Poster Abstract: Getting Out of the Way – Safety Verification without Compromise

Theodore P. Pavlic, Sai Prathyusha Peddi, Paolo A.G. Sivilotti, and Bruce W. Weide
Computer Science and Engineering
The Ohio State University
Columbus, OH, USA
Email: {pavlic.3,peddi.2,sivilotti.1,weide.1}@osu.edu

***Abstract*—The intelligent transportation systems problems of adaptive cruise control and variable timing for traffic intersection signals are explored with emphasis on verification of safety properties.**

***Keywords*-verification; hybrid systems; safety; adaptive cruise control; signal coordination and timing; yellow light**

I. Introduction

Safety is often viewed as a quantity to be traded off for better performance. We look to provide safety verification approaches that enhance rather than compromise on performance. Two examples are presented here. First, we discuss verifably safe adaptive cruise control (ACC) that maintains short following distances and prescribes smooth braking trajectories. Finally, intersection signal timing is implemented with guards that maintain safety invariants. We also show how the addition of one other color may improve the performance of intersections without trading off safety.

II. Adaptive Cruise Control

Modern ACC technologies are designed to improve the comfort or safety of the driver, but no safety guarantees are asserted. Moreover, designs for ACC for convoying put emphasis on properties like string stability [1] and take safety for granted. Recent theoretical work in ACC safety verification requires discrete braking modes (i.e., any acceleration is allowed in one mode and a sufficiently large braking deceleration required in the other) and, in the case of heterogeneous vehicles, usually overly conservative separation distances to make such safety guarantees [2]. Thus, existing work both risks reducing driver comfort while also eliminating any of the performance gains typically associated with automated highways.

A. Hybrid Systems Model Checking for Safety

Rather than assuming that no information is known about the braking capabilities of adjacent vehicles, we assume that the braking class of that surrounding vehicles can be inferred. This assumption does not require sophisticated communication systems; the information may be functionally static and updated at regular service intervals. Moreover, rather than generating safety pre-conditions that are agnostic to the acceleration of the egocentric vehicle, we parameterize those pre-conditions with measured information from the vehicle. The result is an upper bound on acceleration that varies with samples of the state of the environment. So acceleration requirements vary smoothly while still guaranteeing collision-free safety in each leader–follower pair.

B. From Model Checking to Software Verification

To verify the safety of software (as opposed to behavioral models) in hybrid systems, we embed the continuous dynamics into the software specifications themselves. The result is a software paradigm consistent with Hoare's vision of a verifying compiler. Superficially sampled versions of the continuous-time dynamics are provided in the specifications within loop-like structures that induce the continuous-time dynamics. Using modest modifications to existing tools, verification conditions are generated from the annotated code that must be consistent with differential invariants [3] that are required for safety. Some of these verification conditions can be discharged by an SMT solver, and others can be discharged manually until sufficiently rich lemmas are available to the solver.

III. Signal Timing for Intersections

Using an approach similar to the ACC model checking described above, we design several novel *crossing guards* for intersection signal timing that guarantee safety while allowing for several different performance metrics. These guards are equipped with safety invariants that guarantee safety between signal decision times. We also propose that an additional light color can be added to improve traffic throughput with no impact on safety.

References

[1] R. M. Murray, "Recent research in cooperative control of multivehicle systems," *J. Dyn. Syst., Meas., Control.*, vol. 129, no. 5, pp. 571–583, 2007.

[2] S. M. Loos, A. Platzer, and L. Nistor, "Adaptive cruise control: hybrid, distributed, and now formally verified," in *Proceedings of the 17th International Symposium on Formal Methods*, ser. Lecture Notes in Computer Science, M. Butler and W. Schulte, Eds., vol. 6664, Limerick, Ireland, June 20–24, 2011, pp. 42–56.

[3] A. Platzer, *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, 2010.