Li *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2020) 9:65
https://doi.org/10.1186/s13677-020-00209-3

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

A spatio-temporal specification language and its completeness & decidability

Tengfei Li[1], Jing Liu[1], Haiying Sun[1*†], Xiang Chen[2], Lipeng Zhang[2†] and Junfeng Sun[2]

Abstract

In the past few years, significant progress has been made on spatio-temporal cyber-physical systems in achieving spatio-temporal properties on several long-standing tasks. With the broader specification of spatio-temporal properties on various applications, the concerns over their spatio-temporal logics have been raised in public, especially after the widely reported safety-critical systems involving self-driving cars, intelligent transportation system, image processing. In this paper, we present a spatio-temporal specification language, $STSL_{PC}$, by combining Signal Temporal Logic (STL) with a spatial logic $S4_u$, to characterize spatio-temporal dynamic behaviors of cyber-physical systems. This language is highly expressive: it allows the description of quantitative signals, by expressing spatio-temporal traces over real valued signals in dense time, and Boolean signals, by constraining values of spatial objects across threshold predicates. $STSL_{PC}$ combines the power of temporal modalities and spatial operators, and enjoys important properties such as finite model property. We provide a Hilbert-style axiomatization for the proposed $STSL_{PC}$ and prove the soundness and completeness by the spatio-temporal extension of maximal consistent set and canonical model. Further, we demonstrate the decidability of $STSL_{PC}$ and analyze the complexity of $STSL_{PC}$. Besides, we generalize STSL to the evolution of spatial objects over time, called $STSL_{OC}$, and provide the proof of its axiomatization system and decidability.

Keywords: Signal temporal logic (STL), $S4_u$, Spatio-temporal specification language (STSL), Axiomatization system; Decidability

Introduction

It is a challenging work to model cyber-physical systems, not only because cyber-physical systems integrate cyber systems, physical environment and the interactive part of them, but also because cyber-physical systems combine temporal and spatial aspects, discrete and continuous behaviors, and nondeterministic models [1]. Describing spatio-temporal aspects is one of the important areas in cyber-physical systems. Many works have been done with concurrent [2], hybrid [3–5] and stochastic [6, 7] behaviors of motion-based spatially distributed systems [8], but fewer researchers concentrate on spatio-temporal aspects. The major problem is multidimensional expressiveness and expensive verifiability for modeling and analysis of the spatio-temporal behaviors of cyber-physical systems.

This work aims at building a spatio-temporal specification language by solving spatio-temporal constraints concerning dense time and real-valued variables, because an intelligent object in physical environment is equipped with changes in specified space and continuous time. More specifically, we confine ourselves to the combination of topometric space [9] and time constraints with real-valued interval, which is a half-open and half-closed interval in a time flow of a strict partial ordering of time points. We adopt the modal spatial logic $S4_u$ to express topometric constraints, which is one of the most influential form and the most expressiveness for topometric relations. For signal temporal logic (STL) [10, 11], there are two interpretations for signals, quantitative semantics and Boolean semantics. Quantitative semantics obtains

*Correspondence: hysun@sei.ecnu.edu.cn
†Haiying Sun and Lipeng Zhang contributed equally to this work.
[1]Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, No. 3663, North Zhongshan Road, 200062 Shanghai, China
Full list of author information is available at the end of the article

Springer Open

© The Author(s). 2020 **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

real-valued signals from *satisfaction degree* of a trace over real-valued interval. While Boolean semantics evaluates Boolean signals from a trace which can be booleanized through a set of threshold predicates.

Because the changes of spatial entities and the flows of time are not independent, the combination between modal spatial and temporal logic is divided into two forms: STSL_{PC} and STSL_{OC}. STSL_{PC} means the changes of spatial propositions over time, while STSL_{OC} represents the changes or evolution of spatial objects over time. Each form is equipped with different expressiveness, so Boolean semantics and quantitative semantics for the two forms need to be provided respectively. Combining spatio-temporal constraints from temporal logic and modal spatial logic is a very important problem. Given a topometric temporal model $\mathfrak{M}$ and an STSL_{PC} formula φ, the satisfiability problem of the formula φ is to check whether φ is satisfiable against model $\mathfrak{M}$ or not. We present the semantics for the proposed language according to the satisfaction relations.

Many works have been done on the axiomatization and completeness of combined logics. The completeness of normal modal logic is present through maximal consistent set and canonical model [12]. J.M. Davoren [13] proposes topological semantics for intuitionistic tense logics and multi-modal logic and provide the Hilbert-style axiomatization and the completeness result. F.D. David [14] proves the absolute completeness of S4_u for its measure-theoretic semantics. Based on our previous work [15], in this paper, we present an axiomatization system for STSL_{PC} and prove the soundness and completeness result of the axiomatization system based on maximal consistent set and canonical model. Further, the notation of finite model property provides a basis for the decidability of logics. The filtration, which is similar to bisimulation quotients with respect to equivalences generated by sets of formulae [16], can serve as an approach to achieve the finite model property. By way of the finite frame property, decidability can be proved by applying subframe transformations and a variant of the filtration technique [17]. The decidability of STSL_{PC} is proved according to the finite model property. For the decidable fragment, we present the complexity for the satisfiability problem and the decision procedure.

Compared with the another work [18] reasoning cyber-physical systems, DTL defines the trace to uniform discrete jumps and continuous evolution. Control operations in discrete jumps can control the continuous evolution along differential equations, which are interpreted in hybrid trace and verified through the differential invariant. Our proposed STSL_{PC} is interpreted on the sampling trace of state-based cyber-physical systems, where the formulas are verified through monitoring partial trace, instead of classical model checking, which needs to achieve all the behaviors of the systems. Further, A time scale is defined as arbitrary nonempty closed subset of the real numbers [19]. The continuity is defined according to the density of time scale. A differential equations employ the notation of differentiation and density of a time scale by delta derivative of a function at time t, while STSL_{PC} applies the time interval to express a duration. When STSL involves in dense time, we can use the notation of "time scale", but we never mention the notation of "differentiation". This paper is an expanded version of the SEKE 2019 conference paper [15], and includes all the notions required for the construction for proving the decidability. We reorganize the work to make the idea more clear for readers. Also, we provide incomplete and undecidable result of STSL_{OC} and prove the result.

In this work, there are three contributions:

1. We propose a spatio-temporal specification language STSL_{PC}, based on STL and S4_u, to specify the changes in topometric space and dense time. We present STSL_{PC}, and provide syntax, Boolean semantics and quantitative semantics,
2. We present an axiomatization system and prove the completeness and decidability for the proposed STSL_{PC}.
3. We extend the expressiveness of STSL_{PC}, called STSL_{OC}, to the changes or evolution of spatial objects over time, and prove the incompleteness and undecidability.

The next section introduces temporal logic STL and modal spatial logic S4_u. "Spatio-temporal specification language" section presents the spatio-temporal specification language STSL_{PC}, and completeness of axiomatization system and decidability of STSL_{PC} is proved in "Completeness and decidability of STSL_{PC}" section. In "STSL_{OC}" section, we present STSL_{OC} through extending the expressiveness of STSL_{PC}, and the completeness and complexity are provided. "Case study" section presents a case study about train collision avoidance system. "Related work" section compares the related works. We conclude the work and talk about the future work in "Conclusion and future work" section.

Preliminary

The section provides the background to the proposed spatio-temporal logic, including signal temporal logic (STL) and spatial logic S4_u.

Spatial logic: S4_u

S4 [20] is a proposition modal logic and τ is a spatial term under the interpretation of topological space. In the absence of ambiguity, the terminology a spatial term denotes a spatial object. According to the

observation by [21], S4 is a logic of topological spaces, and the propositional variable is interpreted as an element of a subset of the topological space. From the perspective of the topometric space [9], propositional variables of S4 will be understood as spatial variables [22]. In this paper, we restrict the formula of S4 to topometric space. The syntax of S4 can be defined on the topometric space as follows:

$$\tau ::= p \mid \overline{\tau} \mid \tau_1 \sqcap \tau_2 \mid \mathbb{I}_\tau$$

where p is a spatial variable on topometric space and $\overline{\tau}$ is the complementary of τ, $\tau_1 \sqcap \tau_2$ the *intersection* operation of τ_1 and τ_2. $\mathbb{I}$ is an *interior* operator under the topometric space interpretation. The *union* and *closure* operator can be defined by:

$$\tau_1 \sqcup \tau_2 = \overline{(\overline{\tau_1} \sqcap \overline{\tau_2})}, \quad \mathbb{C}_\tau = \overline{\mathbb{I}_{\overline{\tau}}}$$

$\mathbb{C}_\tau$ refers to the *closure* of a spatial object τ. The 1-dimensional interpretation is shown in Fig. 1.

Let $\mathfrak{L} = (M, d)$ is a metric space, where M is a nonempty set denoting the universe of the space, and d is the metric operator on the elements of M, i.e., a function $d : M \times M \to \mathbb{R}$ such that for any spatial objects $x, y, z \in M$, the equations follow $d(x,y) = 0 \Rightarrow x = y, d(x,y) = d(y,x)$ and $d(x,z) \leq |d(x,y) \pm d(y,z)|$. A metric model is a pair of the form $\mathfrak{M} = (\mathfrak{L}, \mathfrak{V}(d))$, where $\mathfrak{V}(d) \subseteq M$, denotes a set of valuations on the metric of spatial variables. A topometric space is a tuple $(M, \mathbb{I}_d)$, where $\mathbb{I}_d$ is an *interior* operator on M induced by the metric space (M, d), and $\forall X \subseteq M, \mathbb{I}_d(X) = \{x \in X \mid \exists a > 0 \, \forall y \ (d(x,y) < a \to y \in X)\}$. The topometric model is defined as $\mathfrak{M} = (M, d, \mathbb{I}_d, P_1^{\mathfrak{M}}, P_2^{\mathfrak{M}} ...)$, where $\mathfrak{M} = (M, d, P_1^{\mathfrak{M}}, P_2^{\mathfrak{M}} ...)$ is a metric model and $\mathbb{I}_d$ is the *interior* operator induced by (M, d). Therefore, we get the valuation of other spatial formulas as follows:

$$\mathfrak{V}(\overline{\tau}) = \mathrm{U} - \mathfrak{V}(\tau), \mathfrak{V}(\tau_1 \sqcup \tau_2) = \mathfrak{V}(\tau_1) \cup \mathfrak{V}(\tau_2),$$
$$\mathfrak{V}(\mathbb{I}\tau) = \mathbb{I}\mathfrak{V}(\tau), \mathfrak{V}(\tau_1 \sqcap \tau_2) = \mathfrak{V}(\tau_1) \cap \mathfrak{V}(\tau_2),$$
$$\mathfrak{V}(\mathbb{C}\tau) = \mathbb{C}\mathfrak{V}(\tau).$$

The interpretation of region-based spatial entities and their relations between them in 2-dimensional space can be seen in Fig. 1. In the figure, a spatial entity τ is present and the spatial complementary, interior, closure operators is defined on τ, where the spatial term U means the universal set. Meanwhile, the spatial union and intersection on spatial terms τ_1 and τ_2 are present.

A spatial logic is a formal language interpreted over a class of structures featuring geometrical entities and relations. Among the well-known spatial logics such as RCC-8 [23, 24], BRCC-8 and $S4_u$, the most expressive spatial form is $S4_u$ [25]. $S4_u$ extends S4 with the *universal* and *existential* quantifiers $\boxdot$, $\diamondsuit$based on a spatial term τ. $\diamondsuit\tau$ refers to that there is at least one element in space τ, and $\boxdot\tau$ means that all elements in the space belong to τ. The formula φ is defined in the form of BNF:

$$\varphi ::= \boxdot\tau \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2$$

where, $\neg\varphi$ is the negation of φ and $\varphi_1 \wedge \varphi_2$ the conjunction of φ_1 and φ_2.

Correspondingly, the *disjunction* and *existential* operators and the spatial subset $\sqsubseteq$ can be derived by:

$$\varphi_1 \vee \varphi_2 = \neg(\neg\varphi_1 \wedge \neg\varphi_2), \quad \diamondsuit\tau = \neg\boxdot\overline{\tau}, \quad \boxdot\tau = \top \sqsubseteq \tau$$

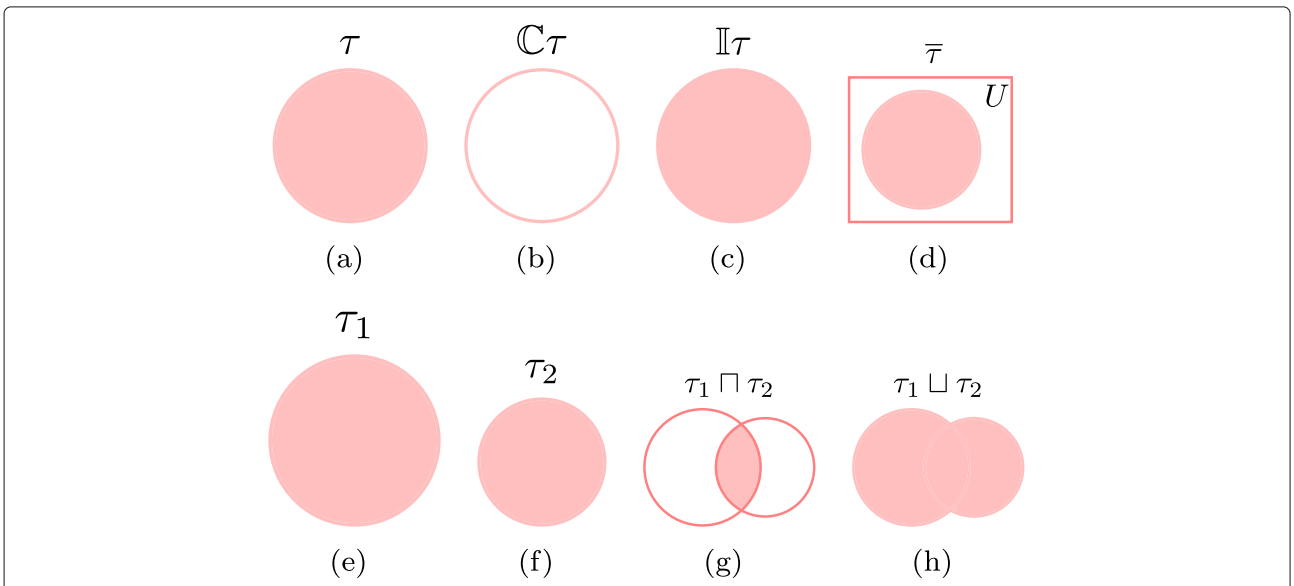

Fig. 1 The 2-dimensional interpretation of spatial terms and relations

The axiomatization system for $S4_u$ includes the classical propositional logic in topology $\mathfrak{L}$, the modal logic $S4$ and extended universal operator $\forall$ and inference rules.

$$
\begin{array}{ll}
\text{CP} & \text{Axioms of classical propositional logic in } \mathfrak{L} \\
\mathbb{I}K & \mathbb{I}(\phi \to \varphi) \to (\mathbb{I}\phi \to \mathbb{I}\varphi) \\
\forall K & \forall(\phi \to \varphi) \to (\forall\phi \to \forall\varphi) \\
\mathbb{I}T & \mathbb{I}\phi \to \phi \\
\forall T & \forall\phi \to \phi \\
\mathbb{I}4 & \mathbb{I}\phi \to \mathbb{I}\mathbb{I}\phi \\
\forall 4 & \forall\phi \to \forall\forall\phi
\end{array}
$$

and the inference rules

$$
\begin{array}{ll}
\text{MP} & \dfrac{\phi \quad \phi \to \varphi}{\varphi} \\
N_{\mathbb{I}} & \dfrac{\phi}{\vdash \mathbb{I}\phi} \\
N_{\forall} & \dfrac{\phi}{\vdash \forall\phi}
\end{array}
$$

The soundness and completeness of $S4_u$ is given in [26]. It is worth noting that the current axiomatization is considerably different from the version in [26]. For one thing, the current logic $S4_u$ can be used to interpret spatial logic, while Shehtman's work only employs it in modal logic. The interpretation in spatial domain makes $S4_u$ enjoy more meanings. For another, we want to use soundness and completeness result of the axiomatization as a basic to consider quantitative axioms temporal axioms.

Signal temporal logic

LTL is proposed by Pnueli [27] to specify sequential and parallel programs. The logic is built on a finite set P of propositional letters. The Boolean connectives and temporal operators are defined based on the propositional letters. When the domain of time is extended from discrete time to dense time, the logic metric interval temporal logic (MITL) [28] emerges. While STL extends the signals of MITL [29] from Boolean value to real value. An STL signal [10, 30] is defined on dense-time domain $\mathbb{T}$, which depends on the sampling times and frequency within an interval. A *signal function* $\varepsilon : \mathbb{T} \to \mathbb{E}$ associates a set of time domain with a set of signals. Signals with $\mathbb{E} = \mathbb{B} = \{0, 1\}$ are called Boolean signals, while these with $\mathbb{E} = \mathbb{R}^+$ are called real-valued or quantitative signals. A Boolean signal, transformed from real-valued one through a set of predicates, can be represented by MITL [31].

An execution trace w is a set of real-valued signals $x_1^w, ..., x_k^w$ bound in some interval I of $\mathbb{R}^+$, which is called the time domain of w [11]. We constrain such an interval $I \subseteq \mathbb{R}^+$ to be half-closed and half-open $[t_1, t_2)$. The syntax of STL is given by

$$\varphi ::= ap \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2$$

where $ap \in AP$ is a atomic predicate and AP a finite set of atomic predicates $\{x_i \bowtie c | \bowtie \in \{<, \leq, \geq, >\}\}$ whose truth value is determined by the sign of an evaluation based on the signal x_i. Let $y_i = x_i - c$, an atomic predicate with the format $x_i \geq c$ can be translated as $y_i \geq 0$. The Boolean operators $\neg$ and $\wedge$ are negation and conjunction, respectively. The temporal *bounded until* operator $\mathcal{U}_I$ is defined on the time interval I. The bounded temporal operators $\Box_I$ and $\Diamond_I$, and binary disjunction $\vee$ can be derived as follows:

$$
\begin{aligned}
\varphi_1 \vee \varphi_2 &= \neg(\neg\varphi_1 \wedge \neg\varphi_2), \\
\Diamond_I\varphi = \top\mathcal{U}_I\varphi, \quad \Box_I\varphi &= \neg\Diamond_I\neg\varphi.
\end{aligned}
$$

Formula $\Diamond_I\varphi$ indicates that φ is eventually satisfiable within the time interval I, while $\Box_I\varphi$ denotes that φ is always satisfiable.

The fundamental composition of the axiomatization system for LTL contains all the tautologies like atomic proposition, Boolean operators in first-order logic. Temporal expressiveness and inference rules are shown as follows:

$$
\begin{array}{ll}
\text{A0} & \text{All classical tautologies of first-order logic} \\
\text{A1} & \Box(\phi \to \varphi) \to (\Box\phi \to \Box\varphi) \\
\text{A2} & \neg \bigcirc \phi \leftrightarrow \bigcirc\neg\phi \\
\text{A3} & \bigcirc(\phi \to \varphi) \to (\bigcirc\phi \to \bigcirc\varphi) \\
\text{A4} & \Box(\phi \to \bigcirc\varphi) \to (\phi \to \Box\varphi) \\
\text{A5} & (\phi U \varphi) \leftrightarrow \varphi \vee \bigcirc(\phi U \varphi) \\
\text{A6} & (\phi U \varphi) \to \Diamond\varphi
\end{array}
$$

and the inference rules:

$$
\begin{array}{ll}
\text{MP} & \dfrac{\phi \quad \phi \to \varphi}{\varphi} \\
N_{\Box} & \dfrac{\phi}{\vdash \Box\phi} \\
N_{\bigcirc} & \dfrac{\phi}{\vdash \bigcirc\phi}
\end{array}
$$

Gabbay et al. [32] present the completeness of the deductive systems of LTL. Also, Lichtenstein and Pnueli [33] prove the complete system of LTL from three parts: the general part, domain part and program part. The temporal operator *next* expresses dynamic behaviors in discrete time, so it is unsuitable to express dense time. So the axioms A2-A6 and the inference rule $N_{\bigcirc}$ will be ignored for the axiomatization of STL.

Spatio-temporal specification language

STL provides an approach that combines the truth value and quantitative value of general signals. But it is inadequate to represent the changes of a spatial entity and the binary relation between spatial entities and temporal aspects. We propose the spatio-temporal specification language that combines STL and $S4_u$ to describe the evolution in spatial and temporal domain.

Spatio-temporal signals

A spatio-temporal signal is defined with continuous time and topometric space [29, 34]. A real-valued interval $[0, t)$ is defined in the dense time domain $\mathbb{T}$, where $t \in \mathbb{R}_{\geq 0}$. Because the time domain inherits STL, it will keep consistency with the interval in STL. The *signal function* is extended to spatial-temporal domain with $\varepsilon : \mathbb{T} \times \mathbb{L} \to \mathbb{E}$, where $\mathbb{L}$ denotes the topometric space. Firstly, an elementary signal evaluates a spatial entity or the connections between spatial entities. That is, the elementary signal is quantitative signals Secondly, a Boolean signal can be transformed from a quantitative signal by the threshold predicate $x_i \geq 0$. The signals stem from topometric space, therefore, the Boolean and quantitative signals are extended from the domain of STL signals to topometric space.

An atomic spatial entity enjoys two meanings: point-based interpretation, point set-based interpretation and region-based interpretation. The points interpret discrete location coordinates. It is consistent with your comment. But, the point set-based interpretation and region-based interpretation denote the discrete and continuous space respectively. When involving in changes of spatial entities, we are talking about motion. The motion of spatial entities can be discrete or dense time. We define a spatio-temporal trace w as the changes of spatial objects over time. Formally, a spatio-temporal trace assigns $\mathbb{T} \times \mathbb{L}$ to a multi-dimensional signal $\mathbb{R}^n$, where n refers to the number of variables.

A spatio-temporal trace provides a notation about execution sequence of temporal and spatial domain.

Definition 3.1 (Spatio-temporal signal)**.** *A spatio-temporal signal ε is an evaluation of spatial entities in a trace w. A Boolean signal $\mu_i^{w(t)} (i \in \mathbb{N})$ is an evaluation of an atomic proposition transferred from quantitative signals $\boldsymbol{x}_i^{w(t)}$ by atomic predicate $\mu_i^{w(t)} = \left(\boldsymbol{x}_i^{w(t)} \geq 0\right)$ in the trace.*

$$\varepsilon_i^{w(t)} := \begin{cases} \mu_i^{w(t)} & if \quad \varepsilon_i^{w(t)} \in \mathbb{B} \\ \boldsymbol{x}_i^{w(t)} & if \quad \varepsilon_i^{w(t)} \in \mathbb{R}_{\geq 0} \end{cases}$$

where $\mathbb{B}$ refers to the domain of Boolean signals and $\mathbb{R}_{\geq 0}$ quantitative signals.

For a spatio-temporal trace w, there are two different interpretations:

- A trace represents a sequence of spatial objects and time point and each point in the trace evaluates a pair of spatial objects and time.
- Another interpretation means that a spatio-temporal trace takes spatial objects as the basic entities and spatio-temporal primitive relations could be obtained by the changes of ontology of space over time.

In this work, we treat the spatio-temporal trace as the second interpretation. The changes of spatial objects are influenced by the flow of time.

The interpretation of the combined logic

It is essential that a combined spatio-temporal form should be provided with enough expressiveness to contain the three parameters [22]:

1 the expressiveness of the spatial component;
2 the expressiveness of the temporal component;
3 the interaction between the two components allowed in the combined logic.

Based on the principle of *PC* [22], which expresses that the language should be able to express changes over time of the truth-values of purely spatial propositions. We interpret an STSL$_{PC}$ formula based on the topometric temporal model, which is defined on topometric space and temporal interval structure in strict partial ordering with a set of sampling time point. The model can be treated as a set of sampling trace monitoring from state-based cyber-physical systems, rather than differential equations [18]. Firstly, the scene snapshot of a system is abstracted to be a topometric model. As the system executes, the system is sampled as a sequence of traces at dense time. At each time instant, the spatial structure denotes a topometric model. And the topometric temporal model in dense time and topometric space can be a sequence of sampling traces. Formally, a topometric temporal model is defined as a triple $\mathfrak{M} = (\mathfrak{T}, \mathfrak{L}, \mathfrak{V})$, where

- $\mathfrak{T}$ is an interval structure $(\mathcal{T}, \mathcal{I}(\mathcal{T}))$, where $\mathcal{T} = (\mathbb{T}, <)$ is strict partial ordering with a set of time point $\mathbb{T}$ and $<$ an irreflexive, transitive and asymmetric relation on $\mathbb{T}$ with a linear strict time flow, and $\mathcal{I}(\mathcal{T})$ is a set of intervals,
- $\mathfrak{L}$ is a topometric space with the definition of $(M, \mathbb{I}_d)$ in which M is a nonempty set, the universe of the space, and $\mathbb{I}_d$ is the interior operator on M induced by the metric space (M, d), which satisfies the standard Kuratowski axioms [35]: $\forall X, Y \subseteq M, \mathbb{I}(X \cap Y) = \mathbb{I}X \cap \mathbb{I}Y, \mathbb{I}X \subseteq \mathbb{I}\mathbb{I}X$ and $\mathbb{I}(M) = M$,
- $\mathfrak{V}$ is a valuation on the time domain $\mathfrak{T}$ and the spatial term set $\mathbb{L}$, i.e., $\forall \tau \in \mathbb{L}$, and $t \in \mathbb{T}$. Formally, $\mathfrak{V}(\tau, t) = \{\mu_i \mid \forall i \in \mathbb{N}, x_i \geq 0\}$ means the space occupied by a spatial term τ at time point t. As for the spatial term τ, the valuation can be defined as: $\mathfrak{V}(\overline{\tau}, t) = \neg\mathfrak{V}(\tau, t), \mathfrak{V}(\tau_1 \sqcap \tau_2, t) = \mathfrak{V}(\tau_1, t) \cap \mathfrak{V}(\tau_2, t), \mathfrak{V}(\mathbb{I}\tau, t) = \mathbb{I}\mathfrak{V}(\tau, t)$.

The ontology of space includes the static spatial entities and dynamic spatial entities. We describe the ontology of

static spatial entities with $S4_u$ atomic spatial terms and spatial operators like complementary, intersection and union, interior and closure. And the spatial until operator is employed to represent the dynamic spatial ontology. However, the changes of ontology of space means that the evolution of spatial entities can be changed by external event or the arrival of a time slice. The changes of spatial terms in topometric model over time can be shown in Fig. 2.

A topometric temporal model is an abstraction of a cyber-physical system, while a spatio-temporal trace is an execution of topometric temporal model. Generally, classical model checking provides an approach to verify whether a topometric temporal model, i.e., all the traces, satisfies spatio-temporal properties. However, the state space explosion makes it difficult for model checking to verify the reliability and security of real cyber-physical systems. Monitoring verifies whether the spatio-temporal signals on one execution of the system hold the specified spatio-temporal properties. Especially, online monitoring can provide the verification results to help analyze the potential hazards, which can avoid unnecessary loss.

Example 3.1. *One point represents a spatial entity and an edge between two points means the connection between spatial entities. The weight on the edge denotes the metric between spatial entities. At any time instant, the points, edges and weight on the edges consist a undirected weighted graph, which denotes the topological metric models. As time goes, the topometric model leads to the topometric temporal model. In this figure, a spatial term τ is characterized as a 2-dimensional space and the spatial terms change over time in the model $\mathfrak{M}$.*

Example 3.2. *The changes of spatial terms in topometric model over time can be shown in Fig. 3. In this figure, a spatial term p is characterized as a 2-dimensional space and the spatial terms change over time in the model $\mathfrak{M}$. The model describes the changes of spatial relations. The y axis describe the spatial relations. In the x axis, the time instant samples the spatial relations between the spatial entities red, blue and green. The black time instants describe the tangential proper part (TPP) relations between three region-based spatial entities green and red. While the red time instants express the partial overlap (PO) relations between green and red. The spatial relations are expressed by $S4_u$ terms and the spatial relations are sampled with dense time and represented in STL.*

Firstly, a cyber-physical system involves in discrete and continuous time. The cyber system describes the execution of an actual system, and the signal is sampled in discrete time. The physical system generally expresses the continuous changes of a spatial entity. A topometric temporal model is an abstract of a cyber-physical system.

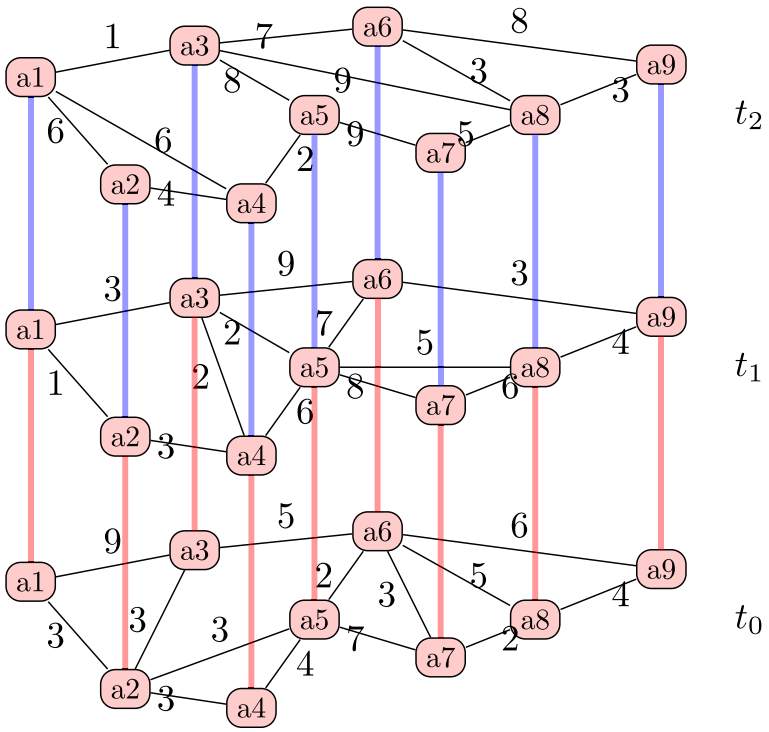

Fig. 2 The changes of point-based spatial terms over time in topometric model

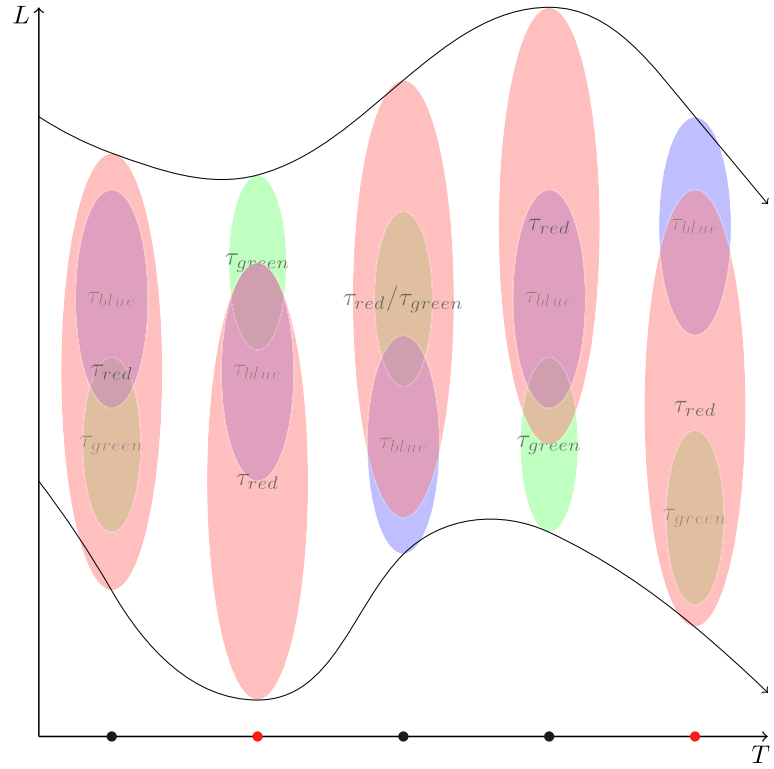

Fig. 3 The changes of region-based spatial terms over time in topometric model

A spatio-temporal trace is sampled from the topometric temporal model. And the trace is an execution of a cyber-physical system. Further, when the trace describes spatial relations among spatial entities and is sampled in dense time, it will be able to be monitored by STSL formulas.

The concurrency can be interpreted in topometric model. Mainly, we interpret the region through borrowing the notation from Milner's Bigraph [36], which presents the agent and the communication between different agents. We treat a spatial entity as an agent. Meanwhile, we define the concurrence of topometric model as the concurrency between spatial entities. We present the topometric model in region-based and point-based interpretation. So, we will illustrate the model from two perspectives.

Firstly, the point-based topometric model can consider a list of regions. For instance, $S4_u$ terms can specify the properties that *the region made by spatial entities* a_6, a_7 *and* a_8 *exists in the region occupied by the union of the spatial entities* a_5, a_6, a_7, a_8 *and* a_9 as:

$$(a_6 \sqcup a_7 \sqcup a_8) \sqsubseteq (a_5 \sqcup a_6 \sqcup a_7 \sqcup a_8 \sqcup a_9) \tag{1}$$

Another properties can be that *the spatial entity* a_5 *belongs to the intersection of the region that made up of spatial entities* a_1, a_2, a_3, a_5 *and* a_6, *and the region that made up of spatial entities* a_5, a_6, a_7, a_8 *and* a_9. The property can be specified with $S4_u$ as:

$$a_5 \sqsubseteq (a_1 \sqcup a_2 \sqcup a_3 \sqcup a_5 \sqcup a_6) \sqcap (a_5 \sqcup a_6 \sqcup a_7 \sqcup a_8 \sqcup a_9) \tag{2}$$

From the perspective of agent, the spatial entities are hierarchical, which lead a tree-like structure. The tree-like structure is a place graph in Bigraph. Here, we didn't define the interfaces or names between spatial entities for communication. Instead, we define the metric between the spatial entities. If we ignore the interfaces or names, the graph in Fig. 4 can be treated as a link graph. The place graph and link graph from topometric model compose the Bigraph. So, the topometric model is able to express concurrency.

Secondly, region-based topometric model is relatively concise with spatial complementary, intersection, union, interior, closure and until operators. So it is easier to be interpreted. Figure 5 shows the spatial relations between the spatial entities *green*, *red* and *blue*.

Based on the notation of Bigraph with sharing [37], the overlapping part between two spatial entities can be treated as the sharing part. The hierarchical relations between region-based topometric model are more clear. For instance, we can say that the spatial entity *blue* and

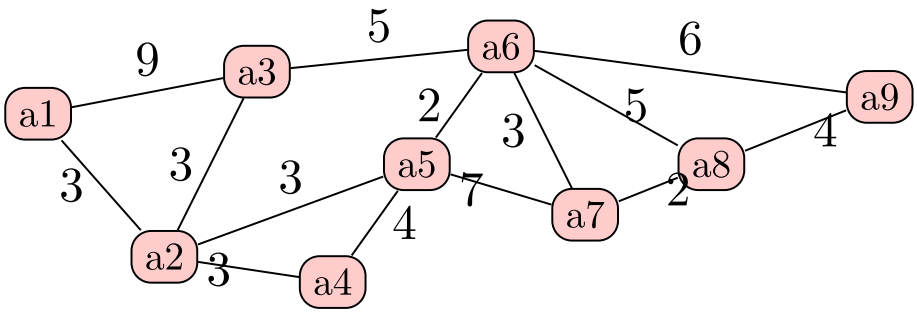

Fig. 4 The point-based spatial terms in topometric model

green are concurrent, and their parent spatial entity is concurrent with the *red* entity.

The spatio-temporal signals are divided into Boolean and quantitative signals. According to the category of spatio-temporal signals, we will present syntax and semantics for the proposed spatio-temporal specification language from two sides:

- The Boolean semantics returns true or false depending on whether the trace of topometric temporal model satisfies the properties or not.
- The quantitative semantics returns a real value in different time that can be interpreted as an evaluation of satisfaction.

The Boolean semantics of the spatio-temporal specification language interprets that an STSL$_{PC}$ formula over spatio-temporal traces returns true or false, so it is able to express purely spatial *propositions' changes* with the truth-values. Meanwhile, the $\mathcal{U}_I$ and $\Box_I$ operators of the quantitative semantics of STSL$_{PC}$ are able to express satisfaction degree of spatial entities over some fixed finite periods and the whole duration of time, respectively.

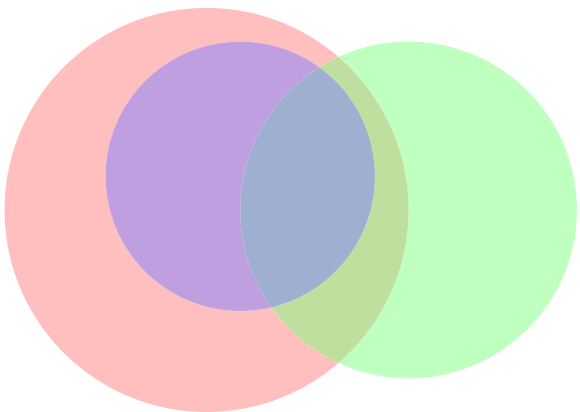

Fig. 5 The region-based spatial terms in topometric model

The syntax of STSL$_{PC}$

As usual, we define the real-value interval in temporal domain. Formally, we confine the temporal interval I to be left-closed right-open $[t, t')$, $\forall t, t' \in \mathbb{T}$ and $t < t'$. The STSL$_{PC}$ fuses the temporal logic STL and modal spatial logic S4$_u$ so that the language can express the changes of purely spatial propositions over time. Specifically, the language is defined on spatial terms τ and spatial operators *complementary*, *intersection*, *union*, *interior* and *closure*, atomic predicates, Boolean connectives and temporal operators *globally*, *finally* and *until* over the temporal interval *I*. There are two kinds of atomic predicates: the binary *subset* operator of two spatial terms $\tau_1 \sqsubseteq \tau_2$ and the threshold predicates on a signal $x_i \geq 0$. The spatial subset relation describes the relations between region-based spatial entities. Specifically, the binary *subset* can be derived by the unary spatial operator *universal* with the form $\boxtimes\tau = \top \sqsubseteq \tau$, where $\top$ denotes the spatial universal set. The quantitative signals evaluate the spatial entities. The Boolean signals can be achieved from the quantitative signals by the threshold predicates. The atomic predicate $\tau_1 \sqsubseteq \tau_2$ means that the elements in the spatial term τ_1 must belong to τ_2. And $x_i \geq 0$ is a threshold predicate, which transfers general real-valued signals to Boolean value. The syntax of STSL$_{PC}$ is given by:

$$\tau ::= p \mid \overline{\tau} \mid \tau_1 \sqcap \tau_2 \mid \mathbb{I}\tau$$
$$\varphi ::= \tau_1 \sqsubseteq \tau_2 \mid x_i \geq 0 \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1 \mathcal{U}_I \varphi_2$$

- τ is a spatial term,
- p is an atomic spatial variable,
- $\overline{\tau}$ is the complementary of τ,
- $\tau_1 \sqcap \tau_2$ is the intersection of τ_1 and τ_2,
- $\mathbb{I}$ is the *interior* operator under the topometric space interpretation. Moreover, the dual operator of $\mathbb{I}$ is the *closure* operator $\mathbb{C}$, which means possible or consistent,
- $\tau_1 \sqsubseteq \tau_2$ implies the spatial subset relations, which means that for all points $p, p \in \tau_1$ implies $p \in \tau_2$,
- $x_i \geq 0$ is an atomic predicate,
- $\neg$, $\vee$ and $\wedge$ are the Boolean operators,
- $\mathcal{U}_I$ is the *until* operator.

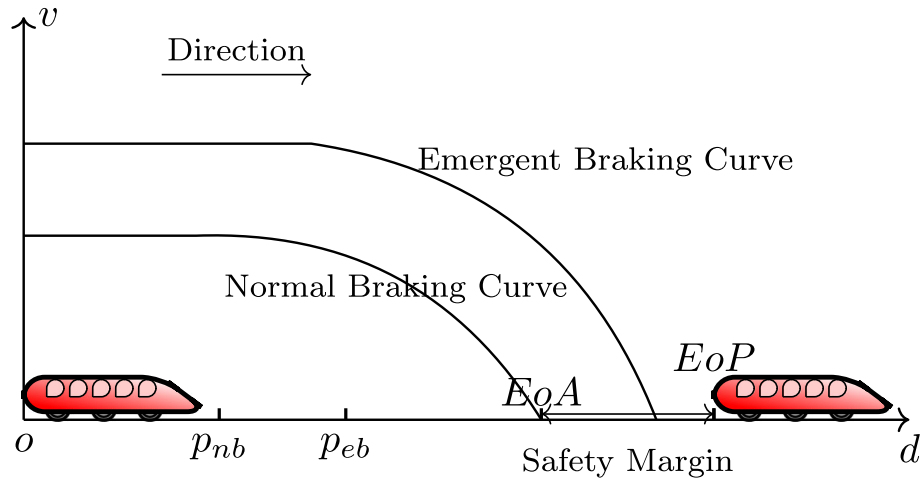

Fig. 6 The safety braking model of automatic train protection

We can define equivalence of operators as syntactic abbreviations:

$$\begin{aligned}
\mathbb{C}\tau &= \overline{\mathbb{I}\overline{\tau}} \\
\tau_1 \sqcup \tau_2 &= \overline{\overline{\tau_1} \sqcap \overline{\tau_2}} \\
\mathbb{I}(\tau_1 \sqcup \tau_2) &= (\mathbb{I}\tau_1 \sqcup \mathbb{I}\tau_2) \\
\mathbb{C}(\tau_1 \sqcup \tau_2) &= (\mathbb{C}\tau_1 \sqcup \mathbb{C}\tau_2) \\
\varphi_1 \vee \varphi_2 &= \neg(\neg\varphi_1 \wedge \neg\varphi_2) \\
\Diamond_I \varphi &= \top \mathcal{U}_I \varphi \\
\Box_I \varphi &= \neg\Diamond_I \neg\varphi.
\end{aligned}$$

Atomic predicates, Boolean operators, and the temporal *bounded until* operator $\mathcal{U}_I$ are from STL. The new spatial operators are the *interior* operator $\mathbb{I}$ and the *closure* operator $\mathbb{C}$ with reference to $S4_u$. The $\Diamond_I$ and $\Box_I$ operators are derived unary operators. $\Box_I\varphi$ denotes that φ holds within the whole interval I, and $\Diamond_I\varphi$ means that φ holds in at least one time point of the interval I.

Example 3.3. *In the mobile blocking mode, the protection point is located behind the forward train to protect the position uncertainty and the back boundary. The protection point is the zero speed limit point, which is a limit that is absolutely not allowed to be crossed by the signal system control. The core of the train's automatic protection is the safe braking model of the train. It describes how to calculate the emergency braking curve and the normal braking curve of the train in Fig. 6. The emergency braking curve considers the emergency braking deceleration of the train protection, the current protection point calculated by the trackside ATP, the most restrictive speed curve and the slope section of the line. The normal braking curve takes into account the ATP response delay time and the cut-off traction after emergency braking. The ATP on-board computer unit dynamically calculates and continuously monitors the normal braking curve. The safe braking model ensures that the train will not exceed the most restricted speed and the train will stop in front of the protection point. Formally, the location of end of mobility authority is marked with EoA, and that of the end of protection is marked with EoP. The distance from the location of the following train to EoA denotes τ_{ma}. The distance from the location of the beginning of following train to EoP means τ_p. Also, the braking distance in normal and emergent braking mode is represented as τ_{nb} and τ_{eb}. A spatio-temporal property can be expressed as After receiving the signals, the train brakes in the normal braking mode and it keeps running in the region of τ_{ma}. While the train keeps running without braking in emergent braking model within 10 seconds. After the train brakes in the emergent braking mode, there exists a moment that the velocity of normal braking is larger than that of the emergent braking mode. And the train keeps running in the emergent braking mode in the region of τ_p within 40 seconds. The property can be specified with $STSL_{PC}$ formula as:*

$$\begin{aligned}
&\Box_{[0,10)}\left((a_{nb} \leq a_{eb}) \wedge (\tau_{nb} \sqsubseteq \tau_{ma})\right) \wedge \\
&\Diamond_{[0,40)}\left(\left(\tau_{eb} \sqsubseteq \tau_p\right) \wedge (v_{nb} \geq v_{eb})\right)
\end{aligned} \tag{3}$$

where a_{nb} and a_{eb} denote the acceleration in normal and emergent braking mode, respectively. v_{nb} and v_{eb} represent the velocity in normal and emergent braking mode, respectively.

Example 3.4. *In the example 3.1, we can employ an $STSL_{PC}$ formula to specify the properties that the region made by spatial entities a_6, a_7 and a_8 exists in the region occupied by the union of the spatial entities a_5, a_6, a_7, a_8 and a_9, until the region made by spatial entities a_3, a_6 and*

a_8 exists in the region occupied by the union of the spatial entities a_3, a_5, a_6, a_7 and a_8 as

$$\begin{aligned} &\boxtimes((a_6 \sqcup a_7 \sqcup a_8) \sqsubseteq (a_5 \sqcup a_6 \sqcup a_7 \sqcup a_8 \sqcup a_9))\mathcal{U}_{[0,5)} \\ &\boxtimes ((a_3 \sqcup a_6 \sqcup a_8) \sqsubseteq (a_3 \sqcup a_5 \sqcup a_6 \sqcup a_7 \sqcup a_8)) \end{aligned} \tag{4}$$

Example 3.5. *In Fig. 3 of example 3.2, we can specify the property that for any execution within 4 seconds, there is an inclusion between two spatial entities τ_{blue} and τ_{grey}, and it will follow an overlapping between them within 1.5 seconds. The property can be specified with STSL$_{PC}$ formula as*

$$\square_{[0,4)}(\tau_{green} \sqsubseteq \tau_{red} \rightarrow \Diamond_{[0,1.5)]}\boxtimes(\tau_{green} \sqcap \tau_{red})) \tag{5}$$

The semantics of STSL$_{PC}$

The semantics of STSL$_{PC}$ is divided into Boolean semantics and quantitative semantics, which return the truth value of purely spatial propositions and real-valued spatial objects. We define μ_i as a predicate because the spatial entities are a discrete set and each signal is evaluated by a threshold predicate μ_i. The quantitative semantics can be transformed to Boolean semantics by a predicate μ_i.

The spatial element of the spatio-temporal specification language exists in spatial entity τ. The value of the spatial entity τ can be achieved by the definition $\mathfrak{V}(\tau, w, t)$. That is, we interpret a spatio-temporal formula in simulated trace rather than topometric temporal model. The satisfaction relation for an STSL$_{PC}$ formula φ over a topometric temporal model $\mathfrak{M}$ is given by:

- $(w,t) \models \tau_1 \sqsubseteq \tau_2 \Leftrightarrow \mathfrak{V}(\tau_1, w, t) \leq \mathfrak{V}(\tau_2, w, t)$
- $(w,t) \models x_i \geq 0 \Leftrightarrow \mathfrak{V}(x_i, w, t) \geq 0$
- $(w,t) \models \neg\varphi \Leftrightarrow (w,t) \not\models \varphi$
- $(w,t) \models \varphi_1 \wedge \varphi_2 \Leftrightarrow (w,t) \models \varphi_1$ and$(w,t) \models \varphi_2$
- $(w,t) \models \varphi_1 \mathcal{U}_I \varphi_2 \Leftrightarrow \exists t' \in t + I$ s.t.$(w,t') \models \varphi_2$ and$\forall t'' \in [t,t'], (w,t'') \models \varphi_1$

A trace w satisfies an STSL$_{PC}$ formula φ at t, denoted by $(w,t) \models \varphi$. For the satisfaction relation, the "$\Rightarrow$" answers whether the implementation procedure of computation holds the specification relation. The "$\Leftarrow$" can be achieved from the definition of *satisfaction relation* of an STSL$_{PC}$ formula φ.

For a given formula φ and execution trace w, we define the *satisfaction* signal $\chi(\varphi, w, t)$ over a trace $w(t, l)$:

$$\forall t \in I,\ \chi(\varphi, w, t) := \begin{cases} \top & \text{if } (w,t) \models \varphi \\ \bot & \textbf{otherwise} \end{cases} \tag{6}$$

where $\top$ and $\bot$ respectively denote Boolean value true and false. Therefore, $\chi(\tau_1 \sqsubseteq \tau_2, w, t)$ returns true if spatial subset relation $\tau_1 \sqsubseteq \tau_2$ holds over the model. For a general signal x_i, $\chi(x_i, w, t)$ returns true if $x_i \geq 0$ in the trace $w(t)$. $\chi(\square_I \varphi, w, t)$ means that for all $t \in I$, φ always returns trues in the interval I over the model. While $\chi(\Diamond_I \varphi, w, t)$ denotes that there exists $t \in I$, φ returns trues in the interval I over the model.

In order to compute the *satisfaction* of a formula φ, we divide the formula φ into each subformula ϕ_i until atomic formula so that formula φ can be computed through the subformula and atomic formulas instead of the entire *satisfaction* signal $\chi(\varphi, w, t)$. The procedure can be treated as a hierarchical structure from the full formula φ down to each atomic formula.

We define ρ to quantify the *satisfaction degree* of the property φ over the trace $w(t)$, and it returns a real value $\rho(\varphi, w, t)$. For an atomic spatial formula $\boxtimes\tau$, the *satisfaction degree* can be evaluated as $\mathcal{V}(\tau, w, t)$. And for a atomic predicate $x_i \geq 0$ can be evaluated as $x_i^{w(t)}$. The quantitative satisfaction relation for a formula φ over a spatio-temporal trace w at the time t by the notation of *satisfaction degree* is given by:

- $\rho(\boxtimes\tau, w, t) = \mathcal{V}(\tau, w, t)$.
- $\rho(x_i \geq 0, w, t) = x_i^{w(t)}$
- $\rho(\neg\varphi, w, t) = -\rho(\varphi, w, t)$
- $\rho(\varphi_1 \wedge \varphi_2, w, t) = \min\{\rho(\varphi_1, w, t), \rho(\varphi_2, w, t)\}$
- $\rho(\varphi_1 \vee \varphi_2, w, t) = \max\{\rho(\varphi_1, w, t), \rho(\varphi_2, w, t)\}$
- $\rho(\square_I \varphi, w, t) = \inf_{t' \in t+I}\{\rho(\varphi, w, t')\}$
- $\rho(\Diamond_I \varphi, w, t) = \sup_{t' \in t+I}\{\rho(\varphi, w, t')\}$
- $\rho(\varphi_1 \mathcal{U}_I \varphi_2, w, t) =$ $\sup_{t' \in t+I}(\min\{\rho(\varphi_2, w, t'), \inf_{t'' \in [t,t']}(\rho(\varphi_1, w, t''))\})$

The negation of a formula is evaluated as the negative of its *satisfaction degree*. The conjunction and disjunction of two formulas are evaluated as the minimum and maximum of the *satisfaction degree* of the two formulas. $\rho(\square_I \varphi, w, t)$ refers to that the infimum of $\rho(\varphi, w, t'), \forall t' \in t + I$ is always true in the interval I over the trace. Similar to $\rho(\square_I \varphi, w, t)$, $\rho(\Diamond_I \varphi, w, t)$ returns the truth value of the supremum of $\rho(\varphi, w, t'), \forall t' \in t+I$. The *satisfaction degree* of until formula $\varphi_1 \mathcal{U}_I \varphi_2$ is evaluated complexly. Firstly, we achieve the *satisfaction degree* of the formula φ_2 in the time t', which belongs to the interval $t + I$. Secondly, the infimum of the formula φ_1 is evaluated in the interval of $[t, t')$. Thirdly, the minimum of the result of first steps is achieved. At last, the *satisfaction degree* of until formula $\varphi_1 \mathcal{U}_I \varphi_2$ is evaluated as supremum of the minimum in the third step. It is worthy noting that the infimum of the *satisfaction degree* of a formula means that the minimum value of the signals within temporal interval I. Similarly, the supremum of the *satisfaction degree* of a formula denotes the maximum value of signals with a temporal interval I.

The connection between Boolean and quantitative signals is built by the way of predicate $x_i \geq 0$ and obtain the satisfaction signal $\chi(x_i \geq 0, w, t)$, which returns a real value of the quantitative signals x_i representing the distance to satisfaction. Specifically, the satisfaction degree of quantitative signal can be derived from the Lemire's

algorithm [38] through MAX-MIN filter of a running sequence.

Example 3.6. *In Fig. 3, we can specify the property that for any execution within 4 seconds, there is an inclusion between two spatial entities τ_{blue} and τ_{grey}, and it will follow an overlapping between them within 1.5 seconds. The property can be specified as*

$$\Box_{[0,4)}\left(\tau_{blue} \sqsubseteq \tau_{grey} \rightarrow \Diamond_{[0,1.5)]}\diamondsuit(\tau_{blue} \sqcap \tau_{grey})\right) \tag{7}$$

Completeness and decidability of STSL$_{PC}$

The language STSL$_{PC}$ describes the spatial changes in dense time, which is used to monitor the execution of continuous systems at run time. So we ignore the temporal *next* operator that describes the next step of the discrete systems.

An axiomatization system of STSL$_{PC}$

We will present a Hilbert-style proof system for STSL$_{PC}$ according to expressiveness of the proposed language. STSL$_{PC}$ combines temporal logic and spatial logic, so the proof system will be introduced from spatial and temporal part. Further, the temporal operators $\Box_I$, $\Diamond_I$ and $\mathcal{U}_I$ are defined in an interval I in dense time, so we will add the quantitative part for the proof systems.

Spatial part

The spatial part of the axiomatization presents the subset relation of spatial terms with *complementary*, *intersection* and *union* operators:

S0 $\mathbb{I}\tau \sqsubseteq \tau$
S1 $\tau \sqsubseteq \mathbb{C}\tau$
S2 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \overline{\tau_2} \sqsubseteq \overline{\tau_1}$
S3 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \mathbb{C}\tau_1 \sqsubseteq \tau_2$
S4 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \tau_1 \sqsubseteq \mathbb{I}\tau_2$
S5 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \mathbb{I}\tau_1 \sqsubseteq \mathbb{I}\tau_2$
S6 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \mathbb{C}\tau_1 \sqsubseteq \mathbb{C}\tau_2$
S7 $\tau_1 \sqsubseteq \mathbb{I}\tau_2 \rightarrow \tau_1 \sqsubseteq \mathbb{C}\tau_2$
S8 $(\tau_1 \sqcup \tau_2) \sqsubseteq \tau_3 \rightarrow (\tau_1 \sqsubseteq \tau_3) \vee (\tau_2 \sqsubseteq \tau_3)$
S9 $\tau_1 \sqsubseteq (\tau_2 \sqcap \tau_3) \rightarrow (\tau_1 \sqsubseteq \tau_2) \wedge (\tau_1 \sqsubseteq \tau_3)$
S10 $\diamondsuit\tau \leftrightarrow \neg\boxdot\overline{\tau}$
S11 $\boxdot(\tau_1 \sqcap \tau_2) \rightarrow \boxdot\tau_1 \wedge \boxdot\tau_2$
S12 $\diamondsuit(\tau_1 \sqcup \tau_2) \rightarrow \diamondsuit\tau_1 \vee \diamondsuit\tau_2$

And the inference rules:

$$N_{\sqsubseteq}\ \frac{\tau_1 \sqsubseteq \tau_2 \quad \tau_2 \sqsubseteq \tau_3}{\vdash \tau_1 \sqsubseteq \tau_3}$$

Temporal part

The temporal part of STSL$_{PC}$ in real time with interval implies that the temporal *next* operator is forbidden.

T0 All classical tautologies of propositional logic
T1 $\Diamond_I\phi \leftrightarrow \neg\Box_I\neg\phi$
T2 $\Box_I(\phi \wedge \varphi) \rightarrow (\Box_I\phi \wedge \Box_I\varphi)$
T3 $\Diamond_I(\phi \vee \varphi) \rightarrow (\Diamond_I\phi \vee \Diamond_I\varphi)$
T4 $\phi U_I\varphi \rightarrow \Diamond_I\varphi$

And the inference rules:

$$\text{MP}\ \frac{\phi \quad \phi \rightarrow \varphi}{\varphi}$$

$$N_{\Box}\ \frac{\phi}{\vdash \Box_I\phi}$$

Axiom (T0) and Modus Ponens (MP) are from the Hilbert-style axiomatization of propositional logic. Axioms (T1-T4) are achieved from by Manna and Pnueli's temporal logic [39]. A complete proof system for quantitative version is proposed in [40].

Quantitative part

The quantitative part of spatio-temporal logic involves the execution of system in dense time , so the quantitative axioms need to be provided. We follow the way of [41] to present the quantitative axioms for STSL$_{PC}$. However, we forbid the appearance of the punctuality in interval as the metric logic MITL and ban the temporal *next* operator because of the continuous time. The quantitative axioms characterize the translation from the intersection, union of intervals into conjunction, disjunction of temporal operators with interval. Specifically, the intersection of two intervals is bounded in finally operator with the form $\Diamond_{I\cup J}\varphi$, and it implies the disjunction of finally operator bounded with their respective interval. Conversely, the disjunction of finally operator bounded with their respective interval implies the finally operator bounded with the union of the two intervals. However, the globally operator bounded with the intersection of the two intervals and the conjunction of globally operator bounded with their respective interval imply each other. For until operator, the axiom generalizes $\phi U_I\varphi \rightarrow \Diamond_I\varphi$ with the union of two intervals $I \cup J$.

Q0 $\Diamond_{I\cup J}\varphi \leftrightarrow \Diamond_I\varphi \vee \Diamond_J\varphi$
Q1 $\Box_{I\cap J}\varphi \leftrightarrow \Box_I\varphi \wedge \Box_J\varphi$
Q2 $\phi U_{I\cup J}\varphi \rightarrow \Diamond_{I\cup J}\varphi$

Soundness and completeness of the axiomatization system

Once an axiomatization system is present, the soundness and completeness of the axiomatization system need to be proved, including spatial, temporal and quantitative axioms. Soundness refers to that all the theorems in STSL$_{PC}$ are logically valid. Equivalently, a spatio-temporal logic is *sound* with respect to topometric temporal model if for all the formulas ϕ, $\vdash_{\mathcal{ST}}\phi$ implies $\Vdash \phi$. Let $\mathcal{ST}$ be a class of topometric temporal model. A spatio-temporal logic is *strongly complete* in $\mathcal{ST}$ if for any set of formulas $\Gamma \cup \{\phi\}$, if $\Gamma \Vdash_{\mathcal{ST}} \phi$ then $\Gamma \vdash_{\mathcal{ST}} \phi$. If the

semantics of Γ satisfies ϕ on $\mathcal{ST}$ then ϕ is deducible from Γ.

Theorem 4.1. *The above axiomatization is sound for topometric temporal model, i.e., for any $\phi \in STSL_{PC}$, if $\vdash_\Gamma \phi$ implies $\Vdash_{\mathcal{ST}} \phi$*

Proof The soundness theorem proof need guarantee each axiom is sound and the inference rules preserve soundness from the sound hypothesis. This follows the fact that all axioms are valid and all rules preserve validity. We provide the proof in Appendix A. □

It is well-known that weak completeness plus compactness implies strong completeness [42]. The lexicographic products of modal logic with linear temporal logic are sound and complete [43]. MTL, which empowers more expressiveness in punctuality operator than MITL, is complete in two-sorted model [44]. But temporal logic in the flow of real time has weak completeness [45], which proposes *finitely complete* and *expressively complete*, but fails compactness theorem. These conclusions contribute to the result of weak completeness.

Theorem 4.2. *The system for $STSL_{PC}$ is weakly complete with respect to topometric temporal model, i.e., for every $STSL_{PC}$ formulas, $\Vdash_{\mathcal{ST}} \phi$ implies $\vdash_\Gamma \phi$.*

Before presenting the complete proof of the axiomatization system of STSL_{PC}, we will introduce the notation of *maximal consistent set* [46].

The axiomatization system of STSL_{PC} is a logical system. A proof in STSL_{PC} is a sequence of finite formula: $A_0, A_1, ..., A_n$, where each of them is an axiom, or there exists $j, k < i$, such that A_i is the conclusion derived from A_j and A_k using *MP* inference rule. The last term A_n is a theorem in STSL_{PC}, using the sign $\vdash A_n$, where n is the length of proof.

The concepts of *deducibility* and *consistency* from [12, 47] are fundamental to deduce the logic system STSL_{PC}. A formula A is *deducible* from a set of formulas Γ in a system $\mathcal{ST}$, written $\Gamma \Vdash_{\mathcal{ST}} A$, if and only if $\mathcal{ST}$ contains a theorem of the form $(A_1 \wedge ... \wedge A_n) \rightarrow A$, where the conjunctions $A_i (i = 1, ..., n)$ of the antecedent are formulas in Γ. A set of formulas Γ is consistent in $\mathcal{ST}$, written $Con_{\mathcal{ST}}\Gamma$, just in case the formula $\perp$ is not $\mathcal{ST}$-deducible from Γ.

Definition 4.1 ($\mathcal{ST}$-MCS)**.** *A set of formulas Γ is maximal $\mathcal{ST}$-consistent iff*

(i) *Γ is $\mathcal{ST}$-consistent, and*
(ii) *for every formula A, if $\Gamma \cup \{A\}$ is $\mathcal{ST}$-consistent, then $A \in \Gamma$.*

If Γ is a maximal $\mathcal{ST}$-consistent set of formulas then we say it is an $\mathcal{ST}$-MCS. The *(ii)* condition refers to that any set of formulas properly containing Γ is $\mathcal{ST}$-inconsistent.

The canonical model is defined in [47] to induce the soundness and completeness of modal logics. We extend the notation of *canonical model* to spatio-temporal systems for completeness of STSL_{PC}.

Definition 4.2 ($\mathcal{ST}$-canonical Model)**.** *The $\mathcal{ST}$-canonical model $\mathfrak{M}^\Gamma$ for a spatio-temporal logic is a triple $\left(W^\Gamma, R^\Gamma, V^\Gamma\right)$ where:*

(i) *W^Γ is the set of all Γ-MCSs;*
(ii) *R^Γ is the metric relation on topometric space over a quasi-order on time. It is the canonical binary relation on W^Γ defined by $sR_i^\Gamma s'$ over state s and s' if for all formulas ϕ, $\phi \in s$ implies $\phi \in s'$.*
(iii) *V^Γ is the valuation defined by $V^\Gamma(p) = \left\{s \in W^\Gamma \mid p \in s\right\}$. V^Γ is called the canonical valuation.*

Lemma 4.3 (Truth Lemma)**.** *Let $\mathcal{ST}$-canonical model be a class of topometric temporal model. For all $\phi \in \mathcal{ST}$-MCS, $\mathcal{ST} \Vdash \phi$ iff $\phi \in \mathcal{ST}$-MCS.*

Proof The proof is by induction on the structure of ϕ.

Base case: Suppose ϕ is a spatial formula $\boxbslash\tau$ or an atomic predicate $x_i \geq 0$.

$(\mathcal{ST}, s) \Vdash \boxbslash\tau \Leftrightarrow V^\Gamma(\boxbslash\tau, s) = \top \Leftrightarrow \boxbslash\tau \in s$,

$(\mathcal{ST}, s) \Vdash x_i \geq 0 \Leftrightarrow V^\Gamma(x_i \geq 0, s) = x_i \Leftrightarrow x_i \geq 0 \in s$.

Inductive step: Suppose ϕ is an atomic predicate $\neg\phi$, $\phi_1 \wedge \phi_2$, $\phi_1 \vee \phi_2$, $\Box_I\phi$, $\Diamond_I\phi$, $\phi\mathcal{U}_I\varphi$. We show the proof of the case $\Box_I\phi$, and leave the others to reader. We have $(\mathcal{ST}, s) \Vdash \Box_I\phi \Leftrightarrow \Box_I\phi \in s$ (assuming the inductive hypothesis).

$(\mathcal{ST}, s) \Vdash \Box_I\phi$
$\Leftrightarrow \forall s', sR^\Gamma s' \Rightarrow \mathcal{ST}, s' \Vdash \phi$
$\Leftrightarrow \forall, sR^\Gamma s' \Rightarrow \phi \in s'$

we need to show that $\Box_I\phi \in s \Leftrightarrow \forall s', sR^\Gamma s' \Rightarrow \phi \in s'$.

$\Rightarrow$ follows immediately from the Definition 4.2.

As for $\Leftarrow$: suppose $\Box_I\phi \notin s$. We need to show
$\exists s', sR^\Gamma s'$ and $\phi \notin s'$
$\Leftrightarrow \exists s', sR^\Gamma s'$ and $\neg\phi \in s'$
$\Leftrightarrow \exists s', \{\varphi \mid \Box_I\varphi \in s\} \subseteq s'$ and $\neg\phi \in s'$
$\Leftrightarrow \exists s', \{\varphi \mid \Box_I\varphi \in s\} \cup \{\neg\phi\} \subseteq s'$

It is easy to show that $\{\varphi \mid \Box_I\varphi \in s\} \cup \{\neg\phi\}$ is $\mathcal{ST}$-consistent. Suppose not, i.e., $\{\varphi \mid \Box_I\varphi \in s\} \cup \{\neg\phi\}$ is $\mathcal{ST}$-inconsistent. Then $\vdash_{\mathcal{ST}} (\varphi_1 \wedge ... \wedge \varphi_n) \rightarrow \phi$ for some $\{\Box_I\varphi_1, ...\Box_I\varphi_n\} \subseteq s$. But $\mathcal{ST}$ is canonical and s is $\mathcal{ST}$-MCS, so s must contain $(\Box_I\varphi_1 \wedge ... \wedge \varphi_n) \rightarrow \Box_I\phi$. From $\Box_I\varphi_i \in s$, it follows $\Box_I\phi \in s$. This contradicts the hypothesis that $\Box_I\phi \notin s$ □

The proof of the weakly complete system of STSL_{PC} is immediately the result of Lemma 4.3.

Decidability of of STSL$_{PC}$

We present the decidability of STSL$_{PC}$ based on the *finite model property* [12]. A decision procedure for the decidable fragment will be present.

Definition 4.3 (Filtration). *Let $\mathfrak{M}$ be the topometric temporal model and φ subformula closed set of formulas. $\approx$ is an equivalence relation on the states of $\mathfrak{M}$ defined by:*

$(t,l) \approx (t',l')$ iff for all ϕ in φ: $(\mathfrak{M},t,l) \Vdash \phi$ iff $(\mathfrak{M},t',l') \Vdash \phi$.

We denote the equivalence class of a state with respect to $\approx$ by $|(t,l)|$. Let $(\mathbb{T},\mathbb{U}) = \{|(t,l)| \mid (t,l) \in (\mathbb{T},\mathbb{U})\}$. Suppose $\mathfrak{M}^f$ is any model $(\mathfrak{T}^f,\mathfrak{L}^f,\mathfrak{V}^f)$ such that:

i) $(\mathfrak{T}^f,\mathfrak{L}^f) = (\mathfrak{T},\mathfrak{L})$.
ii) *if $(t,l) \approx (t^f,l^f)$ then $|(t,l)| \approx |(t^f,l^f)|$.*
iii) *if $|(t,l)| \approx |(t^f,l^f)|$ then for all $\Diamond\phi \in \varphi$, if $(\mathfrak{M},t,l) \Vdash \phi$ then $(\mathfrak{M},t',l') \Vdash \Diamond\phi$.*
iv) $\mathfrak{V}^f(p) = \{|(t,l)| \mid (\mathfrak{M},t,l) \Vdash p\}$ *for all proposition letters p in φ.*

Then $\mathfrak{M}^f$ is a filtration of $\mathfrak{M}$ through φ.

Proposition 4.1. *Let φ subformula closed set of STSL$_{PC}$ formulas. For any model $\mathfrak{M}$ if $\mathfrak{M}^f$ is a filtration of $\mathfrak{M}$ through a subformula closed set φ, then $\mathfrak{M}^f$ contains at most 2^n nodes (where n denotes the size of φ).*

Theorem 4.4 (Filtration Theorem). *Let $\mathfrak{M}^f = (\mathfrak{T}^f,\mathfrak{L}^f,\mathfrak{V}^f)$ be a filtration of $\mathfrak{M}$ through a subformula closed set φ. Then for all formulas $\phi \in \varphi$, and all nodes (t,l) in $\mathfrak{M}$, we have $(\mathfrak{M},t,l) \Vdash \phi$ iff $(\mathfrak{M}^f,|(t,l)|) \Vdash \phi$*

Theorem 4.5 (Finite Model Property). *If ϕ is satisfiable, then it is satisfiable on a finite model. Indeed, it is satisfiable on a finite model containing at most z^n, where n is the number of subformulas of ϕ.*

Proof If ϕ is satisfiable in the filtration is immediate from Theorem 4.4, and the bound od size of the filtration is immediate from Proposition 4.1. It is well-known in standard case [12, 16]. □

The satisfiability means for all STSL$_{PC}$ formula ϕ there is a spatio-temporal trace in topometric temporal model $\mathfrak{M}$ such that $(\mathfrak{M},t,l) \Vdash \phi$. Theorem 4.5 shows the searching is finite in the nodes of topometric temporal model. So it follows Theorem 4.6.

Theorem 4.6. *The satisfiability problem for STSL$_{PC}$ against topometric temporal model is decidable.*

Further, we have the complexity of the decidable STSL$_{PC}$.

Theorem 4.7. *The satisfiability problem for STSL$_{PC}$ against topometric temporal models $\mathfrak{M}$ based on $(\mathbb{N},<)$, $(\mathbb{Z},<)$ is EXPSPACE-complete.*

Proof Recall that STSL$_{PC}$ refers to the changes over time of truth-values of purely spatial propositions. The interaction between spatial and temporal components of STSL$_{PC}$ is very restricted to the elementary unit: purely spatial propositions. The proof will be carried through construction step, reduction step and a decision procedure.

Construction step: For every STSL$_{PC}$-formula φ, one can construct an STL-formula ϕ by replacing every occurrence of a spatial proposition $\tau_1 \sqsubseteq \tau_2$ and atomic predicate $x_i \geq 0$ in φ with a fresh propositional variable. Specifically, given an STL-model $\mathfrak{M} = (\mathfrak{T},\mathfrak{V})$ and an STL-formula ϕ with a time point t in $\mathfrak{T}$, we construct the set

$\phi_t = \{\tau_1 \sqsubseteq \tau_2 \mid (\mathfrak{M},t) \models \varphi\} \cup \{x_i \geq 0 \mid (\mathfrak{M},t) \models \varphi\}$.

of spatial formulas as a collection of STL proposition variables. If ϕ_t is satisfiable for every t in $\mathfrak{T}$, then there is a topometric temporal model $\mathfrak{M}$ satisfying φ and based on the flow $\mathfrak{T}$.

Reduction step: Definitely, one can obtain the formulas $\Box_I\varphi$ and $\Diamond_I\varphi$ from $\varphi_1 U_I \varphi_2$, so checking whether an STL formula ϕ is satisfiable or not depends on the complexity of computing a formula with U_I operators. In fact, the time domain of STL is bound in the interval I, and an STL formula in Boolean signal returns true or false for a given STL model $\mathfrak{M}$. The bound STL only with Boolean value has the same expressiveness with MITL [29]. It suffices to reduce the satisfiability problem of STL to the satisfiability problem for MITL [48] over infinite trace with interval to check satisfiability of ϕ_t. Further, STL is interpreted in a temporal trace, while MITL is interpreted in timed automata, which capture all trace. The Boolean semantics of STL returns Boolean value, which is equal to MITL. However, STL can be interpreted in quantitative semantics, which returns real value. It makes STL enjoy more powerful expressiveness. STL and MITL have the same expressiveness in temporal interval because the interval in both of them is dense time.

Decision Procedure: We divide the procedure for deciding the satisfiability of STSL$_{PC}$ into two steps: the first is deciding spatial formula ϕ_t in *PC*, the second is dealing with STL. According to the observation [29], an STL formula in Boolean semantics is as expressive as an MITL formula, so an Satisfiability Modulo Theories (SMT) [49]-based decision procedure for an MITL is suitable to decide an STL formula in Boolean semantics. We present a decision procedure to satisfiability checking of MITL, which is similar to the approach in [50]. The difference is that we restrict our MITL formula without past tense and the counting modality. We propose the encoding of MITL to Constraint LTL over clock (CLTLoc) [51], which is an extension of Constraint LTL [52] with clocks. □

Lemma 4.8 ([50]). *Let M be a signal, and ϕ be an MITL formula. For any $(\pi,\sigma) \in r_{sub(\phi)}(M)$, we have $(\pi,\sigma),0 \models$*

$\bigwedge_{\theta\in sub(\phi)} ck_\theta \wedge \bigwedge_{\theta=F_{(a,b)}(\gamma)} auxck_\theta$ *and for all* $k \in \mathbb{N}, \theta \in sub(\phi)$, *we have* $(\pi,\sigma),k \models m(\theta)$.
Conversely, if $(\pi,\sigma),0 \models \bigwedge_{\theta\in sub(\phi)}(ck_\theta \wedge G(m(\theta))) \wedge \bigwedge_{\theta=F_{(a,b)}(\gamma)} auxck_\theta$, *then there is a signal* M *such that* $(\pi,\sigma) \in r_{sub(\phi)}(M)$.

The proof can be found in [50]. Let θ be the subformula of MITL formula ϕ, then θ is one of the form $\neg\phi, \phi \wedge \varphi, \phi\mathcal{U}_I\varphi, \Diamond_I\phi$. The function $m(\theta)$ is defined to describe the translation of subformula θ of an MITL formula to a corresponding CLTLoc formula, which is the form:

$$init_\theta \bigwedge_{\theta\in sub(\phi)} (ck_\theta \wedge G(m(\theta))) \wedge \bigwedge_{\theta=F_{(a,b)}(\gamma)} auxck_\theta \quad (8)$$

The transformation from MITL to CLTLoc is implemented by qtlsolver [53]. The decision procedure of the CLTLoc formula is described in [54], which relies on the Zot toolkit [53]. In [50], it shows the satisfiability of an CLTLoc formula is PSPACE in the size of the formula and in the binary encoding of the constants, the decision procedure induced the encoding is in EXPSPACE.

STSL$_{OC}$

The interaction between the spatial and temporal components should comply with the principle of *PC* and *OC* [22], which is used to evaluate the interaction:

- STSL$_{PC}$: the language should be able to express changes over time of the truth-values of purely spatial propositions.
- STSL$_{OC}$: the language should be able to express changes or evolution of spatial objects over time.

STSL$_{PC}$ expresses the change of truth-value of proposition and it is the elementary requirement for a combined spatio-temporal logic. For STSL$_{OC}$, spatio-temporal properties are specified about the changes of spatial objects over dense time with interval through extending the temporal *globally, eventually, until* operators to spatial terms of STSL$_{PC}$. The spatio-temporal trace comply the finite variability. The trace are divided into some intervals. The STSL$_{OC}$ formulas with these intervals are also verified at runtime.

The difference between STSL$_{PC}$ and STSL$_{OC}$ exists that STSL$_{PC}$ involves in the change of truth-values of propositions, while STSL$_{OC}$ describes the change of extensions of predicates. Specifically, STSL$_{PC}$ expresses static spatial terms in topometric space over dense time through spatial *complementary*, *intersection* and *union* operators. The dynamic evolution of STSL$_OC$ is achieved by admitting spatial *until* operators with interval $[l_1, l_2)$ to spatial terms in topometric temporal model.

The spatial until $\tau_1\mathcal{U}_{[l_1,l_2)}\tau_2$ at spatial location l_1 consists of those points x of the topometric space for which there is $l_2 > l_1$ such that x belongs to τ_2 at moment l_2 and x is in τ_1 at all l whenever $l_1 < l < l_2$. The difference between spatial until and temporal until exists in that spatial until is interpreted as spatial interval $[l_1, l_2)$, and temporal until is defined in a temporal interval $[t_1, t_2)$. Further, spatial until operates two spatial terms τ_1 and τ_2, while temporal until operates two formulas φ_1 and φ_2. The syntax of STSL$_{OC}$ is given by:

$\tau ::= p \mid \overline{\tau} \mid \tau_1 \sqcap \tau_2 \mid \mathbb{I}\tau \mid \tau_1\mathcal{U}_{[l_1,l_2)}\tau_2$
$\varphi ::= \tau_1 \sqsubseteq \tau_2 \mid x_i \geq 0 \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \varphi_1\mathcal{U}_{[t_1,t_2)}\varphi_2$

Similar to the atomic formulas, the unary operators $\Box_I$ and $\Diamond$ of spatio-temporal term can also be derived from the operator $\mathcal{U}_I$. The occupied spaces of term $\Box_I\tau$ and $\Diamond_I\tau$ at moment w are interpreted as the *intersection* and *union* of all spatial extensions of τ at moments $v > w$, respectively.

Example 5.1. *In the Example 3.3, what we can also guarantee is that After the train brakes in the emergent braking mode, there exists a moment that the velocity of normal braking is larger than that of the emergent braking mode within 40 s. And the train keeps running in the normal braking mode in the region of* τ_{nb} *until it runs in the region of* τ_{eb} *within the spatial interval* $[p_{nb}, EoA)$. *The specification can be expressed as*

$$\Diamond_{[0,40)}\left((v_{eb} \leq v_{nb}) \wedge \boxdot\left(\tau_{nb}\mathcal{U}^l_{[p_{nb},EoA)}\tau_{eb}\right)\right) \quad (9)$$

where v_{eb} *and* v_{nb} *mean the velocity of the emergent and normal braking mode.*

Example 5.2. *The railway traffic with sensors, present by Liu et.al [2], provides a good perspective to discuss the proposed spatio-temporal specification language. In their example, a train and a control zone can be treated as a region-based spatial terms. Obviously, the spatial region of control zone seems bigger than the region of train. Therefore, the spatial relation between control zone and the train can be characterized as* $S4_u$ *formulas or RCC-8 relations, i.e., disconnected (DC), externally connected (EC), partial overlap (PO), equal (EQ), tangential proper part (TPP) and tangential proper part inverse (TPPI), and non-tangential proper part (NTPP) and nontangential proper part inverse (NTPPI). The changes of spatial relations over dense time can be specified by STSL*$_{PC}$. *The specification a train intersects with the control zone until the train leaves within 10 min can be expressed as*

$$PO(\tau_{train}, \tau_{cz})\mathcal{U}_{[0,10)}DC(\tau_{train}, \tau_{cz}) \quad (10)$$

where τ_{cz} *means the region of control zone. The predicate* $PO(\tau_{train}, \tau_{cz})$ *is equal to the STSL*$_{PC}$ *formula* $\diamondsuit(\boldsymbol{I}\tau_{train} \sqcap \boldsymbol{I}\tau_{cz} \wedge \neg\boxdot(\tau_{train} \sqsubseteq \tau_{cz}) \wedge \neg\boxdot(\tau_{cz} \sqsubseteq \tau_{train})$, *and the predicate* $DC(\tau_{train}, \tau_{cz})$ *can be expressed by the STSL*$_{PC}$ *formula* $\neg\diamondsuit(\tau_{train} \sqcap \tau_{cz})$.

However, it is not enough to specify spatio-temporal properties with STSL$_{OC}$ *because there is no evolution of*

spatial entities. Further, it can not even be specified with the spatial relation between point-based spatial terms in topometric space.

Example 5.3. *In example 3.1, the spatio-temporal properties that the spatial entity a_1 reaches a_9 within 20, until the distance from the spatial entity a_1 to a_9 is reduced 18 within 8 min can be specified with STSL$_{OC}$ as*

$$\boxtimes(a_1\mathcal{U}^{l}_{[0,20)}a_9)\mathcal{U}_{[0,8)}\boxtimes(a_1\mathcal{U}^{l}_{[0,18)}a_9) \tag{11}$$

The production of temporal logic and spatial logic expresses the spatial evolution in real time with spatial *until*. The axioms for STSL$_{OC}$ will add the spatial *until*. The added operator has no influence on STSL$_{OC}$. So the STSL$_{OC}$ enjoys the same soundness as STSL$_{PC}$.

Theorem 5.1. *STSL$_{OC}$ isn't complete with respect to topometric temporal model.*

Proof The incomplete STSL$_{OC}$ can be proved by the counter example: $\Box_I(\Diamond_I(\tau_1 \sqcup \tau_2) \sqsubseteq \Diamond_I\tau_1 \sqcup \Diamond_I\tau_2) \rightarrow \Box_I\Diamond_I(\tau_1 \sqcup \tau_2) \sqsubseteq \Box_I(\Diamond_I\tau_1 \sqcup \Diamond_I\tau_2)$. Although the axioms $T2$ can be applied into temporal deduction, the formula $\Box_I$ on the spatial terms returns the quantitative space. □

A spatio-temporal trace w is a sequence over signals ε. The Boolean satisfaction relation and *satisfaction degree* for an STSL$_{OC}$ formula φ over a spatio-temporal trace w are similar to that of STSL$_{PC}$ formula.

The decidability of STSL$_{OC}$ will follow:

Theorem 5.2. *The satisfiability problem for STSL$_{OC}$ formulas based on $(\mathbb{N}, <), (\mathbb{Z}, <)$ is undecidable.*

Before providing the proof of Theorem 5.2, we present the lemma 5.3:

Lemma 5.3. *There exists a natural number $\mathbb{N} \geq 1$ and a sequence $i_1, ..., i_N$ of indices such that $v_{i_1}, ..., v_{i_N} = w_{i_1}, ..., w_{i_N}$, then the satisfiability problem for STSL$_{OC}$ formulas based on $(\mathbb{N}, <), (\mathbb{Z}, <)$ is undecidable.*

Proof As we all know, Post's correspondence problem is undecidable [55]. Given a finite alphabet $A = \{a_1, ..., a_m\}$ and a finite set P of pairs $(v_1, w_1), ..., (v_k, w_k)$ of nonempty finite sequences (words) v_i, w_i over A, decide whether there exists an $N \geq 1$ and a sequence $i_1, ..., i_N$ of indices such that $v_{i_1}, ..., v_{i_N} = w_{i_1}, ..., w_{i_N}$.

An execution trace w is a set of STL signals $\{x^w_1, ..., x^w_k\}$ defined over some interval D of $\mathbb{R}^+$ [11]. Assume the real-valued signals are finite variability. The interval $[t_i, t_{i+1})_{i\in\mathbb{N}}$ and threshold predicates divide the execution trace to be piecewise Boolean signals.

We encode the satisfiability problem of STSL$_{OC}$ formulas to Post's correspondence problem as the way of [22]. The decidability with less expressive language initially is proved in [56]. We construct a formula $\varphi_{A,P}$ which is STSL$_{OC}$-satisfiable iff for each $1 \leq i \leq k$, let l_i and r_i be the length of words v_i and w_i, respectively, and let

$$v_i = \left(b^i_0, ..., b^i_{l_i}\right),$$
$$w_i = \left(c^i_0, ..., c^i_{l_i}\right).$$

The formula $\varphi_{A,P}$ is construct as:

$$\varphi_{A,P} = \varphi_{range} \wedge \varphi_{stripe} \wedge \varphi_{pair} \wedge \varphi_{eq} \wedge \varphi_{left} \wedge \varphi_{right}$$

where

$\varphi_{range} = range \wedge \Diamond_I\neg range \wedge \Box_I(\neg range \rightarrow \Box_I\neg range)$

$\varphi_{pair} = \Box_I(\Diamond_I range \rightarrow \bigvee_{1\leq i\leq k} pair_i \wedge \bigwedge_{1\leq i<j\leq k} \neg(pair_i \wedge pair_j))$

$\varphi_{stripe} = \Box_I\boxtimes(stripe \sqsubseteq \Box stripe) \wedge \Box_I\boxtimes(\overline{stripe} \sqsubseteq \Box\overline{stripe}))$

$\varphi_{eq} = \Diamond_I(range \wedge \bigwedge_{a\in A} \boxtimes(left_a \equiv left_b))$

where $left_a$ and $right_a$ $(a \in A)$, *left*, *right* and *stripe* are spatial variables, for every pair $(v_i, w_i)(1 \leq i \leq k)$, $pair_i$ are propositional variables. The variable *range* is required to 'relativise' temporal operators $\Box_I$ and $\Diamond_I$ in order to ensure that we can construct a model based on a finite flow of time.

ψ_{left} is a conjunction of (12)-(18), for all i in $1 \leq i \leq k$, and for all $j < l_i$,

$$\bigwedge_{a\neq b, a,b\in A} \neg\Diamond\left(left_a \sqcap left_b\right) \wedge \Box_I\boxtimes\left(left \equiv \bigsqcup_{a\in A} left_a\right) \tag{12}$$

$$\bigwedge_{a\in A} \Box_I\left(left_a \rightarrow \boxtimes\left(left_a \sqsubseteq \Box^l_I left_a\right)\right) \tag{13}$$

$$\Box^l_I\overline{left} \wedge \Box_I\boxtimes\left(\overline{left} \sqsubseteq \overline{Sleft}\right)\Big) \tag{14}$$

$$\Box_I\left(pair_i \rightarrow \boxtimes\left(\overline{left} \sqsubseteq \Diamond^l_I S^{l_i}\overline{left}\right)\right) \tag{15}$$

$$\Box_I(pair_i \rightarrow \bigwedge_{j<l_i} \boxtimes(\overline{left} \sqcap \Box^l_I left \sqsubseteq \Box_I\left(S^j left \sqcap \overline{S^{j+1}left} \sqsubseteq left_{b^i_{l_i-j}}\right))) \tag{16}$$

$$pair_i \rightarrow \Box_I\Diamond\tau^{left}_i \tag{17}$$

$$\Box_I\left(pair_i \rightarrow \boxtimes\left(left \sqcap \overline{Sleft}\right) \sqsubseteq \Box^l_I S\tau^{left}_i\right) \tag{18}$$

The conjunct ψ_{right} is defined by replacing in ψ_{left} all occurrences of *left* with *right*, left_a with right_a (for $a \in A$) l_i with r_i and the sequence of $left_{b^i_j}$(for $1 \leq j \leq l_i$) with $right_{c^i_j}$(for $1 \leq j \leq r_i$). (Note that pair_i occurs in both ψ_{left} and ψ_{right}.)

Because of the difference between spatio-temporal logics and the corresponding model from [57], we change the Aleksandrov tt-model $\mathfrak{M} = ((\mathbb{N}, <), \mathfrak{G}, \mathfrak{V})$ with $\mathfrak{G} = (V, R)$ to topometric temporal model $\mathfrak{M} = (\mathfrak{T}, \mathfrak{L}, \mathfrak{V})$ with $\mathfrak{L} = (M, \mathbb{I}_d)$.

Since *stripe* holds in $\mathfrak{M}$ at 0, we have, for every $y \in M$, $\mathfrak{M}, (0, y) \models stripe$ iff $\mathfrak{M}, (j, y) \models stripe$ for all j, $1 \leq j \leq N$. The transitive binary relation R_s on V defined by taking xR_sy will be modified to the distance relation d on the topometric space M defined by taking $d(x, y)$. The condition will be changed to that if there is $z \in M$ such that $\exists \epsilon, d(x, z) < \epsilon$ and $d(z, y) < \epsilon$, and $(M, (0, x)) \models stripe$ holds iff $(M, (0, z)) \not\models stripe$. □

Theorem 5.2 is the immediate result of Lemma 5.3.

Case study

The example of the train collision avoidance system can be treated as a cyber-physical system. In cyber system, the electrical signals are discrete, and the system clock ticks discretely. However, in physical environment, the running of the train follows kinetic equation, which is continuously changing. The execution of the train collision avoidance system is characterized a sequence of trace, which describes the evolution of spatial region.

The region of movement authority is defined as a special rail sections from the position that an train is authorized to enter to the end of movement authority (EoA), which is the position that the train reaches the safety margin of the leading train. A train must send a movement authority request and receive a permission before the train can enter the next section. In case of emergency, the following train must brake without the permission. In Fig. 7, p_{ma_req} and p_{brake} refer to the position that the following train sends a movement authority request and the braking position, respectively. The braking distance τ_{bd} occupies the section from the braking position p_{brake} to EoA. If the region of movement authority τ_{ma} is treated as the universal set, we can describe the spatial relation as

$$\tau_{bd} \sqsubseteq \tau_{ma} \tag{19}$$

And $\overline{\tau_{bd}}$ refers to the distance that the movement authority τ_{ma} minus the braking distance τ_{bd}, i.e., $\mathfrak{V}(\overline{\tau_{bd}}) = \mathfrak{V}(\tau_{ma}) - \mathfrak{V}(\tau_{bd})$, where $\mathfrak{V}(\tau_{ma})$, $\mathfrak{V}(\overline{\tau_{bd}})$ and $\mathfrak{V}(\tau_{bd})$ denote the value of the corresponding spatial terms τ_{ma}, $\overline{\tau_{bd}}$ and τ_{bd}.

Also, *before the following train receives a movement authority, the position of the train is less than* p_{brake}, i.e., the spatial entities of the train τ_{train} and the braking distance τ_{bd} doesn't overlap. The spatial relation can be specified as

$$\neg \diamondsuit_{\epsilon} (\tau_{train} \sqcap \tau_{bd}) \tag{20}$$

There are two kinds of braking modes: service braking (SB) and emergency braking (EB). Service braking refers to that a train decelerates until it stops in EoA. Emergency braking means the maximal acceleration a_{max} of a train to EoA if its velocity is greater than some critical value v_c. *In order to ensure collision avoidance, after receiving movement authority, the following train decelerates by a given velocity v until it stops within the time t*. Its formalization in STL is straightforward by formula 21:

$$\begin{aligned} &(((v \leq v_c) \wedge (a \leq 0)) \mathcal{U}_{[0,t)} (s \leq EoA) \\ &\vee ((v \geq v_c) \wedge (a \leq -a_{max})) \mathcal{U}_{[0,t)} (v \leq 0)) \end{aligned} \tag{21}$$

where v, a and s is the velocity, acceleration and position of the following train.

Suppose the time from sending movement authority to stopping of the following train is t_0, and the braking time of the following train is t_1. In order to ensure collision

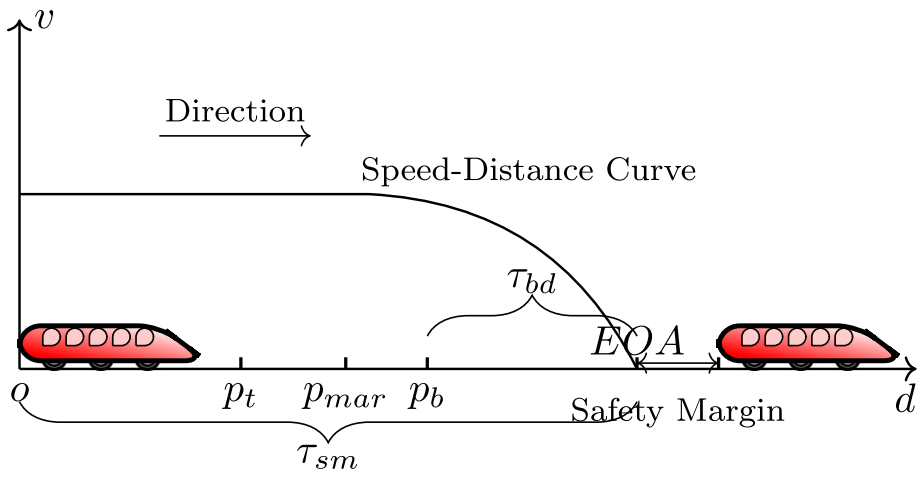

Fig. 7 The speed-distance curve of mobility authority

avoidance, *after sending movement authority at time 0, the train doesn't overlap with the braking distance, until the train stops within* t_0. The specification will be expressed as an STSL$_{PC}$ formula

$$\square_{[0,t_0)}\left(\neg\diamondsuit(\tau_{train}\sqcap\tau_{bd})\mathcal{U}_{[t_0-t_1,t_0]}(\nu\leq 0)\right) \tag{22}$$

After sending the movement authority, the following train runs to the braking region. And after receiving movement authority, the train and the braking distance don't overlap until it stops from t_0 *to* t_1. Its formalization in an STSL$_{OC}$ formula is straightforward the formula

$$\begin{aligned}&\square_{[0,t_0)}(\tau_{train}\mathcal{U}_{[p_{ma\_req},p_{bd})}\tau_{bd}\wedge\\&\quad(\neg\diamondsuit(\tau_{train}\sqcap\tau_{bd})\mathcal{U}_{[t_0-t_1,t_0)}(\nu\leq 0))\end{aligned} \tag{23}$$

Related work

In order to specify spatio-temporal properties of cyber-physical systems, the spatio-temporal logics, which enjoy discrete or dense time domain and Boolean or quantitative value, attract some researchers' attention in Table 1. Generally, there are two kinds of logic-based approaches to specify spatio-temporal properties: the extension of temporal logic with spatial modalities and the combinations of spatial logic and temporal logic.

Some spatio-temporal logics are extensions of temporal logic with spatial modality. In [66], temporal modalities are extended with spatial directions to reason reaction diffusion systems. SSTL [60] is presented to combine the temporal modality *until* with two spatial modalities, so that one can express that something is true somewhere nearby and being surrounded by a region that satisfies a given spatio-temporal property. STREL [61] extends SSTL with spatial *reachability*, *escape* operators to describe the mobile and spatially distributed cyber-physical systems. Balbiani [67] explores the 2-dimensional space in multi-agent systems through extending dynamic logic with formulas representing the agents' positions and programs moving from one position to another position. But these works face the problem of the expressiveness of discrete spatial representation, rather than more complex continuous space. Andreas [68] et al. present Shape Calculus based on Duration Calculus extended bounded polyhedron for the n-dimensional space for the specification and verification of mobile real-time systems. Mardare [64] presents Dynamic Spatial Logic, $\mathcal{L}_{DS}$, as an extension of Hennessy-Milner logic with parallel operator to distinguish processes. MLSL [63] is a two-dimensional extension of spatial interval temporal logic, where one dimension is characterized by a continuous space to describe the position in each lane and the other denotes a discrete space to count the number of the lane.

The combinations of temporal logic and spatial logic inherit the expressiveness of the two kinds of logics. LTL and CTL imply discrete time in temporal part. Bennett et al. [65] construct a multi-dimensional modal logic named PSTL through the Cartesian product of the temporal logic PTL and the modal logic S4$_u$ to specify the discrete time and "general" topological space. Gabelaia et al. [22] present the principles for the requirements of a combined spatio-temporal form, and apply properly those principles and propose the combined spatio-temporal logic between PTL and some fragments of modal spatial logic S4$_u$. They prove that the complexity of combination of PTL with S4$_u$ is PSPACE-complete. Kremer and Mints [62] provide dynamic topological logic (DTL) as a combination of LTL and S4$_u$ to describe the dynamic changes of spatial objects over time. Shao et al. [69] also consider the combination of proposition temporal logic PTL and S4$_u$ and apply it to several classical properties of train control systems. Ciancia et.al [58] present STLCS through enhancing SLCS with temporal operators that features the CTL path quantifiers ∀ (for all paths) and ∃ (there exists a path). All these work are trying to answer how to specify spatio-temporal properties in discrete time, rather than dense time.

In order to express spatial changes in dense time, MTSL [31] is proposed to specify spatio-temporal properties of cyber-physical systems by integrating MTL with S4$_u$. They follow the traditional S4$_u$ with truth value to specify spatial changes and extend the domain of time to real-valued interval within bounded time in the principle of PC and OC.

The above proposed language are employing classical model checking to verify the system from the specified properties. The approach achieves the model of a system to check whether the model satisfies the properties specified by the proposed language. However, we may need an approach to get the satisfaction degree, rather than satisfaction or violation.

STL expresses the changes of real-valued signals in dense time. The system can be verified at run time to monitor the satisfaction degree of the signals from an STL formula [11]. But it is not enough to specify spatial properties using an STL formula. Haghighi et al. [59] present SpaTeL as a combination of signal temporal logic (STL) and tree spatial superposition logic (TSSL) in networked systems. While, TSSL is a discrete structure to describe spatial static relations. To specify the spatial terms with changeable shape over dense time, we propose STSL$_{PC}$ through integrating STL with S4$_u$, to describe the spatio-temporal properties of cyber-physical systems with dense time and real-valued variables. STSL$_{PC}$ interprets spatial subset relation and threshold predicate ad atomic proposition, and returns Boolean value to satisfaction or violation and the satisfaction degree of signals and spatial terms according to Boolean and quantitative interpretation. We extend STSL$_{PC}$ to express the spatial evolution over dense time through extending the interpretation temporal *globally, eventually* and *until* bounded

Table 1 Logics for specifying spatio-temporal properties

Spatio-Temporal Logic	Temporal representation			Spatial representation			Applications
	Temporal Logic	Temporal Operator	Temporal Domain	Spatial Logic	Spatial Operator	Spatial Domain	
STSL [15]	STL	Threshold predicate, Boolean connectives,*Globally, eventually, until with interval*	Dense time	$S4_u$	spatial *intersection, union, complementary, interior, closure + universal, existential*	Both changeable and unchangeable spatial terms in topometric space	Runtime verification for cyber-physical systems
STLCS [58]	CTL	Boolean connectives, branching *next, globally, eventually, until*	Branching time	SLCS	*next, surrounded, reachability, touch, everywhere, somewhere*	Discrete closure space	Public transport systems
SpaTeL [59]	STL	Threshold predicate, Boolean connectives,*Globally, eventually, until with interval*	Dense time	TSSL	*next, globally, eventually, until* bounded with direction	Quad transition system	Networked dynamical systems
SSTL [60]	STL	*Globally, eventually, until with interval*	Dense time	Spatial modality	*somewhere, everywhere, until, surround*	Discrete space	Turing reaction diffusion system and bike-sharing system
STREL [61]	STL	*Globally, eventually, until and since with interval*	Dense time	Spatial modality	*reachability, escape, somewhere, everywhere, until, surround*	Euclidean spatial model	Mobile Ad hoc sensor network
DTL [62]	LTL	Boolean connectives, linear *next, globally, eventually, until*	Discrete time	S4	spatial *intersection, union, complementary, interior, closure*	Topological space	Dynamic topological systems
MLSL [63]	ITL	*equal, before, meets, overlap, during, starts, finishes*, temporal interval *chop*	Dense time	Shape Calculus	*claimed by, reserved by, occupied by, horizontal chop, vertical chop*	Traffic snapshots	Multi-lane motorway traffic
$\mathcal{L}_{DS}$ [64]	HML	modal diamond operator $\langle\mu\rangle$ and branching temporal operators	Discrete time	π-calculus	*composition, guarantee, hiding, revelation, next*	Mobile agent	Distributed concurrent systems
PSTL [65]	PTL	Boolean connectives,*next, globally, eventually, until*	Discrete time	$S4_u$	*intersection, union, complementary, interior, closure, universal, existential*	Topological space	Geographical region
MTSL [31]	MTL	Boolean connectives, *Globally, eventually, until with interval*	Bounded time	$S4_u$	*intersection, union, complementary, interior, closure, universal, existential*	Topological space	Train control systems

with interval as spatial operators. We assume that the systems satisfy finite variability so that the STSL$_{PC}$ formulas are verified at run-time. The decidability and complexity of the two formalisms are analyzed, and the soundness and completeness of their axiomatization are proved.

Conclusion and future work

In this paper, we build STSL$_{PC}$, a spatio-temporal specification language by combining STL with spatial logic S4$_u$, specifically containing dense time and topometric space. We provide the syntax and semantics of the proposed language, and guarantee the seamless integration of spatial logic with temporal aspect from the perspective of the changes of purely spatial proposition in STSL$_{PC}$ and spatial objects in STSL$_{OC}$ over time. A Hilbert-style proof axiomatization system and the soundness and completeness results show that the completeness of STSL$_{PC}$ and the incompleteness of STSL$_{OC}$. The decidability indicates the undecidable STSL$_{OC}$ and the decidable STSL$_{PC}$. Further, we present that the complexity for the STSL$_{PC}$ is EXPSPACE-complete and a decision procedure is present for the decidable fragment. Currently, the proposed STSL has a powerful expressiveness.

However, the insufficiency of the paper exists in that there is no concrete monitoring technique, like other works [60, 70] have done. In order to verify a cyber-physical system, it is not the situation that we can achieve all the model of the system. However, monitoring provides an approach to verify a trace of the system to guarantee the reliability of the current execution. We have already presents the feasibility of the proposed language in the semantics. One can implement the language and present the monitoring algorithm to verify the spatio-temporal specification language. The reason why we are trying to monitor an STSL formula exists in the interpretation of STSL on spatio-temporal traces. This makes traditional model checking insufficient to verify the spatio-temporal properties specified with STSL. The spatio-temporal traces for monitoring an STSL specification can be automata, petri nets [2], process algebra, neural networks, differential equations et al. We are developing the monitoring tool. Firstly, we are developing the offline monitoring through sampling spatio-temporal traces for a simulated system against the spatio-temporal specification language. Secondly, the runtime verification like online monitoring will be interesting to achieve spatio-temporal traces from the executing systems to verify an STSL formula. Thirdly, the more applications, like mobile systems [71] and cloud service-based systems, will be developed.

Appendix A: Proof of soundness of STSL$_{PC}$

The proof of Theorem 4.1:

S0 and S1 can be immediately got from the definition.

S2: $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \overline{\tau_2} \sqsubseteq \overline{\tau_1}$

Proof $\tau_1 \sqsubseteq \tau_2$,
$\Leftrightarrow$ If $x \in \tau_1$, then $x \in \tau_2$,
$\Leftrightarrow$ If $x \notin \tau_2$, then $x \notin \tau_1$,
$\Leftrightarrow \overline{\tau_2} \sqsubseteq \overline{\tau_1}$. □

S3 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \mathbb{C}\tau_1 \sqsubseteq \tau_2$

Proof $\tau_1 \sqsubseteq \tau_2$,
$\mathfrak{V}(\tau) = \mathfrak{V}(\mathbb{C}\tau)$,
$\Leftrightarrow \mathbb{C}\tau_1 \sqsubseteq \tau_2$. □

S4 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \tau_1 \sqsubseteq \mathbb{I}\tau_2$

Proof $\tau_1 \sqsubseteq \tau_2$,
$\Leftrightarrow$, if $x \in \tau_1$, then $x \in \tau_2$,
and $\mathfrak{V}(\tau_1) \neq \mathfrak{V}(\tau_2)$,
$\Leftrightarrow$, $\tau_1 \sqsubseteq \mathbb{I}\tau_2$, □

S5 $\tau_1 \sqsubseteq \tau_2 \rightarrow \mathbb{I}\tau_1 \sqsubseteq \mathbb{I}\tau_2$

Proof $\tau_1 \sqsubseteq \tau_2$,
$\Leftrightarrow$, $\tau_1 \sqsubseteq \mathbb{I}\tau_2$,
$\mathbb{I}\tau_1 \sqsubseteq \tau_1$,
$\Rightarrow$, $\mathbb{I}\tau_1 \sqsubseteq \mathbb{I}\tau_2$. □

S6 $\tau_1 \sqsubseteq \tau_2 \leftrightarrow \mathbb{C}\tau_1 \sqsubseteq \mathbb{C}\tau_2$

Proof $\tau_1 \sqsubseteq \tau_2$,
$\Leftrightarrow$, $\mathbb{C}\tau_1 \sqsubseteq \tau_2$,
$\tau_2 \sqsubseteq \mathbb{C}\tau_2$,
$\Rightarrow$, $\mathbb{C}\tau_1 \sqsubseteq \mathbb{C}\tau_2$. □

S7 $\tau_1 \sqsubseteq \mathbb{I}\tau_2 \rightarrow \tau_1 \sqsubseteq \mathbb{C}\tau_2$

Proof $\tau_1 \sqsubseteq \mathbb{I}\tau_2$,
$\Leftrightarrow$, $\mathbb{I}\tau_2 \sqsubseteq \tau_2$,
$\tau_2 \sqsubseteq \mathbb{C}\tau_2$,
$\Rightarrow$, $\tau_1 \sqsubseteq \mathbb{C}\tau_2$. □

S8 $(\tau_1 \sqcup \tau_2) \sqsubseteq \tau_3 \rightarrow (\tau_1 \sqsubseteq \tau_3) \vee (\tau_2 \sqsubseteq \tau_3)$

Proof $(\tau_1 \sqcup \tau_2) \sqsubseteq \tau_3$,
$\Leftrightarrow$, if $x \in \tau_1$ or $x \in \tau_2$, then $x \in \tau_3$,
$\Rightarrow$, if $x \in \tau_1$, then $x \in \tau_3$ or $x \in \tau_2$, then $x \in \tau_3$,
$\Leftrightarrow$, $\tau_1 \sqsubseteq \tau_3$, or $\tau_2 \sqsubseteq \tau_3$,
$\Leftrightarrow$, $(\tau_1 \sqsubseteq \tau_3) \vee (\tau_2 \sqsubseteq \tau_3)$ □

S9 $\tau_1 \sqsubseteq (\tau_2 \sqcap \tau_3) \rightarrow (\tau_1 \sqsubseteq \tau_2) \wedge (\tau_1 \sqsubseteq \tau_3)$

Proof $\tau_1 \sqsubseteq (\tau_2 \sqcap \tau_3)$,
$\Leftrightarrow$, if $x \in \tau_1$, then $x \in \tau_2$ and $x \in \tau_3$,
$\Rightarrow$, if $x \in \tau_1$, then $x \in \tau_2$ and $x \in \tau_1$, then$x \in \tau_3$,

$\Leftrightarrow, \tau_1 \sqsubseteq \tau_2$, and $\tau_1 \sqsubseteq \tau_3$,
$\Leftrightarrow, (\tau_1 \sqsubseteq \tau_2) \wedge (\tau_1 \sqsubseteq \tau_3)$. □

S10: $\Diamond\!\!\!\!-\tau \leftrightarrow \neg\boxdot\overline{\tau}$

Proof $\Diamond\!\!\!\!-\tau$,
$\Leftrightarrow, \exists x \in \mathcal{L}, x \in \tau$,
$\Leftrightarrow, \forall y \notin \mathcal{L}, y \notin \tau$,
$\Leftrightarrow, \neg\boxdot\overline{\tau}$. □

S11: $\boxdot(\tau_1 \sqcap \tau_2) \rightarrow \boxdot\tau_1 \wedge \boxdot\tau_2$

Proof $\boxdot(\tau_1 \sqcap \tau_2)$,
$\Leftrightarrow, \forall x \in \mathcal{L}, x \in \tau_1$ and $x \in \tau_2$,
$\Rightarrow \forall x \in \mathcal{L}, x \in \tau_1$ and $\forall x \in \mathcal{L}, x \in \tau_2$,
$\Leftrightarrow \boxdot\tau_1 \wedge \boxdot\tau_2$. □

S12: $\Diamond\!\!\!\!-(\tau_1 \sqcup \tau_2) \rightarrow \Diamond\!\!\!\!-\tau_1 \vee \Diamond\!\!\!\!-\tau_2$

Proof $\Diamond\!\!\!\!-(\tau_1 \sqcup \tau_2)$,
$\Leftrightarrow \exists x \in \mathcal{L}, x \in \tau_1$ or $x \in \tau_2$,
$\Rightarrow \exists x \in \mathcal{L}, x \in \tau_1$ or $\exists x \in \mathcal{L}, x \in \tau_2$,
$\Leftrightarrow \Diamond\!\!\!\!-\tau_1 \vee \Diamond\!\!\!\!-\tau_2$. □

T1: $\Diamond_I\phi \leftrightarrow \neg\Box_I\neg\phi$

Proof $\Diamond_I\phi$,
$\Leftrightarrow \exists t \in I, \phi$ holds,
$\Leftrightarrow$ The proposition $\forall t \in I, \phi$ doesn't hold is false,
$\Leftrightarrow \neg\Box_I\neg\phi$. □

T2: $\Box_I(\phi \wedge \varphi) \rightarrow (\Box_I\phi \wedge \Box_I\varphi)$

Proof $\Box_I(\phi \wedge \varphi)$,
$\Leftrightarrow, \forall t \in I, \phi$ and φ hold,
$\Rightarrow, \forall t \in I, \phi$ holds and $\forall t \in I, \varphi$ holds,
$\Leftrightarrow, \Box_I\phi \wedge \Box_I\varphi$ □

T3 $\Diamond_I(\phi \vee \varphi) \rightarrow (\Diamond_I\phi \vee \Diamond_I\varphi)$

Proof $\Diamond_I(\phi \vee \varphi)$,
$\Leftrightarrow, \exists t \in I, \phi$ or φ hold,
$\Rightarrow, \exists t \in I, \phi$ holds or $\exists t \in I, \varphi$ holds,
$\Leftrightarrow, \Diamond_I\phi \vee \Diamond_I\varphi$ □

T4: $\phi U_I\varphi \rightarrow \Diamond_I\varphi$

Proof $\phi U_I\varphi$,
$\Leftrightarrow \exists t' \in [t + I], \varphi$ holds, and $\forall t'' \in [t, t'], \phi$ holds,
$\Rightarrow \exists t' \in [t + I], \varphi$ holds,
$\Leftrightarrow \Diamond_I\varphi$ □

Q0: $\Diamond_{I\cup J}\varphi \leftrightarrow \Diamond_I\varphi \vee \Diamond_J\varphi$

Proof $\Diamond_{I\cup J}\varphi$,
$\Leftrightarrow \exists t \in I$ or J, φ holds,
$\Leftrightarrow \exists t \in I, \varphi$ holds, or $\exists t \in J, \varphi$ holds,
$\Leftrightarrow \Diamond_I\varphi \vee \Diamond_J\varphi$. □

Q1: $\Box_{I\cap J}\varphi \leftrightarrow \Box_I\varphi \wedge \Box_J\varphi$

Proof $\Box_{I\cap J}\varphi$,
$\Leftrightarrow \forall t \in I$ and J, φ holds,
$\Leftrightarrow \forall t \in I, \varphi$ holds, and $\forall t \in J, \varphi$ holds,
$\Leftrightarrow Box_I\varphi \wedge \Box_J\varphi$. □

Q2: $\phi U_{I\cup J}\varphi \rightarrow \Diamond_{I\cup J}\varphi$

Proof $\phi U_{I\cup J}\varphi$,
$\Leftrightarrow \exists t' \in [t + I \cup J], \varphi$ holds, and $\forall t'' \in [t, t'], \phi$ holds,
$\Rightarrow \exists t' \in [t + I \cup J], \varphi$ holds,
$\Leftrightarrow \Diamond_{I\cup J}\varphi$ □

Abbreviations

STL: Signal temporal logic; STSL: Spatio-temporal specification language; LTL: Linear temporal logic; MITL: Metric interval temporal logic; CP: Classical propositional logic; BNF: Backus-Naur form; PST: Propositional spatio-temporal logic; SMT: Satisfiability modulo theories

Acknowledgments

We would like to thank the anonymous reviewers for their valuable comments and suggestions, which helped improve the quality of this paper. Also, we want to express our heartfelt gratitude to the authors of the literature cited in this paper for contributing useful ideas to this study.

Authors' contributions

Tengfei Li, Jing Liu and Haiying Sun have written this paper and have done the research which supports it. Tengfei Li writes the paper and is responsible to prove the completeness and decidability of the proposed language. Jing Liu is the lead of the laboratory. She is responsible for obtaining the funding of the work. Also, she contributes to the fundamental idea of the work. Haiying Sun is responsible for maneging the schedule and provides feasible plan. She provides the initial idea of the proposed language and takes participate in the proof work. Further, she proofreads the paper to improve the English writing and has a great influence on the revision process. So it is bettwe for her to be the corresponding author. Both Xiang Chen and Lipeng Zhang contribute to the applications and case study of our proposed spatio-temporal specification language. Xiang Chen mainly considers the train collision avoidance system and provides the spatio-temporal properties according to the specification. Lipeng Zhang contributes to several related work and discusses the difference from other applications. Also, Lipeng provides a perspective to interpret the concurrency for the topometric model. Junfeng Sun has collaborated in the examples of this paper as an assistant president of CASCO Signal Ltd. The authors read and approved the final manuscript.

Authors' information

Tengfei Li received the B.S. degree in mathematics from the School of Mathematics and Statistics in 2014. He is currently pursuing the Ph.D. degree in Software Engineering at School of Software Engineering, East China Normal University, Shanghai, China. From April to October 2018, he visited INRIA Sophia Antipolis, Nice, France. His research interests are in the area of spatio-temporal logics, safety-critical cyber physical systems, formal verification and hybrid systems. **Jing Liu** is currently a professor of computer science with East China Normal University, China. In recent years, she has been involved in the area of model-driven architecture. She currently focuses on the design of real-time embedded systems and cyber-physical systems. **Haiying Sun** received a Ph.D. degree in East China Normal University, China, her research interests include formal method, system simulation and

model-driven engineering. **Xiang Chen** is engineer of Urban Train Control System Development Department in CASCO, he has rich experience in safety-related software development, and leads a team to develop automatic train control(ATC) system for urban rail transit., he has done a lot of research on safety software technology, and introduces formal-method/semi-method and Model Based Software Engineering(MBSE) for ATC software. **Lipeng Zhang** is currently a Manager of the Safetd platform department, CASCO Signal Ltd. In recent years, he has been involved in the area of safety critical software verification and validation. Currently, he focuses on the design of CBTC(Communication Based Train Control) system based on vehicle-vehicle communication. **JunFeng Sun** is currently an assistant president of CASCO Signal Ltd and a vice director of R&D Institute of CASCO Signal Ltd. In recent years, he is working on the area of train control system design. Now his work focuses on the design of railway signal security computer platform.

Funding
This document is the results of the research project funded by the National Key Research and Development Project 2017YFB1001800, NSFC 61972150 and Shanghai Knowledge Service Platform Project ZF1213.

Availability of data and materials
Not applicable.

Competing interests
The authors declare that they have no competing interests regarding the publication of this manuscript.

Author details
[1]Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, No. 3663, North Zhongshan Road, 200062 Shanghai, China. [2]CASCO SIGNAL LTD., No.489, North Xizang Road, Shanghai, China.

Received: 1 June 2020 Accepted: 22 October 2020
Published online: 25 November 2020

References

1. Lee EA, Seshia SA (2016) Introduction to Embedded Systems: A Cyber-physical Systems Approach. MIT Press, California
2. Liu G, Jiang C, Zhou M (2018) Time-soundness of time Petri nets modelling time-critical systems. ACM Trans Cyber Phys Syst 2(2):1–27
3. Fan C, Qi B, Mitra S, Viswanathan M, Duggirala PS (2016) Automatic reachability analysis for nonlinear hybrid models with C2E2. In: International Conference on Computer Aided Verification, Springer. pp 531–538
4. Gao H, Liu C, Li Y, Yang X (2020) V2VR: reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability. IEEE Trans Intell Transp Syst 21:1–14. https://doi.org/10.1109/TITS.2020.2983835
5. Liu J, Li T, Ding Z, Qian Y, Sun H, He J (2019) AADL+: a simulation-based methodology for cyber-physical systems. Front Comput Sci 13(3):1–23
6. Gao H, Chu D, Duan Y, Yin Y (2017) Probabilistic model checking-based service selection method for business process modeling. Int J Softw Eng Knowl Eng 27(6):897–923
7. An D, Liu J, Chen X, Li T, Yin L (2019) A Modeling Framework of Cyber-Physical-Social Systems with Human Behavior Classification Based on Machine Learning. In: 21st International Conference on Formal Engineering Methods, Springer. pp 522–525
8. Gao H, Kuang L, Yin Y, Guo B, Dou K (2020) 'Mining consuming behaviors with temporal evolution for personalized recommendation in mobile marketing Apps. Mob Netw Appl (MONET) 25(4):1233–1248
9. Wolter F, Zakharyaschev M (2005) A logic for metric and topology. J Symb Log 70(3):795–828
10. Raman V, Donzé A, Sadigh D, Murray RM, Seshia SA (2015) Reactive synthesis from signal temporal logic specifications. In: Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control, ACM. pp 239–248
11. Donzé A, Ferrere T, Maler O (2013) Efficient robust monitoring for STL. In: International Conference on Computer Aided Verification, Springer. pp 264–279
12. Blackburn P, De Rijke M, Venema Y (2002) Modal Logic: Graph. Darst, Vol. 53. Cambridge University Press, Dallas, America
13. Davoren JM (2007) Topological semantics and bisimulations for intuitionistic modal logics and their classical companion logics. In: International Symposium on Logical Foundations of Computer Science, Springer. pp 162–179
14. Fernández-Duque D (2010) Absolute completeness of S4u for its measure-theoretic semantics. Adv Modal Log 8:100–119
15. Li T, Jing L, An D, Sun H (2019) A Sound and Complete Axiomatisation for Spatio-Temporal Specification Language. In: The 31st International Conference on Software Engineering & Knowledge Engineering, KSI. pp 153–204
16. Demri S, Goranko V, Lange M (2016) Temporal Logics in Computer Science: Finite-state Systems, Vol. 58. Cambridge University Press, Cambridge, United Kingdom
17. Zhang Y, Li K (2015) Decidability of logics based on an indeterministic metric tense logic. Stud Logica 103(6):1123–1162
18. Platzer A (2018) Logical foundations of cyber-physical systems. Springer, Gewerbestrasse, Switzerland
19. Bohner M, Peterson A (2012) Dynamic equations on time scales: An introduction with applications. Birkhäuser Boston, Washington D.C., USA
20. Ladner RE (1977) The computational complexity of provability in systems of modal propositional logic. SIAM J Comput 6(3):467–480
21. McKinsey JCC (1941) A solution of the decision problem for the Lewis systems S2 and S4, with an application to topology. J Symb Log 6(4):117–124
22. Gabelaia D, Kontchakov R, Kurucz A, Wolter F, Zakharyaschev M (2005) Combining spatial and temporal logics: expressiveness vs. complexity. J Artif Intell Res 23:167–243
23. Randell DA, Cui Z, Cohn AG (1992) A spatial logic based on regions and connection. In: Proceedings of the 3rd International Conference on Principles of Knowledge Representation and Reasoning, Morgan. pp 165–176
24. Liu W, Li S, Renz J (2009) Combining RCC-8 with Qualitative Direction Calculi: Algorithms and Complexity. In: Proceedings of the 21st International Joint Conference on Artificial Intelligence, Morgan Kaufmann Vol. 2009. pp 854–859
25. Kontchakov R, Kurucz A, Wolter F, Zakharyaschev M (2007) Spatial logic+ temporal logic=? In: Handbook of Spatial Logics, Springer. pp 497–564
26. Shehtman V (1999) Everywhere and here. J Appl Non-Class Log 9(2-3):369–379
27. Pnueli A (1977) The temporal logic of programs. In: 18th Annual Symposium on Foundations of Computer Science, IEEE. pp 46–57
28. Pradella M, Morzenti A, Pietro PS (2013) Bounded satisfiability checking of metric temporal logic specifications. ACM Trans Softw Eng Methodol (TOSEM) 22(3):1–54
29. Maler O, Nickovic D (2004) Monitoring temporal properties of continuous signals. In: Formal Techniques, Modeling and Analysis of Timed and Fault-Tolerant Systems, Springer. pp 152–166
30. Donzé A, Maler O (2010) Robust satisfaction of temporal logic over real-valued signals. In: International Conference on Formal Modeling and Analysis of Timed Systems, Springer. pp 92–106
31. Sun H, Liu J, Chen X, Du D (2015) Specifying cyber physical system safety properties with metric temporal spatial logic. In: 2015 Asia-Pacific Software Engineering Conference (APSEC), IEEE. pp 254–260
32. Gabbay D, Pnueli A, Shelah S, Stavi J (1980) On the temporal analysis of fairness. In: Proceedings of the 7th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, ACM. pp 163–173
33. Lichtenstein O, Pnueli A (1985) Checking that finite state concurrent programs satisfy their linear specification. In: Proceedings of the 12th ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages, ACM. pp 97–107
34. Nenzi L, Bortolussi L, Ciancia V, Loreti M, Massink M (2015) Qualitative and quantitative monitoring of spatio-temporal properties. In: Runtime Verification, Springer. pp 21–37
35. Kuratowski K (2014) Topology, Vol. 1. Elsevier Science, London, England
36. Milner R (2001) Bigraphical reactive systems. In: International Conference on Concurrency Theory. pp 16–35
37. Sevegnani M, Calder M (2015) Bigraphs with sharing. Theor Comput Sci 577:43–73

38. Lemire D (2007) Streaming maximum-minimum filter using no more than three comparisons per element. Nordic J Comput 13(4):328–339
39. Pnueli A (1981) The temporal semantics of concurrent programs. Theor Comput Sci 13(1):45–60
40. Kesten Y, Pnueli A (2002) Complete proof system for QPTL. J Log Comput 12(5):701–745
41. Schobbens PY, Raskin J-F, Henzinger TA (2002) Axioms for real-time logics. Theor Comput Sci 274(1-2):151–182
42. Jacquette D (2002) A Companion to Philosophical Logic. Wiley Online Library, Viotoria, Australia
43. Balbiani P, Fernández-Duque D (2016) Axiomatizing the lexicographic products of modal logics with linear temporal logic. In: International Conference on Advances in Modal Logic. pp 78–96
44. Montanaria A, de Rijkeb M (1997) Two-sorted metric temporal logics. Theor Comput Sci 183(2):187–214
45. Gabbay DM, Hodkinson IM (1990) An axiomatization of the temporal logic with until and since over the real numbers. J Log Comput 1(2):229–259
46. Kojima K, Igarashi A (2011) Constructive linear-time temporal logic: Proof systems and Kripke semantics. Inf Comput 209(12):1491–1503
47. Chellas BF (1980) Modal Logic: An Introduction. Cambridge university press, New York, USA
48. Alur R, Feder T, Henzinger TA (1996) The benefits of relaxing punctuality. J ACM 43(1):116–146
49. Barrett C, Tinelli C (2018) Satisfiability modulo theories. In: Handbook of Model Checking. Springer, Cham, Switzerland. pp 305–343
50. Bersani MM, Rossi M, San Pietro P (2015) An SMT-based approach to satisfiability checking of MITL. Inf Comput 245:72–97
51. Bersani MM, Rossi M, San Pietro P (2013) Deciding continuous-time metric temporal logic with counting modalities. In: International Workshop on Reachability Problems, Springer. pp 70–82
52. Demri S, D'Souza D (2007) An automata-theoretic approach to constraint LTL. Inf Comput 205(3):380–415
53. Bersani MM, Rossi M, Pietro PS (2013) Deciding the satisfiability of MITL specifications. In: 4th International Symposium on Games, Automata, Logics and Formal Verification. pp 64–78
54. Bersani MM, Rossi MG, San Pietro P (2014) On the satisfiability of metric temporal logics over the reals. Electron Commun EASST 66:1–15
55. Hopcroft JE, Motwani R, Ullman JD (2001) Introduction to automata theory, languages, and computation. Acm Sigact News 32(1):60–65
56. Gabbay DM, Kurucz A, Wolter F, Zakharyaschev M (2003) Many-dimensional modal logics: theory and applications. Elsevier North Holland, London, United Kingdom
57. Gabelaia D, Kontchakov R, Kurucz A, Wolter F, Zakharyaschev M (2003) On the Computational Complexity of Spatio-Temporal Logics. In: FLAIRS Conference. pp 460–464
58. Ciancia V, Gilmore S, Grilletti G, Latella D, Loreti M, Massink M (2018) Spatio-temporal model checking of vehicular movement in public transport systems. Int J Softw Tools Technol Transfer 20(3):289–311
59. Haghighi I, Jones A, Kong Z, Bartocci E, Gros R, Belta C (2015) SpaTeL: a novel spatial-temporal logic and its applications to networked systems. In: Proceedings of the 18th International Conference on Hybrid Systems: Computation and Control, ACM. pp 189–198
60. Nenzi L, Bortolussi L, Ciancia V, Loreti M, Massink M (2017) Qualitative and quantitative monitoring of spatio-temporal properties with SSTL. Log Methods Comput Sci 14(4):1–38
61. Bartocci E, Bortolussi L, Loreti M, Nenzi L (2017) Monitoring mobile and spatially distributed cyber-physical systems. In: Proceedings of the 15th ACM-IEEE International Conference on Formal Methods and Models for System Design, ACM. pp 146–155
62. Kremer P, Mints G (2005) Dynamic topological logic. Ann Pure Appl Log 131(1):133–158
63. Xu B, Li Q (2016) A spatial logic for modeling and verification of collision-free control of vehicles. In: 2016 21st International Conference on Engineering of Complex Computer Systems (ICECCS), IEEE. pp 33–42
64. Mardare R (2006) Logical analysis of complex systems: Dynamic epistemic spatial logics. PhD thesis, University of Trento
65. Bennett B, Cohn AG, Wolter F, Zakharyaschev M (2002) Multi-dimensional modal logic as a framework for spatio-temporal reasoning. Appl Intell 17(3):239–251
66. Bartocci E, Gol EA, Haghighi I, Belta C (2018) A formal methods approach to pattern recognition and synthesis in reaction diffusion networks. IEEE Trans Control Netw Syst 5(1):308–320
67. Balbiani P, Fernández-Duque D, Lorini E (2017) Exploring the bidimensional space: a dynamic logic point of view. In: The 16th Conference on Autonomous Agents and MultiAgent Systems, Springer. pp 132–140
68. Schäfer A (2004) A calculus for shapes in time and space. In: International Colloquium on Theoretical Aspects of Computing, Springer. pp 463–477
69. Shao Z, Liu J, Ding Z, Chen M, Jiang N (2013) Spatio-temporal properties analysis for cyber-physical systems. In: 2013 18th International Conference on Engineering of Complex Computer Systems, IEEE. pp 101–110
70. Gao H, Xu Y, Yin Y, Zhang W, Li R, Wang X (2020) Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services. IEEE Internet Things J 7(5):4532–4542
71. Gao H, Huang W, Duan Y (2020) The cloud-edge based dynamic reconfiguration to service workflow for mobile ecommerce environments: A QoS prediction perspective. ACM Trans Internet Technol. https://doi.org/10.1145/3391198

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen journal and benefit from:

- ► Convenient online submission
- ► Rigorous peer review
- ► Open access: articles freely available online
- ► High visibility within the field
- ► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com