Checking EMTLK properties of Timed Interpreted Systems via Bounded Model Checking *

Bożena Woźna-Szcześniak

IMCS, Jan Długosz University.
Al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland.
b.wozna@ajd.czest.pl

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 (TIS). 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 illustrate how TISs can be applied to the analysis of a variant of a Generic Timed Pipeline Paradigm scenario.

1 Introduction

The formalism of *interpreted systems* (IS) [5] was designed to model multi-agent systems (MASs) [13], and to reason about the agents' epistemic and temporal properties. The formalism of *timed interpreted systems* (TIS) extends IS 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 TIS, 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 *timed 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. A finite model, which is required by the model checking [3, 13] algorithms, can be obtained by defining an appropriate equivalence relation inducing a finite number of equivalence classes, and appropriate representation of equivalence classes that will preserve time and action transitions. In the paper, we call such a model the *abstract model*.

The main idea of SAT-based bounded model checking (BMC) methods [2, 12] consists in translating the existential model checking problem for a modal language and for a Kripke model to the satisfiability problem of a propositional formula, and taking advantage of the power of modern SAT-solvers. The usefulness

* Partly supported by National Science Center under the grant No. 2011/01/B/ST6/05317.

of SAT-based BMC for error tracking and complementarity to the BDD-based model checking have already been proven in several works, e.g. [1, 10].

To describe the requirements of MASs various extensions of standard temporal logics [4] with epistemic [5], doxastic [7], and deontic (to represent correct functioning behaviour) [9] modalities have been proposed. In this paper we consider MTLK which is an epistemic extension of Metric Temporal Logic (MTL) [6] 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 *timed models* generated by TISs.

The original contributions of the paper are as follows: (1) We define TIS as a model of MASs with the agents that have real-time deadlines to achieve intended goals. (2) We introduce two languages: MTLK and HLTLK - *hard reset* linear-time temporal epistemic logic. (3) We propose a SAT-based BMC technique for TIS and for the existential fragment of MTLK (called EMTLK). This BMC method consists of the following two steps: (1) We translate the EMTLK existential model checking problem over TIS to the HLTLK existential model checking problem over an *augmented timed interpreted system* (ATIS). This translation is based on [15], where a translation of the existential model checking problem for MITL and for timed automata to the existential model checking problem for HLTL and for *augmented timed automata* has been presented. (2) We define a SAT-based BMC algorithm for HLTLK and for ATIS[1].

The rest of the paper is organised as follows. In Section 2 we introduce TIS, the MTLK logic, and its subset EMTLK. In Section 3 we show how to translate the existential model checking problem for EMTLK to the existential model checking problem for HLTLK. In Section 4 we provide a BMC method for HLTLK and for ATIS. In Section 5 we apply the BMC technique to an example close to the multi-agent systems literature: a Generic Timed Pipeline Paradigm scenario. In the last section we conclude the paper with a short discussion and an outline of our future work.

2 Preliminaries

Let us start by fixing some notation used through the paper. $\mathbb{N}$ is the set of non-negative integers, $\mathbb{N}_+ = \mathbb{N}\backslash\{0\}$, $\mathcal{PV}$ is a set of propositional variables, and X is a finite set of non-negative integers 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 $\forall x \in X \backslash X'$, $v'(x) = v(x)$. 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: $\phi := x \sim c \mid \phi \wedge \phi$. Let v be

[1] We would like to point out that the presented model checking technique is based on the BMC method for EMTL and for discrete timed automata that has been published but only in the informal proceedings of the c&sp 2013 workshop [14].

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 $v \models \phi'$. Furthermore, let c_{max} be a constant, and $v, v' \in \mathbb{N}^{|X|}$ two clock valuations. We say that $v \simeq v'$ iff the following conditions holds for all $x \in X$: (1) $v(x) > c_{max}$ iff $v'(x) > c_{max}$, and (2) if $v(x) \leq c_{max}$ and $v'(x) \leq c_{max}$, then $v(x) = v'(x)$. Finally, by the *time successor* of v (written $succ(v)$) we denote the clock valuation v' such that $v \neq v'$ and $\forall x \in X$, if $v(x) \leq c_{max}$, then $v'(x) = v(x) + 1$, else $v'(x) = c_{max} + 1$.

Timed Interpreted Systems. Let $\mathcal{A} = \{1, \ldots, n, \mathcal{E}\}$ denote the non-empty and finite set of agents with $\mathcal{E}$ being a special agent that is used to model the environment in which the agents operate. The set of agents $\mathcal{A}$ constitute a multi-agent system (MAS). In the paper we use the *timed interpreted system* to model MAS. In this formalism, each agent $\mathbf{c} \in \mathcal{A}$ is modelled using a non-empty set $L_{\mathbf{c}}$ of *local states*, a non-empty set $\iota_{\mathbf{c}} \subseteq L_{\mathbf{c}}$ of initial states, a non-empty set $Act_{\mathbf{c}}$ of *possible actions* such that the special *null* action $\epsilon_{\mathbf{c}}$ belongs to $Act_{\mathbf{c}}$, a non-empty 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* $t_{\mathbf{c}} : L_{\mathbf{c}} \times \mathcal{C}(X_{\mathbf{c}}) \times 2^{X_{\mathbf{c}}} \times Act \to L_{\mathbf{c}}$ with $Act = \prod_{\mathbf{c} \in \mathcal{A}} Act_{\mathbf{c}}$ (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* $\mathcal{V}_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{\mathcal{PV}}$ 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 $t_{\mathbf{c}}(\ell_{\mathbf{c}}, \phi_{\mathbf{c}}, X, (a_1, \ldots, a_n, a_{\mathcal{E}})) = \ell_{\mathbf{c}}$ for $a_{\mathbf{c}} = \epsilon_{\mathbf{c}}$, any $\phi_{\mathbf{c}} \in \mathcal{C}(X_{\mathbf{c}})$, and any $X \in 2^{X_{\mathbf{c}}}$. Further, we assume that local states and clocks for $\mathcal{E}$ are public. Finally, we assume that the sets of clocks are pairwise disjoint.

For a given set of agents $\mathcal{A}$ and a set of propositional variables $\mathcal{PV}$, we define the *timed interpreted system* (TIS) as a tuple $(\{\iota_{\mathbf{c}}, L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c} \in \mathcal{A}})$. For a given TIS, $S = \prod_{\mathbf{c} \in \mathcal{A}} L_{\mathbf{c}} \times \mathbb{N}^{|X_{\mathbf{c}}|}$ defines a set of all *possible global states*. Next, if $s = ((\ell_1, v_1), \ldots, (\ell_n, v_n), (\ell_{\mathcal{E}}, v_{\mathcal{E}})) \in S$ and $\mathbf{c} \in \mathcal{A}$, then $l_{\mathbf{c}}(s) = \ell_{\mathbf{c}}$ and $v_{\mathbf{c}}(s) = v_{\mathbf{c}}$. Furthermore, for a given TIS we define a *timed model* as a tuple $M = (\iota, S, T, \mathcal{V})$, where $\iota = \prod_{\mathbf{c} \in \mathcal{A}} \iota_{\mathbf{c}} \times \{0\}^{|X_{\mathbf{c}}|}$ is the set of all possible initial global states, 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 $\mathcal{V}(s) = \bigcup_{\mathbf{c} \in \mathcal{A}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$, and $T \subseteq S \times (Act \cup \mathbb{N}) \times S$ is a total transition relation defined by action and time transitions. Namly, for $a \in Act$ and $\delta \in \mathbb{N}$:

1. Action transition: $(s, a, s') \in T$ iff for all $\mathbf{c} \in \mathcal{A}$, there exists a local transition $t_{\mathbf{c}}(l_{\mathbf{c}}(s), \phi_{\mathbf{c}}, X', a) = l_{\mathbf{c}}(s')$ 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 $v'_{\mathbf{c}}(s') \models \mathcal{I}(l_{\mathbf{c}}(s'))$.
2. Time transition: $(s, \delta, s') \in T$ iff for all $\mathbf{c} \in \mathcal{A}$, $l_{\mathbf{c}}(s) = l_{\mathbf{c}}(s')$ and $v_{\mathbf{c}}(s) \models \mathcal{I}(l_{\mathbf{c}}(s))$ and $v'_{\mathbf{c}}(s') = v_{\mathbf{c}}(s) + \delta$ and $v'_{\mathbf{c}}(s') \models \mathcal{I}(l_{\mathbf{c}}(s))$.

Given a TIS one can define the indistinguishability relation $\sim_{\mathbf{c}} \subseteq S \times S$ for agent $\mathbf{c}$ as follows: $s \sim_{\mathbf{c}} s'$ iff $l_{\mathbf{c}}(s') = l_{\mathbf{c}}(s)$ and $v_{\mathbf{c}}(s') \simeq v_{\mathbf{c}}(s)$.

A *run* of TIS is an infinite sequence $\rho = s_0 \stackrel{\delta_0,a_0}{\rightarrow} s_1 \stackrel{\delta_1,a_1}{\rightarrow} s_2 \stackrel{\delta_2,a_2}{\rightarrow} \dots$ of global states such that the following conditions hold for all $i \in \mathbb{N}$: $s_i \in S$, $a_i \in Act$, $\delta_i \in \mathbb{N}_+$, and there exists $s'_i \in S$ such that $(s_i, \delta, s'_i) \in T$ and $(s'_i, a, s_{i+1}) \in T$. 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.*

MTLK. Let $p \in \mathcal{PV}$, $\mathbf{c} \in \mathcal{A}$, $\Gamma \subseteq \mathcal{A}$, 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 release positive normal form is defined by the following grammar:

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

The temporal modalities U_I and R_I are named as the *bounded until* and the *bounded release*, respectively. The derived basic temporal modalities for *bounded eventually* and *bounded globally* are defined as follows: $\mathrm{F}_I \varphi \stackrel{def}{=} \top \mathrm{U}_I \varphi$ and $\mathrm{G}_I \varphi \stackrel{def}{=} \bot \mathrm{R}_I \varphi$. Hereafter, if the interval I is of the form $[0, \infty)$, then we omit it for the simplicity of the presentation. The epistemic modalities are named in the standard manner.

EMTLK is the existential fragment of MTLK, which is defined by the following grammar: $\varphi := \top \mid \bot \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \varphi \mathrm{U}_I \varphi \mid \varphi \mathrm{R}_I \varphi \mid \overline{\mathrm{K}}_{\mathbf{c}}\varphi \mid \overline{\mathrm{E}}_\Gamma \varphi \mid \overline{\mathrm{D}}_\Gamma \varphi \mid \overline{\mathrm{C}}_\Gamma \varphi$. Observe that EMTLK is existential only with respect to the epistemic modalities.

To define the satisfiability relation for MTLK, we define the notion of a *discrete path* λ_ρ *corresponding to run* ρ (this can be done in a unique way because of the assumption that the runs are strongly monotonic), and we assume the following definitions of epistemic relations: $\sim^E_\Gamma \stackrel{def}{=} \bigcup_{\mathbf{c} \in \Gamma} \sim_{\mathbf{c}}$, $\sim^C_\Gamma \stackrel{def}{=} (\sim^E_\Gamma)^+$ (the transitive closure of $\sim^E_\Gamma$), $\sim^D_\Gamma \stackrel{def}{=} \bigcap_{\mathbf{c} \in \Gamma} \sim_{\mathbf{c}}$, where $\Gamma \subseteq \mathcal{A}$.

Let $\Delta_0 = [b_0, b_1), \Delta_1 = [b_1, b_2), \dots$ 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 $t \in \Delta_i$. A *discrete path* (or *path*) λ_ρ *corresponding to* ρ is a mapping $\lambda_\rho : \mathbb{N} \to S$ such that $\lambda_\rho(t) = ((\ell^i_1, v^i_1 + t - b_i), \dots, (\ell^i_n, v^i_n + t - b_i), (\ell^i_{\mathcal{E}}, v^i_{\mathcal{E}} + t - b_i)) = s_i + t - b_i$, 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: $\forall i \in \mathbb{N}$, $\lambda^t_\rho(i) = \lambda_\rho(t + i)$. $\Pi(s)$ denotes the set of all the paths starting at $s \in S$, and $\Pi = \bigcup_{s^0 \in \iota} \Pi(s^0)$.

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:

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

A MTLK formula φ *existentially holds* in the model M (denoted $M \models \varphi$) iff $M, \lambda_\rho^0 \models \varphi$ for some path $\lambda_\rho \in \Pi$. The *existential model checking problem* asks whether $M \models \varphi$.

3 From EMTLK to HLTLK

In this section we show how to translate 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* (ATIS). We start by introducing the notion of ATIS.

Let $(\{\iota_{\mathbf{c}}, L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c}\in\mathcal{A}})$ be a TIS, φ an EMTLK formula, and m the number of intervals appearing in φ. An *augmented timed interpreted system* ATIS is defined as a tuple $(\{\iota_{\mathbf{c}}, L_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}\}_{\mathbf{c}\in\mathcal{A}}, \{X_{\mathbf{c}}, Act_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}\}_{\mathbf{c}\in\mathcal{A}\backslash\{\mathcal{E}\}}$, $X'_{\mathcal{E}}$, $Act'_{\mathcal{E}}, P'_{\mathcal{E}}, t'_{\mathcal{E}})$ 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.
- $Act'_{\mathcal{E}} = Act_{\mathcal{E}} \cup (2^Y \backslash \{\emptyset\})$; $Act' = \prod_{i=1}^n Act_i \times Act'_{\mathcal{E}}$.
- $P'_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act'_{\mathcal{E}}}$ is an extension of the protocol function $P_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act_{\mathcal{E}}}$ such that $(2^Y \backslash \{\emptyset\}) \subseteq P'_{\mathcal{E}}(\ell)$ 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 $t'_{\mathcal{E}}(\ell_{\mathcal{E}}, true, \mathcal{Y}, (\epsilon_1, \ldots, \epsilon_n, \mathcal{Y})) = \ell_{\mathcal{E}}$ for all $\mathcal{Y} \in 2^Y$ and $\mathcal{Y} \neq \emptyset$.

Now we are ready to define the abstract model for ATIS. Let φ be an EMTLK formula, $\mathcal{PV}' = \mathcal{PV} \cup \mathcal{PV}_y$ with $\mathcal{PV}_y = \{q_{y_h \in I_h} \mid h = 1, \ldots, m\}$ and m being a number of intervals appearing in φ, $\mathbb{D}_{\mathbf{c}} = \{0, \ldots, c_{\mathbf{c}} + 1\}$ with $c_{\mathbf{c}}$ being the largest constant appearing in any enabling condition or state invariants of agent $\mathbf{c}$ and in intervals appearing in φ, and $\mathbb{D} = \bigcup_{\mathbf{c}\in\mathcal{A}} \mathbb{D}_{\mathbf{c}}^{|X_{\mathbf{c}}|}$. The *abstract model* for ATIS is a tuple $M_\varphi = (\iota_\varphi, S_\varphi, T_\varphi, \mathcal{V}_\varphi)$, where $\iota_\varphi = \prod_{\mathbf{c}\in\mathcal{A}} \iota_{\mathbf{c}} \times \{0\}^{|X_{\mathbf{c}}|}$ is the set of all possible initial global states, $S_\varphi = \prod_{\mathbf{c}\in\mathcal{A}} L_{\mathbf{c}} \times \mathbb{D}_{\mathbf{c}}^{|X_{\mathbf{c}}|}$ is the set of all possible abstract 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 $p \in \bigcup_{\mathbf{c}\in\mathcal{A}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$ 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 $v_{\mathcal{E}}(y_h) \in I_h$, and $T_\varphi \subseteq S_\varphi \times (Act'' \times 2^Y) \times S_\varphi$, where $Act'' = \{\tau\} \cup Act$, is a total transition relation defined by action and time transitions. Let $a \in Act$ and $\mathcal{Y} \in 2^Y$. Then,

1. Action transition: $(s, (a, \mathcal{Y}), s') \in T_\varphi$ iff $(\forall \mathbf{c} \in \mathcal{A}\backslash\{\mathcal{E}\})$ $(\exists \phi_{\mathbf{c}} \in \mathcal{C}(X_{\mathbf{c}}))(\exists X'_{\mathbf{c}} \subseteq X_{\mathbf{c}})(t_{\mathbf{c}}(l_{\mathbf{c}}(s), \phi_{\mathbf{c}}, X'_{\mathbf{c}}, a) = l_{\mathbf{c}}(s')$ 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 $(\exists \phi_{\mathcal{E}} \in \mathcal{C}(X_{\mathcal{E}}))$ $(\exists X'_{\mathcal{E}} \subseteq X_{\mathcal{E}})$ $(t'_{\mathcal{E}}(l_{\mathcal{E}}(s), \phi_{\mathcal{E}}, X'_{\mathcal{E}} \cup \mathcal{Y}, a) = l_{\mathcal{E}}(s')$ and $v_{\mathcal{E}}(s) \models \phi_{\mathcal{E}} \wedge \mathcal{I}(l_{\mathcal{E}}(s))$ and $v'_{\mathcal{E}}(s') = v_{\mathcal{E}}(s)[X'_{\mathcal{E}} \cup \mathcal{Y} := 0]$ and $v'_{\mathcal{E}}(s') \models \mathcal{I}(l_{\mathcal{E}}(s')))$
2. Time transition: $(s, (\tau, \mathcal{Y}), s') \in T_\varphi$ iff $(\forall \mathbf{c} \in \mathcal{A})(l_{\mathbf{c}}(s) = l_{\mathbf{c}}(s')$ and $v_{\mathbf{c}}(s) \models \mathcal{I}(l_{\mathbf{c}}(s))$ and $succ(v_{\mathbf{c}}(s)) \models \mathcal{I}(l_{\mathbf{c}}(s)))$ and $(\forall \mathbf{c} \in \mathcal{A}\backslash\{\mathcal{E}\})$ $(v'_{\mathbf{c}}(s') = succ(v_{\mathbf{c}}(s)))$ and $v'_{\mathcal{E}}(s') = succ(v_{\mathcal{E}}(s))[\mathcal{Y} := 0]$.

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 $v_{\mathbf{c}}(s') = v_{\mathbf{c}}(s)$.

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

$$\varphi := \top \mid \bot \mid p \mid \neg p \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \mathrm{H}_h(\varphi \mathrm{U} \varphi) \mid \mathrm{H}_h(\varphi \mathrm{R} \varphi) \mid \overline{\mathrm{K}}_{\mathbf{c}} \varphi \mid \overline{\mathrm{E}}_\Gamma \varphi \mid \overline{\mathrm{D}}_\Gamma \varphi \mid \overline{\mathrm{C}}_\Gamma \varphi$$

The symbols U and R denote the *until* and *release* modalities, respectively. 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. The indexed symbol H_h denotes the *reset* modality representing setting to zero the clock number h. In addition, we introduce some useful derived temporal modalities: $\mathrm{H}_h \mathrm{G} \alpha \stackrel{def}{=} \mathrm{H}_h(\bot \mathrm{R} \alpha)$ (*always*), $\mathrm{H}_h \mathrm{F} \alpha \stackrel{def}{=} \mathrm{H}_h(\top \mathrm{U} \alpha)$ (*eventually*).

The HLTLK formulae are interpreted over the abstract model M_φ. Let $s_i = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^i))$ for all $i \geq 0$. Then, a *path* π in M_φ is a sequence $\pi = (s_0, s_1, \ldots)$ of states such that $(s_i, s_{i+1}) \in T_\varphi$, for each $i \in \mathbb{N}$. For a path π, $\pi(i)$ denotes the i-th state s_i of π, $\pi^i = (s_i, s_{i+1}, \ldots)$ 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 $\Pi_\varphi = \bigcup_{s^0 \in \iota_\varphi} \Pi_\varphi(s^0)$. Next, for $t \in \mathbb{N}$, $y \in Y$, and π in M_φ, we define the (unique) path $\Upsilon_y^t(\pi) = (s'_0, s'_1, \ldots)$ as follows. $(\forall j \in \mathbb{N})$ $((\forall \mathbf{c} \in \mathcal{A})$ $(\ell'^j_{\mathbf{c}} = \ell^j_{\mathbf{c}})$ and $(\forall \mathbf{c} \in \mathcal{A} \backslash \{\mathcal{E}\})(v'^j_{\mathbf{c}} = v^j_{\mathbf{c}})$ and

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

Let M_φ be the abstract model for ATIS, ψ a HLTL formula "connected" to φ, π a path in M_φ and $t \geq 0$. The satisfiability relation $\models$, which indicates truth of ψ in 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 (we omit the model M_φ for simplicity):

- $\pi^t \models \mathrm{H}_h(\alpha \mathrm{U} \beta)$ iff $(\exists i \geq t)(\widetilde{\pi}^i \models \beta$ and $(\forall t \leq j < i)$ $\widetilde{\pi}^j \models \alpha)$, where $\widetilde{\pi} = \Upsilon^t_{y_h}(\pi)$,
- $\pi^t \models \mathrm{H}_h(\alpha \mathrm{R} \beta)$ iff $(\forall i \geq t)(\widetilde{\pi}^i \models \alpha$ or $(\exists t \leq j < i)\widetilde{\pi}^j \models \beta)$, where $\widetilde{\pi} = \Upsilon^t_{y_h}(\pi)$,
- $\pi^t \models \overline{\mathrm{K}}_{\mathbf{c}} \alpha$ iff $(\exists \pi' \in \Pi_\varphi)(\exists i \geq 0)(\pi'(i) \sim_{\mathbf{c}} \pi(t)$ and $M, \pi'^i \models \alpha)$,
- $\pi^t \models \overline{Y}_\Gamma \alpha$ iff $(\exists \pi' \in \Pi_\varphi)(\exists i \geq 0)(\pi'(i) \sim^Y_\Gamma \pi(t)$ and $M, \pi'^i \models \alpha)$, where $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$.

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 $M_\varphi \models \psi$.

Translation. Having defined the HLTLK language, we can now introduce a translation ("connection") of the EMTLK formula φ into an HLTLK formula

$\psi = \mathcal{H}(\varphi)$. This translation preserves the existential model checking problem, i.e., the existential model checking of φ over the timed model for TIS can be reduced to the existential model checking of ψ over the abstract model for ATIS.

Formally, let φ be a EMTLK formula and $p \in \mathcal{PV}$. We translate the formula φ inductively into the HLTLK formula $\mathcal{H}(\varphi)$ in the following way: $\mathcal{H}(\top) = \top$, $\mathcal{H}(\bot) = \bot$, $\mathcal{H}(p) = p$, $\mathcal{H}(\neg p) = \neg p$, $\mathcal{H}(\alpha \vee \beta) = \mathcal{H}(\alpha) \vee \mathcal{H}(\beta)$, $\mathcal{H}(\alpha \wedge \beta) = \mathcal{H}(\alpha) \wedge \mathcal{H}(\beta)$, $\mathcal{H}(\alpha \mathrm{U}_{I_h} \beta) = \mathrm{H}_h(\mathcal{H}(\alpha) \mathrm{U} (\mathcal{H}(\beta) \wedge p_{y_h \in I_h}))$, $\mathcal{H}(\alpha \mathrm{R}_{I_h} \beta) = \mathrm{H}_h(\mathcal{H}(\alpha) \mathrm{R} (\neg p_{y_h \in I_h} \vee \mathcal{H}(\beta)))$, $\mathcal{H}(\overline{\mathrm{K}}_{\mathbf{c}} \alpha) = \overline{\mathrm{K}}_{\mathbf{c}} \mathcal{H}(\alpha)$, $\mathcal{H}(\overline{Y}_{\Gamma} \alpha) = \overline{Y}_{\Gamma} \mathcal{H}(\alpha)$, 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_h} operator ensures that: (1) the translation of β holds in the interval I_h, which is expressed by the requirement $\mathcal{H}(\beta) \wedge p_{y_h \in I_h}$; (2) the translation of α holds always before the translation of β. The translation of the R_{I_h} operator ensures that: (1) if the value of the clock y_h is in interval I_h, then the translation of β holds; (2) the translation of α does not have to become true in the interval I_h, but it may become true before the beginning of I_h.

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 corresponding HLTLK formula $\mathcal{H}(\varphi)$ over the abstract model for ATIS. The proof of the theorem can be completed by induction on the length of formula φ.

Theorem 1. *Let M be a timed model for TIS, φ an EMTLK formula, and M_φ the abstract model for ATIS. Then, $M \models \varphi$ iff $M_\varphi \models \mathcal{H}(\varphi)$.*

4 A SAT-based BMC method for HLTLK

Bounded semantics. Let $M_\varphi = (\iota_\varphi, S_\varphi, T_\varphi, \mathcal{V}_\varphi)$ be an abstract model for ATIS, $k \in \mathbb{N}$, and $0 \leq l \leq k$. 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 $(s_j, s_{j+1}) \in T_\varphi$ for each $0 \leq j < k$. Next, let $\pi(i) = ((\ell_1^i, v_1^i), \ldots, (\ell_n^i, v_n^i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^i))$ for all $i \leq k$. Then, a k-path π_l is a *loop* if $l < k$ and $(\forall \mathbf{c} \in \mathcal{A})(\ell_{\mathbf{c}}^k = \ell_{\mathbf{c}}^l)$ and $(\forall \mathbf{c} \in \mathcal{A} \backslash \{\mathcal{E}\})(v_{\mathbf{c}}^k = v_{\mathbf{c}}^l)$ and $v_{\mathcal{E}}^k \downarrow X_{\mathcal{E}} = v_{\mathcal{E}}^l \downarrow X_{\mathcal{E}}$, where $\downarrow X_{\mathcal{E}}$ denoted the projection of the clock valuation $v_{\mathcal{E}} : X_{\mathcal{E}} \cup Y \to \mathbb{D}$ on the clock valuation $v'_{\mathcal{E}} : X_{\mathcal{E}} \to \mathbb{D}$. Further, $\mathit{\Pi}_k(s)$ is the set of all the k-paths π_l with $\pi(0) = s$, and $\mathit{\Pi}_k = \bigcup_{s^0 \in \iota_\varphi} \mathit{\Pi}_k(s^0)$.

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. $(\forall 0 \leq j \leq k)((\forall \mathbf{c} \in \mathcal{A})(\ell'^j_{\mathbf{c}} = \ell^j_{\mathbf{c}})$ and $(\forall \mathbf{c} \in \mathcal{A} \backslash \{\mathcal{E}\})(v'^j_{\mathbf{c}} = v^j_{\mathbf{c}})$ and

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

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. $(\forall 0 \leq j \leq k)((\forall \mathbf{c} \in \mathcal{A})(\ell'^j_{\mathbf{c}} = \ell^j_{\mathbf{c}})$ and $(\forall \mathbf{c} \in \mathcal{A} \backslash \{\mathcal{E}\})(v'^j_{\mathbf{c}} = v^j_{\mathbf{c}})$ and

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

Let φ be an EMTLK formula, $\psi = \mathcal{H}(\varphi)$ a corresponding HLTLK formula, M_φ an abstract model, $k \geq 0$ a bound, $0 \leq t \leq k$, and $right(h)$ denote the right end of the h-th interval appearing in φ. 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:

- $\pi_l^t \models_k \mathrm{H}_h(\alpha \mathrm{U} \beta)$ 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 $(\forall t \leq j \leq k)$ $\widetilde{\pi_l}^j \models_k \alpha]$,
- $\pi_l^t \models_k \mathrm{H}_h(\alpha \mathrm{R} \beta)$ iff $[\widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi)$ and $(\exists t \leq i \leq k)$ $(\widetilde{\pi_l}^i \models_k \alpha$ and $(\forall t \leq j \leq i)$ $\widetilde{\pi_l}^j \models_k \beta)]$ or $[\pi_l$ is a loop with $l < t$ and $\widetilde{\pi} = \Psi_{y_h}^{t,k}(\pi)$ and $(\exists l < i < t)$ $(\widetilde{\pi_l}^i \models_k \alpha$ and $(\forall l \leq j \leq i)$ $\widetilde{\pi_l}^j \models_k \beta)$ and $(\forall t \leq j \leq k)$ $\widetilde{\pi_l}^j \models_k \beta]$ or $[\widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi)$ and $right(h) \leq v'^k_{\mathcal{E}}(y_h)$ and $(\forall t \leq i \leq k)$ $\widetilde{\pi_l}^i \models_k \beta]$ or $[right(h) > v'^k_{\mathcal{E}}(y_h)$ and π_l is a loop with $t \leq l < k$ and $\widetilde{\pi} = \Phi_{y_h}^{t,k}(\pi)$ and $(\forall t \leq i \leq k)\widetilde{\pi_l}^i \models_k \beta]$ or $[right(h) > v'^k_{\mathcal{E}}(y_h)$ and π_l is a loop with $l < t$ and $\widetilde{\pi} = \Psi_{y_h}^{t,k}(\pi)$ and $(\forall t \leq i \leq k)$ $\widetilde{\pi_l}^i \models_k \beta$ and $(\forall l < i < t)$ $\widetilde{\pi_l}^i \models_k \beta]$,
- $\pi_l^t \models \overline{\mathrm{K}}_{\mathbf{c}} \alpha$ 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 $M_\varphi \models_k \psi$.

The following theorem shows that for some particular bound the bounded and unbounded semantics are equivalent. The theorem can be proven by induction on the length of the formula ψ.

Theorem 2. *Let φ be an EMTLK formula, M_φ an abstract model, and $\psi = \mathcal{H}(\varphi)$ a HLTLK formula. Then, the following equivalence holds: $M_\varphi \models \psi$ iff there exists $k \geq 0$ such that $M_\varphi \models_k \psi$.*

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 [16], and it relies on defining the propositional formula $[M_\varphi, \psi]_k := [M_\varphi^{\psi,\iota_\varphi}]_k \wedge [\psi]_{M_\varphi,k}$, which is satisfiable if and only if $M_\varphi \models_k \psi$ holds.

The definition of $[M_\varphi^{\psi,\iota_\varphi}]_k$ assumes that both the states and the joint actions of M_φ are encoded symbolically. This is possible, since both the set of states and the set of joint actions are finite; we recall that the set $\mathbb{D}$ of clock valuations is finite. Formally, let $\mathbf{c} \in \mathcal{A}$. Then, 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*, where each symbolic local state $(\mathsf{w}_\mathbf{c}, \mathsf{v}_\mathbf{c})$ is a pair of vectors of propositional variables; the first element encodes local states of $L_\mathbf{c}$ and the second element encodes the clock valuations over $\mathbb{D}_\mathbf{c}$. Next, each action $a \in Act \cup \{\tau\}$ 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. Moreover, each action $a \in Act' \setminus Act$ is represented by a vector $\mathbf{y} = (\mathsf{y}_1, \ldots, \mathsf{y}_r)$ of propositional variables (called a *symbolic clock action*), whose length $r = max(1, \lceil log_2(|2^Y|)\rceil)$. Further, in order to define $[M_\varphi^{\psi,\iota_\varphi}]_k$ we need to specify the number of k-paths of M_φ that are sufficient to validate ψ. To calculate the number, we define the following auxiliary function $f_k : HLTLK \to \mathbb{N}$: $f_k(\top) = f_k(\bot) = f_k(p) = f_k(\neg p) = 0$, where $p \in \mathcal{PV}'$; $f_k(\alpha \wedge \beta) = f_k(\alpha) + f_k(\beta)$; $f_k(\alpha \vee \beta) = max\{f_k(\alpha), f_k(\beta)\}$; $f_k(\mathrm{H}_h(\alpha \mathrm{U} \beta)) = k \cdot f_k(\alpha) + f_k(\beta) + 1$; $f_k(\mathrm{H}_h(\alpha \mathrm{R} \beta)) = (k+1) \cdot f_k(\beta) + f_k(\alpha) + 1$; $f_k(\overline{\mathrm{C}}_\Gamma \alpha) = f_k(\alpha) + k$; $f_k(Y\alpha) = f_k(\alpha) + 1$ for $Y \in \{\overline{\mathrm{K}}_\mathbf{c}, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma\}$. Now, since in the BMC method we deal with the existential validity, the number of k-paths sufficient to validate ψ is given by the function $\widehat{f_k} : HLTLK \to \mathbb{N}$ that is defined as $\widehat{f_k}(\psi) = f_k(\psi) + 1$.

Further, we need to represent k-paths π_l in a symbolic way. We call this representation a *j-th symbolic k-path* $\boldsymbol{\pi}_j$ and define it as a pair $((\mathbf{w}_{0,j}, \mathbf{a}_{0,j}, \mathbf{y}_{0,j}, \ldots, \mathbf{w}_{k,j}, \mathbf{a}_{k,j}, \mathbf{y}_{k,j}), \mathbf{u}_j)$, where $\mathbf{w}_{i,j}$, $\mathbf{a}_{i,j}$, $\mathbf{y}_{i,j}$ are symbolic states, symbolic actions, symbolic clock actions, respectively, and $\mathbf{u}_j$ is a *symbolic number*, for $0 \leq j < \widehat{f_k}(\psi)$ and $0 \leq i \leq k$. The *symbolic number* $\mathbf{u}_j$ is a vector $\mathbf{u}_j = (\mathsf{u}_{1,j}, \ldots, \mathsf{u}_{t,j})$ of propositional variables, whose length t equals to $max(1, \lceil log_2(k+1)\rceil)$.

Let $\mathbf{w}$ and $\mathbf{w}'$ be two different symbolic states, $\mathbf{a}$ a symbolic action, $\mathbf{y}$ a symbolic clock action, and $\mathbf{u}$ a symbolic number. Moreover, let $Ix_\mathbf{c}$ ($Vx_\mathbf{c}$) denote the set of indices of propositional variables that encodes local states (clock valuations) of agent $\mathbf{c}$. 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.
- $H_\mathbf{c}(\mathbf{w}, \mathbf{w}') = \bigwedge_{i \in Ix_\mathbf{c}} \mathsf{w}_\mathbf{c}[i] \Leftrightarrow \mathsf{w'}_\mathbf{c}[i] \wedge \bigwedge_{i \in Vx_\mathbf{c}} \mathsf{v}_\mathbf{c}[i] \Leftrightarrow \mathsf{v'}_\mathbf{c}[i]$ - encodes the equivalence of two local states and two local clock valuations of agent $\mathbf{c} \in \mathcal{A}$.
- $H(\mathbf{w}, \mathbf{w}') := \bigwedge_{\mathbf{c} \in \mathcal{A}} H_\mathbf{c}(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states.
- $H_X(\mathbf{w}, \mathbf{w}') = \bigwedge_{\mathbf{c} \in \mathcal{A} \setminus \{\mathcal{E}\}} H_\mathbf{c}(\mathbf{w}, \mathbf{w}') \wedge \bigwedge_{i \in Ix_\mathcal{E}} \mathsf{w}_\mathcal{E}[i] \Leftrightarrow \mathsf{w'}_\mathcal{E}[i] \wedge \bigwedge_{i \in Vx_\mathbf{c} \downarrow X_\mathcal{E}} \mathsf{v}_\mathcal{E}[i] \Leftrightarrow \mathsf{v'}_\mathcal{E}[i]$ - encodes equality of two global states on local states and values of the original clocks.

- $H_{h=0}(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states on local states and values of the original clocks (i.e., clocks from $\bigcup_{\mathbf{c}\in\mathcal{A}} X_{\mathbf{c}}$), 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 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 $\mathbf{u}$.
- $\mathcal{L}_k^l(\boldsymbol{\pi}_n) := \mathcal{N}_l^{=}(u_n) \wedge H_X(\mathbf{w}_{k,n}, \mathbf{w}_{l,n})$.
- $\mathcal{T}(\mathbf{w}, (\mathbf{a}, \mathbf{y}), \mathbf{w}')$ - encodes the transition relation of M_φ.

Let $F_k(\psi) = \{j \in \mathbb{N} \mid 1 \leq j \leq \widehat{f_k}(\psi)\}$, $\mathbf{w}_{i,j}$, $\mathbf{a}_{i,j}$, $\mathbf{y}_{i,j}$ and $\mathbf{u}_j$ be, respectively, symbolic states, symbolic actions, symbolic clock actions, and symbolic numbers, for $0 \leq i \leq k$ and $j \in F_k(\psi)$. The formula $[M_\varphi^{\psi,\iota_\varphi}]_k$, which encodes the unfolding of the transition relation of M_φ $\widehat{f_k}(\psi)$-times to the depth k, is defined as follows:

$$[M_\varphi^{\psi,\iota_\varphi}]_k := \bigvee_{s\in\iota_\varphi} I_s(\mathbf{w}_{0,0}) \wedge \bigvee_{j=1}^{\widehat{f_k}(\psi)} H(\mathbf{w}_{0,0}, \mathbf{w}_{0,j}) \wedge \bigwedge_{j=1}^{\widehat{f_k}(\psi)} \bigvee_{l=0}^{k} \mathcal{N}_l^{=}(\mathbf{u}_j) \wedge \bigwedge_{j=1}^{\widehat{f_k}(\psi)} \bigwedge_{i=0}^{k-1} \mathcal{T}(\mathbf{w}_{i,j}, (\mathbf{a}_{i,j}, \mathbf{y}_{i,j}), \mathbf{w}_{i+1,j})$$

The next step is a translation of a HLTLK formula ψ to a propositional formula $[\psi]_{M_\varphi,k} := [\psi]_k^{[0,1,F_k(\psi)]}$, where $[\alpha]_k^{[m,n,A]}$ denotes the translation of α along the n-th symbolic path $\boldsymbol{\pi}_n^m$ with the starting point m by using the set $A \subseteq F_k(\psi)$. To define $[\psi]_k^{[0,1,F_k(\psi)]}$, we have to know how to divide the set $F_k(\psi)$ into subsets needed for translating the subformulae of ψ. To accomplish this goal we use some auxiliary functions (g_l, g_r, g_s, h_k^{U}, h_k^{R}) that were defined in [16].

Let M_φ be an abstract model, ψ a HLTLK formula, and $k \geq 0$ a bound. Moreover, let $cl(\mathsf{v}_\mathcal{E}, h)$ denote the fragment of the local symbolic state $(\mathsf{w}_\mathcal{E}, \mathsf{v}_\mathcal{E})$ of $\mathcal{E}$ that encodes the h-th clock from the set Y. We define inductively the translation of ψ over a path number $n \in F_k(\psi)$ starting at the symbolic state $\mathbf{w}_{m,n}$ as shown below, where $A \subseteq F_k(\psi)$, $n' = min(A)$, and $h_k^{\mathrm{U}} = h_k^{\mathrm{U}}(g_s(A), f_k(\beta))$, and $h_k^{\mathrm{R}} = h_k^{\mathrm{R}}(g_s(A), f_k(\alpha))$; the translation of propositional operators is as in [16], so, we omit it.

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

$\wedge \bigwedge_{i=0}^{j}(\mathcal{N}_i^{>}(\mathbf{u}_{n'}) \rightarrow [\beta]_k^{[i,n',h_k^{\mathrm{R}}(i)]}))) \wedge \bigwedge_{i=m}^{k}[\beta]_k^{[i,n',h_k^{\mathrm{R}}(i)]}\Big] \vee \Big[\bigwedge_{j=0}^{m-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'})$
$\wedge H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \mathcal{N}^{\leq}_{right(h)}(cl(\mathbf{v}_{\mathcal{E}}^{k,n'}, h)) \wedge \bigwedge_{j=m}^{k}$
$[\beta]_k^{[j,n',h_k^{\mathrm{R}}(j)]}\Big] \vee \Big[\bigwedge_{j=0}^{m-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigwedge_{j=m+1}^{k}$
$H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \mathcal{N}^{>}_{right(h)}(cl(\mathbf{v}_{\mathcal{E}}^{k,n'}, h)) \wedge (\bigvee_{l=m}^{k-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_{n'})) \wedge \bigwedge_{j=m}^{k}[\beta]_k^{[j,n',h_k^{\mathrm{R}}(j)]}\Big] \vee$
$\Big[\mathcal{N}^{>}_{right(h)}(cl(\mathbf{v}_{\mathcal{E}}^{k,n'}, h)) \wedge H_{h=0}(\mathbf{w}_{m,n}, \mathbf{w}_{m,n'}) \wedge \bigwedge_{j=m+1}^{k} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge$
$\bigwedge_{j=m}^{k}[\beta]_k^{[j,n',h_k^{\mathrm{R}}(j)]} \wedge \big(\bigvee_{l=0}^{m-1}(\mathcal{L}_k^l(\boldsymbol{\pi}_{n'}) \wedge \bigwedge_{j=0}^{l-1} H(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge H(\mathbf{w}_{l,n'}, \mathbf{w}_{k,n'}) \wedge$
$\bigwedge_{j=l+1}^{m-1} H_{\neq h}(\mathbf{w}_{j,n}, \mathbf{w}_{j,n'}) \wedge \bigwedge_{j=l+1}^{m-1}[\beta]_k^{[j,n',h_k^{\mathrm{R}}(j)]})\Big)\Big],$

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

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.

Theorem 3. *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.*

Our encoding of the HLTLK formulae is defined recursively over: (1) the structure of a HLTLK formula ψ; (2) the current position m of the n-th symbolic k-path; (3) the set A of symbolic k-paths, which is initially equal to $F_k(\psi)$. Further, our encoding does not translate looping and non-looping witnesses separately, but it combines both of them. Next, it is parameterised by the bound $k \in \mathbb{N}$, the set A of symbolic k-paths, and closely follows the bounded semantics. Therefore, for fixed n, m, k and A, each subformula α of ψ requires the constraints of size $O(k \cdot f_k(\psi))$ using the encoding of α at various positions. Moreover, since the encoding of a subformula α is only dependent on m, n, k, and A, and, multiple occurrences of the encoding of α over the same set of parameters can be shared, the overall size can be bounded by $O(|\psi| \cdot k \cdot f_k(\psi))$. Further the size of the formula $[M_\varphi, \psi]_k$ is bounded by $O(|T| \cdot k \cdot f_k(\psi) + |\psi| \cdot k \cdot f_k(\psi))$.

5 Example

We adapted the scenario of *a generic pipeline paradigm* [11], and we called it the *generic timed pipeline paradigm* (GTPP). The GTPP involves $n + 2$ agents: the Producer that is able to produce data ($ProdReady$) within certain time interval ($[a, b]$) or being inactive, the Consumer that is able to receive data ($ConsReady$) within certain time interval ($[c, d]$) or being inactive within certain time interval ($[g, h]$), and a chain of n intermediate Nodes which can be ready for receiving data ($Node_iReady$) within certain time interval ($[c, d]$), processing data ($Node_iProc$) within certain time interval ($[e, f]$), or sending data ($Node_iSend$),

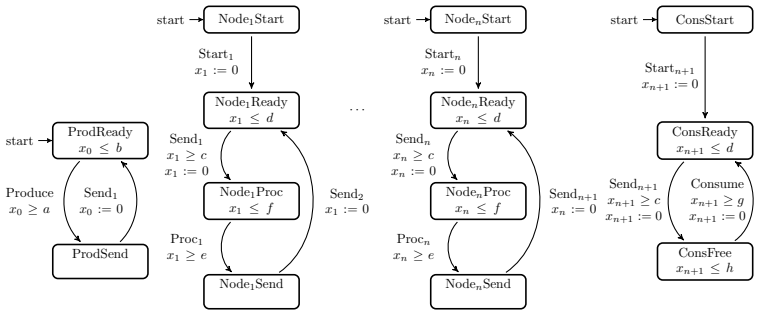

Fig. 1. A Generic Timed Pipeline Paradigm Scenario

communicating over a possibly faulty communication channel (the environment). The example can be scaled by adding intermediate 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, Consumer, and of the intermediate Nodes.

Fig. 1 shows the local states, the possible actions, the local clocks, the clock constraints, invariants, and the protocol for each agent, but for the environment $\mathcal{E}$. Null actions are omitted in the figure. Further, we assume that the following local states $ProdReady$, $Node_iStart$, and $ConsStart$ are initial, respectively, for Producer, Node i, and Consumer; hereafter, let P, C, and Ni denote, respectively, Producer, Consumer, and the i-th Node.

For the environment $\mathcal{E}$, to simplify the presentation, we shall consider just one local state: $L_{\mathcal{E}} = \{\cdot\} = \iota_{\mathcal{E}}$. Thus, 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 actions for $\mathcal{E}$ correspond to the transmission of data between agents on the unreliable communication channel. The set of actions for $\mathcal{E}$ is $Act_{\mathcal{E}} = \{\leftrightarrow, -\}$, where $\leftrightarrow$ represents the action in which the channel transmits any data successfully trough the channel, and $-$ represents the action in which the channel loses data. Thus, the set $Act = Act_P \times \prod_{i=1}^{n} Act_{Ni} \times Act_C \times Act_{\mathcal{E}}$ with $Act_P = \{Produce, Send_1, \epsilon_P\}$, $Act_C = \{Start_{n+1}, Send_{n+1}, Consume, \epsilon_C\}$, and $Act_{Ni} = \{Start_i, Send_i, Send_{i+1}, Proc_i, \epsilon_{Ni}\}$ defines the set of joint actions for the scenario. Moreover, the local protocols of $\mathcal{E}$ is the following: $P_{\mathcal{E}}(\cdot) = Act_{\mathcal{E}}$.

Let $state$ denote a local state of an agent, $\widehat{a} \in Act$, and $act_P(\widehat{a})$, $act_{Ni}(\widehat{a})$, and $act_C(\widehat{a})$, respectively, denote an action of Producer, Node i, and Consumer. In the TIS model of the GTPP scenario we assume the following local evaluation functions (we provide definitions for $Producer$ and $Consumer$, the remaining ones are equally straightforward):

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

- $t_C(state, true, \emptyset, \widehat{a}) = state$, if $act_C(\widehat{a}) = \epsilon_C$
- $t_C(ConsStart, true, \{x_{n+1}\}, \widehat{a}) = ConsReady$, if $act_C(\widehat{a}) = Start_{n+1}$
- $t_C(ConsReady, x_{n+1} \geq c, \{x_{n+1}\}, \widehat{a}) = ConsFree$, if $act_C(\widehat{a}) = Send_{n+1}$ and $act_{Nn}(\widehat{a}) = Send_{n+1}$
- $t_C(ConsFree, x_{n+1} \geq g, \{x_{n+1}\}, \widehat{a}) = ConsReady$, if $act_C(\widehat{a}) = Consume$

It should be straightforward to infer the timed model that is induced by the informal description of the GTPP scenario together with the local states, actions, clocks, protocols, and local evolution functions defined above. Next, in the timed model of the scenario we assume the following set of proposition variables: $\mathcal{PV} = \{ProdSend, ConsReady, ConsFree\}$ with the following interpretation:

- $(M, s) \models ProdSend$ if $l_{Producer}(s) = ProdSend$,
- $(M, s) \models ConsReady$ if $l_{Consumer}(s) = ConsReady$,
- $(M, s) \models ConsFree$ if $l_{Consumer}(s) = ConsFree$.

The specifications we may be interested in checking, for the described benchmark are given in the universal form, for which we verify the EMTLK formulae that are negated and interpreted existentially. Let n be the number of nodes. Then:

φ_1 $= \mathrm{G}(\mathrm{K}_P(ProdSend \Rightarrow \mathrm{F}_{[2n+1,2n+2)}ConsFree))$. It expresses that Producer knows that each time Producer produces data, then Consumer receives this data in $2n + 1$ time units.

φ_2 $= \mathrm{G}(\mathrm{K}_P(ProdSend \Rightarrow \mathrm{F}_{[2n+1,2n+2)}(ConsFree \wedge \mathrm{F}_{[1,2)}ConsReady)))$. It expresses that Producer knows that each time Producer produces data, then Consumer receives this data in $2n + 1$ time units and one unit after that it will be ready to receive another data.

To apply the BMC method for the above scenario and, e.g, for formula φ_1, we first have to define an augmented TIS 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. Now, since there are two intervals in φ_1 (i.e., $I_1 = [0, \infty)$ and $I_2 = [2n + 1, 2n + 2)$) and the set $X_{\mathcal{E}}$ is empty, the new set $X'_{\mathcal{E}}$ is equal to $\{y_1, y_2\}$. Moreover, the set of actions is of the form $Act'_{\mathcal{E}} = Act_{\mathcal{E}} \cup \{\{y_1\}, \{y_2\}, \{y_1, y_2\}\}$, and the protocol is defined as $P'_{\mathcal{E}}(\cdot) = Act'_{\mathcal{E}} = \{\leftrightarrow, -, \{y_1\}, \{y_2\}, \{y_1, y_2\}\}$. Finally, the local evolution function is defined as follows: $t'_{\mathcal{E}}(\cdot, true, \mathcal{Y}, \widehat{a}) = \cdot$, if $\widehat{a} \neq \overline{\epsilon}$ and $act_{\mathcal{E}}(\widehat{a}) = \mathcal{Y}$ and $\mathcal{Y} \in \{\{y_1\}, \{y_2\}, \{y_1, y_2\}\}$.

Having defined the ATIS for the GTPP scenario and for φ_1, it should be straightforward to infer the abstract 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 $\mathcal{H}(\varphi'_1)$. Namely, let $p = ProdSend$, $q = ConsFree$, and $\varphi'_1 = \mathrm{F}\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{[2n+1,2n+2)}(\neg q))$, we have $\mathcal{H}(\mathrm{F}\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{[2n+1,2n+2)}(\neg q))) = \mathrm{H}_{y_1}\mathrm{F}(p_{y_1 \in I_1} \wedge \mathcal{H}(\overline{\mathrm{K}}_P(p \wedge \mathrm{G}_{[2n+1,2n+2)}(\neg q)))) = \mathrm{H}_{y_1}\mathrm{F}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P\mathcal{H}(p \wedge \mathrm{G}_{[2n+1,2n+2)}(\neg q))) = \mathrm{H}_{y_1}\mathrm{F}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P(p \wedge \mathcal{H}(\mathrm{G}_{[2n+1,2n+2)}(\neg q)))) = \mathrm{H}_{y_1}\mathrm{F}(p_{y_1 \in I_1} \wedge \overline{\mathrm{K}}_P(p \wedge \mathrm{H}_{y_2}\mathrm{G}(\neg p_{y_2 \in I_2} \vee \neg q)))$.

Next, we need to apply the BMC method for the HLTLK formula $\mathcal{H}(\varphi'_1)$ and for the abstract model M_{φ_1}. Thus, we have to encode the local states of agents, the clock valuations, the joint actions, and the new clock actions in the in binary form. Since the Producer can be in 2 different local states and it has one

clock with the maximal value equal to b, we shall need 1 bit to encode its local states and $c_P = \lceil log_2(m1) \rceil$ with $m1 = max(b, 2n+2)$ bits to encode the clock valuations. Since the Consumer can be in 3 different local states and it has one clock with the maximal value equal to $max(d, h)$, we shall need 2 bits to encode its local states and $c_C = \lceil log_2(m2) \rceil$ with $m2 = max(max(d, h), 2n+2)$ bits to encode the clock valuations. Since the Nodes can be in 4 different local states and they have one clock with the maximal value equal to $max(d, f)$, we shall need 2 bits to encode local states of each Node and $c_{Ni} = \lceil log_2(m3) \rceil$ with $m2 = max(max(d, f), 2n+2)$ bits to encode the clock valuations of each Node. The modelling of the environment $\mathcal{E}$ requires only one bit to encode the local state, and since $\mathcal{E}$ has two clocks with the maximal value equal to $2n+3$ we shall need $c_{\mathcal{E}} = 2 \cdot \lceil log_2(2n+3) \rceil$ bits to encode the clock valuations. Having the fixed values of a, b, c, d, e, f, g, h and n, it should be straightforward to calculate the number of bits/propositional variables, say t, that model/represents a global state of the GTPP system; it should be of the following form $((\mathsf{w}_P[0], \mathsf{v}_P[0], \ldots, \mathsf{v}_P[c_P])$, $(\mathsf{w}_{N1}[0], \mathsf{w}_{N1}[1], \mathsf{v}_{N1}[0], \ldots, \mathsf{v}_{N1}[c_{N1}]), \ldots, (\mathsf{w}_{Nn}[0], \mathsf{w}_{Nn}[1], \mathsf{v}_{Nn}[0], \ldots, \mathsf{v}_{Nn}[c_{Nn}])$, $(\mathsf{w}_C[0], \mathsf{w}_C[1], \mathsf{v}_C[0], \ldots, \mathsf{v}_C[c_C])$, $(\mathsf{w}_{\mathcal{E}}[0], \mathsf{v}_{\mathcal{E}}[0], \ldots, \mathsf{v}_{\mathcal{E}}[c_{\mathcal{E}}]))$. Now, we can assume that the initial state of GTPP is represented by the tuple of t-zeros. Thus the propositional encoding of initial states is the following: $I_{s^0}(\mathbf{w}_{0,0}) = \bigwedge_{i=1}^{t} \neg \mathbf{w}_{0,0}[i]$. Now we can encode the model of the example up to the depth $k \in \mathbb{N}$, but we do not do it here. The translation of the propositions used in our formula is the following: $ProdSend(\mathbf{w}) := \mathsf{w}_P[0]$ (this means that $ProdSend$ holds at all the global states with the first local state of the agent Producer equal to 1); $ConsFree(\mathbf{w})$ $:= \mathsf{w}_C[0] \wedge \neg \mathsf{w}_C[1]$ (this means that $ConsFree$ holds at all the global states with the local state of the agent Consumer equal to $(1, 0)$); $ConsReady(\mathbf{w}) := \neg \mathsf{w}_C[0] \wedge \mathsf{w}_C[1]$ (this means that $Consready$ holds at all the global states with the local state of the agent Consumer equal to $(0, 1)$).

Having the above encoding and definitions of the auxiliary propositional formulae, we can easily infer propositional formulae that encode all the properties mentioned above. Further, checking that the GTPP satisfies the properties φ_1 and φ_2 can now be done by feeding a SAT solver with the propositional formulae generated in the way explained above.

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 introduced 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.

Our future work include an implementation of the presented BMC method, a careful evaluation of experimental results to be obtained, and a comparison of the OBDD-, SMT-, and SAT-based BMC method for TISs. Further, in [8] a for-

malism 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. G. Cabodi, P. Camurati, and S. Quer. Can BDDs compete with SAT solvers on bounded model checking? In *Proceedings of the 39th annual Design Automation Conference*, pp. 117–122. ACM, 2002.
2. E. Clarke, A. Biere, R. Raimi, and Y. Zhu. Bounded model checking using satisfiability solving. *Formal Methods in System Design*, 19(1):7–34, 2001.
3. E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. The MIT Press, 1999.
4. E. A. Emerson. Temporal and modal logic. *Handbook of Theoretical Computer Science*, volume B, chapter 16, pp. 996–1071. Elsevier Science Publishers, 1990.
5. R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.
6. C. A. Furia and P. Spoletini. Tomorrow and all our yesterdays: MTL satisfiability over the integers. In *Proceedings of the Theoretical Aspects of Computing*, volume 5160 of *LNCS*, pp. 253–264. Springer-Verlag, 2008.
7. H. Levesque. A logic of implicit and explicit belief. In *Proceedings of the 6th National Conference of the AAAI*, pp. 198–202. Morgan Kaufman, 1984.
8. A. Lomuscio, W. Penczek, and B. Woźna. Bounded model checking for knowledge and real time. *Artificial Intelligence*, 171:1011–1038, 2007.
9. A. Lomuscio and M. Sergot. Deontic interpreted systems. *Studia Logica*, 75(1):63–92, 2003.
10. A. Męski, 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. Springer, 2014.
11. D. Peled. All from one, one for all: On model checking using representatives. In *Proceedings of CAV'93*, volume 697 of *LNCS*, pp. 409–423. Springer, 1993.
12. W. Penczek and A. Lomuscio. Verifying epistemic properties of multi-agent systems via bounded model checking. *Fundamenta Informaticae*, 55(2):167–185, 2003.
13. M. Wooldridge. *An introduction to multi-agent systems*. Second Edition. John Wiley & Sons, 2009.
14. B. Woźna-Szcześniak and A. Zbzrzezny. Checking MTL Properties of Discrete Timed Automata via Bounded Model Checking (Extended Abstract). In *Proceedings of CS&P 2013*, vol. 1032 of CEUR Workshop Proceedings, pp 469-477, 2013.
15. B. Woźna-Szcześniak and A. Zbrzezny. A translation of the existential model checking problem from MITL to HLTL. *Fundamenta Informaticae*, 122(4):401–420, 2013.
16. A. Zbrzezny. A new translation from ECTL* to SAT. *Fundamenta Informaticae*, 120(3-4):377–397, 2012.