Robustness-Guided Temporal Logic Testing for Stochastic Hybrid Systems

Houssam Abbas[(1)], Bardh Hoxha[(1)], Georgios Fainekos[(1)] and Koichi Ueda[(2)]

(1) ASU Arizona State University — CPS Lab

(2) MBD Toyota Technical Center

Sponsors: CNS 1116136, CNS 1319560, IIP-0856090 (NSF); Center for Embedded Systems, an NSF Industry/University Cooperative Research Center

Problem Formulation

Model: A Stochastic Cyber-Physical System Σ whose output is modeled as a parameterized stochastic process $Y(t, \theta)$. The parameter θ is a couple (x_0, u), where x_0 is the initial condition of the system, and u parameterizes the input signal to Σ.The randomness can be the result of sensor noise and other physical factors. All testing happens within a bounded time domain R.

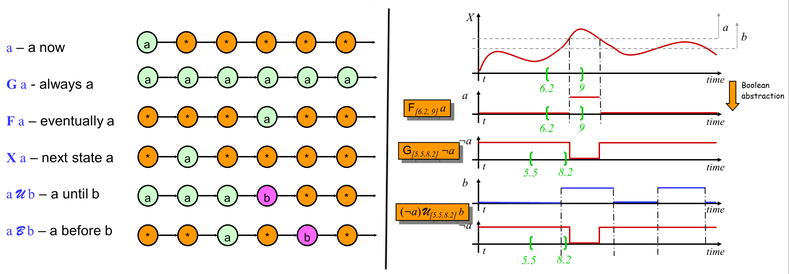
Specification: A metric temporal logic (MTL) formula ϕ that captures the system's desired behavior.

Problem: For an MTL specification ϕ, the falsification problem for SCPS consists of finding a parameter value $\theta = (x_0, u)$ of the system Σ such that, *on average*, Σ driven by θ does not satisfy specification ϕ.

Average MTL robustness

The formulas are built from a finite number of atomic propositions which label regions of interest in the state space. The propositional formulas are formed using the traditional operators of *conjunction* ($\wedge$), *disjunction* ($\vee$), *negation* ($\neg$), *implication* ($\Rightarrow$), and *equivalence* ($\Leftrightarrow$). MTL formulas are obtained from the standard propositional logic by adding temporal operators such as *eventually* ($\Diamond$), *always* ($\Box$), and *until* (U). MTL also allows timing constraints.

MTL intuition



Robustness of MTL formulae

Robustness is a functional that associates a real extended number to each sample path y of Y. A positive robustness indicates that the signal satisfies the formula, and a negative value indicates that it falsifies it.

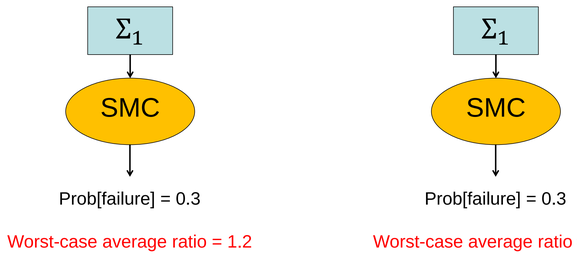
$$\rho_\varphi : y(\cdot, \omega; \theta) \mapsto \rho_\varphi(y(\cdot, \omega; \theta)) \equiv \rho_\varphi(\omega, \theta) \in [-\infty, \infty]$$

The *average* robustness $U(\theta)$ captures the average behavior of the system for that θ. We minimize $U(\theta)$ to find worst-case average behavior.

$$U(\theta) = \mathbb{E}_P[\rho_\varphi(\omega, \theta)] = \int_\Omega \rho_\varphi(\omega, \theta) dP(\omega)$$

Robustness minimization and Statistical MC

Specification: the normalized air-to-fuel ratio is always within [0.9, 1.1]



Worst-case average ratio = 1.2

Worst-case average ratio = 2.1

P. Zuliani, A. Platzer, and E. M. Clarke. Bayesian statistical model checking with application to simulink/stateflow verification, HSCC 2010

Recent examples of Automotive Recalls due to CPS Errors (2011-2012)

No downshifting from 5th to 4th under certain operating conditions

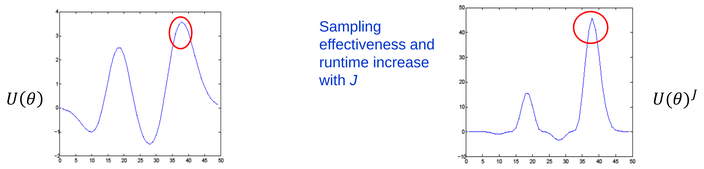
Rough idling or stalling due to complicated adaptive ECU

Cruise control does not disengage unless turning off the ignition

Minimization and guarantees

$$U_* = \inf\{U(\theta) | \theta \in \Theta\}$$

Use a variant of Simulated Annealing adapted to minimizing expectations.



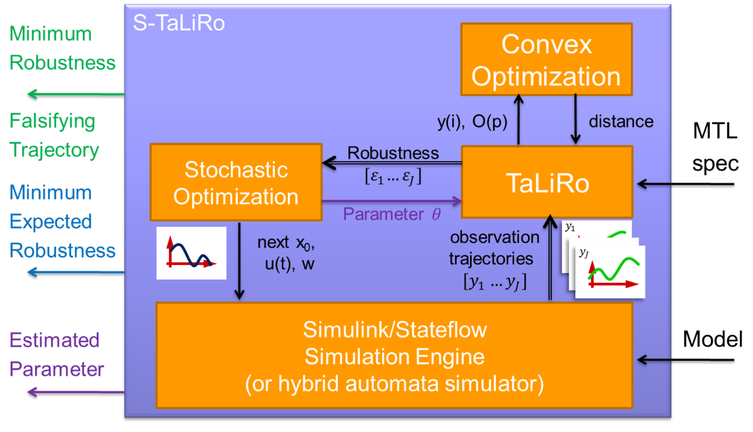
Sampling effectiveness and runtime increase with J

Example guarantee: for a given $\varepsilon > 0$ and $\delta > 0$, find number of samples s.t.

$$\Pr[|U(\theta_\varepsilon) - U(\theta_*)| < \varepsilon] > \delta$$

A. Lecchini, J. Lygeros, and J. M. Maciejowski. Stochastic optimization on continuous domains with finite-time guarantees by Markov chain Monte Carlo methods. IEEE Transactions on Automatic Control, 2010.

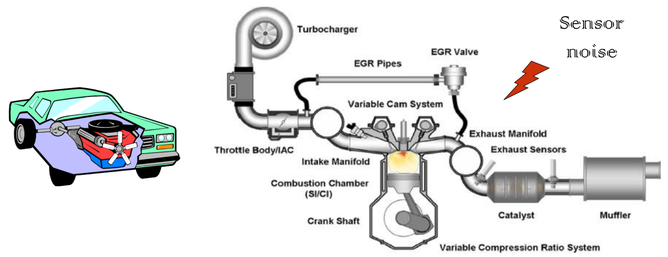
Implemented in the S-TaLiRo Toolbox



- Finding Falsifying Trajectories for Deterministic Cyber Physical Systems
- Minimum Expected Robustness for Stochastic Cyber Physical Systems
- Parameter Estimation of MTL formulas for Cyber Physical Systems

www.tinyurl.com/Staliro

High-fidelity engine model with sensor noise



56 state variables and black boxes

Modeling from physics first principles

LUTs, FSMs and regression models

SimuQuest® engine model

Find values for the parameter vector θ such that ϕ is falsified:

Formal Specification ϕ

Whenever the normalized air-to-fuel ratio is outside [0.9,1.1], it will settle back inside the range within 1 sec, and stay there for at least 1 sec.

$\phi = G_{[0,102]}(\text{OutOfBounds} \rightarrow F_{[0,1]}(G_{[0,1]}\,\text{InBounds}))$

Verification results