Exact Monitoring of Cyber-Physical Systems Against Safety Specifications when System State is Observed Through Noisy Sensors

Robert Sheng[1], Martin Fränzle[2]

[1]Vanderbilt University, [2]Carl von Ossietzky Universität Oldenburg

Overview

Monitoring dynamic systems using imprecise measurement devices presents a significant challenge in metrology. While methods like Kalman filtering enable precise state estimation, evaluating complex safety properties expressed in temporal logics remains a largely unsolved issue when the ground-truth state is unknown. Traditional approaches of sequential state estimation followed by temporal-logic evaluation suffer from information loss, while recent interval reasoning methods also have limitations. To address this, our project explores the implementation and use of affine-arithmetic encodings. These encodings allow for more precise evaluation of temporal-logic specifications over uncertain time series, providing definite truth values for monitoring conditions in cases where previous approaches systematically fail. We hope to showcase the benefits of affine-arithmetic encodings to demonstrate their potential in enhancing the monitoring of complex safety properties in cyber-physical systems. Our research contributes to advancing metrology by enabling more accurate and reliable monitoring techniques for dynamic systems.

Objective

We seek to continuously monitor truth of a condition ϕ as a bounded time Signal Temporal Logic (STL) formula by

- implementing a STL to affine-arithmetic encodings compiler for a monitoring condition ϕ,
- deciphering the encodings for satisfiability with traditional SMT solvers, and
- decomposing per-sample error into fixed offset and per-sample error to infer determinate truth values for ϕ.

Methods

From the definitions of the Signal Temporal Logic designed in the cited works, we

1. constructed a compiler to translate bounded-time STL into SMT-LIB encodings
2. simplified these encodings using the Tseitin transformation to prevent the exponential blowup of size, and
3. produced Boolean formulas in conjunctive normal form to be solved by CNF-SAT modulo theory algorithms.

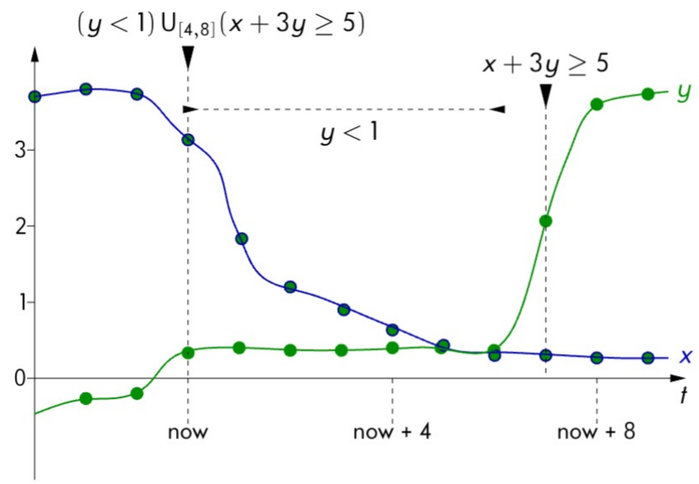
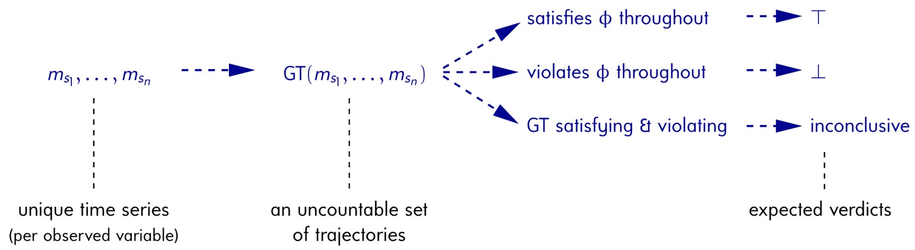


Figure: example of Signal Temporal Logic

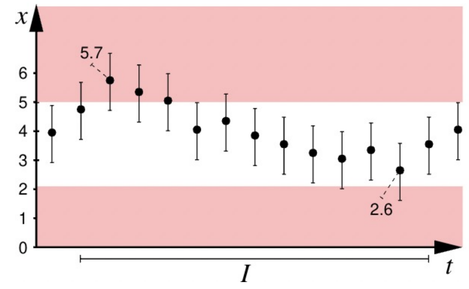
From here, we plan to characterize the possible ground truth exactly and determine the truth values of the monitoring condition ϕ across the possible ground truth, where the term “possible” is defined below.



Given a ground-truth trajectory τ, measuring a time series m_s is possible if and only if

$$\exists o \in [-\varepsilon, \varepsilon] : \forall t \in T : \exists e \in [-\delta, \delta] : \tau(s)(t) + o + e = m_s(t),$$

where T is the set of time instants where the measurements are taken.



We simplify the above equation by:

1. eliminating ∀ by specifying time domain,
2. Skolemization for quantifiers
3. interpretation as a satisfiability problem, and
4. solve affine encoding with SMT solvers.

For cases in which state estimations inherently remain inconclusive, we are now able to provide conclusive monitoring verdicts.

$$\begin{aligned}\psi = \quad & \ldots \wedge x_3 + o + e_3 = m_3 \wedge \ldots \wedge x_{12} + o + e_{12} = m_{12} \wedge \ldots \\ \wedge \quad & o, \ldots, e_3, \ldots, e_{12}, \ldots \in [-0.5, 0.5] \\ \wedge \quad & \ldots \wedge m_3 = 5.7 \wedge \ldots \wedge m_{12} = 2.6 \wedge \ldots \wedge \\ \wedge \quad & \ldots, x_3, \ldots, x_{12}, \ldots \in [2, 5]\end{aligned}$$

Discussion

In principle, this monitoring is NP-complete, although we deem NP-hardness irrelevant as it only arises with uninformative time-series. We demonstrate that the monitoring of durational properties is not equivalent to the combination of state estimation and property evaluation. Possible directions for future research may include extending our model to a stochastic model of per-sample measurement error and offset to allow for the application of work done in the areas of Kalman and Bayesian filtering to temporal logic monitoring. Another direction may include finding ways to limit the linear growth of the SMT encoding in history length when monitoring unbounded temporal properties.

References

Finkbeiner, B.; Fränzle, M.; Kohn, F.; Kröger, P. A Truly Robust Signal Temporal Logic: Monitoring Safety Properties of Interacting Cyber-Physical Systems under Uncertain Observation. *Algorithms* **2022**, *15*, 126. https://doi.org/10.3390/a15040126

Acknowledgement: This material is based upon work supported by the National Science Foundation under Grant No. 1743772.