Safety Verification for Automated Platoon Maneuvers: A Case Study

Ekaterina Dolginova and Nancy Lynch

MIT Laboratory for Computer Science
Cambridge, MA 02139, USA
{katya, lynch}@theory.lcs.mit.edu

Abstract. A system consisting of two platoons of vehicles on a single track, plus controllers that operate the vehicles, plus communication channels, is modeled formally, using the hybrid input/output automaton model of Lynch, Segala, Vaandrager and Weinberg [7]. A key safety requirement of such a system is formulated, namely, that the two platoons never collide at a relative velocity greater than a given bound \( v_{allow} \). Conditions on the controller of the second platoon are given, designed to ensure the safety requirement regardless of the behavior of the first platoon. The fact that these conditions suffice to ensure safety is proved. It is also proved that these conditions are “optimal”, in that any controller that does not satisfy them can cause the safety requirement to be violated. The model includes handling of communication delays and uncertainty. The proofs use composition, invariants, levels of abstraction, together with methods of mathematical analysis.

This case study is derived from the California PATH intelligent highway project, in particular, from the treatment of the platoon join maneuver in [3].

1 Introduction

Increasing highway congestion has spurred recent interest in the design of intelligent highway systems, in which cars operate under partial or total computer control. An important new effort in this area is the California PATH project (see, for example, [9]), which has developed a design for automating the operation of cars in several lanes of selected California highways. In this design, cars become organized into platoons consisting of a leader car and several following cars; the followers do not operate independently, but follow the control instructions of the leader.

An important maneuver for the proposed PATH system is the platoon join maneuver, in which two or more adjacent platoons combine to form a single platoon. The design of such a maneuver is described and analyzed in [3]. This maneuver involves both discrete and continuous behavior: discrete behavior appears in the form of synchronization and agreement among the controllers about the join process, plus communication among the various system components,
whereas continuous behavior appears in the motion of the cars. The combination forms a hybrid system of considerable complexity.

A key issue for the platoon join maneuver is its safety, represented by the requirement that cars never collide at too great a relative speed. In [3], a proof of such a safety property is outlined, for the specific platoon join maneuver given in that paper. The key to the proof turns out to be that the given maneuver always ensures that either (a) the platoons are sufficiently far apart that the second platoon can slow down sufficiently before hitting the first platoon, or (b) the relative speeds of the two platoons are already close enough.

Although the outline [3] gives the key ideas, from our point of view, it is incomplete as a safety verification. It does not include a complete model of all system components – in particular, the discrete components are not modeled. It does not seem to cover all cases that could arise: for instance, only some types of communication delay are handled, and uncertainties in the values of some parameters are not considered. The analysis contains informal “jumps” in which certain types of behavior are claimed to be the “worst possible”, and then only these cases are analyzed carefully; however, it is not made clear how one can be sure that the claimed worst cases are in fact the worst. Another problem is that the analysis is presented for just the single maneuver, and is intertwined with the proofs of other properties for that maneuver (successful join, optimality of join time). However, it seems that the analysis should be decomposable, for example, proving the safety requirement in a way that allows the proof to apply to other maneuvers besides just the platoon join.

In previous work [7], Lynch, Segala, Vaandrager and Weinberg have developed a formal model, the hybrid input/output automaton model, for hybrid systems, together with associated proof techniques. These techniques include methods based on automaton composition, on invariant assertions, on levels of abstraction, and on mathematical analysis for reasoning about continuous behavior. They have developed methods of incorporating standard methods of analysis into automaton-based proofs. So far, these methods have been used to model and verify a variety of simple real-time systems, including several very simple maneuvers arising in automated transportation systems ([11], [10], [6]).

In this case study, we apply the hybrid I/O automaton model and its associated proof methods to the task of describing and verifying safety for the PATH platoon join maneuver. This is a more complex example than those previously considered using hybrid I/O automata. We aim for an accurate, complete model of the system, plus proofs that cover all cases and accommodate all realistic variations, including delays and uncertainties. Our safety proofs should apply as generally as possible, for instance, to other maneuvers besides platoon join. Our model should also be usable for proving other properties, such as successful join and optimality. The system and its proofs should admit decomposition into separate parts, as far as possible, and should be easy to extend.

In the work we have completed so far, we have made certain simplifications. Namely, we consider the case of two platoons only (as in [3]), and we consider uncertainties in only some of the parameter values. Moreover, we pretend that