Scientific Issues
Jan Długosz University
in Częstochowa
Mathematics XX (2015)
69–81
DOI http://dx.doi.org/10.16926/m.2015.20.08

SAT-BASED BOUNDED MODEL CHECKING FOR TIMED INTERPRETED SYSTEMS AND THE RTECTLK PROPERTIES

BOŻENA WOŹNA-SZCZEŚNIAK, IRENEUSZ SZCZEŚNIAK

Abstract

We define an SAT-based bounded model checking (BMC) method for RTECTLK (the existential fragment of the real-time computation tree logic with knowledge) that is interpreted over timed models generated by timed interpreted systems. Specifically, we translate the model checking problem for RTECTLK to the model checking problem for a variant of branching temporal logic (called E_yCTLK) interpreted over an abstract model, and we redefine an SAT-based BMC technique for E_yCTLK.

1. Introduction

The *Interpreted system* (IS) [5] is the formalism, which was designed to model multi-agent systems (MASs) [11], and to reason about the agents' epistemic and temporal properties. The *timed interpreted system* (TIS) [14] is the formalism that extends ISs to make feasible reasoning about real-time aspects of MASs. The TIS gives a computationally grounded semantics on which it is feasible to interpret both the time-bounded temporal modalities and the conventional epistemic modalities.

The fundamental thought of the SAT-based bounded model checking (BMC) systems [2, 10] comprises in translating the existential model checking problem for a modal logic and for a Kripke structure to the SAT problem [6], furthermore, exploiting the sophistication of present day SAT-solvers, i.e., programs (tools) that automatically decide whether a propositional formula is satisfiable.

To express the specifications of MASs different extensions of classic temporal logics [3] with epistemic [5], doxastic [7], and deontic (to represent the correct functioning behaviour) [9] modalities have been proposed. In this paper we consider RTECTLK, i.e., an epistemic extension of the existential fragment of the soft real-time CTL (RTECTL) [4], which is a propositional branching-time temporal logic with bounded operators, and which was introduced to permit specification and reasoning about time-critical correctness properties. We interpret RTECTLK over *timed models* generated by timed interpreted systems.

A version of the SAT-based BMC method for specifications expressed in RTECTLK has been published in [12, 13]. However, the underling model for RTECTLK was the interpreted system [5] with the asynchronous semantics (interleaving semantics). Here we use, as the underling model for RTECTLK, the timed interpreted systems with the synchronous semantics, thus the agents over this semantics perform a joint action at a given time in a global state. Moreover, the RTECTLK properties cannot be expressed using nested applications of the next state operators.

In the paper we make the following contribution. We define the SAT-based BMC method for RTECTLK interpreted over timed models generated by timed interpreted systems. Specifically, we translate the model checking problem for RTECTLK to the model checking problem for a variant of branching temporal logic (called E_yCTLK) interpreted over an abstract model, and we redefine and improve the SAT-based BMC technique for E_yCTLK of [8]. The improvement of the SAT-based BMC [8] consists in utilizing the SAT-based BMC method for ECTL [15]. Its main idea is to translate every subformula ψ of the formula φ using only $f_k(\psi)$ paths of length k. So, our new BMC algorithm uses a reduced number of paths, what results in significantly smaller and less complicated propositional formulae that encode the RTECTLK properties.

The rest of the paper is organised as follows. In Section 2 we introduce the TIS and the RTECTLK logic. In Section 3 we show how to translate the model checking problem for RTECTLK to the model checking problem for E_yCTLK. In Section 4 we provide a BMC method for E_yCTLK and for ATIS. Finally in Section 5 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, $\mathbb{N}_+ = \mathbb{N} \setminus \{0\}$, $\mathcal{PV}$ 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:

$$\phi := true \mid x \sim c \mid \phi \wedge \phi$$

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:
$v \models true$,
$v \models x \sim c$ iff $v(x) \sim c$,
$v \models \phi \wedge \phi'$ iff $v \models \phi$ and $v \models \phi'$.
Finally, by the *time successor* of v (written $succ(v)$) we denote the clock valuation v' such that $\forall x \in X$, $v'(x) = v(x) + 1$.
Timed Interpreted Systems. Let $\mathcal{A} = \{1, \ldots, n\}$ be 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 $\mathcal{PV} = \bigcup_{\mathbf{c} \in \mathcal{A}} \mathcal{PV}_{\mathbf{c}} \cup \mathcal{PV}_{\mathcal{E}}$ be a set of propositional variables such that $\mathcal{PV}_{\mathbf{c}_1} \cap \mathcal{PV}_{\mathbf{c}_2} = \emptyset$ for all $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{A} \cup \{\mathcal{E}\}$. The set of agents $\mathcal{A}$ together with the environment constitute a multi-agent system (MAS), to model which we utilize the formalism of *timed interpreted system* (TIS).

In TIS, each agent $\mathbf{c} \in \mathcal{A}$ is modelled by:

- $L_{\mathbf{c}}$ - a non-empty and finite set of *local states*,
- $Act_{\mathbf{c}}$ - a non-empty and finite set of *possible actions* such that the special *null* action $\epsilon_{\mathbf{c}}$ belongs to $Act_{\mathbf{c}}$; it is assumed that actions are "public",
- $X_{\mathbf{c}}$ - a non-empty and finite set of *clocks*,
- $P_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{Act_{\mathbf{c}}}$ - a *protocol function* that characterizes rules according to which actions may be performed in every local state,
- $t_{\mathbf{c}} : L_{\mathbf{c}} \times L_{\mathcal{E}} \times \mathcal{C}(X_{\mathbf{c}}) \times 2^{X_{\mathbf{c}}} \times Act \to L_{\mathbf{c}}$ with $Act = \prod_{\mathbf{c} \in \mathcal{A}} Act_{\mathbf{c}} \times Act_{\mathcal{E}}$ - a (partial) *evolution function* which defines local transitions; each element of Act and $\mathcal{C}(X_{\mathbf{c}})$ is called a *joint action* and an *enabling condition*, respectively,
- $\mathcal{V}_{\mathbf{c}} : L_{\mathbf{c}} \to 2^{\mathcal{PV}}$ - a *valuation function* which assigns to every local state a set of propositional variables that are assumed to be true at that state,
- $\mathcal{I}_{\mathbf{c}} : L_{\mathbf{c}} \to \mathcal{C}(X_{\mathbf{c}})$ - an *invariant function* 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 $X \in 2^{X_{\mathbf{c}}}$. Finally, we assume that the sets of clocks are pairwise disjoint.

Correspondingly to the other agents, the environment $\mathcal{E}$ is modelled by

- $L_{\mathcal{E}}$ - a non-empty and finite set of *local states*,
- $Act_{\mathcal{E}}$ - a non-empty and finite set of *possible actions*,
- $X_{\mathcal{E}}$ - a non-empty and finite set of *clocks*,

- $P_\mathcal{E} : L_\mathcal{E} \to 2^{Act_\mathcal{E}}$ - a protocol 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 (partial) *evolution function*,
- $\mathcal{V}_\mathcal{E} : L_\mathcal{E} \to 2^{\mathcal{PV}_\mathcal{E}}$ - a *valuation function*,
- $\mathcal{I}_\mathcal{E} : L_\mathcal{E} \to \mathcal{C}(X_\mathcal{E})$ - and an *invariant function* 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".

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

$$\mathbb{I} = (\{L_\mathbf{c}, Act_\mathbf{c}, X_\mathbf{c}, P_\mathbf{c}, t_\mathbf{c}, \mathcal{V}_\mathbf{c}, \mathcal{I}_\mathbf{c}\}_{\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}}, \iota)$$

For a given time interpreted system $\mathbb{I}$ we define a *timed model* as a tuple

$$M = (\Sigma, \iota, S, T, \mathcal{V}) :$$

- $\Sigma = Act \cup \mathbb{N}$ is the set of labels (i.e., joint actions and natural numbers),
- S and $\iota \in S$ are defined as above,
- $\mathcal{V} : S \to 2^{\mathcal{PV}}$ is the valuation function defined as $\mathcal{V}(s) = \bigcup_{\mathbf{c} \in \mathcal{A}} \mathcal{V}_\mathbf{c}(l_\mathbf{c}(s))$,
- $T \subseteq S \times (Act \cup \mathbb{N}) \times S$ 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 $\mathbf{c} \in \mathcal{A}$, 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 $\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}$, $l_\mathbf{c}(s) = l_\mathbf{c}(s')$ 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 time interpreted system $\mathbb{I}$ 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 $v_\mathbf{c}(s') = v_\mathbf{c}(s)$.

Let M be a timed model generated by a TIS $\mathbb{I}$. A *run* of $\mathbb{I}$ is an infinite sequence $\rho = s_0 \stackrel{\delta_0, \overline{a}_0}{\to} s_1 \stackrel{\delta_1, \overline{a}_1}{\to} s_2 \stackrel{\delta_2, \overline{a}_2}{\to} \ldots$ of global states such that the following conditions hold for all $i \in \mathbb{N}$: $s_i \in S$, $\overline{a}_i \in Act$, $\delta_i \in \mathbb{N}_+$, and there exists $s'_i \in S$ such that $(s_i, \delta_i, s'_i) \in T$ and $(s'_i, \overline{a}_i, s_{i+1}) \in T$. Note that the definition of the run does not allow two consecutive joint actions to be performed one after the other, i.e., between each two joint actions some time must pass.

The symbol $\Pi_{\mathbb{I}}(s)$ denotes the set of all the runs in $\mathbb{I}$ that start at the state s. $\Pi = \bigcup_{s^0 \in \iota} \Pi_{\mathbb{I}}(s^0)$.

RTECTLK. 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 $a \neq b$. The existential fragment of RTCTL with knowledge (RTECTLK) is defined by the following grammar:

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

The symbol E (*for some path*) is the path quantifier. The symbols U_I(*bounded until*) and G_I (*bounded globally*) are temporal modalities. The derived basic temporal modalities for *bounded eventually* and *bounded release* are defined as follows: $\mathrm{EF}_I \varphi \stackrel{def}{=} \mathrm{E}(\top \mathrm{U}_I \varphi)$, $\mathrm{E}(\varphi \mathrm{R}_I \psi) \stackrel{def}{=} \mathrm{E}(\psi \mathrm{U}_I(\psi \wedge \varphi)) \vee \mathrm{EG}_I \psi$. Hereafter, if the interval I is of the form $[0, \infty)$, then we omit it for the simplicity of the presentation. The symbols $\overline{\mathrm{K}}_{\mathbf{c}}$ (agent $\mathbf{c}$ considers possible), $\overline{\mathrm{E}}_{\Gamma}$ (possibly everyone in Γ knows), $\overline{\mathrm{D}}_{\Gamma}$ (possible distributed knowledge in the group Γ), and $\overline{\mathrm{C}}_{\Gamma}$ (possible common knowledge among agents in Γ) are the dualities to standard epistemic modalities.

To define the satisfiability relation for RTECTLK, 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: $\sim_{\Gamma}^{E} \stackrel{def}{=} \bigcup_{\mathbf{c} \in \Gamma} \sim_{\mathbf{c}}$, $\sim_{\Gamma}^{C} \stackrel{def}{=} (\sim_{\Gamma}^{E})^{+}$ (the transitive closure of $\sim_{\Gamma}^{E}$), $\sim_{\Gamma}^{D} \stackrel{def}{=} \bigcap_{\mathbf{c} \in \Gamma} \sim_{\mathbf{c}}$, where $\Gamma \subseteq \mathcal{A}$.

Let $\Delta_0 = [b_0, b_1), \Delta_1 = [b_1, b_2), \ldots$ 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 $t \in \Delta_i$. A *path λ_ρ corresponding to ρ* is a mapping $\lambda_\rho : \mathbb{N} \to S$ such that $\lambda_\rho(t) = ((\ell_1^i, v_1^i + t - b_i), \ldots, (\ell_n^i, v_n^i + t - b_i), (\ell_{\mathcal{E}}^i, v_{\mathcal{E}}^i + t - b_i)) = s_i + t - b_i$, where $i = idx_\rho(t)$.

Let $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$. The *satisfiability* relation $\models$, which indicates truth of a RTECTLK formula in the timed model M at state s, is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

$M, s \models \mathrm{E}(\alpha \mathrm{U}_I \beta)$ iff $(\exists \rho \in \Pi_{\mathbb{I}}(s))(\exists i \in I)(M, \lambda_\rho(i) \models \beta$ and $(\forall 0 \leq j < i)\ M, \lambda_\rho(j) \models \alpha)$

$M, s \models \mathrm{EG}_I \alpha$ iff $(\exists \rho \in \Pi_{\mathbb{I}}(s))\ (\forall i \in I)(M, \lambda_\rho(i) \models \alpha)$

$M, s \models \overline{\mathrm{K}}_{\mathbf{c}} \alpha$ iff $(\exists \rho \in \Pi_{\mathbb{I}})(\exists i \geq 0)(s \sim_{\mathbf{c}} \lambda_\rho(i)$ and $M, \lambda_\rho(i) \models \alpha)$

$M, s \models \overline{Y}_{\Gamma} \alpha$ iff $(\exists \rho \in \Pi_{\mathbb{I}})(\exists i \geq 0)(s \sim_{\Gamma}^{Y} \lambda_\rho(i)$ and $M, \lambda_\rho(i) \models \alpha)$

An RTECTLK formula φ *holds* in the model M (denoted $M \models \varphi$) iff $M, s^0 \models \varphi$ for some state $s^0 \in \iota$. The *model checking problem* asks whether $M \models \varphi$.

3. From RTECTLK to E$_y$CTLK

The translation of the model checking problem for RTECTLK to the model checking problem for E$_y$CTLK, a language defined below and interpreted over an *abstract model* for an *augmented timed interpreted system* is based on [8], where the translation of the model checking problem for the existential part of TCTL [1] augmented with knowledge (TECTLK) with a dense-time semantics defined over timed automata to the model checking problem for E$_y$CTLK with a semantics defined over the region graph has been introduced.

We start by defining *augmented timed interpreted systems* (ATIS) for a given timed interpreted system $\mathbb{I} = (\{L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}}, \iota)$, and an RTECTLK formula φ.

Let m be the number of intervals appearing in φ. Then, an ATIS $\mathbb{I}_\varphi$ is defined as the following tuple

$$(\{L_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}}, \{Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}\}_{\mathbf{c} \in \mathcal{A}}, Act'_{\mathcal{E}}, X'_{\mathcal{E}}, P'_{\mathcal{E}}, t'_{\mathcal{E}}) :$$

- $Act'_{\mathcal{E}} = Act_{\mathcal{E}} \cup \{a_y\}$, where a_y is a new action corresponding to setting to zero a new clock y.
- $X'_{\mathcal{E}} = X_{\mathcal{E}} \cup \{y\}$, where the new clock y corresponds to all the intervals appearing in φ; one clock is sufficient to perform the BMC algorithm that is presented in the next section.
- $P'_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act'_{\mathcal{E}}}$ is an extension of the protocol function $P_{\mathcal{E}} : L_{\mathcal{E}} \to 2^{Act_{\mathcal{E}}}$ such that $\{a_y\} \subseteq P'_{\mathcal{E}}(\ell)$ 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 $t'_{\mathcal{E}}(\ell_{\mathcal{E}}, true, \{a_y\}, (\epsilon_1, \ldots, \epsilon_n, a_y)) = \ell_{\mathcal{E}}$.

An abstract model for ATIS. Let φ be an RTECTLK formula, $\mathcal{PV}' = \mathcal{PV} \cup \{p_{y \in I} \mid I \text{ is an interval in } \varphi\}$, and $\mathbb{I}_\varphi = (\{L_{\mathbf{c}}, Act_{\mathbf{c}}, X_{\mathbf{c}}, P_{\mathbf{c}}, t_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, \mathcal{I}_{\mathbf{c}}\}_{\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}}, \iota)$ 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 $Act = \prod_{\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}} Act_{\mathbf{c}}$,
- $S_\varphi = \prod_{\mathbf{c} \in \mathcal{A} \cup \mathcal{E}} L_{\mathbf{c}} \times \mathbb{N}^{|X_{\mathbf{c}}|}$ 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 $p \in \bigcup_{\mathbf{c} \in \mathcal{A} \cup \mathcal{E}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$ for all $p \in \mathcal{PV}$,
  (2) $p_{y \in I} \in \mathcal{V}_\varphi(((\ell_1, v_1), \ldots, (\ell_n, v_n), (\ell_{\mathcal{E}}, v_{\mathcal{E}})))$ iff $v_{\mathcal{E}}(y) \in I$,
- $T_\varphi \subseteq S_\varphi \times \Sigma_\varphi \times S_\varphi$ 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 $(\forall \mathbf{c} \in \mathcal{A})$ $(\exists \phi_\mathbf{c} \in \mathcal{C}(X_\mathbf{c}))$ $(\exists X'_\mathbf{c} \subseteq X_\mathbf{c})$ $(t_\mathbf{c}(l_\mathbf{c}(s), l_\mathcal{E}(s), \phi_\mathbf{c}, X'_\mathbf{c}, \overline{a}) = l_\mathbf{c}(s')$ 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 $(\forall \mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\})(l_\mathbf{c}(s) = l_\mathbf{c}(s')$ 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 augmented time interpreted system $\mathbb{I}_\varphi$ 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 E_yCTLK language. In order to translate a RTECTLK formula φ into the corresponding E_yCTLK formula ψ we map the RTECTLK language into E_yCTLK by reinterpreting the temporal operators, denoted by $\mathrm{E}_y\mathrm{U}$ and $\mathrm{E}_y\mathrm{G}$. Formally, for $p \in \mathcal{PV}'$, $\mathbf{c} \in \mathcal{A}$, and $\Gamma \subseteq \mathcal{A}$, the E_yCTLK formulae are defined by the following grammar:

$$\varphi := \top \,|\, \bot \,|\, p \,|\, \neg p \,|\, \varphi \wedge \varphi \,|\, \varphi \vee \varphi \,|\, \mathrm{E}_y(\varphi \mathrm{U} \varphi) \,|\, \mathrm{E}_y \mathrm{G} \varphi \,|\, \overline{\mathrm{K}}_\mathbf{c} \varphi \,|\, \overline{\mathrm{E}}_\Gamma \varphi \,|\, \overline{\mathrm{D}}_\Gamma \varphi \,|\, \overline{\mathrm{C}}_\Gamma \varphi$$

In addition, we introduce some useful derived temporal modalities:

- $\mathrm{E}_y(\varphi \mathrm{R} \psi) \stackrel{def}{=} \mathrm{E}_y(\psi \mathrm{U}(\varphi \wedge \psi)) \vee \mathrm{E}_y \mathrm{G} \psi$ (*release*),
- $\mathrm{E}_y \mathrm{F} \varphi \stackrel{def}{=} \mathrm{E}_y(\top \mathrm{U} \varphi)$ (*eventually*).

The E_yCTLK formulae are interpreted over the abstract model M_φ. Let $T_\mathbb{I}$ denote the part of T_φ, where transitions are labelled with elements of $Act \cup \{\tau\}$, and T_y denotes the transitions that reset the clock y.

Definition 1. *A* path π *in* M_φ *is a sequence* $\pi = (s_0, s_1, \ldots)$ *of states such that* $(s_0, \tau, s_1) \in T_\mathbb{I}$*, and for each* $i > 0$*, either* $(s_i, \overline{a}_i, s_{i+1}) \in T_\mathbb{I}$ *or* $(s_i, \tau, s_{i+1}) \in T_\mathbb{I}$*, and if* $(s_i, \overline{a}_i, s_{i+1}) \in T_\mathbb{I}$ *holds, then* $(s_{i+1}, \tau, s_{i+2}) \in T_\mathbb{I}$ *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 π, $\pi(i)$ denotes the i-th state s_i of π. $\Pi_\varphi(s)$ denotes the set of all the paths starting at $s \in S_\varphi$, and $\Pi_\varphi = \bigcup_{s^0 \in \iota_\varphi} \Pi_\varphi(s^0)$.

The satisfiability relation $\models$, which indicates truth of ψ in M_φ at state s (in symbols $M_\varphi, s \models \psi$), is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

- $M_\varphi, s \models \mathrm{E}_y(\alpha \mathrm{U} \beta)$ iff $(\exists s' \in S_\varphi)((s, (\epsilon_1, \ldots, \epsilon_n, a_y), s') \in T_y$ and $(\exists \pi \in \Pi_\varphi(s'))(\exists m \geq 0)\ [M_\varphi, \pi(m) \models \beta$ and $(\forall j < m) M_\varphi, \pi(j) \models \alpha])$,
- $M_\varphi, s \models \mathrm{E}_y \mathrm{G}\alpha$ iff $(\exists s' \in S_\varphi)((s, (\epsilon_1, \ldots, \epsilon_n, a_y), s') \in T_y$ and $(\exists \pi \in \Pi_\varphi(s'))(\forall m \geq 0)\ M_\varphi, \pi(m) \models \alpha)$,
- $M_\varphi, s \models \overline{\mathrm{K}}_{\mathbf{c}}\alpha$ iff $(\exists \pi \in \Pi_\varphi)(\exists m \geq 0)(s \sim_{\mathbf{c}} \pi(m)$ and $M_\varphi, \pi(m) \models \alpha)$,
- $M_\varphi, s \models \overline{Y}_\Gamma\alpha$ iff $(\exists \pi \in \Pi_\varphi)(\exists m \geq 0)(s \sim_\Gamma^Y \pi(m)$ and $M_\varphi, \pi(m) \models \alpha)$.

An E_yCTLK formula φ is *valid on* M_φ (denoted $M_\varphi \models \varphi$) iff $M_\varphi, s^0 \models \varphi$ for some $s^0 \in \iota$, i.e., φ is true at some initial state of the model M_φ.

Having defined syntax and semantics of the E_yCTLK logic, we can now introduce the translation mentioned above. An RTECTLK formula φ is translated inductively into the E_yCTLK formula $\mathcal{H}(\varphi)$ as follows:

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

The main theorem of the section states that the validity of the RTECTLK formula φ over the timed model is equivalent to the validity of the corresponding E_yCTLK formula $\mathcal{H}(\varphi)$ over the abstract model. The proof of the theorem can be completed by an induction of the formula φ.

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

4. An SAT-based BMC method for E_yCTLK

Bounded semantics. Let $M_\varphi = (\Sigma_\varphi, \iota, S_\varphi, T_\varphi, \mathcal{V}_\varphi)$ be an abstract model, $k \in \mathbb{N}$, and $0 \leq l \leq k$. As before, we denote by $T_{\mathbb{I}}$ the subset of T_φ, where transitions are labelled with elements of $Act \cup \{\tau\}$, and by T_y the set of transitions resetting the clock y.

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

The symbol $\Pi_k(s)$ denotes the set of all the k-paths starting at s in M_φ, and $\Pi_k = \bigcup_{s^0 \in \iota_\varphi} \Pi_k(s^0)$.

Definition 3. *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 $i \leq k$. A k-path $\pi = (\pi(0), \ldots, \pi(k))$ is a* loop *if there exists $0 \leq l < k$ and $(\forall \mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\})(\ell_{\mathbf{c}}^k = \ell_{\mathbf{c}}^l)$ and $(\forall \mathbf{c} \in \mathcal{A})(v_{\mathbf{c}}^k = v_{\mathbf{c}}^l)$ and $v_{\mathcal{E} \downarrow X_{\mathcal{E}}}^k = v_{\mathcal{E} \downarrow X_{\mathcal{E}}}^l$, where $\downarrow X_{\mathcal{E}}$*

denoted the projection of the clock valuation $v_{\mathcal{E}} : X_{\mathcal{E}} \cup \{y\} \to \mathbb{N}$ *on the clock valuation* $v'_{\mathcal{E}} : X_{\mathcal{E}} \to \mathbb{N}$.

Satisfaction of the temporal operator $\mathrm{E}_y\mathrm{G}$ on a k-path π in the bounded case depends on whether or not π is a loop. Therefore, we assume a function $loop : \Pi_k \mapsto 2^{\mathbb{N}}$ which returns the set of all the indices of the states for which there is a transition from the last state of a k-path π. Note that if a k-path is a loop, then it represents an *infinite* path.

The *bounded satisfiability* relation $\models_k$, which indicates truth of ψ in M_φ at state s (denoted $M_\varphi, s \models_k \psi$) is defined inductively with the classical rules for propositional operators and with the following rules for the temporal and epistemic modalities:

- $M_\varphi, s \models_k \mathrm{E}_y(\alpha \mathrm{U} \beta)$ iff $(\exists s' \in S_\varphi)((s, (\epsilon_1, \ldots, \epsilon_n, a_y), s') \in T_y$ and $(\exists \pi \in \Pi_k(s'))(\exists 0 \leq m \leq k)$ $(M_\varphi, \pi(m) \models_k \beta$ and $(\forall j < m) M_\varphi, \pi(j) \models \alpha))$,
- $M_\varphi, s \models_k \mathrm{E}_y\mathrm{G}\alpha$ iff $(\exists s' \in S_\varphi)((s, (\epsilon_1, \ldots, \epsilon_n, a_y), s') \in T_y$ and $(\exists \pi \in \Pi_k(s'))(\forall 0 \leq j \leq k)$ $(M_\varphi, \pi(j) \models \alpha$ and $loop(\pi) \neq \emptyset)$,
- $M_\varphi, s \models \overline{\mathrm{K}}_{\mathbf{c}}\alpha$ iff $(\exists \pi \in \Pi_k)(\exists 0 \leq m \leq k)(s \sim_{\mathbf{c}} \pi(m)$ and $M_\varphi, \pi(m) \models \alpha)$,
- $M_\varphi, s \models \overline{Y}_\Gamma\alpha$ iff $(\exists \pi \in \Pi_k)(\exists 0 \leq m \leq k)(s \sim_\Gamma^Y \pi(m)$ and $M, \pi(m) \models \alpha)$, where $Y \in \{\mathrm{D}, \mathrm{E}, \mathrm{C}\}$.

We use the following notation $M_\varphi \models_k \psi$ iff $M_\varphi, s^0 \models_k \psi$ for some $s^0 \in \iota_\varphi$. 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.

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

Translation to SAT. Let M_φ be an abstract model, ψ an E_yCTLK formula, and $k \geq 0$ a bound. The presented propositional encoding of the BMC problem for E_yCTLK improves the BMC encoding of [8] and it is based on the BMC encoding of [16]. 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 set of 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 $f_k : E_yCTLK \to \mathbb{N}$: $f_k(\top) = f_k(\bot) = f_k(p) = f_k(\neg p) = 0$, where $p \in \mathcal{PV}'$; $f_k(\alpha \wedge \beta) = f_k(\alpha) + f_k(\beta)$; $f_k(\alpha \vee \beta) = max\{f_k(\alpha), f_k(\beta)\}$; $f_k(E_y(\alpha \mathrm{U} \beta)) = k \cdot f_k(\alpha) + f_k(\beta) + 1$; $f_k(\mathrm{E}_y\mathrm{G}\alpha) = (k+1) \cdot f_k(\alpha) + 1$; $f_k(\overline{\mathrm{C}}_\Gamma \alpha) = f_k(\alpha) + k$; $f_k(Y\alpha) = f_k(\alpha) + 1$ for $Y \in \{\overline{\mathrm{K}}_\mathbf{c}, \overline{\mathrm{D}}_\Gamma, \overline{\mathrm{E}}_\Gamma\}$.

Formally, let $\mathbf{c} \in \mathcal{A}$. We assume that each state $s \in S_\varphi$ is represented by a *symbolic state* $\mathbf{w} = ((\mathsf{w}_1, \mathsf{v}_1) \ldots, (\mathsf{w}_n, \mathsf{v}_n), (\mathsf{w}_\mathcal{E}, \mathsf{v}_\mathcal{E}))$, 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 $\mathbb{D}$. Next, we assume that each join action $\overline{a} \in Act$ is represented by a *symbolic action* $\mathbf{a} = (\mathsf{a}_1, \ldots, \mathsf{a}_n, \mathsf{a}_\mathcal{E})$, where each symbolic local action $\mathsf{a}_\mathbf{c}$ is a vector of propositional variables. Moreover, we assume that the time action τ is represented by a proposition variable $\wp_\tau$. Finally, we assume a symbolic representation of a k-path π, the number of which is j, and we call it the *j-th symbolic k-path* $\boldsymbol{\pi}_j = (\mathbf{w}_{0,j}, \ldots, \mathbf{w}_{k,j})$, where $0 \leq j < f_k(\psi)$, $0 \leq i \leq k$, and $\mathbf{w}_{i,j}$ is a symbolic state.

Let $\mathbf{w}$ and $\mathbf{w}'$ be two different symbolic states, and $\mathbf{a}$ a symbolic action. 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 $\mathbf{c} \in \mathcal{A}$.
- $H(\mathbf{w}, \mathbf{w}') := \bigwedge_{\mathbf{c} \in \mathcal{A} \cup \{\mathcal{E}\}} H_\mathbf{c}(\mathbf{w}, \mathbf{w}')$ - encodes equality of two global states.
- $\mathcal{T}(\mathbf{w}, \mathbf{a}, \mathbf{w}')$ is a formula over $\mathbf{w}$, $\mathbf{w}'$, and $\mathbf{a}$, which is true for valuations $s_\mathbf{w}$ of $\mathbf{w}$, $s_{\mathbf{w}'}$ of w', and $s_\mathbf{a}$ of $\mathbf{a}$ iff either $(s_\mathbf{w}, s_\mathbf{a}, s_{\mathbf{w}'}) \in T_\mathbb{I}$ or $(s_\mathbf{w}, \wp_\tau, s_{\mathbf{w}'}) \in T_\mathbb{I}$ (encodes non-resetting transitions of M_φ).
- $\mathcal{T}_y(\mathbf{w}, \mathbf{w}')$ is a formula over $\mathbf{w}$ and $\mathbf{w}'$, which is true for two valuations $s_\mathbf{w}$ of $\mathbf{w}$ and $s_{\mathbf{w}'}$ of $\mathbf{w}'$ iff $(s_\mathbf{w}, (\epsilon_1, \ldots, \epsilon_n, a_y), s_{\mathbf{w}'}) \in T_y$ (encodes transitions resetting the clock y).

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

$$[M_\varphi^{\psi,\iota}]_k := \bigvee_{s \in \iota} I_s(\mathbf{w}_{0,0}) \wedge \bigwedge_{n=1}^{f_k(\psi)} \bigwedge_{m=0}^{k-1} \mathcal{T}(\mathbf{w}_{m,n}, \mathbf{a}_{m,n}, \mathbf{w}_{m+1,n}).$$

The next step is a translation of a E_yCTLK formula ψ to a propositional formula $[\psi]_{M_\varphi,k} := [\psi]_k^{[0,0,F_k(\psi)]}$, where $[\alpha]_k^{[m,n,A]}$ denotes the translation of α at the symbolic state $\mathbf{w}_{m,n}$ by using the set $A \subseteq F_k(\psi)$. To define $[\psi]_k^{[0,0,F_k(\psi)]}$, 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^{G}) that were defined in [16].

Let M_φ be a model, ψ a E_yCTLK formula, and $k \geq 0$ a bound. The formula $[\psi]_k^{[0,0,F_k(\psi)]}$ that encodes the bounded semantics for E_yCTLK is inductively defined as shown below.

Namely, let $0 \leqslant n < f_k(\psi)$, $m \leqslant k$, $n' = min(A)$, $h_k^{\mathrm{U}} = h_k^{\mathrm{U}}(g_s(A), f_k(\beta))$, and $h_k^{\mathrm{G}} = h_k^{\mathrm{G}}(g_s(A),\ f_k(\alpha))$.

$[\top]_k^{[m,n,A]} := \top, [\bot]_k^{[m,n,A]} := \bot,$
$[p]_k^{[m,n,A]} := p(w_{m,n}), [\neg p]_k^{[m,n,A]} := \neg p(w_{m,n}),$

$$
\begin{aligned}
[\alpha \wedge \beta]_k^{[m,n,A]} &:= [\alpha]_k^{[m,n,g_l(A,f_k(\alpha))]} \wedge [\beta]_k^{[m,n,g_r(A,f_k(\beta))]},\\
[\alpha \vee \beta]_k^{[m,n,A]} &:= [\alpha]_k^{[m,n,g_l(A,f_k(\alpha))]} \vee [\beta]_k^{[m,n,g_l(A,f_k(\beta))]},\\
[\mathrm{E}_y(\alpha \mathrm{U} \beta)]_k^{[m,n,A]} &:= \mathcal{T}_y(\mathbf{w}_{m,n}, \mathbf{w}_{0,n'}) \wedge \bigvee_{i=0}^{k} ([\beta]_k^{[i,n',h_k^{\mathrm{U}}(k)]} \wedge \bigwedge_{j=0}^{i-1} [\alpha]_k^{[j,\,n',h_k^{\mathrm{U}}(j)]}),\\
[\mathrm{E}_y \mathrm{G} \alpha]_k^{[m,n,A]} &:= \mathcal{T}_y(\mathbf{w}_{m,n}, \mathbf{w}_{0,n'}) \wedge \bigwedge_{j=0}^{k} [\alpha]_k^{[j,n',h_k^{\mathrm{G}}(k)]} \wedge \bigvee_{l=0}^{k} H(\mathbf{w}_{k,n'}, \mathbf{w}_{l,n'}),\\
[\overline{\mathrm{K}}_{\mathbf{c}} \alpha]_k^{[m,n,A]} &:= (\bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n'})) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,n',g_\mu(A)]} \wedge H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'})),\\
[\overline{\mathrm{D}}_\Gamma \alpha]_k^{[m,n,A]} &:= (\bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n'})) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,n',g_\mu(A)]} \wedge \bigwedge_{\mathbf{c} \in \Gamma} H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'})),\\
[\overline{\mathrm{E}}_\Gamma \alpha]_k^{[m,n,A]} &:= (\bigvee_{s \in \iota} I_s(\mathbf{w}_{0,n'})) \wedge \bigvee_{j=0}^{k} ([\alpha]_k^{[j,n',g_\mu(A)]} \wedge \bigvee_{\mathbf{c} \in \Gamma} H_{\mathbf{c}}(\mathbf{w}_{m,n}, \mathbf{w}_{j,n'})),\\
[\overline{\mathrm{C}}_\Gamma \alpha]_k^{[m,n,A]} &:= [\bigvee_{j=1}^{k} (\overline{\mathrm{E}}_\Gamma)^j \alpha]_k^{[m,n,A]}.
\end{aligned}
$$

The following theorem guarantees that the BMC problem for E_yCTLK and for an augmented timed interpreted system 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 an $E_y CTLK$ 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. Conclusions

We have defined an SAT-based BMC for timed interpreted system and for properties expressed in RTECTLK. The method is based on a translation of the model checking problem for RTECTLK to the model checking problem for E_yCTLK, and then on the translation of the model checking problem for E_yCTLK to the SAT-problem.

In [8] a formalism of real time interpreted systems (RTIS) has been defined to model MASs with hard real-time deadlines and an SAT-based BMC for the existential version of the timed CTLK (TECTLK) has been defined. However, in contrast to the semantics adopted in this work, the semantics of the RTIS model is asynchronous, the agents are just pure timed automata, and the E_yCTLK logic is interpreted on the region graph for timed automata.

In the future, we plan to implement and experimentally evaluate the proposed SAT-based BMC. Next, we plan to define SMT-based BMC for TIS and for RTECTLK, and compare it with the SAT-based one.

References

[1] R. Alur, C. Courcoubetis, and D. Dill. Model checking in dense real-time. *Information and Computation*, 104(1):2–34, 1993.

[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. A. Emerson. Temporal and modal logic. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 16, pages 996–1071. Elsevier Science Publishers, 1990.

[4] E. A. Emerson, A.K. Mok, A. P. Sistla, and J. Srinivasan. Quantitative temporal reasoning. *Real-Time Systems*, 4(4):331–352, December 1992.

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

[6] J. Gu, P. Purdom, J. Franco, and B. Wah. Algorithms for the satisfiability (SAT) problem: a survey. In *Satisfiability Problem: Theory and Applications*, volume 35 of *Discrete Mathematics and Theoretical Computer Science(DIMASC)*, pages 19–152. American Mathematical Society, 1996.

[7] H. Levesque. A logic of implicit and explicit belief. In *Proceedings of the 6th National Conference of the AAAI*, pages 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] W. Penczek and A. Lomuscio. Verifying epistemic properties of multi-agent systems via bounded model checking. *Fundamenta Informaticae*, 55(2):167–185, 2003.

[11] M. Wooldridge. *An introduction to multi-agent systems*. John Wiley & Sons, 2002.

[12] B. Woźna-Szcześniak. Bounded model checking for the existential part of Real-Time CTL and knowledge. In *Proceedings of 4th IFIP TC2 Central and Eastern European Conference on Software Engineering Techniques*, pages 178–191, 2009.

[13] B. Woźna-Szcześniak, A. M. Zbrzezny, and A. Zbrzezny. The BMC method for the existential part of RTCTLK and interleaved interpreted systems. In *Proceedings of the 15th Portuguese Conference on Artificial Intelligence (EPIA'2011)*, volume 7026 of *LNAI*, pages 551–565. Springer-Verlag, 2011.

[14] Bożena Woźna-Szcześniak. Checking EMTLK properties of timed interpreted systems via bounded model checking. In *Proceedings of the 2014 International Conference on Autonomous Agents and Multi-agent Systems*, pages 1477–1478. IFAAMS, 2014.
[15] A. Zbrzezny. Improving the translation from ECTL to SAT. *Fundamenta Informaticae*, 85(1-4):513–531, 2008.
[16] A. Zbrzezny. A new translation from ECTL* to SAT. *Fundamenta Informaticae*, 120(3-4):377–397, 2012.

Received: September 2015

Bożena Woźna-Szcześniak
Jan Długosz University in Częstochowa
Institute of Mathematics and Computer Science
Al. Armii Krajowej 13/15, 42-200 Częstochowa, Poland
E-mail address: b.wozna@ajd.czest.pl

Ireneusz Szcześniak
Częstochowa University of Technology
Institute of Computer and Information Sciences
ul. Dąbrowskiego 69, 42-201 Częstochowa, Poland
E-mail address: iszczesniak@icis.pcz.pl