero at the starting point of a path along which the until (globally) will be interpreted. The symbols $\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{E}}_\Gamma, \overline{\mathrm{D}}_\Gamma$, and $\overline{\mathrm{C}}_\Gamma$ denote the existential epistemic modalities as defined in the previous section. In addition, we introduce some useful derived temporal modalities: $\varphi \mathrm{R}^h \psi \overset{def}{=} \psi \mathrm{U}^h (\varphi \wedge \psi) \vee \mathrm{G}^h \psi$ (*indexed release*), $\mathrm{F}^h \varphi \overset{def}{=} \top \mathrm{U}^h \varphi$ (*indexed eventually*).

Turning to semantics, HLTLK formulae are interpreted on abstract models M_φ. Let $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}, t \geq 0, \pi$ a path in M_φ, and $\widetilde{\pi} = \Upsilon^t_{y_h}(\pi)$. The satisfiability relation $\models$, which indicates truth of a HLTLK formula ψ in the abstract model M_φ along a path π at time t (in symbols $M_\varphi, \pi^t \models \psi$) is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

- $M_\varphi, \pi^t \models \alpha \mathrm{U}^h \beta$ iff $(\exists i \geq t)(M_\varphi, \widetilde{\pi}^i \models \beta$ and $(\forall t \leq j < i) M_\varphi, \widetilde{\pi}^j \models \alpha)$
- $M_\varphi, \pi^t \models \mathrm{G}^h \alpha$ iff $(\forall i \geq t)(M_\varphi, \widetilde{\pi}^i \models \alpha)$
- $M_\varphi, \pi^t \models \overline{\mathrm{K}}_{\mathbf{c}} \alpha$ iff $(\exists \pi' \in \Pi_\varphi)(\exists i \geq 0)(\pi'(i) \sim_{\mathbf{c}} \pi(t)$ and $M_\varphi, \pi'^i \models \alpha)$
- $M_\varphi, \pi^t \models \overline{Y}_\Gamma \alpha$ iff $(\exists \pi' \in \Pi_\varphi)(\exists i \geq 0)(\pi'(i) \sim^Y_\Gamma \pi(t)$ and $M_\varphi, \pi'^i \models \alpha)$

We use the following notation $M_\varphi \models \psi$ iff $M_\varphi, \pi^0 \models \psi$ for some $\pi \in \Pi_\varphi$. The *existential model checking problem* consists in finding out whether $M_\varphi \models \psi$.

3.5. Translation and Its Correctness

Let φ be an EMTLK formula, $p \in \mathcal{PV}$, I an interval, $y \in Y$ a clock associated with the interval I, and h the index of the clock y. We translate the formula φ inductively into the HLTLK formula $\mathcal{H}(\varphi)$ in the following way:

- $\mathcal{H}(\top) = \top, \mathcal{H}(\bot) = \bot, \mathcal{H}(p) = p$, $\mathcal{H}(\neg p) = \neg p$,
- $\mathcal{H}(\alpha \vee \beta) = \mathcal{H}(\alpha) \vee \mathcal{H}(\beta), \mathcal{H}(\alpha \wedge \beta) = \mathcal{H}(\alpha) \wedge \mathcal{H}(\beta)$,
- $\mathcal{H}(\alpha \mathrm{U}_I \beta) = \mathcal{H}(\alpha) \mathrm{U}^h (\mathcal{H}(\beta) \wedge p_{y \in I}), \mathcal{H}(\mathrm{G}_I \alpha) = \mathrm{G}^h(\neg p_{y \in I} \vee \mathcal{H}(\alpha))$,
- $\mathcal{H}(\overline{\mathrm{K}}_{\mathbf{c}} \alpha) = \overline{\mathrm{K}}_{\mathbf{c}} \mathcal{H}(\alpha), \mathcal{H}(\overline{Y}_\Gamma \alpha) = \overline{Y}_\Gamma \mathcal{H}(\alpha)$, where $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$.

Observe that the translation of literals, Boolean connectives, and epistemic modalities is straightforward. The translation of the U_I operator ensures that: (1) the translation of β holds in the interval I, which is expressed by the requirement $\mathcal{H}(\beta) \wedge p_{y \in I}$; (2) the translation of α holds always before the translation of β. The translation of the G_I operator ensures that if the value of the clock y is in interval I, then the translation of α holds.

Example 3.4. Consider TTCS described in Sect. 2.3.2 for two trains T_1 and T_2, and the following EMTLK formula $\varphi = \mathrm{F}\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{[5,20)}(\neg q))$ with $p = \mathit{ProdSend}, q = \mathit{ConsFree}$. Furthermore, assume that y_1 and y_2 are clocks belonging to the set Y, and that correspond to the intervals $I_1 = [0, \infty)$, and $I_2 = [5, 20)$, respectively. Then the HLTLK formula $\mathcal{H}(\varphi)$ is calculated as follows:

$$\begin{aligned}
\mathcal{H}(\varphi) &= \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \mathcal{H}(\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{I_2}(\neg q)))) \\
&= \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P \mathcal{H}(p \wedge \mathrm{G}_{I_2}(\neg q))) \\
&= \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P(p \wedge \mathcal{H}(\mathrm{G}_{I_2}(\neg q)))) \\
&= \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P(p \wedge \mathrm{G}^{y_2}(\neg p_{y_2 \in I_2} \vee \neg q))).
\end{aligned}$$

Observe that the length of $\mathcal{H}(\varphi)$ is linear in the length of φ. Furthermore, our translation preserves the existential model checking problem, i.e., the existential model checking of φ interpreted over the timed model for TIS can be reduced to the existential model checking of $\mathcal{H}(\varphi)$ interpreted over the abstract model for ATIS.

Lemma 3.5. *Let $\mathbb{I}$ be a timed interpreted system, φ an EMTLK formula, $\mathbb{I}_\varphi$ an augmented timed interpreted system, and M_φ the abstract model for $\mathbb{I}_\varphi$. For each run ρ of $\mathbb{I}$ there exists a path π_ρ of M_φ that is generated by ρ.*

Proof. By the definition of a run, we have that ρ must be of the following form: $\rho = s_0 \overset{\delta_0, \overline{a}_0}{\longrightarrow} s_1 \overset{\delta_1, \overline{a}_1}{\longrightarrow} s_2 \overset{\delta_2, \overline{a}_2}{\longrightarrow} \ldots$, where $\overline{a}_i \in \mathit{Act}, \delta_i \in \mathbb{N}_+$, and $s_i = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^i)) \in S$ for all $i \in \mathbb{N}$. Now, consider the following "augmented" run ρ^* of $\mathbb{I}_\varphi$: $\rho^* = s_0^* \overset{\delta_0, \overline{a}_0}{\longrightarrow} s_1^* \overset{\delta_1, \overline{a}_1}{\longrightarrow} s_2^* \overset{\delta_2, \overline{a}_2}{\longrightarrow} \ldots$, where for all $i \in \mathbb{N}, \overline{a}_i \in \mathit{Act}', \delta_i \in \mathbb{N}_+$, and $s_i^* = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^{*i})), (\forall y \in Y) v_{\mathcal{E}}^{*0}(y) = 0$, and $(\forall i \geq 0)(\forall x \in X_{\mathcal{E}}) v_{\mathcal{E}}^{*i}(x) = v_{\mathcal{E}}^i(x)$. By the definition of the discrete path λ_{ρ^*} corresponding to run ρ^*, we have that for all $t \in \mathbb{N}$ and $i = idx_\rho(t), \lambda_{\rho^*}(t) = s_i^* + t - b_i = ((\ell_1^i, v_1^i + t - b_i), \ldots, (\ell_n^i, v_n^i + t - b_i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^{*i} + t - b_i))$. Observe that $\lambda_{\rho^*}(t) \in \prod_{\mathbf{c} \in \mathbb{A}} L_{\mathbf{c}} \times \mathbb{N}_{\mathbf{c}}^{X_{\mathbf{c}}} \times L_{\mathcal{E}} \times \mathbb{N}_{\mathcal{E}}^{X'_{\mathcal{E}}} = S_\varphi$. Thus, $\pi_\rho = \lambda_{\rho^*}(0), \lambda_{\rho^*}(1), \lambda_{\rho^*}(2), \ldots$ is a path M_φ. ■

Lemma 3.6. *For each path λ of M there exists a path λ^* of M_φ that is generated by λ.*

Proof. Observe that each path $\lambda = (\lambda(0), \lambda(1), \ldots)$ of M is generated by a run $\rho = s_0 \overset{\delta_0,\overline{a}_0}{\longrightarrow} s_1 \overset{\delta_1,\overline{a}_1}{\longrightarrow} s_2 \overset{\delta_2,\overline{a}_2}{\longrightarrow} \ldots$ of $\mathbb{I}$, where $\overline{a}_i \in \mathit{Act}, \delta_i \in \mathbb{N}_+$, and $s_i = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^i)) \in S$ for all $i \in \mathbb{N}$. By Lemma 3.5, we have that there exists a path π_ρ of M_φ that is generated by ρ. Thus, it is enough to take $\lambda^* = \pi_\rho$. ■

Lemma 3.7. *Let $\mathbb{I}$ be a timed interpreted system, M the timed model for $\mathbb{I}, \varphi$ an EMTLK formula, $\mathbb{I}_\varphi$ an augmented timed interpreted system, M_φ the abstract model for $\mathbb{I}_\varphi$, and ρ a run of $\mathbb{I}$. For each subformula ψ of φ and for each $t \in \mathbb{N}, M, \lambda_\rho^t \models \psi$ implies $M_\varphi, \pi_\rho^t \models \mathcal{H}(\psi)$.*

Proof. We proceed by induction on the length of formulae.

1. $\psi = p$, for some $p \in \mathcal{PV}$. We have that $M, \lambda_\rho^t \models p$ iff $p \in \mathcal{V}(\lambda_\rho(t))$. By Lemma 3.5 and the construction of the path π_ρ of M_φ that is generated by ρ we have that $p \in \mathcal{V}_\varphi(\pi_\rho(t))$. Thus, for each $t \in \mathbb{N}, M, \lambda_\rho^t \models \psi$ implies $M_\varphi, \pi_\rho^t \models \mathcal{H}(\psi)$.
2. $\psi = \neg p$, for some $p \in \mathcal{PV}$. The proof is analogous to the case $\psi = p$.
3. $\psi = \alpha \vee \beta$. By the definition of the satisfiability relation we have $M, \lambda_\rho^t \models \alpha \vee \beta$ iff $M, \lambda_\rho^t \models \alpha$ or $M, \lambda_\rho^t \models \beta$. Proceeding by induction we have $M_\varphi, \pi_\rho^t \models \mathcal{H}(\alpha)$ or $M_\varphi, \pi_\rho^t \models \mathcal{H}(\beta)$. Thus, it follows that $M_\varphi, \pi_\rho^t \models \mathcal{H}(\alpha) \vee \mathcal{H}(\beta)$.
4. $\psi = \alpha \wedge \beta$. The proof is analogous to the case $\psi = \alpha \vee \beta$.
5. $\psi = \alpha \mathrm{U}_I \beta$. Assume that $y \in Y$ is a clock associated with the interval I, and $M, \lambda_\rho^t \models \psi$. By the definition of the satisfiability relation we have $(\exists i \in I)(M, \lambda_\rho^{t+i} \models \beta$ and $(\forall 0 \leq j < i)\ M, \lambda_\rho^{t+j} \models \alpha)$. Proceeding by induction it follows that $M_\varphi, \pi_\rho^{t+i} \models \mathcal{H}(\beta)$ and $M_\varphi, \pi_\rho^{t+j} \models \mathcal{H}(\alpha)$ for all $0 \leq j < i$. Consider the unique path $\widetilde{\pi} = \Upsilon_y^t(\pi_\rho)$. By the definition of $\widetilde{\pi}$ it follows that $p_{y \in I} \in \mathcal{V}_\varphi(\widetilde{\pi}(t+i))$. Thus, since $M_\varphi, \pi_\rho^{t+i} \models \mathcal{H}(\beta)$, by the construction of $\widetilde{\pi}$ we have $M_\varphi, \widetilde{\pi}^{t+i} \models \mathcal{H}(\beta) \wedge p_{y \in I}$. Furthermore, since $M_\varphi, \pi_\rho^{t+j} \models \mathcal{H}(\alpha)$ for all $0 \leq j < i$, by the construction of $\widetilde{\pi}$, we have that $M_\varphi, \widetilde{\pi}^{t+j} \models \mathcal{H}(\alpha)$, for all j such that $0 \leq j < i$.

   Thus, by the semantics we get that $M_\varphi, {\pi_\rho}^t \models \mathcal{H}(\alpha) \mathrm{U}^h (\mathcal{H}(\beta) \wedge p_{y \in I})$, where h is the index of the clock y. Therefore, we can conclude that $M_\varphi, {\pi_\rho}^t \models \mathcal{H}(\alpha \mathrm{U}_I \beta)$.
6. $\psi = \mathrm{G}_I \alpha$. Assume that $M, \lambda_\rho^t \models \psi$. By the definition of the satisfiability relation we have $(\forall i \in I)(M, \lambda_\rho^{t+i} \models \alpha)$. Proceeding by induction it follows that $M_\varphi, \pi_\rho^{t+i} \models \mathcal{H}(\alpha)$ for all $i \in I$. Consider the unique path $\widetilde{\pi} = \Upsilon_y^t(\pi_\rho)$. By the definition of $\widetilde{\pi}$ it follows that $p_{y \in I} \in \mathcal{V}_\varphi(\widetilde{\pi}(t+i))$, for

all $i \in I$. Thus, since $M_\varphi, \pi_\rho^{t+i} \models \mathcal{H}(\alpha)$ for all $i \in I$, by the construction of $\widetilde{\pi}$ we have $M_\varphi, \widetilde{\pi}^{t+i} \models p_{y \in I} \wedge \mathcal{H}(\alpha)$ for all $i \in I$. Therefore, for all $i \geq t$ we have $M_\varphi, \widetilde{\pi}^{t+i} \models \neg p_{y \in I} \vee \mathcal{H}(\alpha)$. Thus, by the semantics we get that $M_\varphi, {\pi_\rho}^t \models \mathrm{G}^h(\neg p_{y \in I} \vee \mathcal{H}(\alpha))$, where h is the index of the clock y. Therefore, we can conclude that $M_\varphi, {\pi_\rho}^t \models \mathcal{H}(\mathrm{G}_I \alpha)$.

7. $\psi = \overline{\mathrm{K}}_{\mathbf{c}}\alpha$. Assume that $M, \lambda_\rho^t \models \psi$. By the definition of the satisfiability relation we have that $(\exists \lambda \in \Pi)(\exists i \geq 0)(\lambda(i) \sim_{\mathbf{c}} \lambda_\rho(t)$ and $M, \lambda^i \models \alpha)$. Proceeding by induction it follows that $M_\varphi, \pi_\lambda^i \models \mathcal{H}(\alpha)$. By Lemmas 3.5 and 3.6 we have that for λ_ρ there exists a path π_ρ of M_φ that is generated by λ_ρ. Since $\lambda(i) \sim_{\mathbf{c}} \lambda_\rho(t)$ holds, by the construction of the paths π_λ and π_ρ we have that $\pi_\lambda(i) \sim_{\mathbf{c}} \pi_\rho(t)$ holds. Therefore, we have $M_\varphi, {\pi_\rho}^t \models \mathcal{H}(\overline{\mathrm{K}}_{\mathbf{c}}\alpha)$.
8. $\psi = \overline{Y}_\Gamma \alpha$ and $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$. The proof is analogous to the case $\psi = \overline{\mathrm{K}}_{\mathbf{c}}\alpha$. ■

LEMMA 3.8. *Let $\mathbb{I}$ be a timed interpreted system, φ an EMTLK formula, $\mathbb{I}_\varphi$ an augmented timed interpreted system, M_φ the abstract model for $\mathbb{I}_\varphi$.*

For each path π of M_φ there exists a run ρ of $\mathbb{I}$ that is induced by π and such that for all $i \geq 0, \pi(i)|_X = \lambda_\rho(i)$, where $X = \bigcup_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} X_{\mathbf{c}}$ and $\pi(i)|_X$ denotes the state of M_φ from which the values of auxiliary clocks from Y have been removed.

PROOF. Each path of M_φ is of the form $\pi = (s_0, s_1, \ldots)$ with $(s_0, \tau, s_1) \in T_\varphi$, and for each $i \geq 0, s_i = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_\mathcal{E}^i, v_\mathcal{E}^i))$, and either $(s_i, \overline{a}_i, s_{i+1}) \in T_\varphi$ or $(s_i, \tau, s_{i+1}) \in T_\varphi$, and if $(s_i, \overline{a}_i, s_{i+1}) \in T_\varphi$ holds, then $(s_{i+1}, \tau, s_{i+2}) \in T_\varphi$ holds, and $\overline{a}_i \in Act$ for each $i \geq 0$. This implies that π has the following shape:

$$s_0, \underbrace{\ldots}_{\tau_0,\ldots,\tau_{i-1}}, s_i \underbrace{,}_{\overline{a}_0} s_{i+1}, \underbrace{\ldots}_{\tau_{i+1},\ldots,\tau_{j-1}}, s_j \underbrace{,}_{\overline{a}_1} s_{j+1}, \underbrace{\ldots}_{\tau_{j+1},\ldots,\tau_{k-1}}, s_k \underbrace{,}_{\overline{a}_2} s_{k+1}, \ldots$$

with $i \geq 1, j > i$, and $k > j$. Thus, we have that the path π is generated by the following run ρ^* of $\mathbb{I}_\varphi$: $\rho^* = w_0 \overset{\delta_0^*, \overline{a}_0}{\longrightarrow} w_1 \overset{\delta_1^*, \overline{a}_1}{\longrightarrow} w_2 \overset{\delta_2^*, \overline{a}_2}{\longrightarrow} w_3 \ldots$ with $w_0 = s_0, w_1 = s_{i+1}, w_2 = s_{j+1}, w_3 = s_{k+1}$, and so on. Now, assume that $w_i = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_\mathcal{E}^i, v_\mathcal{E}^i))$ for all $i \geq 0$, and consider the following run $\rho = r_0 \overset{\delta_0^*, \overline{a}_0}{\longrightarrow} r_1 \overset{\delta_1^*, \overline{a}_1}{\longrightarrow} r_2 \overset{\delta_2^*, \overline{a}_2}{\longrightarrow} r_3 \ldots$ with $r_0 = ((\ell_1^0, v_1^0), \ldots, (\ell_n^0, v_n^0), (\ell_\mathcal{E}^0, v_\mathcal{E}^0|_{X_\mathcal{E}}))$, and for all $i > 0, r_i = ((\ell_1^i, v_1^{i*}), \ldots, (\ell_n^i, v_n^{i*}), (\ell_\mathcal{E}^i, v_\mathcal{E}^{i*}|_{X_\mathcal{E}}))$ and $(\forall \mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\})(\forall x \in X_{\mathbf{c}})(v_{\mathbf{c}}^{i*}(x) = v_{\mathbf{c}}^{i-1*}(x) + \delta_{i-1}^*)$. Observe that ρ is a valid run of $\mathbb{I}$, and moreover $\pi(i)|_X = \lambda_\rho(i)$ for all $i \geq 0$. ■

Lemma 3.9. *Let $\mathbb{I}$ be a timed interpreted system, M the timed model for $\mathbb{I}, \varphi$ an EMTLK formula, $\mathbb{I}_\varphi$ the augmented timed interpreted system, M_φ the abstract model for $\mathbb{I}_\varphi, \pi$ a path of M_φ that is induced by a run ρ of $\mathbb{I}$. Then, for each subformula ψ of φ and for each $t \in \mathbb{N}, M_\varphi, \pi^t_\rho \models \mathcal{H}(\psi)$ implies $M, \lambda^t_\rho \models \psi$.*

Proof. We proceed by induction on the length of formulae.

1. $\psi = p$, for some $p \in \mathcal{PV}$. We have that $M_\varphi, \pi^t_\rho \models \mathcal{H}(\psi)$ iff $p \in \mathcal{V}_\varphi(\pi_\rho(t))$. By Lemma 3.8 we have that $p \in \mathcal{V}(\lambda_\rho(t))$. Thus, for each $t \in \mathbb{N}, M_\varphi, \pi^t_\rho \models \mathcal{H}(\psi)$ implies $M, \lambda^t_\rho \models \psi$.
2. $\psi = \neg p$, for some $p \in \mathcal{PV}$. The proof is analogous to the case $\psi = p$.
3. $\psi = \alpha \vee \beta$. By the definition of the function $\mathcal{H}$ and the satisfiability relation we have $M_\varphi, \pi^t_\rho \models \mathcal{H}(\alpha \vee \beta)$ iff $M_\varphi, \pi^t_\rho \models \mathcal{H}(\alpha)$ or $M_\varphi, \pi^t_\rho \models \mathcal{H}(\beta)$. Proceeding by induction we have $M, \lambda^t_\rho \models \alpha$ or $M, \lambda^t_\rho \models \beta$. Thus, it follows that $M, \lambda^t_\rho \models \alpha \vee \beta$.
4. $\psi = \alpha \wedge \beta$. The proof is analogous to the case $\psi = \alpha \vee \beta$.
5. $\psi = \alpha \mathrm{U}_I \beta$. Assume that a clock $y \in Y$ is associated with the interval I, h is the index associated to the clock y, and $M_\varphi, \pi^t_\rho \models \mathcal{H}(\psi)$.

   By the definition of the function $\mathcal{H}$ we have $M_\varphi, \pi^t_\rho \models \mathcal{H}(\alpha)\mathrm{U}^h(\mathcal{H}(\beta) \wedge p_{y \in I})$. By the definition of the satisfiability relation we have $(\exists i \geq t)(M_\varphi, \widetilde{\pi}^i \models \mathcal{H}(\beta) \wedge p_{y \in I}$ and $(\forall t \leq j < i) M_\varphi, \widetilde{\pi}^j \models \mathcal{H}(\alpha))$, where $\widetilde{\pi} = \Upsilon^t_y(\pi)$. Observe that by the definition of the path $\widetilde{\pi}$, and by the construction of the run ρ of $\mathbb{I}$ given in the proof of Lemma 3.8, we have that the run ρ is also induced by the path $\widetilde{\pi}$. Moreover, since $M_\varphi, \widetilde{\pi}^i \models p_{y \in I}$ holds, we have $p_{y \in I} \in \mathcal{V}_\varphi(\widetilde{\pi}(i))$. Thus we have $i - t \in I$. Furthermore, by induction, we have $M, \lambda^i_\rho \models \beta$ and $(\forall t \leq j < i) M, \lambda^j_\rho \models \alpha$. Therefore, we conclude that $M, \lambda^t_\rho \models \alpha \mathrm{U}_I \beta$.
6. $\psi = \mathrm{G}_I \alpha$. Assume that a clock $y \in Y$ is associated with the interval I, h is the index associated to the clock y, and $M_\varphi, \pi^t_\rho \models \mathcal{H}(\psi)$. By the definition of the function $\mathcal{H}$ we have $M_\varphi, \pi^t_\rho \models \mathrm{G}^h(\mathcal{H}(\alpha) \vee \neg p_{y \in I})$. By the definition of the satisfiability relation we have $(\forall i \geq t)(M_\varphi, \widetilde{\pi}^i \models \mathcal{H}(\alpha) \vee \neg p_{y \in I})$, where $\widetilde{\pi} = \Upsilon^t_y(\pi)$. Observe that by the definition of the path $\widetilde{\pi}$, and by the construction of the run ρ of $\mathbb{I}$ given in the proof of Lemma 3.8, we have that the run ρ is also induced by the path $\widetilde{\pi}$. Thus, if $M_\varphi, \widetilde{\pi}^i \models p_{y \in I}$ holds, then we have $p_{y \in I} \in \mathcal{V}_\varphi(\widetilde{\pi}(i))$, and thus we have $i - t \in I$. Therefore, we have that $(\forall i \geq t)(i - t \in I$ implies

$M_\varphi, \widetilde{\pi}^i \models \mathcal{H}(\alpha))$. By induction, we have that $(\forall i \in I)(M, \lambda_\rho^{t+i} \models \alpha)$. Therefore, we have $M, \lambda_\rho^t \models \mathrm{G}_I\alpha$.

7. $\psi = \overline{\mathrm{K}}_{\mathbf{c}}\alpha$. Assume that $M_\varphi, \pi_\rho^t \models \mathcal{H}(\psi)$. By the definition of the satisfiability relation we have $(\exists \pi' \in \Pi_\varphi)(\exists i \geq 0)(\pi'(i) \sim_{\mathbf{c}} \pi_\rho(t)$ and $M_\varphi, {\pi'}^i \models \mathcal{H}(\alpha))$. By Lemma 3.8 we have that there exists a run ρ' of TIS that is induced by π'. Thus, by induction, we have $(\exists \lambda_{\rho'} \in \Pi)(\exists i \geq 0)(M, {\lambda_{\rho'}}^i \models \alpha)$. Further, by the construction of the run of $\mathbb{I}$ in Lemma 3.8 we have that $\lambda_{\rho'}(i) \sim_{\mathbf{c}} \lambda_\rho(t)$. Thus, we can conclude that $M, \lambda_\rho^t \models \overline{\mathrm{K}}_{\mathbf{c}}\alpha$.

8. $\psi = \overline{Y}_\Gamma\alpha$ and $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$. The proof is analogous to the case $\psi = \overline{\mathrm{K}}_{\mathbf{c}}\alpha$. ■

The main theorem of the section states that existential validity of the EMTLK formula φ over the timed model for TIS is equivalent to the existential validity of the HLTLK formula $\mathcal{H}(\varphi)$ over the abstract model for ATIS.

THEOREM 3.10. *Let M be the timed model, φ an EMTLK formula, and M_φ the abstract model. Then, $M \models \varphi$ iff $M_\varphi \models \mathcal{H}(\varphi)$.*

PROOF. The proof of the theorem follows from Lemmas 3.7 and 3.9. ■

The construction of the augmented timed interpreted system for the timed interpreted system and an EMTLK formula φ involves an exponential blow-up, the reduction of φ into $\mathcal{H}(\varphi)$ involves only a linear blow-up, and the HLTLK language can be viewed as an existential LTLK; notice that LTLK is a multi-dimensional logic obtained by the fusion (or independent join) [5] of LTL with $\mathrm{S5}^n$, where n is the number of distinct epistemic modalities. Since, the (symbolic) model checking problem for LTLK is PSPACE [12], Theorem 3.10 suggests a PSPACE model checking algorithm for the existential model checking problem of EMTLK.

4. A SAT-Based BMC Method for HLTLK

In this section we present a SAT-based BMC method for HLTLK. In SAT-based BMC we construct a propositional formula that is satisfiable if and only if there exists a finite set of prefixes of paths of the underlying model that is a solution to the existential model checking problem. To construct the propositional formula, first of all we need to define the bounded semantics for the underlying logic (i.e., in our case for HLTLK), then to encode the semantics by means of a propositional formula, and finally to represent a part of the model by a propositional formula.

We begin the section by introducing the definition of the bounded semantics for HLTLK and proving that the bounded and unbounded semantics are equivalent. Then, we define a translation of the existential model checking problem for HLTLK to the propositional satisfiability problem, and we formulate the theorem about the correctness and completeness of the proposed translation.

4.1. Bounded Semantics

Let $M_\varphi = (\iota_\varphi, S_\varphi, T_\varphi, \mathcal{V}_\varphi)$ be an abstract model, $k \in \mathbb{N}$, and $0 \leq l \leq k$.

Definition 4.1. A *k-path* π_l is a pair (π, l), where π is a finite sequence $\pi = (s_0, \ldots, s_k)$ of states such that $(s_0, \tau, s_1) \in T_\varphi$, and for each $0 < i < k$, either $(s_i, \overline{a}_i, s_{i+1}) \in T_\varphi$ or $(s_i, \tau, s_{i+1}) \in T_\varphi$, and if $(s_i, \overline{a}_i, s_{i+1}) \in T_\varphi$ holds, then $(s_{i+1}, \tau, s_{i+2}) \in T_\varphi$ holds, and $\overline{a}_i \in \mathit{Act}$ for each $0 \leq i < k$.

Definition 4.2. Let $\pi(i) = ((\ell^i_1, v^i_1), \ldots, (\ell^i_n, v^i_n), (\ell^i_{\mathcal{E}}, v^i_{\mathcal{E}}))$ for all $i \leq k$. A k-path π_l is a *loop* if $l < k$ and $(\forall \mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\})(\ell^k_{\mathbf{c}} = \ell^l_{\mathbf{c}})$ and $(\forall \mathbf{c} \in \mathbb{A})(v^k_{\mathbf{c}} = v^l_{\mathbf{c}})$ and $v^k_{\mathcal{E}\downarrow X_{\mathcal{E}}} = v^l_{\mathcal{E}\downarrow X_{\mathcal{E}}}$, where $\downarrow X_{\mathcal{E}}$ denoted the projection of the clock valuation $v_{\mathcal{E}} : X_{\mathcal{E}} \cup Y \rightarrow \mathbb{N}$ on the clock valuation $v'_{\mathcal{E}} : X_{\mathcal{E}} \rightarrow \mathbb{N}$.

The set of all the k-paths π_l with $\pi(0) = s$ is denoted by $\Pi_k(s)$, and $\Pi_k = \bigcup_{s^0 \in \iota_\varphi} \Pi_k(s^0)$.

Example 4.3. To illustrate the notion of k-paths and loops let us consider the TTCS scenario described in Sect. 2.3.2 for two trains T_1 and $T_2, \Delta = 2$ and $\delta = 0$, and an EMTLK formula φ with one interval. Assume that we have the following states:

$s_0 = ((away, 0), (away, 0), (0), (\cdot, 0)), s_1 = ((away, 1), (away, 1), (0), (\cdot, 1)),$
$s_2 = ((away, 2), (away, 2), (0), (\cdot, 2)), s_3 = ((away, 3), (away, 3), (0), (\cdot, 3)),$
$s_4 = ((try, 0), (away, 3), (0), (\cdot, 3)), s_5 = ((try, 1), (away, 4), (0), (\cdot, 4)),$
$s_6 = ((wait, 0), (away, 4), (1), (\cdot, 4)), s_7 = ((wait, 1), (away, 5), (1), (\cdot, 5)),$
$s_8 = ((tunnel,1), (away,5), (1), (\cdot, 5)), s_9 = ((tunnel,2), (away,6), (1), (\cdot, 6)),$
$s_{10} = ((away,2), (away,6), (0), (\cdot, 6)), s_{11} = ((away,3), (away,7), (0), (\cdot, 7)),$
$s_{12} = ((away, 3), (try, 0), (0), (\cdot, 7)), s_{13} = ((away, 4), (try, 1), (0), (\cdot, 8)),$
$s_{14} = ((away, 4), (wait, 0), (2), (\cdot, 8)), s_{15} = ((away, 5), (wait, 1), (2), (\cdot, 9)),$
$s_{16} = ((away,5),(tunnel,1),(2),(\cdot,9)), s_{17} = ((away,6),(tunnel,2),(2),(\cdot,10)),$
$s_{18} = ((away,6),(away,2), (0),(\cdot,10)), s_{19} = ((away,7),(away,3), (0),(\cdot,11)),$
$s_{20} = ((try, 0), (away, 3), (0), (\cdot, 11)),$ and observe that the pairs:

$\pi_0 = ((s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14},$
$s_{15}, s_{16}, s_{17}, s_{18}, s_{19}, s_{20}), 0), \ldots,$
$\pi_4 = ((s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9,$
$s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}, s_{19}, s_{20}), 4), \ldots,$
$\pi_{20} = ((s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12},$
$s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}, s_{19}, s_{20}), 20)$ are k-paths for $k = 20$.

Moreover, only π_4 is loop.

Further, let $\pi_l = ((s_0, \ldots, s_k), l)$ be a k-path, $t \leq k$ a natural number, and $y \in Y$ a new clock. If either π_l is not a loop or π_l is a loop with $l \geq t$, then $(\Phi_y^{t,k}(\pi), l) = ((s'_0, \ldots, s'_k), l)$ is the k-path defined as follows. $(\forall 0 \leq j \leq k)((\forall \mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\})(\ell'^j_{\mathbf{c}} = \ell^j_{\mathbf{c}})$ and $(\forall \mathbf{c} \in \mathbb{A})(v'^j_{\mathbf{c}} = v^j_{\mathbf{c}})$ and

$$v'^j_{\mathcal{E}} = \begin{cases} v^j_{\mathcal{E}}, & \text{if } 0 \leq j < t \\ v^j_{\mathcal{E}}[\{y\} := 0], & \text{if } j = t \\ succ(v'^{j-1}_{\mathcal{E}}), & \text{if } t < j \leq k \text{ and } v^j_{\mathcal{E}} = succ(v^{j-1}_{\mathcal{E}}) \\ v'^{j-1}_{\mathcal{E}}[X := 0], & \text{if } t < j \leq k \text{ and } v^j_{\mathcal{E}} = v^{j-1}_{\mathcal{E}}[X := 0] \\ succ(v'^{j-1}_{\mathcal{E}})[X := 0], & \text{if } t < j \leq k \text{ and } v^j_{\mathcal{E}} = succ(v^{j-1}_{\mathcal{E}})[X := 0]). \end{cases}$$

EXAMPLE 4.4. To illustrate the notion of k-path $(\Phi_y^{t,k}(\pi), l)$ let us consider the 20-path $\pi_9 = ((s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}, s_{16}, s_{17}), 9)$ which we have described in Example 4.3, and which is not loop. The 20-path $(\Phi_y^{t,20}(\pi), 9)$ with $t = 11$ is the following: $((s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s^*_{11}, s^*_{12}, s^*_{13}, s^*_{14}, s^*_{15}, s^*_{16}, s^*_{17}, s_{18}, s_{19}, s_{20}), 9)$, where

$s^*_{11} = ((away, 3), (away, 7), (0), (\cdot, 0)), s^*_{12} = ((away, 3), (try, 0), (0), (\cdot, 0)),$
$s^*_{13} = ((away, 4), (try, 1), (0), (\cdot, 1)), s^*_{14} = ((away, 4), (wait, 0), (2), (\cdot, 1)),$
$s^*_{15} = ((away, 5), (wait, 1), (2), (\cdot, 2)), s^*_{16} = ((away, 5), (tunnel, 1), (2), (\cdot, 2)),$
$s^*_{17} = ((away, 6), (tunnel, 2), (2), (\cdot, 3)), s^*_{18} = ((away, 6), (away, 2), (0), (\cdot, 3)),$
$s^*_{19} = ((away, 7), (away, 3), (0), (\cdot, 4)), s^*_{20} = ((try, 0), (away, 3), (0), (\cdot, 4)).$

If π_l is a loop with $l < t$, then $(\Psi_y^{t,k}(\pi), l) = ((s'_0, \ldots, s'_k), l)$ is the k-path defined as follows. $(\forall 0 \leq j \leq k)((\forall \mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\})(\ell'^j_{\mathbf{c}} = \ell^j_{\mathbf{c}})$ and $(\forall \mathbf{c} \in \mathbb{A})(v'^j_{\mathbf{c}} = v^j_{\mathbf{c}})$ and

$$
{v'}^{j}_{\mathcal{E}} = \begin{cases}
v^{j}_{\mathcal{E}}, & \text{if } 0 \leq j < l \\
v^{j}_{\mathcal{E}}[\{y\} := 0], & \text{if } j = t \\
succ({v'}^{j-1}_{\mathcal{E}}), & \text{if } t < j \leq k \text{ and } v^{j}_{\mathcal{E}} = succ(v^{j-1}_{\mathcal{E}}) \\
{v'}^{j-1}_{\mathcal{E}}[X := 0], & \text{if } t < j \leq k \text{ and } v^{j}_{\mathcal{E}} = v^{j-1}_{\mathcal{E}}[X := 0] \\
succ({v'}^{j-1}_{\mathcal{E}})[X := 0], & \text{if } t < j \leq k \text{ and } v^{j}_{\mathcal{E}} = succ(v^{j-1}_{\mathcal{E}})[X := 0] \\
{v'}^{k}_{\mathcal{E}}, & \text{if } j = l \\
succ({v'}^{j-1}_{\mathcal{E}}), & \text{if } l < j < t \text{ and } v^{j}_{\mathcal{E}} = succ(v^{j-1}_{\mathcal{E}}) \\
{v'}^{j-1}_{\mathcal{E}}[X := 0], & \text{if } l < j < t \text{ and } v^{j}_{\mathcal{E}} = v^{j-1}_{\mathcal{E}}[X := 0] \\
succ({v'}^{j-1}_{\mathcal{E}})[X := 0], & \text{if } l < j < t \text{ and } v^{j}_{\mathcal{E}} = succ(v^{j-1}_{\mathcal{E}})[X := 0]
\end{cases}
$$

EXAMPLE 4.5. To illustrate the notion of k-path $(\Phi^{t,k}_{y}(\pi), l)$ let us consider the 20-path $\pi_4 = ((s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}, s_{16}, s_{17}, s_{18}, s_{19}, s_{20}), 4)$ which we have described in Example 4.3, and which is loop. The 20-path $(\Phi^{t,20}_{y}(\pi), 4)$ with $t = 11$ is the following: $((s_0, s_1, s_2, s_3, s^*_4, s^*_5, s^*_6, s^*_7, s^*_8, s^*_9, s^*_{10}, s^*_{11}, s^*_{12}, s^*_{13}, s^*_{14}, s^*_{15}, s^*_{16}, s^*_{17}, s^*_{18}, s^*_{19}, s^*_{20}), 4)$, where

$$
\begin{aligned}
s^*_4 &= ((try, 0), (away, 3), (0), (\cdot, 4)), \\
s^*_5 &= ((try, 1), (away, 4), (0), (\cdot, 5)), \\
s^*_6 &= ((wait, 0), (away, 4), (1), (\cdot, 5)), \\
s^*_7 &= ((wait, 1), (away, 5), (1), (\cdot, 6)), \\
s^*_8 &= ((tunnel, 1), (away, 5), (1), (\cdot, 6)), \\
s^*_9 &= ((tunnel, 2), (away, 6), (1), (\cdot, 7)), \\
s^*_{10} &= ((away, 2), (away, 6), (0), (\cdot, 7)), \\
s^*_{11} &= ((away, 3), (away, 7), (0), (\cdot, 0)), \\
s^*_{12} &= ((away, 3), (try, 0), (0), (\cdot, 0)), \\
s^*_{13} &= ((away, 4), (try, 1), (0), (\cdot, 1)), \\
s^*_{14} &= ((away, 4), (wait, 0), (2), (\cdot, 1)), \\
s^*_{15} &= ((away, 5), (wait, 1), (2), (\cdot, 2)), \\
s^*_{16} &= ((away, 5), (tunnel, 1), (2), (\cdot, 2)), \\
s^*_{17} &= ((away, 6), (tunnel, 2), (2), (\cdot, 3)), \\
s^*_{18} &= ((away, 6), (away, 2), (0), (\cdot, 3)), \\
s^*_{19} &= ((away, 7), (away, 3), (0), (\cdot, 4)), \\
s^*_{20} &= ((try, 0), (away, 3), (0), (\cdot, 4)).
\end{aligned}
$$

Let φ be an EMTLK formula, $\psi = \mathcal{H}(\varphi)$ the HLTLK formula, M_φ an abstract model, $k \geq 0$ a bound, and $0 \leq t \leq k$. The *bounded satisfiability* relation $\models_k$, which indicates truth of ψ in M_φ along the k-path π_l at time t (denoted π_l^t), is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

$\pi_l^t \models_k \alpha \mathrm{U}^h \beta$ iff $[\widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi)$ and $(\exists t \leq i \leq k)(\widetilde{\pi}_l{}^i \models_k \beta$ and $(\forall t \leq j < i)$ $\widetilde{\pi}_l{}^j \models_k \alpha)]$ or $[\pi_l$ is a loop with $l < t$ and $\widetilde{\pi} = \Psi_{y_h}^{t,k}(\pi)$ and $(\exists l < i < t)(\widetilde{\pi}_l{}^i \models_k \beta$ and $(\forall l \leq j < i)$ $\widetilde{\pi}_l{}^j \models_k \alpha)$ and $(\forall t \leq j \leq k)$ $\widetilde{\pi}_l{}^j \models_k \alpha]$,

$\pi_l^t \models_k \mathrm{G}^h \alpha$ iff $[\pi_l$ is a loop with $t \leq l < k$ and $\widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi)$ and $(\forall t \leq i \leq k)\widetilde{\pi}_l{}^i \models_k \alpha]$ or $[\pi_l$ is a loop with $l < t$ and $\widetilde{\pi} = \Psi_{y_h}^{t,k}(\pi)$ and $(\forall t \leq i \leq k)\widetilde{\pi}_l{}^i \models_k \alpha$ and $(\forall l < i < t)$ $\widetilde{\pi}_l{}^i \models_k \alpha]$,

$\pi_l^t \models \overline{\mathrm{K}}_{\mathbf{c}}\alpha$ iff $(\exists \pi'_{l'} \in \Pi_k)(\exists 0 \leq i \leq k)(\pi'(i) \sim_{\mathbf{c}} \pi(t)$ and $M, \pi'^{i}_{l'} \models \alpha)$,

$\pi_l^t \models \overline{Y}_\Gamma \alpha$ iff $(\exists \pi'_{l'} \in \Pi_k)(\exists 0 \leq i \leq k)(\pi'(i) \sim_\Gamma^Y \pi(t)$ and $M, \pi'^{i}_{l'} \models \alpha)$, where $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$.

We use the following notation $M_\varphi \models_k \psi$ iff $M_\varphi, \pi_l^0 \models_k \psi$ for some $\pi_l \in \Pi_k$. The *bounded model checking problem* consists in finding out whether there exists $k \in \mathbb{N}$ such that $M_\varphi \models_k \psi$.

4.2. Equivalence of Bounded and Unbounded Semantics

Lemma 4.6. *Let M_φ an abstract model, $\psi = \mathcal{H}(\varphi)$ an HLTLK formula, $k > 0$ a bound, π_l a k-path in M_φ, and $0 \leq t \leq k$. The following implication holds: $M, \pi_l^t \models_k \psi$ implies*

- *if π_l is not a loop, then $M_\varphi, \pi'^t \models \psi$ for each path π' in M_φ such that k-prefix of π' is equal to π_l.*
- *if π_l is a loop, then $M_\varphi, \pi'^t \models \varphi$, where π' is the path generated by the loop π_l.*

Proof. We proceed by induction on the length of formulae ψ. The lemma follows directly for the propositional variables and their negations. Consider the following cases:

- If $\psi = \alpha \vee \beta \mid \alpha \wedge \beta$, then the proof is straightforward.
- Let $\psi = \overline{\mathrm{K}}_{\mathbf{c}}\alpha \mid \overline{Y}_{\Gamma}\alpha$. By induction hypothesis - see Lemma 2 of [17]
- $\psi = \alpha \mathrm{U}^h \beta$ and $M_\varphi, \pi_l^t \models_k \psi$. By the definition of the bounded semantics we have that either

$$(\dagger)[\widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi) \text{ and } (\exists t \leq i \leq k)(M_\varphi, \widetilde{\pi}_l{}^i \models_k \beta \text{ and}$$
$$(\forall t \leq j < i) M_\varphi, \widetilde{\pi}_l{}^j \models_k \alpha)] \text{ or } (\dagger\dagger)[\pi_l \text{ is a loop with } l < t\text{and}$$
$$\widetilde{\pi} = \Psi_{y_h}^{t,k}(\pi) \text{ and } (\exists l < i < t)(M_\varphi, \widetilde{\pi}_l{}^i \models_k \beta \text{ and}$$
$$(\forall l \leq j < i) M_\varphi, \widetilde{\pi}_l{}^j \models_k \alpha)$$
$$\text{and } (\forall t \leq j \leq k) M_\varphi, \widetilde{\pi}_l{}^j \models_k \alpha].$$

Assume that ($\dagger$) holds and that π_l is a loop. By the definition of $(\Phi_{y_h}^{t,k}(\pi), l)$ we have $l \geq t$. By induction and fact that $\widetilde{\pi'}$ is generated by $\widetilde{\pi}_l$ we have $(\exists i \geq t)(M_\varphi, \widetilde{\pi'}^i \models \beta$ and $(\forall t \leq j < i)$ $M_\varphi, \widetilde{\pi'}^j \models \alpha)$. Thus, we conclude that $M_\varphi, \pi'^t \models \alpha \mathrm{U}^h \beta$.
Assume now that ($\dagger$) holds and that π_l is not a loop. By the definition of $\Phi_{y_h}^{t,k}(\pi)$ and by induction we have $(\exists i \geq t)(M_\varphi, \widetilde{\pi'}^i \models \beta$ and $(\forall t \leq j < i)$ $M_\varphi, \widetilde{\pi'}^j \models \alpha)$ for each $\widetilde{\pi'}$ in M_φ such that k-prefix of $\widetilde{\pi'}$ is equal to $\widetilde{\pi}_l$. Thus, we have $M_\varphi, \pi'^t \models \alpha \mathrm{U}^h \beta$.

Assume now that ($\dagger\dagger$) holds. Since π_l is a loop, by the definition of $(\Psi_{y_h}^{t,k}(\pi), l)$ we have $l < t$. By induction and fact that $\widetilde{\pi'}$ is generated by $\widetilde{\pi}_l$ we have $(\exists k < i < k + t - l)(M_\varphi, \widetilde{\pi}^i \models_k \beta$ and $(\forall t \leq j < i) M_\varphi, \widetilde{\pi}^j \models_k \alpha)$. Thus, we have $M_\varphi, \pi'^t \models \alpha \mathrm{U}^h \beta$.

- $\psi = \mathrm{G}^h \alpha$ and $M_\varphi, \pi_l^t \models_k \psi$. By the definition of the bounded semantics we have

$$(\dagger)[\pi_l \text{ is a loop with } t \leq l < k \text{ and } \widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi)$$
$$\text{and } (\forall t \leq i \leq k) M_\varphi, \widetilde{\pi}_l{}^i \models_k \alpha] \text{ or}$$
$$(\dagger\dagger)[\pi_l \text{ is a loop with } l < t \text{ and } \widetilde{\pi} = \Psi_{y_h}^{t,k}(\pi) \text{ and}$$
$$(\forall t \leq i \leq k) M_\varphi, \widetilde{\pi}_l{}^i \models_k \alpha \text{ and } (\forall l < i < t) M_\varphi, \widetilde{\pi}_l{}^i \models_k \alpha].$$

Assume that ($\dagger$) holds. Since π_l is a loop, by the definition of $(\Phi_{y_h}^{t,k}(\pi), l)$ we have $t \leq l < k$. By induction and fact that $\widetilde{\pi'}$ is generated by $\widetilde{\pi}_l$ we have $(\forall i \geq t) M_\varphi, \widetilde{\pi'}^i \models \alpha$. Thus, we have $M_\varphi, \pi'^t \models \mathrm{G}^h \alpha$.

Assume that (††) holds. Since π_l is a loop, by the definition of $(\Psi^{t,k}_{y_h}(\pi), l)$ we have $l < t$. By induction and fact that $\widetilde{\pi'}$ is generated by $\widetilde{\pi}_l$ we have $(\forall i \geq t) M_\varphi, \widetilde{\pi'}^i \models \alpha$. Thus, we have $M_\varphi, \pi'^t \models \mathrm{G}^h\alpha$. ■

Lemma 4.7. *Let M_φ be an abstract model, α an HLTL formula, π a path of M_φ. The following implication holds: $M_\varphi, \pi \models \alpha$ implies that for some $k \geq 0$ and $0 \leq l \leq k, M_\varphi, \pi_l \models_k \alpha$ with π_l being the k-prefix of π.*

Proof. The proof can be completed by the similar arguments as in the proof of Theorem 3.1 of [4]. ■

Lemma 4.8. *Let M_φ be an abstract model, α an HLTL formula, $Y \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma, \overline{\mathrm{C}}_\Gamma\}$, and π a path of M_φ. The following implication holds: $M_\varphi, \pi \models Y\alpha$ implies that for some $k \geq 0$ and $0 \leq l \leq k, M_\varphi, \pi_l \models_k Y\alpha$ with π_l being the k-prefix of π.*

Proof. The proof follows from Lemma 4.7 and Lemma 4 of [17]. ■

Lemma 4.9. *Let M_φ be an abstract model, $\psi = \mathcal{H}(\varphi)$ an HLTLK formula, and π a path. The following implication holds: $M_\varphi, \pi \models \psi$ implies that for some $k \geq 0$ and $0 \leq l \leq k, M_\varphi, \pi_l \models_k \psi$ with π_l being the k-prefix of π.*

Proof. We proceed by induction on the length of formulae φ. The lemma follows directly for the propositional variables and their negations. Assume that the hypothesis holds for all the proper subformulae of φ and consider φ to be of the following form:

1. $\varphi = \alpha \vee \beta \mid \alpha \wedge \beta \mid \alpha \mathrm{U}^h \beta \mid \mathrm{G}^h\alpha$. Straightforward by the induction hypothesis and Lemma 4.7.
2. Let $\varphi = Y\alpha$, and $Y, Y_1, \ldots, Y_n, Z \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma, \overline{\mathrm{C}}_\Gamma\}$. Moreover, let $Y_1\alpha_1, \ldots, Y_n\alpha_n$ be the list of all "top level" proper Y-subformulae of α (i.e., each $Y_i\alpha_i$ is a subformula of $Y\alpha$, but it is not a subformula of any subformula $Z\beta$ of $Y\alpha$, where $Z\beta$ is different from $Y\alpha$ and from $Y\alpha_i$ for $i = 1, \ldots, n$).

   If this list is empty, then α is a "pure" HLTL formula with no nested epistemic modalities. Hence, by Lemma 4.8 we have $M, \pi \models \psi$ implies that for some $k \geq 0$ and $0 \leq l \leq k, M, \pi_l \models_k \varphi$ with π_l being the k-prefix of π.

   Otherwise, introduce for each $Y_i\alpha_i$ a new proposition q_i, where $i = 1, \ldots, n$. By Lemma 1 of [17], we can augment with q_i the labelling of each state s of M initialising some path along which the epistemic formula $Y_i\alpha_i$ holds, and then translate the formula α to the formula α', which instead of each subformula $Y_i\alpha_i$ contains adequate propositions q_i. Therefore, we obtain "pure" HLTL formula. Hence, by Lemma 4.8 we have $M, \pi \models \varphi$ implies that for some $k \geq 0$ and $0 \leq l \leq k$, $M, \pi_l \models_k \varphi$ with π_l being the k-prefix of π. ■

The following theorem shows that for some particular bound the bounded and unbounded semantics are equivalent. A proof of the theorem follows from Lemmas 4.6 and 4.9.

THEOREM 4.10. *Let φ be an EMTLK formula, M_φ an abstract model, and $\psi = \mathcal{H}(\varphi)$ the HLTLK formula. The following equivalence holds: $M_\varphi \models \psi$ iff there exists $k \geq 0$ such that $M_\varphi \models_k \psi$.*

4.3. Translation to SAT

Let M_φ be an abstract model, ψ a HLTLK formula, and $k \geq 0$ a bound. The presented propositional encoding of the BMC problem for HLTLK is based on the BMC encoding of [24], and it relies on defining the propositional formula $[M_\varphi, \psi]_k := [M_\varphi^{\psi,\iota}]_k \wedge [\psi]_{M_\varphi,k}$, which is satisfiable if and only if $M_\varphi \models_k \psi$ holds.

The definition of $[M_\varphi, \psi]_k$ assumes that both the states and the joint actions of M_φ are encoded symbolically. This is possible, since both the sets of agents' states and the set of joint actions are finite. Also, since we work with a set of k-paths, we can bound the clocks valuation to the set $\mathbb{D} = \{0, \ldots, c{+}1\}$ with c being the largest constant appearing in any enabling condition or state invariants of all the agents and in intervals appearing in φ. Moreover, this definition assumes knowledge of the number of k-paths of M_φ that are sufficient to validate ψ. To this aim, as usually, we define the auxiliary function $\widehat{f_k} : HLTLK \to \mathbb{N}$ as $\widehat{f_k}(\psi) = f_k(\psi) + 1$, where the function $f_k : HLTLK \to \mathbb{N}$ is defined as follows. Let $p \in \mathcal{PV}'$. Then, $f_k(\top) = f_k(\bot) = f_k(p) = f_k(\neg p) = 0$, $f_k(\alpha \wedge \beta) = f_k(\alpha) + f_k(\beta)$; $f_k(\alpha \vee \beta) = max\{f_k(\alpha), f_k(\beta)\}$; $f_k(\alpha \mathrm{U}^h \beta) = k \cdot f_k(\alpha) + f_k(\beta) + 1$; $f_k(\mathrm{G}^h\alpha) = (k+1) \cdot f_k(\alpha) + 1$; $f_k(\overline{\mathrm{C}}_\Gamma\alpha) = f_k(\alpha) + k$; $f_k(Y\alpha) = f_k(\alpha) + 1$ for $Y \in \{\overline{\mathrm{K}}_{\mathbf{c}}, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma\}$.

Let us formally define the first conjunct of $[M_\varphi, \psi]_k$ (i.e., $[M_\varphi^{\psi,\iota}]_k$). We start by introducing the fundamental notation. First of all we assume that each state $s \in S_\varphi$ is represented by a vector $\mathbf{w} = ((\mathsf{w}_1, \mathsf{v}_1), \ldots, (\mathsf{w}_n, \mathsf{v}_n), (\mathsf{w}_\mathcal{E}, \mathsf{v}_\mathcal{E}))$ (called a *symbolic state*) of *symbolic local states*. Each symbolic local state $(\mathsf{w}_\mathbf{c}, \mathsf{v}_\mathbf{c})$ is a pair of vectors of propositional variables; the first vector $\mathsf{w}_\mathbf{c}$ encodes elements of $L_\mathbf{c}$, and the second vector $\mathsf{v}_\mathbf{c}$ encodes the clock valuations of agent $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$ over $\mathbb{D}$. Secondly, we assume that each joint action $\overline{a} = (a_1, \ldots, a_n, a_{\mathcal{E}}) \in Act$ is represented by a vector $\mathbf{a} = (\mathsf{a}_1, \ldots, \mathsf{a}_n, \mathsf{a}_{\mathcal{E}})$ (called a *symbolic action*) of *symbolic local actions*, where each symbolic local action $\mathsf{a}_{\mathbf{c}}$ is a vector of propositional variables. Next, we assume that the time action τ is represented by a proposition variable $\wp_\tau$, and we consider the vector $\mathbf{u} = (\mathsf{u}_1, \ldots, \mathsf{u}_t)$, which we call the *symbolic number*. It consists of propositional variables (called *natural variables*) of length $t = max(1, \lceil log_2(k+1) \rceil)$. Finally, we assume a symbolic representation of a k-path π_l, the number of which is j, and we call it the *j-th symbolic k-path* $\boldsymbol{\pi}_j = ((\mathbf{w}_{0,j}, \ldots, \mathbf{w}_{k,j}), \mathbf{u}_j)$, where $0 \leq j < \widehat{f}_k(\psi), 0 \leq i \leq k, \mathbf{w}_{i,j}$ is a symbolic state, and $\mathbf{u}_j$ is a symbolic number.

Let $\mathbf{w}$ and $\mathbf{w}'$ be two different symbolic states, $\mathbf{a}$ a symbolic action, and $\mathbf{u}$ a symbolic number. We assume definitions of the following auxiliary propositional formulae:

- $p(\mathbf{w})$ - encodes the set of states of M_φ in which $p \in \mathcal{PV}$ holds.
- $I_s(\mathbf{w})$ - encodes the state s of M_φ.
- $H_{\mathbf{c}}(\mathbf{w}, \mathbf{w}')$ - encodes the equality of two local states and two local clock valuations of agent $\mathbf{c} \in \mathbb{A}$.
- $H(\mathbf{w}, \mathbf{w}') := \bigwedge_{\mathbf{c} \in \mathbb{A}} H_{\mathbf{c}}(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states.
- $H_{h=0}(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states on local states and values of the original clocks, and the equality of values of the new clocks (i.e., clocks from Y) but the value of clock y_h.
- $H_{\neq h}(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states on local states and on values of the original clocks, and on the values of the new clocks with the potential exception of clock y_h. For clock y_h the formula guarantees that its value in the 2nd global state is greater than zero.
- $\mathcal{N}_j^{\sim}(\mathbf{u})$ - encodes that the value j is in the arithmetic relation $\sim \in \{<, \leqslant, =, \geqslant, >\}$ with the value represented by the symbolic number $\mathbf{u}$.
- $\mathcal{T}_{Act}(\mathbf{w}, \mathbf{a}, \mathbf{w}')$ - encodes the action transition relation of M_φ.
- $\mathcal{T}_\tau(\mathbf{w}, \wp_\tau, \mathbf{w}')$ - encodes the time transition relation of M_φ.
- $H_X(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states on local states and values of the original clocks.
- $\mathcal{L}_k^l(\boldsymbol{\pi}_j) := \mathcal{N}_l^{=}(\mathbf{u}_j) \wedge H_X(\mathbf{w}_{k,j}, \mathbf{w}_{l,j})$, where $\boldsymbol{\pi}_j$ is a jth symbolic k-path.

Having introduced the fundamental auxiliary propositional formulae, we can formally define the propositional formula $[M_\varphi^{\psi,\iota}]_k$, which encodes the unfolding of the transition relation of the abstract model M_φ $f_k(\psi)$-times to the depth k. Specifically, let $\mathbf{w}_{i,j}, \mathbf{a}_{i,j}$, and $\mathbf{u}_j$ be, respectively, symbolic states, symbolic actions, and symbolic numbers, for $0 \leq i \leq k$ and $0 \leq j < \widehat{f_k}(\psi)$. The formula $[M_\varphi^{\psi,\iota}]_k$, is defined as follows:

$$
\begin{aligned}
&[M_\varphi^{\psi,\iota}]_k := \bigvee_{s\in\iota} I_s(\mathbf{w}_{0,0}) \wedge \bigwedge_{j=0}^{\widehat{f_k}(\psi)-1} \bigvee_{l=0}^{k} \mathcal{N}_l^{=}(\mathbf{u}_j)\\
&\wedge \bigwedge_{j=0}^{\widehat{f_k}(\psi)-1} (\mathcal{T}_\tau(\mathbf{w}_{0,j}, \wp_\tau, \mathbf{w}_{1,j}) \wedge \bigwedge_{i=1}^{k-1} (\mathcal{T}_\tau(\mathbf{w}_{i,j}, \wp_\tau, \mathbf{w}_{i+1,j})\\
&\vee \mathcal{T}_{Act}(\mathbf{w}_{i,j}, \mathbf{a}_{i,j}, \mathbf{w}_{i+1,j})))\\
&\wedge \bigwedge_{i=1}^{k-2} (\mathcal{T}_\tau(\mathbf{w}_{i,j}, \wp_\tau, \mathbf{w}_{i+1,j}) \vee \mathcal{T}_\tau(\mathbf{w}_{i+1,j}, \wp_\tau, \mathbf{w}_{i+2,j}))
\end{aligned}
$$

Let us now formally define the second conjunct of $[M_\varphi, \psi]_k$ (i.e., $[\psi]_{M_\varphi,k}$), which encodes the bounded semantics of the HLTL formula ψ. In the definition of $[\psi]_{M_\varphi,k}$ we assume the same fundamental notation and the same crucial ancillary propositional formulae which have been introduced above. Additionally, we assume knowledge of auxiliary functions that are defined in [24]. Their purpose is to divide the set $A \subset \mathbb{N}_+$ of numbers of k-paths such that $|A| = f_k(\psi)$ into subsets needed for translating the subformulae of ψ. Their names and arguments are the following: $g_l(A,m), g_r(A,m), g_s(A) = A \setminus \{min(A)\}, h_k^{\mathrm{U}}(A,m), h_k^{\mathrm{G}}(A,m)$, where $A \subset \mathbb{N}_+$ is a finite non-empty set and $m \leq |A|$. Finally, let $F_k(\psi) = \{j \in \mathbb{N} \mid 0 \leq j < \widehat{f_k}(\psi)\}, [\alpha]_k^{[m,n,A]}$ denotes the translation of α along the n-th symbolic path $\boldsymbol{\pi}_n^m$ with the starting point m by using the set $A \subseteq F_k(\psi), n' = min(A), h_k^{\mathrm{U}} = h_k^{\mathrm{U}}(g_s(A), f_k(\beta))$, and $h_k^{\mathrm{G}} = h_k^{\mathrm{G}}(g_s(A), f_k(\alpha))$. The propositional formula $[\psi]_{M_\varphi,k}$ is defined as $[\psi]_k^{[0,0,F_k(\psi)]}$, where

$$
\begin{aligned}
&[\top]_k^{[m,n,A]} && := \top, \qquad [\bot]_k^{[m,n,A]} := \bot,\\
&[p]_k^{[m,n,A]} && := p(\mathbf{w}_{m,n}), \qquad [\neg p]_k^{[m,n,A]} := \neg p(\mathbf{w}_{m,n}),\\
&[\alpha \wedge \beta]_k^{[m,n,A]} && := [\alpha]_k^{[m,n,g_l(A,f_k(\alpha))]} \wedge [\beta]_k^{[m,n,g_r(A,f_k(\beta))]},\\
&[\alpha \vee \beta]_k^{[m,n,A]} && := [\alpha]_k^{[m,n,g_l(A,f_k(\alpha))]} \vee [\beta]_k^{[m,n,g_l(A,f_k(\beta))]},\\
&[\alpha \mathrm{U}^h \beta]_k^{[m,n,A]} && := \bigwedge_{j=0}^{m-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge\\
& && \quad \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge (\bigvee_{j=m}^{k} ([\beta]_k^{[j,n',h_k^{\mathrm{U}}(k)]} \wedge
\end{aligned}
$$

$$
\begin{aligned}
&\bigwedge_{i=m}^{j-1} [\alpha]_k^{[i,n',h_k^{\mathrm{U}}(i)]})\big) \vee \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})\wedge \\
&H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \big(\bigvee_{l=0}^{m-1} (\mathcal{L}_k^l(\boldsymbol{\pi}_{n'})\wedge \bigwedge_{j=0}^{l-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})\wedge \\
&H(\mathbf{w}_{l,n'}, \mathbf{w}_{k,n'}) \wedge \bigwedge_{j=l+1}^{m-1} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}))\big)\wedge \\
&\big(\bigvee_{j=0}^{m-1} (\mathcal{N}_j^{>}(\mathbf{u}_{n'}) \wedge [\beta]_k^{[j,n',h_k^{\mathrm{U}}(k)]} \wedge \bigwedge_{i=0}^{j-1} (\mathcal{N}_i^{>}(\mathbf{u}_{n'}) \rightarrow \\
&[\alpha]_k^{[i,n',h_k^{\mathrm{U}}(i)]}))\big) \wedge \bigwedge_{i=m}^{k} [\alpha]_k^{[i,n',h_k^{\mathrm{U}}(i)]},
\end{aligned}
$$

$$
\begin{aligned}
[\mathrm{G}^h\alpha]_k^{[m,n,A]} \quad := &\Big[\bigwedge_{j=0}^{m-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \bigwedge_{j=m+1}^{k} H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'})\wedge \\
&H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})\wedge \big(\bigvee_{l=m}^{k-1} (\mathcal{L}_k^l(\boldsymbol{\pi}_{n'})) \wedge \bigwedge_{j=m}^{k} [\alpha]_k^{[j,n',h_k^{\mathrm{G}}(j)]} \Big]\vee \\
&\Big[H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})\wedge \\
&\bigwedge_{j=m}^{k} [\alpha]_k^{[j,n',h_k^{\mathrm{G}}(j)]} \wedge \big(\bigvee_{l=0}^{m-1} (\mathcal{L}_k^l(\boldsymbol{\pi}_{n'}) \wedge \bigwedge_{j=0}^{l-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})\wedge \\
&H(\mathbf{w}_{l,n'}, \mathbf{w}_{k,n'}) \wedge \bigwedge_{j=l+1}^{m-1} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})\wedge \\
&\bigwedge_{j=l+1}^{m-1} [\alpha]_k^{[j,n',h_k^{\mathrm{G}}(j)]})\big)\Big],
\end{aligned}
$$

$$
\begin{aligned}
[\overline{\mathrm{K}}_{\mathbf{c}}\alpha]_k^{[m,n,A]} \quad &:= \bigvee_{s\in\iota_\varphi} I_s(\mathbf{w}_{0,n'}) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,n',g_s(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'})), \\
[\overline{\mathrm{D}}_{\Gamma}\alpha]_k^{[m,n,A]} \quad &:= \bigvee_{s\in\iota_\varphi} I_s(\mathbf{w}_{0,n'}) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,n',g_s(A)]} \wedge \bigwedge_{\mathbf{c}\in\Gamma} H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'})), \\
[\overline{\mathrm{E}}_{\Gamma}\alpha]_k^{[m,n,A]} \quad &:= \bigvee_{s\in\iota_\varphi} I_s(\mathbf{w}_{0,n'}) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,n',g_s(A)]} \wedge \bigvee_{\mathbf{c}\in\Gamma} H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'})), \\
[\overline{\mathrm{C}}_{\Gamma}\alpha]_k^{[m,n,A]} \quad &:= [\bigvee_{j=1}^{k} (\overline{\mathrm{E}}_{\Gamma})^j \alpha]_k^{[m,n,A]}.
\end{aligned}
$$

First of all, observe that in the translation of $\alpha \mathrm{U}^h \beta$ the propositional formula $\bigwedge_{j=0}^{m-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})$ encodes the k-path $(\Phi_{y_h}^{t,k}(\pi), l)$. Next, the propositional formula $\bigvee_{j=m}^{k}([\beta]_k^{[j,n',h_k^{\mathrm{U}}(k)]} \wedge \bigwedge_{i=m}^{j-1}[\alpha]_k^{[i,n',h_k^{\mathrm{U}}(i)]})$ encodes the part of the bounded semantics where we look for β on a k-path which is not a loop or the looping state is after the state t. Further, the propositional formula $\bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \; H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigvee_{l=0}^{m-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_{n'}) \wedge \bigwedge_{j=0}^{l-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge H(\mathbf{w}_{l,n'}, \mathbf{w}_{k,n'}) \wedge \bigwedge_{j=l+1}^{m-1} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}))$ encodes the k-path $(\Psi_{y_h}^{t,k}(\pi), l)$, which is a loop with $l < t$. Next, the propositional formula $\bigvee_{j=0}^{m-1}(\mathcal{N}_j^{>}(\mathbf{u}_{n'}) \wedge [\beta]_k^{[j,n',h_k^{\mathrm{U}}(k)]} \wedge \bigwedge_{i=0}^{j-1}(\mathcal{N}_i^{>}(\mathbf{u}_{n'}) \rightarrow [\alpha]_k^{[i,n',h_k^{\mathrm{U}}(i)]}))) \wedge \bigwedge_{i=m}^{k}[\alpha]_k^{[i,n',h_k^{\mathrm{U}}(i)]}$, encodes the part of the bounded semantics where we look for β on a k-path which is a loop with $l < t$. Thus, β must hold at some state j that is between states l and m, and α must hold at all the states form m to k, and from l to $j-1$.

Next, observe that in the translation of $\mathrm{G}^h \alpha$ the propositional formula $\bigwedge_{j=0}^{m-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \; H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \; \wedge \; \bigwedge_{j=m+1}^{k} \; H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge (\bigvee_{l=m}^{k-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_{n'}))$ encodes k-path $(\Phi_{y_h}^{t,k}(\pi), l)$, and it ensures that it is a loop with $l \geq t$. Further, the propositional formula $\bigwedge_{j=m}^{k}[\alpha]_k^{[j,n',h_k^{\mathrm{G}}(j)]}$ encodes the part of the bounded semantics where we ensure that α holds at all the states between the states m and k. Further, the propositional formula $H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \big(\bigvee_{l=0}^{m-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_{n'}) \wedge \bigwedge_{j=0}^{l-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \; \wedge H(\mathbf{w}_{l,n'}, \mathbf{w}_{k,n'}) \; \wedge \; \bigwedge_{j=l+1}^{m-1} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \; \wedge \; \clubsuit)\big)$ encodes the k-path $(\Psi_{y_h}^{t,k}(\pi), l)$, which is a loop with $l < t$. Next, the nested propositional formula $\clubsuit := \bigwedge_{j=l+1}^{m-1}[\alpha]_k^{[j,n',h_k^{\mathrm{G}}(j)]}$ encodes the part of the bounded semantics where we ensure that α holds between states $l+1$ and $m-1$. Lastly, the propositional formula $\bigwedge_{j=m}^{k}[\alpha]_k^{[j,n',h_k^{\mathrm{G}}(j)]}$ encodes the part of the bounded semantics where we ensure that α holds between states m and k.

Finally, observe that in the translation of $\overline{\mathrm{K}}_{\mathbf{c}} \alpha$ the propositional formula $\bigvee_{s \in \iota_\varphi} I_s(\mathbf{w}_{0,n'})$ ensures that we look for a new k-path that starts at an initial state. Next, the propositional formula $\bigvee_{j=0}^{k}([\alpha]_k^{[j,n',g_s(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'}))$ encodes the part of the bounded semantics where we ensure that α holds at some state j on the new initial k-path and that this state is in the epistemic relation with the state encoded by the symbolic state $\mathbf{w}_{m,n}$; the translation of other epistemic modalities follows from the translation of $\overline{\mathrm{K}}_{\mathbf{c}} \alpha$.

The following theorem guarantees that the BMC problem for HLTLK and for ATIS can be reduced to the SAT-problem. The theorem can be proven by induction on the length of the formula ψ. Moreover, the scheme of the proof follows closely the proof of Theorem 2 of [17].

THEOREM 4.11. *Let M_φ be an abstract model, and ψ a HLTLK formula. For every $k \in \mathbb{N}, M_\varphi \models_k \psi$ if, and only if, the propositional formula $[M_\varphi, \psi]_k$ is satisfiable.*

5. Experimental Results

5.1. The Timed Generic Pipeline Protocol (TGPP)

The specifications we checked for TGPP are given in the universal form, for which we verify the EMTLK formulae that are negated and interpreted existentially. For every specification given, there exists a counterexample in the model of the benchmark. Let n be the number of nodes. Then:

$\varphi_1 = \mathrm{G}(\mathrm{K}_P(\mathit{ProdSend} \Rightarrow \mathrm{F}_{[0,2n+2)}\mathit{ConsFree}))$. It expresses that Producer knows that each time Producer produces data, then Consumer receives this data not later than in $2n+1$ time units.

$\varphi_2 = \mathrm{G}_{[0,2n+3)}(\mathit{ConsFree} \Rightarrow \mathrm{K}_P(F(\mathit{ProdSend} \wedge \mathit{ConsFree})))$. It expresses that always in the interval $[0, 2n+3)$ if Consumer receives data, then Producer knows that eventually it will produce data again and Consumer will keep the old data.

$\varphi_3 = \mathrm{G}_{[2n-2,2n+2)}(\mathit{ConsReady} \Rightarrow \mathrm{K}_P(\mathrm{F}_{[0,2)}(\mathit{ConsFree})))$. It expresses that always in the interval $[2n-2, 2n+2)$ if Consumer is ready to receive data, then Producer knows that no later than one unit after that Consumer will receive data.

To apply the BMC method for the TGPP scenario and, e.g., for formula φ_1, first, we have to define the ATIS for the given TIS and for the negation of φ_1. To this aim, it is enough to extend the set of clocks, the set of actions, the protocol function, and the evolution function of the environment $\mathcal{E}$ by taking into account the intervals appearing in φ_1. Since there are two intervals in φ_1 (i.e., $I_1 = [0, \infty)$ and $I_2 = [2n-2, 2n+2)$) and the set $X_\mathcal{E}$ is empty, the new set $X'_\mathcal{E}$ is equal to $\{y_1, y_2\}$. The set $\mathit{Act'}_\mathcal{E}$ of actions is of the form $\mathit{Act}_\mathcal{E} \cup \{\{y_1\}, \{y_2\}, \{y_1, y_2\}\}$, and the protocol is defined as $P'_\mathcal{E}(\cdot) = \mathit{Act'}_\mathcal{E} = \{\epsilon_\mathcal{E}, \{y_1\}, \{y_2\}, \{y_1, y_2\}\}$. Finally, the local evolution function is defined as follows: $t'_\mathcal{E}(\cdot, \mathit{true}, B, \overline{a}) = \cdot$, if either $\mathit{act}_\mathcal{E}(\overline{a}) = \epsilon_\mathcal{E}$ and $B = \emptyset$ or $\mathit{act}_\mathcal{E}(\overline{a}) = B$ and $B \in \{\{y_1\}, \{y_2\}, \{y_1, y_2\}\}$. Having defined the ATIS for TIS and for

φ_1, it should be straightforward to infer the model M_{φ_1}. Further, we need to translate the negation of φ_1, denoted φ_1', (which is in EMTLK) into the HLTLK formula $\mathcal{H}(\varphi_1')$. Let $p = ProdSend, q = ConsFree$, and $\varphi_1' = \mathrm{F}\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{I_2}(\neg q))$.$\mathcal{H}(\varphi_1') = \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \mathcal{H}(\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{I_2}(\neg q)))) = \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P \mathcal{H}(p \wedge \mathrm{G}_{I_2}(\neg q))) = \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P(p \wedge \mathcal{H}(\mathrm{G}_{I_2}(\neg q)))) = \mathrm{F}^{y_1}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P(p \wedge \mathrm{G}^{y_2}(\neg p_{y_2 \in I_2} \vee \neg q)))$.

Finally, we apply the BMC method for the HLTLK formula $\mathcal{H}(\varphi_1')$ (similarly for $\mathcal{H}(\varphi_2')$ and $\mathcal{H}(\varphi_3')$) and for the model M_{φ_1} (resp. for M_{φ_2} and M_{φ_3}). Checking that the TGPP does not satisfy the properties φ_1, φ_2, and φ_3 can now be done by feeding a SAT solver with the propositional formulae generated in the way explained above.

5.2. The Timed Train Controller System (TTCS)

The specifications we checked for TTCS are given in the universal form, for which we verify the EMTLK formulae that are negated and interpreted existentially. Moreover, for every specification given, there exists a counterexample in the model of the benchmark.

$\varphi_4 = \mathrm{G}_{[0,2\delta+7)}(\bigwedge_{i=1}^{n-1} \bigwedge_{j=i+1}^{n} (\neg tunnel_i \vee \neg tunnel_j))$. It expresses that the system satisfies mutual exclusion property.

$\varphi_5 = \mathrm{G}_{[0,2\delta+7)}(tunnel_1 \implies \mathrm{K}_{T_1}(\mathrm{G}_{[0,\infty)}(\bigwedge_{j=2}^{n} \neg tunnel_j)))$. It expresses that always at time in the interval $[0, 2\delta + 7)$ if the $Train_1$ enters its critical section, then it knows that always in the future no other train will enter its critical section.

Analogously as for TGPP we apply the BMC method for the HLTLK formulae $\mathcal{H}(\neg\varphi_4)$ and $\mathcal{H}(\neg\varphi_5)$, and for the models M_{φ_4} and M_{φ_5} respectively. Checking that the TTCP does not satisfy the properties φ_4 and φ_5 is done by feeding a SAT solver with the propositional formulae generated in the way explained in Sect. 4.6.

5.3. Performance Evaluation

For the tests we used a computer with I7-3770 processor, 32 GB of RAM, and running Arch Linux 3.19.3. We set the CPU time limit to 3600 seconds. Moreover, we used PicoSAT [3] in version 957 to test the satisfiability of the propositional formulae generated by our SAT-based BMC encoding. We did not compare our results with other model checkers for MASs, e.g. MCMAS [16] or MCK [11], simply because they do not support EMTLK and TIS.

5.3.1. Timed Generic Pipeline Paradigm. The number of considered k-paths for all the tested properties is equal to 4. The length of the counterexample for formula φ_1 is is equal to $4n+7$. The length of the counterexample for formula φ_2 is equal to 12 if $n = 1$, and $4n + 10$ if $n > 1$. The length of the counterexample for formula φ_3 is equal to $n + 1$ if $n \in \{1, 2\}, 2n - 1$ if $n \in \{3, 4\}$, and $2n$ if $n > 4$.

5.3.2. Timed Train Controller System. The number of considered k-paths for the formula φ_4 is equal to 2 and for the formula φ_5 is equal to 3. The length of the counterexample for both the formulae φ_4 and φ_5 depends on δ and is equal to $2\delta+12$. We tested both of the formulae by scaling separately the number of trains and the value of the constant delta.

5.3.3. Performance Evaluation Summary. As one can see from the line charts in Figures 3, 4, and 5 showing the total time and the memory consumption for all the tested properties, the experimental results confirm that our new SAT-based BMC for TIS and for EMTLK is indeed feasible. Moreover, we can observe that as in the case of other known SAT-based BMC methods, this new method is also sensitive on the size of the counterexample, where the size of the counterexample is defined as the length of the k-path in the counterexample (i.e., the value k) multiplied by the number of k-paths (i.e., the value of the function $\widehat{f_k}$). The high efficiency of our method in the case of the formula φ_3 results from the shorter length of the counterexample.

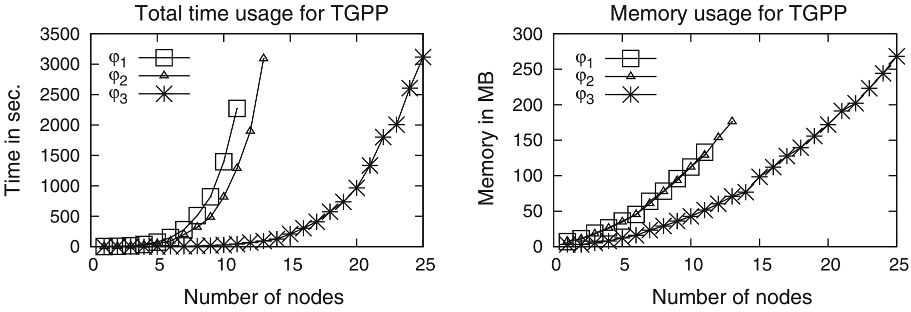

Figure 3. SAT-based BMC. TGPP with n nodes. All properties

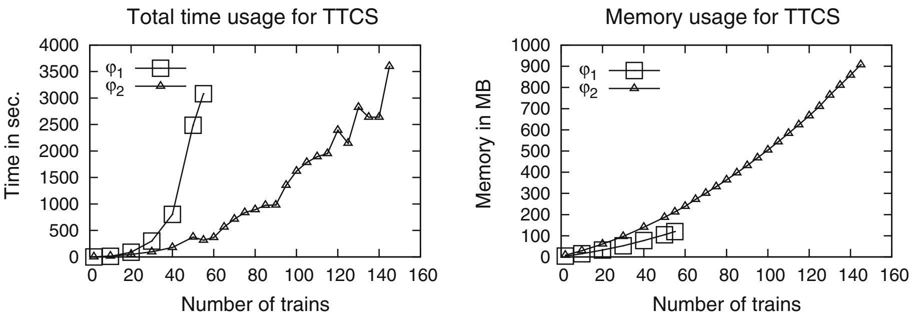

Figure 4. SAT-based BMC. TTCS with n trains, $\delta = 1$ and $\Delta = 5$. Both properties

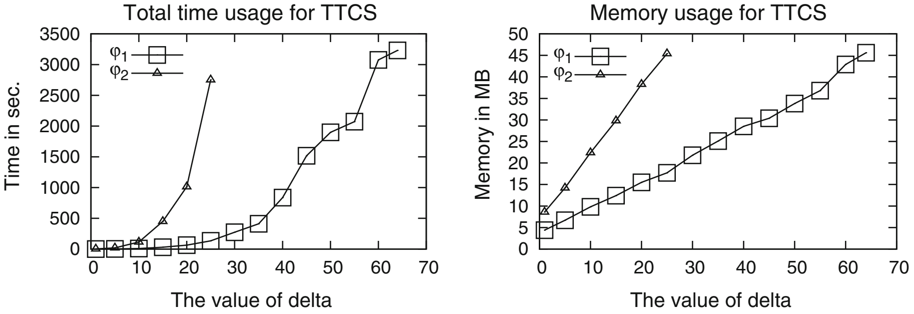

Figure 5. SAT-based BMC. TTCS with 2 trains. Scaling δ. $\Delta = \delta + 4$. Both properties

6. Conclusions

We have proposed TISs as a new formalism to model MASs with the agents that have real-time deadlines to achieve intended goals, and that possess their private clocks. Further, we have defined, implemented, and experimentally evaluated a SAT-based BMC for TISs and for properties expressed in EMTLK. The method is based on a translation of the existential model checking problem for EMTLK to the existential model checking problem for HLTLK, and then on the translation of the existential model checking problem for HLTLK to the SAT-problem.

In [15] a formalism of Real Time Interpreted Systems has been defined to model MASs with hard real-time deadlines. However, the agents of this model do not enjoy having access to the private clocks, namely, all the clocks are public. This constraint, in our opinion, violates the self governance (autonomy) of agents. Therefore, we plan to extend the TIS to a formalism that is able to model MASs with the agents that have hard real-time deadlines, and to define SAT-based BMC for this new formalism and for both the branching and the linear real time epistemic logics.

References

[1] Alur, R., and T. A. Henzinger, Real-time logics: complexity and expressiveness, *Information and Computation* 104:390–401, 1993.

[2] Alur, R., T. Feder, and T. Henzinger, The benefits of relaxing punctuality, *Journal of the ACM* 43(1):116–146, 1996.

[3] Biere, A., Picosat essentials, *Journal on Satisfiability, Boolean Modeling and Computation (JSAT)* 4:75–97, 2008.

[4] Biere, A., K. Heljanko, T. Junttila, T. Latvala, and V. Schuppan, Linear encodings of bounded ltl model checking, *Logical Methods in Computer Science* 2(5:5):1–64, 2006.

[5] Blackburn, P., M. de Rijke, and Y. Venema, *Modal Logic*, vol. 53 of *Cambridge Tracts in Theoretical Computer Science*, Cambridge University Press, Cambridge, 2001.

[6] Cabodi, G., P. Camurati, and S. Quer, Can BDDs compete with SAT solvers on bounded model checking?, in *Proceedings of the 39th Annual Design Automation Conference (DAC'2002)*, ACM, New York, 2002, pp. 117–122.

[7] Clarke, E., A. Biere, R. Raimi, and Y. Zhu, Bounded model checking using satisfiability solving, *Formal Methods in System Design* 19(1):7–34, 2001.

[8] Emerson, E. A., Temporal and modal logic, in J. van Leeuwen, (ed.), *Handbook of Theoretical Computer Science*, vol. B, Chap. 16, Elsevier Science Publishers, 1990, pp. 996–1071.

[9] Fagin, R., J. Y. Halpern, Y. Moses, and M. Y. Vardi, *Reasoning about Knowledge*, MIT Press, Cambridge, 1995.

[10] Furia, C. A., and P. Spoletini, Tomorrow and all our yesterdays: MTL satisfiability over the integers, in *Proceedings of the Theoretical Aspects of Computing (ICTAC'2008)*, vol. 5160 of *LNCS*. Springer-Verlag, New York, 2008, pp. 253–264.

[11] Gammie, P., and R. van der Meyden, MCK: Model checking the logic of knowledge, in *Proceedings of 16th International Conference on Computer Aided Verification (CAV'04)*, vol. 3114 of *LNCS*, Springer-Verlag, New York, 2004, pp. 479–483.

[12] Huang, X., and R. van der Meyden, The complexity of epistemic model checking: Clock semantics and branching time, in *Proceedings of the 2010 Conference on ECAI 2010: 19th European Conference on Artificial Intelligence*, IOS Press, Amsterdam, 2010, pp. 549–554.

[13] Levesque, H., A logic of implicit and explicit belief, in *Proceedings of the 6th National Conference of the AAAI*, Morgan Kaufman, Palo Alto, 1984, pp. 198–202.

[14] Lomuscio, A., and M. Sergot, Deontic interpreted systems, *Studia Logica* 75(1):63–92, 2003.

[15] Lomuscio, A., W. Penczek, and B. Woźna, Bounded model checking for knowledge and real time, *Artificial Intelligence* 171:1011–1038, 2007.

[16] Lomuscio, A., H. Qu, and F. Raimondi, Mcmas: A model checker for the verification of multi-agent systems, in *Proceedings of the 21st International Conference on Computer Aided Verification (CAV 2009)*, vol. 5643 of *LNCS*, Springer-Verlag, New York, 2009, pp. 682–688.

[17] Męski, A., W. Penczek, M. Szreter, B. Woźna-Szcześniak, and A. Zbrzezny, BDD- versus SAT-based bounded model checking for the existential fragment of linear temporal logic with knowledge: algorithms and their performance, *Autonomous Agents and Multi-Agent Systems* 28(4):558–604, 2014.

[18] Peled, D., All from one, one for all: On model checking using representatives, in *Proceedings of the 5th International Conference on Computer Aided Verification (CAV'93)*, vol. 697 of *LNCS*, Springer-Verlag, New York, 1993, pp. 409–423.

[19] Penczek, W., and A. Lomuscio, Verifying epistemic properties of multi-agent systems via bounded model checking, *Fundamenta Informaticae* 55(2):167–185, 2003.

[20] Tripakis, S., Minimization of timed systems. http://verimag.imag.fr/~tripakis/dea.ps.gz, 1998.

[21] Wooldridge, M., *An introduction to multi-agent systems*, Wiley, Chichester, 2002.

[22] Woźna-Szcześniak, B., and A. Zbrzezny, A translation of the existential model checking problem from MITL to HLTL, *Fundamenta Informaticae* 122(4):401–420, 2013.

[23] Woźna-Szcześniak, B., and A. Zbrzezny, Checking MTL properties of discrete timed automata via bounded model checking, *Fundamenta Informaticae* 135(4):553–568, 2014.

[24] Zbrzezny, A., A new translation from ECTL* to SAT, *Fundamenta Informaticae* 120(3–4):377–397, 2012.

B. Woźna-Szcześniak, A. Zbrzezny
Institute of Mathematics and Computer Science
Jan Długosz University
Al. Armii Krajowej 13/15
42-200 Częstochowa
Poland
bwozna@gmail.com; b.wozna@ajd.czest.pl

A. Zbrzezny
a.zbrzezny@ajd.czest.pl