Modeling and Formal Verification of Vehicle Platooning System

Promit Panja
Dept. of Electrical and Computer Engineering
Virginia Tech
Blacksburg, United States
ppanja@vt.edu

Rakesh Kumar Bhavandlapelli
Dept. of Electrical and Computer Engineering
Virginia Tech
Blacksburg, United States
rakeshkumarb@vt.edu

***Abstract*—The operation of group of vehicles at small inter-vehicular distances, known as vehicle platooning, lowers the overall aerodynamic drag and, therefore, reduces fuel consumption and greenhouse gas emissions. But successfully implementing a vehicle platooning system in real-world requires various safety considerations. Through this project we try to study, model, and formally verify a vehicle platooning system for the follower vehicle which maintains a constant safe distance from the lead vehicle and we also incorporate communication delay between the lead vehicle and the control decision taken by the follower vehicle.**

***Index Terms*—Hybrid systems, differential dynamic logic, vehicle platoons**

I. INTRODUCTION

With the ever increasing demand for personal and public transportation there has been a steady rise in traffic congestion and other serious problems like accidents. Autonomous vehicles and smart traffic management can prove to be promising solutions for these problems. The concept of vehicle platooning, where a group of vehicles travel in close proximity with the help of advanced communication and control systems, has gained significant interest in recent years as a means to improve transportation efficiency, reduce fuel consumption and emissions, and enhance road safety. However, the development and deployment of platooning systems raise several challenges related to their reliability and safety, which can be addressed through rigorous modeling and verification techniques.

Vehicle platooning is an effective method to reduce fuel consumption and, consequently, greenhouse gas emission. Groups of vehicles with small inter-vehicular distances, reduces the aerodynamic drag experienced by the follower vehicles. This phenomenon is caused by a slipstream effect taking place behind a moving vehicle and leads to a reduced pressure on a vehicle moving at a short distance from the first one [1]. Due to this reason industries using heavy-vehicles especially the trucking industry are interested in connected autonomous vehicles to implement platooning. Driving heavy-vehicles with a short inter-vehicular distance would reduce aerodynamic drag significantly and in turn can reduce fuel consumption by up to 10% [1].

One of the crucial aspects of maintaining a safe and efficient platoon is gathering the position, velocity, and acceleration of the other vehicles in the platoon. In early days radar and other sensors were popular for collecting this data, for example in a radar guided cruise control system the vehicle uses radar and other sensors to estimate the distance and velocity of the vehicle in front to try to maintain a safe distance and a constant velocity. But such sensors are limited in their range and are affected by weather [5]. In platooning, an efficient inter-vehicle communication (IVC) protocol is required to communicate the control decisions that needs to be taken by the follower vehicles in the platoon [5]. Another important thing that needs to be kept in mind while modeling such systems is, from the communication of control messages from the lead vehicle to the follower vehicles to the actuation of the control mechanism carries significant delay and does not happen instantaneously.

There are several challenges in deploying such a system in the real-world. One of the biggest challenges is designing a safety critical *cyber-physical* system which satisfies all the above conditions and its correct functioning and reliability has been ensured. Otherwise the failure in such system can cause catastrophic damages.

Through this project we try to study such a vehicle platooning system, model it using appropriate assumptions and try to formally verify the model to ensure the model is safe under all conditions. To model such a system we use *Differential Dynamic Logic* [3], [4] and try to verify it using KeYmaera X which is an axiomatic tactical theorem prover for hybrid systems [8].

II. RELATED WORK

Vehicle platoon systems have been studied extensively previously by many different scientific communities researching not just autonomous systems and control systems but also more recently by machine learning and machine perception communities with the advent of modern deep learning techniques. We discuss related work that focuses on modeling the overall system considering the safety conditions and taking a *cyber-physical* systems approach.

Turri [1] through their thesis studied and addressed the problem of safe and fuel-efficient control for heavy-duty vehicle platooning. From experiments conducted they claim that such a platooning system can significantly reduce aerodynamic drag of the follower vehicles and can effectively reduce fuel consumption by up to 10%. They studied and modeled the control of longitudinal dynamics of a platoon with $\mathcal{N}$ vehicles which maximizes fuel-efficiency while guaranteeing safety. They propose a hierarchical control architecture which that splits this complex control problem into two layers. The layers are responsible for the fuel-optimal control based on look-ahead information on road topography and the real-time vehicle control, respectively [1].

When designing an autonomous platooning system ensuring its safety requires studying the dynamics and kinematics of the vehicles. A lot of the studies focus on modeling linear models for highway driving scenarios but in the real-world vehicle dynamics are not always linear.

Kong et al. [2] studied the kinematics and dynamics of vehicle models for autonomous driving and analyze the statistics of the forecast error using experimental data. They also design a controller for an autonomous vehicle using model predictive control (MPC). From their results by conducting experiments on a closed street at low speed, tracking of a sinusoidal path, and path following on a winding track they show the effectiveness of their proposed controller.

Loos et al. [3] modeled and formally verified multiple models of a distributed car control system in which each car in the system is controlled by adaptive cruise control for highway driving with increasing complexity. They model the systems using Quantified Differential Dynamic Logic (Qd$\mathcal{L}$) to form distributed hybrid systems to formally verify them. They take a cyber-physical systems approach and make the assumption that the cars utilize V2V and V2I communication. They first model and verify a local lane control model consisting of only two vehicles operating on a single lane and then expand this model to incorporate $\rangle$ number of vehicles operating on multiple lanes on an highway and verifying this for global highway control.

Another important aspect in vehicle platooning models is the communication framework used intra-platoon vehicle to vehicle (V2V) and inter-platoon vehicle to infrastructure (V2I). When modeling the system a communication delay needs to be incorporated as the communication of the state and the control decision are not instantaneous.

C. Hong et al. [5] through their study develop a joint systematic design of platoon communication and control to reduce position errors of consecutive vehicles to improve platoon safety based on LTE-V2V. They also present an adaptive distributed model predictive control (DMPC) based controller. From their simulation results they verify their proposed controller, and also show that their scheme performs well in vehicle failure cases where collisions can be avoided and platoon safety improved [5].

Guillermo et al. [6] in their study conducted a thorough safety assessment of networked vehicle platoon controllers using various hybrid verification tools such as PHAVer which stands for Polyhedral Hybrid Automaton Verifyer for linear hybrid systems with piecewise constant bounds on the derivatives [9], Hsolver which is based on splitting the state space in a rectangular grid and using interval arithmetic to check if the dynamic evolution of the hybrid automaton remains within the boundaries of this grid [10], and KeYmaera which is a theorem prover for differential dynamic logic (d$\mathcal{L}$), a logic for specifying and verifying properties of hybrid systems with mixed discrete and continuous dynamics. (older version of KeYmaera X) [8].

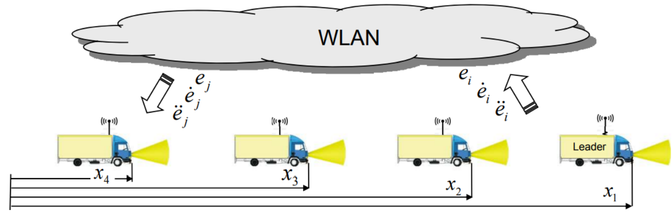

Fig. 1. Controlled Platoon of Vehicles [6].

Other studies conducted like the ones by Baskar et. al. [7] and Mitsch et. al. [4] focus on dynamic speed limit control for controlling merging on-ramp traffic and freeway traffic control respectively. These systems rely on V2I communication to control the traffic flow and do not depend on V2V communication. But both of these studies strive to improve vehicle platooning safety using their proposed techniques.

III. Platooning System Model

In this project our goal is to design and verify a vehicle platooning system for the follower vehicles. In this model the follower vehicles maintain a safe small distance with the lead vehicle. Due to the complexity of the system we divide the system into parts starting from two vehicles lead and follower model on a straight highway to extending this model to multiple vehicles.

A. Two Vehicle Highway Platoon

For this system we considered two vehicles in a platoon. Follower vehicle f is following the lead vehicle l with constant minimum distance of d between them such that at all times $x_l - x_f \geq d$. The kinematic states of the vehicles are represented by x, v, and a for position, velocity, and acceleration respectively.

The continuous dynamics of the above parameters are guided by the set differential equations $x' = v, v' = a, t' = 1$ with time component t. In order to incorporate the communication delay between the vehicles we assume a constant non-zero value δ which governs how long does it take the actuators to receive and implement a control decision. We also assume a limit for maximum acceleration of $A \geq 0$ and the braking is assumed in the range $B \geq b > 0$. In order to make the model as close to real-world as possible we assume the lead vehicle can brake and accelerate arbitrarily at any time depending on the situation i.e., the follower vehicle has no prior knowledge of the behaviour of the lead vehicle.

Based on the findings from [3] we derived the following safety condition for a two vehicle system—

$$(x_f < x_l \wedge x_l - x_f \geq d \wedge x_f + \frac{v_f^2}{2b} + (\frac{A}{b}+1)(\frac{A}{2}\delta^2 + \delta v_f) < x_l + \frac{v_l^2}{2B} \wedge v_f \geq 0 \wedge v_l \geq 0) \quad (1)$$

The above safety condition is also used a loop invariant to verify the model using formal proof rules. Below shown is the model of the two vehicle platoon system in the form of Hybrid Program using differential dynamic logic $d\mathcal{L}$.

$$hp \equiv (ctrl; dyn)^* \quad (2)$$
$$ctrl \equiv l_{ctrl} || f_{ctrl}; \quad (3)$$
$$l_{ctrl} \equiv (a_l := *; ?(-B \leq a_l \leq A)) \quad (4)$$
$$f_{ctrl} \equiv (a_f := *; ?(-B \leq a_l \leq A)) \quad (5)$$
$$\cup (?\mathbf{Safe}_\delta; a_f := *; ?(-B \leq a_l \leq A)) \quad (6)$$
$$\cup (?(v_f = 0); a_f := 0) \quad (7)$$
$$\mathbf{Safe}_\delta \equiv x_f + \frac{v_f^2}{2b} + (\frac{A}{b}+1)(\frac{A}{2}\delta^2 + \delta v_f) < x_l + \frac{v_l^2}{2B} \quad (8)$$
$$dyn \equiv (t := 0; x'_f = v_f, v'_f = a_f, x'_l = v_l, v'_l = a_l, \quad (9)$$
$$v_f \geq 0 \wedge v_l \geq 0 \wedge t \leq \delta) \quad (10)$$

Model for two vehicle highway platoon

B. Three Vehicle Highway Platoon

Although the previous two vehicle model covered most of the requirements for modeling such as dynamics and control decisions but such a system does not provide the gains that vehicle platooning claims. In real-world deployment of such a system more than two vehicles are required in order to observe any improvement in fuel-efficiency.

In this section we try to expand the model from the previous section to incorporate another follower vehicle making the total vehicles in the platoon three. We base our model from the one shown in [3] which is a *quantified hybrid program* (QHP) and is based on *quantified differential dynamic logic* Q$d\mathcal{L}$. The model in [3] shows a system of n vehicles, based on this global model we modeled our three vehicle platoon system.

Similar to previous section the kinematic states of the vehicles are represented by x, v, and a for position, velocity, and acceleration respectively. Here l is the lead vehicle and f_1 and f_2 are the two follower vehicles where f_2 follows the f_1 vehicle which in turn follows the l vehicle. The continuous dynamics of the above parameters are guided by the set differential equations $x' = v, v' = a, t' = 1$ with time component t.

The safety condition for this model is given by—

$$(x_1 < x_l \wedge x_2 < x_1 \wedge x_l - x_1 \geq d \wedge x_l - x_1 \geq d \wedge x_1 + \frac{v_1^2}{2b} + (\frac{A}{b}+1)(\frac{A}{2}\delta^2 + \delta v_1) < x_l + \frac{v_l^2}{2B} \wedge x_2 + \frac{v_2^2}{2b} + (\frac{A}{b}+1)(\frac{A}{2}\delta^2 + \delta v_2) < x_1 + \frac{v_1^2}{2B} \wedge v_1 \geq 0 \wedge \wedge v_2 \geq 0 \wedge v_l \geq 0) \quad (11)$$

The above safety condition is also used a loop invariant to verify the model using formal proof rules. Below shown is the model of the three vehicle platoon system in the form of Hybrid Program using differential dynamic logic $d\mathcal{L}$.

$$hp \equiv (ctrl; dyn)^* \quad (12)$$
$$ctrl \equiv l_{ctrl} || f_{ctrl1} || f_{ctrl2}; \quad (13)$$
$$l_{ctrl} \equiv (a_l := *; ?(-B \leq a_l \leq A)) \quad (14)$$
$$f_{ctrl1} \equiv (a_1 := *; ?(-B \leq a_l \leq A)) \quad (15)$$
$$\cup (?\mathbf{Safe}_\delta; a_1 := *; ?(-B \leq a_l \leq A)) \quad (16)$$
$$\cup (?(v_1 = 0); a_1 := 0) \quad (17)$$
$$f_{ctrl2} \equiv (a_2 := *; ?(-B \leq a_1 \leq A)) \quad (18)$$
$$\cup (?\mathbf{Safe}_\delta; a_2 := *; ?(-B \leq a_1 \leq A)) \quad (19)$$
$$\cup (?(v_2 = 0); a_2 := 0) \quad (20)$$
$$\mathbf{Safe}_\delta \equiv x_1 + \frac{v_1^2}{2b} + (\frac{A}{b}+1)(\frac{A}{2}\delta^2 + \delta v_1) < x_l + \frac{v_l^2}{2B} \quad (21)$$
$$\mathbf{Safe}_\delta \equiv x_2 + \frac{v_2^2}{2b} + (\frac{A}{b}+1)(\frac{A}{2}\delta^2 + \delta v_2) < x_1 + \frac{v_1^2}{2B} \quad (22)$$
$$dyn \equiv (t := 0; x'_2 = v_2, v'_2 = a_2, x'_1 = v_1, v'_1 = a_1, \quad (23)$$
$$x'_l = v_l, v'_l = a_l v_1 \geq 0 \wedge v_2 \geq 0 \wedge v_l \geq 0 \wedge t \leq \delta) \quad (24)$$

Model for three vehicles highway platoon

IV. Experimental Analysis

Both the two vehicle and three vehicle models discussed in the previous section were implemented as HP in KeYmaera X in order to formally verify and prove their soundness.

A. Two Vehicle Platoon Verification

For the two vehicle model we first divided the model into three parts to simplify the complexity and then ran the auto proof rule on them individually. It took quite some time to complete and required multiple runs as KeYmaera kept on crashing. Unfortunately, the model was not proven completely out of three two branches were proven successfully but the third failed to prove.

B. Three Vehicle Platoon Verification

For the three vehicle model similar to the two vehicle case we first simplified the model into three parts and then ran the auto proof rule on them individually. But similar to the two vehicle model the model was not proven completely, out the three branches two were successfully proven.

V. Conclusion and Future Work

Our aim in this project was to study, model, and formally verify a vehicle platooning system with constant inter-vehicular distance and appropriate safety conditions. We successfully modeled the vehicle dynamics and the control mechanism.

We modeled two variants of the platoon system— two vehicle and three vehicle. We verified the models by proving them in KeYmaera X but from our testing we were not able to completely verify the models. Both the models got proved partially, and ran into error.

For future work we can include non-linear motion dynamics, when the platoon has to make turns or during winding tracks as shown in [2]. Another thing that can be done is modeling the length and cross-sectional area of the vehicle to take aerodynamic drag into account through which gain in fuel-efficiency can be estimated as shown in [1]. The two models discussed above can also be improved and extended for n vehicles by using *quantified differential dynamic logic* Qd$\mathcal{L}$, as currently we do not know how to model QHP in KeYmaera X.

References

[1] Turri, V., 2015. Fuel-efficient and safe heavy-duty vehicle platooning through look-ahead control (Doctoral dissertation, KTH Royal Institute of Technology).

[2] J. Kong, M. Pfeiffer, G. Schildbach and F. Borrelli, "Kinematic and dynamic vehicle models for autonomous driving control design," 2015 IEEE Intelligent Vehicles Symposium (IV), 2015, pp. 1094-1099, doi: 10.1109/IVS.2015.7225830.

[3] Loos, S.M., Platzer, A., Nistor, L. (2011). Adaptive Cruise Control: Hybrid, Distributed, and Now Formally Verified. In: Butler, M., Schulte, W. (eds) FM 2011: Formal Methods. FM 2011. Lecture Notes in Computer Science, vol 6664. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21437-0_6

[4] S. Mitsch, S. M. Loos and A. Platzer, "Towards Formal Verification of Freeway Traffic Control," 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, Beijing, China, 2012, pp. 171-180, doi: 10.1109/ICCPS.2012.25.

[5] C. Hong et al., "A Joint Design of Platoon Communication and Control Based on LTE-V2V," in IEEE Transactions on Vehicular Technology, vol. 69, no. 12, pp. 15893-15907, Dec. 2020, doi: 10.1109/TVT.2020.3037239.

[6] Martín Guillermo, Ibtissem Ben Makhlouf, Stefan Kowalewski, Chavez Grunewald, Dirk Abel, Safety Assessment of Networked Vehicle Platoon Controllers – Practical Experiences With Available Tools, IFAC Proceedings Volumes, Volume 42, Issue 17, 2009, Pages 292-297, ISSN 1474 6670, ISBN 9783902661593, https://doi.org/10.3182/20090916-3-ES 3003.00051. (https://www.sciencedirect.com/science/article/pii/S1474667015307771)

[7] L. D. Baskar, B. De Schutter and H. Hellendoorn, "Dynamic Speed Limits and On-Ramp Metering for IVHS using Model Predictive Control," 2008 11th International IEEE Conference on Intelligent Transportation Systems, Beijing, China, 2008, pp. 821-826, doi: 10.1109/ITSC.2008.4732580.

[8] Fulton, N., Mitsch, S., Quesel, JD., Völp, M., Platzer, A. (2015). KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems. In: Felty, A., Middeldorp, A. (eds) Automated Deduction - CADE-25. CADE 2015. Lecture Notes in Computer Science(), vol 9195. Springer, Cham. https://doi.org/10.1007/978-3-319-21401-6_36

[9] Frehse, G. PHAVer: algorithmic verification of hybrid systems past HyTech. Int J Softw Tools Technol Transf 10, 263–279 (2008). https://doi.org/10.1007/s10009-007-0062-x

[10] Ratschan, S. and She, Z. (2007). Safety verification of hybrid systems by constraint propagation based abstraction refinement. ACM Transactions in Embedded Computing Systems, 6(1).