




SMT-based BMC for Dense Timed Interpreted Systems and EMTLK Properties

Agnieszka M. Zbrzezny¹^a, Andrzej Zbrzezny²^b and Bożena Woźna-Szcześniak²^c

¹Faculty of Mathematics and Computer Science, University of Warmia and Mazury,
Słoneczna 54, 10-710 Olsztyn, Poland

²Department of Mathematics and Computer Science, Jan Długosz University in Częstochowa,
Armii Krajowej 13/15, 42-200 Częstochowa, Poland

Keywords: Satisfiability Modulo Theories, Bounded Model Checking, The Existential Fragment of the Epistemic Metric Temporal Logic, Dense Timed Interpreted Systems.


Abstract: The use of automated verification, performed by the analysis of their models, is often recommended to assess the correctness of safety-critical systems, failure of which could cause dramatic consequences for both people and hardware. In the past, several automated verification methods, including model checking, have been proposed and consequently applied for the trustworthy development of real-time multi-agent systems (RTMAS). In this paper, we investigate a Satisfiability Modulo Theories based Bounded Model Checking (SMT-BMC) method for EMTLK (the existential fragment of an epistemic Metric Temporal Logic) that is interpreted over models generated by Dense Timed Interpreted Systems (DTIS). In particular, we translate the existential model checking problem for EMTLK to the existential model checking problem for a variant of an epistemic Linear Temporal Logic with a new set of propositional variables (called ELTLK_q), and we provide an SMT-BMC technique for ELTLK_q. We have implemented our technique and tested it using the Timed Generic Pipeline Paradigm scenario. Our preliminary experimental results allow us to draw positive conclusions regarding the future applications of our new method in the automated verification of other benchmarks for RTMAS modelled by DTIS.


1 INTRODUCTION


With the development and deployment of multi-agent systems (MAS) (Wooldridge, 2009) growing demand has emerged to develop robust and comprehensive MAS verification techniques. Model checking (Clarke et al., 1999) is a well known, automatic verification technique, which helps to establish the correctness of systems. Its main idea is to represent a system as a labelled transition system (model) and a property as a modal formula, and automatically check whether the formula holds in the model. However, model checking of even moderately large MAS can be difficult due to an exponential growth of the number of states with the number of components. This phenomenon is known as the *state explosion problem*. Several state reduction techniques and symbolic model checking approaches have been developed to

avoid this problem.

One of the symbolic model checking approaches is bounded model checking (BMC) (Meški et al., 2014; Zbrzezny et al., 2015). BMC is a verification technique designed for finding witnesses of existential properties. Its main idea is to represent a witness of finite length by a propositional formula or a quantifier-free first-order formula; next, check the resulting formula with a SAT solver or an SMT solver. If the formula is satisfiable, a satisfying assignment returned by the SAT or SMT solver can be translated into a concrete witness showing that the property is violated. Otherwise, the bound is increased. Furthermore, the process repeated. Note that the satisfiability modulo theories problem (SMT) (Biere et al., 2009) is a generalisation of the SAT problem (Biere et al., 2009), where propositional variables are replaced by predicates from various background theories, such as linear, real, and integer arithmetic. In this paper, we investigate an SMT-based BMC for a real-time version of MAS with semantics based on *interpreted systems* (IS) (Fagin et al., 1995).

^a <https://orcid.org/0000-0001-9897-3561>

^b <https://orcid.org/0000-0003-2771-9683>

^c <https://orcid.org/0000-0002-1486-6572>

The formalism of IS provides a useful framework to model MASs, and to verify various classes of temporal and epistemic properties of MAS. The *timed interpreted system* (TIS) (Woźna-Szcześniak and Zbrzezny, 2016) formalism extends the IS formalism to make possible reasoning about *discrete real-time* and epistemic properties of MASs. Especially, TIS provides computationally grounded semantics on which it is possible to interpret *discrete time-bounded temporal modalities* as well as epistemic modalities. In this paper, we extend the TIS formalism to a new *dense timed interpreted system* (DTIS) formalism that yields computationally grounded semantics for real-time MAS, enabling the interpretation of both the *dense time-bounded temporal modalities* and traditional epistemic modalities. The resulting transition system that models the DTIS behaviour, which we call the *dense timed model* (DTM), can evolve in two different ways: with *action transitions* and with *time transitions*. An action transition occurs whenever an enabled join action is taken. It takes no time and may cause a change of agents' location and clock resets. A time transition affects only the clocks, which are increased by a certain (real) value and correspond to the passage of continuous time. Furthermore, due to the real-valued clock variables, the state space of DTM is infinite. To represent infinite paths of DTM by finite paths, thereby making the bounded model checking analysis feasible, we define an equivalence relation in the set of all the valuations for the clock variables that induce a finite number of states that preserve time and action transitions.

To express the MASs' requirements various extensions of standard temporal logics, for example Linear Temporal Logic (LTL) (Clarke et al., 1999) or Metric Temporal Logic (MTL) (Koymans, 1990), with epistemic (Fagin et al., 1995) modalities have been proposed. LTL allows for expressing properties about each execution of a system, e.g., *any occurrence of a problem eventually triggers the alarm*. LTL, however, is inadequate to express specifications for MAS whose correct behaviour depends on quantitative timing requirements. MTL extends LTL by constraining the temporal operators by time intervals and admits the specification of quantitative time requirements, e.g., *every problem is followed within 30 time units by an alarm*. MTLK (Woźna-Szcześniak and Zbrzezny, 2016) is an epistemic extension of MTL interpreted over discrete timed models generated by TIS, and it allows for the representation of the quantitative, but discrete-time, the temporal evolution of epistemic states of the agents. For example, *an agent P knows that each time a problem occurs, then is it followed within 30 discrete-time units by an alarm*.

In this paper, we consider an existential version of MTLK (called EMTLK) with the pointwise semantics (Bouyer, 2009) and the time domain being the non-negative real numbers. We interpret EMTLK over models generated by DTIS. The EMTLK allows for the representation of the quantitative temporal evolution of epistemic states of the agents. For example, *it is not true that an agent P knows that each time a problem occurs, then is it followed within 30 time units by an alarm*.

Contributions. We study an SMT-based BMC method for EMTLK that is interpreted over models generated by DTIS. We first define the DTIS and its dense timed model. Next, we translate the existential model checking problem for EMTLK to the existential model checking problem for a variant of an epistemic LTL with a new set of propositional variables (called ELTLK_q). Finally, we define an SMT-based BMC technique for ELTLK_q. We have implemented our technique and tested it using the Timed Generic Pipeline Paradigm scenario to illustrate new model checking techniques.

2 DENSE TIMED INTERPRETED SYSTEM

Each interpreted systems formalism consists of a set of agents and the environment in which the agents operate. Therefore, we assume a non-empty and finite set of agents $\mathbb{A} = \{1, \dots, n\}$, and a special agent \mathcal{E} that models the environment. The set of agents \mathbb{A} together with the environment \mathcal{E} constitute a MAS.

In order to model our agents formally, and to define the DTIS, we start by establishing the notation used through the paper. By \mathbb{R} we denote the set of non-negative real numbers, and by \mathbb{R}_+ the set of positive real numbers. We also assume the following:

- $\mathcal{X} = \bigcup_{c \in \mathbb{A}} \mathcal{X}_c \cup \mathcal{X}_{\mathcal{E}}$ is a finite set of non-negative real variables, called *clocks*, such that $\mathcal{X}_c \cap \mathcal{X}_d = \emptyset$, for all $c, d \in \mathbb{A} \cup \{\mathcal{E}\}$.
- $v : \mathcal{X} \mapsto \mathbb{R}$ is a total *clock valuation* function that assigns to each clock $x \in \mathcal{X}$ a non-negative real value $v(x)$.
- The set $\mathbb{R}^{|\mathcal{X}|}$ consists of all the clock valuations.
- For $Y \subseteq \mathcal{X}$ the valuation $v' = v[Y := 0]$ is defined as: $\forall x \in Y, v'(x) = 0$ and $\forall x \in \mathcal{X} \setminus Y, v'(x) = v(x)$.
- For $\delta \in \mathbb{R}$, the valuation $v' = v + \delta$ is defined as: $\forall x \in \mathcal{X}, v'(x) = v(x) + \delta$.
- Let $x \in \mathcal{X}$, $c \in \mathbb{N}$, and $\sim \in \{\leq, <, =, >, \geq\}$. The set $\mathcal{C}(\mathcal{X})$ of *clock constraints* over the set of clocks \mathcal{X} is defined by the following grammar: $cc := x \sim c \mid cc \wedge cc$.

- For any clock valuation $v \in \mathbb{R}^{|\mathcal{X}|}$ and $cc \in \mathcal{C}(\mathcal{X})$, the satisfaction relation $v \models cc$ is defined as follows: $v \models x \sim c$ iff $v(x) \sim c$, and $v \models cc \wedge cc'$ iff $v \models cc$ and $v \models cc'$.
- $\mathcal{P}\mathcal{V} = \bigcup_{\mathbf{c} \in \mathbb{A}} \mathcal{P}\mathcal{V}_{\mathbf{c}} \cup \mathcal{P}\mathcal{V}_{\mathcal{E}}$ is a set of propositional variables such that $\mathcal{P}\mathcal{V}_{\mathbf{c}} \cap \mathcal{P}\mathcal{V}_{\mathbf{d}} = \emptyset$, for all $\mathbf{c}, \mathbf{d} \in \mathbb{A} \cup \{\mathcal{E}\}$.

The formalism of *dense timed interpreted system* (DTIS) is a tuple $\mathbb{D} = (\{L_{\mathbf{c}}, \iota_{\mathbf{c}}, \Sigma_{\mathbf{c}}, \mathcal{X}_{\mathbf{c}}, P_{\mathbf{c}}, \mathcal{V}_{\mathbf{c}}, I_{\mathbf{c}}\}_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}}, \{t_{\mathbf{c}}\}_{\mathbf{c} \in \mathbb{A}}, t_{\mathcal{E}})$, where

- $L_{\mathbf{c}}$ is a non-empty and finite set of *local states* of agent (environment) \mathbf{c} . Each local state of an agent captures the complete information about the system that the agent has at a given moment. We assume that the local states of \mathcal{E} are "public".
- $\iota_{\mathbf{c}} \subseteq L_{\mathbf{c}}$ is a non-empty set of *initial local states* of agent (environment) \mathbf{c} .
- $\Sigma_{\mathbf{c}}$ is a non-empty and finite set of *local actions* of agent (environment) \mathbf{c} that are used to model the temporal evolution of the system. It is assumed that the special *null action* $\varepsilon_{\mathbf{c}}$ belongs to $\Sigma_{\mathbf{c}}$, and that all actions are "public". Each element of the set $\Sigma = \Sigma_1 \times \dots \times \Sigma_n \times \Sigma_{\mathcal{E}}$ is called the *joint action*.
- $\mathcal{X}_{\mathbf{c}}$ is a non-empty and finite set of *clocks* of agent (environment) \mathbf{c} . We assume that the clocks of the environment \mathcal{E} are "public".
- $P_{\mathbf{c}} : L_{\mathbf{c}} \mapsto 2^{\Sigma_{\mathbf{c}}}$ is a *local protocol function* that assigns to every local state a set of local actions that can be executed at that state.
- $\mathcal{V}_{\mathbf{c}} : L_{\mathbf{c}} \rightarrow 2^{\mathcal{P}\mathcal{V}_{\mathbf{c}}}$ is a *valuation function* that assigns to each local state a set of propositional variables that are true at that state.
- $I_{\mathbf{c}} : L_{\mathbf{c}} \rightarrow \mathcal{C}(\mathcal{X}_{\mathbf{c}})$ is an *invariant function* that specifies the amount of time agent (environment) \mathbf{c} may spend in its local states.
- $t_{\mathbf{c}} : L_{\mathbf{c}} \times L_{\mathcal{E}} \times \mathcal{C}(\mathcal{X}_{\mathbf{c}}) \times 2^{\mathcal{X}_{\mathbf{c}}} \times \Sigma \rightarrow L_{\mathbf{c}}$ is a (partial) *evolution function* for agent $\mathbf{c} \in \mathbb{A}$.
- $t_{\mathcal{E}} : L_{\mathcal{E}} \times \mathcal{C}(\mathcal{X}_{\mathcal{E}}) \times 2^{\mathcal{X}_{\mathcal{E}}} \times \Sigma \rightarrow L_{\mathcal{E}}$ is a (partial) *evolution function* for the environment \mathcal{E} .

We define the semantics of DTIS \mathbb{D} by associating a *dense timed model* that is a tuple $M = (\Sigma, S, \iota, T, \mathcal{V})$, where

- Σ is the set of joint actions.
- $S = \prod_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} (L_{\mathbf{c}} \times \mathbb{R}^{|\mathcal{X}_{\mathbf{c}}|})$ is the non-empty set of all *global states*. For a global state $s = ((\ell_1, v_1), \dots, (\ell_n, v_n), (\ell_{\mathcal{E}}, v_{\mathcal{E}})) \in S$, the symbol $l_{\mathbf{c}}(s) = \ell_{\mathbf{c}}$ denotes the local component of agent $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$ in s , and $v_{\mathbf{c}}(s) = v_{\mathbf{c}}$ denotes the clock valuation of agent $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$ in s .
- $\iota = \prod_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} (\iota_{\mathbf{c}} \times \{0\}^{|\mathcal{X}_{\mathbf{c}}|})$ is the non-empty set of all *initial global states* such that $\iota \subseteq S$.
- $T \subseteq S \times (\Sigma \cup \mathbb{R}) \times S$ is a transition relation defined by action and time transitions:

- Action transition: for any $\bar{a} \in \Sigma$, $(s, \bar{a}, s') \in T$ iff for all $\mathbf{c} \in \mathbb{A}$, there exists a transition $t_{\mathbf{c}}(l_{\mathbf{c}}(s), l_{\mathcal{E}}(s), cc_{\mathbf{c}}, Y, \bar{a}) = l_{\mathbf{c}}(s')$ such that $v_{\mathbf{c}}(s) \models cc_{\mathbf{c}} \wedge I_{\mathbf{c}}(l_{\mathbf{c}}(s))$ and $v'_{\mathbf{c}}(s') = v_{\mathbf{c}}(s)[Y := 0]$ and $v'_{\mathbf{c}}(s') \models I_{\mathbf{c}}(l_{\mathbf{c}}(s'))$, and there exists a transition $t_{\mathcal{E}}(l_{\mathcal{E}}(s), cc_{\mathcal{E}}, Y, \bar{a}) = l_{\mathcal{E}}(s')$ such that $v_{\mathcal{E}}(s) \models cc_{\mathcal{E}} \wedge I_{\mathcal{E}}(l_{\mathcal{E}}(s))$ and $v'_{\mathcal{E}}(s') = v_{\mathcal{E}}(s)[X' := 0]$ and $v'_{\mathcal{E}}(s') \models I_{\mathcal{E}}(l_{\mathcal{E}}(s'))$.
- Time transition: let $\delta \in \mathbb{R}_+$, $(s, \delta, s') \in T$ iff for all $\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}$, $l_{\mathbf{c}}(s) = l_{\mathbf{c}}(s')$ and $v_{\mathbf{c}}(s) \models I_{\mathbf{c}}(l_{\mathbf{c}}(s))$ and $v'_{\mathbf{c}}(s') = v_{\mathbf{c}}(s) + \delta$ and $v'_{\mathbf{c}}(s') \models I_{\mathbf{c}}(l_{\mathbf{c}}(s))$.

- $\mathcal{V} : S \rightarrow 2^{\mathcal{P}\mathcal{V}}$ is the valuation function defined as $\mathcal{V}(s) = \bigcup_{\mathbf{c} \in \mathbb{A} \cup \{\mathcal{E}\}} \mathcal{V}_{\mathbf{c}}(l_{\mathbf{c}}(s))$

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 $\bar{a} \in \Sigma$ or real number $\delta \in \mathbb{R}$ such that it holds $T(s, \bar{a}, s')$ or $T(s, \delta, s')$. Furthermore, given a DTIS and an agent $\mathbf{c} \in \mathbb{A}$, we assume the following definition of the *indistinguishability relation* : for any $s, s' \in S$, $s \sim_{\mathbf{c}} s'$ iff $l_{\mathbf{c}}(s') = l_{\mathbf{c}}(s)$.

A *run* ρ in a dense timed model that is based on the transition relation T is an infinite sequence of global states $s_0 \xrightarrow{\delta_0, \bar{a}_0} s_1 \xrightarrow{\delta_1, \bar{a}_1} s_2 \xrightarrow{\delta_2, \bar{a}_2} \dots$ such that $s_i \in S$, $\bar{a}_i \in \Sigma$, and $\delta_i \in \mathbb{R}_+$ for all $i \in \mathbb{N}$. An assumption that $\delta_i \in \mathbb{R}_+$ implies that runs are strongly monotonic, that is, every two action transitions must be separated by a time one.

3 EMTLK WITH A DENSE SEMANTICS

In what follows we assume that $\circ \in \{\wedge, \vee\}$.

Definition 3.1. Let $p \in \mathcal{P}\mathcal{V}$, $\mathbf{c} \in \mathbb{A}$, and I be an interval in \mathbb{R} of the form: $[a, b)$ or $[a, \infty)$, for $a, b \in \mathbb{N}$ and $a \neq b$. Then the formulae α of EMTLK are defined inductively:

$$\alpha := t \mid f \mid p \mid \neg p \mid \alpha \circ \alpha \mid \alpha \mathbf{U}_I \alpha \mid \mathbf{G}_I \alpha \mid \bar{\mathbf{K}}_{\mathbf{c}} \alpha.$$

The linear-time operators \mathbf{U}_I and \mathbf{G}_I are read as "bounded until" and "bounded globally", respectively. The derived basic modal operators for "bounded eventually" and "bounded release" are defined as follows: $\mathbf{F}_I \alpha \stackrel{\text{def}}{=} t \mathbf{U}_I \alpha$ and $\alpha \mathbf{R}_I \beta \stackrel{\text{def}}{=} \beta \mathbf{U}_I (\beta \wedge \alpha) \vee \mathbf{G}_I \beta$. Hereafter, if the interval I is of the form $[0, \infty)$, we omit it for the simplicity of the presentation. The epistemic operator $\bar{\mathbf{K}}_{\mathbf{c}}$ is read as "agent \mathbf{c} considers possible" and it is dual to the standard epistemic operator $\mathbf{K}_{\mathbf{c}}$, which is read as "agent \mathbf{c} knows".

To define the semantics we need the notions of a *path* λ_{ρ} corresponding to run ρ , and of a *duration function* $\mathcal{D}_{\rho} : \mathbb{N} \mapsto \mathbb{R}_+$ as in (Bouyer, 2009).

Let $M = (\Sigma, S, \iota, T, \mathcal{V})$ be a dense timed model, and $\rho = s_0 \xrightarrow{\delta_0, a_0} s_1 \xrightarrow{\delta_1, a_1} s_2 \xrightarrow{\delta_2, a_2} \dots$ a run in M . Each run generates the unambiguous path $\lambda_\rho : \mathbb{N} \rightarrow S$, because we consider only the strongly monotonic runs. Further, $\Pi(s)$ denotes the set of all the paths starting at $s \in S$, and $\Pi = \bigcup_{s \in S} \Pi(s^0)$ is the set of all the paths starting at all initial states. Finally, given a run ρ and a position $j \geq 0$, a *duration function* $\mathcal{D}_\rho(j)$ returns the sum of all the time transitions along the run ρ till the position j .

Definition 3.2. Let α and β be EMTLK formulae, M the dense timed model, and λ_ρ a path. By $\lambda_\rho[n]$ we denote the path λ_ρ with a designated formula evaluation position $n \in \mathbb{N}$. An EMTLK formula α is true along a path λ_ρ (in symbols $M, \lambda_\rho \models \alpha$) iff $M, \lambda_\rho[0] \models \alpha$, where

- $M, \lambda_\rho[n] \models p$ iff $p \in \mathcal{V}(\lambda_\rho(n))$,
- $M, \lambda_\rho[n] \models \neg p$ iff $p \notin \mathcal{V}(\lambda_\rho(n))$,
- $M, \lambda_\rho[n] \models \alpha \mathbf{U}_I \beta$ iff $(\exists j \geq n) ((\mathcal{D}_\rho(j) - \mathcal{D}_\rho(n)) \in I \text{ and } M, \lambda_\rho[n+j] \models \beta \text{ and } (\forall n \leq i < j) (M, \lambda_\rho[n+i] \models \alpha))$,
- $M, \lambda_\rho[n] \models \mathbf{G}_I \beta$ iff $(\forall j \geq n) ((\mathcal{D}_\rho(j) - \mathcal{D}_\rho(n)) \in I \text{ implies } M, \lambda_\rho[n+j] \models \beta)$,
- $M, \lambda_\rho[n] \models \overline{\mathbf{K}}_c \alpha$ iff $(\exists \pi \in \Pi)(\exists i \geq 0)(\pi(i) \sim_c \lambda_\rho(n) \text{ and } M, \pi[i] \models \alpha)$.

The semantics of the Boolean constants t and f , and propositional operators \vee and \wedge is defined in the standard way.

The EMTLK formula φ is *existentially valid* in the model M (written $M \models \varphi$) iff $M, \lambda_\rho \models \varphi$ for some path $\lambda_\rho \in \Pi$. The *existential model checking* problem asks whether $M \models \varphi$.

4 TRANSLATION FROM EMTLK TO ELTLK_q

Definition 4.1. Let I be an interval as assumed in Def. 3.1, $I\mathcal{V}$ the set of all intervals in \mathbb{R} , and $\mathcal{P}\mathcal{V}_{I\mathcal{V}} = \{q_I \mid I \in I\mathcal{V}\}$. The formulae α of ELTLK_q are defined inductively:

$$\alpha := t \mid f \mid v \mid \neg v \mid \alpha \circ \alpha \mid \alpha \mathbf{U} \alpha \mid \mathbf{G} \alpha \mid \overline{\mathbf{K}}_c \alpha$$

where $v \in \mathcal{P}\mathcal{V} \cup \mathcal{P}\mathcal{V}_{I\mathcal{V}}$ and $c \in \mathbb{A}$.

The modal operators \mathbf{U} and \mathbf{G} are read as the “*until*” and the “*globally*”, respectively. The modal operator $\overline{\mathbf{K}}_c$ is the standard epistemic modality for “agent c considers possible”.

Definition 4.2. Let α and β be ELTLK_q formulae, M the dense timed model, and λ_ρ a path. By $\lambda_\rho[n]$ we denote the path λ_ρ with a designated formula evaluation position $n \in \mathbb{N}$. The satisfiability relation \models^d , which

indicates truth of an ELTLK_q formula in the model M along the path λ_ρ with the starting point n and at the depth $d \geq n$, is defined inductively as follows:

- $M, \lambda_\rho[n] \models^d p$ iff $p \in \mathcal{V}(\lambda_\rho(d))$,
- $M, \lambda_\rho[n] \models^d \neg p$ iff $p \notin \mathcal{V}(\lambda_\rho(d))$,
- $M, \lambda_\rho[n] \models^d q_I$ iff $\mathcal{D}_\rho(d) - \mathcal{D}_\rho(n) \in I$,
- $M, \lambda_\rho[n] \models^d \neg q_I$ iff $\mathcal{D}_\rho(d) - \mathcal{D}_\rho(n) \notin I$,
- $M, \lambda_\rho[n] \models^d \alpha \mathbf{U} \beta$ iff $(\exists j \geq d) (M, \lambda_\rho[d] \models^j \beta \text{ and } (\forall d \leq i < j) (M, \lambda_\rho[d] \models^i \alpha))$,
- $M, \lambda_\rho[n] \models^d \mathbf{G} \beta$ iff $(\forall i \geq d) M, \lambda_\rho[d] \models^i \beta$,
- $M, \lambda_\rho[n] \models^d \overline{\mathbf{K}}_c \alpha$ iff $(\exists \lambda_{\rho'} \in \Pi)(\exists i \geq 0) (\lambda_{\rho'}(i) \sim_c \lambda_\rho(d) \text{ and } M, \lambda_{\rho'}[0] \models^i \alpha)$.

The semantics of the Boolean constants t and f , and propositional operators \vee and \wedge is defined in the standard way.

An ELTLK_q formula φ is *existentially valid* in the model M (written $M \models \varphi$) iff $M, \lambda_\rho[0] \models^0 \varphi$ for some path $\lambda_\rho \in \Pi$. The *existential model checking* problem asks whether $M \models \varphi$.

Let $p \in \mathcal{P}\mathcal{V}$, α, β be formulae of EMTLK. We define the translation from EMTLK into ELTLK_q as a function $\text{tr} : \text{EMTLK} \rightarrow \text{ELTLK}_q$ in the following way: $\text{tr}(t) = t$, $\text{tr}(f) = f$, $\text{tr}(p) = p$, $\text{tr}(\neg p) = \neg p$, $\text{tr}(\alpha \wedge \beta) = \text{tr}(\alpha) \wedge \text{tr}(\beta)$, $\text{tr}(\alpha \vee \beta) = \text{tr}(\alpha) \vee \text{tr}(\beta)$, $\text{tr}(\alpha \mathbf{U}_I \beta) = \text{tr}(\alpha) \mathbf{U} \text{tr}(q_I \wedge \beta)$, $\text{tr}(\mathbf{G}_I \beta) = \mathbf{G}(\neg q_I \vee \text{tr}(\beta))$, $\text{tr}(\overline{\mathbf{K}}_c \alpha) = \overline{\mathbf{K}}_c \text{tr}(\alpha)$.

Observe that the translation of literals as well as Boolean connectives is straightforward. The translation of \mathbf{U}_I ensures that β holds somewhere in the interval I (expressed by the requirement $q_I \wedge \text{tr}(\beta)$), and α holds always before β . Similarly, the translation of \mathbf{G}_I ensures that β always holds in the interval I (expressed by the requirement $\neg q_I \vee \text{tr}(\beta)$).

The following theorem can be proven by induction on the length of the EMTLK formula.

Theorem 4.1. Let M be the dense timed model, and φ an EMTLK formula. Then, $M \models \varphi$ iff $M \models \text{tr}(\varphi)$.

5 SMT-BASED BMC OF ELTLK_q PROPERTIES

5.1 Bounded Semantics

We start by recalling some basic definitions of k -path and *loop* that allow to represent infinite paths of the dense timed model M in a finite way.

Definition 5.1. Let M be the dense timed model, $k \in \mathbb{N}$, and $0 \leq l \leq k$. A k -path is a pair (π, l) , also denoted by π_l , where π is a finite sequence $\pi = (s_0, \dots, s_k)$ of states such that for each

$0 \leq j < k$, either $(s_j \xrightarrow{\delta} s_{j+1})$ for some $\delta \in \mathbb{R}_+$, or $(s_j \xrightarrow{\bar{a}} s_{j+1})$ for some $\bar{a} \in \Sigma$, and every action transition is preceded by at least one time transition. A k -path π_l is a loop, written $\tilde{\pi}_l$ for short, if $l < k$, $l_c(\pi(k)) = l_c(\pi(l))$ for each agent $\mathbf{c} \in \mathbb{A}$, and $(v_1(\pi(k)), \dots, v_n(\pi(k)), v_{\mathcal{E}}(\pi(k))) \simeq (v_1(\pi(l)), \dots, v_n(\pi(l)), v_{\mathcal{E}}(\pi(l)))$, where \simeq is the equivalence relation on the set of all the clock valuations defined as in (Alur et al., 1993).

If a k -path π_l is a loop, then it represents the infinite path of the form uv^ω , where $u = (\pi(0), \dots, \pi(l))$ and $v = (\pi(l+1), \dots, \pi(k))$. We denote this unique path by $\tilde{\pi}_l$. Note that for each $j \in \mathbb{N}$, $\tilde{\pi}_l^{l+j} = \tilde{\pi}_l^{k+j}$. Furthermore, by $\Pi_k(s)$ we denote the set of all the k -paths starting at $s \in S$, and we define the set of all the k -paths starting at all initial states in S as: $\Pi_k = \bigcup_{s^0 \in I} \Pi_k(s^0)$.

Definition 5.2 (Bounded Semantics). *Let α and β be ELTLK_q formulae, M the dense timed model, π_l a k -path, and $0 \leq n, d \leq k$. The satisfiability relation \models_k^d , which indicates truth of an ELTLK_q formula in the model M along the k -path π_l with the starting point n and at the depth d is defined inductively as follows:*

- $M, \pi_l[n] \models_k^d p$ iff $p \in \mathcal{V}(\pi_l(d))$,
- $M, \pi_l[n] \models_k^d \neg p$ iff $p \notin \mathcal{V}(\pi_l(d))$,
- $M, \pi_l[n] \models_k^d q_l$ iff
 1. $\mathcal{D}_{\tilde{\pi}_l}(d) - \mathcal{D}_{\tilde{\pi}_l}(n) \in I$, if π_l is not a loop,
 2. $\mathcal{D}_{\tilde{\pi}_l}(d) - \mathcal{D}_{\tilde{\pi}_l}(n) \in I$, if π_l is a loop and $d \geq n$,
 3. $\mathcal{D}_{\tilde{\pi}_l}(d+k-l) - \mathcal{D}_{\tilde{\pi}_l}(n) \in I$, if π_l is a loop and $d < n$,
- $M, \pi_l[n] \models_k^d \neg q_l$ iff $M, \pi_l[n] \not\models_k^d q_l$
- $M, \pi_l[n] \models_k^d \alpha \cup \beta$ iff $(\exists d \leq j \leq k) (M, \pi_l[d] \models_k^j \beta$ and $(\forall d \leq i < j) M, \pi_l[d] \models_k^i \alpha)$ or $(\pi_l$ is a loop and $(\exists l < j < d) M, \pi_l[d] \models_k^j \beta$ and $(\forall l < i < k) M, \pi_l[d] \models_k^i \alpha$ and $(\forall d \leq i \leq k) M, \pi_l[d] \models_k^i \alpha)$,
- $M, \pi_l[n] \models_k^d \mathbf{G}\beta$ iff $\text{loop}(\pi_l)$ and $(\forall i \leq k) (i \geq \min(d, l) \text{ implies } M, \pi_l[d] \models_k^i \beta)$,
- $M, \pi_l[n] \models_k^d \bar{\mathbf{K}}_c \alpha$ iff $(\exists \pi'_l \in \Pi_k) (\exists 0 \leq i \leq k) (M, \pi'_l[0] \models_k^i \alpha$ and $\pi(d) \sim_c \pi'(i)$).

The semantics of the Boolean constants t and f , and propositional operators \vee and \wedge is defined in the standard way.

Observe that to evaluate propositional variables we use only finite prefixes of the sequence $(\mathcal{D}_{\pi_l}(0), \mathcal{D}_{\pi_l}(1), \dots)$. Namely, if a k -path π_l is not a loop, then we have to consider the prefix of the length k only. However, if a k -path π_l is a loop, then we have to consider the prefix of the length $k + k - l$.

An ELTLK_q formula φ is *existentially k -valid* in the model M , written $M \models_k \varphi$, iff $M, \pi_l[0] \models_k^0 \varphi$ for some k -path π_l starting at the initial state.

The proof of Lemma 5.1 below is based on induction on the length of the given formula. It is analogous to the proof of Lemma 7 from the paper (Biere et al., 1999).

Lemma 5.1. *Let M be the dense timed model. For each ELTLK_q formula φ , each k -path π_l in M , each $0 \leq m \leq k$ and each $0 \leq d \leq k$, if $M, \pi_l[m] \models_k^d \varphi$, then there exists a path π' such that $\pi'[\dots] = \pi_l$ and: $m \leq d$ and $M, \pi'[m] \models^d \varphi$ or $m > d$ and $M, \pi'[m] \models^{d+k-l} \varphi$.*

The proof of the Lemma 5.2 below is based on the well-known fact that if the LTL formula is true on some infinite path, it is also true on an infinite path of the form uv^ω , where u and v are finite sequences of states (Biere et al., 1999).

Lemma 5.2. *Let M the dense timed model, π a path in the model, and $k \geq 0$. For each ELTLK_q formula φ , each $0 \leq m \leq k$ and each $0 \leq d \leq k$, if $M, \pi[m] \models^d \varphi$, there exists a k -path π_l such that $M, \pi_l[m] \models_k^d \varphi$.*

Theorem 5.1 shows that for some specific bound, bounded and unbounded semantics are equivalent. The proof of Theorem 5.1 follows directly from Lemmas 5.1 and 5.2.

Theorem 5.1. *Let M be the dense timed model for the dense timed interpreted system \mathbb{D} , φ an ELTLK_q formula, and $\psi = \text{tr}(\varphi)$ an ELTLK_q formula. Then, $M \models \psi$ iff there exists $k \geq 0$ such that $M \models_k \varphi$.*

5.2 Translation to SMT

The presented SMT encoding of the BMC problem for ELTLK_q and for a DTIS is based on the SMT encoding presented in (Zbrzezny and Zbrzezny, 2017). It consists in encoding of both the transition relation of the dense timed model M , and the ELTLK_q formula $\text{tr}(\varphi)$ as a quantifier-free first-order formula. The novelty of the encoding lies in encoding of both the transition relation of the dense timed model, and the finite prefix of the sequence $(\mathcal{D}_{\pi_l}(0), \mathcal{D}_{\pi_l}(1), \dots)$.

Let M be a dense timed model, φ an EMTLK formula, $\psi = \text{tr}(\varphi)$ the ELTLK_q formula, and $k \in \mathbb{N}$ a bound. The main idea of the SMT-based BMC method consists in translating the BMC problem, i.e., $M \models_k \psi$, to the satisfiability problem of the following formula:

$$[M, \psi]_k := [M^{\Psi, 1}]_k \wedge [\psi]_{M, k}.$$

The definition of the formula $[M, \psi]_k$ assumes that each global state $s \in S$ of M can be represented by a valuation of a symbolic global state $\bar{\mathbf{w}} = (\bar{\mathbf{w}}_1, \dots, \bar{\mathbf{w}}_n, \bar{\mathbf{w}}_{\mathcal{E}})$ that consists of symbolic local states. Each $\bar{\mathbf{w}}_c$ is a pair (w_c, v_c) of individual integer variables ranging over the natural numbers (encoding a local state of the agent \mathbf{c}) and individual real

variables ranging over the real numbers (encoding a clock valuation of the agent \mathbf{c}). Similarly, each action $a \in \Sigma$ can be represented by a valuation of a symbolic joint action $\bar{\mathbf{a}}$ that is a vector of the individual variables ranging over the natural number.

The formula $[M^{\Psi,1}]_k$ constrains the $f_k(\Psi)$ symbolic k -paths to be valid k -paths of M , while the formula $[\Psi]_{M,k}$ encodes a number of constraints that must be satisfied on these sets of k -paths for $\Psi = \text{tr}(\Phi)$ to be satisfied. Note that the exact number of necessary symbolic k -paths depends on the checked formula Ψ , and it can be calculated using the function $f_k : \text{EMTLK} \rightarrow \mathbb{N}$ as in (Meški et al., 2014). The number of k -paths sufficient to validate Ψ is given by the function that is defined as $\hat{f}_k(\Psi) = f_k(\Psi) + 1$.

Let $\bar{\mathbf{w}}$ and $\bar{\mathbf{w}}'$ be two different symbolic states, $\bar{\mathbf{a}}$ a symbolic action, $\hat{\delta}$ a symbolic time passage, and u be a symbolic number. We assume definitions of the following auxiliary quantifier-free first-order formulae as in (Zbrzezny, 2012): $I_s(\bar{\mathbf{w}})$ that encodes the state s of the dense timed model M , $p(\bar{\mathbf{w}})$ that encodes the set of states of M in which $p \in \mathcal{PV}$ holds, $H_{\mathbf{c}}(\bar{\mathbf{w}}_{\mathbf{c}}, \bar{\mathbf{w}}'_{\mathbf{c}})$ that encodes equivalence of two local states for $\mathbf{c} \in \mathbb{A} \cup \mathbb{E}$, $H(\bar{\mathbf{w}}, \bar{\mathbf{w}}')$ that encodes equivalence of two global states such that $(w_1, \dots, w_n, w_{\mathbb{E}}) = (w'_1, \dots, w'_n, w'_{\mathbb{E}})$ and $(v_1, \dots, v_n, v_{\mathbb{E}}) \simeq (v'_1, \dots, v'_n, v'_{\mathbb{E}})$, $\mathcal{T}_{\Sigma}(\bar{\mathbf{w}}, \bar{\mathbf{a}}, \bar{\mathbf{w}}')$ that encodes action transitions of M , and $\mathcal{T}_{\delta}(\bar{\mathbf{w}}, \hat{\delta}, \bar{\mathbf{w}}')$ that encodes time transitions of M . A pair consisting of a sequence of symbolic transitions and a symbolic number is called a symbolic k -path. Let π_j denote the j -th symbolic k -path: $(\bar{\mathbf{w}}_{0,j} \xrightarrow{\hat{\delta}} \dots \xrightarrow{\hat{\delta}} \bar{\mathbf{w}}_{0,j} \xrightarrow{\bar{\mathbf{a}}_{1,j}} \bar{\mathbf{w}}_1 \xrightarrow{\hat{\delta}} \dots \xrightarrow{\hat{\delta}} \bar{\mathbf{w}}_{1,j} \xrightarrow{\bar{\mathbf{a}}_{2,j}} \dots \xrightarrow{\hat{\delta}} \bar{\mathbf{w}}_{k-1} \xrightarrow{\bar{\mathbf{a}}_{k,j}} \bar{\mathbf{w}}_{k,j}, u_j)$, where $\bar{\mathbf{w}}_{i,j}$ are symbolic states, $\bar{\mathbf{a}}_{i,j}$ are symbolic actions, and u_j is a symbolic number for $0 \leq i \leq k$ and $1 \leq j \leq \hat{f}_k(\Psi)$. Further, let the function $Gt^m(\pi_n)$ encode a global time on the symbolic k -path π_n at the depth m .

The formula $[\Psi]_{M,k}$ encodes the bounded semantics of an EMTLK_q formula $\Psi = \text{tr}(\Phi)$, and it is defined on the same sets of individual variables as the formula $[M^{\Psi,1}]_k$.

Let $F_k(\Psi) = \{j \in \mathbb{N} \mid 1 \leq j \leq \hat{f}_k(\Psi)\}$, and $[\Psi]_k^{[m,n,A]}$ denote the translation of Ψ along the n -th symbolic path π_n^m with the starting point m by using the set $A \subseteq F_k(\Psi)$. Then, the next step is a translation of an EMTLK_q formula Ψ to a quantifier-free first-order formula

$$[\Psi]_{M,k} := [\Psi]_k^{[0,1,F_k(\Psi)]}.$$

Definition 5.3 ((Zbrzezny, 2012)). *Let M be a dense timed model, Ψ an EMTLK_q formula, and $k \geq 0$ a*

bound. We define inductively the translation of Ψ over a path number $n \in F_k(\Psi)$ starting at the symbolic state $\bar{\mathbf{w}}_{d,n}$ at the depth m as shown below, where $n' = \min(A)$:

- $[qI]_{[k,m]}^{[d,n,A]} :=$
 1. $\bigvee_{l=0}^{k-1} (Gt^d(\pi_n) - Gt^m(\pi_n) \in I \wedge \neg H(\bar{\mathbf{w}}_{k,n}, \bar{\mathbf{w}}_{l,n})) \vee \bigvee_{l=0}^{k-1} (Gt^d(\pi_n) - Gt^m(\pi_n) \in I \wedge H(\bar{\mathbf{w}}_{k,n}, \bar{\mathbf{w}}_{l,n}))$, if $m \geq d$,
 2. $\bigvee_{l=0}^{k-1} (Gt^d(\pi_n) - Gt^m(\pi_n) \in I \wedge \neg H(\bar{\mathbf{w}}_{k,n}, \bar{\mathbf{w}}_{l,n})) \vee \bigvee_{l=0}^{k-1} (Gt^{d+k-l}(\pi_n) - Gt^m(\pi_n) \in I \wedge H(\bar{\mathbf{w}}_{k,n}, \bar{\mathbf{w}}_{l,n}))$, if $d < m$,
- $[\neg qI]_{[k,m]}^{[d,n,A]} := \neg[qI]_{[k,m]}^{[d,n,A]}$,
- $[\bar{\mathbf{K}}\mathbf{c}\alpha]_{[k,m]}^{[d,n,A]} := \bigvee_{s \in I} I_s(\bar{\mathbf{w}}_{0,n'}) \wedge \bigvee_{j=0}^k ([\alpha]_{[k,m]}^{[j,n',g_s(A)]} \wedge H_{\mathbf{c}}(\bar{\mathbf{w}}_{d,n}, \bar{\mathbf{w}}_{j,n'}))$.

For the Boolean constants t and f , propositional variables $\in \mathcal{PV}$, propositional operators \vee and \wedge , and temporal operators \mathbf{U} and \mathbf{G} the translation is defined as in (Zbrzezny, 2012; Woźna-Szcześniak and Zbrzezny, 2016; Zbrzezny and Zbrzezny, 2017).

Let $\bar{\mathbf{w}}_{i,j}$, $\bar{\mathbf{a}}_{i,j}$, and $\hat{\delta}_{i,j}$ are, respectively, symbolic states, symbolic actions, and symbolic time passage for $0 \leq i \leq k$ and $1 \leq j \leq \hat{f}_k(\Psi)$. Now, we can define the formula $[M^{\Psi,1}]_k$ as follows:

$$\bigvee_{s \in I} I_s(\bar{\mathbf{w}}_{0,0}) \wedge \bigvee_{j=1}^{\hat{f}_k(\Psi)} H(\bar{\mathbf{w}}_{0,0}, \bar{\mathbf{w}}_{0,j}) \wedge \bigwedge_{j=1}^{\hat{f}_k(\Psi)} \bigvee_{l=0}^{k-1} l = u_j \wedge \bigwedge_{j=1}^{\hat{f}_k(\Psi)} \left(\mathcal{T}_{\delta}(\bar{\mathbf{w}}_{0,j}, \hat{\delta}, \bar{\mathbf{w}}_{1,j}) \wedge \bigwedge_{i=1}^{k-1} \left(\mathcal{T}_{\delta}(\bar{\mathbf{w}}_{i,j}, \hat{\delta}, \bar{\mathbf{w}}_{i+1,j}) \vee \mathcal{T}_{\Sigma}(\bar{\mathbf{w}}_{i,j}, \bar{\mathbf{a}}_{i,j}, \bar{\mathbf{w}}_{i+1,j}) \right) \wedge \bigwedge_{i=1}^{k-2} \left(\mathcal{T}_{\delta}(\bar{\mathbf{w}}_{i,j}, \hat{\delta}, \bar{\mathbf{w}}_{i+1,j}) \vee \mathcal{T}_{\delta}(\bar{\mathbf{w}}_{i+1,j}, \hat{\delta}, \bar{\mathbf{w}}_{i+2,j}) \right) \right).$$

The following theorem states that the translation is correct and complete.

Theorem 5.2. *Let M be a dense timed model, Φ an EMTLK formula, and $\text{tr}(\Phi)$ an EMTLK_q formula. Then, for every $k \in \mathbb{N}$, $M \models_k^d \text{tr}(\Phi)$ iff, the quantifier-free first-order formula $[M, \text{tr}(\Phi)]_k$ is satisfiable.*

6 EXPERIMENTAL RESULTS

In this section, we experimentally evaluate the performance of our new translation. To this aim, we have conducted the experiments using the slightly modified

timed generic pipeline paradigm (TGPP) (Woźna-Szcześniak and Zbrzezny, 2014).

The DTIS for the TGPP (Zbrzezny and Zbrzezny, 2017) consists of $n + 2$ agents: a *Producer* producing data within the certain time interval $([a, b])$ or being inactive, a *Consumer* receiving data within the certain time interval $([c, d])$ or being inactive within the certain time interval $([g, h])$, and a chain of n intermediate *Nodes* that can be ready for receiving data within the certain time interval $([c, d])$, processing data within the certain time interval $([e, f])$ or sending data. We assume that $a = c = e = g = 1$ and $b = d = f = h = 2 \cdot n + 2$, where n represents a number of nodes. We have tested the TGPP dense timed interpreted system model, scaled in the number of intermediate nodes on the following EMTLK formulae that existentially hold in the model of TGPP (n is the number of nodes, *ConRec* stands for *ConsReceived*, and *PrdSend* stands for *ProdSend*):

- $\varphi_1 = \mathbf{G}(\mathbf{K}_P(\text{PrdSend} \Rightarrow \mathbf{F}_{[0, 2n+2]}(\text{ConRec})))$. It states that Producer knows that each time Producer produces data, then Consumer receives this data in time less than $2n + 1$.
- $\varphi_2 = \mathbf{K}_C(\mathbf{K}_P(\mathbf{F}_{[0, 2n+2]}(\text{ConRec})))$. It states that Consumer knows that Producer knows that finally Consumer will receive data in time less than $2n + 2$.
- $\varphi_3 = \mathbf{K}_P(\text{ConRec} \Rightarrow \mathbf{F}_{[0, 2n+1]}(\neg \text{ConRec}))$. It states that Producer knows that time Consumer receives data, then Consumer is ready to receive data in time less than $2n + 1$ after that Consumer will receive data.

The number of considered k -paths for the properties φ_1 , and φ_3 is equal to 2, and for the property φ_2 is equal to 3.

We have performed our experiments on a computer equipped with I7-3770 processor, 32 GB of RAM, and the operating system Linux. We implemented our SMT-BMC algorithm as a standalone program that is written in C++. We used the SMT-solvers Z3 (Moura and Bjørner, 2008) in version 4.8.9, and Yices2 (Dutertre, 2014) in version 2.6.2.

The line charts in Figures 1-3, show the total time and the memory consumption for all the tested properties. Our SMT-BMC program generated SMT files that we have tested using SMT-solvers. The results we have got allowed us to confirm the efficiency of our method. By the way, we can compare the efficiency of mentioned above SMT-solvers. For all the formulae Yices SMT-solver outperforms Z3, and it could verify the TGPP system with more nodes.

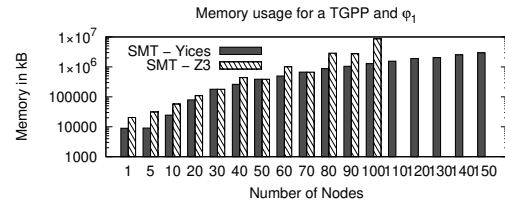
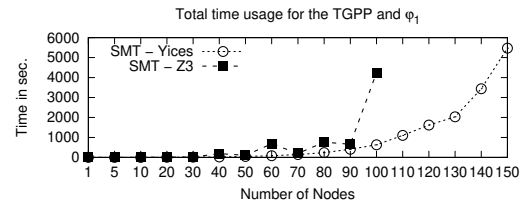


Figure 1: φ_1 : TGPP with n nodes.

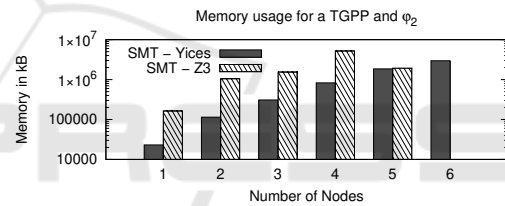
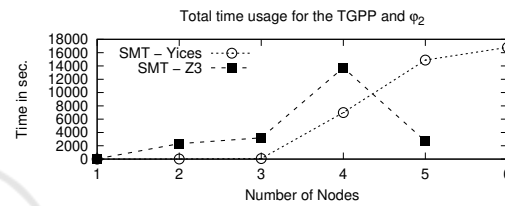


Figure 2: φ_2 : TGPP with n nodes.

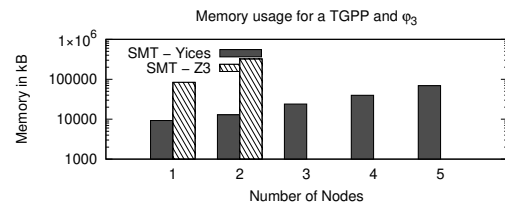
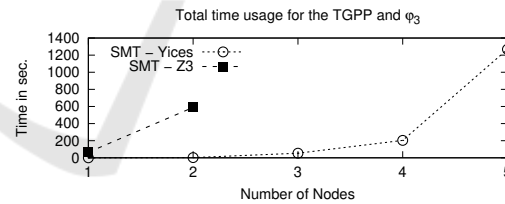


Figure 3: φ_3 : TGPP with n nodes.

7 CONCLUSIONS AND FUTURE WORK

We have proposed, implemented, and experimentally evaluated SMT-based BMC method for dense timed interpreted systems and for properties expressible in

EMTLK with the semantics over dense timed interpreted systems. The method is based on a translation of the existential model checking for EMTLK to the existential model checking for ELTLK_q, and then on the translation of the existential model checking for ELTLK_q to the quantifier-free first-order formula.

The paper presents preliminary experimental results only, but they show that the proposed verification method is quite efficient and worth exploring. We plan to explore also the SAT-based BMC method.

Zbrzezny, A. M., Woźna-Szcześniak, B., and Zbrzezny, A. (2015). SMT-based bounded model checking for weighted epistemic ECTL. In *Proceedings of EPIA'2015*, pages 651–657. Springer.

Zbrzezny, A. M. and Zbrzezny, A. (2017). Simple SMT-based bounded model checking for timed interpreted systems. In *Proceedings of IJCRS'2017*, volume 10314 of *LNAI*, pages 487–504. Springer.

REFERENCES

- Alur, R., Courcoubetis, C., and Dill, D. (1993). Model checking in dense real-time. *Information and Computation*, 104(1):2–34.
- Biere, A., Cimatti, A., Clarke, E., and Zhu, Y. (1999). Symbolic model checking without BDDs. In *TACAS'99*, volume 1579 of *LNCS*, pages 193–207. Springer-Verlag.
- Biere, A., Heule, M., van Maaren, H., and Walsh, T. (2009). *Handbook of Satisfiability: Volume 185 Frontiers in Artificial Intelligence and Applications*. IOS Press.
- Bouyer, P. (2009). Model-checking timed temporal logics. *Electr. Notes Theor. Comput. Sci.*, 231:323–341.
- Clarke, E., Grumberg, O., and Peled, D. (1999). *Model Checking*. The MIT Press.
- Dutertre, B. (2014). Yices 2.2. In *Proceedings of CAV'2014*, pages 737–744.
- Fagin, R., Halpern, J., Moses, Y., and Vardi, M. Y. (1995). *Reasoning about Knowledge*. MIT Press. ISBN: 0-262-06162-7.
- Koymans, R. (1990). Specifying real-time properties with metric temporal logic. *Real-Time Systems*, 2(4):255–299.
- Męski, A., Penczek, W., Szreter, M., Woźna-Szcześniak, B., and Zbrzezny, A. (2014). 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.
- Moura, L. D. and Bjørner, N. (2008). Z3: an efficient SMT solver. In *Proceedings of TACAS'2008*, volume 4963 of *LNCS*, pages 337–340. Springer-Verlag.
- Woźna-Szcześniak, B. and Zbrzezny, A. (2014). Checking MTL properties of discrete timed automata via bounded model checking. *Fundam. Inform.*, 135(4):553–568.
- Wooldridge, M. (2009). *An introduction to multi-agent systems - Second Edition*. John Wiley & Sons.
- Woźna-Szcześniak, B. and Zbrzezny, A. (2016). Checking EMTLK properties of timed interpreted systems via bounded model checking. *Studia Logica*, 104(4):641–678.
- Zbrzezny, A. (2012). A new translation from ECTL* to SAT. *Fundamenta Informaticae*, 120(3-4):377–397.