Hierarchical Approach for Safety of Multiple Cooperating Vehicles

Jain, Varun; Heß, Daniel; Löper, Christian; Frankiewicz, Tobias; Hesse, Tobias

DLR/Institute of Transportation Systems

Lilienthalplatz 7, 38108 Braunschweig, +49 531 295 2035,

Varun.Jain@DLR.de

Abstract

In this paper we present a hierarchical structure consisting of offline and online verification, ensuring the safety properties of cooperating vehicles; communicating either implicitly (e.g.: vehicle on left lane slowly opens gap, indicating the vehicle on right lane to merge in front of it) or explicitly via Car-to-Car communication with each other.

The offline verification is based on the concept of reachability analysis of hybrid systems and aims at building formally correct and safe cooperative maneuvers for a group of vehicles.

The online verification layer has the task of negotiating the possible cooperative maneuvers with other traffic participants and send the selected optimal plan to a low-level tube based Model Predictive Control (MPC). The MPC then calculates the control inputs to be applied to the actuators in order to guide the vehicle safely under the presence of model uncertainty and disturbance. In case MPC offers no feasible solution to the constraint optimization problem i.e. there occurs a constraint violation during the prediction horizon, the safety of the cooperative maneuver is ensured by an emergency planner, which aborts the current cooperative maneuver and brings the vehicle to safe state. The effectiveness and the performance of the hierarchical concept presented here are shown with an exemplary cooperative lane change scenario involving multiple vehicles.

Appeared in: ITS automotive nord e.V. (Hrsg.) AAET - Automatisiertes und vernetztes Fahren, Beiträge zum gleichnamigen 18. Braunschweiger Symposium vom 8. und 9. Februar 2017. ISBN: 978-3-937655-41-3

1. Motivation

Safety and reliability of automated road vehicles are one of the most important aspects for the introduction of such systems into the market and its acceptance by the road users. Simulation-based verification methods such as Monte-Carlo simulations, suffer from the drawback that a very large number of tests need to be performed for proving the safety of such systems. The problem at hand is escalated even further when automated vehicles need to cooperate with other communicating and non-communicating, automated or manually driven vehicles for example to avoid collisions or to increase the efficiency of traffic flow.

Formal verification methods through its rigorous mathematical specification can provide guarantees for the safe and reliable behavior of automated vehicles, thus requiring a smaller number of tests and increased safety and reliability of automated vehicles. The work presented here focuses on the formal methods of reachability analysis of continuous and hybrid systems. In order to overcome the problem of real-time implementation of the formal methods of reachability analysis, a hierarchical structure including offline and online modules has been selected for the tasks of cooperative maneuver planning and execution respectively. The hierarchical structure has the advantage that the time consuming task of maneuver planning can be done offline for various initial conditions (e.g.: state of the vehicle, number of vehicles, number of lanes etc.). These offline computed cooperative maneuvers are stored in a Cooperative Maneuver Database (CMD), along with the information about the cooperating participants, cost of maneuver etc. and are available for the online verification layer. The online verification layer negotiates these cooperative maneuvers with other vehicles via Car-to-Car communications. A cost optimized safe cooperative maneuver for the group, defining the role of each participant in the maneuver is selected based on the decision by other cooperating partners. The cooperative maneuver selected by the online verification layer provides constraints for the tube based MPC that are tightened based on the current disturbances and prediction of other non-cooperating traffic partners. The output from the tube based MPC is then applied to the actuators to guide the vehicle safely.

In order to aid the understanding of the upcoming sections and to show the effectiveness of the approach, simulation scenario

involving cooperative lane change as shown in Figure 1 has been used. The presented scenario shall be used as a reference in the upcoming sections.

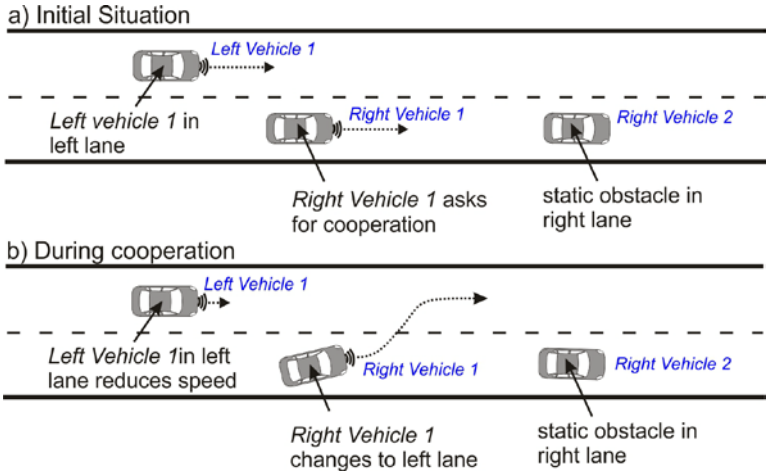

Figure 1: simulation scenario initially and during cooperation

The paper is structured as follows: the next section presents the state of the art of formal safety guarantees in automated driving and the concepts of reachability analysis and tube based MPC used in this paper. Section 3 presents the hierarchical structure. Section 4 along with its subsections presents the concept of Cooperative Maneuver Automata and Tube based MPC used in this work. Section 5 presents the simulation scenario and results of the simulation. The paper closes with a short conclusion and future work.

2. State of the art

Despite an extensive advancement in the field of automated driving, the formal safety guarantees of automated driving is still an open area of research. Formal verification techniques such as theorem proving [16], barrier certificates [17] and reachability analysis [18] have found their application in verification of robotic systems and automated cars, but only some of the aspects are considered. In [19] theorem proving is used to verify the automatic cruise control system under the assumption of automated vehicles. The same concept has also been used in [20] for obstacle avoidance scenario for mobile

robots. The concepts of reachability analysis of continuous systems in the form of tube based MPC have also been applied for computation of the safe or hazardous states for mobile robots in an unknown environment [1] [4]. The concepts of reachability analysis have been used in [21] [22] for verifying the maneuvers of a quadcopter. Although limited to only one vehicle, the concepts of reachability analysis have also been used in verification of automated driving, where the offline created maneuver automata is used for collision avoidance of road vehicles [8] [15].

The formal verification of cooperative driving (i.e. cooperative maneuver planning) including multiple vehicles on the other hand is still an untouched area of research. In this we work we extend the applications of reachability analysis of hybrid system for cooperative maneuver planning, with an aim to formally verify the correctness and safety of cooperative maneuvers.

The simultaneous advances in the algorithms for computation of exact reachable sets for hybrid system with linear or piece-wise constant derivatives [6] [14] have made the use of these concepts possible. The advances in the tools such as SpaceEx [3], MPT [2], Flow* [11] etc. for computation of reachable sets represented as zonotopes, ellipsoids [12] and support functions [11] have also greatly reduced the computation time [6], thereby allowing the use of these concepts for formal safety guarantees for a group of vehicles.

3. System overview

In order to ease the task of cooperative maneuver planning involving multiple vehicles and at the same time providing formal safety guarantees for a group of vehicles, a hierarchical structure using the concept of reachability analysis of hybrid and continuous systems has been proposed as shown in Figure 2. The hierarchical system architecture consists of an offline and an online verification layer for the creation and execution of the cooperative maneuvers in the presence of disturbance and uncertainty. A cooperative maneuver is a set of trajectories of cooperating vehicles that is formally correct and safe i.e. avoids collision between traffic participants.

The offline verification layer has the purpose of creating a database of such cooperative maneuvers for different initial conditions such as relative distance, velocity, number of participating vehicles etc. The

cooperative maneuvers are computed based on the reachability analysis of the Cooperative Maneuver Automata (hybrid system) and are stored in a Cooperative Maneuver Database (CMD) along with the information about cooperating vehicles, cost of the maneuver etc. The cooperative maneuvers stored offline in CMD are selected by the online decision layer i.e. Cooperative Maneuver Planner based on the vehicle state, environment and cooperation by other vehicles and are communicated to each of the vehicle over C2C communication. Based on the decision of the explicitly via C2C communication communicating vehicles to either accept or decline the proposal, the cooperative maneuver is either performed or aborted.

As depicted in Figure 2, the decision about the cooperative maneuver to be executed by a group of vehicles is made by the Cooperative Maneuver Planner based on the availability/cost of the maneuver and acceptance or rejection of the cooperative maneuver by other traffic participants. Here it should be noted that cooperative maneuver planning is initiated by the vehicle requiring cooperation. In case of a vehicle initiating the cooperation, the maneuvers are selected from CMD and in case of participating vehicles; the maneuver is obtained as a proposal over C2C communications.

The selected cost optimal maneuver along with the upper and lower limits of the vehicle states (the set representation provides upper and lower limits for the vehicle states) are then passed onto the tube based MPC layer for the calculation of the control inputs that ensure the vehicle state lies within the limits. Since the tube based MPC uses a vehicle model that cannot exactly describe the real vehicle's behavior, the uncertainty in the model determined using the vehicle conformance tests is used to tighten the constraints for the MPC formulation (section 4.2). The control output is sent to the actuators and applied to the vehicle. The predictive nature of the tube based MPC used here, helps to identify if a collision can occur in future under the presence of disturbance and uncertainty and thus abort the current cooperative maneuver and apply the emergency maneuver. The sensors/observers block provides the Cooperative Maneuver Planner information about the state of other vehicles such as relative distance and velocity etc. In each iteration of the hierarchical structure the Cooperative Maneuver Planner uses this information to verify if the states of participating vehicles are inside a

safe state-space set of the cooperative maneuver. The cooperative maneuver is aborted if any of the vehicles leaves the communicated safe regions.

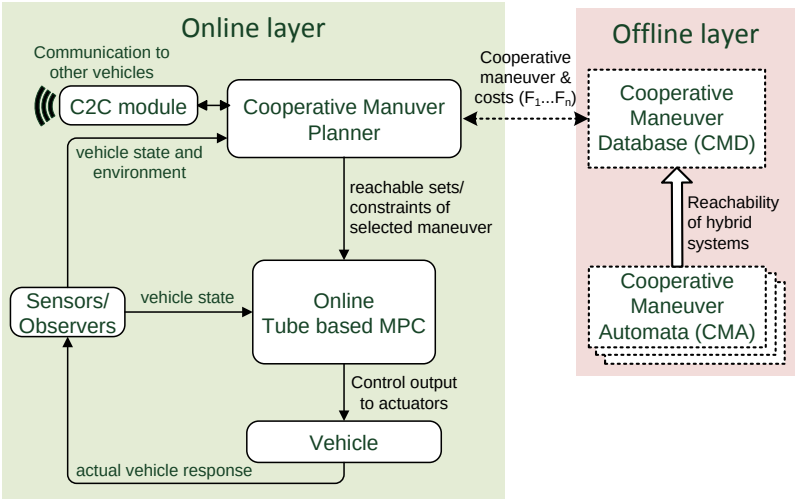

Figure 2: hierarchical structure used for the cooperative planning

Additionally in order to consider the cooperation by the vehicles communicating implicitly (e.g.: vehicle on left lane slowly opens gap, indicating the vehicle on right lane to merge in front of it), the allowed regions for such vehicles is also determined using the Cooperative Maneuver Automata, as described in the next section. The Cooperative Maneuver Planner then monitors/checks if the state i.e. the position and velocity of the vehicle lies within these defined safe regions or reachable sets. The cooperative maneuver is aborted in case the vehicle leaves the anticipated safe region. This approach has the advantage that the amount of conservativeness in selection of the cooperative maneuvers can be reduced since non-communicating vehicles can also be included in cooperation.

4. Detailed concept

The following subsections aims at explaining the important modules of the presented hierarchical structure i.e. Cooperative Maneuver Automata which generates the Cooperative Maneuver Database and Tube based MPC that have been extensively used in this work.

These modules are based on the concepts of reachability of hybrid and continuous systems respectively.

4.1 Cooperative Maneuver Automata (CMA) as hybrid automata

The CMA presented in this section is used for the offline computation of the CMD. The CMA is modelled as a hybrid automaton (*pl.* automata) and an example CMA for the cooperative lane change scenario of Figure 1(a) is shown in Figure 3. It has the representation of the form: *H= (Loc, Var, Lab, Inv, Flow, Trans, Init)* and has discrete states *Loc* called locations, each of the discrete locations is associated with an invariant (*Inv*) which defines the boundaries of each location and a *Flow* that defines the time-driven evolution of continuous variables *Var*. A set of discrete transitions *Trans* defines how the system jumps from one location to another and instantaneously modifies the values of continuous variables (shown as assignments in Figure 3). The behavior of the system originates from the initial states *Init* [5]. It should be noted that Figure 3 depicts only an example CMA, involving some of the maneuvers; other maneuvers such as follow vehicle in front, turn right and turn left etc. can also be used for modelling of CMA.

As explained above, each participating vehicle is modelled as a hybrid automaton i.e. each of them has an initial state and a set of locations and discrete transitions between them as shown in Figure 3. The locations define the maneuvers such as follow lane, change lane, open gap etc., flow defines the equations of motion of vehicle in these locations and guards determine the possibility to change from one location to another. For example: a transition from “FollowRightLane” to “EmergencyManeuver” is only possible when the distance to vehicle in front is smaller than the threshold. The assignments on the transitions are used to modify the set or reference points for vehicle velocity and lateral position in the lane. The states of the vehicle used in the CMA depend upon the choice of the vehicle model and as shown in Figure 3: distance travelled, velocity, lateral position in the lane, lateral velocity with respect to the right lane, desired longitudinal velocity and desired lateral position in the lane have used for vehicle modelling. The reachability analysis of this system shall compute all the possible reachable sets for the vehicle starting in one maneuver, evolving over time and switching to other maneuvers.

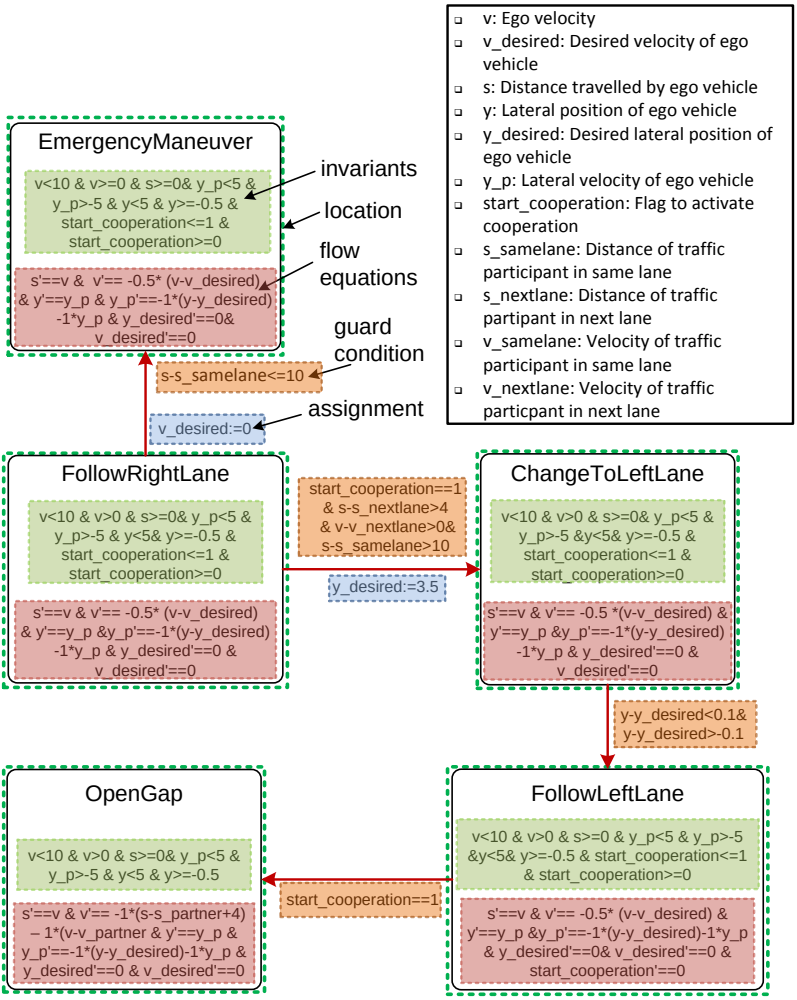

Figure 3: example maneuver automata for a vehicle

The important steps for reachability analysis of such a hybrid system are shown below. The interested reader is referred to [14] for details.

- Defining the initial state X_0 for the system. The initial state comprises of the values for the vehicle state e.g.: v, v_desired etc. and initial location e.g.: FollowRightLane, OpenGap etc.

- Computation of reachable sets starting from an initial state X_0 through continuous time operator. The continuous time operator refers to the flow equations in a location.
- Computation of the reachable state after discrete transition from one location to another.

Since the task of the CMA is to generate cooperative maneuvers that are safe i.e. avoids collision between traffic participants, the states of all the participating vehicles such as distance, velocity etc. have been used as guard conditions. Thus these guards allow the vehicle to switch from one maneuver to another only when no collision between participants occurs. One such example is to allow the lane change to left (from "FolowRightLane" to "ChangetoLeftLane") only when the vehicle in the right lane is faster than vehicle in left lane and has a distance large enough to avoid collision. The guard conditions thus ensure that the safety properties are fulfilled. But since the vehicle states of each of the participating vehicle continuously evolves as per the flow equations, the reachability analysis of all the participating vehicles needs to be performed in parallel. Figure 4 shows three instances of maneuver automata for a vehicle (of Figure 3) and the connections between the vehicles states modelled in the tool SpaceEx [3]. In SpaceEx representation, each of these instances are known as *base components*, connected together to form a *network component* (Figure 4).

The reachable sets for distance and velocity of *Right Vehicle 1* starting in location "FollowRightLane" and making a transition either to "EmergencyManeuver" or "ChangeToLeftLane" is shown in Figure 5. In case of transition to "ChangeToLeftLane", the vehicle continues to move forward and thus the reachable sets also evolve over time. In case of transition to "EmergenvyManeuver" the vehicle comes to stop and thus the reachable sets for distance do finally not change over time.

A cooperative maneuver is made up of such reachable sets for all of the participating vehicles. In order to obtain a CMD with possibly large safe or allowed regions of movement of the participating vehicles, the reachability analysis is performed with different initial conditions and different number of participating vehicles. The reachable sets thus obtained are stored in a CMD together with the information about number of participating vehicles, cost of the

maneuver, which is further calculated based on the vehicle accelerations, distance between vehicles etc.

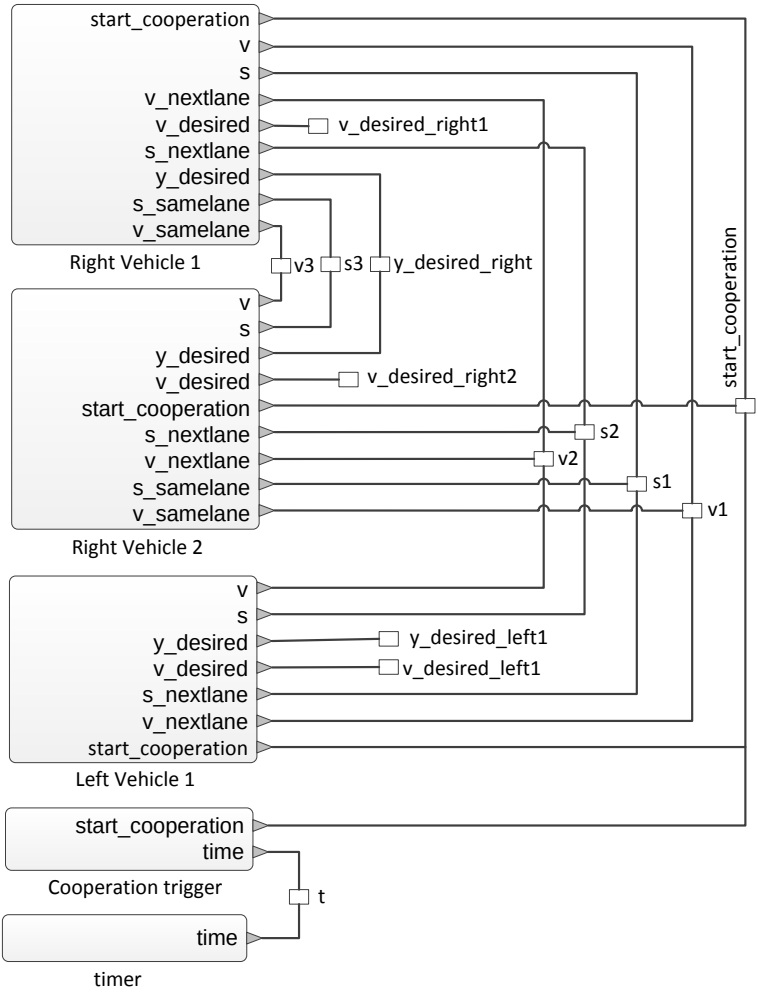

Figure 4: example maneuver automata for a vehicle

During the online phase, the Cooperative Maneuver Planner checks for feasible cooperative maneuvers based on the state i.e. the relative distance and relative velocity of other traffic participants. A cost optimal i.e. a cooperative maneuver with minimum total

acceleration is selected. The selected maneuver is then negotiated with other participants via C2C communication.

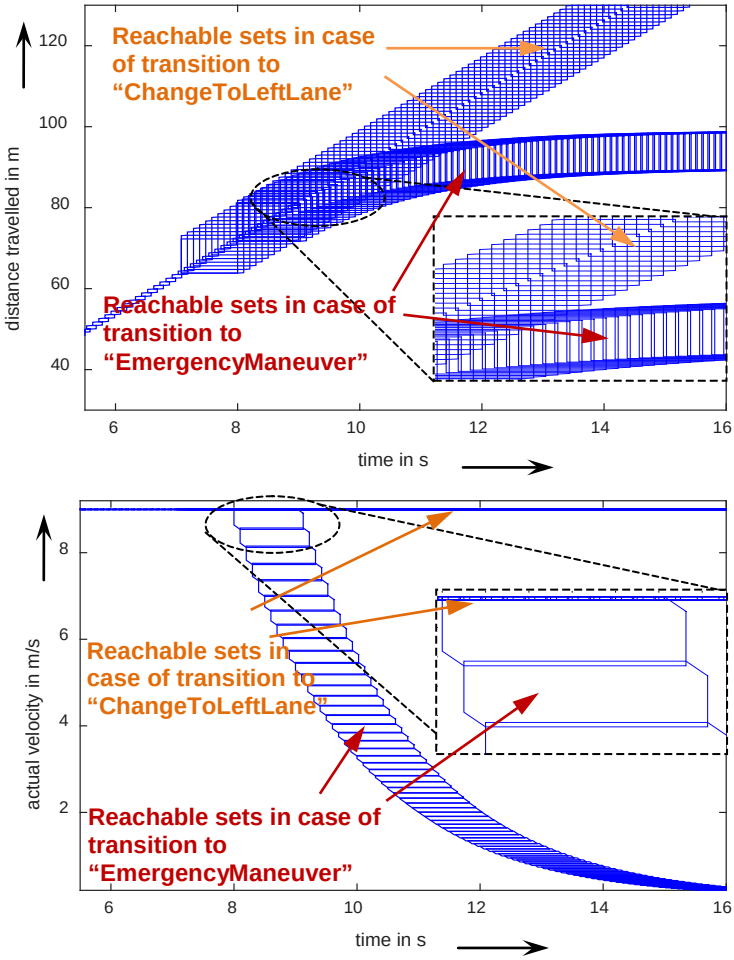

Figure 5: reachable sets for some of the vehicle states

The participating vehicles can either accept or decline the cooperative maneuver based on their vehicle's state, goals and ability to cooperate (e.g.: vehicle already in cooperation with another group). In case a maneuver is selected for cooperation, the

reachable sets of this maneuver is also sent to online tube based MPC for calculation of the control inputs under the presence of uncertainty and disturbance.

4.2 Tube based MPC

In this section we present the online tube based MPC that calculates the control inputs to actuators in order to maintain the vehicle trajectory within the upper and lower limits of the selected optimal maneuver. The reachable sets obtained from the Cooperative Maneuver Planner act as upper and lower limits for the MPC problem. But since the vehicle model used for the MPC formulation cannot exactly describe the vehicle behavior, the uncertainty and disturbance needs to be explicitly considered for safety guarantees.

In order to explicitly consider the uncertainty in the vehicle model, the maximum deviation between the vehicle model used in MPC and the actual vehicle (also denoted as difference between nominal system and actual system) i.e. the error model is determined. Since it is desired that the deviation in the error model converges to zero, a local stabilizing control law is used. The deviation of this closed-loop error system is determined by the calculation of the continuous reachable sets with additive disturbance for the entire prediction horizon of MPC. The amount of uncertainty in the error model shall be determined with the difference between the real vehicle measurements and the MPC model for a set of standard maneuvers. The reachable sets determined are then subtracted from the reachable sets of cooperative maneuver to obtain the tightened upper and lower limits as shown in Figure 6.

The consideration of uncertainty/disturbance and data flow inside the tube based MPC is explained with Figure 7 and can be summarized as follows:

1. First a local stabilizing control law (K_s) is determined for minimizing the deviation of error model.
2. Reachable sets having following characteristics are calculated:
    - Reachable sets are calculated for closed loop error system (including local stabilizing control K_s)
    - Reachable sets are calculated online for length of prediction horizon H_p
    - Reachable sets are calculated through flow equations of the error model and represented as polytopes in this work.

3. Reachable sets are then subtracted from reachable sets of CMA (selected plan)
4. Tightened constraints are used for MPC formulation and calculation of control input u_N
5. Total control input ($u_s + u_N$) is applied to the vehicle actuators

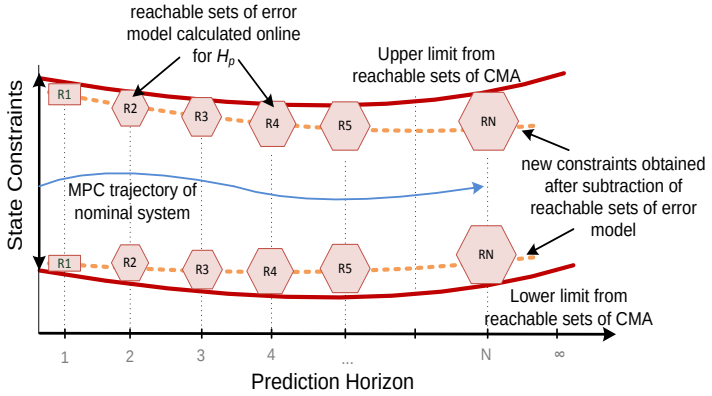

Figure 6: tube based MPC concept

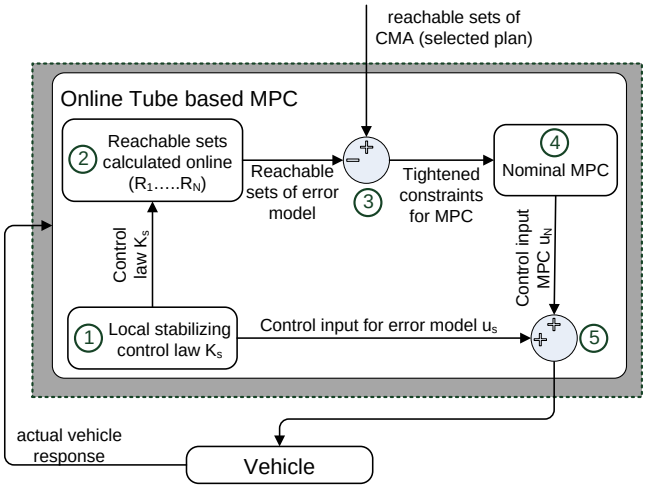

Figure 7: data flow inside the tube based MPC

Since the MPC problem ensures that the constraints are satisfied for the entire prediction horizon, a non-feasible solution due to constraint

violation leads to aborting of cooperative maneuver. In case the cooperative maneuver is aborted, an emergency planner brings the vehicle to safe state e.g.: vehicle brakes to standstill in its own lane. The interested reader is referred to [8] for more details.

The implementation of the tube based MPC including the calculation of the online reachable sets and the nominal MPC formulation was done using the Multi-Parametric Toolbox (MPT) [2] and YALMIP solver [7] in MATLAB [9]. A simple vehicle model with point mass was used for the MPC formulation. The reachable sets of CMA computed with the tool SpaceEx were imported in MATLAB [9] and made available to tube based MPC manually.

The next section presents the simulation results for an example scenario involving cooperative lane change as shown in Figure 1.

5. Simulation Results

In this section we present the simulation results for a cooperative lane change scenario using the previously presented hierarchical structure. The scenario used for the simulation is shown in Figure 1, as can be seen in the figure, during the initial situation *Right Vehicle 1* on right lane requests for cooperation per C2C communication in order to avoid the collision with *Right Vehicle 2* in its lane.

Here it should be noted that since this work focuses on the detailed concept of CMA and tube based MPC, the Cooperative Maneuver Planner was not modelled for the simulation purposes. The cost optimal cooperative maneuver was therefore selected manually and made available to the tube based MPC for calculation of control inputs. In order to show the effectiveness of the approach in case of model uncertainty/disturbance (between MPC vehicle model and simulation model), a linear bicycle model with random additive disturbance was used for the simulation.

As is evident from the Figure 1(a), in order to avoid the static obstacle in the right lane (*Right Vehicle 2*), *Right Vehicle 1* can either brake and reach standstill or can perform a lane change and continue to move with the same velocity. The Figure 8 shows the reachable sets for distance, velocity, and lateral deviation of *Right Vehicle 1* having two possible cooperative maneuvers (Maneuver 1: transition to “ChangeToLeftLane” and Maneuver 2: transition to

"EmergencyManeuver"). It should be noted that amount of safety distance between the two vehicles was defined during the modelling of CMA along with other safety properties.

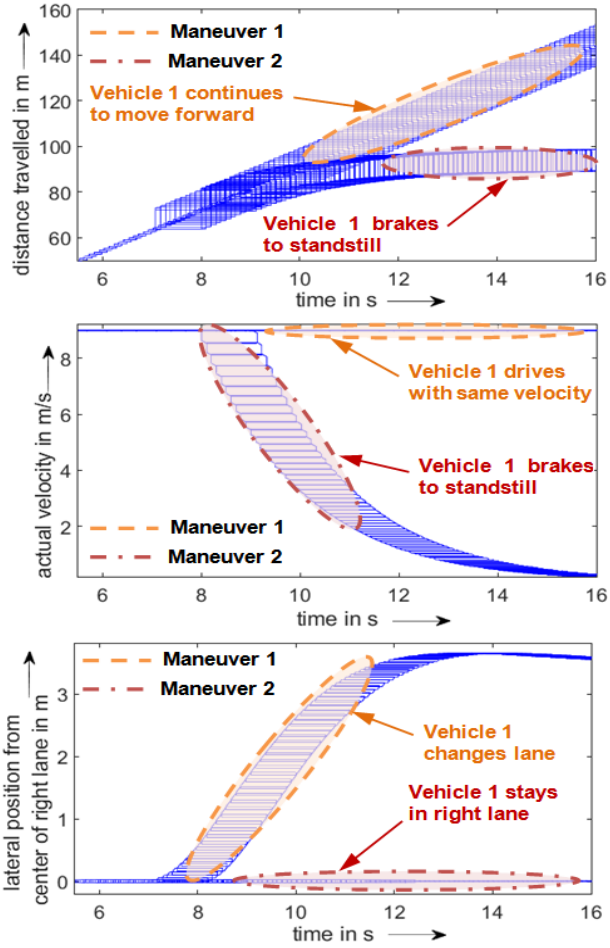

Figure 8: possible maneuvers for *Right Vehicle 1* to avoid a collision

For the simulation purpose the lane change maneuver by *Right Vehicle 1* has been selected as the possible cooperative maneuver. The scenario during the cooperation can be seen in Figure 1(b). Figure 9 shows the actual velocity and lateral deviation from the

center of the right lane (center of right lane as zero) for *Right Vehicle 1* and Figure 10 shows the actual velocity and distance travelled by *Left Vehicle 1*. As can be seen in the figures, during the cooperative maneuver the *Left Vehicle 1* first reduces its speed (at 5sec). After a large enough gap has been created the lane change maneuver by *Right Vehicle 1* is started (at 8sec, see Figure 9). After that *Left Vehicle 1* accelerates again to reach its desired velocity set point of 9m/s.

Additionally as seen in Figure 9 the upper and lower MPC constraints for velocity overlap with the boundaries of the reachable sets from CMA, this is because the amount of uncertainty along longitudinal direction is modelled to be small. But in case of lateral distance from right lane, the reachable sets of error model are large and thus the upper/lower MPC constraints lie within the reachable sets from CMA. Also in Figure 10, the upper and lower MPC constraints overlap with reachable sets from CMA (because the uncertainty along longitudinal direction is small). In both the figures the actual state of vehicle satisfies the MPC constraints.

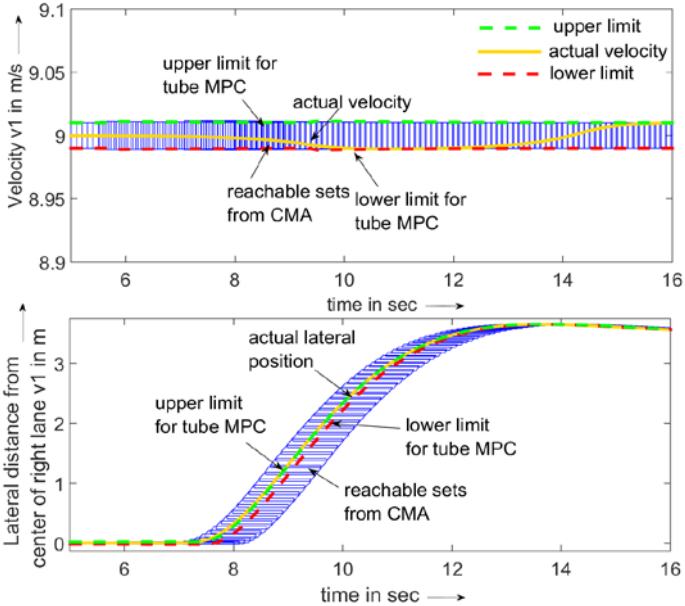

Figure 9: plots depicting the velocity and lateral distance from center of right lane for *Right Vehicle 1*

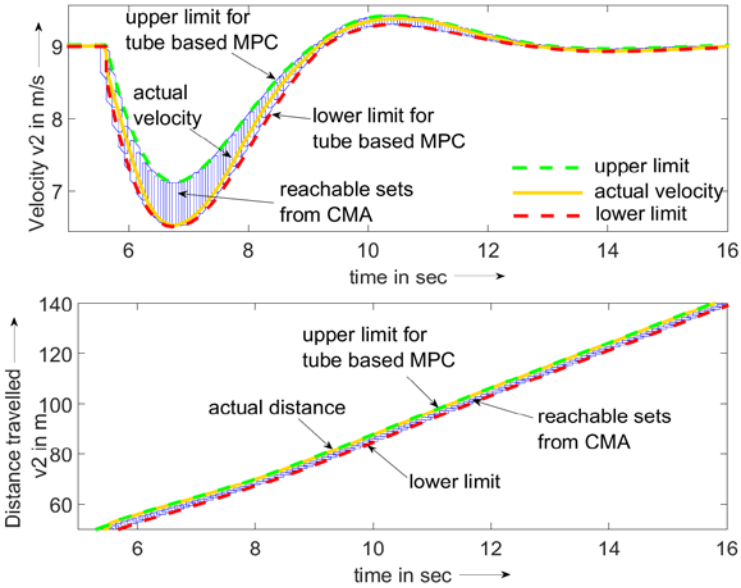

Figure 10: plots for velocity and distance travelled by *Left Vehicle 1*

The results provide formal safety guarantees for planning and execution of the cooperative maneuvers under specific amount of uncertainty. It should be noted that the maximum amount of uncertainty or disturbance that can considered is limited, since a large uncertainty in the model can lead to large reachable sets for error model and thus small regions within the upper and lower MPC constraints.

6. Conclusion and outlook

In this paper we presented a hierarchical structure using formal methods of reachability analysis for planning and execution of cooperative maneuvers. The simulation results for a cooperative lane change scenario involving three vehicles show the effectiveness of the approach. Since the maneuver planning and execution are done independently, the CMD can be extended to include additional cooperative scenarios without necessitating any changes in lower level control. The future work focuses on efficient design of CMA (and CMD) for generation of several cooperative maneuvers resembling the real life cooperation scenarios. The future work also focuses on the use of efficient set representation such as ellipsoids

etc. for the tube based MPC in order to deal with issue of real-time implementation in vehicle and demonstrate the proposed idea with field tests.

7. Acknowledgements

The authors greatly acknowledge the financial support by Deutsche Forschungsgemeinschaft (DFG) for the project CoInCiDE under grant number 623093.

References

[1] R. Gonzalez, M. Fiacchini, T. Alamo, J.L. Guzman & F. Rodriguez, „Online robust tube-based MPC for time-varying systems: a practical approach," *International Journal of Control,* pp. 84:6, 1157-1170, 2011.

[2] M. Herceg, M. Kvasnica, C.N. Jones, and M. Morari, „Multi-Parametric Toolbox 3.0," *In Proc. of the European Control Conference,* pp. 502-510, 17-19 July 2013.

[3] Goran Frehse, Colas Le Guernic, Alexandre Donzé, Scott Cotton, Rajarshi Ray, Olivier Lebeltel, Rodolfo Ripado, Antoine Girard, Thao Dang, Oded Maler, „SpaceEx: Scalable Verification of Hybrid Systems," in *Proc. 23rd International Conference on Computer Aided Verification (CAV)*, 2011.

[4] Ramón Gonzáleza, Mirko Fiacchinib, José Luis Guzmána, Teodoro Álamoc, Francisco Rodrígueza,, „Robust tube-based predictive control for mobile robots in off-road conditions," *Robotics and Autonomous Systems,* pp. 711-726, 2011.

[5] T. A. Henzinger, „The theory of hybrid automata," in *IEEE Symp. Logic in Computer Science*, 1996.

[6] Colas Le Guernic and Antoine Girard, „Reachability analysis of hybrid systems using support functions," in *In Ahmed Bouajjani and Oded Maler, editors*, 2009.

[7] J. Lofberg, „YALMIP : A Toolbox for Modeling and Optimization in MATLAB," in *In Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[8] Heß, Daniel; Löper, Christian; Hesse, Tobias, „Safe Cooperation of Automated Vehicles," in *18. Braunschweiger Symposium: AAET 2017, Automatisiertes & Vernetztes Fahren*, Braunschweig, 2017.

[9] MATLAB 2015a, Natick, Massachusetts: The MathWorks Inc., 2015.

[10] Yiqi Gao, Andrew Gray, H. Eric Tseng & Francesco Borrelli, „A tube based robust nonlinear predictive control approach to semiautonomous ground vehicles," *Vehicle System Dynamics: International Journal of Vehicle Mechanics and Mobility,* pp. 52:6, 802-823, DOI: 10.1080/00423114.2014.902537, 2014.

[11] S. Boyd and L. Vandenberghe, Convex optimization, Cambridge University Press, 2004.

[12] A. B. Kurzhanski and P. Varaiya, „Ellipsoidal techniques for reachability analysis," in *in HSCC'00, vol. 1790 in LNCS*, 2000.

[13] X. Chen, E. Abraham, and S. Sankaranarayanan, „Flow*: An analyser for non-linear hybrid systems.," in *E. Abraham, and S. Sankaranarayanan. Flow*: An analyser for non-linear hybrid systems. In Proceedings of the 25th International Conference on Computer Aided Verification (CAV'13), volume 8044 of Lecture Notes in Computer Science*, 2013.

[14] Goran Frehse and Rajarshi Ray, „"Flowpipe-Guard Intersection for Reachability Computations with Support Functions," in *4th IFAC Conference on Analysis and Design of Hybrid Systems*, 2012.

[15] Heß, Daniel, Matthias Althoff, and Thomas Sattel, „Formal verification of manoeuvre automata for parameterized motion primitives," IEEE/RSJ International Conference on Intelligent Robots and Systems, 2014.

[16] A. Platzer, Logical Analysis of Hybrid Systems: Proving Theorems for, Springer, ISBN 978-3-642-14508-7, 2010.

[17] S. Prajna, „Barrier certificates for nonlinear model validation," *Automatica,* pp. 117-126, 2006.

[18] E. Asarin, T. Dang, G. Frehse, A. Girard, C. Le Guernic, and O. Maler, „Recent progress in continuous and hybrid reachability analysis," *In Proc. of the 2006 IEEE Conference on Computer Aided Control Systems Design,* pp. 1582-1587, 2006.

[19] S. M. Loos, D. Witmer, P. Steenkiste, and A. Platzer, „Efficiency analysis of formally verified adaptive cruise controllers," *In Proc. of the 16th International IEEE Conference on Intelligent Transportation Systems,* pp. 1565-1570, 2013.

[20] S. Mitsch, K. Ghorbal, and A. Platzer, „On provably safe

obstacle avoidance for autonomous robotic ground vehicles," *In Proc. of Robotics: Science and Systems IX,* 2013.

[21] J. Ding, E. Li, H. Huang, and C. J. Tomlin., „Reachability-based synthesis of feedback policies for motion planning under bounded disturbances," *In Robotics and Automation (ICRA), 2011 IEEE International Conference,* pp. 2160-2165, 2011.

[22] J. H. Gillula, H. Huang, M. P. Vitus, and C. J. Tomlin, „Design of guaranteed safe maneuvers using reachable sets: Autonomous quadrotor aerobatics in theory and practice," *In IEEE International Conference on Robotics and Automation,* pp. 1649-1654, 2010.