Automatic verification of reliability requirements of spatio-temporal analysis using Three-Valued Spatio-Temporal Logic

Automatic verification of reliability requirements of spatio-temporal analysis using Three-Valued Spatio-Temporal Logic

Fast Abstract

Ludovica Luisa Vissat, Jane Hillston
School of Informatics, University of Edinburgh, UK

Michele Loreti
DiSIA, University of Firenze, Italy

Laura Nenzi
Faculty of Informatics, Vienna University of Technology, Austria

ABSTRACT

In this paper we present the recently introduced Three-Valued Spatio-Temporal Logic (TSTL), which extends the available spatio-temporal analysis of stochastic systems, and an automatic procedure to verify whether this analysis satisfies given reliability requirements. The novel spatio-temporal logic TSTL enriches the analysis of properties expressed in Signal Spatio-Temporal Logic (SSTL), providing further insight into the dynamic behaviour of systems. Starting from the estimated satisfaction probabilities of given SSTL properties, it enables the analysis of their temporal and spatial evolution. We use a three-valued approach in our verification procedure to include the uncertainty associated with the simulation-based statistical method used to estimate the satisfaction probabilities. In relation to this aspect, we introduce a reliability specification for the TSTL analysis and we present a specific algorithm to automatically assess whether it is satisfied by the evaluation of TSTL formulas.

CCS CONCEPTS

• **Theory of computation → Verification by model checking**;

1 INTRODUCTION

The study of spatial stochastic systems seeks to analyse and predict their spatio-temporal dynamics, typically studied through stochastic simulations. Formal analysis of these systems verifies properties of their evolution expressed in terms of spatial and temporal modalities. Spatio-temporal logics and model checking techniques provide suitable analysis to evaluate the satisfaction probabilities of given properties, which are expressed through logical formulas. In many cases, performing statistical model checking [1] is the only feasible approach to estimate these values, using a finite set of simulation trajectories. A single trajectory is not descriptive enough to fully study the dynamic behaviour and to compare different systems and the complete exploration of all the possible trajectories is computationally infeasible. The outcome of this simulation-based method is an estimation of the satisfaction probabilities over the spatial domain. In [2] we presented a novel logic, called Three-Valued Spatio-Temporal Logic (TSTL), which widens the available analysis by enabling the study of spatio-temporal properties of the estimated satisfaction probabilities, in this case expressed using the spatio-temporal logic SSTL [3]. TSTL atomic propositions are inequalities on these values, estimated using statistical model checking. TSTL uses a three-valued approach to keep track of the unavoidable and associated uncertainty of this model checking procedure. We interpret the inequalities with different degrees of truth, using *true*, *false* and a third value *unknown*. In addition to the extended analysis, TSTL permits initial explorations of the system dynamics with relatively few simulations trajectories. Moreover, it can be used to evaluate if the analysis results are provided with enough accuracy. Given the uncertainty related to the model checking procedure, we introduce a reliability requirement, based on the amount of *unknown* values, and an automatic procedure to evaluate if it is matched by the results of TSTL monitoring. This automatic procedure will give an indication of when more simulations trajectories are needed, in order to draw stronger conclusions. Additional simulations will allow more precise SSTL initial analysis, followed by more precise analysis of TSTL propositions.

VALUETOOLS 2017, December 5–7, 2017, Venice, Italy

ACM ISBN 978-1-4503-6346-4/17/12.
https://doi.org/10.1145/3150928.3150961

2 SIGNAL SPATIO-TEMPORAL LOGIC

Signal Spatio-Temporal Logic (SSTL) [3] is a spatial extension of Signal Temporal Logic (STL) [4], a temporal logic suitable for describing properties of real-valued signals. SSTL focusses on properties of spatial population models, with a discrete representation of space using a finite undirected weighted graph. Spatial population models can be seen as a collection of agents which can interact, take different states and move in space. SSTL formulas are evaluated over a *spatio-temporal trajectory*, output of a stochastic simulation, which keeps track of the population counts in the different locations of the discrete spatial structure. The syntax of SSTL is given by:

$$\varphi ::= \mu \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \varphi_1 \mathcal{U}^{[t_1,t_2]} \varphi_2 \mid \diamondsuit_{[w_1,w_2]}\, \varphi \mid \varphi_1 \mathcal{S}_{[w_1,w_2]} \varphi_2$$

The SSTL *atomic proposition* μ describes an inequality on expressions with population counts, provided in the spatio-temporal trajectory. *Negation* $\neg$ and *disjunction* $\vee$ are the standard boolean operators and $\mathcal{U}$ is the *bounded until* operator. SSTL introduces two spatial operators: the *bounded somewhere* operator $\diamondsuit_{[w_1,w_2]}$, which requires that the property φ holds in a location reachable from the current one, with a cost w, $w \in [w_1, w_2]$, with $w_1 \leq w_2$, real values, and the *bounded surround* operator $\mathcal{S}_{[w_1,w_2]}$, which describes the property of being in a φ_1-region, surrounded by a

φ_2-region, reachable with a bounded cost. For more detailed description of the SSTL operators, see [3]. SSTL is provided with a *boolean* semantics that returns the value true/false depending on whether the observed spatio-temporal trajectory satisfies the defined SSTL formula or not. To estimate the probability that a given SSTL property φ is satisfied, we perform statistical model checking [1]. We shift the analysis from a single spatio-temporal trajectory to a set of spatio-temporal trajectories, assigning to each one a truth value, according to the boolean semantics. After this step we can estimate the satisfaction probability of the formula φ. It is provided with a confidence interval and calculated in a frequentistic manner, as the proportion of the number of spatio-temporal trajectories for which the property is satisfied, over their total number.

3 THREE-VALUED SPATIO-TEMPORAL LOGIC

The syntax of Three-Valued Spatio-Temporal Logic (TSTL) is given by:

$$\psi ::= \mathcal{P}_{<p}(\varphi) \mid \tilde{\neg}\psi \mid \psi_1 \tilde{\vee} \psi_2 \mid \psi_1 \tilde{\mathcal{U}}^{[t_1,t_2]} \psi_2 \mid \tilde{\diamondsuit}_{[w_1,w_2]} \psi \mid \psi_1 \tilde{\mathcal{S}}_{[w_1,w_2]} \psi_2$$

where $p \in [0,1]$ and φ is a given SSTL formula. The atomic TSTL formula $\mathcal{P}_{<p}(\varphi)$ expresses an inequality on the estimated satisfaction probability of the SSTL formula φ, checking if it is below the given threshold p. Conceptually all these operators are identical to the SSTL operators, but they operate on a three-valued domain, reasoning about estimated satisfaction probabilities and not population counts. The *three-valued* semantics of the atomic TSTL proposition returns the value true/unknown/false, evaluated depending on the respective position of p and the estimated confidence interval, as explained in [2]. In particular, the truth value *unknown* is assigned when the value p lies inside the estimated confidence interval.

4 RELIABILITY REQUIREMENT

In decision-making situations, such as at the beginning of a disease outbreak, we want to quickly compare different control strategies, evaluating properties of the systems with enough accuracy to draw appropriate conclusions. To perform the exploration of spatio-temporal properties with sufficient precision, which can vary depending on the applications, we introduce a reliability requirement and an automatic procedure to evaluate its satisfaction. The output of this verification will be a boolean value which expresses if the current analysis matches the reliability requirement $\mathcal{R}$ or not. This specification $\mathcal{R}$ will be defined as the proportion of *unknown* values which we can tolerate during the exploration of the TSTL property satisfaction. As shown in Algorithm 1, given a TSTL formula ψ, a set of spatio-temporal trajectories Σ and the reliability requirement $\mathcal{R}$, we perform TSTL monitoring for each location l of the spatial domain L. At each time step of the temporal horizon $\mathcal{T}$, which depends on the length of the spatio-temporal trajectories and the given logical formulas, our algorithm will check if the reliability specification is matched, identifying if more simulations are needed. If $\mathcal{R}$ is matched for each time-step in the given time horizon, we will return *true* as output, which expresses that the TSTL verification satisfies the reliability requirement. The output *false* is given if the requirement $\mathcal{R}$ is not matched. Therefore, we will need to carry out more simulations, performing the monitoring procedure of the formula and checking the reliability again. We observe that the proportion of *unknown* values decreases with the increase of the number of the analysed spatio-temporal trajectories. Since the width of the confidence intervals depends to a large extent on this value, by acquiring more spatio-temporal trajectories we tend to give a more precise estimation of the satisfaction probability. Therefore we provide narrower confidence intervals as input for TSTL monitoring and we have a consequent smaller proportion of unknown values. In a future version of our algorithm, we will introduce a spatio-temporal specialisation of this initial version, defining specific area of interest and specific time interval for which we want the reliability requirement to be satisfied. For example, in case of a spread of a disease, we will have specific areas of interest, e.g. hospitals, schools, for which we want a quick but accurate evaluation of the risk assessment.

Algorithm 1:
Automatic verification of the reliability specification

```
input: ψ, Σ, R
for all t ∈ T do
    for all l ∈ L do
        TSTL monitoring of ψ, location l, time t
    evaluate R
    if R false then
        return F
return T
```

5 CONCLUSIONS

In this paper we introduced the recently proposed Three-Valued Spatio-Temporal Logic and an automatic procedure to define and verify reliability requirements of the analysis results. The spatio-temporal logic TSTL was introduced to enable further analysis on the dynamics of spatial stochastic systems. Starting from the estimated satisfaction probabilities of given logical formulas, TSTL allows the study of their spatio-temporal evolution, introducing a three-valued approach to consider the intrinsic uncertainty related to the used estimation statistical method. We present an initial refinement algorithm which will be used to specify and verify the accuracy requirement for the TSTL monitoring. The requirement specifies the maximum tolerated proportion of unknown values on the spatial domain. By checking this requirement, the algorithm defines if more simulation trajectories are needed. The acquisition of more spatio-temporal trajectories will tend to give more precise monitoring results, both of SSTL properties and of the following TSTL ones but at a computational cost.

REFERENCES

[1] Axel Legay, Benoît Delahaye, and Saddek Bensalem. Statistical Model Checking: An Overview. In *Runtime Verification 2010*. 122–135.

[2] Ludovica Luisa Vissat, Michele Loreti, Laura Nenzi, Jane Hillston, and Glenn Marion. Three-Valued Spatio-Temporal Logic: a further analysis on spatio-temporal properties of stochastic systems. In *Quantitative Evaluation of Systems 2017*. 317–332.

[3] Laura Nenzi, Luca Bortolussi, Vincenzo Ciancia, Michele Loreti, and Mieke Massink. Qualitative and Quantitative Monitoring of Spatio-Temporal Properties. In *Runtime Verification 2015*. 21–37.

[4] Oded Maler and Dejan Nickovic. Monitoring Temporal Properties of Continuous Signals. In *Formal Modeling and Analysis of Timed Systems 2004*. 152–166.