Dependability modeling and evaluation of an automated highway system

Ossama Hamouda, Mohamed Kaâniche, Karama Kanoun

Dependability Modeling and Evaluation of an Automated Highway System

Ossama Hamouda, Mohamed Kaâniche, and Karama Kanoun
LAAS-CNRS; Université de Toulouse, 7, Avenue du Colonel Roche, F-31077 Toulouse, France
{firstname.lastname}@laas.fr

1. Introduction

Traffic congestion is increasingly growing, especially in urban areas. One of the solutions for this problem is automated traffic. Many research programs have been carried out or are currently underway to implement automated road or highway systems, based on automatically controlled platoons of vehicles. The aim is to improve the flow and the safety of traffic by reducing accidents, while reducing fuel consumption and pollution [1].

Automatic collaborative driving systems make use of inter-vehicles or vehicles-to-fixed infrastructure communications to autonomously guide cooperative vehicles on an Automated Highway System, e.g., for the aim of sharing the necessary information to ensure safe driving. The expected gains from automatic driving are the target of many research studies in this domain. However, to the best of our knowledge there was no previous work dedicated particularly to the dependability modeling and evaluation of such systems.

2. Context and Objectives

We address the evaluation of quantitative measures for characterizing the dependability in the context of the Automated Highway System, based on platoons in which vehicles are driven by more or less autonomous agents, interacting in a multi-agent environment [1]. Our work aims at developing evaluation methods and models that make it possible to analyze the safety of such platooning applications implemented in a mobile context with ad-hoc networks. Several phenomena such as accidental faults occurrence, vehicles mobility, frequent communication disconnection, are taken into consideration. This problem is challenging in the domain of automated highway applications and systems implemented in ad-hoc networks.

The developed models and measures are aimed at providing support to the designers for the selection and analysis of candidate architectures that are well suited to fulfill the dependability requirements of such a system. We consider as a case study the architectures developed in the framework of a project of intelligent transport systems (*Partners for Advanced Transit and Highways* "PATH" [2]), at Berkeley University. These architectures implement automatic maneuvers to ensure the platoons safety in the presence of different types of failure modes affecting the vehicles, their environment, and the inter-vehicle communication. The objective of our work is to propose a methodology based on analytical modeling techniques such as Markov chains and generalized stochastic Petri nets (GSPN) allowing us to model these maneuvers and evaluate their impact on the platoons safety.

3. PATH Architecture

The PATH research program proposed an hierarchical control architecture for controlling platoons of vehicles. This architecture improved the traffic throughput up to four times, while reinforcing safety. In this program, the vehicles platoons use lateral and longitudinal controllers (of positioning) in order to follow each others on roads equipped with magnetic marks. The automated vehicles are coordinated by both vehicle-to-vehicle and vehicle-to-fixed infrastructure communications, using a road-side infrastructure for traffic management purpose.

A *platoon* (*p*) is a series of vehicles that are moving in the same direction on a specified highway [2]. Each platoon contains a number of vehicles directed with one *leader* that is the first car of the platoon. The vehicles that follow the leader are called *followers*. A platoon that contains one vehicle is called free agent. Figure 1 shows three platoons: *p1* that contains three vehicles, a leader and two followers, *p2* an adjacent platoon, and *p3* an example of free agent.

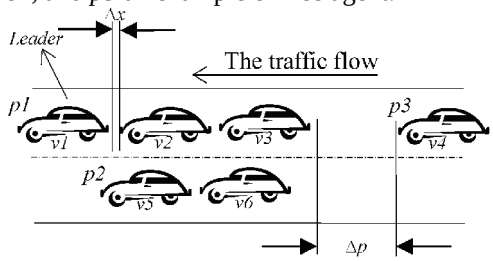

Figure 1: Context of a platooning application

The main maneuvers are: splitting of a platoon, merging of platoons, or making a vehicle exit or enter the platoon. In particular, in case of a failure affecting

a vehicle in the platoon, the maneuvers allow the vehicle to leave its platoon without any hazard, for the purpose of continuously running the platoon without any problem [3].

For starting a maneuver, the faulty vehicle communicates with its platoon's leader that determines the exit strategy and ensures the coordination for the maneuvers associated to this strategy. If the faulty vehicle is the leader, other maneuvers must be applied to allow the platoon vehicles to select the new leader. According to the failure mode, certain maneuvers may require a communication between the leaders of several platoons in the environment [3].

4. Methodology

Our objective is to evaluate dependability measures characterizing the safety of the automated highway system taking into account: i) the occurrence of different types of faults and failure modes affecting the vehicles or their communications, and ii) the strategies and maneuvers that have been designed to allow a faulty vehicle to leave a platoon without affecting the safety of the whole system including the adjacent platoons. The evaluation of these measures should take into consideration the different ways of vehicles coordination in the automated highway system.

Two main steps can be distinguished. The first step consists in identifying representative platooning scenarios, the failure modes to be taken into account, and their severities and the maneuvers needed to ensure safe platooning. The second step is dedicated to the elaboration of the GSPN analytical models incorporating the information identified in the first step to quantify safety and dependability measures.

As illustrated in Table 1 different failure modes with different levels of severities can be distinguished. The corresponding maneuvers to be applied to ensure the safety of the platoon are also identified. When multiple failure modes occur or when a maneuver fails, the maneuver with the highest priority is applied (see Figure 2). The success of a given maneuver depends on several factors, e.g., the states of the vehicles involved in the platoon and the density of the traffic.

The dependability modeling consists in the elaboration of GSPNs describing the behaviors of each vehicle involved in the considered platooning scenarios as well as the dependencies resulting from interactions between vehicles inside a platoon and between platoons during the execution of the safety maneuvers. One of the critical aspects to be addressed during modeling is to master the complexity of the models at the model construction and processing levels and to take into account the dynamicity of the vehicles. Hierarchical compositional approaches are currently investigated to address this problem.

Table 1: Examples of failure modes and maneuvers

Failure mode	Severity	Maneuver
FM1 (No Breaks)	A3	Aided Stop (AS)
FM2 (Inability to sense vehicles in adjacent lanes)	A2	Crash Stop (CS)
FM3 (Inter-vehicle communication failure)	A1	Gentle Stop (GS)
FM4 (Transmission failure)	B/B2	Take Immediate Exit-Escorted (TIE-E)
FM5 (acceleration controller down)	B2	Take Immediate Exit (TIE)
FM6 (communication between link and network layers down)	C	Take Immediate Exit-Normal (TIE-N)

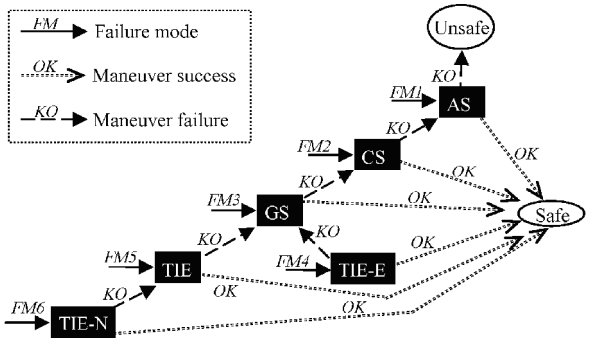

Figure 2: Failures modes, maneuvers, safety impact

5. Ongoing Work

Ongoing work is focused on the elaboration of the GSPN modeling framework considering platooning scenarios involving a limited number of vehicles and platoons. Sensitivity analyses will be performed to compare different communication and coordination schemes between the vehicles: e.g., centralized vs. decentralized inter-platoon or intra-platoon communication. Particular attention is also devoted to the investigation of efficient means to take into account vehicles mobility in the models.

Acknowledgment: This work was partially supported by the HIDENETs project *(HIghly DEpendable ip-based NETworks and Services)* http://www.hidenets.aau.dk/ (EU-IST- 26979).

6. References

[1] S. Hallé, "Automated Highway Systems: Platoons of Vehicles Viewed as a Multiagent System, M.Sc., "Faculté des études supérieures de l'Université Laval. Québec, 2005.

[2] P. Varaiya, "Smart Cars on Smart Roads: Problems of Control," IEEE Transaction on Automatic Control, vol. 38 No. 2, pp. 195-207, Feb. 1993.

[3] D. N. Godbole et al. A. Deshpande, and A. E. Lindsey, "Towards a Fault Tolerant AHS Design Part II: Design and verification of communication protocols," Institute of Transportation Studies, University of California, Berkeley, *paper* UCB-ITS-PRR-96-15 1996.