Performance evaluation of safety critical ITS-G5 V2V communications for cooperative driving applications

Nikita Lyamin

School of ITE
Halmstad University
Halmstad, Sweden

Supervisors:

Alexey Vinel, Magnus Jonsson, Boris Bellalta

Abstract

Intelligent Transport Systems (ITS) are aiming to provide innovative services related to different modes of transport and traffic management, and enable various users to be better informed and make safer, more coordinated and smarter use of transport networks. Cooperative-ITS (C-ITS) support connectivity between vehicles, vehicles and roadside infrastructure, traffic signals as well as with other road users. In order to enable vehicular communications European Telecommunication Standards Institute (ETSI) delivered ITS-G5 – a of set of C-ITS standards. Considering the goals of C-ITS, inter-vehicle communications should be reliable and efficient.

The subject of this thesis is evaluation of the performance, efficiency, and dependability of ITS-G5 communications for cooperative driving applications support. This thesis includes eight scientific papers and extends the research area in three directions: evaluation of the performance of ITS-G5 beaconing protocols; studying the performance of ITS-G5 congestion control mechanisms; and studying the radio jamming Denial-of-Service (DoS) attacks and their detection methods.

First, an overview of currently available and ongoing standardization targeting communications in C-ACC/platooning cooperative driving application is provided. Then, as part of the first research direction, we demonstrate via number of studies, that adaptive beaconing approach where message generation is coupled to the speed variation of the originating ITS-s may lead to a similar message synchronization effect in the time domain when vehicles follow mobility scenarios that involve cooperative speed variation. We explain in detail the cause of this phenomenon and test it for a wide range of parameters. In relation to the second problem, we, first, study the influence of different available ITS-G5 legitimate setups on the C-ACC/platooning fuel efficiency and demonstrate that proper communication setup may enhance fuel savings. Then we thoroughly study the standardization of the congestion control mechanism for ITS-G5, which will affect the operation of all cooperative driving C-ITS applications as a mandatory component. We study the influence of congestion control on application performance and give recommendations for improvement to make the congestion control to target at optimizing the applications performance metrics. In the scope of the last research direction, we propose two real-time jamming DoS detection methods. The main advantage of our detection techniques is their short learning phase that not exceed a few seconds and low detection delay of a few hundreds of milliseconds. Under some assumptions, the proposed algorithms demonstrates the ability to detect certain types of attacks with high detection probability.

CONTENTS

ACKNOWLEDGMENTS

This thesis is a result of four years of my studies at Halmstad University at the School of Information Technology within the Computer Communication group.

First, I want to thank Professor Alexey Vinel without whom this thesis would not be possible. I am grateful for the efforts and time he allocated to me, for his support of my ideas and his contribution in their development. Alexey, I want to sincerely express my gratitude for your guidance. Thank you for your openness, for our enormous discussions and all that great time I had a fortune to spend with you. Also, I want to thank my co-supervisors Professor Magnus Jonsson and Associate Professor Boris Bellalta for their support and contribution.

I want to thank all of the co-authors of the papers which are included and not included in this thesis. Dear colleagues, I want to say that it was a pleasure to work with all of you.

I am honored to thank Professor Oleg Melentyev, who has been my first supervisor and without whom my formation as a researcher would not be possible. He has always been an example of the fortitude and dedication that inspired me.

Finally, I want to thank my beloved wife Natalya, who not only supported all my ideas, but also to a great extent contributed to my personal development.

Part I

Chapter 1

Thesis Introduction

1.1 Motivation

Cooperative Intelligent Transportation Systems (C-ITS) use the connectivity between vehicles, roadside infrastructure, and other road users to enhance driving safety and comfort, and improve traffic management. Regular exchange of information between road users (*beaconing*) keeps them informed about each other's position, driving kinematics, and other attributes. This is one of the cornerstone of road safety and traffic efficiency applications on the way towards autonomous driving. European Commission in its strategic document "Deployment and Operation of European Cooperative Intelligent Transport Systems" (June 2017) highlights, that "Depending on the nature of the applications (e.g. information supply, awareness, assistance, warning to avoid an accident, traffic management), C-ITS can contribute to improving road safety by avoiding accidents and reducing their severity, to decreasing congestion, by optimising performance and available capacity of existing road transport infrastructure, to enhancing vehicle fleet management, by increasing travel time reliability and to reducing energy use and negative environmental impact. Further C-ITS are considered a first milestone towards higher levels of automation in road transport."

Cooperative adaptive cruise control (C-ACC) and platooning are two emerging automotive C-ITS applications. In this thesis, we will refer to that class of automotive systems as C-ACC/platooning. In C-ACC/platooning the leading vehicle is driven by a human, while the following vehicles automatically maintain the velocity of the leading one, but their directions are still controlled by the drivers. Platooning is aiming to reduce the air-drag in the caravan of heavy-duty vehicles, which could significantly benefit from the fuel consumption point of view, while C-ACC is mostly oriented towards increasing the driving experience enabling comfort semi-autonomous driving [1]. The cooperation between the vehicles in the C-ACC/platooning is achieved by the frequent exchange of periodic broadcast messages, which we refer to as beacons. Beacons may contain various related information like vehicle's ID, kinematic information of a vehicle, such as its current speed, position, direction, etc. European Commission in its strategy document "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" (November 2016) highlight, that "Communication between vehicles, infrastructure and with other road users is crucial also to increase the safety of automated vehicles and their full integration into the overall transport system. Truck platooning (trucks communicating to automatically and safely follow each other at very short distance) is a good example: connectivity, cooperation and automation must all come together to make it work."

To enable inter-vehicle communications in the Dedicated Short Range Communications (DSRC) 5.9 GHz band, IEEE 802.11p, which is currently integrated into the recent IEEE 802.11-2012 standard, has been introduced by the Institute of Electrical and Electronics Engineers (IEEE). IEEE 802.11p provides the medium access control (MAC) and physical (PHY) layers for wireless communications in a vehicular environment. The IEEE 1609 working group has defined the protocol stack IEEE 1609.x, also known as WAVE (Wireless Access in Vehicular Environment). The scope of these standards is the extension of the IEEE 802.11p MAC layer functions for multi-channel operation as well as the specification of the upper layers, functionality in security and management planes.

At the same time, European Telecommunication Standard Institute (ETSI) delivered the first release of the C-ITS standards under European Commission Mandate M/453. ETSI specified the first set of ITS-G5 communication protocols and architecture regulating operation in the 5 GHz spectrum for C-ITS. ITS-G5 reuses the PHY and MAC layers of the IEEE 802.11p framework.

At present, pre-standardization activities are still ongoing at ETSI TR 103 301 and TR 103 299, which are studying the applicability of currently available standards for CACC/platooning applications [1]. Therefore, a way to enable inter-vehicular cooperation and collaboration within the platoon based on the current standardization framework is considered in this thesis.

Considering the goals of C-ITS, inter-vehicle communications should be reliable and efficient. Obviously, C-ITS communications became a field of intensive research activities. However, there are still a lot of open issues and white spots in the field of assessing the performance of C-ITS protocols and approaches. The goal of this PhD thesis is to study the performance of ITS-G5 vehicular communications for CACC/platooning.

1.2 Problem statement

Beaconing, i.e. broadcasting of status updates by all the vehicles on a dedicated channel, is a key enabler for C-ITS. Reliable real-time beacons delivery is crucial for the operation of C-ACC/platooning applications. The beacon delivery might be poor due to the several reasons: improper design of communication protocol stack, congested vehicular communication channel or even malicious jamming interference[1], Figure 1.1.

Thus, we identify three main research areas targeting the aforementioned: studying the performance of ITS-G5 beaconing protocols; studying the performance of ITS-G5 congestion control mechanisms; and studying the sources of radio Denial-of-Service (DoS) attacks and their detection methods and countermeasures. In the ITS-G5 framework ETSI defines the Cooperative Awareness Message (CAM) to support beaconing. It is worth noting, that Cooperative Awareness basic service is mandatory for all kind of ITS-stations (ITS-S) operating in ITS-G5 [2]. In order to support C-ACC/platooning CAM should demonstrate performance that is sufficient to enable coordination among its member vehicles. Thus, the assessment of CAM performance in C-ACC/platooning is of high importance.

Decentralized Congestion Control (DCC) is also a mandatory component of ITS-G5 stations operating in the ITS-G5 band [3, 4] and will accordingly affect the communication exchange of messages in C-ACC/platooning. Despite the main objective of DCC to control channel occupancy and support fair access for all the ITS-S, improper DCC configuration and not justified choice of metrics to be controlled may have a negative influence on the efficiency and stability of safety and time-critical C-ITS applications (e.g., C-ACC/platooning).

Vehicular networks will become a basis for a number of safety and time-critical C-ITS applications. It is obvious, that even a short period of communication disruption in a C-ACC/platooning beaconing exchange may be crucial for its stability and safety. DoS attacks on radio channels could be rather intelligent and not easy to detect, but may disrupt the communication significantly. Thus, there is a demand in methods to detect DoS attacks in cooperative driving applications and in appropriate countermeasures.

The main objective of my research is to facilitate reliable and secure Vehicle-to-vehicle (V2V) delivery of beacons. This can be further broken into three following problems:

1. What is the performance of the currently issued ITS-G5 beaconing approach and its applicability to support C-ACC/platooning vehicular applications?

2. What is the performance of the ITS-G5 decentralized congestion control mechanisms when applied to C-ACC/platooning scenarios?

3. What methods could be applied to detect radio jamming DoS attacks in C-ACC/platooning vehicular applications?

---

[1] This thesis does not consider PHY layer issues and abstracts from channel impairments (e.g. signal propagation attenuation, signal reflection, shadowing, signal multipath, etc.).

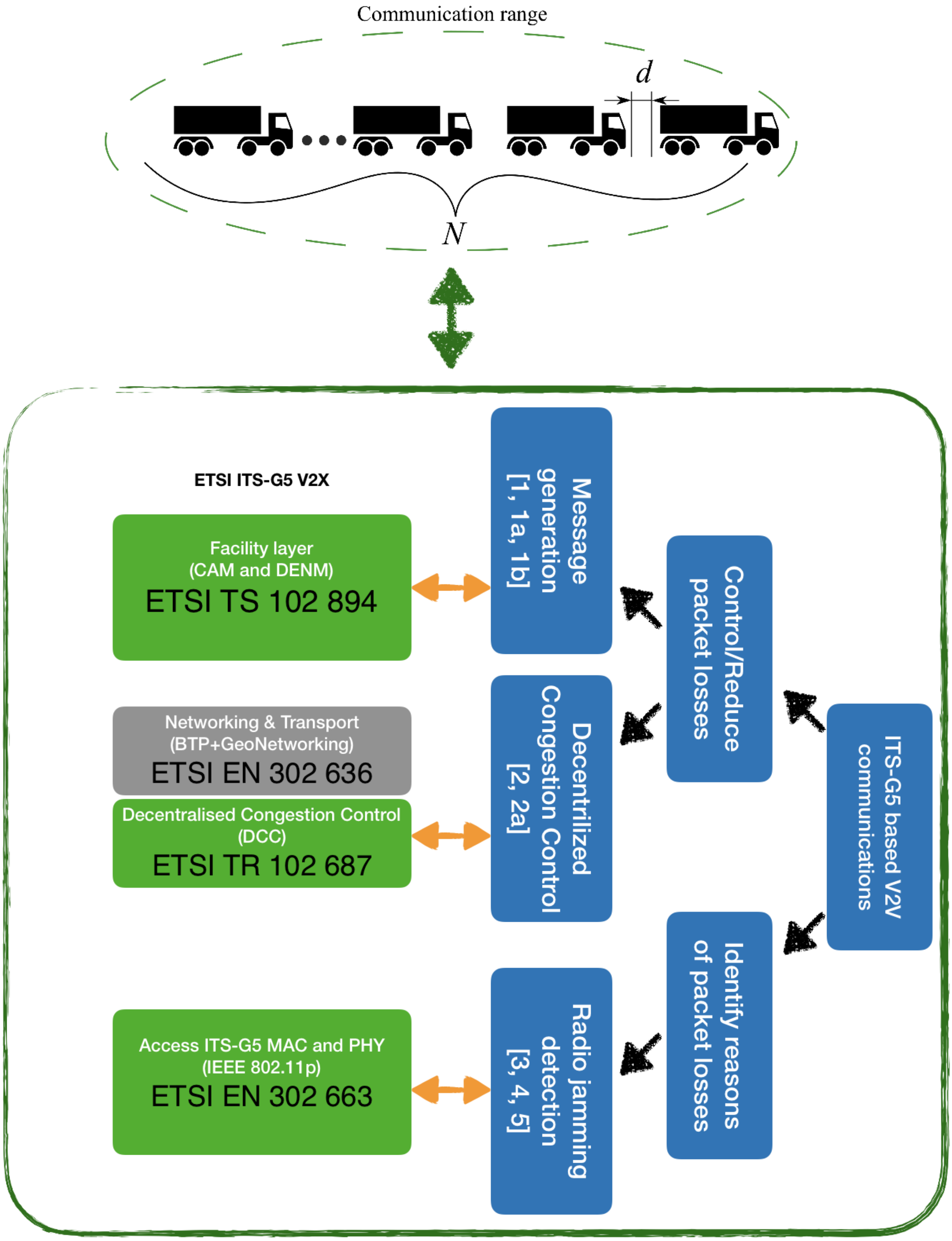


Figure 1.1: Structure of the research activities

1.3 Methodology

In scope of VANETs and, especially, C-CACC/platooning systems the real-world measurements and testbeds become highly expensive and are possible only after a thorough simulation study. To study the IEEE 802.11p wireless communications standard there are several well-known established network simulators can be utilized. Two examples are: Network Simulator 3 [5], OMNeT++ [6]. Also, depending on the research goal, self-written simulators can be utilized. Simulation studies of wireless communications allow to asses the performance of various communication technologies, standards and protocols in a controlled environment/setup. Based on the simulation result conclusions on the effectiveness, reliability and how various parameters affect the communication performance can be done. However, due to the specific properties of VANETs, its complex behavior and extremely high mobility, simulation platforms that combine mobility and communications are necessary. Moreover, in case of the C-ACC/platooning systems, the simulator should be able to support cooperation between vehicles in real-time, relying on the data exchange via wireless communications. Veins [7] and VSimRTI [8] are two widely-used platforms that allow to model V2V and V2X communications and to some extent provide the implementation of WAVE and the C-ITS protocol stack. However, necessary for C-ACC/platooning simulation, real-time interaction with the vehicles' control system is not implemented in these frameworks.

In C-ACC/platooning the design of most communication mechanisms and protocols is based on the information on dynamics of the originating ITS-S, which make it unrealistically to model communication and mobility parts separately. In order to model C-ACC/platooning systems realistically there are several systems that should be coupled: communication simulator, mobility simulator and control system simulator. To the best of our knowledge, there is only one simulation framework that provides all of the aforementioned functionalities, Plexe. Plexe is an C-ACC/platooning extension for the Veins simulator [9]. Plexe allows to model and measure the communication performance of automotive driving systems enabled by inter-vehicle communications closely coupled with the control system of the vehicle. The simulator itself is a combination of the two well-known widely used simulators Omnet++ [10] and SUMO [11]. Omnet++ is a C++ based simulation framework that models the network part. SUMO is an microscopic multi-modal traffic simulation, that handles the mobility of the nodes (vehicles) in plexe. For each communication node in OMNET++ plexe can associate a corresponded node in SUMO. The interaction between OMNET++ and SUMO is supported through TraCI (Traffic Control Interface) interface that uses a TCP based client/server architecture to provide access to SUMO and designed by SUMO developers. The TraCI interface in bidirectional, i.e. OMNET++ may request data from SUMO as well as pass data/commands to SUMO part. Plexe specifies the interaction interface between Omnet++ and SUMO allowing the support of platooning protocols and applications. As part of the plexe on the SUMO side, a platooning control part is implemented. The current version of Plexe supports modeling of platooning application with any longitudinal control algorithm, due to very limited functionality of lateral movements simulation in SUMO. It should be noted, here, that SUMO is a time step-based simulator, i.e. the simulation of vehicles behavior of vehicles is discrete with pre-defined time step (0.01 s by default).

The Plexe simulator provides a detailed implementation of the two bottom ITS-G5 MAC and PHY layers. To better comply with ITS-G5 we also implement ETSI DCC and CAM. Thus, in our framework we closely follow the ITS-G5 framework coupled with the vehicle dynamics. However, so far Plexe uses a simple path-loss channel model to simulate signal propagation, which could be seen as a potential source of channel condition overestimation. In scope of this thesis we used extensive realistic simulations using both a self-written detailed simulator and Plexe, and through deriving analytical models.

1.4 Contributions

Contributions of this thesis are directly related to the three problems we are focusing on, Figure 1.2. Papers 1, 1a, 1b are mostly focusing on the communication problems at the Facilities layer. Papers 2, 2a, 3 are related to decentralized congestion control and its implications. Papers 4, 5, 6 discuss the importance of malicious interference in safety and time-critical C-ITS applications and present a techniques to detect jamming DoS attacks in ITS-G5 V2X communications.

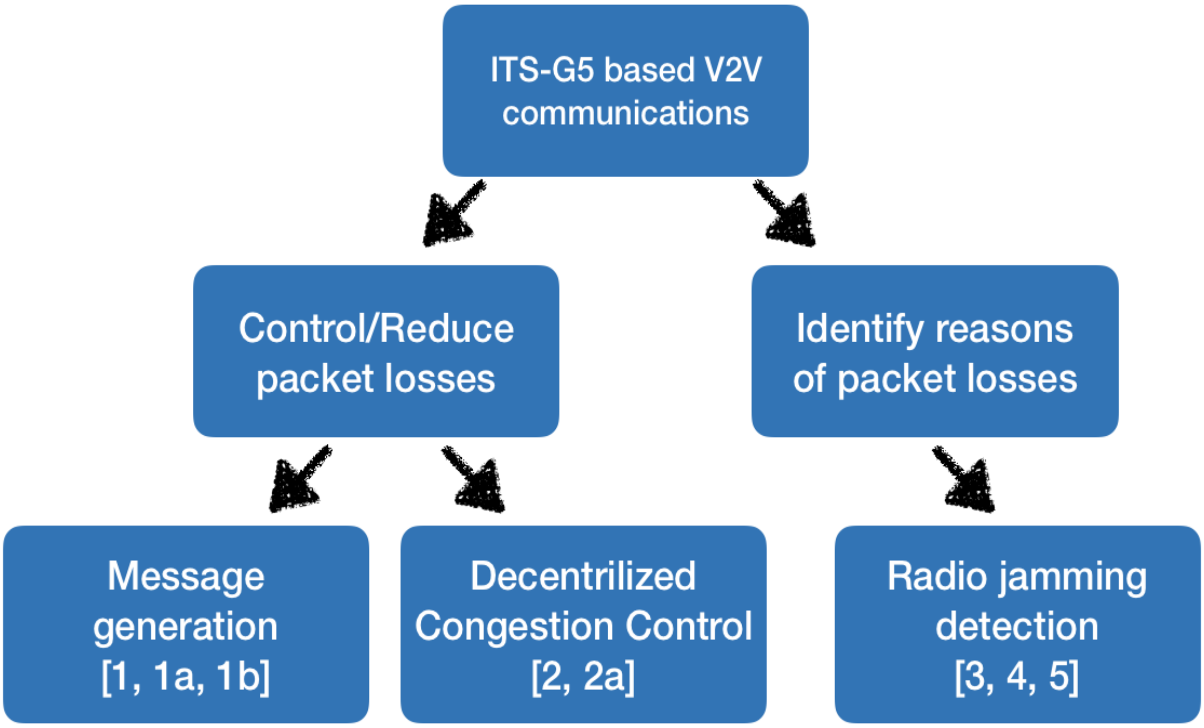


Figure 1.2: Overview of papers

Papers 1, 1a, 1b are related to the first research problem (see Figure 1.1) of message generation in ITS-G5 V2v.

In paper **Paper 1** [12] the communication performance of the ETSI EN 302 637-2 CAM [2] (Cooperative Awareness Message) beaconing in two scenarios is studied. The paper gives an explanation of the specifics in the CAM triggering mechanism design that leads to a grouping of CAMs that, as a consequence, causes degradation in the communication performance. First, we demonstrate that the implementation of ETSI EN 302 637-2 CAM kinematic rules to support C-ACC/platooning in its current form may lead to the degradation of the communication performance, when speed of the C-ACC/platooning is varied. We also demonstrated that ETSI EN 302 637-2 CAM kinematic-based generation may negatively affect the basic C-ITS scenarios, like sequence of vehicles equipped with ITS-G5 V2X communications under stop-and-go mobility patterns, e.g., approaching the intersection under red light.

Paper 1a [1] is a tutorial article explaining the principles of C-ACC and platooning, describing related ongoing ITS-G5 standardization activities, and presenting performance evaluation of the underlying communication technology.

Paper 1b [13] In this short study we have first discovered that the improper choice of the sampling rate value may increase the number of collisions between CAMs at the ITS-G5 IEEE 802.11p MAC layer and, therefore, diminish the efficiency of beaconing in a platoon.

Papers 2 and 2a are related to the second research problem (see Figure 1.1) of decentralized congestion control in ITS-G5 V2V.

Paper 2 [14] is a tutorial paper, where we discussed ETSI standardization process regarding decentralized congestion control (DCC) mechanism for ETSI ITS-G5 V2X communications, covered the main approaches to studying DCC in the literature. We also presented a study, in which we tested various legacy DCC configurations to support C-ITS application. Finally, based on the literature review and the study presented, we draw a conclusions regarding ability of current DCC version to support safety-critical C-ITS applications and suggest a directions in which DCC can be improved.

In **Paper 2a** we take an attempt to evaluate the performance of platoons enabled by ITS-G5 vehicular communications through a number of simulation experiments. We assess the influence of different ITS-G5 communication setups on C-ACC/platoon fuel efficiency. ETSI Decentrilized Congestion Control is an essential part of the ITS-G5 protocol stack. In our study we show that the choice of ETSI DCC setup may directly influence the platooning efficiency. This study is related to both problem one and two, Figure 1.1.

Papers 3, 4, 5 are related to the third research problem (see Figure 1.1) of jamming DoS attacks detection in safety-critical ITS-G5 V2V C-ITS applications.

In **Paper 3** [15] we study jamming attacks in VANETs with focus on the platooning scenario. The paper treats the third research problem. Paper 4 proposes a simple algorithm for real-time detection of jamming attacks against beaconing in IEEE 802.11p vehicular networks. The proposed algorithm is able to detect unlikely loss of beacons in the platooning communication exchange in real time after a short training period.

In **Paper 4** [16] we discuss the problem of malicious interference in safety-critical C-ITS applications. We highlight, that the current development process (both, standardization and research community) do not pay enough attention to the problems of detection and mitigation of malicious interference in V2X communications. We also discuss, that considering the operation and mobility of the safety-critical C-ITS applications, one should consider detection and mitigation of malicious intrusion withing fraction of second. We conclude, that there no methods or techniques for real-time detection of malicious interference available today and, moreover, the countermeasures to such intrusion are almost completely missing. As part of the study presented in the paper we compare few available in the literature jamming DoS detection techniques (both, conventional and data-driven). We conclude, that the development of the data-driven detection techniques may help to improve the detection performance, however, data-driven methods' development should be closely tightened with the knowledge of the V2X communication system operation.

Paper 5 [17] suggests a methods that improves the jamming detection technique proposed in [15]. The original method was derived under the assumption , that CAMs are arriving to the MAC layer with a fixed period. Although, in theory this assumption on a perfect CAM periodicity pattern makes sense, there are sources of jitter in real systems. In the Paper 6 we propose a technique, that combines knowledge of the ITS=G5 V2X communication system operation and a data-driven approach. As a result we come up with the jamming detection method, that can operate under jitter in CAM generation. The proposed real-time detector has a detection delay of order of couple hundreds of milliseconds and a training time below 5 seconds.

1.5 Organization of Thesis

The rest of the thesis is organized as follows. Background material and literature review are presented in Chapter 2. Chapter 3 overviews the Papers included into this thesis. Chapter 4 discusses future studies and concludes the thesis.

Chapter 2

Background and related works

The section is organized in accordance with the three main research problems, divided into corresponding subsections.

2.1 State-of-the-art beaconing approaches

To support cooperative awareness withing ITS-G5, ETSI delivered EN 302 637-2, the standard defining Cooperative Awareness Messages (CAMs) [2]. Note, that Cooperative Awareness basic service is mandatory for all kinds of ITS-stations (ITS-S) operating in ITS-G5. Each ITS-S puts kinematic and other related data into periodically sent CAMs. The content of the message may vary depending on type of the ITS-S. In this thesis we focus on the cooperative awareness on the road and a vehicles as an ITS-S. The standard defines a kinematically-driven mechanism to trigger CAMs. This means, that each vehicle generates a new CAM depending on its current position, speed and direction. The vehicle compares its current kinematic measurements with the ones it put into the last generated message and, if the difference between one of them is above some specified threshold, the vehicle has to trigger next CAM. The reasoning behind that is to allow the vehicle to trigger more messages when its behaviour is highly dynamic and vice versa. In other words, the vehicle will transmit less messages when its behaviour is predictable and more messages, when accelerating/decelerating, turning or driving at high speed. However, as a consequence, the ETSI CAM protocol has a behaviour that is much more difficult to analyse in comparison to a traditional beaconing approaches that have a fixed frequency for the message generation process.

In [18] Liu showed that even small information delays in a platoon may lead to its string instability. Information delay in this context is a time between two subsequent inputs into the controller, which is directly related to the time between two subsequent received beacons from the same vehicle. Traditionally, the operation of a C-ACC/platoon control algorithms is considered either under assumption of a TDMA-like slotted beaconing [19] or CSMA/CA having a fixed beaconing rate [20, 21]. However, ETSI CAMs have much more complex and unpredictable behaviour, which make it difficult to analyse and predict actual informational delay to design an appropriate controller. Moreover, the standard contains a number of parameters with non-specified values, that also need to be tested.

Many studies applying CAMs are either not considering kinematic rules [21, 22, 23] at all or implement CAM according to the standard, but are testing their content structure applicability and not the performance of the mechanism itself. There are very few studies focusing on assessing the effectiveness of the rules proposed by ETSI for CAM generation. The performance evaluation of CAM beaconing under various parameters set has been studied in [24, 25, 26, 27]. In [28], the authors evaluate the CAM rules to understand the actual beaconing rate and corresponding channel load in a highway scenario. In [29], the authors present more the detailed study of the CAM kinematic rules. This paper attempts to find optimal parameters' thresholds to enhance the network performance in terms of packet delivery ratio (PDR), channel load and message age.

Here we overview the most relevant (in terms of of our study) state-of-the-art research into adaptive beaconing in C-ITS.

The authors of [30] present results of an extensive measurement study estimating the performance of CAM cooperative awareness in terms of neighborhood awareness ratio and packet delivery rate. The paper provides substantial results on CAM ability to support awareness at certain level depending on different factors (environment, transmission power level, beaconing generation frequency, etc.). However, the study discuss the results in terms of averaged performance metrics and does not focus on the CAM generation mechanism's functioning itself.

In [31] the authors provide an extensive survey of adaptive beaconing for C-ITS. They provide a taxonomy of adaptive beaconing approaches, summarize performance metrics used for their design, and present their qualitative comparison.

In [32] the authors propose an ATB (Adaptive Traffic Beacon) adaptive beaconing protocol for C-ITS that adapts its beacon generation rate based on two metrics - channel quality and message utility. To estimate channel quality, the authors propose the use of collision statistics collected by the ITS-S, the Signal to Noise Ratio (SNR) levels measurements, and the number of neighboring ITS-S. Message utility is expressed through message age and beacon target dissemination range. Adaptive beaconing for enhancing the cooperative awareness by minimizing the tracking error of ITS-s is presented in [33]. The simulation results presented in the paper demonstrate that the proposed protocol outperforms ETSI CAM beaconing, supporting the lower figures of ITS-S tracking error. In [34], a Dynamic Beaconing Scheduling (DBS) adaptive beaconing approach based on the current kinematics of the ITS-S is presented. The beacon generation interval is proportional to the speed of the originating ITS-S: the higher the speed, the lower the beacon generation interval. The main idea of the proposed protocol is very similar to ETSI CAM kinematic rules, however, the authors do not provide any comparison of the performance of DBS and CAM. The adaptive beaconing protocol AND (Adaptive Neighbor Discovery) is presented in [35] and controls the beacon generation interval in order to maximize the discovery rate of the neighboring ITS-S in the specified road area. The simulation experiment performed by the authors shows that AND outperforms ETSI CAM in terms of ITS-S discovery accuracy at higher channel noise levels, while demonstrating similar performance when packet loss rates are low. In [36] the authors propose FABRIC (Fair Adaptive Beaconing Rate for Intervehicular Communications) - an algorithm that enables fair beaconing rate assignment for ITS-S. In FABRIC the transmission rate of each ITS-S in the one-hop neighborhood is recursively optimized. To enable this, it is assumed that all ITS-S share its beacon generation rate. The set of simulation experiments presented in the paper demonstrates that FABRIC has a fast convergence to fair beacon generation rate even in a highly dynamic environment.

ETSI CAM beaconing is an example of adaptive beaconing design for C-ITS to enable cooperative awareness in the vehicular environment. To adapt the CAM generation rate it adjusts the beaconing rate based on the current kinematics of the originating ITS-S.

Very few studies focus on assessing the effectiveness of the rules proposed by ETSI for CAM generation. In [37] the applicability of ETSI EN 302 637-2 to support platooning was studied. The main conclusion was that CAM may support cooperative autonomous driving, while having gaps in application functionality: support of platooning merging/disaggregation, and, importantly, the lack of an appropriate authentication mechanism that can be used for secure platooning aggregation. The study concludes that improvements of the CAM data structure are necessary.

The authors of [30] present results of an extensive measurement study estimating the performance of CAM cooperative awareness in terms of neighborhood awareness ratio and packet delivery rate. The paper provides substantial results on CAM ability to support awareness at a certain level depending on various factors (environment, transmission power level, beaconing generation frequency, etc.). However, they discuss the results in terms of averaged performance metrics and do not focus on the functioning of the CAM generation mechanisms itself.

2.2 Decentralized congestion control mechanisms

Considering the number of stations in a VANET and limited frequency resources, congestion control (CC) mechanisms are necessary. Since a VANET is an ad-hoc network and does not have a centralised infrastructure, the operation of the CC mechanism should be performed by each vehicle independently from each ITS-S. To cope with these requirements ETSI issued technical specifications defining a decentralized congestion control (DCC) mechanism [38, 39, 3]. Each ITS-S will perform the DCC algorithm independently from the other stations (which makes it fully distributed and decentralized), but since its operation relies on the measured channel load, neighboring vehicles are supposed to have a fair access to the channel resources. Note that in EU, DCC will be a mandatory component of all stations operating in ITS-G5 5.9 GHz frequency band to maintain network stability, throughput efficiency and fair resource allocation, which makes this mechanism a component of key importance.

ETSI TC ITS WG4 first introduced DCC in ETSI TS 102 687 [3] and this standard is the focus of our work. It introduced a state machine approach at access layer to adapt several transmission parameters to the measured channel load. Each state is associated with a certain channel load range and a set of transmission parameters. Our study presented in this article inspired the revision of [3]. In this revision [40] the DCC algorithms are adapted to the channel load limit approach specified by ETSI TC ITS WG2 in ETSI TS 103 175 [38]. Specification [40] also allows for different algorithms to be implement ed. DCC can operate as gatekeeper on the medium access layer, but higher layer DCC functionalities are possible, as specified in [38]. DCC as specified in [3] is based on a state machine that has three states: Relax, Active and Restrictive. In each DCC state the restrictions on the transmission parameters are defined. ETSI DCC in general considers the five following mechanisms to control the vehicle's channel access: "Transmit Power Control" (TPC), "Transmit Rate Control" (TRC), "Transmit Datarate Control" (TDC), "DCC Sensitivity Control" (DSC), "Transmit Access Control" (TAC). The choice of the DCC state is performed based on the evaluation of a so-called *Channel Busy Ratio* (CBR). ETSI suggests the following reference method to estimate the value of CBR. The ITS-S makes periodic channel probes and calculates the proportion of time the channel was busy during a measuring interval $T = 1\ s$ [3]. To calculate the time the channel was occupied, the ITS-S should take m measurements of the received signal level uniformly distributed within the measuring interval. The time between two channel probes should be set to detect the transmission of the smallest possible packet at the highest available datarate. For all channel probes of length 10 μs the average signal level P is determined. Then the CBR measure for the received signal level threshold $P\_threshold$ (-85 dBm by default) is given as: $CBR = \sum_{i=1}^{m}(\text{probes} \quad \text{with} \quad P > P\_threshold)/m$.

Each transition in the state machine has a corresponding CBR value as threshold, the transition is performed under one of the two following conditions: *a*) *Transition to a more restrictive state:* If the CBR value was above the threshold during the last observed measuring interval. *b*) *Transition to a less restrictive state*: If the CBR was below the threshold during the last five consecutive observed measuring intervals.

In each state of the state machine, TRC specifies the minimum time interval between two subsequent transmissions, i.e. TRC specifies the maximum possible transmission rate (messages per second) for each appropriate state.

ETSI DCC also allows state-machine configurations containing a set of sub-states in the "Active" state. This approach enables finer granularity of the DCC state transitions possible. The state machine is fully meshed to allow for transitions between any two states, depending solely on the CBR measurements history, i.e. in defining the current state DCC relies only on the recent CBR measurements and may switch from one state to another in a single step. Thus, DCC-configurations with a reasonable number of sub-states may help prevent rapid changes in the C-ITS transmission behavior, maintaining the targeted level of congestion.

In [41] the performance of ETSI DCC in dense environment, where the number of vehicles in the same communication range is relatively high, was studied. The simulations show that since DCC is decentralized (each vehicle performs algorithm independently without any coordination) an ITS-S may experience unfairness in terms of channel access. The reason for that is a situation when two neighboring vehicles (that are in the same communication range) are placed in different states of the DCC state-machine.

According to [3], ETSI DCC will be the mechanism that each ITS-S should follow. Despite the importance of the DCC, there has been done quite few studies on its performance. The authors of [42] present the performance evaluation of the DCC under various levels of channel load. The authors also determine the impact of different parameters that are affected by DCC operation on overall VANET performance. Based on the simulation results, the paper provides discussion on the effectiveness of ETSI DCC from the communication and application point of view.

The performance of ETSI DCC has been discussed in several studies. The authors of [42] present an extensive performance evaluation of the 3-states ETSI DCC for various CBR values. Based on simulation results, the paper considers the effectiveness of various ETSI DCC CBR control mechanisms (TPC, DSC, TRC, DCC) from the communication and application point of view. Other studies of ETSI DCC demonstrated that the basic 3-state DCC configuration may show low performance. In [43] it is demonstrated that the basic 3-state configuration of DCC [3] tends to oscillate, i.e. to repeatedly switch between relaxed to active and restrictive states. The "unfairness" of the 3-state ETSI DCC configuration [3] was also explained in [41]. The authors show that in a high vehicle density scenario ITS-S may experience unfairness in terms of channel access. The reason for this is a condition when two neighboring ITS-S (i.e. that are in the same communication range) choose different states of the DCC state-machine. Based on the simulation study presented in [44], the authors conclude that a DCC state machine with 3 states has poor performance in terms of its ability to adjust its state to varying CBR values.

Thus, alternative ETSI DCC configurations and parameter sets have been proposed in the literature to overcome aforementioned drawbacks. For example, in [45] the focus is on to the tuning of the TDC configuration. Following the outcome of their previous study, in [46], the authors propose using only TDC (transmit datarate control) for a 3-state DCC configuration, keeping the transmit power level and the sensitivity level for all states at a constant value equal to the Active state of the ETSI DCC 3-state configuration of [3]. In [45] the authors also focus on adjusting the TDC. The novelty of their DCC design is that the switch between different DCC states is performed using a hysteresis curve for the CBR instead of conventional thresholds. The hysteresis mechanism allows a better control of the CBR trend based on the last measurement interval. It also allows different CBR values for the same state, depending on whether the local CBR increases or decreases in comparison to the previous measurement interval. To determine suitable data rates for each state of the DCC state machine, the authors estimate the expected CBR for all data rates available in ITS-G5, considering a fixed beacon size and a fixed generation rate of 10 Hz, and by quantifying the number of ITS-S in the network based on the vehicle density per square kilometer.

Another way to enhance DCC performance suggested in the literature is to increase the number of sub-states in the active state. Thus, the authors in [44] propose a 6-state DCC configuration based on TPC in combination with different CBR thresholds for each state to introduce a negative feedback to the control loop. To obtain the CBR thresholds, the authors identify the channel load that they considered to be an optimum balance between improving channel utilization and packet collisions and select the state transition parameters so that the state machine operates close to this optimal channel load. The target CBR value was identified through simulations of various vehicular densities. The simulation results presented in the paper show that a CBR value of 0.65 is a reasonable value for the channel load, regardless of the vehicle density or the CBR threshold.

Following a similar approach, the authors in [47] propose the use of DCC with several sub-states in Active state together with TPC. The CBR thresholds for the state transitions are selected according to CCA (clear channel assessment) value. The authors introduce a TRC implementation that gradually decreases the beaconing rate from 10 Hz to 1 Hz following the increase of CBR. Finally, it was shown that a DCC configuration with more Active sub-states has a better performance due to its improved adaptivity to varying CBR values.

Other attempts are taken in the direction of avoiding the ETSI DCC re-active state-machine involve controlling the CBR pro-actively. In [48] the authors perform a simulation study to compare the performance of the ETSI DCC state machine with several sub-states in Active state with a linear adaptive DCC packet rate control mechanism called LIMERIC. For both configurations, only TRC is considered. In the presented setup LIMERIC outperforms the state-machine approach in terms of IPG (inter packet gap).

2.3 Denial-of-service attacks detection approaches

Since the IEEE 802.11p medium access control (MAC) protocol specifies random access, during its normal operation the beacons can be lost either due to the wireless channel impairments or due to collisions (overlapping transmissions of beacons from several vehicles). The probability of collisions can be reduced by the proper choice of the MAC protocol parameters [49]. However, the beacons can also be intentionally corrupted by malicious node in case of a jamming Denial of Service (DoS) attack [50]. To support safety applications in a vehicular environment with extremely high mobility of the wireless nodes, inter-vehicular communications should provide a relatively high level of reliability. Various types of DoS attacks could significantly compromise the reliability of the communications. Obviously, DoS attacks may have different types/sources of intrusion. The most relevant types of DoS attacks for vehicular environments are summarized in [51] (a short summary is given later in this section). In scope of this study we focus on radio jamming attacks. A jamming DoS attack it is usually defined as the situation when a malicious node (hereafter, jammer) emits according to some jamming strategy aiming to disrupt the exchange of messages over the communication channel. The jammer can damage certain messages/parts of the messages or jam the communication channel completely depending on its own goals and strategy [50]. It was experimentally shown in [52], that jamming may have significant influence on the stability of the communications in vehicular environments.

According to TS 101 559 – 1 (RHS) [53], the end to end latency of CAM should be less than 300 ms for a road hazard signalling application. In the presence of a jamming node, the loss of a few subsequent beacons will lead to the failure of the requirements. For platooning and C-ACC applications, this end to end latency requirement may be further reduced. Thus, to reduce the air-drag in the platoon of heavy-duty vehicles (which would significantly reduce the fuel consumption), the inter-vehicle gap in the platoon should be in the order of several meters [54]. This means that the reaction time of the vehicles in the platoon will be very tight and interruption in the beacons' exchange might compromise security of the automotive systems and endanger the safety of road traffic.

Packet losses in VANETs may be caused not only by legitimate IEEE 802.11p CSMA/CA collisions or ITS-G5/DSRC channel impairments, but also by malicious interference originated from a radio transmitter located in the vicinity of communicating vehicles.

Experiments in [55] demonstrated that Denial-of-Service (DoS) attacks via jamming of CAMs are easy to implement and may have a crucial impact on the platooning performance. Specifically, jammer with the reaction time in order of tens microseconds can be created with an open access wireless research platform. When located along the road, such a reactive jammer can substantially increase the packet loss ratio at V2V links of platooning vehicles up to the level of a complete blackout for few seconds.

The simulation study in [56] demonstrated that the platoon system is highly sensitive to jamming attacks and its performance can be compromised by a reactive jammer, in particular it was shown that the presence of reactive jammer may lead to string instability phenomena. In [57] authors perform a simulation experiment for radio jamming countermeasures effectiveness, i.e. beamforming. Results demonstrate that in static configuration of nodes like platooning beamforming may reduce the harmful influence of radio jamming on platooning performance. However, no jamming detection technique was proposed in study to identify the presence of jammer, also the power of the jammer was limited, which make efficiency of beamforming questionable under stronger jamming signal.

Thus, reliable methods to detect radio jamming DoS intrusion into platooning C-ITS are required. Moreover, taking into account that platooning vehicles are moving with only a few meters inter-vehicle gap, the jamming DoS detection methods should be able to detect an attack in *real-time* within a fraction of second.

In [51] the authors consider various types of potential scenarios when communications between autonomous vehicles participating in C-ACC/platooning are compromised. Throughout the paper they classify possible security attacks on a C-ACC/platooning vehicle stream by the influence on different levels of the communication stack:

- *Application layer* attacks are oriented to disrupt the functionality of applications, like C-ACC/platoon beaconing exchange or the management protocol. The adversary can use message falsification (modification), spoofing (masquerading), or replay attacks to maliciously affect the vehicle stream. In the case of a message falsification attack the adversary starts listening to the wireless medium and, upon receiving each beacon, manipulates the content meaningfully and rebroadcasts it. Spoofing assumes that the adversary impersonates another vehicle in the

C-ACC/platoon stream in order to inject fraudulent information into a specific vehicle. During replay attacks the adversary receives and stores a beacon sent by a member of the C-ACC/platoon stream and tries to replay it at a later time with malicious intent – the replayed beacon contains old information, which can lead to hazardous effects.

- *Network layer* attacks have a focus to affect not a particular application, but multiple applications by violating the TCP/IP stack operation. Examples of network layer attacks could be various denial-of-service (DoS) or distributed DoS (DDoS), like radio jamming on the control channel (CCH) [15]. Another possible example is enormous number of messages emitted on the CCH by the adversary, which cause an enormous number of CPU-intensive operations (due to the complexity of cryptographic operations). That kind of attacks may make CACC/platoon members unable to support proper communications in a vehicle stream.
- *System level* attacks are characterized as a tempering with vehicle hardware or software, which can be performed by a malicious insider at the manufacturing level or by a malicious outsider. In that case even if V2V communication is stable and secure, tampered hardware/software can provide wrong/incorrect information to the vehicle itself or to another CACC/platoon member via communication facilities.
- *Privacy leakage* attacks. Due to the periodic beaconing exchange in the C-ACC/platoon systems there is a possibility for an intruder for eavesdropping. Each message may contain various information about the originating vehicle and the C-ACC/platoon system in general (vehicle ID, speed, position, acceleration and others), which could be further potentially used by the malicious node for its own benefits.

The authors also present simulation results showing the stability of the C-ACC/platooning system under message falsification and network layer DoS attacks through the set of simulations. In both cases C-ACC/platooning experiences significant downgrade in the performance from the longitudinal stability (inter-vehicle gap), which shows the actuality of the attacks on security in that type of systems.

In [58] a jamming-detection method based on machine learning algorithms is presented. The authors propose to use the following metrics:

- channel busy ratio;
- channel noise;
- inactive time;
- packet delivery ratio.

The proposed method is splitted into 2 phases: training and detection. During the training phase, a number of training sequences are obtained under controlled experiments that should be performed both with and without the presence of the jamming node. This result could then be used to construct a Random Forest [59] classifier that later can be used as a classifier in the detection phase. The authors tested the performance of the detector in the presence of constant and reactive jammers. Experiments showed a detector accuracy of over 90%. The main drawback of the proposed method is its high dependency on the training sequences. All the metrics that have been used for decision tree construction are highly dependent on the current VANET conditions, which are constantly influenced by high dynamics. That fact makes offline training of the proposed system almost an impossible task. Although, the authors do not posses their method as an real-time solution. If the considered VANET has a relatively static behaviour like platoon/C-ACC, the detector can be trained offline, and the proposed method may have potential application in the scope of such type of systems.

Chapter 3

Summary of Appended Papers

The section presents a summary of the appended papers. In Paper I we provide an overview of the current ETSI ITS-G5 standardization activities aiming to support CACC/platooning, while Paper II-IV are related to the research problems 1-3 accordingly, as illustrated in Figure 1.2.

3.1 Paper 1

Title: Cooperative awareness in VANETs: On ETSI EN 302 637-2 performance
Authors: Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Boris Bellalta
Published in: IEEE Transactions on Vehicular Technology
Summary: In this paper we carefully study the CAM synchronization effect, discovered in Paper 1a. The synchronization effect occur due to the design of CAM kinematic rules. In short, CAM kinematic rules assume that the generation of a new CAM is coupled with the current kinematic parameters of the ITS-s, i.e. speed, position, heading. The general CAM generation mechanism is the following: ITS-s stores the speed, position, heading that was put in the last generated CAM and periodically compares them with the current according values received from CAN bus. For all three parameters there are a thresholds (0.5 m/s, 4m, 4° respectively), when the absolute difference between current value of the corresponded parameter and the value put in the last message exceeds the threshold, a new CAM is triggered. The original idea behind this approach could be described as follows: ITS-s generates more messages, when it experience more rapid kinematic changes (e.g. moves at high speed, accelerate/decelerate, make a turn, etc.) and triggers less CAM when it's less mobile. However, when one start to apply this rules in the scenario when number of ITS-s more relatively synchronously, implementation of CAM rules may cause the negative effect when CAM from different ITS-s become synchronized in the time domain (several ITS-s trigger their CAM roughly at the same time). In Paper 1 we explain this mechanism of "CAM synchronization" in details. To quantify the CAM synchronization we study how it affects two following scenarios:

- Scenario 1: platooning. In this scenario we consider a platoon of CACC-enabled (Cooperative Adaptive Cruise Control) vehicles moving on a highway.
- Scenario 2: traffic jam. In this scenario, we consider a set of ITS-s moving on the road with no coordination between them, while still exchanging CAM messages. The mobility scenario emulated here was the following: a string of vehicles approaching traffic lights. In the situation where the lights switch to red, the vehicles closest to the intersection at the road lanes start to decelerate roughly at the same time. Vehicles decelerate until they completely stop at the intersection, wait until the lights turn green and accelerate again to cross the intersection.

Based on the results of the simulation experiments, we concluded, that a) the better vehicles in the string are synchronized (the more simultaneous the mobility changes ITS-s experience) and b) the more precise ITS-s follows kinematic rules, the stronger the negative effect of CAM synchronization (higher the CAM collision rate).

Another important conclusion was that the nature of the CAM synchronization phenomenon presented in this manuscript is not dependent on any particular form of the speed curve as long as its mobility follows a deceleration/acceleration pattern. In other words the studied effect will be observed when the string of vehicles decelerates due to any disturbance in front of it (e.g., slower vehicle, speed limit, etc.), which will obviously occur during road operation. The CAM synchronization phenomenon itself is a result of triggering rules design – in particular the nature of $v_{\min}$ related condition – that leads to CAM synchronization.

Moreover, ETSI EN 302 637-2 CAM is only chosen for representative purposes as an existing available standard of the adaptive beaconing based on the originating vehicle's dynamic in order to demonstrate the phenomenon of the beacon synchronization effect in a string of vehicles performing cooperative maneuvers. Generally, any adaptive beaconing approach that relies on the track of the speed variation of the originating ITS-S may lead to a similar message synchronization effect in the time domain when vehicles follow mobility scenarios that involve cooperative speed variation.

3.2 Paper 1a

Title: Vehicle-to-Vehicle Communication in C-ACC/Platooning Scenarios
Authors: Alexey Vinel, Lin Lan, Nikita Lyamin
Published in: IEEE Communications Magazine
Summary: ITS-G5 defines the overall vehicular communication protocol stack. So far there has been no dedicated message type or DCC configuration standardized for platooning. However, there is currently pre-standardization activity (ETSI TR 103 301, TR 103 299) studying how to apply currently available standards for a platooning application. In Paper I we give a brief description of C-ACC and platooning, also depicting major differences between these applications. In compliance with the idea of using current standards in order to enable CACC/platooning operation, Paper I provides results of a simulation study. In this study communication exchange in platooning is enabled by

currently available ETSI EN 302 637-2 CAM. In scope of the simulation setup we tested both CAM kinematically driven message triggering and a fixed beaconing rate of 10 Hz. To estimate the information delay, data-age metrics has been used as a performance metrics. Based on the results, the paper concludes that fixed beaconing with a proper message generation frequency outperforms CAMs in terms of data-age. Our conclusion is that the current CAM rates could be insufficient to support platooning requirements. Moreover, due to the dynamic-dependent nature of CAM generation, the data-age may vary significantly depending on the mobility pattern of the platoon. It is worth to be noted here, that DCC operation was disabled in scope of this study, so the results could be generalized and extended to a system supporting both CAM and DCC.

3.3 Paper 1b

Title: Does ETSI beaconing frequency control provide cooperative awareness?
Authors: Nikita Lyamin, Alexey Vinel, Magnus Jonsson
Published in: 1st IEEE ICC 2015 Workshop on Dependable Vehicular Communications.
Summary: In this paper we evaluate the performance of ETSI EN 302 637-2 CAM in the platooning scenario. CAM triggering conditions [2] are based on the dynamics of an originating vehicle. These conditions are checked repeatedly with a certain sampling rate. An ITS-S generates CAM whenever the kinematic event occurs, with an upper bound of 10 messages/second (10 Hz). If no kinematic event is observed for 1 second after the last CAM generation, the ITS-S should also generate a message, which corresponds to a lower bound of 1 message/second (1 Hz). By kinematic event it is meant here that the ITS-S tracks its current speed, position and direction and compares them to the values sent in the last triggered CAM. If the differences exceeded any of the pre-defined thresholds, a kinematic event is detected and a CAM is generated. In the scope of the study we consider a platoon, following disturbance mobility pattern, where information exchange is enabled by CAM. Disturbance mobility pattern is when a vehicle (platoon) performs acceleration/deceleration maneuvers, which is aiming to emulate a slower vehicle in front. The slower vehicle may appear due to a lane changing process (e.g. the vehicle is trying to take off-ramp) or it could be considered as a vehicle coming from metering ramp, etc. Our simulation setup shows, that due to the design of kinematic rules, CAM triggering times of different platoon members may become synchronized in time domain after subsequent maneuvers. We show that the CAM synchronization effect may further lead to increased CAM collision rate on the wireless channel and subsequent communication performance degradation. The paper describes the mechanism leading to the occurrence of the negative CAM synchronization effect, and proposes a framework allowing to analyze the strength of the effect. Also we study the influence of various CAM sampling rates on the communication performance and make appropriate conclusions.

3.4 Paper 2

Title: ETSI DCC: Decentralized Congestion Control in C-ITS
Authors: Nikita Lyamin, Alexey Vinel, Dieter Smely and Boris Bellalta
Accepted to: IEEE Communications Magazine
Summary: C-ITS communications must also be operational in dense road traffic. Assuming that all vehicles participate in the C-ITS information exchange by broadcasting periodic messages, wireless channel congestion is likely to occur. Thus, to avoid degradation of the system performance caused by too high a channel load and provide a fair access to the channel resources among neighboring ITS-G5 stations (ITS-S), channel congestion control mechanisms are required. To this end ETSI published TS 102 687 [3, 4] – a specification of a decentralized congestion control (DCC) mechanism – as a part of the ITS-G5 protocol stack. Decentralized Congestion Control (DCC) is a mandatory component of 5.9 GHz Intelligent Transportation Systems (ITS-G5) vehicular communication protocol stack that reduces radio channel overload, range degradation, and self interference. In this tutorial article we explain its principle, describe related ongoing standardization activities, evaluate its performance for emerging cooperative driving applications, and identify ways for improvement. We show that failure to use a proper DCC parameterization can impact negatively on the performance of cooperative vehicular applications. Based on the simulation experiment, where we tested all state-machine DCC configurations available ETSI documents, we came to the conclusion, that restricting the communication exchange in safety-critical applications, which are very delay-sensitive could potentially lead to undesirable performance degradation. The most important conclusion of ours, was that the currently specified ETSI DCC configurations are designed to control the Channel Busy Ratio CBR (the percentage of time communication channel is observed as busy) level as such, but not the system level C-ITS application metrics. Standards for several safety-critical C-ITS applications (e.g. platooning) are currently under development. Appropriate control criteria for channel congestion level could be selected to make the DCC to target at optimizing the applications performance metrics. For this purpose, mechanisms are needed to estimate the influence of the CBR limits on the performance of C-ITS applications. In our opinion, mathematical models of the DCC are clearly needed to better characterize and understand the complex dynamics of C-ITS systems further. This demand is especially emerging, since the studies of the ETSI DCC which are currently available in the literature rely on the simulation experiments of specific scenarios and the theoretical foundations to develop the DCC configurations are required.

3.5 Paper 2a

Title: Study of the Platooning Fuel Efficiency under ETSI ITS-G5 Communications
Authors: Nikita Lyamin, Qichen Deng, Alexey Vinel
Accepted to: IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)

Summary: In this paper we make an attempt to estimate the potential influence of the communication system on the efficiency of the platooning. V2V communications, stability and fuel efficiency in a platoon are closely coupled. Proper communication setup can make a platoon follower maintain a desired distance to its predecessor while reducing acceleration and braking frequencies. We evaluated the performance of C-ACC/platoon enabled by ITS-G5 communication standards through a number of simulation experiments. As it was noted in Paper I there are no dedicated communication standard for platooning available, however current ETSI standardization activities are focused around applicability of the existing ITS-G5 set to enable platooning. In conformity with aforementioned, in Paper III we implement and apply ETSI EN 302 637-2 Cooperative Awareness Messages [2] together with DCC to confirm to the ITS-G5 stack. Note, that according to [3]: "Decentralized congestion control (DCC) is a mandatory component of ITS-G5 stations operating in ITS-G5A and ITS-G5B frequency bands to maintain network stability, throughput efficiency and fair resource allocation to ITS-G5 stations". In Chapter 2.2 it was described that there are several DCC state-machine configurations currently available in the documents. Thus, we compared the potential fuel consumption reduction, when platooning is enabled by two different DCC setups available in ITS-G5. To be able to test influence of ITS-G5 on potential fuel savings, the simulation framework that incorporates a communication simulator with a mobility simulator and uses communication as an input to a platooning control part. To cope with this requirements we use a Plexe simulator that is a special C-ACC/platooning extension of Veins, that combines Omnet++ and SUMO, extending it with CAM and DCC functionality to comply with ITS-G5. Our study shows that the communication setup that exploits DCC with more sub-states in Active state (thus, allowing finer granularity in CBR control and allowing slightly higher CBR levels) enhances fuel economy in average with 0.4 L/100 km in a disturbance scenario, indicating that platoon communication setup also plays an important role in fuel consumption. The enhanced fuel efficiency is a result of the platoon's ability to maintain the required inter-vehicle gap with higher precision under this DCC setup. This comes from the fact that DCC setup with a larger number of "Active" sub-states allows better granularity in controlling CBR, while still keeping congestion level at a required low level. We also suggest an approach of how our results on platoon fuel efficiency can be transformed into potential cost reduction gain. However fuel savings and corresponding cost reduction are highly dependent on the frequency of acceleration/deceleration maneuvers performed by platoon, which requires further extensive study of potential traffic flow parameters for platooning.

3.6 Paper 3

Title: Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks
Authors: Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Jonathan Loo
Accepted to: IEEE Communications Letters.
Summary: In this paper we propose a simple method that is able to detect certain types

of jamming DoS attacks in platooning. We consider platooning with cooperation between the vehicles, which is achieved by the frequent exchange of periodic broadcast messages. To derive our method few assumptions on the operation of the system are taken: first, we assume that the number of vehicles in the platoon is always known to the platoon leader; second, platoon members have a static beaconing generation rate. The proposed algorithm is based on the knowledge of IEEE 802.11p MAC operation. The algorithm is divided into two phases. During the first phase, installation, the detector eavesdrop (via legitimate sniffer installed on the leading vehicle) the sequence of transmitted packets. As soon as it detects a sequence of N successful transmissions (where N is the size of the platoon), it performs classification of the areas in time domain, where collisions are possible and where they can not be observed at any circumstances by the the property of the IEEE 802.11p design. During the second phase, operational, the detector tracks the information of successful and non-successful transmissions and classify the cause of collision using the classifier obtained in the installation phase to distinguish between normal (legitimate) collisions and packet losses caused by malicious jammer. To verify the performance of the detection algorithm we assumed two types of jamming strategies: random jamming, when the malicious node jams packets randomly with some probability; and ON-OFF jamming, when the jammer corrupts a number of packets in a row with some probability. For the reference platooning scenario under the aforementioned assumptions our algorithm provides in average the probability of detection not lower than 0.9 and no false alarm for any jamming probability. Moreover, the installation delay of the proposed algorithm does not exceed 1 second for the tested setups.

3.7 Paper 4

Title: AI-based malicious network traffic detection in VANETs
Authors: Nikita Lyamin, Denis Kleyko, Quentin Delooz, Alexey Vinel
Accepted to: IEEE Networks.
Summary: Inherent unreliability of wireless communications may have crucial consequences when safety-critical Cooperative Intelligent Transportation Systems (C-ITS) applications enabled by Vehicular Ad-Hoc Network (VANETs) are concerned. In this paper we discuss the problem of malicious interference in safety-critical C-ITS applications. Although, natural sources of packet losses in VANETs such as network traffic congestion are handled by a Decentralized Congestion Control (DCC), losses caused by malicious interference need to be controlled too. In our opinion, current development process (both, standardization and research community) do not pay enough attention to the problems of detection and mitigation of malicious interference in V2X communications.

V2X communication links are inherently vulnerable to different forms of losses that may endanger vehicular safety of the C-ITS. It is important to identify the sources of packet losses in critical vehicular networked control loop since a source could require a design of specific countermeasure. For example, to control the natural sources of losses (e.g., network traffic congestion) in VANETs the Decentralized Congestion Control (DCC) mechanism, which is a mandatory V2X component, was standardized for

VANETs in both ETSI and IEEE frameworks. The European DCC approach is based on state machines, where in each state the controller limits parameter values that influence the channel load. At the same time, protocol parameters like CAM generation rate or MAC parameters could be adjusted to avoid performance degradation caused by CAM collisions. CAM losses caused by channel impairments may be partially mitigated by adjusting PHY parameters (e.g. decrease channel datarate, increase transmission power) or, again, adjust CAM parameters (e.g. like CAM generation rate if allowed by congestion control mechanism). However, malicious interference needs to be controlled too. Experiments in [55] demonstrated that a reactive jammer can be created with an open access wireless research platform, when located along the road it can substantially increase the packet loss ratio at V2V links of platooning vehicles up to the level of a complete blackout for few seconds. Thus, a jamming Denial-of-Service (DoS) attack on CAMs may endanger vehicular safety and first and foremost is to be detected in real-time. Moreover, none of the above mechanisms is designed for handling losses caused by malicious interference. Besides, trying aforementioned adaptations, a valuable time in safety critical application could be lost. Instead, one could design specific measures for such situation by immediately adjusting the physical part of the system (e.g. increase headway time between vehicles) to presume safety of the C-ITS application. However, no network control mechanism for malicious interference in VANETs was presumed so far. We believe, that certain steps should be undertaken in this direction.

It was demonstrated in [55] that jamming attacks may have a crucial impact on platooning communication performance and are easy to implement. Thus, reliable methods to detect jamming intrusion into safety-critical C-ITS are required. In vehicular scenarios acceptable detection latencies which are imposed by a physical proximity of high-speed road users running C-ITS safety applications, are in the same order. We conclude, that there no methods or techniques for real-time detection of malicious interference available today and, moreover, the countermeasures to such intrusion are almost completely missing.

As part of the study presented in the paper we compare few available in the literature jamming DoS detection techniques (both, conventional and data-driven). First, we compare two reference detection methods: *a*) a model-based; *b*) a data-driven.

The model-based method presented in [60] is purposefully designed for the considered problem taking into account the knowledge about the ITS-G5 MAC (IEEE 802.11p) communication protocol as well as the platooning C-ITS application and making certain simplifying assumptions, hence, it is model-based.

A data-driven approach in its extreme is completely opposite to a model-based approach. It may work without any knowledge of a system but it requires data produced by that system. Additionally, the data-driven approach requires to use a data mining method for processing the available data. For the data-driven detection approach, we use a concrete method suggested in [61] for the case of detecting anomalies in discrete sequences. It is called *the window-based method.*

Based on the results of the simulation experiment we implemented, we concluded that the baseline data-driven window-based method for anomaly detection in a discrete sequence suggested in the literature [61] did not achieve satisfactory results. Therefore, we conclude that it is not trivial to simply apply data mining methods to this problem without using the prior knowledge about the nature of the system. To resolve this issue we suggest to move develop in the direction of combining the knowledge of the system (model-based) and data mining approach (data-driven) – hybrid methods. In contrast to the reference detection methods, the nature of the hybrid detection method is that it should take into account the knowledge about the platoon from the communication protocol point of view (as the model-based method [60]) but it also uses a communication exchange trace produced by a C-ITS application (as the window-based method). Thus, the hybrid detection method tries to avoid the drawbacks of each reference approaches. We demonstrated, that hybrid approached presented in Paper 6 works in the presence on jitter (in contrast to the model-based [60]) and shows much higher detection performance in the presence of jitter in contrast to the data-driven window-based method [61].

3.8 Paper 5

Title: Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining
Authors: Nikita Lyamin, Denis Kleyko, Quentin Delooz, Alexey Vinel
Submitted to: IEEE Communications Letters.
Summary: Experiments in [55] demonstrated that Denial-of-Service (DoS) attacks via jamming of CAMs are easy to implement and may have a crucial impact on the platooning performance. Specifically, jammer with the reaction time in order of tens microseconds can be created with an open access wireless research platform. When located along the road, such a reactive jammer can substantially increase the packet loss ratio at V2V links of platooning vehicles up to the level of a complete blackout for few seconds. The simulation study in [56] demonstrated that the platoon system is highly sensitive to jamming attacks and its performance can be compromised by a reactive jammer, in particular it was shown that the presence of reactive jammer may lead to string instability phenomena. Thus, reliable methods to detect radio jamming DoS intrusion into platooning C-ITS are required. Moreover, taking into account that platooning vehicles are moving with only a few meters inter-vehicle gap, the jamming DoS detection methods should be able to detect an attack in *real-time* within a fraction of second.

In paper 6 we propose a methods that improves the jamming detection technique proposed in [15]. The original method was derived under the assumption , that CAMs are arriving to the MAC layer with a fixed period. Although, in theory this assumption on a perfect CAM periodicity pattern makes sense, there are sources of jitter in real systems. For instance, there will be non-negligible random processing delays between the message generation moment and the time when actual packet is placed in the MAC-queue for the transmission [62]. In the Paper 6 we propose a technique, that combines knowledge of the ITS-G5 V2X communication system operation and a data-driven approach. As a result we come up with the jamming detection method, that can operate under jitter in CAM generation. The proposed method has a hybrid nature. Following data mining approach, it uses historical data of platoon communications. At the same time, the a priori knowledge about a platoon is used in the method.

In terms of data mining, the jamming DoS scenario in this letter can be treated as a problem of anomaly detection in a discrete sequence [61]. There are two types of events in the considered system: natural collisions (legitimate CSMA/CA collisions) and anomalous collisions (jammed CAMs).

On a very high conceptual level, the operation of the detector can be described as follows. There are two phases: *a*) training; *b*) detection. During the training phase, the detector observes the transmissions of CAMs from different vehicles as well as the collisions. Based on the collected data, detector first forms detection periods i, then for each detection period composes detection sets $\mathcal{R}_i$ and, finally, approximates the time of the most probable transmissions τ_V for each V ITS-s (platoon member) on the detection intervals.

During the detection phase, the detector keeps operating on the detection periods of length T (where T is CAM generation interval) and uses intervals of most probable transmissions τ_V for all the vehicles from 1 to N obtained at the learning phase. For each detection period we construct dependent collision set $C = \{C_1, \ldots, C_k\}$ and involved vehicles set $M = \{M_1, \ldots, M_k\}$, in which we try to estimate in which CAM loss (recall, we can't distinguish between legitimate CSMA/CA collision, jammed CAM or CAM lost due to the channel noise) which ITS-s V could be involved. The jamming detection is built on the basic knowledge about the system: *in order to create a legitimate CSMA/CA collision at least two vehicles have to transmit their CAMs simultaneously*, what enables the decision on raising the alarm jamming if inequality $|M_j| \geq 2|C_j|$ does not hold for at least one pair of subsets M_j and C_j.

The two important properties of the hybrid detector are following. First, The proposed real-time detector has a detection delay of order of couple hundreds of milliseconds: the decision delay does not exceed $1.5T$. Second, a training time for hybrid detector is below 5 seconds.

Regarding the detection performance, in our simulation setup probability of attack detection of the hybrid detector against the number of vehicles in a platoon in the presence of jitter and packet looses was never lower than 0.7 (for N=25, PER=0.1). The probability of false alarm, i.e. the probability that the alarm is triggered although no beacons have been jammed in the detection period, did not exceed 1% in our experiments.

Chapter 4

Conclusion and Future Work

4.1 Conclusions

In this thesis the activities in three main research directions are summarized.

We perform an overview of standardization activity with a focus on enabling C-ACC/platooning communications. Following the approach taken in current standardization process, we study the performance of time-critical C-ITS applications enabled by the ITS-G5 V2X communications. We identify and provide a detailed explanation of the specifics in the CAM triggering mechanism design that leads to a grouping of CAMs that, as a consequence, causes degradation in the communication performance. We demonstrate that the implementation of ETSI EN 302 637-2 CAM kinematic rules to support C-ACC/platooning in its current form may lead to the degradation of the communication performance, when speed of the C-ACC/platooning is varied. We also come top the conclusion, that any adaptive beaconing approach that relies on the track of the speed variation of the originating ITS-S may lead to a similar message synchronization effect in the time domain when vehicles follow mobility scenarios that involve cooperative speed variation.

Our other focus if a Decentralized Congestion Control – a mandatory component of 5.9 GHz Intelligent Transportation Systems (ITS-G5) vehicular communication protocol stack that reduces radio channel overload, range degradation, and self interference. In scope of our studies, we, first, show that the configuration of DCC may have a resulting effect on the efficiency of the underlying C-ITS applications (e.g. fuel efficiency in platooning). Then we also demonstrate that the current design DCC approach requires adjustments: for now DCC tries to control the wireless channel occupancy level as such without consideration of how this can affect the performance of the C-ITS application ITS-G5 V2X communications are aiming to enable/support. We suggest that the DCC approach is revised in order to optimize C-ITS application performance via application-level metrics, e.g. data-age. *In progress: Then we propose an analytic framework that is aiming to control the application level data-age metric: the idea is to maximize the*

C-ITS application performance by minimizing the data-age.

Third, we propose a simple algorithm to detect jamming DoS attacks in a real-time CSMA/CA-based VANET environment. The algorithm is able to detect certain types of jamming DoS attacks with a delay of just hundreds of milliseconds. For the platooning scenario our method achieves average probability of detection above 0.9 keeping learning phase in scope of a second.

We also study the problems of malicious interference in safety-critical C-ITS applications enabled by ITS-G5 V2X. We conclude, that there no methods or techniques for real-time detection of malicious interference available today and, moreover, the countermeasures to such intrusion are almost completely missing. First, we propose a simple algorithm to detect jamming DoS attacks in a real-time CSMA/CA-based VANET environment. The algorithm is able to detect certain types of jamming DoS attacks with a delay of just hundreds of milliseconds. For the platooning scenario our method achieves average probability of detection above 0.9 keeping learning phase in scope of a second. Then, to relax the assumptions taken to derive the first algorithm, we propose a new method. We first try to apply a purely data-driven approach that may work without any knowledge of a system. However, based on our experiments, we conclude that it is not trivial to simply apply data mining methods to this problem without using the prior knowledge about the nature of the system. Thus, we suggest to combine the knowledge of the system (model-based) and data mining approach (data-driven) to come with a hybrid solution. To this end we propose a technique, that combines knowledge of the ITS-G5 V2X communication system operation and a data-driven approach. The proposed real-time detector has a detection delay of order of couple hundreds of milliseconds and requires training time below 5 seconds. Probability of attack detection of the hybrid detector in the presence of CAM generation disturbances and packet looses always exceeds 0.7.

4.2 Future Work

The future work in the direction of the message generation and decentralized congestion control should be brought to the more systemic level, i.e. the entire protocol stack should be tuned/redesigned for time-critical C-ITS applications. For instance, the currently designed standard ETSI TR 103 298 for platooning should be adjusted to avoid negative effect of CAM generation mechanism, the DCC should also be tuned to operate in the interest of C-ITS application. This process requires careful additional studies, performance evaluation and fine tuning.

The problem of potential malicious interference detection in safety and time critical C-ITS applications should be further studied, measures to detect intrusion into the system and mitigate its consequences should also be developed. As a future work, we, first, plan to validate the proposed method with measurement data from platooning test trials, second, fine-tune the detecting capabilities based on the results observed. The next step should be development of appropriate countermeasures.

REFERENCES

[1] A. Vinel, L. Lan, and N. Lyamin, “Vehicle-to-Vehicle communication in C-ACC/Platooning scenarios,” *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[2] “Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service,” *ETSI EN 302 637-2 V1.3.2*, 2014.

[3] “Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part,” *ETSI TS 102 687 V1.1.1*, 2011.

[4] “Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part,” *ETSI TS 102 687 V1.2.1*, 2018.

[5] “The NS–3 network simulator http://www.nsnam.org/.”

[6] “The OMNeT++ network simulator https://omnetpp.org.”

[7] C. Sommer, R. German, and F. Dressler, “Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis,” *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[8] “V2x simulation runtime infrastructure (VSimRTI) http://www.dcaiti.tu-berlin.de/research/simulation/.”

[9] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. Lo Cigno, “PLEXE: A Platooning Extension for Veins,” in *6th IEEE Vehicular Networking Conference (VNC 2014)*. Paderborn, Germany: IEEE, December 2014, pp. 53–60.

[10] “The OMNeT++ network simulator https://omnetpp.org.”

[11] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, “Recent development and applications of SUMO–simulation of urban mobility,” *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, 2012.

[12] N. Lyamin, A. Vinel, M. Jonsson, and B. Bellalta, “Cooperative awareness in VANETs: On ETSI EN 302 637-2 performance,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 17–28, January 2018.

[13] N. Lyamin, A. Vinel, and M. Jonsson, “Does ETSI beaconing frequency control provide cooperative awareness?” in *2015 IEEE International Conference on Communications (ICC), IEEE International Conference on*, London, UK, June 2015, pp. 10 459–10 464.

[14] N. Lyamin, A. Vinel, D. Smely, and B. Bellalta, “ETSI DCC: Decentralized congestion control in C-ITS,” *IEEE Communications Magazine*, 2018, accepted, to be appeared.

[15] N. Lyamin, A. V. Vinel, M. Jonsson, and J. Loo, “Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks.” *IEEE Communications letters*, vol. 18, no. 1, pp. 110–113, 2014.

[16] N. Lyamin, D. Kleyko, A. Vinel, and Q. Delooz, “AI-based malicious network traffic detection in VANETs,” *IEEE Networks*, 2018, accepted, to be appeared.

[17] ——, “Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining,” *IEEE Communications Letters*, 2018, accepted, to be appeared.

[18] X. Liu, A. Goldsmith, S. S. Mahal, and J. K. Hedrick, “Effects of communication delay on string stability in vehicle platoons,” in *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE.* IEEE, 2001, pp. 625–630.

[19] P. Fernandes and U. Nunes, “Platooning with IVC-enabled autonomous vehicles: Strategies to mitigate communication delays, improve safety and traffic flow,” *Intelligent Transportation Systems, IEEE Transactions on*, vol. 13, no. 1, pp. 91–106, 2012.

[20] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, “Platoon management with cooperative adaptive cruise control enabled by VANET,” *Vehicular Communications*, vol. 2, no. 2, pp. 110–123, 2015.

[21] A. Böhm, M. Jonsson, and E. Uhlemann, “Performance comparison of a platooning application using the IEEE 802.11p MAC on the control channel and a centralized mac on a service channel.” in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on.* IEEE, 2013, pp. 545–552.

[22] S. Joerer, M. Segata, B. Bloessl, R. L. Cigno, C. Sommer, and F. Dressler, “A vehicular networking perspective on estimating vehicle collision probability at intersections,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1802–1812, May 2014.

[23] M. A. Javed and J. Y. Khan, “A cooperative safety zone approach to enhance the performance of vanet applications,” in *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*, June 2013, pp. 1–5.

[24] S. Joerer, M. Segata, B. Bloessl, R. Lo Cigno, C. Sommer, and F. Dressler, “A vehicular networking perspective on estimating vehicle collision probability at intersections,” *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 4, pp. 1802–1812, 2014.

[25] P. M. d’Orey and M. Boban, “Empirical evaluation of cooperative awareness in vehicular communications,” in *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*. IEEE, 2014, pp. 1–5.

[26] J. Santa, F. Pereniguez, A. Moragón, and A. F. Skarmeta, “Vehicle-to-infrastructure messaging proposal based on CAM/DENM specifications,” in *Wireless Days (WD), 2013 IFIP*. IEEE, 2013, pp. 1–7.

[27] A. Böhm, M. Jonsson, and E. Uhlemann, “Adaptive cooperative awareness messaging for enhanced overtaking assistance on rural roads,” in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*. IEEE, 2011, pp. 1–5.

[28] J. Breu, A. Brakemeier, and M. Menth, “Analysis of cooperative awareness message rates in vanets,” in *ITS Telecommunications (ITST), 2013 13th International Conference on*. IEEE, 2013, pp. 8–13.

[29] T. Lorenzen and H. Tchouankem, “Evaluation of an awareness control algorithm for vanets based on ETSI EN 302 637-2 V1.3.2,” in *Communication Workshop (ICCW), 2015 IEEE International Conference on*. IEEE, 2015, pp. 2458–2464.

[30] M. Boban and P. M. d’Orey, “Exploring the practical limits of cooperative awareness in vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3904–3916, June 2016.

[31] S. A. A. Shah, E. Ahmed, F. Xia, A. Karim, M. Shiraz, and R. M. Noor, “Adaptive beaconing approaches for vehicular ad hoc networks: A survey,” *IEEE Systems Journal*, vol. pp, no. 99, pp. 1–15, 2016.

[32] C. Sommer, O. K. Tonguz, and F. Dressler, “Traffic information systems: efficient message dissemination via adaptive beaconing,” *IEEE Communications Magazine*, vol. 49, no. 5, pp. 173–179, May 2011.

[33] H. H. Nguyen and H. Y. Jeong, “Crosslayer beaconing design toward guaranteed cooperative awareness with contending traffic,” in *2015 IEEE Vehicular Networking Conference (VNC)*, Dec 2015, pp. 131–134.

[34] M. M. Alotaibi and H. T. Mouftah, “Adaptive expiration time for dynamic beacon scheduling in vehicular ad-hoc networks,” in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Sept 2015, pp. 1–6.

[35] H. P. de Moraes and B. Ducourthial, “Adaptive inter-messages delay in vehicular networks,” in *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2016, pp. 1–8.

[36] E. Egea-Lopez and P. Pavon-Marino, “Distributed and fair beaconing rate adaptation for congestion control in vehicular networks,” *IEEE Transactions on Mobile Computing*, vol. 15, no. 12, pp. 3028–3041, Dec 2016.

[37] C. Bergenhem, “Approaches for facilities layer protocols for platooning,” in *2015 IEEE 18th International Conference on Intelligent Transportation Systems.* IEEE, 2015, pp. 1989–1994.

[38] “Intelligent transport systems (ITS); cross layer DCC management entity for operation in the ITS G5A and ITS G5B medium.” *ETSI TS 103 175 V1.1.1*, 2015.

[39] “Intelligent transport systems (ITS); cross layer dcc management entity for operation in the ITS G5A and ITS G5B medium; report on cross layer dcc algorithms and performance evaluation,” *ETSI TS 101 612 V1.1.1*, 2014.

[40] “Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part,” *ETSI TS 102 687 V1.2.1*, 2018.

[41] S. Kuk and H. Kim, “Preventing unfairness in the ETSI distributed congestion control,” *Communications Letters, IEEE*, vol. 18, no. 7, pp. 1222–1225, 2014.

[42] A. Autolitano, C. Campolo, A. Molinaro, R. M. Scopigno, and A. Vesco, “An insight into decentralized congestion control techniques for VANETs from ETSI TS 102 687 V1. 1.1,” in *Wireless Days (WD), 2013 IFIP.* IEEE, 2013, pp. 1–6.

[43] D. Eckhoff, N. Sofra, and R. German, “A performance study of cooperative awareness in ETSI ITS G5 and IEEE WAVE,” in *2013 10th Annual Conference on Wireless On-Demand Network Systems and Services, WONS 2013*, August 2013, pp. 196–200.

[44] S. Subramanian, M. Werner, S. Liu, J. Jose, R. Lupoaie, and X. Wu, “Congestion control for vehicular safety: synchronous and asynchronous mac algorithms,” in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications.* ACM, June 2012, pp. 63–72.

[45] C. B. Math, A. Ozgur, S. H. de Groot, and H. Li, “Data rate based congestion control in V2V communication for traffic safety applications,” in *2015 IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, November 2015, pp. 1–6.

[46] S. Yang, H. Kim, and S. Kuk, “Less is more: need to simplify ETSI distributed congestion control algorithm,” *Electronics Letters*, vol. 50, no. 4, pp. 279–281, February 2014.

[47] A. A. Gómez and C. F. Mecklenbräuker, “Dependability of decentralized congestion control for varying vanet density,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 9153–9167, January 2016.

[48] B. Cheng, A. Rostami, M. Gruteser, J. B. Kenney, G. Bansal, and K. Sjoberg, “Performance evaluation of a mixed vehicular network with CAM-DCC and LIMERIC vehicles,” in *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM).* IEEE, July 2015, pp. 1–6.

[49] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, “Modeling prioritized broadcasting in multichannel vehicular networks,” *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, 2012.

[50] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 2, pp. 245–257, 2011.

[51] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, M. Zhang, J. Rowe, and K. Levitt, “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” *IEEE Communications Magazine*, vol. 53, pp. 126–132, June 2015.

[52] O. Punal, C. Pereira, A. Aguiar, and J. Gross, “Experimental characterization and modeling of RF jamming attacks on VANETs,” *Vehicular Technology, IEEE Transactions on*, vol. 64, no. 2, pp. 524–540, 2015.

[53] “Intelligent transport systems (ITS); V2X applications; part 1: Road hazard signalling (RHS) application requirements specification.” *ETSI TS 101 539-1 V1.1.1*, 2013.

[54] A. A. Alam, A. Gattami, and K. H. Johansson, “An experimental study on the fuel reduction potential of heavy duty vehicle platooning,” in *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on.* IEEE, 2010, pp. 306–311.

[55] O. Punal, C. Pereira, A. Aguiar, and J. Gross, “Experimental characterization and modeling of RF jamming attacks on VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, February 2015.

[56] A. Alipour-Fanid et al., “String stability analysis of cooperative adaptive cruise control under jamming attacks,” in *2017 IEEE 18th Int. Symp. on High Assurance Systems Engineering*, 2017, pp. 157–162.

[57] G. Patounas et al., “Evaluating defence schemes against jamming in vehicle platoon networks,” in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, 2015, pp. 2153–2158.

[58] O. Puñal, I. Aktas, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on.* IEEE, 2014, pp. 1–10.

[59] L. Breiman, "Random forests," *Machine learning*, vol. 45, no. 1, pp. 5–32, 2001.

[60] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks," *IEEE Communications Letters*, vol. 18, no. 1, pp. 110–113, January 2014.

[61] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 5, pp. 823–839, May 2012.

[62] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-vehicle communication in C-ACC/platooning scenarios," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

Part II

Paper 1

Cooperative awareness in VANETs: on ETSI EN 302 637-2 performance

Authors:
Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Boris Bellalta

Reformatted version of paper originally published in:
IEEE Transactions on Vehicular Technology.

Cooperative awareness in VANETs: On ETSI EN 302 637-2 performance

Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Boris Bellalta

Abstract

Cooperative awareness on the road is intended to support the road users by providing knowledge about the surroundings and relies on the information exchange enabled by vehicular communications. To achieve this goal the European Telecommunication Standard Institute (ETSI) delivered the standard EN 302 637-2 for Cooperative Awareness Messages (CAM). The CAM triggering conditions are based on the kinematics of the originating vehicle, which is checked periodically. In this paper, we show that the standardized ETSI protocol may suffer a decrease in communication performance under several realistic mobility patterns. The potential influence of the discovered phenomena on the IEEE 802.11p Medium Access Control (MAC) operation is studied.

1 Introduction

Intelligent Transport Systems (ITS) are aiming to provide innovative services related to different modes of transport and traffic management, and enable various users to be better informed and make safer, more coordinated and smarter use of transport networks [1]. This is supposed to be achieved by integrating telecommunications, electronics and information technologies with transport engineering in order to plan, design, operate, maintain and manage transport systems. Cooperative-ITS (C-ITS) supports connectivity between road users. Road users in this context are all kind of road vehicles like cars, trucks, motorcycles, bicycles or even pedestrians, and roadside infrastructure equipment [2]. Thus, C-ITS is an important component of Intelligent Transportation Systems and aim at increased road safety, efficiency and driving comfort.

To enable inter-vehicle communications in the Dedicated Short Range Communications (DSRC) 5.9 GHz band, IEEE 802.11p, which is currently integrated into the recent IEEE 802.11-2012 standard, has been introduced by the Institute of Electrical and Electronics Engineers (IEEE). IEEE 802.11p provides the medium access control (MAC) and physical (PHY) layers for wireless communications in a vehicular environment. The IEEE 1609 working group has defined the protocol stack IEEE 1609.x, also known as WAVE (Wireless Access in Vehicular Environment). The scope of these standards is the extension of the IEEE 802.11p MAC layer functions for multi-channel operation as well as the specification of the upper layers, functionality in security and management planes.

At the same time, European Telecommunication Standard Institute (ETSI) delivered the first release of the C-ITS standards under the European Commission Mandate

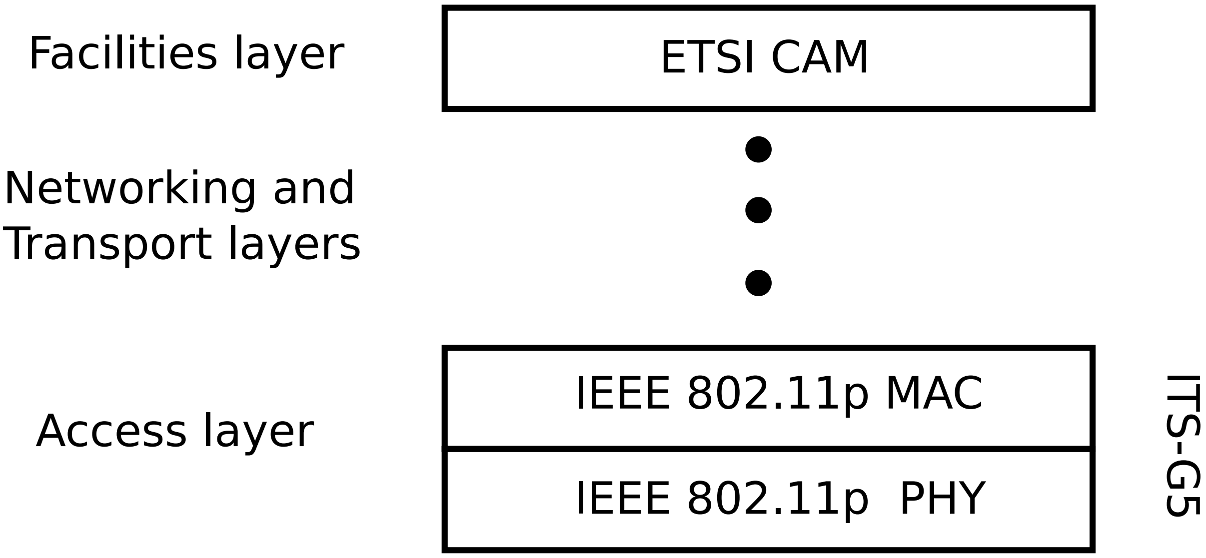


Figure 1: ITS-G5 reference architecture

M/453. ETSI specified the first set of ITS-G5 communication protocols and architecture regulating operation in the 5 GHz spectrum for C-ITS, Fig. 1. ITS-G5 reuses the IEEE 802.11p physical and data-link layers of the IEEE 1609 framework. ITS-G5 also defines protocols to support cooperative awareness of road users, which is intended as the basis for a number of road safety and traffic efficiency applications [3]. It is achieved by regular exchange of information among road users. ETSI defines the cooperative awareness within road traffic in terms of when road users and roadside infrastructure are informed about each other's position, kinematics and attributes. To enable cooperative awareness within ITS-G5, ETSI delivered the EN 302 637-2 standard defining Cooperative Awareness Messages (CAMs) [2]. Note, that Cooperative Awareness basic service is mandatory for all kind of ITS-stations (ITS-S) operating in ITS-G5. Each ITS-S puts kinematic data and other related data into periodically sent CAMs. The content of the message may vary depending on the type of ITS-S. In this paper we focus on the cooperative awareness on the road and the vehicles as ITS-S.

EN 302 637-2 defines a kinematically-driven mechanism that controls CAM triggering. This means, that each vehicle generates new CAMs depending on its current position, speed and direction. A vehicle compares its current kinematic measurements with the ones it put into the last generated message and, if the difference between them is above pre-defined thresholds, the vehicle triggers next CAM transmission. The reason for this is to allow the vehicle to trigger more messages when its behavior is highly dynamic and vice versa. In other words, a vehicle transmits fewer messages when its behavior is predictable, and more messages when accelerating/decelerating, turning or driving at high speed. However, as a consequence, the ETSI CAM protocol has a behaviour that is much more difficult to analyze compared to traditional beaconing approaches that have a fixed frequency of message generation.

In this paper we study the communication performance of the EN 302 637-2 CAM mechanism under realistic mobility patterns for both autonomous and human-driven vehicles. Specifically, we assume two scenarios: *Scenario 1.* platoon of autonomous vehicles where coordination is supported by exchanging CAMs, and *Scenario 2.* string of human driven vehicles approaching a traffic light while exchanging CAMs to support cooperative awareness.

The contribution of this paper is threefold:

- The phenomenon of message synchronization in the time domain in adaptive beaconing relying on speed variation tracking of originated ITS-s is theoretically analyzed.
- The performance of the ETSI EN 302 637-2 standard is evaluated by considering two typical mobility patterns (autonomous vehicles and human-driven vehicles approaching a pedestrian crossing). The negative impact of the synchronization of CAM generation moments (initially found in [4, 5]) is further discussed, analyzed and evaluated.
- The influence of various ETSI EN 302 637-2 parameters in the synchronization of CAM generation moments is studied, and recommendations on how to mitigate the negative effect of CAM synchronization are given.

The manuscript is organized as follows. Section 2 overviews the related work. Section 3 summarizes the studied current ITS-G5 standardization activity. In Section 4, we describe the system model, including the principal assumptions about the inter-vehicle communication and vehicles' mobility. Section 5 explains the discovered phenomena of CAM synchronization. In Section 6, we propose a theoretical framework to evaluate the influence of the discovered CAM synchronization effect on communication performance. In Section 7, we demonstrate the influence of CAM synchronization on typical mobility patterns for both autonomous and human-driven vehicles under different ETSI EN 302 637-2 parameters setup. Conclusions are presented in Section 8.

2 Related work

Here we overview the most relevant (in terms of our study) state-of-the-art research into adaptive beaconing in C-ITS.

In [6] the authors provide an extensive survey of adaptive beaconing for C-ITS. They provide a taxonomy of adaptive beaconing approaches, summarize performance metrics used for their design, and present their qualitative comparison.

In [7] the authors propose an ATB (Adaptive Traffic Beacon) adaptive beaconing protocol for C-ITS that adapts its beacon generation rate based on two metrics - channel quality and message utility. To estimate channel quality, the authors propose the use of collision statistics collected by the ITS-S, the Signal to Noise Ratio (SNR) levels measurements, and the number of neighboring ITS-S. Message utility is expressed through message age and beacon target dissemination range. Adaptive beaconing for enhancing the cooperative awareness by minimizing the tracking error of ITS-s is presented in [8]. The simulation results presented in the paper demonstrate that the proposed protocol outperforms ETSI CAM beaconing, supporting the lower figures of ITS-S tracking error. In [9], a Dynamic Beaconing Scheduling (DBS) adaptive beaconing approach based on the current kinematics of the ITS-S is presented. The beacon generation interval is proportional to the speed of the originating ITS-S: the higher the speed, the lower the beacon generation interval. The main idea of the proposed protocol is very similar to ETSI CAM kinematic rules, however, the authors do not provide any comparison of the performance of DBS and CAM. The adaptive beaconing protocol AND (Adaptive Neighbor Discovery) is presented in [10] and controls the beacon generation interval in order to maximize the discovery rate of the neighboring ITS-S in the specified road area. The simulation experiment performed by the authors shows that AND outperforms ETSI CAM in terms of ITS-S discovery accuracy at higher channel noise levels, while demonstrating similar performance when packet loss rates are low. In [11] the authors propose FABRIC (Fair Adaptive Beaconing Rate for Intervehicular Communications) - an algorithm that enables fair beaconing rate assignment for ITS-S. In FABRIC the transmission rate of each ITS-S in the one-hop neighborhood is recursively optimized. To enable this, it is assumed that all ITS-S share its beacon generation rate. The set of simulation experiments presented in the paper demonstrates that FABRIC has a fast convergence to fair beacon generation rate even in a highly dynamic environment.

ETSI CAM beaconing is an example of adaptive beaconing design for C-ITS to enable cooperative awareness in the vehicular environment. To adapt the CAM generation rate it adjusts the beaconing rate based on the current kinematics of the originating ITS-S.

Many studies on cooperative awareness either ignore ETSI kinematic rules [12, 13, 14] or implement the CAM protocol according to the standard, but do not focus on its performance. The evaluation of CAM beaconing under various parameter sets is performed in [15, 16, 17, 18]. In [19], the authors evaluate the CAM rules to understand the actual beaconing rate and corresponding channel load in a highway scenario. In [20], the authors present a more detailed study of the ETSI CAM kinematic rules. They attempt to find optimal parameters thresholds to enhance the network performance in terms of packet delivery ratio (PDR), channel load and message age.

Very few studies focus on assessing the effectiveness of the rules proposed by ETSI for CAM generation. In [21] the applicability of ETSI EN 302 637-2 to support platooning was studied. The main conclusion was that CAM may support cooperative autonomous driving, while having gaps in application functionality: support of platooning merging/disaggregation, and, importantly, the lack of an appropriate authentication mechanism that can be used for secure platooning aggregation. The study concludes that improvements of the CAM data structure are necessary.

The authors of [22] present results of an extensive measurement study estimating the performance of CAM cooperative awareness in terms of neighborhood awareness ratio and packet delivery rate. The paper provides substantial results on CAM ability to support awareness at a certain level depending on various factors (environment, transmission power level, beaconing generation frequency, etc.). However, they discuss the results in terms of averaged performance metrics and do not focus on the functioning of the CAM generation mechanisms itself.

In [4, 5] the negative effect of CAM synchronization in a platooning scenario was identified. It was shown that in a string of vehicles under synchronous acceleration/deceleration maneuvers CAM generation times may synchronize and lead to an increase of the CAM collision rate. The current study examines the side effect under typical mobility patterns of autonomous and human-driven vehicles within various sets of CAM parameters. We evaluate the strength of such an effect under various conditions and give recommendations on how it may be avoided.

3 Standardization

3.1 ETSI EN 302 637-2

The process of triggering CAMs is controlled by the Cooperative Awareness Basic Service [2] and can be described as follows[1]. The time between two consecutive generated CAMs is controlled within:

- $T_{\min} = T\_GenCamMin$ =100 ms (all the notions used throughout the paper are summarized in Table 1), which is an upper bound corresponding to the maximum CAM generation rate of 10 Hz. The time between two consecutive CAMs shall not be less than $T_{\min}$.
- $T_{\max} = T\_GenCamMax$ =1000 ms, which is an upper bound corresponding to the minimum CAM generation rate of 1 Hz.

Within these bounds CAMs shall be generated depending on the vehicle's kinematics. A vehicle repeatedly every $\Delta = T\_CheckCamGen$ checks the deviation of its current speed, position and direction from the measurements that have been placed in the last triggered CAM. We refer to $1/\Delta$ as the CAMs triggering sampling rate. A new CAM should be triggered if one of the following deviations has been observed:

- *"Event A"*: the absolute difference between the current position of the vehicle and its position included in the previous CAM exceeds $d_{\min}$=4 m;
- *"Event B"*: the absolute difference between the current speed and the speed included in the previous CAM exceeds $v_{\min}$ =0.5 m/s;
- *"Event C"*:[2] the absolute difference between the current direction of the vehicle and the direction included in the previous CAM exceeds 4°.

---

[1] Subsequently, CAMs transmission could also be influenced by the ETSI Decentralized Congestion Control (DCC)[23]. *However, throughout of this paper DCC is not considered.* We exclude DCC to focus on the CAM synchronization effect only and make the analysis presented in the paper easier and more self-explanatory.

[2] Event C is not considered in the paper, since we assume that the vehicles move along a straight route or change its direction slowly. Nevertheless, all the presented considerations and conclusions are valid also in case Event C might occur.

The CAM shall be triggered if the time elapsed since the last CAM generation is greater than or equal to $T_{\max}$. Finally, we set N_{GenCam}, i.e. the number of subsequently triggered CAMs with a fixed current period after kinematic event is detected, to be equal to 1.

3.2 IEEE 802.11p MAC

IEEE Std 802.11 offers several PHY layers and one common MAC sub-layer. At the same time, ETSI delivered the ITS-G5 standard that specifies the two lowest layers to enable vehicle-to-vehicle communications in an ad-hoc network [24]. As mentioned above, the ITS-G5 standard is reusing the IEEE 802.11p MAC and PHY layers, Fig. 1.

In IEEE 802.11p, ITS-S accesses to the media is controlled by the CSMA/CA (Carrier sense multiple access with collision avoidance) function. Before each transmission, a station picks up a random BO (backoff) value from the $[0, W]$ range. Provided the channel remains idle in the current time-slot, the BO value is decremented. The transmission starts when the BO value turns to zero. If the station identifies the channel as busy, it "freezes" the current BO value and starts to decrement it again after it detects the end of the ongoing transmission on the channel. Note that CAM is a broadcast message, which means that no acknowledgment or retransmissions are considered during its exchange.

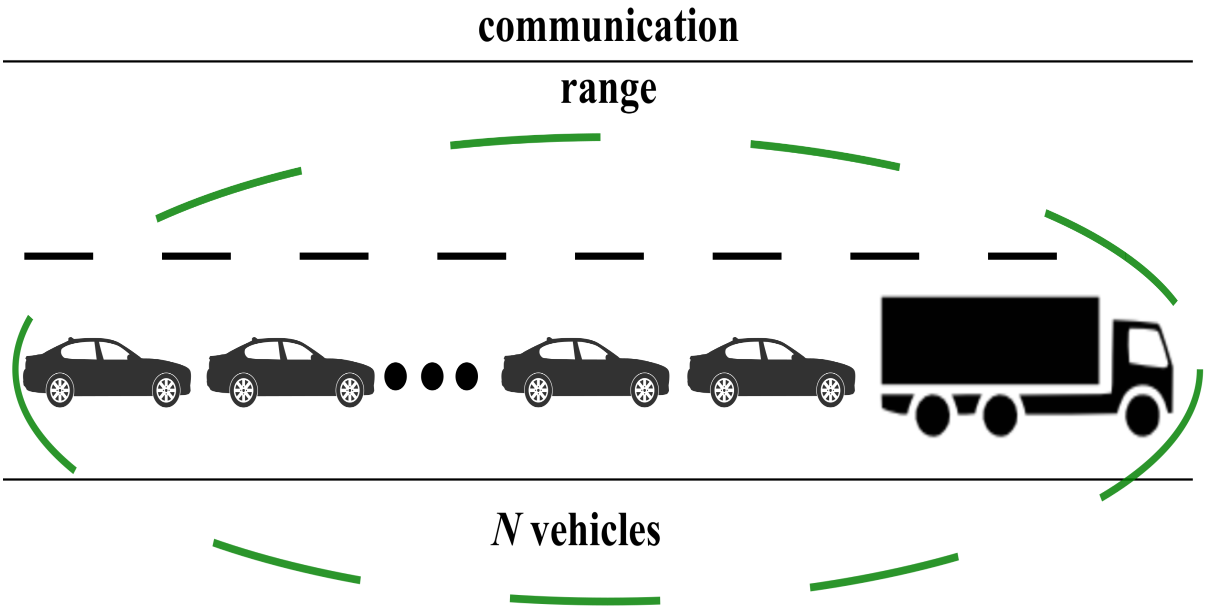


Figure 2: Platooning (Scenario 1)

Table 1: Main Notations

Parameter	Value	Meaning
Δ	–	CAM sampling period
$d_{\min}$	4 m	*"Event A"* threshold
$v_{\min}$	0.5 m/s	*"Event B"* threshold
W	16	contention window size
$AIFS$	110 μs	arbitration inter-frame spacing
$T_{\min}$	100 ms	minimum time allowed between two consecutive CAMs
$T_{\max}$	1 s	maximum time allowed between two consecutive CAMs
N	25	number of vehicles in the caravan
σ	13 μs	IEEE 802.11p *aTimeSlot*
V_{stb}	25 m/s	stable speed in the disturbance scenario
V_{low}	–	low speed in the disturbance scenario
D	–	platoon desynchronization factor
v	–	current speed of the vehicle
t	–	current time value
t_i	–	time when the most recent CAM was generated by the i-th vehicle
V_i	–	speed of the i-th vehicle at time t_i
t_{event}	–	actual time either *"Event A"* or *"Event B"* occurred
τ	–	period with which the vehicle triggers CAMs when moving at a constant speed
T_{CAM}	–	CAM transmission duration
$Q(m)$	–	probability density function (PDF) of the number of groups containing exactly m vehicles
$Q^{*}(m)$	–	empirical $Q(m)$
R	3 Mbit/s	datarate
L	400 bytes	length of CAM message

4 System model

In this study we focus on the following two mobility scenarios, representing the cases of both autonomous and human-driven caravans of vehicles on the road.

To support coordination and awareness between vehicles on the road, each vehicle

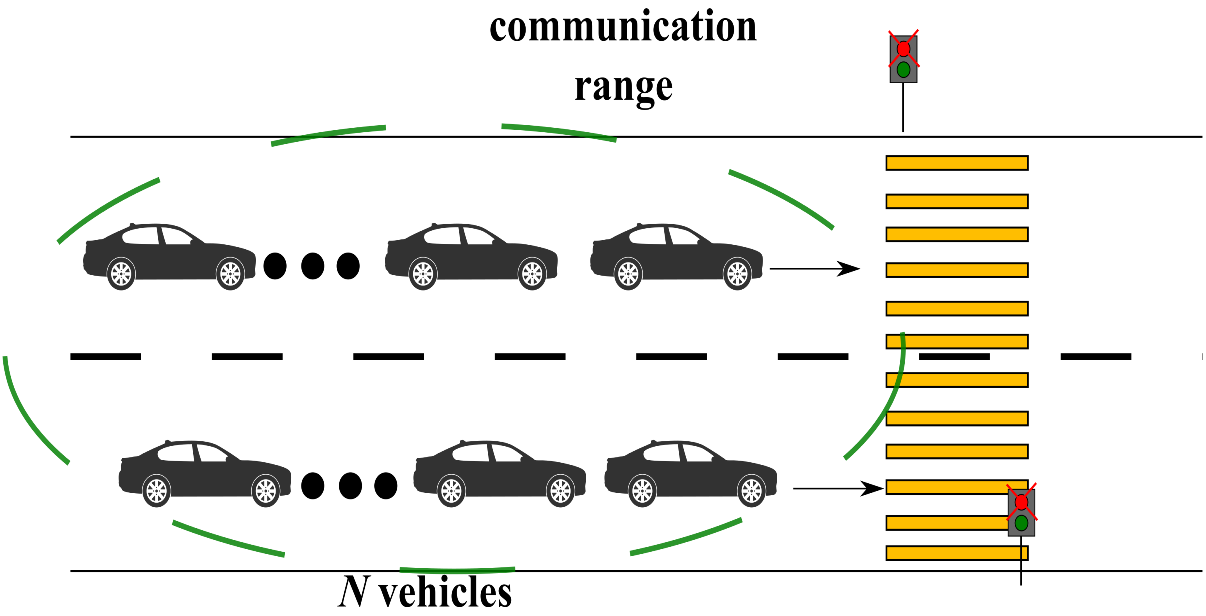


Figure 3: Traffic jam (Scenario 2)

executes the following steps:

- Generate CAMs in accordance with the ETSI EN 302 637-2 specification [2].
- Transmit CAMs on a dedicated channel in accordance with the IEEE 802.11p MAC specification [25].

4.1 Scenario 1: platooning

In this scenario we consider a platoon of CACC-enabled (Cooperative Adaptive Cruise Control) vehicles moving on a highway. In platooning/CACC the leading vehicle is driven by a human driver, while the following vehicles automatically maintain the velocity of the leading one, but their directions are still controlled by the drivers. Platooning aims to reduce the air-drag in the caravan of heavy-duty vehicles, which could significantly improve fuel consumption, while CACC contributes mainly to the driving experience by enabling comfort through semi-autonomous driving [26]. Since, in terms of the focus of this study, there is no difference between the discovered phenomena for CACC and platooning, we refer henceforth to this class of applications as *platooning*. The cooperation between the vehicles in the platoon is achieved by the frequent exchange of periodic broadcast messages, which we refer to as *beacons*. CAMs are European implementation of the beacons for ITS-G5. CAMs may contain various related information like the vehicle's ID and kinematic information for a vehicle, such as its current speed, position, direction, etc.

In the scenario shown in Fig. 2, the leading vehicle decelerates from the desired steady speed ($V_{\mathrm{stb}} \sim 90$ km/h) to a lower speed ($V_{\mathrm{low}} \sim 60$ km/h), maintains this speed for some time, and then accelerates back to the initial speed, see Fig. 4. This disturbance scenario could be regarded as a pattern to describe the appearance of a slow moving vehicle in front of the platoon (coming from another lane or a metering ramp) or a road speed limit.

We consider a platooning system consisting of N vehicles, where the leading vehicle is driven by a human driver, while the remaining $N-1$ vehicles are following automatically. On the basis of our previous works [27, 4, 5], the following assumptions are made in the present study:

- All the vehicles in the platoon are within each other's communication range. This is a valid assumption since for the inter-vehicle distance of 7 m, which for 20–25 vehicles results in a maximum platoon size as of 300 m when the car length is 5 m, and less than 500 m when the truck size is 13 m. A recent measurement exercise (see Fig. 4, [28]) shows that in a convoy of vehicles moving on a highway, exploiting IEEE 802.11p transceivers in the 5.9 GHz band, the communication range, where ITS-S experiences confident packet reception, is at least 500 m.

- We assume noise-free channel and exclude the complementary influence of the CAM losses caused by channel impairments, since they would have no impact on the CAM synchronization effect, which is our focus.

- The kinematic parameters of the leading vehicle are modeled via the intelligent driver model (IDM) state-of-the-art car-following mobility model [29].

- Since in reality vehicles in the platoon are not perfectly synchronized in their maneuvers, i.e., to assess the influence of the CAM synchronization in a more realistic setup, we add disturbance in the coordination between vehicles in the platoon. Random deviations in the velocities of the following vehicles with respect to the leading one are modeled by applying the following approach: we add a uniformly distributed random delay $\delta \sim uniform[0, D \cdot \sigma]$ to a CAM generation moment in order to reflect the non-perfect synchronization between their velocities, where D is the maximum delay expressed in $\sigma = aTimeSlot$ ($aTimeSlot$ is defined in the standard [25]). We refer to D as a *desynchronization factor*.

4.2 Scenario 2: traffic jam

In this scenario, we consider a set of vehicles moving on the road with no coordination between them, while still exchanging CAM messages, Fig. 3. According to [2] *"The Cooperative Awareness (CA) basic service is a mandatory facility for all kind of ITS-Stations (ITS-S), which take part in the road traffic"*. In other words, all the vehicles equipped with DSRC must participate in the CAM exchange. By analogy with scenario 1 in this paper, we focus on the disturbance scenario described above. In case of scenario 2, the disturbance scenario emulates a string of vehicles approaching traffic lights. In the situation where the lights switch to red, the vehicles closest to the intersection at the road lanes start to decelerate roughly at the same time. Vehicles decelerate until they

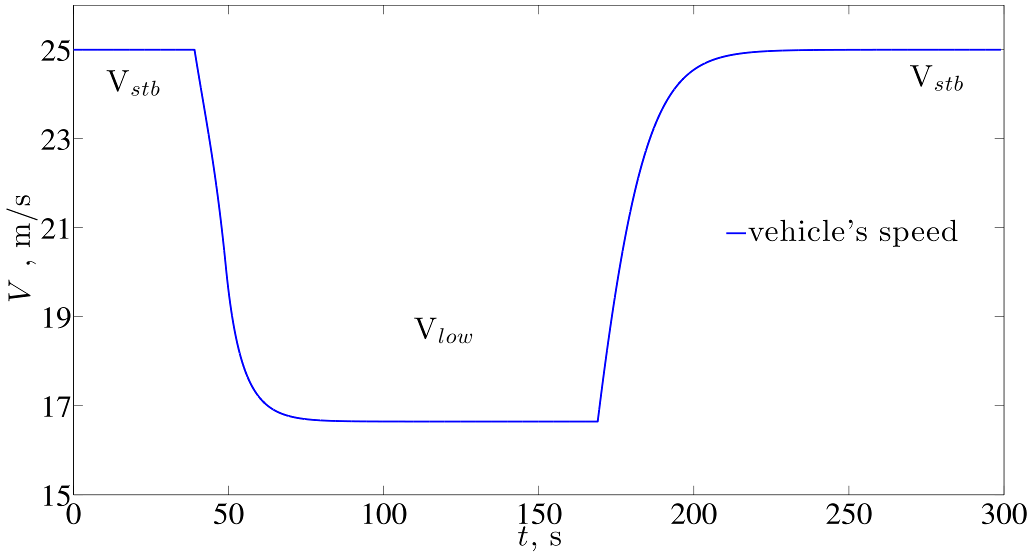


Figure 4: Platoon speed variations due to a temporary obstacle as modeled via the CAH model with recommended comfort parameters [29] (Example 1)

completely stop at the intersection, wait until the lights turn green and accelerate again to cross the intersection. Thus, in this scenario vehicles again follow the disturbance scenario shown in Fig. 4, with $V_{\text{low}} = 0$ km/h. Note that, since the vehicles have human drivers without any additional coordination between them, each vehicle behind starts to decelerate with some delay caused by the driver's reaction time, inter-vehicle gap, etc.

In this scenario we consider several vehicles moving on a multi-lane road. All the vehicles are equipped with transceivers and periodically broadcast CAMs. The assumptions in scenario 2 are as follows:

- All the vehicles are within the same communication range, e.g., we consider 500 m distance prior to the traffic lights, assuming the IEEE 802.11p communication range is in the order of 400–500 m.

- First vehicles on the road lanes (those that are closest to the traffic lights) react to the stoplight simultaneously, while the rest of the vehicles in the lane following them have no C-ITS-enabled coordination.

- The kinematic parameters of all the vehicle are modeled independently via the IDM mobility model.

5 Identified phenomena: synchronized generation of CAMs

5.1 Discovery of the phenomenon in system-level simulations

To illustrate the appearance of the CAM synchronization phenomenon and its negative impact we first set up a platooning experiment in the Plexe/Veins simulation environment [30]. Plexe is a detailed state-of-the art system level platooning simulator which incorporates tightly-coupled mobility, automatic control and communication components. We simulate a platoon of $N = 15$ vehicles enabled by CAM exchange enabled by ETSI EN 302 637-2. The platoon moves along the straight stretch of a highway with a target speed for the leading vehicle $V_{stb} = 27.7$ m/s ($\sim$ 100 km/h). Each vehicle in the platoon adapts its speed based on the kinematic information received from the platoon leader and the preceding vehicle. We use a longitudinal control algorithm based on the sliding surface method of the controller design presented in [31]. Two additional slower vehicles are inserted in front of the platoon at simulation time 200 s and 286 s, Fig. 5. Thus, the platoon approaches slower vehicles and performs appropriate acceleration or deceleration maneuvers according to the disturbance scenario.

Results presented in Fig. 5 provide us with an evidence that the CAM collisions before maneuver are very unlikely to appear. However, after the platoon decelerates and accelerates the number of collisions observed grows significantly. From this we can conclude that certain mobility patterns may lead to a degradation in communication performance of the platoon enabled by CAM. Our hypothesis is that CAM messages of different vehicles become synchronized due to the operation of ETSI CAM kinematic triggering rules.

5.2 Explanation of the CAM synchronization phenomenon

To illustrate the phenomenon of CAM synchronization we study the stream of perfectly synchronized vehicles (all the vehicles in the stream perform acceleration/deceleration maneuvers simultaneously). This pattern could be considered as a perfect operation of a stream of CACC/platooning vehicles. Throughout this section we refer to this mobility pattern as platoon. We also set the value of the CAM sampling period to a very small value $\Delta = \sigma$ to allow vehicles to track precisely the occurrence of CAM kinematic events.

In the scenario shown in Fig. 4, the leading vehicle decelerates from the desired steady speed ($\mathrm{V}_{\mathrm{stb}} \sim 90$ km/h) to a lower speed ($\mathrm{V}_{\mathrm{low}} \sim 60$ km/h), maintains this speed for some time, and then accelerates back to the initial speed.

Proposition A. Let the platoon move with a constant speed v and each vehicle triggers CAMs periodically (with period $\tau = d_{\min}/v$) due to the occurrence of Event A. Consider a moment of time t when the kinematic parameters of the platoon change so that Event B occurs for some vehicles. Let $\{t_1, t_2, \ldots t_N\}$ denote the moments of time when the most recent CAMs were generated by each vehicle in the platoon by time t.

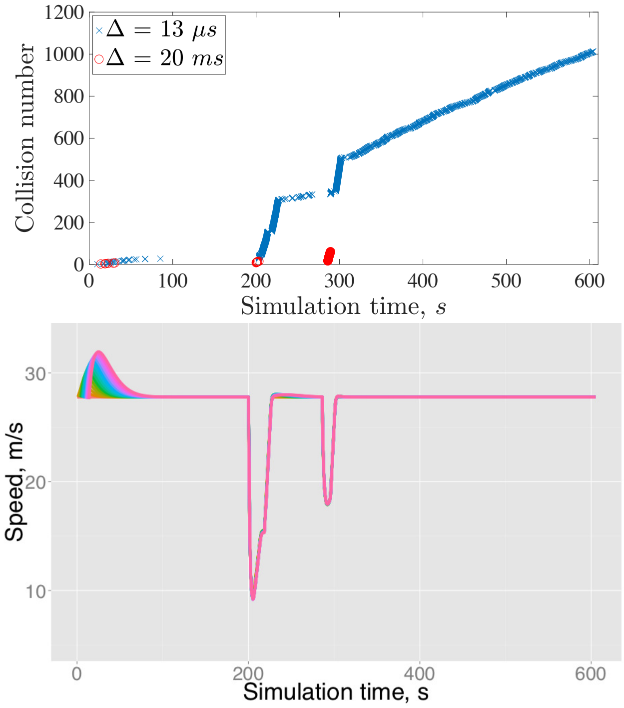


Figure 5: Dynamics of CAM collisions during the maneuvering of a platoon modeled in Plexe

Then all the vehicles, for which the condition

$$t - t_i \geq T_{\min}$$

holds, will generate a new CAM at time t.

Proof: Because $t - t_i$ is the time elapsed since the most recent CAM generation by the i-th vehicle, the proposition directly follows from the CAM triggering rules. ■

To illustrate the effect of possible CAM generation times synchronization, let us consider two examples.

Example 1: Let the platoon change its velocity, e.g., it temporarily slows down due to a reduced speed limit in a road construction segment or due to a slow vehicle ahead, Fig. 4.

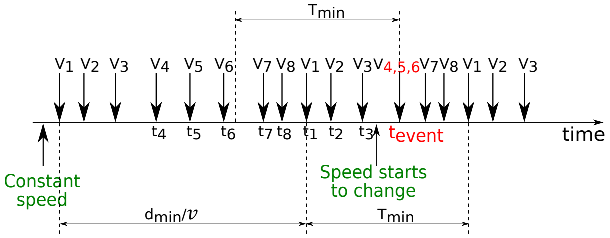


Figure 6: Synchronization of CAM triggering moments in the CACC/platoon due to the synchronous speed changes (Example 1)

Let us denote the CAM generation moments of the i-th vehicle as $t_1, t_2, \ldots t_N$ and corresponding speeds as $V_1, V_2, \ldots V_N$, Fig. 2. When the platoon moves at a constant speed of 90 km/h, each vehicle triggers a CAM every $d_{\min}/V_i$=160 ms due to the periodic occurrence of *Event A*.

Due to the deceleration, in a short time period the change in the platoon speed exceeds 0.5 m/s (*Event B*) and the vehicles with $t_{event} - t_i \geq T_{\min}$ (i.e., 4, 5 and 6) synchronously trigger their CAMs at time t_{event}. Other vehicles (i.e., 1, 2, 3, 7 and 8) trigger their CAMs as soon as the time elapsed since their most recent CAM generation turns to $T_{\min}$ =100 ms.

When the platoon speed stabilizes, the vehicles trigger CAMs with a constant period again (due to periodic occurrence of *Event A*).

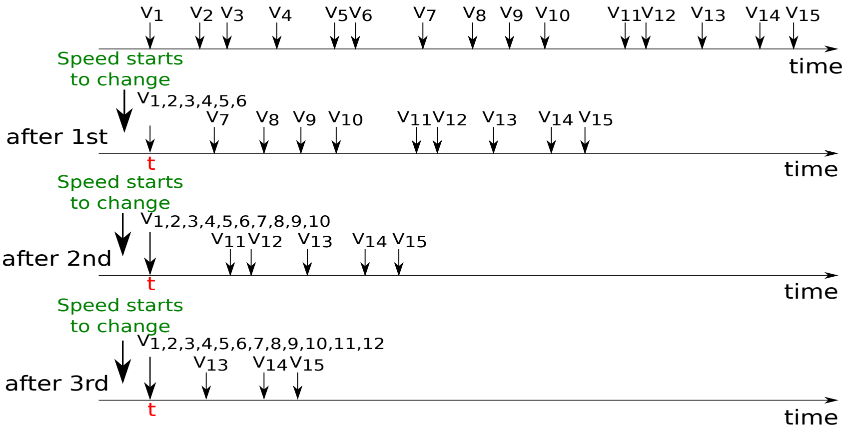


Figure 7: Increased synchronization of CAM triggering moments after several maneuvers (Example 2)

Example 2: Let the platoon slow down and accelerate several times, see Fig. 4.

Each platoon maneuver will influence the CAM triggering process according to the mechanism described in Example 1. More CAMs might become synchronized as long as more maneuvers are performed due to the concurrent occurrence of *Event B*. For example, in Fig. 5 CAMs from vehicles 7, 8, 9 and 10 and 11, 12 become synchronized with those from 1, 2, 3, 4, 5 and 6 after the 2^{nd} and the 3^{rd} maneuvers, respectively.

Notice, that when vehicles in a caravan are perfectly synchronized and Δ is small once the synchronization of CAMs triggering times has occurred, further accelerations/decelerations will not lead to desynchronization. *Event B* occurs simultaneously for all the synchronized vehicles, since their recent CAMs contain the same kinematic information.

6 Theoretical analysis

In Section 5 we explained the mechanism of CAM synchronization. Now we quantitatively characterize the discovered negative effect using:

- the mean number of the synchronized CAMs;

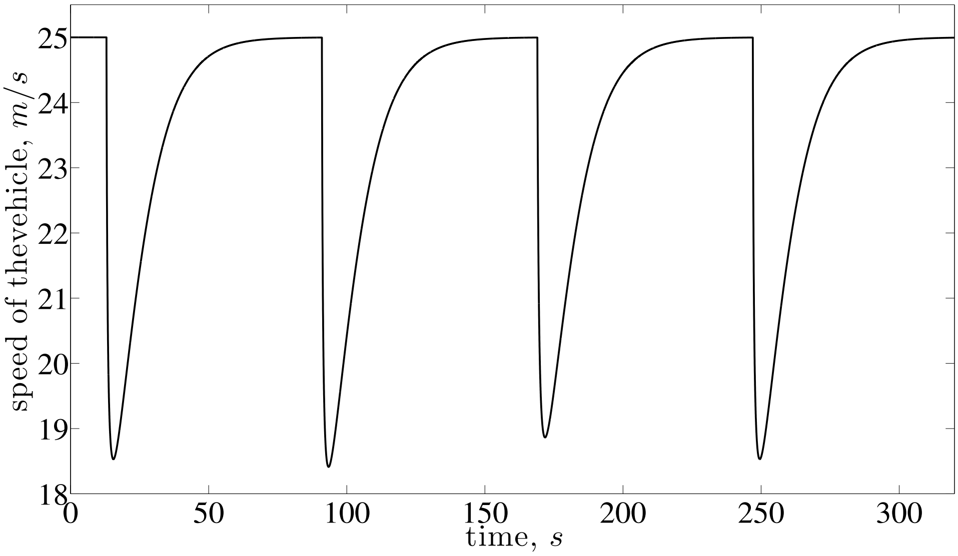


Figure 8: Platoon speed variations in few subsequent deceleration/acceleration maneuvers (Example 2)

- the empirical PDF of the number of vehicles with the synchronized CAMs.

The results presented in this Section might be applicable to any adaptive beaconing approach where the speed variations of the originating ITS-S are used to trigger CAMs.

6.1 Mean number of synchronized CAMs

Let us present a simple analytical model, that estimates the mean number of synchronized CAMs in a string of perfectly synchronous vehicles driving according to the disturbance mobility pattern. Note, that this assumption is adopted to derive the closed-form expression for the mean number of synchronized CAMs. To model the disturbance in the platoon coordination we have introduced a desynchronization factor D, which is used to relax this assumption in Section 7).

Proposition B. Let a platoon of size N move with at a constant speed υ during time interval $[0, t_{event})$. If *Event B* occurs at t_{event} (instantaneous speed variation exceeds $\upsilon_{\min}$), then the mean number of CAM generation moments synchronized at t_{event} is

$$\rho = \frac{\tau - T_{\min}}{\tau} \times N,$$

where $\tau = d_{\min}/\upsilon$.

Proof: Let the CAM generation moments of all the vehicles be enumerated and denoted as t_n, $n \geq 1$. The CAM generation moments in the interval $[0, t_{event})$ represent the following stochastic process:

- Due to the random and independent occurrence of the first CAM generation moment of each of the N vehicles, the $N-1$ intervals between pairs of subsequent CAMs of any N consecutive generation moments are exponentially distributed, i.e. $\forall n : t_{n+k} - t_{n+k-1} \sim exp(\tau/N)$, $k = \overline{1, N-1}$.
- Due to the periodic occurrence of *Event A*, all the vehicles generate CAMs with period τ, i.e. $\forall n : t_{n+N+1} - t_n = \tau$. Therefore, any time interval of duration τ, contains exactly N CAM generation moments (one per vehicle).

Due to the assumptions adopted in this Section, all N vehicles detect *Event B* simultaneously at t_{event}. However, due to the restriction on the value of the minimal possible CAM generation interval $T_{\min}$, only those vehicles, whose CAM generation moments belong to $[t_{event} - \tau, t_{event} - T_{\min})$, are triggered at t_{event}, Fig. 3. Taking into account the above properties of the considered stochastic process, the mean number of CAM generation moments in $[t_{event} - \tau, t_{event} - T_{\min})$ is $\frac{\tau - T_{\min}}{\tau} \times N$. ■

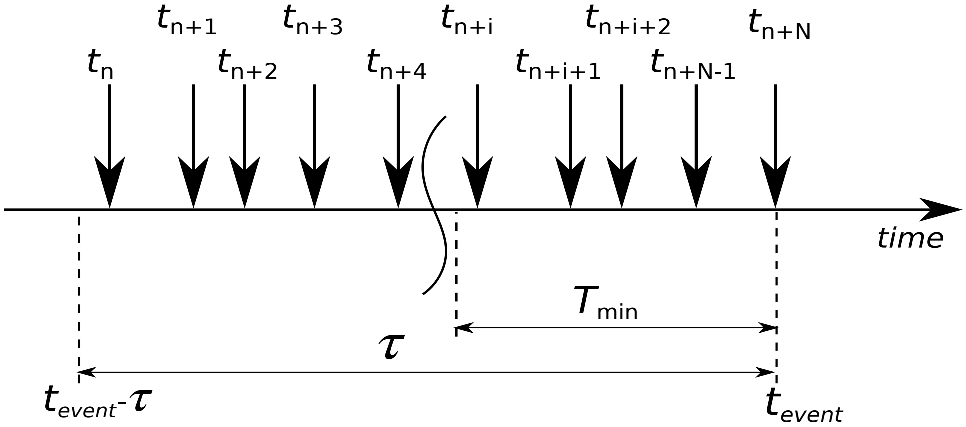


Figure 9: The fraction of the CAM triggering moments (leftside) become synchronized after t_{event}

6.2 Notion of groups

Transmission of CAMs generated as discussed above is governed by the IEEE 802.11p MAC protocol, which presumes that CAMs from different vehicles may collide due to their simultaneous generation. Synchronization of the CAM generation times does not make a collision inevitable in the same way that their desynchronized generations do not make collisions impossible [32], [25]. This phenomenon can be characterized using the notions of *groups*.

Let us consider a platoon moving at a constant speed with all the vehicles periodically triggering CAMs. Let us select a sequence of $t_i \leq t_{i+1} \leq t_{i+2} \leq \cdots \leq t_{i+N-1}$ CAM generation moments of each vehicle in the platoon such that CAMs from vehicles i and $i + N - 1$ cannot collide (formal proof is proposed in [27], p. 112).

Algorithm 1 CAMs Grouping Algorithm

```
 1: for $j \leftarrow 1, N$ do
 2:     $L_j \leftarrow 0$;
 3: end for
 4: $l \leftarrow i$;    $K \leftarrow 1$;
 5: while $l < i + N - 1$ do
 6:     $\Omega \leftarrow \{l\}$;    $m \leftarrow 1$;
 7:     while $T_{l+m} - T_l \leq m \times [\text{AIFS} + (W-1)\sigma] +$
        $+ (m-1) \times T_{\text{CAM}}$ do
 8:         $\Omega \leftarrow \Omega \cup \{l+m\}$;
 9:         $m \leftarrow m + 1$;
10:     end while
11:     $\Phi_K \leftarrow \Omega$;
12:     $L_m \leftarrow L_m + 1$;    $l \leftarrow l + m$;
13:     $K \leftarrow K + 1$;    $m \leftarrow 1$;
14: end while
```

One can execute Algorithm 1, where AIFS is the Arbitrary Inter-Frame Space, σ is a *aSlotTime*, W is the Contention Window [25] and T_{CAM} is the CAM transmission time. The outcome of the Algorithm operation is that all N vehicles are split into K sets denoted as Φ_k, $k = 1 \dots K$ and further referred to as *groups*. L_m is the number of groups consisting of exactly m vehicles.

Proposition C. The CAMs of vehicles belonging to different groups Φ_k $(k = 1 \dots K)$ cannot collide.

Proof: From the IEEE 802.11p backoff rules it follows that in the empty system two CAMs can never collide if their generation moments are spread in time for at least AIFS$+$ $(W-1)\sigma$, see line 7. When the CAMs are generated during the ongoing transmissions of other vehicles, the backoff counters freeze until the channel becomes idle. Respective maximum possible transmission delays are checked at line 7. ■

The PDF of the number of groups with m vehicles is defined as $Q(m) = Pr\{x = m\} = L_m/K$.

For analysis purpose, let us consider time intervals where the speed of the vehicle is constant, i.e., before any maneuvers and after each of the maneuvers (see Fig. 6).

Since the results presented in the paper were obtained using simulations, we will operate with Empirical PDF $Q^*(m)$ for the number of groups with m vehicles[3]. The results are obtained via simulations with standard IEEE 802.11p parameters as in [27].

7 Evaluation of the phenomena

In this Section we present the outcomes of our simulation study. First, we investigate a platoon enabled by inter-vehicular CAM exchange. We then discuss the influence of the

---

[3] For the sake of the plots clarity, the values of $Q^*(1)$ are not depicted.

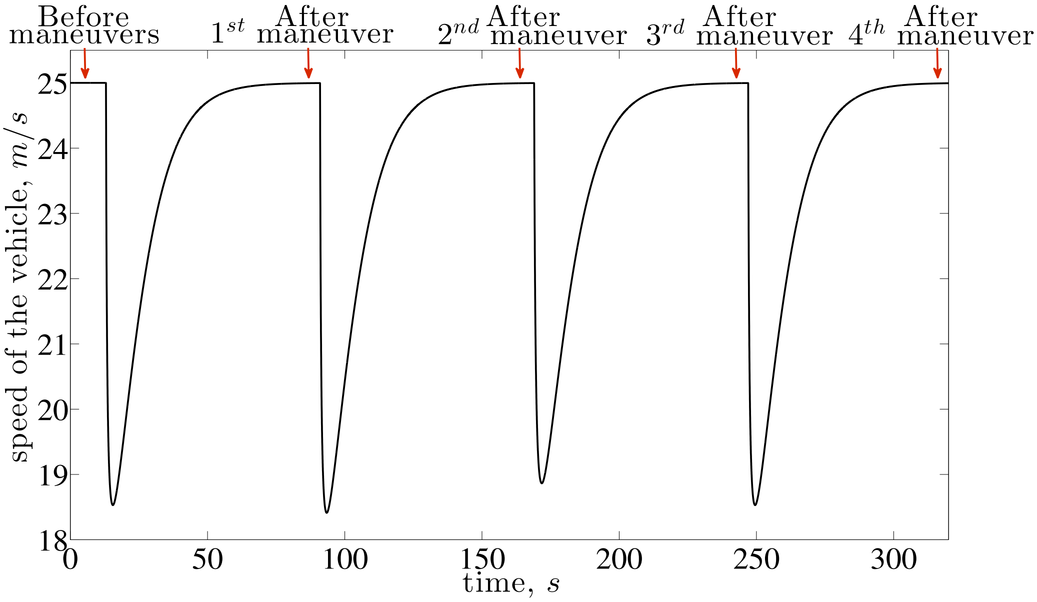


Figure 10: Reference moments (indicated by the arrows) at which the CAM performance is assessed

CAM synchronization effect on a string of human driven vehicles supporting cooperative awareness on the road. The parameters of the study are summarized in Table 1.

7.1 Scenario 1: platooning

In this scenario we independently study the influence of CAM sampling period (Δ) on the described synchronization effect first, and we assess the joint influence of Δ and the desynchronization factor (D) between vehicles in the platoon.

In the first set of simulations reported in Fig. 11, the value of Δ is set to be $\Delta = \sigma$. When the platoon demonstrates a synchronous behavior and the sampling rate is high, after each subsequent maneuver the time diversity between CAMs belonging to different vehicles continuously decreases. Thus, after the 4^{th} maneuver the CAMs belonging to almost all N platoon members are in the same group. Although the formation of a group does not necessarily result in a collision of CAMs, the number of groups and the vehicles in each group could be directly related to the actual CAM collision probability. Fig. 18 shows the result of CAM collision probability for several setups. After each maneuver with the decrease of time diversity, collision probability grows accordingly.

Figs. 12–15 demonstrate results when Δ is gradually increased. Increasing Δ decreases the strength of the effect accordingly. A larger value of Δ makes the reaction of platoon members to diverge in time. With the increase of Δ, a vehicle detects the occurrence of the events with uniformly distributed delays $uniform[0, \Delta\sigma]$ ms. Thus, platoon members register the event at different points in time (depending on their own time they perform sampling). As a result the time each vehicle triggers CAM transmission lies within $[t_{\text{event}}, t_{\text{event}} + \Delta\sigma]$, where t_{event} is the actual time when the message triggering event

Table 2: Simulation Parameters

Parameter	**Value**
Scenario 1	
N	25
Number of road lanes	1
V_{stb}	25 m/s (90 km/h)
V_{low}	18–19 m/s (65–68 km/h)
Δ	$1 \cdot \sigma$ – $1500 \cdot \sigma$
D	500
Scenario 2	
N	25 per lane
Number of road lanes	3
V_{stb}	16.7 m/s (60 km/h)
V_{low}	0 m/s
Δ	$1 \cdot \sigma$

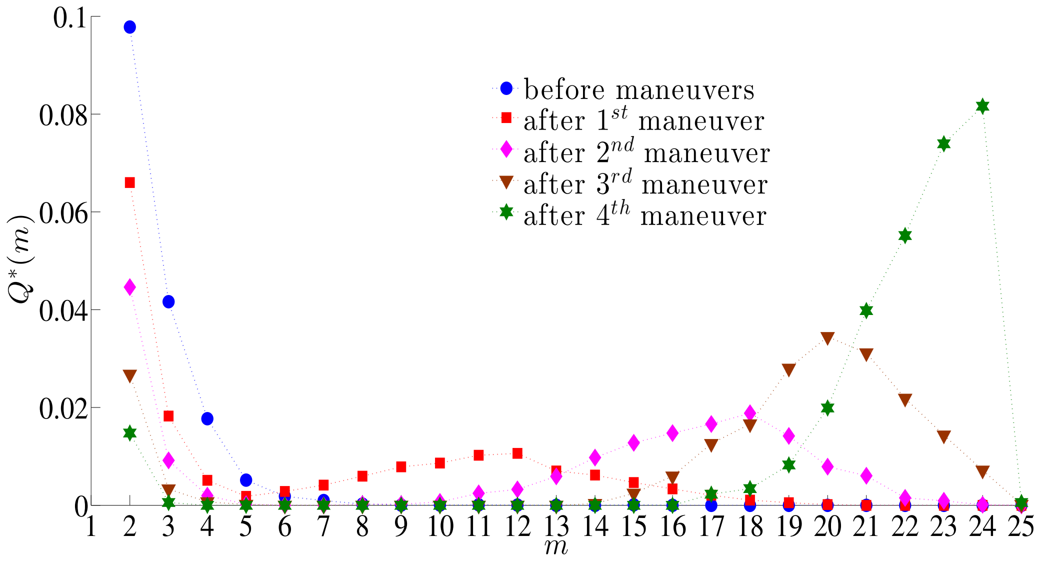


Figure 11: Influence of maneuvers on CAM generation moments when $\Delta = 1 \cdot \sigma$

occurs. The larger Δ, the larger the time interval during which all platoon members trigger their corresponding CAM. *Example:* when $\Delta = 1500\sigma$ (which corresponds to

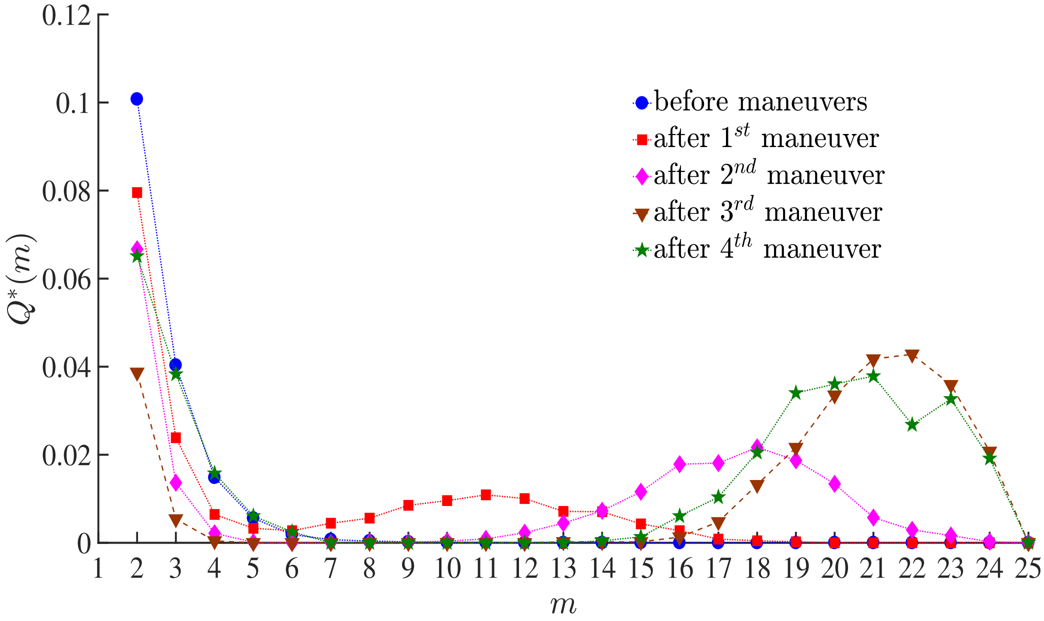


Figure 12: Influence of maneuvers on CAM generation moments when $\Delta = 100 \cdot \sigma$

$\sim$ 20 ms), each vehicle performs samplings approximately every 20 ms. This results in CAM transmission from each platoon member being triggered within 20 ms with some shift from actual t_{event}, which is caused by the random shift between the times each specific vehicle performs its samplings. At the same time, obviously, the increase of Δ results in increasing delays between a kinematic event and its registration.

Figs. 16–17 show the joint influence of sampling period Δ and the desynchronization factor of platoon members coordination on the discovered CAM synchronization effect. Our simulations show that possible disturbances in the coordination between platoon members can have a positive consequence, as it may significantly mitigate the CAMs synchronization phenomenon. From Figs. 16 and 18 one can conclude that large enough values of D may help to mitigate the CAMs synchronization effect significantly. Random disturbance acts in the same way as the random backoff mechanism in the CSMA/CA protocol, by actually, separating concurrent CAM generation in time, Fig. 18. In the case where CAMs were also diversified by larger Δ, an additional random desynchronization component can eliminate the CAM synchronization effect more or less completely, see figure 17.

Fig. 18 shows CAM collision probabilities for corresponding setups, presented on Figs. 11, 14, 16 and 17. It can be seen that the effect of synchronization of CAMs in time can be proportionally related to the actual CAM collision probability.

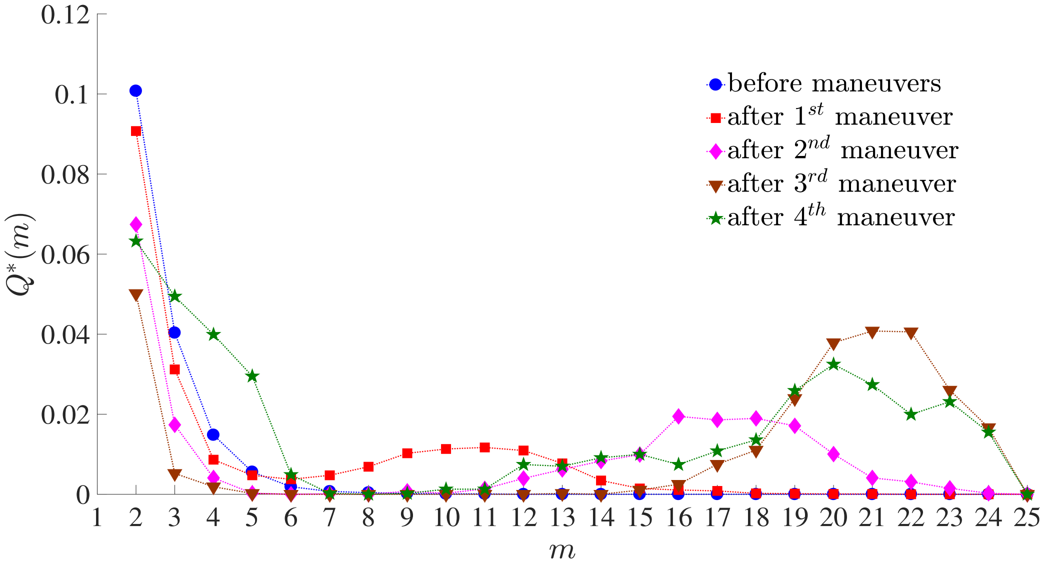


Figure 13: Influence of maneuvers on CAM generation moments when $\Delta = 200 \cdot \sigma$

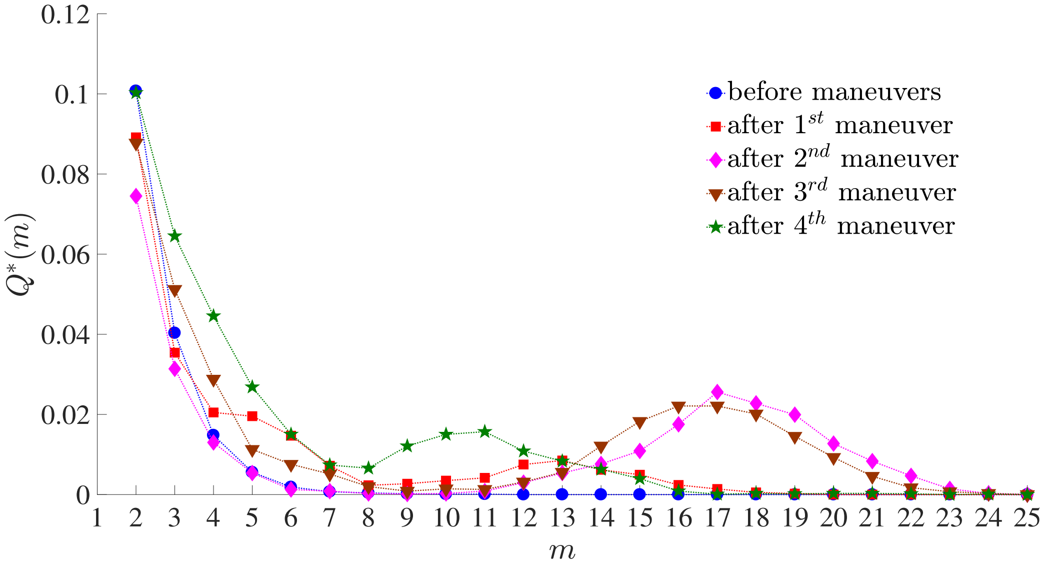


Figure 14: Influence of maneuvers on CAM generation moments when $\Delta = 500 \cdot \sigma$

7.2 Scenario 2: traffic jam

In this scenario we consider independently driven vehicles approaching the traffic lights. We consider a 3-lane road with N=25 vehicles in each lane (75 vehicles in total), following a disturbance speed scenario with $\mathrm{V}_{\mathrm{stb}} = 60$ km/h and $\mathrm{V}_{\mathrm{low}} = 0$ km/h. Vehicles broadcast CAMs according to [2]. To study the synchronization of the CAMs generation moments we plot a histogram, where we place CAM triggering times belonging to the vehicles in

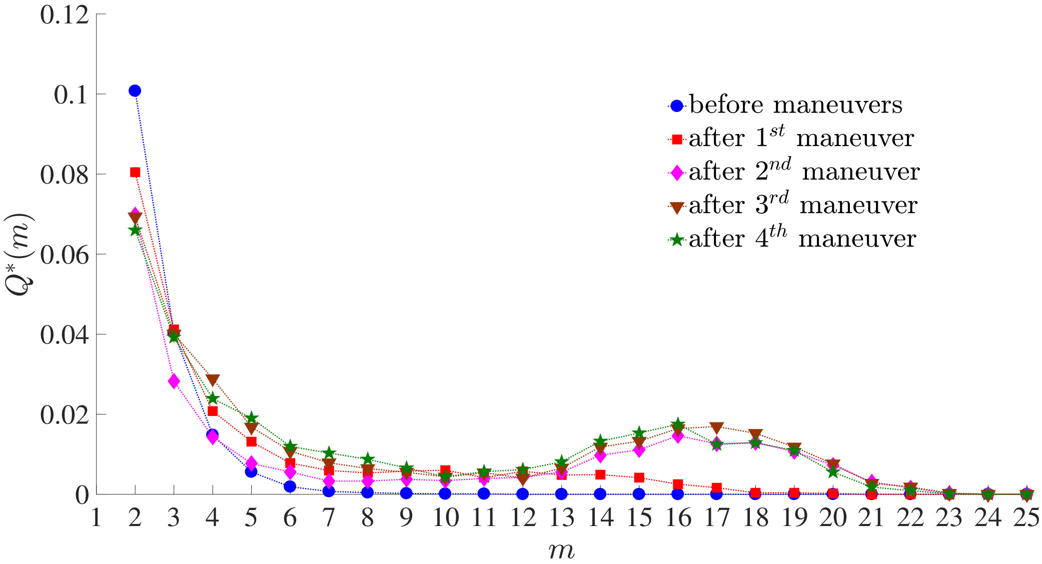


Figure 15: Influence of maneuvers on CAM generation moments when $\Delta = 1500 \cdot \sigma$

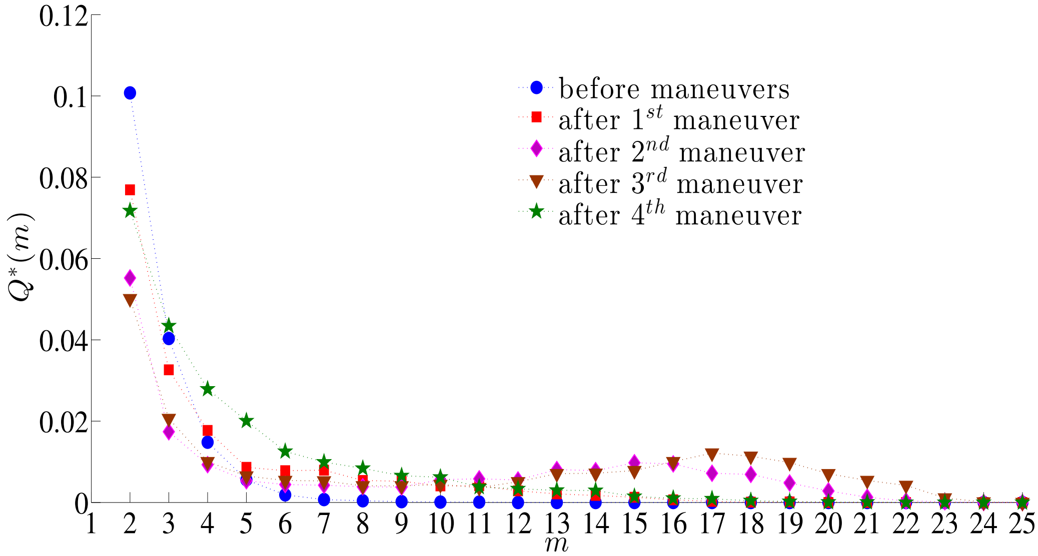


Figure 16: Influence of maneuvers on CAM generation moments when $\Delta = 1 \cdot \sigma$, $D = 500$

time bins of 5 ms each for the duration of 0.5 s. Following our approach, we show CAM synchronization after each subsequent maneuver, Figs. 19, 20, 21. As a benchmark for comparison, together with a plot for the corresponding maneuver, we also show the figure of CAM generation times before maneuvers. The simulations show that time diversity between CAM generation moments decreases after each subsequent maneuver, following the mechanism described in this paper. It is worth noting that in this scenario the strength of the CAM synchronization effect is noticeably lower due to the much higher

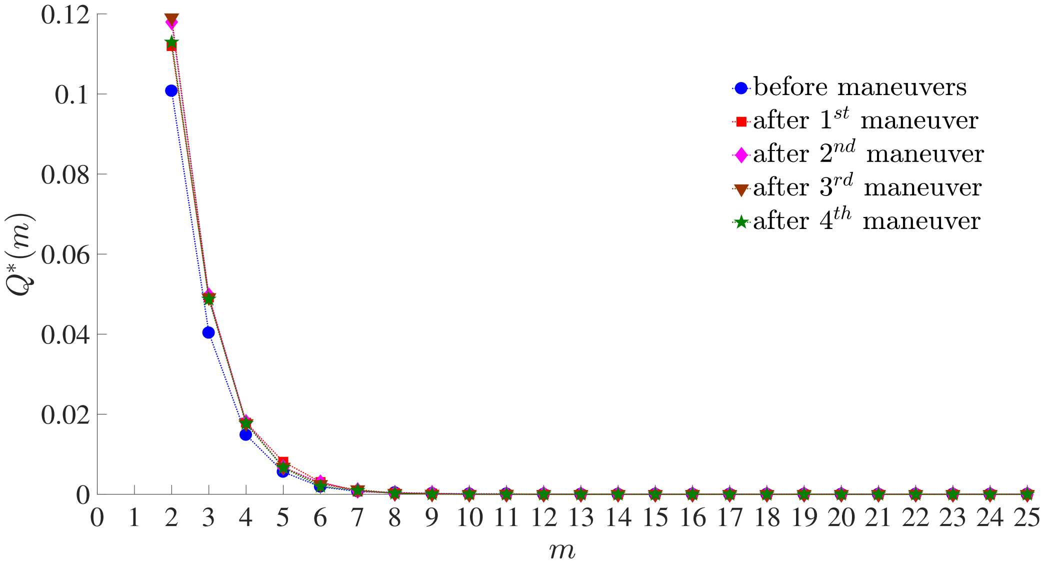


Figure 17: Influence of maneuvers on CAM generation moments when $\Delta = 200 \cdot \sigma$, $D = 500$

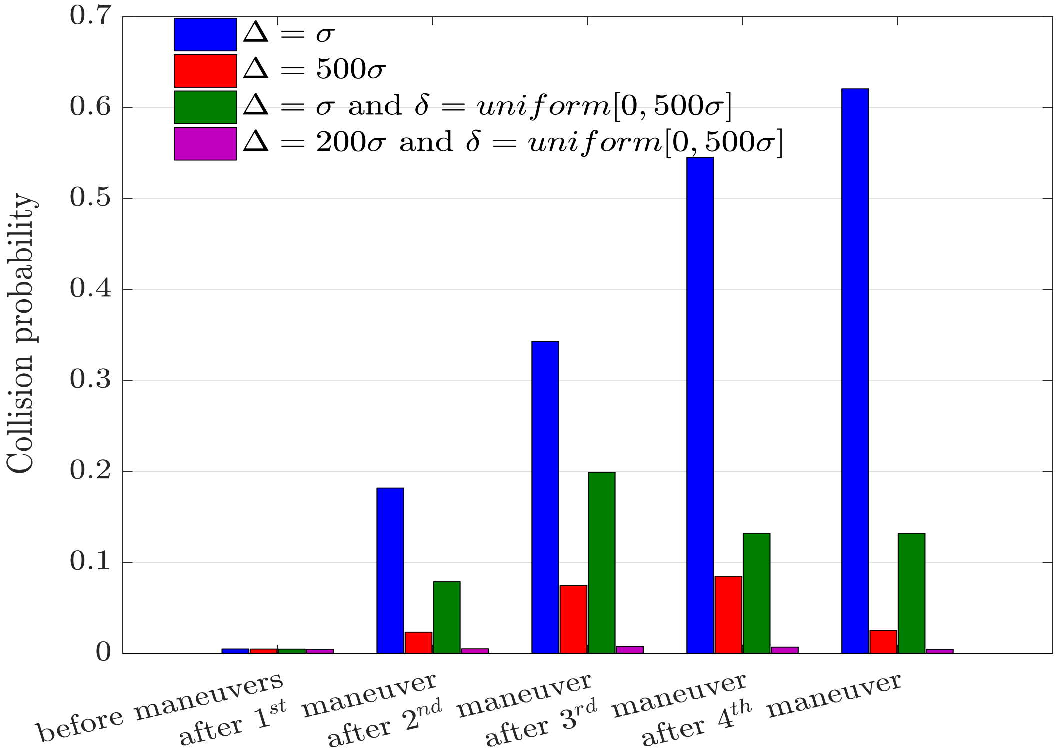


Figure 18: CAM collision probability

independence in the maneuvers of the vehicles. However, the grouping of the CAM generation moments is still clearly visible.

We note, that if the traffic lights are equipped with a Road Side Unit (RSU) that broadcasts the "stoplight" to the vehicles approaching it, this will cause a simultaneous harmonized deceleration maneuver. In this case, the analysis presented for scenario 1 (CACC/platooning) CAM synchronization can be directly inherited by scenario 2 with corresponding conclusions regarding communication performance.

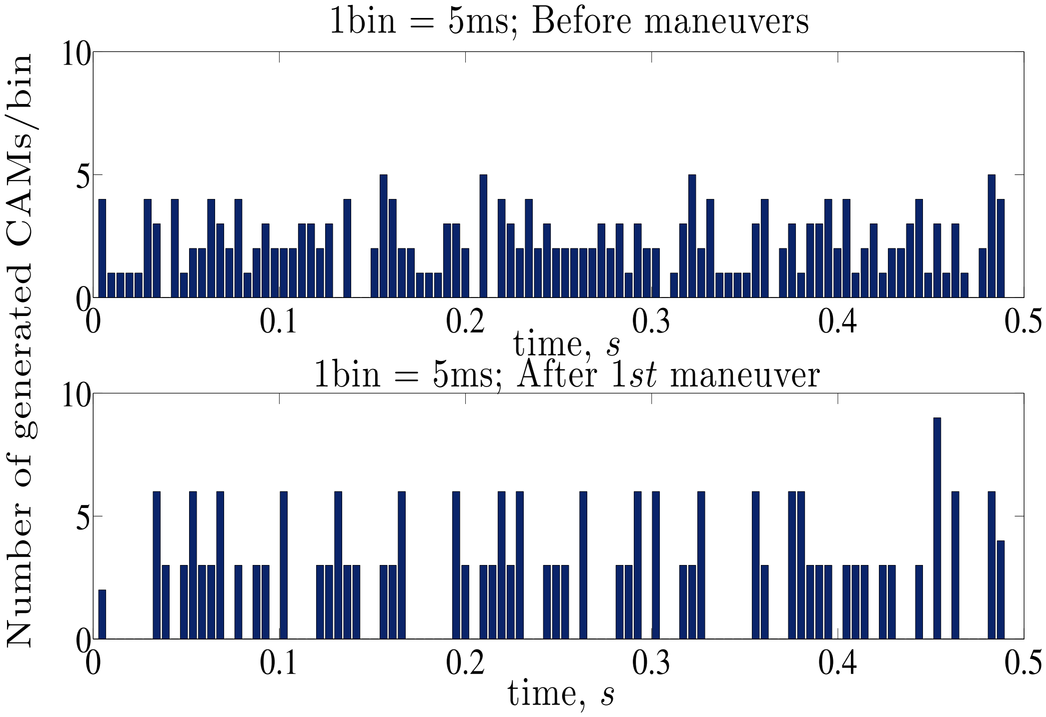


Figure 19: CAMs grouping after $1st$ maneuver

8 Conclusions

Enabling cooperative awareness requires extensive periodic exchange of kinematic information between vehicles. In its turn, this results in an extensive beaconing exchange. Our study has shown that adaptive beaconing based on the kinematc-driven CAMs has a potential performance drawback when implemented in cooperative applications that assume the coordinated behavior of the vehicles. The negative effect of CAM synchronization could be avoided by either:

- Decreasing the sampling rate (increasing Δ). From our simulation study (Figs. 11–15) we conclude that for a value of the sampling period in the order of $\Delta = 1500 \cdot \sigma$ (which is about 20 ms) the CAM synchronization effect observed is considerably reduced.

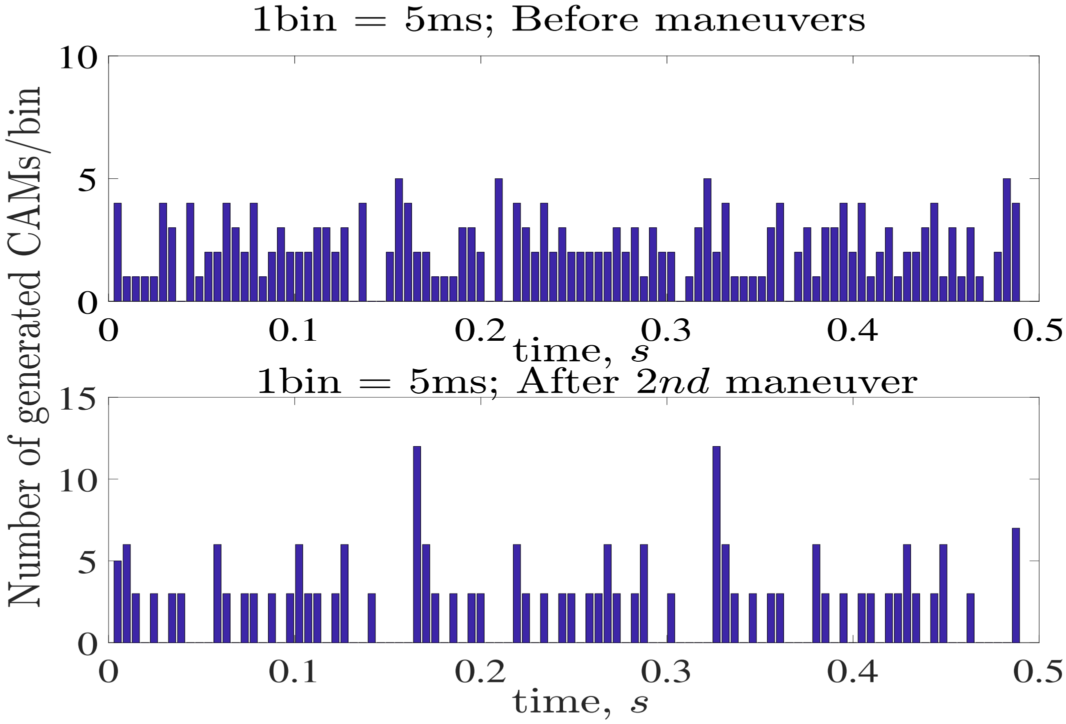


Figure 20: CAMs grouping after $2nd$ maneuver

- Decreasing synchronicity between vehicles (increasing the desynchronization factor). Random disturbance acts in the same way as the random backoff mechanism in the CSMA/CA protocol, by actually, separating concurrent CAM generation in time. In the case when CAMs are also diversified by larger Δ, an additional random desynchronization component can completely eliminate the CAM synchronization effect.

The first option should be implemented carefully, based on the message age requirements of the CACC/platoon control system [26]. The trade-off between how fast a vehicle can detect a kinematic event and the magnitude of the CAM synchronization effect has to be thoroughly evaluated. At the same time, decreasing the level of synchronicity between platoon members contradicts to the spirit of platooning application requirements, which aims at the best possible coordination of all the maneuvers.

It is important to understand, that the nature of the CAM synchronization phenomenon presented in this manuscript is not dependent on any particular form of the platoon's speed curve as long as its mobility follows a deceleration/acceleration pattern. In other words the studied effect will be observed when the platoon decelerates due to any disturbance in front of it (e.g., slower vehicle, speed limit, etc.), which will obviously occur during its operation on the roads. The CAM synchronization phenomenon itself is a result of triggering rules design – in particular the nature of $v_{\min}$ related condition – that leads to CAM synchronization, when the platoon's speed varies.

Moreover, ETSI EN 302 637-2 CAM is only chosen for representative purposes as an

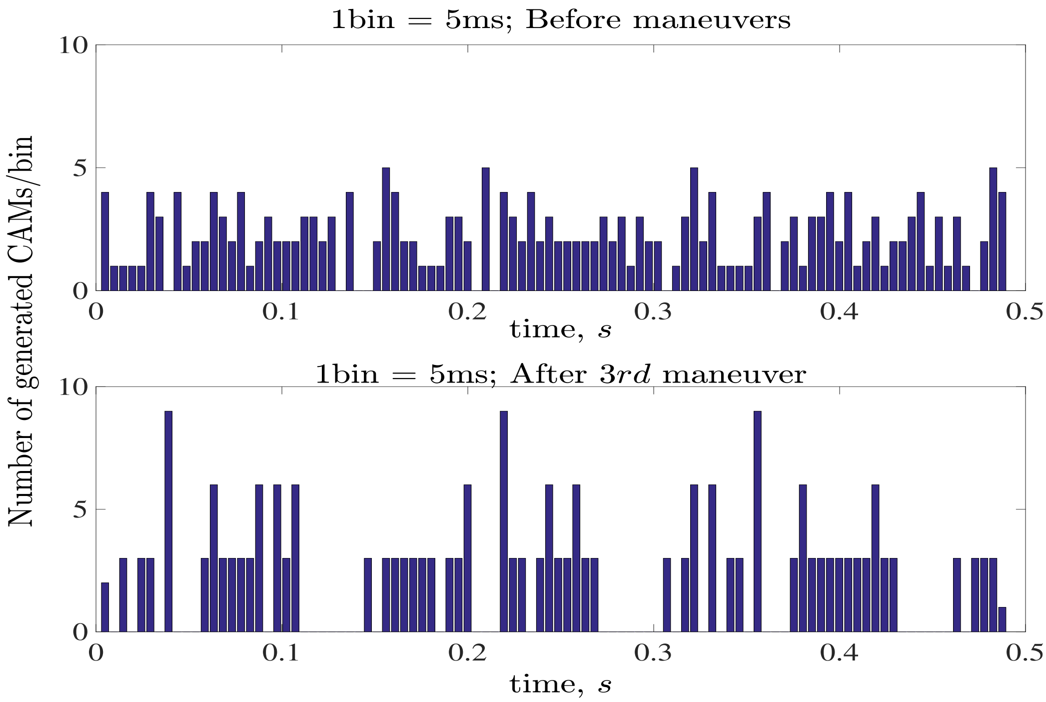


Figure 21: CAMs grouping after $3rd$ maneuver

existing available standard of the adaptive beaconing based on the originating vehicle's dynamic in order to demonstrate the phenomenon of the beacon synchronization effect in a string of vehicles performing cooperative maneuvers. Generally, any adaptive beaconing approach that relies on the track of the speed variation of the originating ITS-S may lead to a similar message synchronization effect in the time domain when vehicles follow mobility scenarios that involve cooperative speed variation.

The discovered negative effect can also influence the functioning of the ETSI congestion control algorithm. This is a subject for our future studies.

Acknowledgment

This work was partially supported by the Excellence Center at Linkoping-Lund in Information Technology (ELLIIT) strategic research environment (Sweden), NFITS - National ITS Postgraduate School (Sweden) and the "ACDC: Autonomous Cooperative Driving: Communications Issues" project (2014-2016) funded by the Knowledge Foundation (Sweden) in cooperation with Volvo GTT, Volvo Cars, Scania, Kapsch TrafficCom and Qamcom Research & Technology.

References

[1] "Directive 2010/40/eu of the european parliament and of the council on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport," *Official Journal of the European Union*, 2010.

[2] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *ETSI EN 302 637-2 V1.3.2*, 2014.

[3] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," *ETSI TR 102 638 V1.1.1*, 2009.

[4] N. Lyamin, A. Vinel, and M. Jonsson, "Poster: On the performance of ETSI EN 302 637-2 CAM generation frequency management," in *2014 IEEE Vehicular Networking Conference (VNC), 3–5 December, Paderborn, Germany.* IEEE Press, 2014, pp. 107–108.

[5] ——, "Does ETSI beaconing frequency control provide cooperative awareness?" in *2015 IEEE International Conference on Communications (ICC), IEEE International Conference on*, London, UK, June 2015, pp. 10 459–10 464.

[6] S. A. A. Shah, E. Ahmed, F. Xia, A. Karim, M. Shiraz, and R. M. Noor, "Adaptive beaconing approaches for vehicular ad hoc networks: A survey," *IEEE Systems Journal*, vol. pp, no. 99, pp. 1–15, 2016.

[7] C. Sommer, O. K. Tonguz, and F. Dressler, "Traffic information systems: efficient message dissemination via adaptive beaconing," *IEEE Communications Magazine*, vol. 49, no. 5, pp. 173–179, May 2011.

[8] H. H. Nguyen and H. Y. Jeong, "Crosslayer beaconing design toward guaranteed cooperative awareness with contending traffic," in *2015 IEEE Vehicular Networking Conference (VNC)*, Dec 2015, pp. 131–134.

[9] M. M. Alotaibi and H. T. Mouftah, "Adaptive expiration time for dynamic beacon scheduling in vehicular ad-hoc networks," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Sept 2015, pp. 1–6.

[10] H. P. de Moraes and B. Ducourthial, "Adaptive inter-messages delay in vehicular networks," in *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2016, pp. 1–8.

[11] E. Egea-Lopez and P. Pavon-Marino, "Distributed and fair beaconing rate adaptation for congestion control in vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 12, pp. 3028–3041, Dec 2016.

[12] A. Böhm, M. Jonsson, and E. Uhlemann, "Performance comparison of a platooning application using the IEEE 802.11p MAC on the control channel and a centralized mac on a service channel." in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on.* IEEE, 2013, pp. 545–552.

[13] S. Joerer, M. Segata, B. Bloessl, R. L. Cigno, C. Sommer, and F. Dressler, "A vehicular networking perspective on estimating vehicle collision probability at intersections," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1802–1812, May 2014.

[14] M. A. Javed and J. Y. Khan, "A cooperative safety zone approach to enhance the performance of vanet applications," in *Vehicular Technology Conference (VTC Spring), 2013 IEEE 77th*, June 2013, pp. 1–5.

[15] S. Joerer, M. Segata, B. Bloessl, R. Lo Cigno, C. Sommer, and F. Dressler, "A vehicular networking perspective on estimating vehicle collision probability at intersections," *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 4, pp. 1802–1812, 2014.

[16] P. M. d'Orey and M. Boban, "Empirical evaluation of cooperative awareness in vehicular communications," in *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th.* IEEE, 2014, pp. 1–5.

[17] J. Santa, F. Pereniguez, A. Moragón, and A. F. Skarmeta, "Vehicle-to-infrastructure messaging proposal based on CAM/DENM specifications," in *Wireless Days (WD), 2013 IFIP.* IEEE, 2013, pp. 1–7.

[18] A. Böhm, M. Jonsson, and E. Uhlemann, "Adaptive cooperative awareness messaging for enhanced overtaking assistance on rural roads," in *Vehicular Technology Conference (VTC Fall), 2011 IEEE.* IEEE, 2011, pp. 1–5.

[19] J. Breu, A. Brakemeier, and M. Menth, "Analysis of cooperative awareness message rates in vanets," in *ITS Telecommunications (ITST), 2013 13th International Conference on.* IEEE, 2013, pp. 8–13.

[20] T. Lorenzen and H. Tchouankem, "Evaluation of an awareness control algorithm for vanets based on ETSI EN 302 637-2 V1.3.2," in *Communication Workshop (ICCW), 2015 IEEE International Conference on.* IEEE, 2015, pp. 2458–2464.

[21] C. Bergenhem, "Approaches for facilities layer protocols for platooning," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems.* IEEE, 2015, pp. 1989–1994.

[22] M. Boban and P. M. d'Orey, "Exploring the practical limits of cooperative awareness in vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3904–3916, June 2016.

[23] "Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part," *ETSI TS 102 687 V1.1.1*, 2011.

[24] "Intelligent transport systems (ITS); access layer specification for intelligent transport systems operating in the 5 ghz frequency band." *ETSI TS 102 687 V1.1.1*, 2013.

[25] "IEEE std. 802.11-2012, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std. 802.11-2012*, jun 2012.

[26] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-Vehicle communication in C-ACC/Platooning scenarios," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[27] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks." *IEEE Communications letters*, vol. 18, no. 1, pp. 110–113, 2014.

[28] M. G. Nilsson, D. Vlastaras, T. Abbas, B. Bergqvist, and F. Tufvesson, "On multi-link shadowing effects in measured V2V channels on highway," in *2015 9th European Conference on Antennas and Propagation (EuCAP)*, May 2015, pp. 1–5.

[29] A. Kesting, M. Treiber, and D. Helbing, "Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 368, no. 1928, pp. 4585–4605, 2010.

[30] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. Lo Cigno, "PLEXE: A Platooning Extension for Veins," in *6th IEEE Vehicular Networking Conference (VNC 2014)*. Paderborn, Germany: IEEE, December 2014, pp. 53–60.

[31] R. Rajamani, H.-S. Tan, B. K. Law, and W.-B. Zhang, "Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons," *IEEE Transactions on Control Systems Technology*, vol. 8, no. 4, pp. 695–708, July 2000.

[32] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, "Modeling prioritized broadcasting in multichannel vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, 2012.

PAPER 1a

Vehicle-to-Vehicle Communication in C-ACC/Platooning Scenarios

Authors:
Alexey Vinel, Lin Lan, Nikita Lyamin

Reformatted version of paper originally published in:
IEEE Communications Magazine.

Vehicle-to-Vehicle Communication in C-ACC/Platooning Scenarios

Alexey Vinel, Lin Lan, Nikita Lyamin

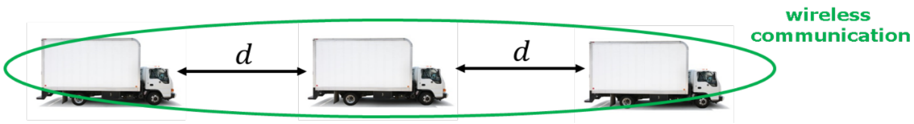
Abstract

Cooperative Adaptive Cruise Control (C-ACC) and platooning are the emerging automotive Intelligent Transportation Systems (ITS) applications. In this tutorial paper, we explain their principles, describe related ongoing standardization activities, and conduct performance evaluation of the underlying communication technology.

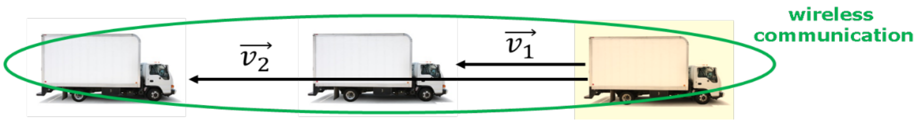
1 Introduction

Sensor-based Cruise Control (CC) systems are nowadays deployed worldwide as common drive assistance systems. CC allows a predefined speed to be maintained and thus reduces a driver's workload on quiet roads. Conventional Adaptive Cruise Control (ACC), which is also on the market, is an enhancement of CC. ACC enables a preset distance from the preceding vehicle to be maintained. The measurements of the distance are handled by automotive radar mounted on the front of the vehicle (Fig. 1a). A line of vehicles connected by the ACC system is subject to the adverse effect of shockwaves because information on the acceleration/breaking of the first vehicle propagates along the caravan with significant radar measurement-induced delays [1]. Recent advances in vehicular networking [2] make it possible to further enhance ACC in order to avoid shockwaves propagating along a caravan of vehicles. This is achieved by direct vehicle to vehicle (V2V) wireless connectivity and information exchange with one or more of the preceding vehicles so as to maintain the predefined inter-vehicle distances (Fig. 1b). Such a system is referred to as Cooperative Adaptive Cruise Control (C-ACC). The information that is transmitted over the wireless connection includes the vehicle's position, velocity, and acceleration. ACC and also C-ACC with automatic longitudinal control only, assume that the driver controls the car using the steering wheel. Thanks to inter-vehicle wireless connectivity, information about the maneuvering of the lead vehicle is available almost instantly to the caravan members. C-ACC can be further enhanced if automatic lateral control of the vehicle is also provided (Fig. 1c). In such a case, a professional, specially-trained driver manually controls the first vehicle in the caravan, while the others follow it automatically. Such a highly automated system means that drivers revert to manual control in certain situations, though most of the time they are not involved in any driving tasks. Further intelligence, e.g., protocols for joining/leaving the caravan or assisting other vehicles during on-ramp highway merging, can be added to such a system into what results as a platooning application. The differences between the C-ACC and platooning are discussed further in Section II. Another motivation for C-ACC/platooning is to further reduce the inter-vehicle distances in the caravan, thereby decreasing air drag, which leads to lower fuel consumption [3]. Typically, an interval of 0.5 seconds (12.5 meters in 90 km/h) for platoons is considered, whilst in a typical ACC (no wireless communication involved and based on radar measurements only) the minimum interval is set at 1.6 seconds. The recommended safety interval in Sweden, for example, with no support is set at 3 seconds. Indeed, under Swedish law "the police impose a fine when the safe distance is less than 1 second. If the safe distance is less than 0.5 seconds, the driver's driving license can be revoked". Therefore, a re-evaluation to or an amendment of the legal framework is key to the future development and deployment of automated driving systems. Several projects on vehicle C-ACC/platooning have recently been carried out. These include Connect&Drive [4], Grand Cooperative Driving Challenge (GCDC) [5], and Safe Road Trains for the Environment (SARTRE). The Connect&Drive and the GCDC projects have C-ACC employing longitudinal control, while the SARTRE project has platoons consisting of heavy-duty vehicles and ordinary passenger cars with both automated longitudinal and lateral control. Demonstration of smart platooning functionalities, like merging of two platoons, is planned for 2016 within the framework of the GCDC II (i-Game) project. The rest of this paper is organized as follows. In Section II, we provide an overview of the relevant standardization activities. Section III briefly discusses V2V communication patterns enabling C-ACC/platooning. A system model, performance metrics and simulation results for the platooning scenario are presented in Section IV. Section V concludes the paper with some plans for future work.

a) ACC



b) C-ACC



c) Platooning

Figure 1: Illustration of ACC/C-ACC/platooning concepts: a) ACC; b) C-ACC; c) platooning.

2 Standardization activities

V2V and Vehicle to Infrastructure (V2I) are also referred to as Cooperative ITS (C-ITS). Key stakeholders in North America and the EU have been driving research and development of C-ITS for over a decade. Standardization is one of the key building blocks of the C-ITS deployment roadmap. In 2014, the European Telecommunication Standard Institute (ETSI) and the European Committee for Standardization (CEN) jointly delivered the first release of C-ITS standards, enabling deployment of a set of day-one applications. The main target applications supported by release one standard can be summarized as the cooperative awareness application and the road hazard signalling applications. These applications do not require any intervention to the vehicle electronic systems, but focus instead on providing information or a warning to the driver of a hazardous road situation (Decentralized Environmental Notification Message (DENM) [6]) as well as the kinematic state of other vehicles (Cooperative Awareness Message (CAM) [7]). Release one standards also enable transmission of infrastructure information to vehicles via a set of Infrastructure to Vehicle (I2V) messages, such as Signal Phase and Timing information (SPAT), Road Topology information (MAP) and road signage information (in-vehicle information). The communication of V2V and V2I messages requires the establishment of direct vehicle to vehicle and vehicle to infrastructure wireless ad hoc network and low latency media access. Release one standards, therefore, also include specifications on a specific networking communication stack (geoNetworking, networking functionalities with addressing scheme based on the geographical position of nodes), and access technologies (e.g., EU profile of IEEE 802.11p operating in the 5.9Ghz spectrum band allocated for ITS applications). In addition, special attention has been paid during the standard specification phase to optimize the network resource usage, given the expected network density level and the amount of data being exchanged between nodes to satisfy the application requirements. For example, ETSI TC ITS operates a decentralized congestion control mechanism to dynamically measure the network load in real time and also to implement functionalities to keep the load below a threshold level. It should be noted that, even though ITS specific technologies standards are made available, the C-ITS does not preclude the use of other technologies, particularly when the penetration rate of the ITS-equipped nodes is low and when the application requirements may be met by other applications (e.g., for non-safety applications). In fact, legacy communication stacks (e.g., TCP/IPv6 stack) and communication technologies (e.g., cellular network) are also included in the overall ITS communication architecture. Nevertheless, in order to ensure communication interoperability between vehicles from different vendors from the beginning of the deployment, a common agreement among stakeholders is required. The European Car 2 Car Communication Consortium (C2C-CC) is currently developing recommendations based on release one standards, with the aim of specifying a minimum set of standardized features and minimum sets of system performance to be implemented by all major car manufacturers and system providers in the EU and worldwide. Among the various messages mentioned, CAM is one of the key basic features required for day one deployment. This is a high-frequency (1-10Hz) periodic heart-beat message, broadcast by every equipped vehicle to its immediate communication neighbours, providing the vehicle is in the traffic flow and the C-ITS system is in operation. CAM includes the following content:

- highly dynamic vehicle kinematic data such as position, time, heading, speed, acceleration, status of acceleration control systems;
- vehicle attributes such as vehicle width, length, vehicle type, vehicle role;
- vehicle movement data, including vehicle historical path and path prediction data e.g. yaw rate, curvature;
- additional information for special vehicle types, e.g. emergency vehicles, buses, road maintenance vehicles, and so on.

In the published standard [7], the CAM transmission rate is dynamically adjusted between 1 and 10Hz according to vehicle speed, movement heading, and changes in acceleration. The transmission rate is increased whenever there is an increase in the vehicle movement dynamics. This is in order to ensure the movement dynamic is correctly reflected in the message content update rate. During its development phase, CAM and the corresponding protocol have been tested, validated in several ETSI conformance and the interoperability test event ETSI Plugtest, as well as in multiple EU R&D and Field Operational Test Projects (FOT). It was published as a European Norm in late 2014. European ITS Standard Organizations are currently preparing for release two of ITS standards. Among the many potential fields of stakeholder interest is the development of C-ITS standards for connected automated driving applications and C-ITS-based advanced driver assistance applications. For example, since April 2014, ETSI TC ITS has established three new work units: namely C-ACC (TR 103 299), Vulnerable Road User safety (TR 103 300) and Platooning (TR 103 301). The focus of these projects is to conduct a pre-standardization study of these three applications. Instead of developing brand new standards from the very beginning, the pre-standardization study provides an overview of the applications, including their functional and operational requirements (e.g., performance requirements, data exchange requirements, communication requirements, communication security requirements). The requirements analysis is essential for estimating the applicability of existing standards for these applications, as well as any new standard features that may be specified (message sets specifications, communication protocol specifications, communication security features, congestion control requirements, etc). The expected outcomes of these projects are the recommended specifications for future standards required for C-ACC, platooning and Vulnerable Road Users safety applications. The initial technical work of the C-ACC and platooning applications in ETSI TC ITS focuses on the development of a high-level definition of C-ACC and platooning applications. This high-level definition is similar to those assumed by us, and can be summarized as follows:

1. C-ACC is an embedded in-vehicle system that extends the ACC function so as to further reduce the time gap between the preceding vehicle or preceding traffic.

The operation of C-ACC is based on kinematic data directly transmitted from the preceding and/or following vehicles via a V2V communication link. Multiple C-ACC-equipped vehicles may be aligned together to form a convoy (or caravan). Each vehicle is, however, responsible for its own manoeuvring. In summary, C-ACC is a distributed automated driving or ADAS system.

2. Platooning: a group of vehicles sharing a similar itinerary over a period of time form a vehicle fleet train, coordinated by a platoon leader. With increased levels of automation, the platoon leader may coordinate with platoon members for group manoeuvring (platoon joining/leaving/group speed), or even make decisions for members in certain situations. The platoon leader is also in charge of monitoring the driving environment not only for him/herself, but also for the platoon members. Members of the platoon may be responsible for following the vehicle ahead, so in this respect, C-ACC may be considered as one technology for platoon operations.

3. Both longitudinal and lateral control functions may be used in two applications, to further increase operation stability.

4. Different levels of automation should be considered in C-ACC and Platooning applications.

Several R&D projects have demonstrated that minor extensions to CAM and DENM may be sufficient to support C-ACC and Platooning applications. For a platooning application, new messages/protocols may also be needed to enable platoon group operations such as negotiation for joining/leaving the platoon or merging different platoons. In addition, for new features such as cooperative sensing (exchange of vehicle environment perception with other vehicles), cooperative manoeuvring would be helpful in realizing automated driving applications. Such projects would bring important technical inputs for standard development work. For example, in January 2015, a new work unit on cooperative sensing (TS 103 324: Cooperative Observation Service) was established by ETSI TC ITS.

3 Communications for platooning/C-ACC

In a platoon situation, the platoon leader should be aware of the kinematic state of the platoon members in real time for monitoring purposes. In addition, the platoon leader may transmit "a platoon control message" to the platoon members for cooperative manoeuvring, e.g., platoon group target speed, configured time gap between platoon members, etc. The present study focuses on the leader receiving messages from all the other vehicles. The "platoon control message" is not, therefore, considered here. In a C-ACC situation, a C-ACC vehicle follows the preceding vehicle/s and maintains a target time gap with the preceding vehicle. For this purpose, the C-ACC vehicle receives kinematic data on the preceding vehicle/s. In the present study, we assume that kinematic status information is transmitted between vehicles by CAM message. The simulation work is done for CAM messages, which represent the most stringent cases. We assume that the CAM messages are broadcast by all the nodes, but we are mainly interested in ensuring that the data age deadline (see Section 4) of the leader is met by all the caravan members. We also assume that the transmitting vehicle should be able to provide kinematic data at an update rate equal to or higher than the maximum CAM transmission rate. This is to ensure that the transmitted CAM always contains actual vehicle's kinematic data. It is assumed that both transmitting and receiving vehicles are equipped with HW/SW solutions that meet certain performance requirements for the processing of CAM messages, including processing at protocol stacks (networking, MAC etc.) and at security. For example, according to TS 101 559 – 1 (RHS) [8], the end to end latency of CAM should be u_{max} =300 ms for a road hazard signalling application. For platooning and C-ACC applications, this end to end time latency requirement may be further reduced.

4 Performance Evaluation

4.1 System Model

In the model it is assumed that the platoon has a leading vehicle that is steered by a human and $N-1$ following automated vehicles moving together along a highway. To enable functioning of the platoon control systems, each vehicle executes the following steps:

- generates CAMs in accordance with ETSI EN 302 637-2 specification [7] (the generation moment is denoted as t_0);
- generates random transmission delay $\sim uniform(0, 50ms)$ (processing delay);
- transmits CAMs on a dedicated channel in accordance with IEEE 802.11p Medium Access Control (MAC) specification [9].

On the receiver side, a random message verification delay $\sim uniform(50, 100ms)$ is introduced (the moment of time that the verification ends is denoted as t_1). Following our previous work [10] and [11] the following assumptions are made in the present study:

- All the vehicles in the platoon are within each other's communication range. This is a valid assumption for the realistic set-up of a platoon with 20–25 vehicles, when the IEEE 802.11p communication range is in the order of 400–500 m, inter-vehicle distance is 7 m and truck length is 13 m.
- The kinematic parameters of the leading vehicle are modelled via the Constant-Acceleration Heuristic (CAH) state-of-the-art car-following mobility model [12].
- Random deviations in the velocities of the following vehicles in the caravan are modelled by applying the following approach: we add a random delay $\delta \sim uniform[0, k \cdot$

$\sigma ms]$ to a CAM generation moment in order to reflect the non-perfect synchronisation between their velocities, where $k = 500$ is the maximum delay expressed in $\sigma = aTimeSlot$ ($aTimeSlot$ is defined in the standard [9]).

- We add independent packet losses to our MAC layer for the each pair of nodes (for this work we only need PER values for each ordinary vehicle transmitting to the leader). The Nakagami-m ($m = 1$) propagation model is used.
- The Decentralized Congestion Control (DCC) functionality is disabled.
- Each vehicle is able to update the CAM content for each generated CAM.

4.2 Performance metrics

Data Age: The data age u_n is a random variable defined as the time elapsed since the last successfully received packet of vehicle $2 \leq n \leq N$ by the leading vehicle. Data age is the difference between $t - t_1$, where t is the current moment of time and t_1 is the moment when the last successfully received packet of vehicle n was received by the leading vehicle.

Note: data age relates to the leader and is computed for an ordinary vehicle. We assume that the platoon leader determines the inter-distance for all platoon members. Platoon members use automated driving to maintain the distance specified by the leader.

Cumulative Distribution Function (CDF) of the Data Age: For a particular vehicle n:

$$F_n(t) = Pr\{u_n \leq t\}$$

We denote the respective empirical CDF (ECDF) of the data age for a particular vehicle n as $F_n^*(t)$.

Data Age Deadline: The data age deadline $u_m ax$ is the maximum acceptable data age of a vehicle from the leader's perspective.

Probability to meet the deadline: The probability that data age value will not exceed deadline:

$$U_n^* = Pr\{u_n \leq u_{max}\}$$

4.3 Current Standardization

Let us evaluate whether the current CAM generation rules are sufficient to meet the platoon/C-ACC needs. We chose the parameters sampling period (Δ) and disturbance parameter (δ) so that the CAM generation moments synchronization effect discussed in [11] is eliminated. We fix the mobility pattern to the disturbance scenario presented in [7]. In the scenario in Fig. 2, the leading vehicle decelerates from the desired steady speed (V_{stb} ~90 km/h) to a lower speed (V_{low} ~60 km/h), maintains this speed for some time and then accelerates back to the initial speed. The disturbance scenario could be regarded as a pattern to describe the appearance of a slow moving vehicle in front of the platoon or a road speed limit. This corresponds to a CAM generation rate change from $1/[4/V_{stb}]$=6.25Hz (generation interval of 160ms) to $1/[4/V_{low}]$=4.25Hz (generation interval of 240ms). Additionally we provide results for the scenario widely used in the literature when CAMs are generated with a fixed frequency of 10 Hz and compare performance of both approaches.

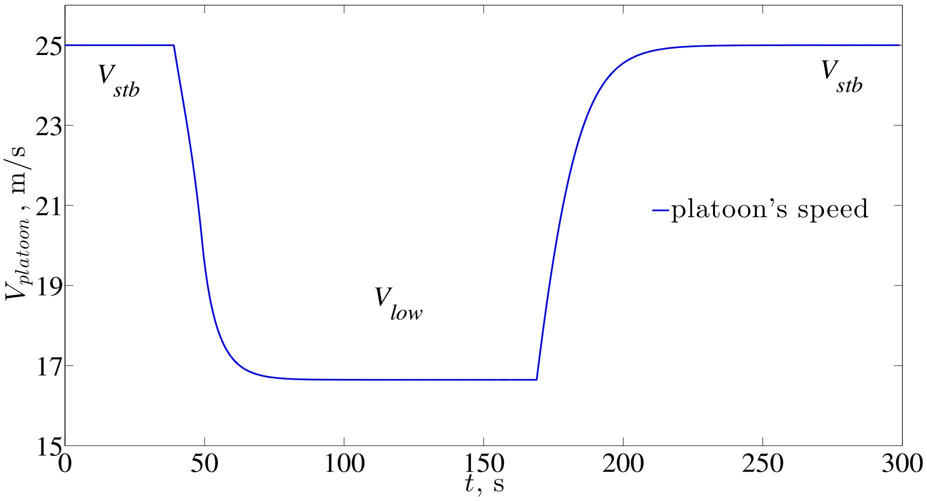


Figure 2: Illustration of the disturbance scenario speed pattern for the platooning application.

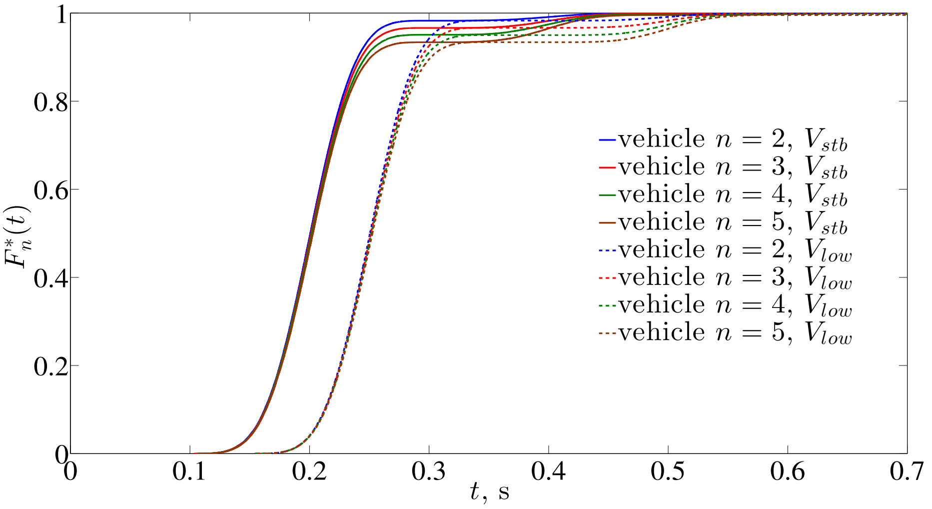


Figure 3: Empirical cumulative distribution functions of data age for the platoon of $N = 5$ vehicles

In Fig. 3 an empirical cumulative distribution functions of data age (hereafter, data

Table 1: Probability $u_n \leq u_{max}$ to meet deadline for vehicle n.

U_n^*	$n = N$	ETSI V_{stb}	ETSI V_{low}
$N = 5$	0.9337	0.8950	0.9974
$N = 10$	0.8530	0.8178	0.9869
$N = 25$	0.6182	0.5943	0.8995

age ECDF) of each ordinary vehicle in the platoon composed of N=5 vehicles is shown. Solid lines show data age ECDF when the platoon maintains (V_{stb}) speed while dashed lines indicate (V_{low}) speed. Since the message-triggering process according to ETSI EN 302 637-2 relies on the current values of kinematic parameters, the data age of each vehicle will proportionally decrease/increase as the respective speed increases/decreases. Obviously, vehicles located farther from the leader experience higher packet loss due to fading and so have higher data age. Later in this paper we focus on the data age of the last vehicle $n = N$ in the platoon. Fig. 4 shows the frequency distribution of data age for the last vehicle in a platoon of $N = 25$ vehicles when the platoon maintains V_{stb}. In our setup, the data age for the most distant vehicle may exceed 1 second. The reason for such high values and the from of the distribution is that data age may increase proportionally to the number of subsequently lost CAMs. Fig. 5 illustrates data age ECDF's for the last vehicle in the platoons of length N =5,10,25 vehicles. With an increase in platoon size, data age could increase significantly, which could make operation of the control system difficult.

Table I shows the probabilities U_n^* of meeting the deadline u_{max} =300 ms for the last vehicle in a platoon of length N =5,10,25. Since the CAM generation rate for ETSI EN 302 637-2 is kinematic-dependent, the probability of missing the deadline when the speed is Vlow, becomes higher. The situation becomes even more acute if the platoon decelerates to lower speed values. In contrast, U_n^* for a fixed 10Hz mechanism is predictable and depends only on the size of the platoon.

Fig. 5 shows a comparative data age distribution between when CAMs are triggered in accordance with ETSI EN 302 637-2 (solid lines) and when employing a constant frequency of 10Hz (dashed lines). It should be noted that when the platoon moves at V_{stb}, the corresponding generation frequency is about 6.25 Hz ($1/[4/V_{stb}]$). Since we propose a dedicated communication channel for platoon coordination, even for N=25 members, 10Hz will always outperform the ETSI EN 302 637-2 approach (they may perform equally when the platoon's speed exceeds $1/[4/V_{stb}]$ =10, V_{stb} = 40m/s = 144 km/h, which is an unrealistic speed pattern for a platooning application). The main conclusion to be drawn is that a 10Hz CAM rate would be preferable to the current triggering condition, particularly when platoon speed is high. Another conclusion is that although the platoon leader receives CAMs from the platoon members, the current standard CAM rates tend to be insufficient for the leader to maintain the desired 0.5 second distance for safe operation. The CAM rate should, therefore, be further increased.

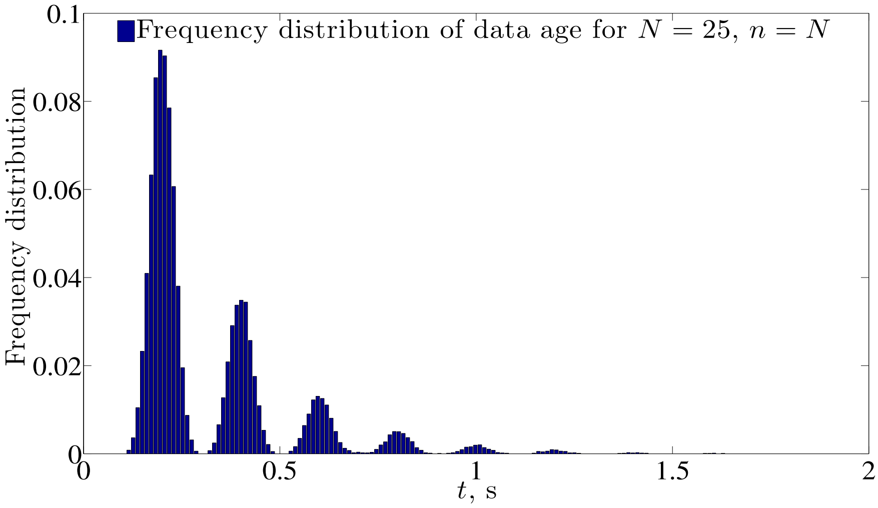


Figure 4: Frequency distribution of data age for last vehicle in platoon of $N = 25$ vehicles when platoon maintains V_{stb}.

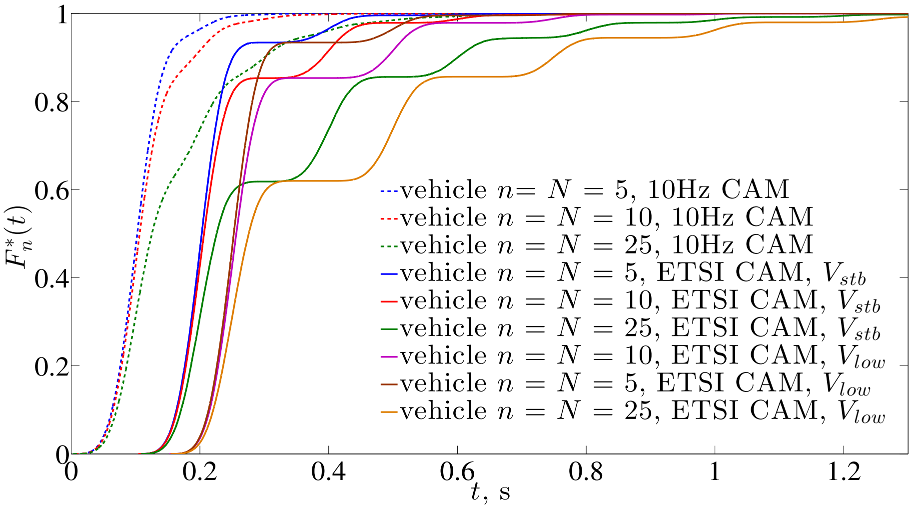


Figure 5: Empirical cumulative distribution functions of data age for a platoon of $N = 5$, 10 and 25 vehicles with fixed and variable CAM rates.

4.4 Recommendations for Improvement

- Enable constant CAM generation rates exceeding 10 Hz in a platoon, especially at higher speeds.

- Further reducing the processing delay at the receiving vehicle may be beneficial, in particular, the security-related processing delay has an important impact on data age.

5 Future Plans

In our future work we will:

- Take DCC into account in future simulation study.
- Improve CAM message content so it can distinguish between platoon and non-platoon members, e.g., group identification.
- Introduce messages and protocols for platoon control in the overall traffic flow, e.g., space reservation for platoon lane change.

6 Acknowledgements

This study is supported by NFITS - the National ITS Postgraduate School (Sweden) and is a part of the "ACDC: Autonomous Cooperative Driving: Communications Issues" project (2014-2016) funded by the Knowledge Foundation (Sweden) in cooperation with Volvo GTT, Volvo Cars, Scania, Kapsch TrafficCom and Qamcom Research & Technology. The authors also express their gratitude to Denis Kleyko from Lulea University of Technology for his valuable comments, which helped to improve the quality of the manuscript.

References

[1] L. Xiao and F. Gao, "Practical string stability of platoon of adaptive cruise control vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1184–1194, Dec 2011.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 584–616, Fourth 2011.

[3] A. A. Alam, A. Gattami, and K. H. Johansson, "An experimental study on the fuel reduction potential of heavy duty vehicle platooning," in *13th International IEEE Conference on Intelligent Transportation Systems*, Sept 2010, pp. 306–311.

[4] J. Ploeg, A. F. Serrarens, and G. J. Heijenk, "Connect & drive: design and evaluation of cooperative adaptive cruise control for congestion reduction," *Journal of Modern Transportation*, vol. 19, no. 3, pp. 207–213, 2011.

[5] J. Ploeg, S. Shladover, H. Nijmeijer, and N. van de Wouw, "Introduction to the special issue on the 2011 grand cooperative driving challenge," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 3, pp. 989–993, 2012.

[6] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 3: Specifications of decentralized environmental notification basic service," *ETSI EN 302 637-3 V1.2.2*, 2014.

[7] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *ETSI EN 302 637-2 V1.3.2*, 2014.

[8] "Intelligent transport systems (ITS); V2X applications; part 1: Road hazard signalling (RHS) application requirements specification." *ETSI TS 101 539-1 V1.1.1*, 2013.

[9] "IEEE std. 802.11-2012, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std. 802.11-2012*, jun 2012.

[10] N. Lyamin, A. Vinel, and M. Jonsson, "Does ETSI beaconing frequency control provide cooperative awareness?" in *2015 IEEE International Conference on Communications (ICC), IEEE International Conference on*, London, UK, June 2015, pp. 10 459–10 464.

[11] ——, "Poster: On the performance of ETSI EN 302 637-2 CAM generation frequency management," in *2014 IEEE Vehicular Networking Conference (VNC), 3–5 December, Paderborn, Germany.* IEEE Press, 2014, pp. 107–108.

[12] A. Kesting, M. Treiber, and D. Helbing, "Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 368, no. 1928, pp. 4585–4605, 2010.

Paper 1b

Does ETSI beaconing frequency control provide cooperative awareness?

Authors:
Nikita Lyamin, Alexey Vinel, Magnus Jonsson

Reformatted version of paper originally published in:
1st IEEE ICC 2015 Workshop on Dependable Vehicular Communications.

Does ETSI beaconing frequency control provide cooperative awareness?

Nikita Lyamin, Alexey Vinel, Magnus Jonsson

Abstract

Platooning is an emergent vehicular application aiming at increasing road safety, efficiency and driving comfort. The cooperation between the vehicles in a platoon is achieved by the frequent exchange of periodic broadcast Cooperative Awareness Messages (CAMs) also known as beacons. CAM triggering conditions are drafted in the standard ETSI EN 302 637–2 and are based on the dynamics of an originating vehicle. These conditions are checked repeatedly with a certain sampling rate. We have discovered that the improper choice of the sampling rate value may increase the number of collisions between CAMs at the IEEE 802.11p medium access control layer and, therefore, diminish the efficiency of beaconing in a platoon.

1 Introduction

Design of the inter-vehicle communication protocols to support coordinated maneuverings and automated driving is recognized by the vehicular networking community as an emergent research topic [1]. Real-time exchange of kinematic information by all the maneuvering vehicles is crucial for their cooperation [2]. Broadcasting of Cooperative Awareness Messages (CAMs) by every vehicle to their neighbors is studied for multichannel scenario [3], for the hidden-nodes case [4] and for enabled congestion control approaches [5], to name a few.

Communication support for platooning is currently getting a lot of attention, but the results so far are limited to, e.g., packet loss measurements [6] and a study on the content of the information to be exchanged and its role in the control application [7]. Still, several studies and proposals of how to use IEEE 802.11p in platooning have been reported, e.g., a slotted approach [8], retransmission schemes together with a TDMA approach [9],[10], analysis of the connectivity probability [11], and a study of send rate adaptation, message type prioritization and warning dissemination strategies [12]. However, the recently proposed CAM generation rules are not taken into account in any of the mentioned work.

In comparison to the studies mentioned above, this paper is focused on the ongoing ETSI standardization efforts for CAMs generation rules [13], which have not received an adequate publication activity so far. We focus on the cooperative awareness provisioning for the emergent platooning application [14], where a caravan of semi-autonomous vehicles perform maneuvering together aiming at increased safety and reduced fuel consumption.

The contribution of this paper is twofold:

- a phenomenon of CAM triggering moments synchronization between platoon members is discovered;
- potentials to diminish a negative influence of this phenomenon on the cooperative awareness are discussed.

The manuscript is organized as follows. The assumptions of the system model are outlined in Section II. ETSI CAMs generation rules are summarized in Section III, while in Section IV the identified problem is described. Sections V and VI discuss potential ways to address the identified problem and conclude the paper, respectively.

2 System Model

We consider a platoon comprised of N vehicles: a leading human-controlled vehicle and a caravan of automated vehicles moving together along the highway, Fig. 1. To enable functioning of the platooning control systems, each vehicle:

- generates CAMs in accordance to ETSI EN 302 637-2 specification [13];
- transmits CAMs on a dedicated channel in accordance to the IEEE 802.11p Medium Access Control (MAC) specification [15].

The following assumptions are adopted in our study:

- All the vehicles in the platoon are in each others communication range. This is a valid assumption for the realistic set-up of a platoon with up to 20–25 vehicles, when the IEEE 802.11p communication range is in the order of 400–500 m, inter-vehicle distance is 5 m and truck length is 15 m (see [16], p. 111).
- All the vehicles in the platoon increase or decrease their speed synchronously. This is a reasonable assumption since the speed deviations within a platoon are targeted to be marginal[1] (see [17], p. 433).
- The kinematic parameters of the leading vehicle are modeled via the Constant-Acceleration Heuristic (CAH) [18] state-of-the-art car-following mobility model[2].

3 ETSI Cooperative Awareness Basic Service

Cooperative Awareness Basic Service [13] sets up the rules for the CAM generation, which are summarized in three items below[3].

Firstly, the generation rate limits for CAMs are defined as follows:

---

[1] In Subsection V.B we discuss the relaxation of this assumption.

[2] This particular mobility model is chosen for the illustrative purposes only, however, the considerations in the paper are valid for any mobility patterns.

[3] CAM generations are also influenced by the ETSI Decentralized Congestion Control (DCC)[19]. However, throughout of this paper DCC is not considered.

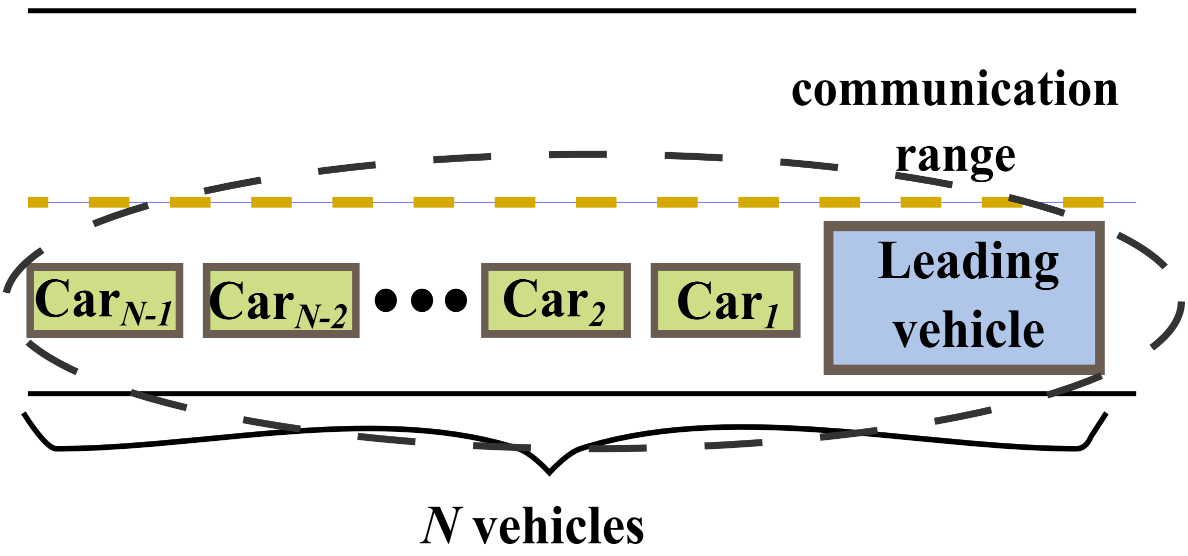


Figure 1: Reference scenario

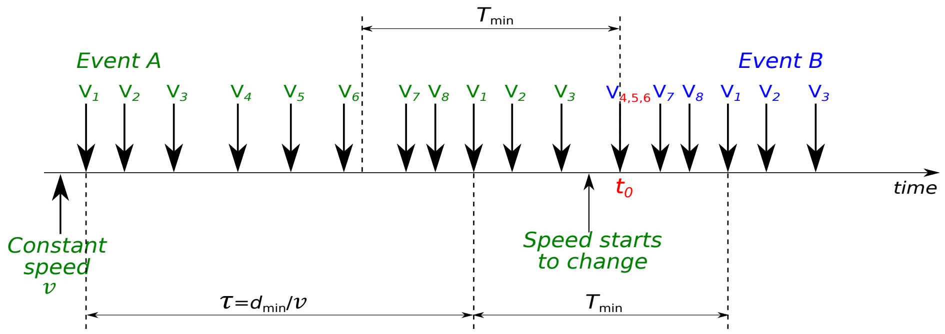


Figure 2: Example 1 – Synchronization of CAM triggering moments in the platoon

- The CAM generation interval shall not be inferior to $T_{\text{min}} = T\_GenCamMin$ =100 ms. This corresponds to the maximal CAM generation rate of 10 Hz.
- The CAM generation interval shall not be superior to $T_{\text{max}} = T\_GenCamMax$ =1000 ms. This corresponds to the minimal CAM generation rate of 1 Hz.

Secondly, the above conditions for triggering the CAM generation shall be checked by a vehicle repeatedly every $\Delta = T\_CheckCamGen$. We refer to $1/\Delta$ as the CAM triggering condition sampling rate.

Thirdly, within the specified limits, the CAM generation depends on the dynamics of the originating vehicle. A CAM shall be triggered in one of two cases:

- The time elapsed since the last CAM generation is equal or larger than $T_{\max}$.
- The time elapsed since the last CAM generation is equal or larger than $T_{\min}$ and any of the following events has occurred:
  - *"Event A"*: the absolute difference between the current position of the vehicle and its position included in the previous CAM exceeds $d_{\min}$=4 m;
  - *"Event B"*: the absolute difference between the current speed and the speed included in the previous CAM exceeds $v_{\min}$ =0.5 m/s;
  - *"Event C"*:[4] the absolute difference between the current direction of the vehicle and the direction included in the previous CAM exceeds 4°.

4 Identified Problem

Throughout this Section we assume that Δ is negligibly small, i.e. the CAM generation rules are continuously checked by every vehicle.

4.1 CAMs Generation Moments: Synchronization

To illustrate the discovered effect of possible CAM generation times synchronization, let us consider two examples.

Example 1: Let the platoon change its velocity, e.g. it temporally slows down due to reduced speed limits in a road construction segment or due to a slow vehicle ahead.

Let us denote the CAM generation moments of the i-th vehicle as $V_1, V_2, \dots V_N$, Fig. 2. When the platoon moves with a constant speed of 90 km/h, each vehicle triggers a CAM every $\tau = d_{min}/v$=160 ms due to the periodic occurrence of *Event A*.

Due to the deceleration, in a short time period a change of the platoon speed exceeds 0.5 m/s (*Event B*) and the vehicles with $t - t_i \geq T_{\min}$ (i.e. 4, 5 and 6) synchronously trigger their CAMs at time t_0. Other vehicles (i.e. 1, 2, 3, 7 and 8) trigger their CAMs as soon as the time elapsed since their recent CAM generation turns to $T_{\min}$ =100 ms. When the platoon speed stabilizes, the vehicles trigger CAMs with a constant period again (*Event A*).

The following proposition characterizes the phenomenon described above.

Proposition A. Let a platoon move with a constant speed v during time interval $[0, t_0)$. If *Event B* occurs at t_0, then the mean number of CAM generation moments synchronized at t_0 is

$$\rho = \frac{\tau - T_{\min}}{\tau} \times N,$$

---

[4] Event C is not considered in the paper, since we assume that the platoon moves along the highway and changes its direction slowly. Nevertheless, all the presented considerations and conclusions are valid also in case Event C might occur.

where $\tau = d_{\min}/\upsilon$.

Proof: Let the CAM generation moments of all the vehicles be enumerated and denoted as T_n, $n \geq 1$. The CAM generation moments in the interval $[0, t_0)$ represent the following stochastic process:

- Due to the random and independent occurrence of the first CAM generation moment of each of the N vehicles, the $N-1$ intervals between pairs of subsequent CAMs of any N consecutive generation moments are exponentially distributed, i.e. $\forall n : T_{n+k} - T_{n+k-1} \sim exp(\tau/N)$, $k = \overline{1, N-1}$.
- Due to the periodic occurrence of *Event A*, all the vehicles generate CAMs with period τ, i.e. $\forall n : T_{n+N} - T_n = \tau$. Therefore, any time interval of duration τ, contains exactly N CAM generation moments (one per vehicle).

All the N vehicles detect *Event B* simultaneously at t_0. However, due to the restriction on the value of the minimal possible CAM generation interval $T_{\min}$, only those vehicles, whose CAM generation moments belong to $[t_0 - \tau, t_0 - T_{\min})$, are triggered at t_0, Fig. 3. Taking into account the above properties of the considered stochastic process, the mean number of CAM generation moments in $[t_0 - \tau, t_0 - T_{\min})$ is $\frac{\tau - T_{\min}}{\tau} \times N$. ■

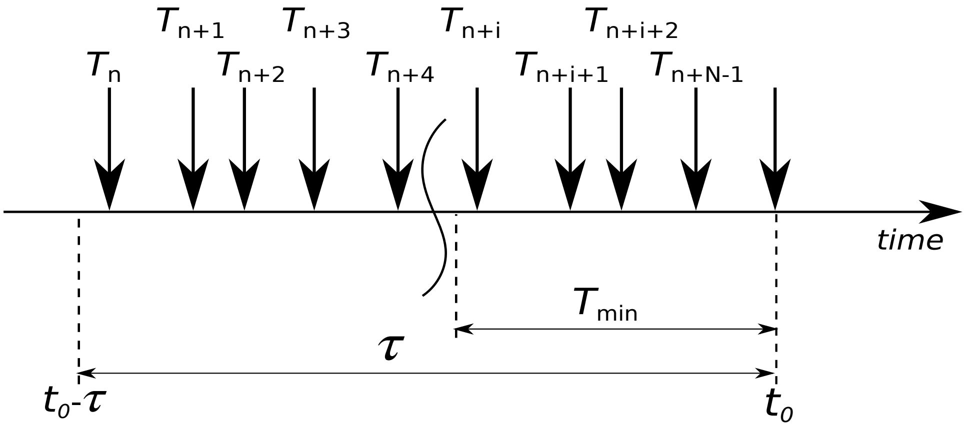


Figure 3: Illustration for the proof of Proposition A

Example 2: Let the platoon slow down and accelerate several times, see Fig. 4.

Each platoon maneuver influences the CAM triggering process according to the mechanism described in Example 1. More CAMs might become synchronized as long as more maneuvers are performed due to the concurrent occurrence of *Event B*. For example, in Fig. 5 CAMs from vehicles 7, 8, 9, 10 and 11, 12 become synchronized with the ones from 1, 2, 3, 4, 5, 6 after the 2^{nd} and the 3^{rd} maneuvers, respectively.

Notice, that once the synchronization of the CAM triggering times has occurred, further accelerations/decelerations will not lead to desynchronization. *Event B* occurs simultaneously for all the synchronized vehicles, since their recent CAMs contain the same kinematic information.

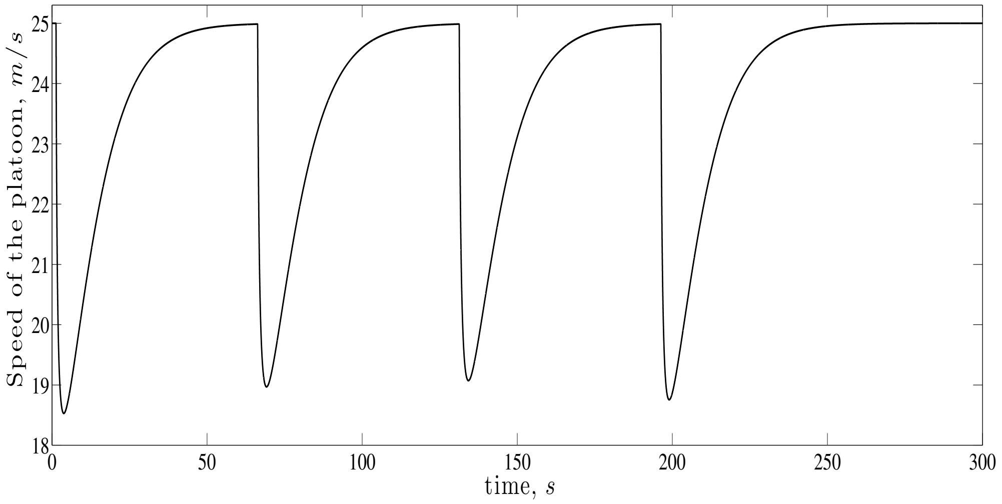


Figure 4: Example 2 – Some subsequent maneuvers

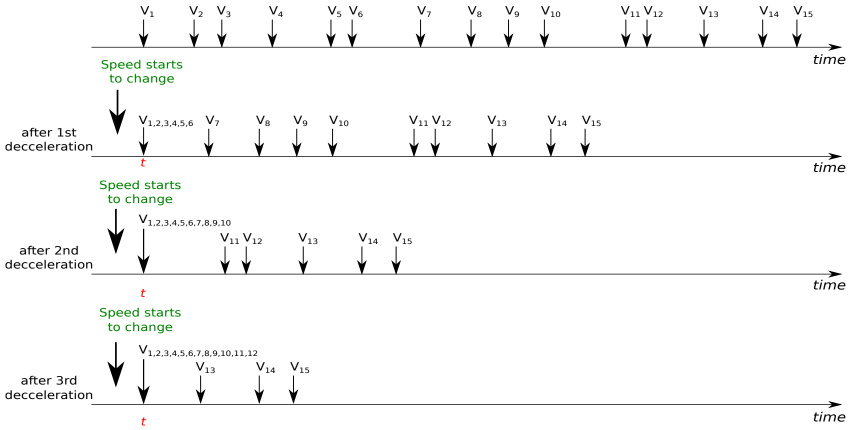


Figure 5: Example 2 – CAM triggering after several deceleration/acceleration maneuvers

4.2 CAM Transmission Moments: Grouping

Transmission of CAMs generated as discussed above is governed by the IEEE 802.11p MAC protocol, which presumes that CAMs from different vehicles may collide due to their simultaneous transmissions. Synchronization of the CAM generation times does not lead to a guaranteed collision as well as their desynchronized generations do not impose that collisions are impossible [3], [15]. This phenomenon can be characterized using the notions of *groups*.

Let us consider a platoon moving with a constant speed with all the vehicles periodically triggering CAMs. Let us select a sequence of $T_i \leq T_{i+1} \leq T_{i+2} \leq \cdots \leq T_{i+N-1}$ CAM generation moments of each vehicle in the platoon such that CAMs from vehicles i and $i+N-1$ cannot collide (formal way to do it is proposed in [16], p. 112).

One can execute Algorithm 1, where $AIFS$ is the Arbitrary Inter-Frame Space, σ

Algorithm 2 CAMs Grouping Algorithm

```
1:  for $j \leftarrow 1, N$ do
2:      $L_j \leftarrow 0;$
3:  end for
4:  $l \leftarrow i;$      $K \leftarrow 1;$
5:  while $l < i + N - 1$ do
6:      $\Omega \leftarrow \{l\};$      $m \leftarrow 1;$
7:      while $T_{l+m} - T_l \leq m \times [AIFS + (W-1)\sigma] +$
        $+ (m-1) \times T_{CAM}$ do
8:          $\Omega \leftarrow \Omega \cup \{l + m\};$
9:          $m \leftarrow m + 1;$
10:     end while
11:     $\Phi_K \leftarrow \Omega;$
12:     $L_m \leftarrow L_m + 1;$      $l \leftarrow l + m;$
13:     $K \leftarrow K + 1;$      $m \leftarrow 1;$
14: end while
```

is a *aSlotTime*, W is the Contention Window [15] and T_{CAM} is the CAM transmission time. The outcome of the Algorithm operation is that all N vehicles are split into K sets denoted as Φ_k, $k = 1 \dots K$ and further referred to as *groups*. L_m is the number of groups consisting of exactly m vehicles.

Proposition B. The CAMs of vehicles belonging to different groups Φ_k ($k = 1 \dots K$) cannot collide.

Proof: From the IEEE 802.11p backoff rules it follows that in the empty system two CAMs can never collide if their generation moments are spread in time for at least $a + (W-1)\sigma$, see line 7. When the CAMs are generated during the ongoing transmissions of other vehicles, the backoff counters freeze until the channel becomes idle. Respective maximum possible transmission delays are checked at line 7. ■

Let us consider time intervals, where the speed of the platoon is constant, i.e. before any maneuvers and after each of the four maneuvers (see Fig. 6).

The probability distribution function (PDF) of the number of groups with m vehicles is defined as $Q(m) = Pr\{x = m\} = L_m/K$. Empirical PDF $Q^*(m)$ for the above distribution is depicted[5] in Fig. 7. The results are obtained via simulations with standard IEEE 802.11p parameters as in [16]. In the first simulations, the value of Δ is set to be very small, namely, $\Delta = \sigma$.

From Fig. 7 it follows that if the CAM triggering conditions are checked by all the vehicles in the platoon continuously with a small step, then the IEEE 802.11p MAC layer CAM collision probability increases after each acceleration/deceleration maneuver due to reduced time diversity of the generation moments.

---

[5] For the sake of the plots clarity, the values of $Q^*(1)$ are not depicted.

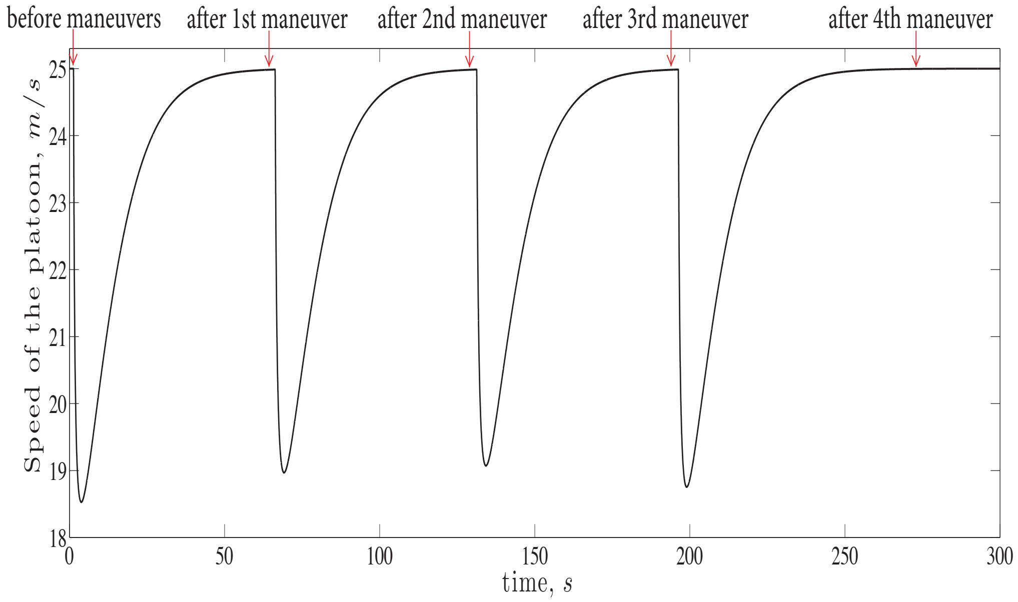


Figure 6: Reference maneuvers

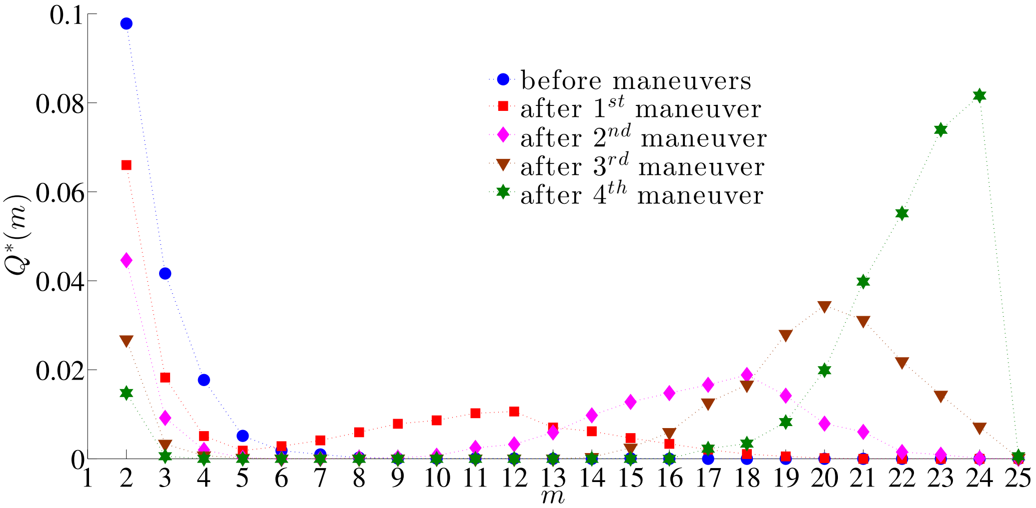


Figure 7: Influence of maneuvers on time diversity of CAM generation moments when $\Delta = \sigma$

5 Potentials to solve the problem

5.1 Reduced sampling rate

Let us examine how the increase of the sampling interval Δ influences CAMs grouping. A reduction of the sampling rate results in the increase of CAM generation moments time diversity (Fig. 8). Moreover, in contrast to the case of $\Delta \to 0$, this time diversity may increase as a result of a maneuver for $\Delta = 500\sigma$ (see $Q^*(m)$ after the 3rd and the 4th maneuvers). A group might be split when *"Event B"* occurs between its CAM generation moments.

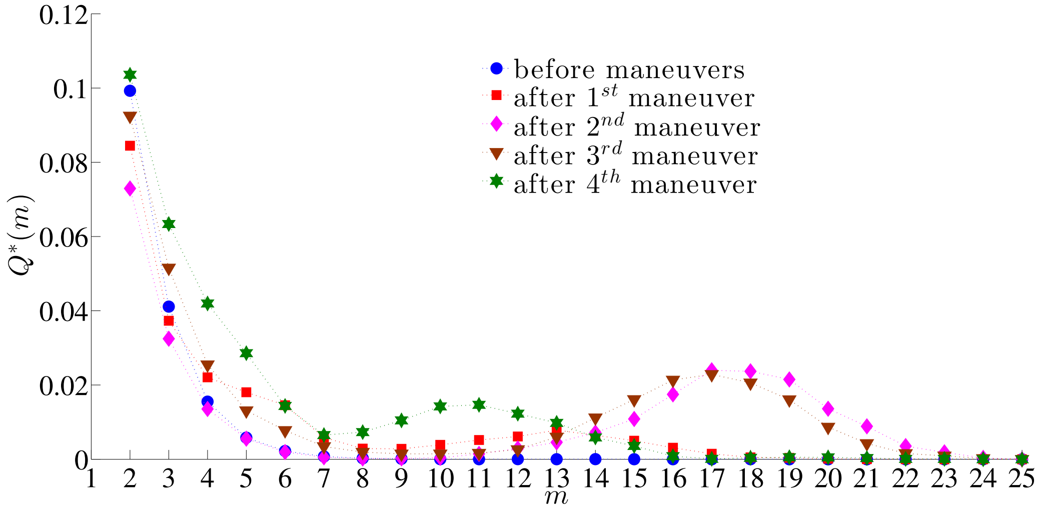


Figure 8: Influence of maneuvers on the time diversity of CAM generation moments when $\Delta = 500\sigma$

5.2 Practical considerations

Although the movements of platoon members are desired to be perfectly synchronized during all the maneuvers, a real system will impose certain restrictions to achieve this goal due to the inter-vehicle communication delays, automated control induced delays, inertness of the braking system and inaccuracies in kinematic parameters measurements.

Let $\delta = uniform[0, k\sigma]$ be a random delay, which is added to each CAM generation moment when the maneuver is performed, where k is the maximum delay expressed in time slots. δ aims at modeling the overall inaccuracies between the instance when the CAM would be triggered in the ideally synchronized platoon studied up to now and in the platoon with a non-synchronized movement of members. A random component in CAM triggering moments may diminish the grouping effect (Fig. 9).

To assess the actual impact of the ETSI rules on the CAM successful delivery per-

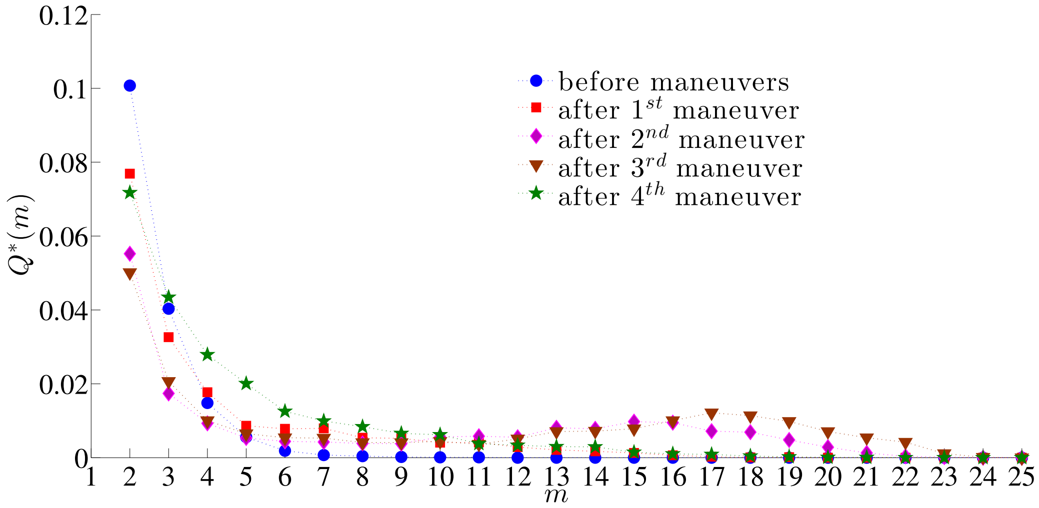


Figure 9: Influence of maneuvers on time diversity of CAM generation moments when $\Delta = \sigma$ and $\delta = uniform[0, 500\sigma]$

formance, we examine the cases when the platoon keeps a constant speed (i.e. Event A triggering CAMs) after each maneuver performed (see Fig. 6). From Fig. 10 one can see that the tunings of the parameters discussed above have a crucial impact on the CAM collision probability.

6 Conclusions and Future Work

Emerging platooning application, where a caravan of heavy-duty vehicles automatically follow a leading one, requires an exchange of updated kinematic information. This is achieved through the triggering of beacons in accordance to the ETSI EN 302 637-2 specification and their transmissions over a dedicated IEEE 802.11p random access channel.

Our study reveals a surprising conclusion: enlarging the sampling rate of the kinematic parameters will not necessarily lead to the improved cooperative awareness, because an increased congestion in the communication channel might decrease the reception rate of beacons.

We believe that our insights should be rapidly delivered to the vehicular communication research and development community and might influence the ongoing ETSI standardization.

Our future work will be dedicated to the detailed analysis of the identified problem and will be focused around two major research questions:

- What are the gains and losses in the kinematic data uptodateness with respect to the sampling rate chosen?

- Is it possible to achieve ungrouping of CAM generation moments through the adjustment of the parameters?

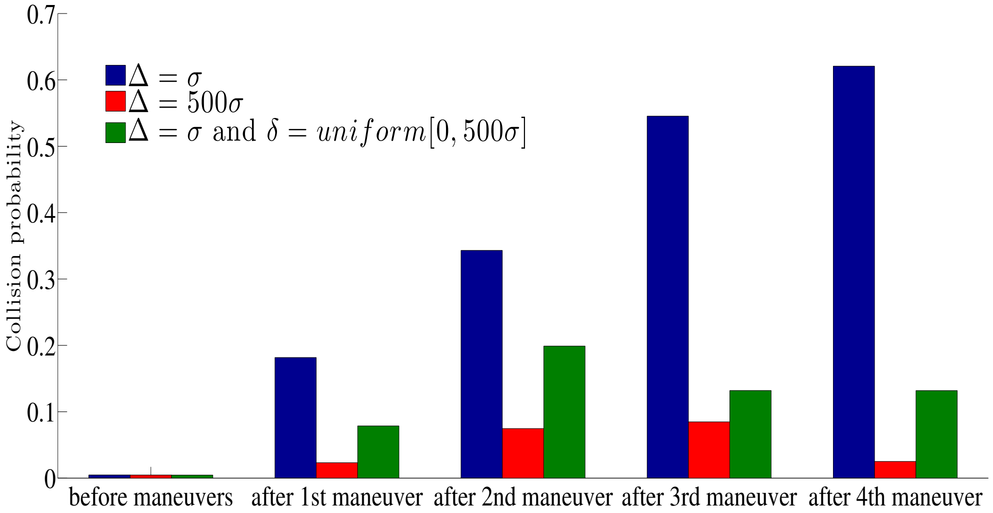


Figure 10: CAM collision probability

Acknowledgment

This study is supported by NFITS - National ITS Postgraduate School (Sweden) and is a part of the "ACDC: Autonomous Cooperative Driving: Communications Issues" project (2014-2016) funded by the Knowledge Foundation (Sweden) in cooperation with Volvo GTT, Volvo Cars, Scania, Kapsch TrafficCom and Qamcom Research & Technology.

References

[1] F. Dressler, H. Hartenstein, O. Altintas, and O. Tonguz, “Inter-vehicle communication: Quo vadis,” *Communications Magazine, IEEE*, vol. 52, no. 6, pp. 170–177, 2014.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 4, pp. 584–616, 2011.

[3] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, "Modeling prioritized broadcasting in multichannel vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, 2012.

[4] X. Ma, J. Zhang, X. Yin, and K. S. Trivedi, "Design and analysis of a robust broadcast scheme for vanet safety-related services," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 1, pp. 46–61, 2012.

[5] E. Egea-Lopez, J. J. Alcaraz, J. Vales-Alonso, A. Festag, and J. Garcia-Haro, "Statistical beaconing congestion control for vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 9, pp. 4162–4181, 2013.

[6] K. Karlsson, C. Bergenhem, and E. Hedin, "Field measurements of ieee 802.11p communication in nlos environments for a platooning application," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, Sept 2012, pp. 1–5.

[7] L. Xu, L. Y. Wang, G. Yin, and H. Zhang, "Communication information structures and contents for enhanced safety of highway vehicle platoons," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4206–4220, Nov 2014.

[8] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. L. Cigno, and F. Dressler, "Towards inter-vehicle communication strategies for platooning support," in *2014 7th International Workshop on Communication Technologies for Vehicles (Nets4Cars-Fall)*, Oct 2014, pp. 1–6.

[9] M. Jonsson, K. Kunert, and A. Böhm, "Increased communication reliability for delay-sensitive platooning applications on top of ieee 802.11p," in *Communication Technologies for Vehicles*, M. Berbineau, M. Jonsson, J.-M. Bonnin, S. Cherkaoui, M. Aguado, C. Rico-Garcia, H. Ghannoum, R. Mehmood, and A. Vinel, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 121–135.

[10] A. Böhm, M. Jonsson, K. Kunert, and A. Vinel, "Context-aware retransmission scheme for increased reliability in platooning applications," in *Communication Technologies for Vehicles*, A. Sikora, M. Berbineau, A. Vinel, M. Jonsson, A. Pirovano, and M. Aguado, Eds. Cham: Springer International Publishing, 2014, pp. 30–42.

[11] C. Shao, S. Leng, Y. Zhang, A. Vinel, and M. Jonsson, "Analysis of connectivity probability in platoon-based vehicular ad hoc networks," in *2014 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Aug 2014, pp. 706–711.

[12] A. Böhm, M. Jonsson, and E. Uhlemann, "Co-existing periodic beaconing and hazard warnings in ieee 802.11p-based platooning applications," in *Proceeding of the Tenth ACM International Workshop on Vehicular Inter-networking, Systems, and Applications*, ser. VANET '13. New York, NY, USA: ACM, 2013, pp. 99–102. [Online]. Available: http://doi.acm.org/10.1145/2482967.2482973

[13] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *ETSI EN 302 637-2 V1.3.2*, 2014.

[14] K. Lidstrom, K. Sjoberg, U. Holmberg, J. Andersson, F. Bergh, M. Bjade, and S. Mak, "A modular cacc system integration and design," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 13, no. 3, pp. 1050–1061, 2012.

[15] "IEEE std. 802.11-2012, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std. 802.11-2012*, 2012.

[16] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks." *IEEE Communications letters*, vol. 18, no. 1, pp. 110–113, 2014.

[17] B. Van Arem, C. J. Van Driel, and R. Visser, "The impact of cooperative adaptive cruise control on traffic-flow characteristics," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 7, no. 4, pp. 429–436, 2006.

[18] A. Kesting, M. Treiber, and D. Helbing, "Enhanced intelligent driver model to access the impact of driving strategies on traffic capacity," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 368, no. 1928, pp. 4585–4605, 2010.

[19] "Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part," *ETSI TS 102 687 V1.1.1*, 2011.

PAPER 2

ETSI DCC: Decentralized Congestion Control in C-ITS

Authors:
Nikita Lyamin, Alexey Vinel, Dieter Smely and Boris Bellalta

Reformatted version of paper accepted for publication in:
IEEE Communications Magazine.

ETSI DCC: Decentralized Congestion Control in C-ITS

Nikita Lyamin, Alexey Vinel, Dieter Smely and Boris Bellalta

Abstract

Decentralized Congestion Control (DCC) is a mandatory component of 5.9 GHz Intelligent Transportation Systems (ITS-G5) vehicular communication protocol stack that reduces radio channel overload, range degradation, and self interference. In this tutorial article we explain its principle, describe related ongoing standardization activities, evaluate its performance for emerging cooperative driving applications, and identify ways for improvement. We show that failure to use a proper DCC parameterization can impact negatively on the performance of cooperative vehicular applications.

1 Introduction

Cooperative Intelligent Transportation Systems (C-ITS) use the connectivity between vehicles, roadside infrastructure, and other road users to enhance driving safety and comfort, and improve traffic management. Regular exchange of information between road users (*beaconing*) keeps them informed about each other's position, driving kinematics, and other attributes. This is one of the cornerstone of road safety and traffic efficiency applications on the way towards autonomous driving.

To facilitate C-ITS, the European Telecommunication Standards Institute (ETSI) in ETSI EN 302 665 specified the ITS-G5 architecture and a communication protocol stack to be used in the 5.9 GHz spectrum. ITS-G5 adopts the medium access control (MAC) and the physical (PHY) layer techniques from the IEEE 802.11 standard like the widely adopted Wi-Fi.

C-ITS communications must also be operational in dense road traffic. Assuming that all vehicles participate in the C-ITS information exchange by broadcasting periodic messages, wireless channel congestion is likely to occur. Thus, to avoid degradation of the system performance caused by too high a channel load and provide a fair access to the channel resources among neighboring ITS-G5 stations (ITS-S), channel congestion control mechanisms are required. To this end ETSI published TS 102 687 [1] – a specification of a decentralized congestion control (DCC) mechanism – as a part of the ITS-G5 protocol stack. DCC is a mandatory component of ITS-S operating in the 5.9 GHz frequency band.

However, restricting the communication exchange in safety-critical applications, which are very delay-sensitive could potentially lead to undesirable performance degradation.

Several studies show, that the performance of the ETSI DCC needs further investigation [2], to find more efficient DCC parameter settings than the default one, to prevent possible performance degradation of C-ITS [3]. Thus, in this tutorial paper we first present an overview of the state-of-the-art in DCC for vehicular communications. Then we evaluate the performance of the cooperative driving application enabled by ETSI ITS-G5 communications via several simulation experiments to assess the potential influence of DCC on the performance of the system.

The paper is organized as follows: Section 2 provides a tutorial on the standardization and the related research literature. In Section 3 we describe the system model, including the principal assumptions on the cooperative driving scenario considered, the mobility model and the communication setups. In Section 4 we present the simulation study of C-ITS system enabled by ITS-G5 vehicular communication stack, discuss the results, and give recommendations for further development. Finally, Section 5 contains the conclusions drawn from the study.

2 Standards and Literature

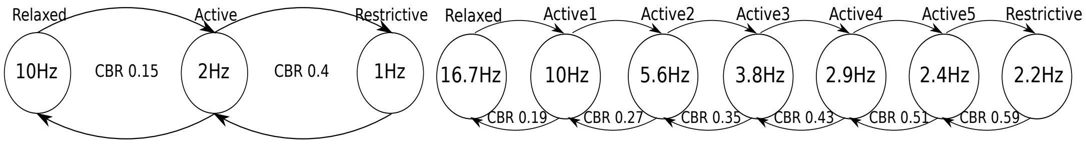
2.1 ETSI DCC standardization

ETSI is an international standardization body based in France. ETSI develops standards – European Norms (EN) and Technical Specifications (TS) – comprising normative requirements that enable interoperability between the devices of different vendors and also avoid harmful radio interference. ETSI also develops non normative documents that contain additional information or guidance. The drafting of the documents is done by Technical Committees (TC), consisting of delegates of ETSI members and by expert groups called Specialist Task Force (STF) consisting of selected experts. All C-ITS documents are drafted by the TC ITS and the associated five Work Groups (WG1 to WG5) temporarily supported by STFs.

ETSI TC ITS WG4 first introduced DCC in ETSI TS 102 687 [1] and this standard is the focus of our work. It introduced a state machine approach at access layer to adapt several transmission parameters to the measured channel load. Each state is associated with a certain channel load range and a set of transmission parameters. Our study presented in this article inspired the revision of [1]. In this revision [4] the DCC algorithms are adapted to the channel load limit approach specified by ETSI TC ITS WG2 in ETSI TS 103 175 [5]. Specification [4] also allows for different algorithms to be implemented.

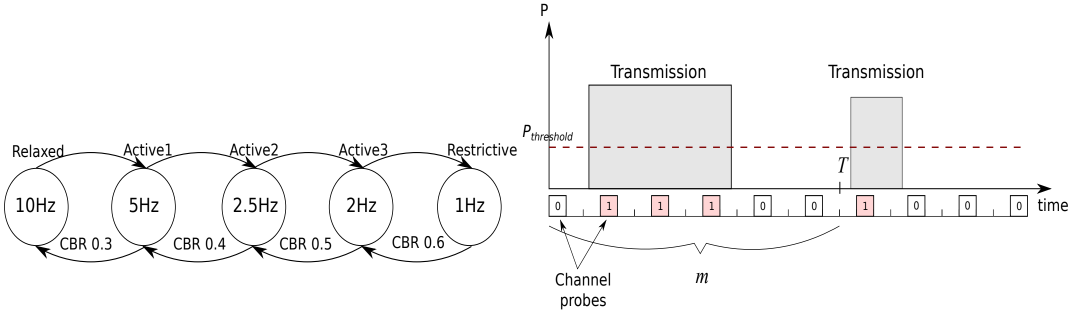
DCC can operate as gatekeeper on the medium access layer, but higher layer DCC functionalities are possible, as specified in [5]. DCC as specified in [1] is based on a state machine that has three states: Relax, Active and Restrictive, as shown in Figure 1.a.

In each DCC state the restrictions on the transmission parameters are defined. ETSI DCC in general considers the five following mechanisms to control the vehicle's channel access: "Transmit Power Control" (TPC), "Transmit Rate Control" (TRC), "Transmit Datarate Control" (TDC), "DCC Sensitivity Control" (DSC), "Transmit Access Control"



a) ETSI TS 102 687 Configuration, "DCC 2+1"

c) ETSI TR 101 612 Configuration, "DCC 2+5"



b)ETSI TS 103 175 Configuration, "DCC 2+3"

d)Channel Busy Ratio (CBR) measurement

Figure 1: DCC state machines and CBR measurement procedure (m is the number of channel probes within the measurement period T)

(TAC).

The choice of the DCC state is performed based on the evaluation of a so-called *Channel Busy Ratio* (CBR). ETSI suggests the following reference method to estimate the value of CBR. The ITS-S makes periodic channel probes and calculates the proportion of time the channel was busy during a measuring interval $T = 1\ s$ [1]. To calculate the time the channel was occupied, the ITS-S should take m measurements of the received signal level uniformly distributed within the measuring interval. The time between two channel probes should be set to detect the transmission of the smallest possible packet at the highest available datarate. For all channel probes of length 10 μs the average signal level P is determined. Then the CBR measure for the received signal level threshold $P\_threshold$ (-85 dBm by default) is given as: $CBR = \sum_{i=1}^{m}(\text{probes} \quad \text{with} \quad P > P\_threshold)/m$, as shown in Figure 1.d.

Each transition in the state machine has a corresponding CBR value as threshold (Fig. 1), the transition is performed under one of the two following conditions:

1. *Transition to a more restrictive state:* If the CBR value was above the threshold during the last observed measuring interval.

2. *Transition to a less restrictive state*: If the CBR was below the threshold during the last five consecutive observed measuring intervals.

In each state of the state machine, TRC specifies the minimum time interval between two subsequent transmissions, i.e. TRC specifies the maximum possible transmission rate (messages per second) for each appropriate state.

ETSI DCC also allows state-machine configurations containing a set of sub-states in the "Active" state. This approach enables finer granularity of the DCC state transitions possible. The state machine is fully meshed to allow for transitions between any two states, depending solely on the CBR measurements history, i.e. in defining the current state DCC relies only on the recent CBR measurements and may switch from one state to another in a single step. For simplicity, transitions between non-neighboring states are omitted in Figure 1. Thus, DCC-configurations with a reasonable number of sub-states may help prevent rapid changes in the C-ITS transmission behavior, maintaining the targeted level of congestion. Figures 1.b and 1.c show the implementations of the DCC state machine with additional number of sub-states in Active state, taken from [5] and [6], accordingly.

Hereafter, we referred to 3 DCC configurations shown in Figure 1 as "DCC 2+1", "DCC 2+5", "DCC 2+3" by the number of sub-states in the Active state of the DCC state machine.

2.2 Literature overview

The performance of ETSI DCC has been discussed in several studies. The authors of [2] present an extensive performance evaluation of the 3-states ETSI DCC for various CBR values. Based on simulation results, the paper considers the effectiveness of various ETSI DCC CBR control mechanisms (TPC, DSC, TRC, DCC) from the communication and application point of view. Other studies of ETSI DCC demonstrated that the basic 3-state DCC configuration may show low performance. In [7] it is demonstrated that the basic 3-state configuration of DCC [1] tends to oscillate, i.e. to repeatedly switch between relaxed to active and restrictive states. The "unfairness" of the 3-state ETSI DCC configuration [1] was also explained in [3]. The authors show that in a high vehicle density scenario ITS-S may experience unfairness in terms of channel access. The reason for this is a condition when two neighboring ITS-S (i.e. that are in the same communication range) choose different states of the DCC state-machine. Based on the simulation study presented in [8], the authors conclude that a DCC state machine with 3 states has poor performance in terms of its ability to adjust its state to varying CBR values.

Thus, alternative ETSI DCC configurations and parameter sets have been proposed in the literature to overcome aforementioned drawbacks. For example, in [9] the focus is on to the tuning of the TDC configuration. Following the outcome of their previous study, in [10], the authors propose using only TDC (transmit datarate control) for a 3-state DCC configuration, keeping the transmit power level and the sensitivity level for all states at a constant value equal to the Active state of the ETSI DCC 3-state configuration of [1]. In [9] the authors also focus on adjusting the TDC. The novelty of their DCC design is that the switch between different DCC states is performed using a hysteresis curve for the CBR instead of conventional thresholds. The hysteresis mechanism allows a better control of the CBR trend based on the last measurement interval. It also allows different CBR values for the same state, depending on whether the local CBR increases or decreases in comparison to the previous measurement interval.

Another way to enhance DCC performance suggested in the literature is to increase the number of sub-states in the active state. Thus, the authors in [8] propose a 6-state DCC configuration based on TPC in combination with different CBR thresholds for each state to introduce a negative feedback to the control loop. To obtain the CBR thresholds, the authors identify the channel load that they considered to be an optimum balance between improving channel utilization and packet collisions and select the state transition parameters so that the state machine operates close to this optimal channel load. The target CBR value was identified through simulations of various vehicular densities. The simulation results presented in the paper show that a CBR value of 0.65 is a reasonable value for the channel load, regardless of the vehicle density or the CBR threshold.

Following a similar approach, the authors in [11] propose the use of DCC with several sub-states in Active state together with TPC. The CBR thresholds for the state transitions are selected according to CCA (clear channel assessment) value. The authors introduce a TRC implementation that gradually decreases the beaconing rate from 10 Hz to 1 Hz following the increase of CBR. Finally, it was shown that a DCC configuration with more Active sub-states has a better performance due to its improved adaptivity to varying CBR values.

Other attempts are taken in the direction of avoiding the ETSI DCC re-active state-machine involve controlling the CBR pro-actively. In [12] the authors perform a simulation study to compare the performance of the ETSI DCC state machine with several sub-states in Active state with a linear adaptive DCC packet rate control mechanism called LIMERIC. For both configurations, only TRC is considered. In the presented setup LIMERIC outperforms the state-machine approach in terms of IPG (inter packet gap).

3 Prerequisites

3.1 Scenario

The simulation study presented in this paper focuses on the C-ITS use case named *platooning* [13], which is one of the applications considered to be an early adopter of C-ITS technology. In platooning the leading vehicle is driven by a professional driver, while the following vehicles execute at least longitudinal automatic control or can even be switched to a fully autonomous mode with a lateral control, as well. The main purpose of platooning is to reduce air-drag in a caravan of heavy-duty vehicles, which can significantly improve fuel consumption.

We choose platooning as an illustrative C-ITS application example to show how even small variations in the configuration of ITS-G5 communications may affect the performance of safety and time-critical C-ITS applications. At present, pre-standardization activities are still ongoing at ETSI TR 103 301 and TR 103 299, which are studying the applicability of currently available standards for platooning applications [13]. Therefore, a way to enable functioning of the platoon's automatic control system based on the current standardization framework is considered in this article (ETSI specifications [1, 5], and [6]), which could be summarized as follows:

- A vehicle generates Cooperative Awareness Messages (CAMs) based on one of the following approaches:

  - fixed triggering frequency f_{CAM} messages per second (henceforth called, *static CAM*).
  - kinematic-based triggering in accordance with ETSI EN 302 637-2 (henceforth called, *ETSI CAM*). In ETSI CAM a vehicle generates new CAMs depending on its current speed, acceleration, deceleration, and change of direction [14].

- The time elapsed since last CAM transmission is checked for compliance with TRC. In the case the TRC timer is still active, the CAM is queued until the TRC timer elapses, or dropped when the CAM lifetime expires.

- If the CAM is not dropped, it is transmitted on the dedicated channel in accordance with the CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) 802.11p MAC protocol. Currently ETSI allocates five channels of 10 MHz bandwidth each (one management channel and four service channels). We assume that platooning operates in one of the four dedicated service channels.

In order to test the effect of various legacy communication configurations on the performance of the platooning application we assume 12 setups, that are obtained by combining of 3 DCC configurations ("DCC 2+1", "DCC 2+3", "DCC 2+5") [1, 5, 6], and 4 CAM generation policies (three static CAM: 10 Hz, 20 Hz, 30 Hz, and ETSI CAM).

In this article we focus on DCC based on TRC, i.e. a state machine for the packet rate control. A pure packet rate control mechanism has several advantages: most importantly it is easy to implement and has an immediate impact on the channel load across the entire radio range. Other concepts, also described in ETSI TS 102 687, either need information exchange between the ITS-S to control the local CBR (datarate control) or influence the communication range (transmit power control). The latter has disadvantages for platooning, since envisaged control strategies require that all the vehicles in the platoon are within the same communication range, enabling one-hop connectivity from the leader to all members. In addition, there are no DCC parameters for TPC, TDC, DSC and TAC available in the literature ([5, 6]) for the configurations shown in Figures 1.b and 1.c.

To test the performance of DCC and both kinematic-based and fixed beaconing approaches, we study the following reference scenario:

- We consider a platoon consisting of N vehicles moving along a highway.

- The platoon moves along the straight stretch of a road with a target speed for the leading vehicle V, and a target gap d between platoon members. Each vehicle in the platoon adapts its speed according to the kinematic information received from the platoon leader and the preceding vehicle. We use a longitudinal control algorithm based on the sliding surface method of the controller design.

- For the speed pattern we assume a "disturbance scenario" as introduced in [14] (see Figure 1). The scenario reflects the situation when a slower vehicle approaches the right-most lane from a highway ramp or after a lane change.

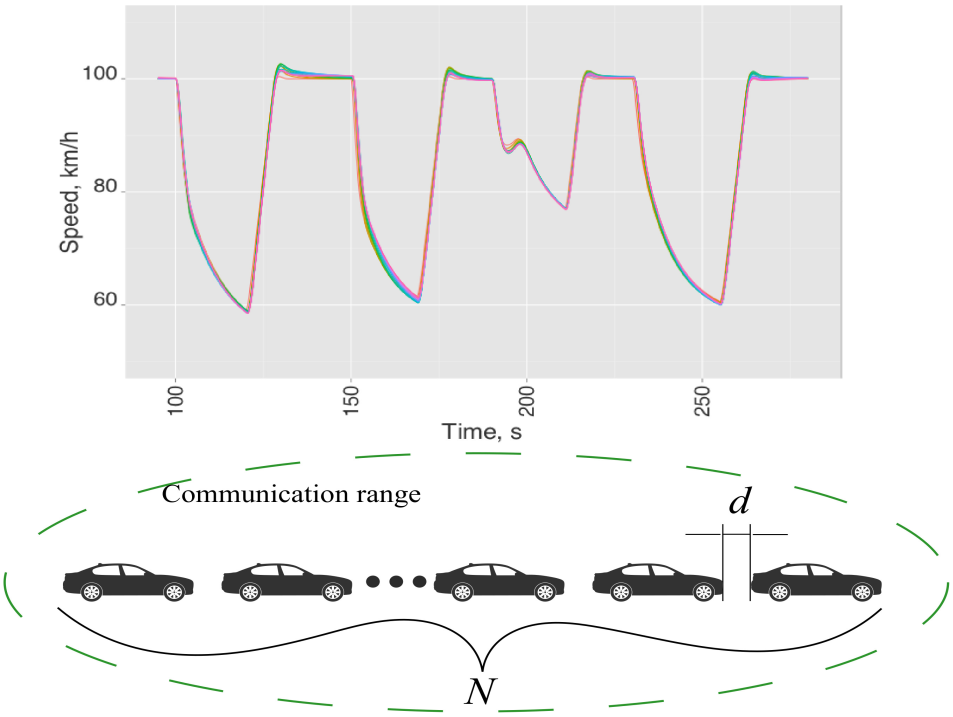


Figure 2: Reference scenario: color lines represent example speed profiles of the vehicles

3.2 Performance metrics

We use the following metrics for performance evaluation:

1. Box-plot of inter-vehicle gaps. The variation of inter-vehicle gaps reflects the ability of platoon members to maintain the target distance from the preceding vehicles. In [15] it is shown that the ability of a platoon to keep precise inter-vehicle gaps contributes to its fuel efficiency. We draw box plots of inter-vehicle gap distances for all vehicles in the platoon and for all runs of a given scenario. In each box, the central red mark indicates the median, and the bottom and top blue edges of the box indicate the 25th and 75th percentiles, respectively. The whiskers extend to the most extreme data points not considered as outliers, and the outliers (minimum and maximum values in a data set) are plotted individually using the red '+' symbol.

2. Box-plot of the CBR. The channel busy ratio characterizes the performance of DCC and its ability to keep the channel load below congestion. As with the inter-vehicle gap, we present CBR measurements in the form of a box plot.

3. Probability Mass Function (PMF) of the data age ($f(t)$). The data age is a random variable defined as the time elapsed since the last successfully received packet of vehicle $2 \leq n \leq N$ by the leading vehicle. Data age is the difference between the current point in time and the latest point when the leading vehicle has successfully received a CAM from a vehicle n [13]. In this article, the PMF of the data age for

the last vehicle N in the platoon is calculated, in order to study the farthest pair of communicating nodes.

4 Performance evaluation

4.1 Simulation environment

In our simulation study we use Plexe – a simulator that supports a realistic simulation of a platooning system. The simulator is a combination of the two well-known and widely-used simulators Omnet++ and SUMO. Omnet++ is an event-driven network simulator that models the network part, while SUMO handles the mobility of the nodes (vehicles).

Our simulation setup uses the following parameters: The platoon consists of $N = 15$ vehicles with a target inter-vehicle gap $d = 5$ m, and a platoon leader target speed of $V = 100$ km/h. We also implemented the DCC state machine together with the kinematic-based ETSI CAM triggering mechanism, to meet the standardization requirements. Static CAM triggering policies with $F_{CAM} = \{10, 20, 30\}$ Hz and kinematic-based ETSI CAM triggering with a sampling rate $T\_CheckCamGen = 50$ ms are tested. The size of the CAM message is $L = 2000$ bytes at a data rate of $R = 6$ Mbit/s.

We set the transmission power level to 23 dBm (200 mW) EIRP, which is the maximum allowed value that can be used in SCH1. The radio channel is simulated by a log-distance path loss model with a path loss exponent γ=2. For the reference length of a vehicle - 5 meters - this setup guarantees that even the last platoon member can detect unequivocally an ongoing transmission or packet collision.

The CBR estimation conforms to the standardized procedure [1] as described in Section II, but for the simplicity of implementation it is adjusted to our modeling assumptions in the simulator. Since in our setup the duration of all CAM transmission times is the same (L/R), and all the vehicles are in each other's communication range, an ITS-S counts the number of message transmissions M observed (including CAM collisions) during T and applies the formula $CBR = (M \cdot L/R)/T$.

4.2 Discussion

Figure 3 shows the box plot for the inter-vehicle distances and Figure 4 shows the box plot of CBR for all the considered communication setups. The plots are clustered in 3 groups based on the number of DCC states.

In all setups, the average inter-vehicle gap is kept close to the desired d of 5 meters. It would be logical to assume, the higher the CAM rate, the better the performance of the platoon, which however, is not always the case. It is noticeable, that for all three DCC configurations ETSI CAM outperforms the static CAM beaconing approach (see Figure 3). This is because ETSI CAM triggers more messages when the ITS-S behavior is highly dynamic and fewer messages for the constant speed movement. Thus, the CBR generated by the ITS-S mimics the platoon's speed pattern (see Figure 5). In other words, the channel is not overloaded when the platoon maintains a stable speed, while

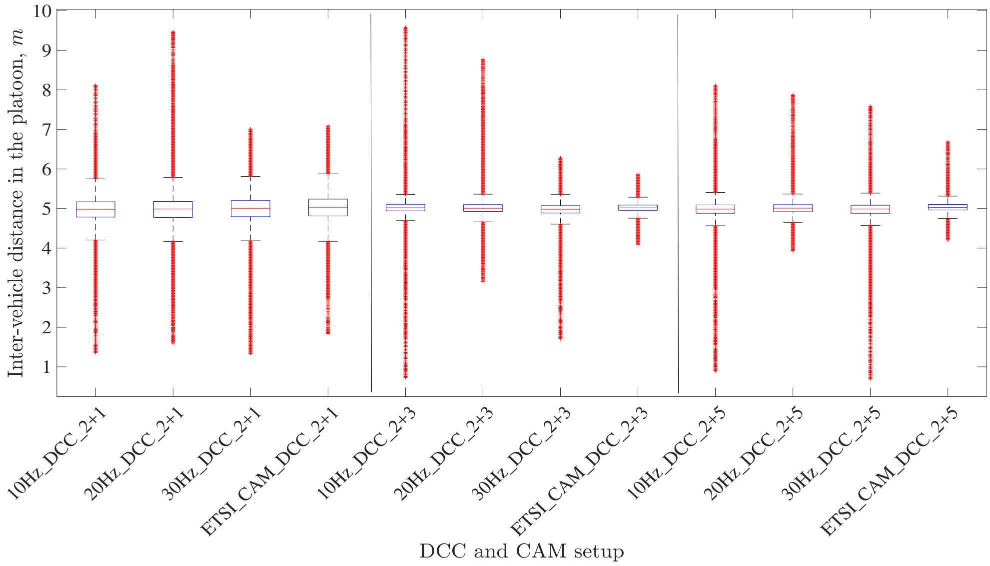


Figure 3: Inter-vehicle distances

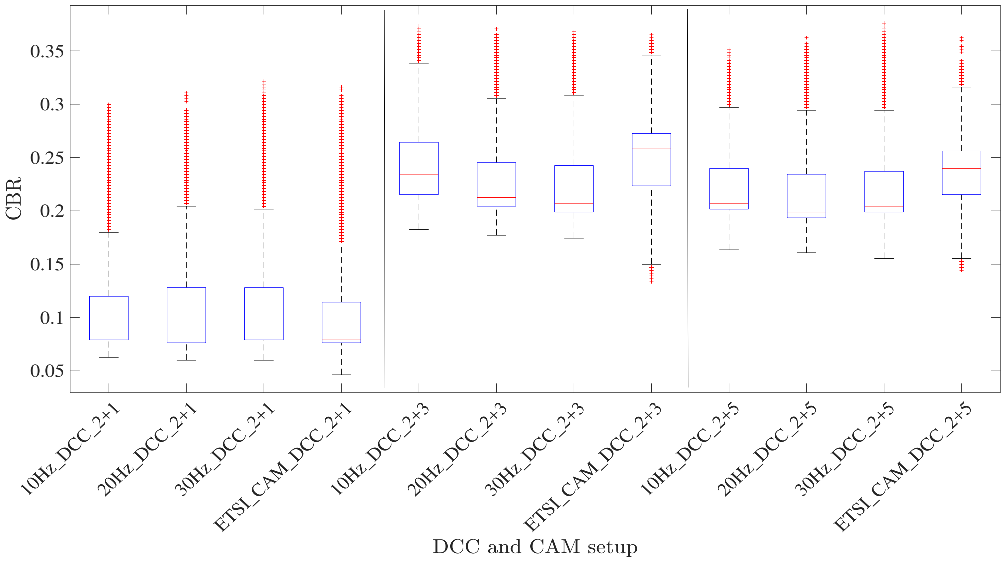


Figure 4: Channel Busy Ratio

channel occupancy grows whenever maneuvers are performed. Such patterns give time for the vehicles to exchange more messages before DCC starts to react on the CBR increase, which at the same time comes at the expense of higher CBR peak values (see Figure 4).

According to [6], when the number of vehicles in the communication range is below 100, DCC should be able to maintain the CBR level below 0.55. In our setup the CBR value never exceeds higher than 0.4, although without DCC the CAM messages transmitted at $F_{CAM} = 30$ Hz may easily overload the channel (the rough estimation of the traffic N vehicles may create without DCC is $\frac{N \cdot F_{CAM} \cdot L}{R} \approx 1.2$). From this we conclude that all three configurations of DCC can control CBR at an allowable level.

Configuration "DCC 2+1" demonstrates inferior performance to the other two configurations, due to limiting the transmission rate even the CBR is well below 0.55 (see Figure 4). This is due to an absence of intermediate sub-states in the "active" state: Whenever the state machine makes a transition from the "relaxed" to the "active" state, it has a 2 Hz allowed transmission rate, while "DCC 2+3" and "DCC 2+5" have a better granularity in terms of allowed transmission rate values (see Figure 1).

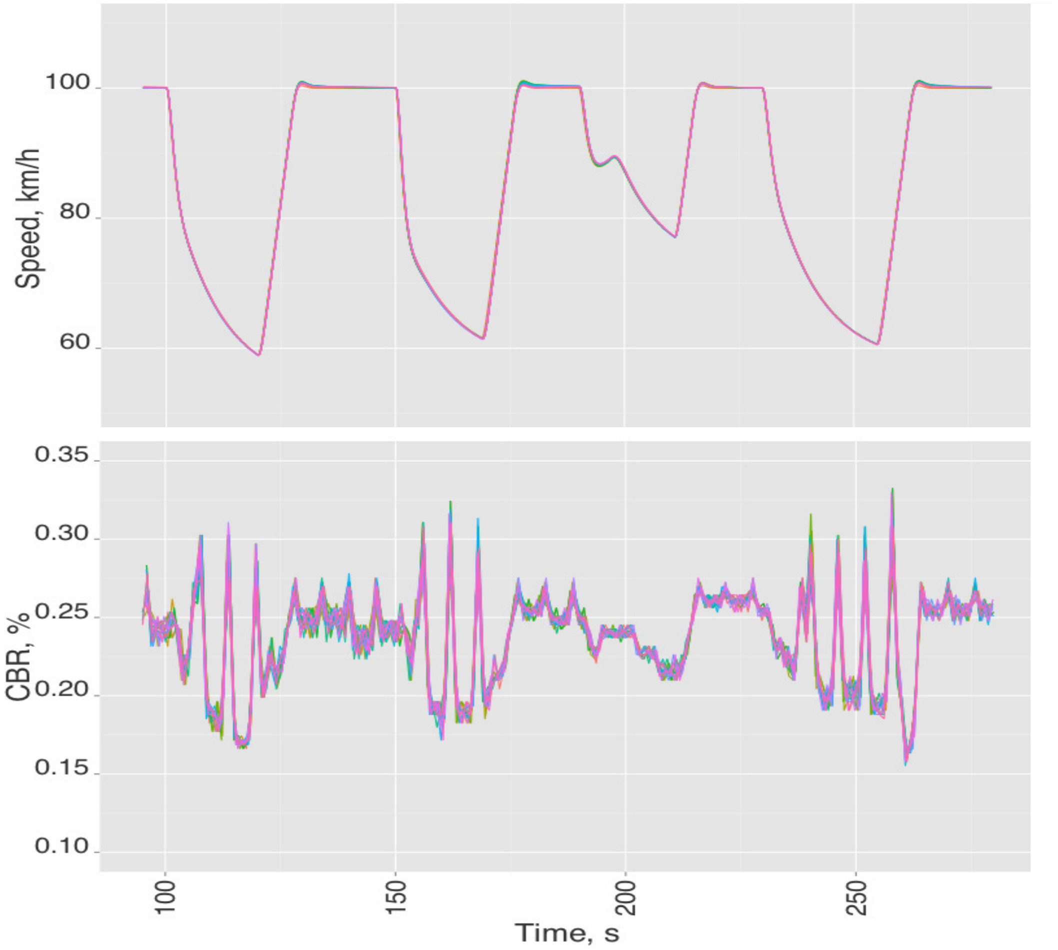


Figure 5: Representation of CBR measurements for one experiment run using "DCC 2+5 ETSI CAM": color lines represent different platoon members.

Figure 6 shows the data-age PMF distributions for all three DCC setups with the ETSI CAM. For "DCC 2+1" most of the data-age values are around 0.1 s and 0.5 s, which corresponds to "Relaxed" (10 Hz) and "Active" (2 Hz) states. The reason for

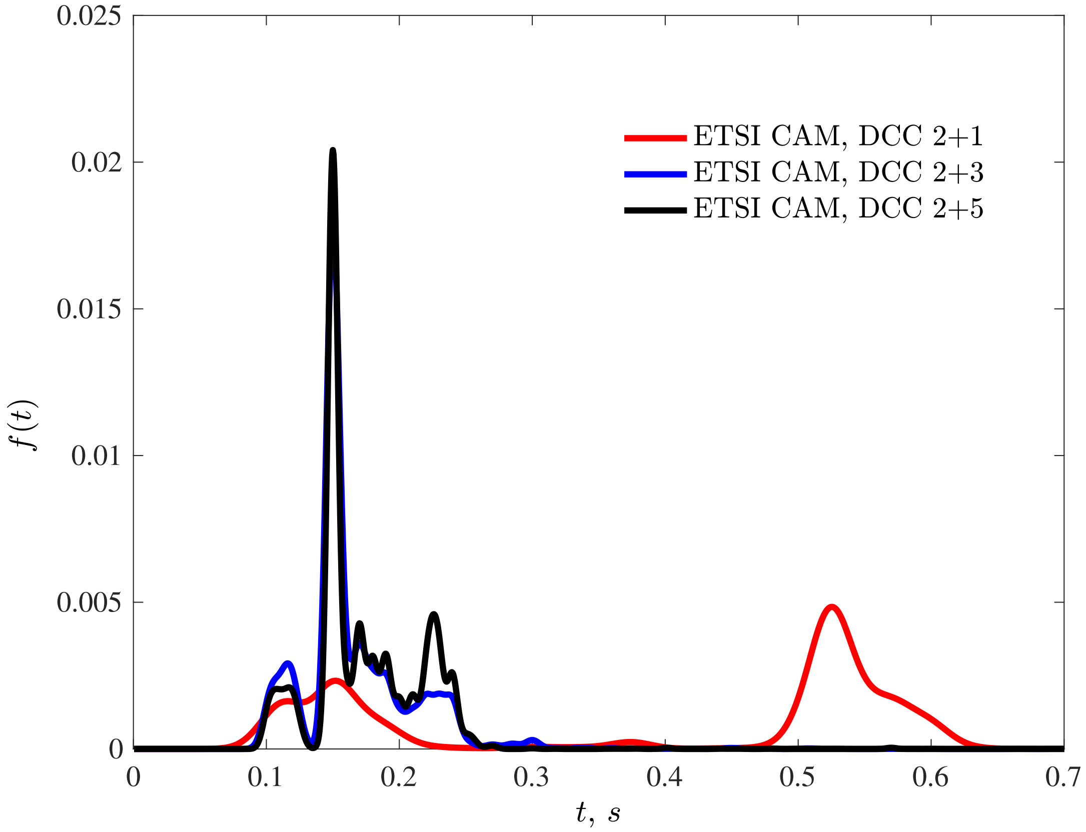


Figure 6: Empirical probability density function of the data age

significant density values around 0.15 s when using the ETSI CAM is as follows. When the platoon maintains a speed of $V = 100$ km/h (27.8 m/s) the CAMs are triggered with $\frac{27.8}{4} \approx 7$ Hz, which corresponds to a data-age value of $1/7 \approx 0.15$ s. Similarly, for "DCC 2+3" and "DCC 2+5" the PDF maximum values are concentrated around the rates defined by the TRC configuration of the corresponding DCC state machine. Thus, we conclude that the configuration of the DCC state machine has a direct impact on the data age distribution shape. It can be seen that the data age values are grouped exactly at the points specified by the DCC TRC configuration and almost never take any other values. This fact provides us with empirical evidence, that platooning may benefit from DCC configurations with more states, which could allow smoother control of data age while maintaining the required CBR level.

5 Conclusion and open challenges

ETSI standardization on the Decentralized Channel Control (DCC), which is a crucial element in controlling the channel load in ITS-G5-based C-ITS networks, is ongoing.

Currently, according to ETSI, a satisfactory range for the channel busy ratio (CBR) is 0.55 to 0.75 [6]. From our study, we conclude that for the legacy ETSI DCC configurations, when the number of closely located cooperatively driving vehicles is below 15, the CBR value is always less than 0.4, even if the assumed message length is as great as 2000 Bytes. We demonstrate that the unnecessary low values of the actual CBR generated by the current ETSI DCC configurations, will have a major negative impact on the performance of C-ITS applications in terms of achieved data age. The under-utilized channel resources for time-critical applications demonstrate the need for further DCC optimization, which includes:

- A justified approach for the selection of CBR thresholds for the ETSI DCC state-machine configurations or a more efficient DCC mechanism/algorithm is required.
- To date, the parameter values settings for ETSI DCC CBR control mechanism, e.g. TPC, TDC and DSC are not well specified in the existing ETSI specifications and need further development.

Having said the above, the most importantly, we would emphasize that the currently specified ETSI DCC configurations are designed to control the CBR level as such, but not the system level C-ITS application metrics. Standards for several safety-critical C-ITS applications (e.g. platooning) are currently under development. Appropriate control criteria for channel congestion level could be selected to make the DCC to target at optimizing the applications performance metrics. For this purpose, mechanisms are needed to estimate the influence of the CBR limits on the performance of C-ITS applications.

In our opinion, mathematical models of the DCC are clearly needed to better characterize and understand the complex dynamics of C-ITS systems further. This demand is especially emerging, since the studies of the ETSI DCC which are currently available in the literature [9, 10, 8, 11] rely on the simulation experiments of specific scenarios and the theoretical foundations to develop the DCC configurations are required.

The results presented in this article were used as one of the inputs for revising [1]. A new version of the ETSI DCC standard [4] includes the following modifications:

- states in state machine are no longer meshed and are adapted to [5],
- TAC and DCS were removed,
- a restriction on the transmission duration was introduced,
- the measurement period T was reduced,
- an alternative linear control algorithm was introduced.

However, the open questions presented above have not yet been fully addressed yet.

Acknowledgments

The research leading to the results reported in this work has received funding from the Knowledge Foundation (Sweden) and from the ELLIIT Strategic Research Network.

References

[1] "Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part," *ETSI TS 102 687 V1.1.1*, 2011.

[2] A. Autolitano, C. Campolo, A. Molinaro, R. M. Scopigno, and A. Vesco, "An insight into decentralized congestion control techniques for VANETs from ETSI TS 102 687 V1. 1.1," in *Wireless Days (WD), 2013 IFIP.* IEEE, 2013, pp. 1–6.

[3] S. Kuk and H. Kim, "Preventing unfairness in the ETSI distributed congestion control," *Communications Letters, IEEE*, vol. 18, no. 7, pp. 1222–1225, 2014.

[4] "Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part," *ETSI TS 102 687 V1.2.1*, 2018.

[5] "Intelligent transport systems (ITS); cross layer DCC management entity for operation in the ITS G5A and ITS G5B medium." *ETSI TS 103 175 V1.1.1*, 2015.

[6] "Intelligent transport systems (ITS); cross layer dcc management entity for operation in the ITS G5A and ITS G5B medium; report on cross layer dcc algorithms and performance evaluation," *ETSI TS 101 612 V1.1.1*, 2014.

[7] D. Eckhoff, N. Sofra, and R. German, "A performance study of cooperative awareness in ETSI ITS G5 and IEEE WAVE," in *2013 10th Annual Conference on Wireless On-Demand Network Systems and Services, WONS 2013*, August 2013, pp. 196–200.

[8] S. Subramanian, M. Werner, S. Liu, J. Jose, R. Lupoaie, and X. Wu, "Congestion control for vehicular safety: synchronous and asynchronous mac algorithms," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications.* ACM, June 2012, pp. 63–72.

[9] C. B. Math, A. Ozgur, S. H. de Groot, and H. Li, "Data rate based congestion control in V2V communication for traffic safety applications," in *2015 IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT)*, November 2015, pp. 1–6.

[10] S. Yang, H. Kim, and S. Kuk, "Less is more: need to simplify ETSI distributed congestion control algorithm," *Electronics Letters*, vol. 50, no. 4, pp. 279–281, February 2014.

[11] A. A. Gómez and C. F. Mecklenbräuker, "Dependability of decentralized congestion control for varying vanet density," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 11, pp. 9153–9167, January 2016.

[12] B. Cheng, A. Rostami, M. Gruteser, J. B. Kenney, G. Bansal, and K. Sjoberg, "Performance evaluation of a mixed vehicular network with CAM-DCC and LIMERIC vehicles," in *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, July 2015, pp. 1–6.

[13] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-Vehicle communication in C-ACC/Platooning scenarios," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[14] N. Lyamin, A. Vinel, M. Jonsson, and B. Bellalta, "Cooperative awareness in VANETs: On ETSI EN 302 637-2 performance," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 17–28, January 2018.

[15] N. Lyamin, Q. Deng, and A. Vinel, "Study of the platooning fuel efficiency under ETSI ITS-G5 communications," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, November 2016, pp. 551–556.

PAPER 2a

Study of the Platooning Fuel Efficiency under ETSI ITS-G5 Communications

Authors:
Nikita Lyamin, Qichen Deng, Alexey Vinel

Reformatted version of paper originally published in:
IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)

Study of the Platooning Fuel Efficiency under ETSI ITS-G5 Communications

Nikita Lyamin, Qichen Deng, Alexey Vinel

Abstract

In this paper we evaluate the performance of platoon enabled by contemporary ITS-G5 vehicular communications through a number of simulation experiments. We assess platooning fuel consumption performance under two communication setups and estimate the potential influence of the communication system on the efficiency of the platooning. We also make an attempt to transform our results on platoon fuel efficiency into potential cost reduction gain. Our study shows that platooning fuel-efficiency may vary depending on the communication setup.

1 Introduction

Vehicle platooning means a group of vehicle driving closely after each other and being controlled as one unit. It allows many vehicles to accelerate or brake simultaneously, while decreasing the distances between vehicles using vehicle-to-vehicle (V2V) communication. Platooning vehicles saves space on highway so that the highway section can accommodate more vehicles. On the other hand, platoon followers experience reduced aerodynamic resistance due to small inter-vehicle distances, which results in fuel saving.

Fuel saving in vehicle platooning, especially for heavy-duty vehicles (HDVs), has been studied extensively by researchers and automotive manufacturers. Vehicle platooning introduces a split-stream effect for the follower vehicle and decreases corresponding air-drag, thus reduces overall restrictive forces. In fact, air-drag constitutes 23% of the total forces acting upon a vehicle at highway speed [1], even modest decrease can have noticeable impact on fuel saving. Previous studies showed that the fuel consumption of HDV platoon follower can achieve 20% saving [2] when the vehicle was operating in small intermediate distance. However, this requires robust controller and appropriate communication scheme to guarantee stability and safety [3]. For example, in the case of KONVOI project, it showed no saving during test on public highway since the platoon follower needed to vary its speed to maintain a desired distance to the preceding vehicle [4], which incurred additional fuel consumption.

V2V communications, stability and fuel efficiency in platoon are closely coupled. Proper communication setup can make a platoon follower maintain a desired distance to its predecessor while reducing acceleration and braking frequencies. To enable inter-vehicle communications European Telecommunication Standard Institute (ETSI) delivered the first ITS-G5 release of set of C-ITS standards under European Commission Mandate M/453 [5]. ITS-G5 defines the overall vehicular communication protocol stack [6]. So far there has been no dedicated message type standardized for platooning. However, there is currently pre-standardization activity (ETSI TR 103 301) studying how to apply currently available standards for platooning application [7]. In conformity with aforementioned in this study we implement and apply recently standardized Cooperative Awareness Messages [8] to enable platooning operation. Also according to [9]: "Decentralized congestion control (DCC) is a mandatory component of ITS-G5 stations operating in ITS-G5A and ITS-G5B frequency bands to maintain network stability, throughput efficiency and fair resource allocation to ITS-G5 stations".

To the best of our knowledge there are no studies available, that test platoon fuel efficiency under the detailed implementation of the ETSI ITS-G5 communication protocol stack. We compare the potential fuel consumption reduction, when platooning is enabled by two different DCC setups available in ITS-G5. The contribution of the paper is twofold:

- performance of the platoon enabled by the V2V communications in accordance with a complete ETSI ITS-G5 protocol stack is studied;
- case study of fuel savings for ITS-G5 enabled HDV platooning on E4 highway is provided.

Throughout this study we show that proper communication setup can further increase the fuel efficiency of the platooning system.

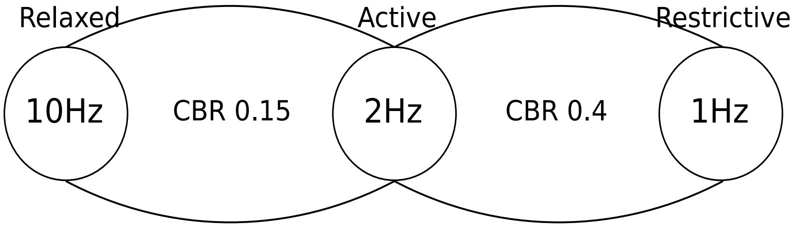
The manuscript is organized as follows. In Section 2 the description of CAM and DCC is summarized. Section 3 presents the reference platooning fuel consumption models, while Section 4 gives specification of the tested reference scenarios. Performance evaluation results are provided in Section 5. Finally, Section 6 concludes the paper.

2 ITS-G5 communications

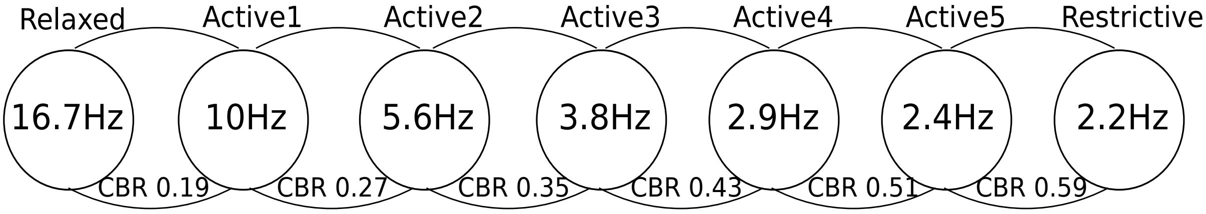
The coordination between vehicles in the platoon relies on the frequent exchange of broadcast communication messages containing information about vehicle's position, speed, acceleration and other attributes. The process of broadcast messages' exchange is usually referred to as beaconing [10]. To support beaconing in the platoon, following [7], we implemented Cooperative Awareness Messages (CAM), which are part of ETSI ITS-G5 stack [8]. For the sake of simplicity we skip the description of CAM, interested reader may to refer to [11] for detailed explanation.

In order to comply with ITS-G5 requirements we also implemented DCC functionality. DCC operates as gate-keeper at the medium access layer (MAC). The operation of DCC relies on the DCC state-machine 1. In each of the states DCC specifies the restrictions on the vehicle's transmission behavior. In particular, DCC defines 5 mechanisms to control the access to the communication channel: "Transmit Power Control" (TPC), "Transmit Rate Control" (TRC), "Transmit Datarate Control" (TDC), "DCC Sensitivity Control" (DSC), "Transmit Access Control" (TAC). In this study we are focusing on the TRC.

TRC defines for each DCC state the minimum allowed time between two consecutive message transmission. In Fig. 1 this time is represented in generation frequency of the messages, i.e. 10 Hz means, that vehicle can not generate more than 10 messages per second or in other words, time between two consecutive transmissions is not allowed to be less than 1/10 = 0.1 s. The transitions between DCC states are performed based on the Channel Busy Ratio (CBR), measured by each vehicles. The detailed DCC operation explanation could be found in [9, 12, 13].



Communication setup 1: ETSI TS 102 687 Configuration



Communication setup 2: ETSI TR 101 612 Configuration

Figure 1: DCC configurations.

To study the influence of the communication setup on the platooning fuel efficiency we implement two different DCC configurations:

- Basic 3-state DCC state-machine, Fig. 1.a, described in [9]. Throughout this paper we will refer to this configuration as Communication Setup 1.
- DCC state-machine configuration with set of sub-states in "Active state", Fig. 1.b, described in [13]. Throughout this paper we will refer to this configuration as Communication Setup 2.

To enable the beaconing in the platoon each vehicle follows the approach below:

- Generates CAM message according to [8];
- The DCC controls the access to the communication channel, according to [9, 13];

- Transmits message on the dedicated ITS-G5 channel according to IEEE 802.11p.

Signal attenuation is modeled using Log-distance path loss model. We also set the sampling rate CAM parameter the value in a way that effect described in [11] is not observed. Other communication parameters are summarized in the Table 1.

Table 1: Simulation Parameters

Parameter	Value
Communication parameters	
CAM size	2000 $bytes$
T_x power	23 dBm
Bitrate	6 $Mbit/s$
Path-loss exponent	2
Common parameters	
Size of the platoon (N)	15 vehicles
Number of disturbing vehicles	4 vehicles
Inter-vehicle gap	5 m
Scenario 1	
Platoon's leader speed	100 km/h
Vehicle acceleration capability	2.5 m/s^2
Vehicle deceleration capability	6 m/s^2
Vehicle length	4 m
Number of simulation runs	10
Scenario 2	
Platoon's leader speed	90 km/h
Vehicle acceleration capability	0.4 m/s^2
Vehicle deceleration capability	6 m/s^2
Vehicle length	15 m
Number of simulation runs	10

3 Fuel consumption in platooning

In order to better understand how communication setup affects the performance of platoon followers, a simplified fuel consumption model is applied to estimate instantaneous fuel usage [14]:

$$f = \frac{\int_{t_0}^{t_f} \delta \left[(\mu \cos\theta + \sin\theta) M g v + \kappa v^3 + M a v \right] \mathrm{d}t}{H\eta} \tag{1}$$

where t_0 and t_f are the initial and final time instances; H and η are energy density and efficiency respectively; v and a are vehicle speed and acceleration; M is the mass of vehicle; δ indicates if the engine is active:

$$\delta(t) = \begin{cases} 1 & \text{if } (\mu \cos\theta + \sin\theta) M g v + \kappa v^3 + M a v > 0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

the air-drag coefficient κ is computed from:

$$\kappa = \frac{1}{2} \rho_a A_a c_D (1 - \phi) \tag{3}$$

The air-drag reduction ϕ is illustrated in Fig. 2 or Fig. 3, depending on inter-vehicle distance, vehicle type and vehicle position in platoon. The n^{th} ($n \geq 4$) vehicle in car platoon has the same air-drag reduction as 4th vehicle, and the n^{th} ($n \geq 3$) vehicle in HDV platoon has the same air-drag reduction as 3rd vehicle. The detail of parameters for fuel consumption model is presented in Table 2.

4 Simulation setup

4.1 Reference scenarios

In this paper we consider two following reference scenarios:

1. Platooning consisting of N passenger cars moving along the road.
2. Platooning consisting of N Heavy Duty Vehicles (HDVs) moving along the road.

For both scenarios we exploit "disturbance scenario" as speed pattern [7, 17]. Moving along the highway platoon repeatedly meets slower vehicles in front of it and performs appropriate acceleration/deceleration maneuver, see Fig. 4. A low speed vehicle is generated on the test highway as disturbance, and this disturbance generation will be repeated 4 times per each simulation run. The scenario is equivalent to the road situation when slower vehicle comes to the right-most lane from metering ramp or after the lane changing.

Table 2: Parameters of Fuel Consumption Models [14].

Vehicle Parameters	Description	Value	Unit
M_{HDV}	Vehicle Mass of HDV	40000	kg
M_{car}	Vehicle Mass of Car	3000	kg
c_D	Air-Drag Coefficient	0.6	—
$A_{a-\mathrm{HDV}}$	Front Area of HDV	10.26	m^2
$A_{a-\mathrm{car}}$	Front Area of car	2.1	m^2
μ_{HDV}	Rolling Resistant Coefficient for HDV	7×10^{-3}	—
μ_{car}	Rolling Resistant Coefficient for car	0.02	—
ρ_a	Air Density	1.29	kg/m^3
g	Standard Gravity	9.8	—
H	Energy Density	36	MJ/L
η	Energy Efficiency	0.4	—

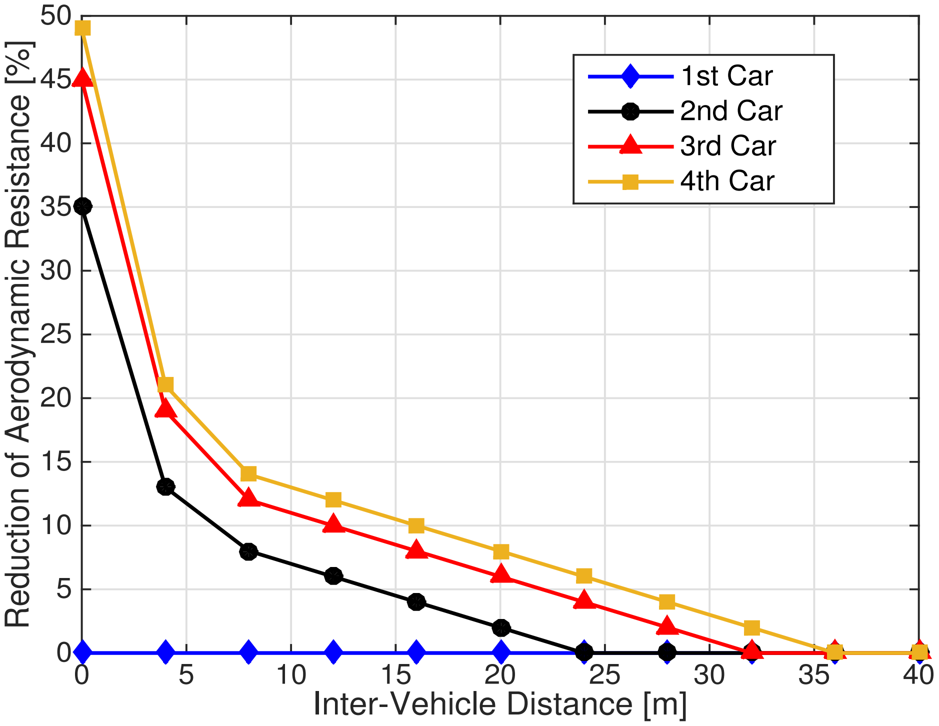


Figure 2: Air-Drag Reduction of Passenger Cars [15]

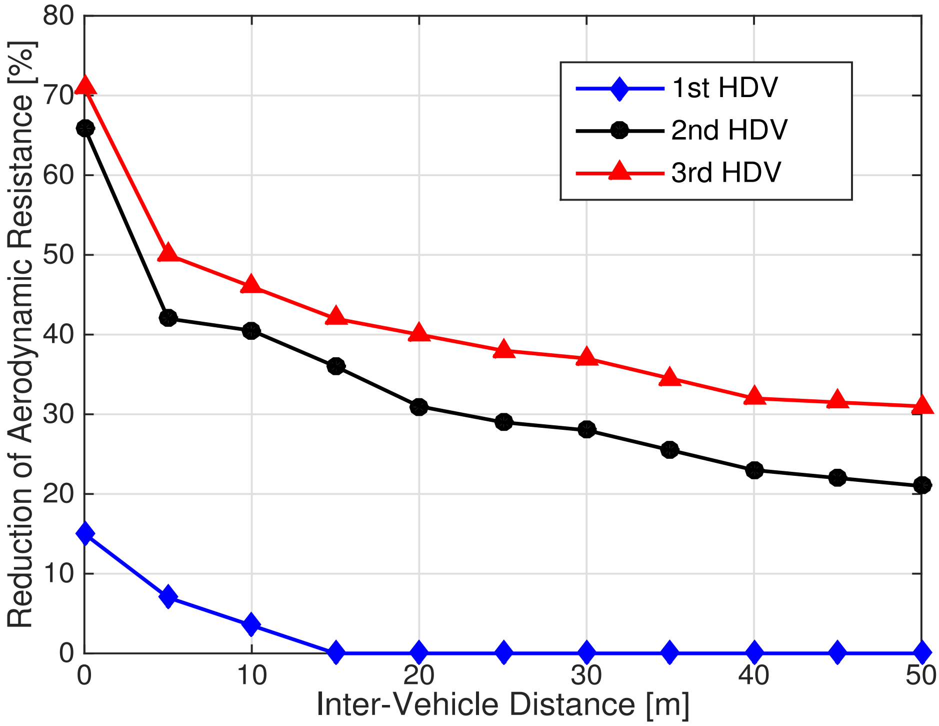


Figure 3: Air-Drag Reduction of HDVs [16]

4.2 Simulation platform

To emulate realistically the operation of the platoon we use novel Plexe simulation platform [18]. Plexe incorporates Omnet++ for the real-time V2V communications simulation together with SUMO as a realistic traffic simulator. Simulator also contains platoon controller part, which allows to control platoon members based on the input obtained from the communication exchange.

To comply with the ITS-G5 protocol stack [6] we additionally implemented ETSI CAM messages on facilities layer [8] and ETSI DCC functionality [12, 9]. The detailed description of the communication setup is given in Section 2. Each vehicle in the platoon utilizes as a control input messages containing kinematic data received from the preceding vehicle and platoon leader, following controller algorithm presented in [19]. Controller implements fixed-spacing policy, which means that inter-vehicle gap between the platoon members is fixed and does not depend on the vehicle's speed.

The detailed simulation parameters are summarized in Table 1.

5 Performance evaluation

In this section, the performance of different communication setups is evaluated in terms of fuel economy, which is the relationship between the amount of fuel consumed and the

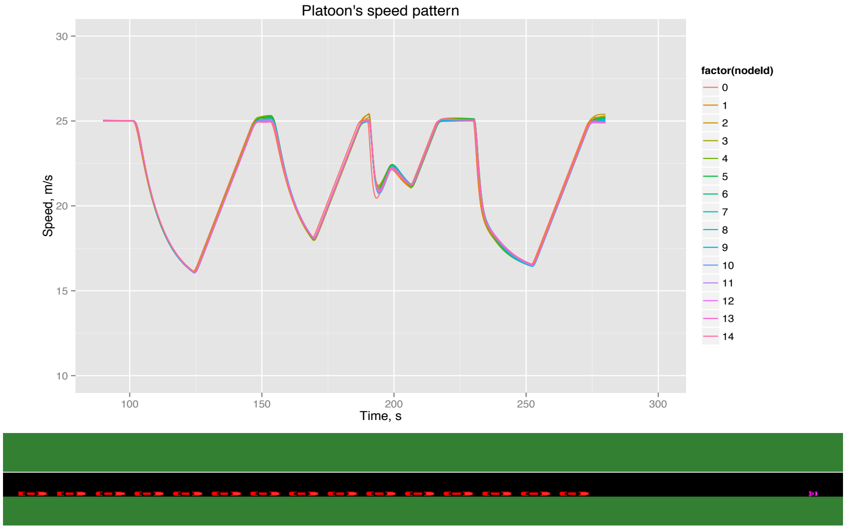


Figure 4: Reference scenario.

distances traveled by the vehicle. Fuel economy of an automobile is generally expressed as liters per 100 kilometers (L/100km) and used in most European countries. In order to estimate the fuel economy of each vehicle in platoon, experiments are conducted in microscopic simulation environment.

5.1 Fuel Economy of Platoon in Each Communication Setup

Fig. 5 corresponds to the fuel economy of the 15-car platoon. Evidently the platoon leader in two different communication setups has identical fuel economy, due to the same settings and reaction to disturbances. It can be seen that there is only minor difference between the no platooning and platooning cases (for passenger car) in fuel economy, about 0.2–0.44L/100km. And the difference between two platoon communication setup is almost negligible, only 0.01–0.07L/100km. This to some extent indicates that passenger cars usually do not have fuel saving incentive to form platoons, and platooning of cars might probably happen for driving comfort in traffic congestion.

Fig. 6 corresponds to the fuel economy of 15-HDV platoon. In the HDV platooning cases, all platoon members, including leader and followers can achieve fuel saving compared with the no platooning case. Communication Setup 1 results in 2.1%– 6.4% improvement in fuel economy, and Communication Setup 2 further enhances the improvement to 2.1%– 6.8%, indicating that platoon communication setup also plays an important role in fuel consumption. An appropriate communication setup will be able to further improve fuel economy and reduce fuel cost.

The enhanced fuel efficiency in Communication Setup 2 is a result of platoon's ability to maintain required inter-vehicle gap with higher precision under this scenario comparing to Setup 1, see Fig. 7. This could be explained by the fact that DCC setup with a larger number of "Active" sub-states allows better granularity in controlling CBR while still

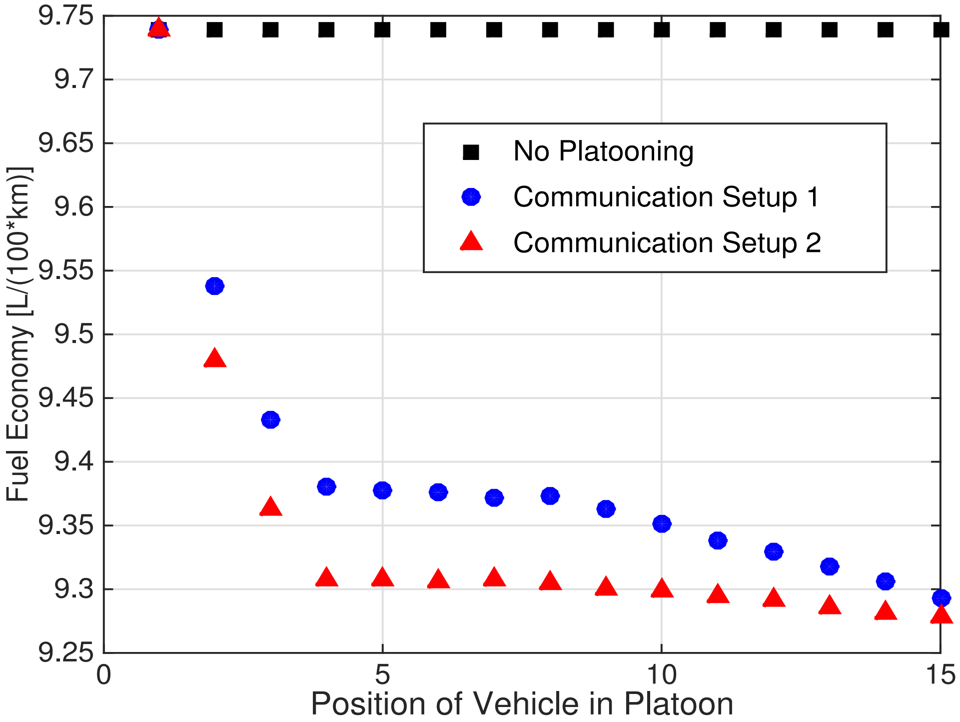


Figure 5: Fuel efficiency. Passenger vehicles

keeping congestion level at required low level. Hereby, even though both Communication Setups are defined in ETSI standards and allowed to exploit they may demonstrate sufficiently different performance in the platooning scenario and influence noticeably on the performance of application in terms of stability and fuel efficiency.

5.2 Numerical Experiment on European route E4

The European route E4 is the highway backbone of Sweden and used by most of freight transport. It starts from the border between Sweden and Finland, and passes through 22 cities of Sweden with a total length of 1590km. An overview of E4 can be seen in Fig. 9.

In this subsection, two communication setups are applied on a 15-HDV platoon which starts from Tornio and travels to Helsingborg. It is assumed that there are two on-ramps and off-ramps from/to each of the 22 cities, the speed limit for on-/off-ramp is 60km/h [20]. Since HDV is restricted to drive on the truck lane at the rightmost, the platoon has to decelerate to 60km/h in the ramp area and accelerate to desired speed 90km/h afterwards. Fuel economy can be estimated from the ratio of total fuel consumption to length of E4.

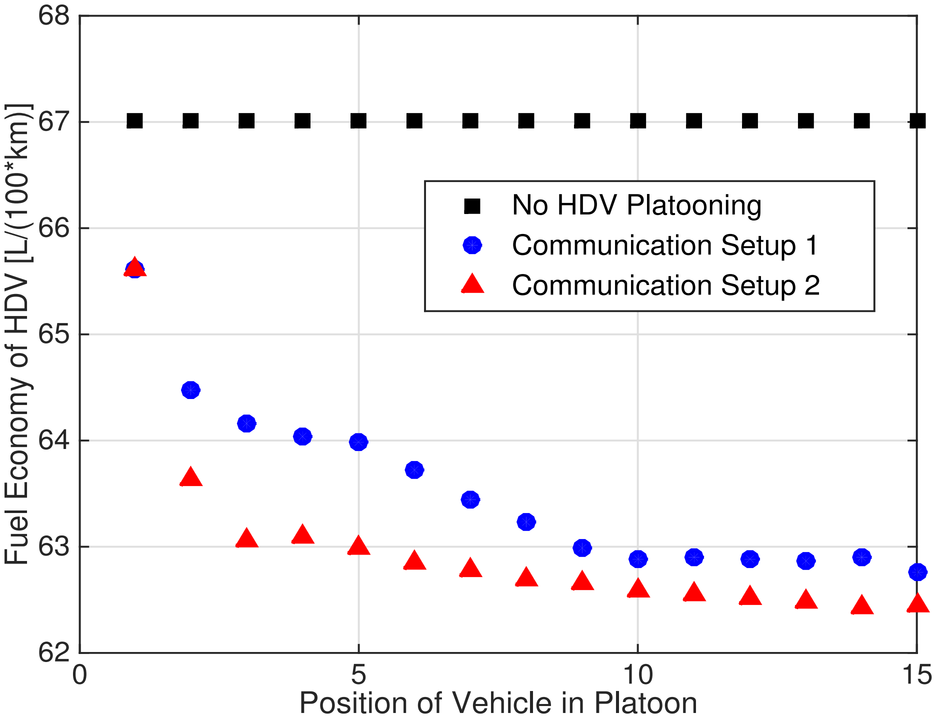


Figure 6: Fuel efficiency. HDV

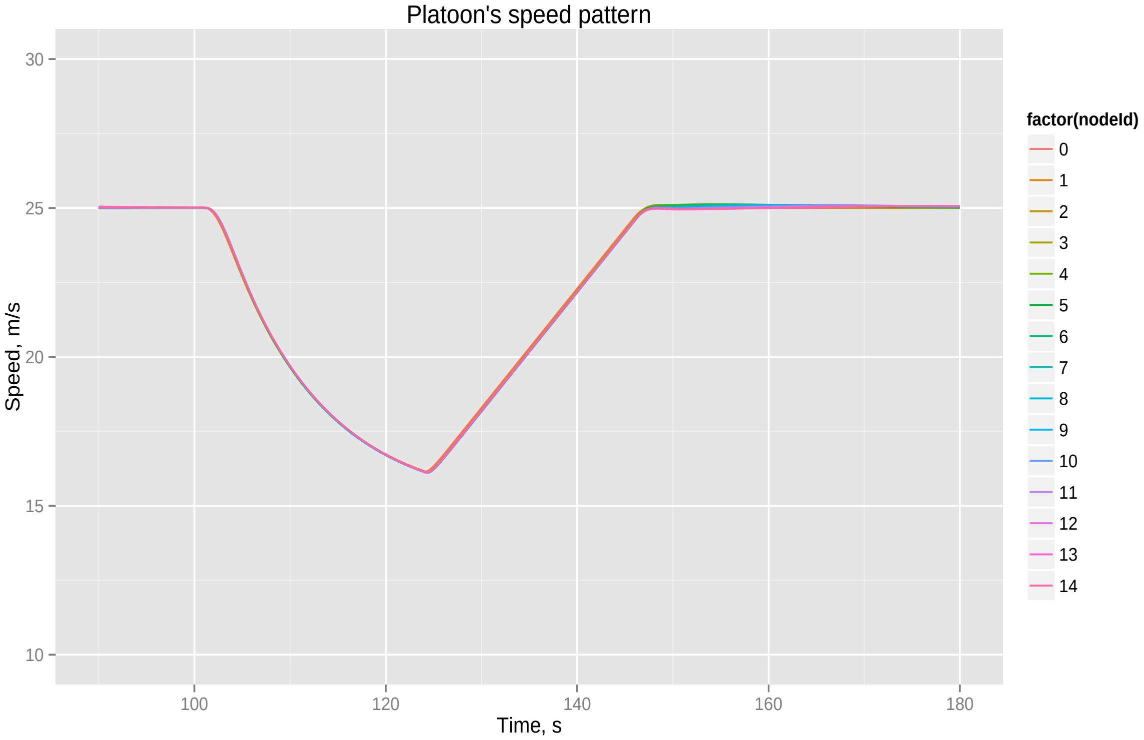


Figure 8: Speed Profile of HDV Platoon at Ramp Area in Communication Setup 2

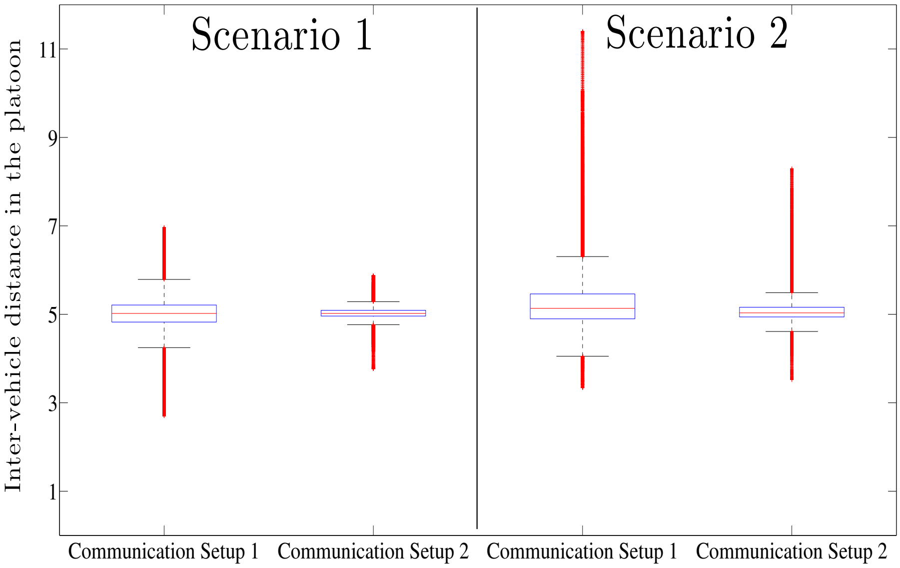


Figure 7: Platoon Inter-vehicle distance

Table 3: Estimated Overall Fuel Economy and Yearly Total Cost of 15-HDV Platoon

Communication Setup	No HDV Platooning	Communi. Setup 1	Communi. Setup 2
Fuel Economy (L/100km)	36.79	30.54	30.31
Yearly Total Cost (MSEK)	15.89	13.11	13.09

HDV platooning improves fuel economy, which can be seen in Table 3. HDVs consume significantly less fuel when operating in platoon for the same travel distance. The platoon saves 6.44L, or equivalently 17.5% in Communication Setup 1 and 6.48L (17.6%) in Communication Setup 2 respectively for every 100km. In general, an HDV travels over 200,000km per year [21], with average diesel cost 14.4SEK/L. Both HDV platooning in Communication Setup 1 and Communication Setup 2 lead to remarkable amount of saving compared with the no HDV platooning scenario. Table 3 shows that HDV platooning in Communication Setup 1 and Communication Setup 2 can potentially save 2.78MSEK and 2.8MSEK respectively. According to simulation outcomes presented in Fig. 10, 3rd–15th HDV contribute the most significant saving, which is inline with the dramatic air-drag reduction for HDV platoon followers. It is also worth mentioning that HDV platooning in Communication Setup 2 has slightly more saving than Communication Setup

1, which can be explained by the fact that Communication Setup 2 results in smaller fluctuation in the speeds of HDV platoon follower (See Fig. 11 and Fig. 8) and more stable inter-vehicle distances (See Scenario 2 in Fig. 7), therefore reduce acceleration and braking efforts and frequencies.

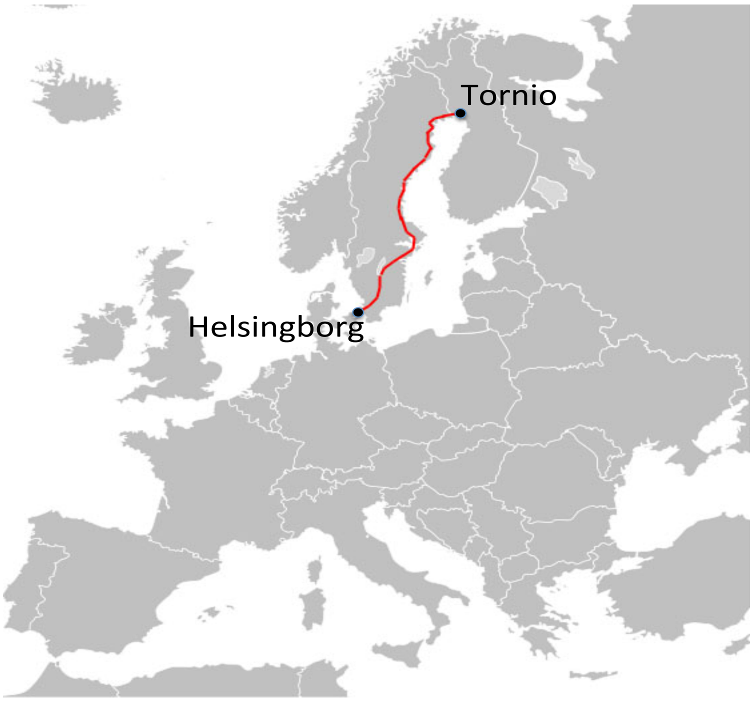


Figure 9: European Route E4

Note that the numerical experiment is presented for illustrative purpose only. In fact, the results from numerical experiment largely depend on the number of disturbances occurred in front of the platoon leader during operation. More disturbance could result in more significant difference in speed profiles, acceleration behaviors, inter-vehicle distances and fuel efficiency of platoon among scenarios. In this manuscript we show, that parameters of communication setup have direct impact on the platoon's air-drag reduction under disturbance scenario, regardless of the frequency they appear.

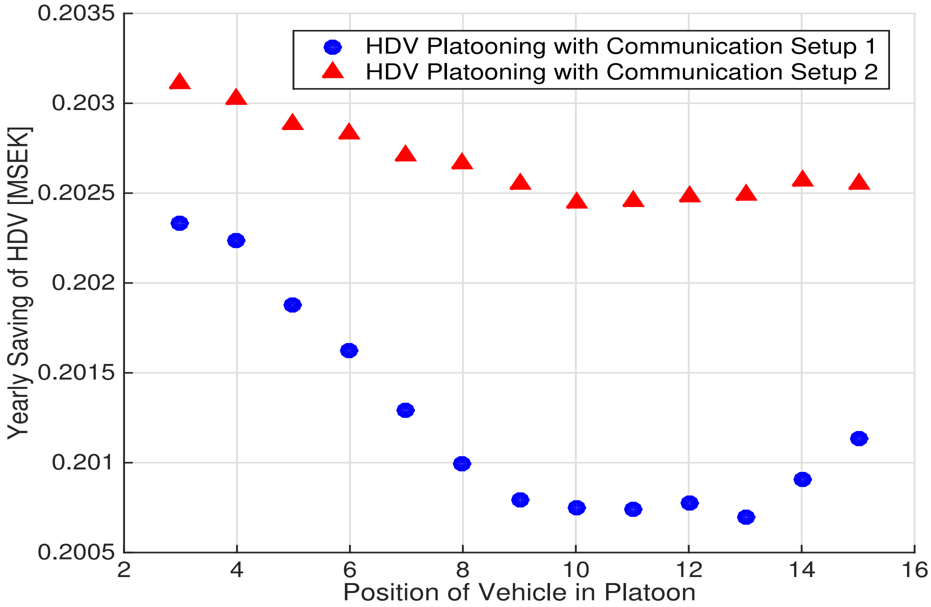


Figure 10: Estimated Yearly Saving of HDV Compared with No HDV Platooning Scenario

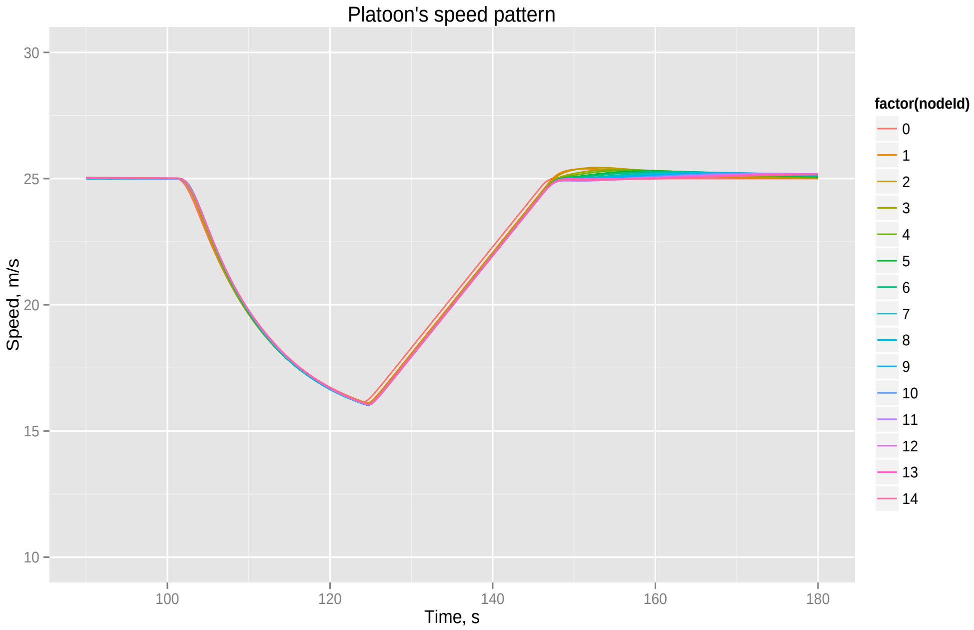


Figure 11: Speed Profile of HDV Platoon at Ramp Area in Communication Setup 1

6 Conclusion

In this manuscript we make a first attempt to assess platooning fuel efficiency performance under realistic ITS-G5 communication setups. Two types of platoons consisting of passenger cars and HDVs have been tested. Our simulation study shows that fuel savings for HDV platooning scenario are much more significant. Moreover the parameters of communication setup may influence notably on platooning fuel efficiency as it influences directly the performance of the vehicle's control system.

Our ongoing work is focusing on the testing the platoon under both realistic communication setups and road traffic patterns. We are also aiming to test the influence of different platooning control algorithms on the potential fuel efficiency performance of application.

Acknowledgment

This study is a part of the "ACDC: Autonomous Cooperative Driving: Communications Issues" project (2014-2016) funded by the Knowledge Foundation, Sweden in cooperation with Volvo GTT, Volvo Cars, Scania, Kapsch TrafficCom and Qamcom Research & Technology. It is also supported by the National ITS Postgraduate School (NFITS), Sweden.

References

[1] T. Sandberg, *Heavy Truck Modeling for Fuel Consumption Simulations and Measurements.* Linköping University, 2001, Licentiate Thesis.

[2] T. Robinson, E. Chan, and E. Coelingh, "Operating Platoons On Public Motorways: An Introduction To The SARTRE Platooning Programme," in *the 17th ITS World Congress*, 2010.

[3] A. Alam, "Fuel-efficient heavy-duty vehicle platooning," 2014.

[4] S. Shladover, "Recent International Activity in Cooperative Vehicle - Highway Automation Systems," Tech. Rep. FHWA-HRT-12-033, 2012.

[5] "Directive 2010/40/eu of the european parliament and of the council on the framework for the deployment of intelligent transport systems in the field of road transport and for interfaces with other modes of transport," *Official Journal of the European Union*, 2010.

[6] "Intelligent transport systems (ITS); access layer specification for intelligent transport systems operating in the 5 ghz frequency band." *ETSI TS 102 687 V1.1.1*, 2013.

[7] A. Vinel, L. Lan, and N. Lyamin, “Vehicle-to-Vehicle communication in C-ACC/Platooning scenarios,” *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[8] “Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service,” *ETSI EN 302 637-2 V1.3.2*, 2014.

[9] “Intelligent transport systems (ITS); decentralized congestion control mechanisms for intelligent transport systems operating in the 5 GHz range; access layer part,” *ETSI TS 102 687 V1.1.1*, 2011.

[10] C. Campolo and A. Molinaro, “Multichannel communications in vehicular ad hoc networks: a survey,” *Communications Magazine, IEEE*, vol. 51, no. 5, pp. 158–169, 2013.

[11] N. Lyamin, A. Vinel, and M. Jonsson, “Does ETSI beaconing frequency control provide cooperative awareness?” in *2015 IEEE International Conference on Communication Workshop (ICCW)*, June 2015, pp. 2393–2398.

[12] “Intelligent transport systems (ITS); cross layer DCC management entity for operation in the ITS G5A and ITS G5B medium.” *ETSI TS 103 175 V1.1.1*, 2015.

[13] “Intelligent transport systems (ITS); cross layer dcc management entity for operation in the ITS G5A and ITS G5B medium; report on cross layer dcc algorithms and performance evaluation,” *ETSI TS 101 612 V1.1.1*, 2014.

[14] Q. Deng, “A General Simulation Framework for Modeling and Analysis of Heavy-Duty Vehicle Platooning,” *IEEE Transactions on Intelligent Transportation Systems*, 2016, accepted for publication.

[15] M. Zabat, N. Stabile, S. Farascaroli, and F. Browand, “The aerodynamic performance of platoons: A final report,” Tech. Rep. UCB-ITS-PRR-95-35, 1995.

[16] H. Wolf-Heinrich and S. Ahmed, “Aerodynamics of road vehicles,” *Society of Automotive Engineers*, 1998.

[17] D. Jia, K. Lu, and J. Wang, “A disturbance-adaptive design for vanet-enabled vehicle platoon,” *Vehicular Technology, IEEE Transactions on*, vol. 63, no. 2, pp. 527–539, 2014.

[18] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. Lo Cigno, “PLEXE: A Platooning Extension for Veins,” in *6th IEEE Vehicular Networking Conference (VNC 2014)*. Paderborn, Germany: IEEE, December 2014, pp. 53–60.

[19] X. Liu, A. Goldsmith, S. S. Mahal, and J. K. Hedrick, “Effects of communication delay on string stability in vehicle platoons,” in *Intelligent Transportation Systems, 2001. Proceedings. 2001 IEEE*. IEEE, 2001, pp. 625–630.

[20] Møde for Forbedret Vejudstyr (NMF), http://nmfv.dk/wp-content/uploads/2014/04/Entry-ramp-designs-in-tunnels-Sweden.pdf.

[21] K.-Y. Liang, *Coordination and Routing for Fuel-Efficient Heavy-Duty Vehicle Platoon Formation.* KTH Royal Institute of Technology, 2014, Licentiate Thesis.

Paper 3

Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks

Authors:
Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Jonathan Loo

Reformatted version of paper originally published in:
IEEE Communications Letters.

Real-time detection of Denial-of-Service attacks in IEEE 802.11p vehicular networks

Nikita Lyamin, Alexey Vinel, Magnus Jonsson and Jonathan Loo

Abstract

A method for real-time detection of Denial-of-Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs) is proposed. The study is focused on the "jamming" of periodic position messages (beacons) exchanged by vehicles in a platoon. Probabilities of attack detection and false alarm are estimated for two different attacker models.

1 Introduction

IEEE 802.11p is an international standard[1] for short-range inter-vehicle communication in the 5.9 GHz frequency band. Vehicular ad-hoc networks (VANETs) comprised of the IEEE 802.11p-enabled vehicles aim at increasing road safety, efficiency and driving comfort and are currently a subject of an intensive research [2]. Platooning is an example of such an application based on vehicle-to-vehicle communication.

In a *platoon* the leading vehicle (normally a truck) is driven by the human, while the following vehicles either automatically maintain the velocity of the leading one, but their direction is still controlled by the driver (e.g. Connect & Drive project [3] and Grand Cooperative Driving Challenge – GCDC [4]), or follow the leading one in a fully automatic manner (e.g. Safe Road Trains for the Environment project – SARTRE [5]).

The cooperation between the vehicles in the platoon is achieved by the frequent exchange of periodic broadcast messages carrying information on vehicle position and velocity, which we refer to as *beacons*[2], in the dedicated channel [8].

Since the IEEE 802.11p medium access control (MAC) protocol specifies random access, during its normal operation the beacons can be lost either due to the wireless channel impairments or due to collisions (i.e. overlapping transmissions of beacons from several vehicles). The probability of collisions can be reduced by the proper choice of the MAC protocol parameters [9]. However, the beacons can also be intentionally corrupted by the malicious node in case of a *jamming* Denial of Service (DoS) attack [10], [11]. In the latter case the safety of the platoon can be jeopardized especially seriously since the vehicles will not be able to update the information about each other within the

---

[1] Currently IEEE 802.11p has been incorporated in the latest version of IEEE 802.11 [1] and, therefore, the former one is superseded. However, following the common approach adopted in the literature, throughout this paper we refer to the "vehicular" part of IEEE 802.11 as IEEE 802.11p.

[2] Beacons are called Cooperative Awareness Messages (CAMs) in European standardization framework [6] and Basic Safety Messages (BSMs) in Unites States [7].

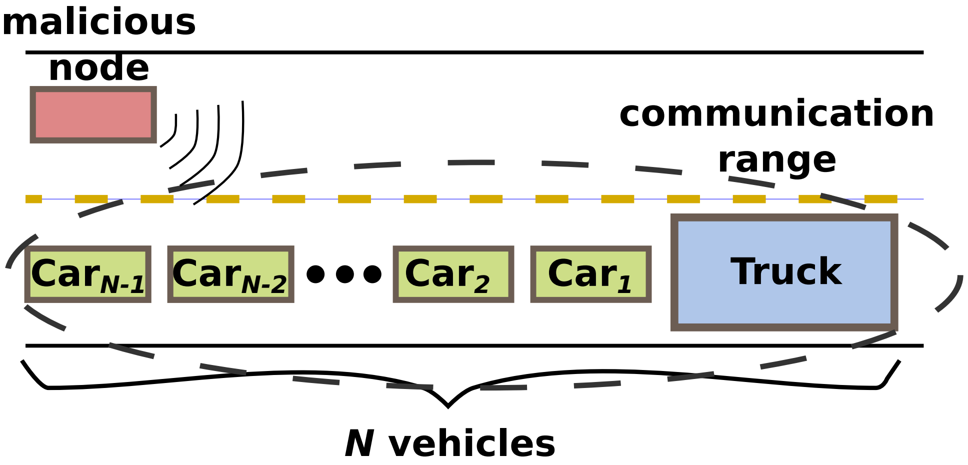


Figure 1: Platooning scenario

delay requirements imposed by the automotive control systems. Therefore, the real-time detection of jammers in IEEE 802.11p VANETs is an important practical problem, which motivates our study.

Real-time detection of DoS attacks in IEEE 802.11 networks have been studied in [12], where the proposed detector observes the events happening in the wireless channel and probabilistically computes how "explainable" occurring of each particular collision is. The method in [12] targets the basic mode of IEEE 802.11 with an arbitrary unicast traffic, which is retransmitted according to the binary exponential backoff algorithm. The method to detect the jammers in VANETs with unicast traffic, which is based on linear regression, is proposed in [13]. However, very limited performance evaluation results are reported in [13], e.g. no results on the detection time are given.

In comparison to the above studies, we consider the beacons, which are transmitted regularly in IEEE 802.11p broadcast mode without retransmissions, making it possible to propose an alternative jamming detector. To the best of our knowledge no literature has considered the problem of jamming DoS attacks detection in VANET platoons so far.

The contribution of this paper is twofold:

- a simple real-time detector of jamming DoS attacks in VANET platoons is proposed;
- the detector is validated in terms of detection and false alarm probabilities within the limited time for two types of jamming attacks.

We emphasize that in this paper we do *not* consider MAC layer *misbehavior*, when some nodes violate IEEE 802.11 rules and choose a small backoff counter to get the channel access more frequently than other nodes, and therefore, degrade their performance. The real-time detection of such cases has been studied recently, e.g. in [14] and [15].

The manuscript is organized as follows. In Section II we describe the system model. Section III presents the proposed DoS detection method. Performance evaluation results are provided in Section IV. Finally, Section V concludes the paper.

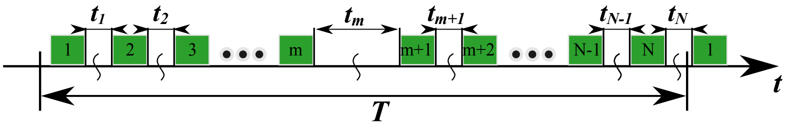


Figure 2: Time diagram of the transmissions before the division into independent detection periods

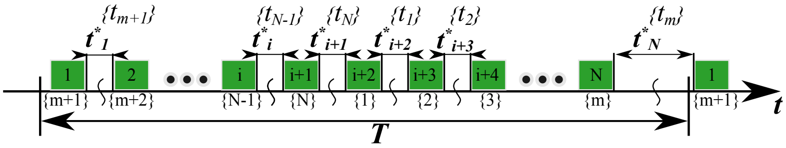


Figure 3: Time diagram of the transmissions after the division into independent detection periods

2 System Model

The following assumptions on the system operation are adopted in our study:

1) The *platoon* is comprised of N vehicles, which are all in each others communication range. We assume a practically feasible case with the following reference values of the parameters: IEEE 802.11p communication range – 400-500 meters, inter-vehicle distances in the platoon – 5 meters, truck length – 15 meters, this assumption holds for platoons with $N \leq 25$. The current value of N is known to the vehicles since joining and leaving of the platoon involves some negotiation protocol [5].

2) The time between the generation of two subsequent beacons, which is chosen by a vehicle, is *fixed* and denoted as T and referred to as beaconing period. According to [6] the possible range for T is 0.1–1 second and varies accordingly to the current rapidity of its kinematic information change. Therefore, the assumption roughly holds for the platoon keeping constant velocity on a highway.

3) Each generated beacon is broadcasted into the channel according to the IEEE 802.11p MAC rules. The random backoff counter value is chosen uniformly from the interval $[0, W-1]$, where W is the minimal Contention Window (CW). The counter is decremented by one after each slot of length σ when no activity is sensed in the channel. In case transmission is detected, the vehicle has to ensure that the channel becomes idle for the Arbitrary InterFrame Space (AIFS) before further decreasing the backoff counter[3]. The transmission is performed, when the counter turns to zero[4]. The beacons are neither acknowledged by the recipients nor retransmitted. The beacon transmission time is $\tau = T_h + L/R$, where T_h is the header transmission time, L is the beacon payload size and R is the channel rate.

4) The communication channel is assumed to be *error-prone* with independent losses

---

[3] If the jammer receives the preamble of a packet and starts to corrupt only its payload, then Extended InterFrame Space (EIFS) should be used instead of AIFS [16]. In this paper we assume that the packet is completely destroyed by the attacker.

[4] In the IEEE 802.11p if the channel was sensed as idle for the AIFS time prior to the packet generation it is allowed to transmit it immediately without entering the backoff process. Throughout of this paper we ignore this option to avoid persistent collisions at each beaconing period in case two (or more) beacons are generated at a nearby time instances.

of beacons and fixed packet error rate (PER). As it follows from the practical measurements reported in [17], when the platoon length does not exceed 400 meters, PER is lower than 1%, given the line-of-sight condition between the antennas of vehicles holds (this can be achieved by placing them, e.g. at the outdoor rear-view mirrors). Apart from the noise, collisions with beacons from any of the $N-1$ remaining vehicles are also possible.

Two attacker models are assumed [12]:

- *"Random jamming"*. Each packet transmitted in the channel is corrupted independently with probability p.
- *"ON-OFF jamming"*. In the OFF state no packets are jammed, while in the ON state K subsequent beacons are destroyed with probability one. Then the attacker switches to the OFF state. The OFF–ON transitions occur at the moments of beacon transmission start with probability p.

3 Simple Jamming Detection Method

3.1 Preliminaries

Let us assume that there is a node (detector), which continuously listens to the channel, where the exchange of beacons between the vehicles in the platoon occurs. Practically the detector can be envisioned as a *sniffer* mounted on the leading vehicle.

The operation of the proposed jamming detector comprises two phases: *installation* phase and *normal* operation.

3.2 Installation phase

The objective of the installation phase is to divide all the vehicles in the platoon into groups in a way that the beacons from different groups never collide with each other. For this reason the detector tries to obtain some estimates for the beacons generation moments of all the vehicles in the platoon. The actual transmissions may occur at a later moments due to the random backoff delays.

The detector listens to the channel until it has received the sequence of $N+1$ successfully transmitted beacons in a row[5]. The sequence of time intervals between these transmissions is denoted as $(t_1, t_2, \ldots, t_N)$, where t_i is the duration between the end of transmission of the i-th beacon and start of the transmission of the $(i+1)$-th one, see Fig. 2.

Proposition 1. Beacons from nodes i and $i+1$ never collide if both the following conditions hold:

$$\tau + AIFS > (W-1)\sigma, \tag{1}$$

$$t_i > AIFS + (W-1)\sigma. \tag{2}$$

---

[5] The mean time needed to receive such a sequence is studied later in the paper.

Proof: Let x be the moment of time when the transmission of node i has finished. From (1) it follows that independently of its backoff counter choice, node i could not start its transmission later than $x + AIFS$. Analogously from (2) it follows that node $i+1$ could not start its transmission earlier than $x + AIFS$. ■

In the following we assume that system parameters are chosen in a way that (1) is satisfied (see Section IV) and we adopt the notation $S = AIFS + (W-1)\sigma$.

Proposition 2. Let $t_m = \max_{1 \leq i \leq N} t_i$, then nodes m and $m+1$ never collide if $\frac{T}{N} > \tau + S$.

Proof: The minimal possible value of t_m is achieved when the transmissions of all the N vehicles are uniformly spread in time within the beaconing period T, i.e. the difference between their transmission times is T/N. Taking this into account, it is easy to see that inequality (2) for t_m holds. ■

Applying Proposition 2 the detector operation is divided into *independent detection periods* of duration T. We define that the first detection period begins $\sigma(W-1)$ prior to the transmission start of the m-th beacon, see Fig. 3.

Let $\bar{t} = (t_{m+1}, t_{m+2}, \ldots, t_N, t_1, t_2, \ldots, t_m)$. For easiness of notation let us renumber the components of this vector as $\bar{t} = (t_1^*, t_2^*, \ldots, t_N^*)$, where t_j^* is the duration between the end of transmission of the j-th beacon and start of the transmission of the $(j+1)$-th one.

Applying Proposition 1 it is possible to divide all the vehicles into groups in a way that beacons from different groups never collide. For this reason vector $\bar{t}$ should be analyzed:

- If for some vehicle j: $t_{j-1}^* > S$ and $t_j^* > S$, then the beacons of this vehicle never collide with other beacons.
- Analogously if there is a group of $K > 1$ vehicles $j_1, j_2, \ldots, j_K$ such as $t_k^* \leq S$ holds for for all $k : 1 \leq k \leq (K-1)$, but $t_{k-1}^* > S$ and $t_K^* > S$, then the beacons of these K vehicles can collide with each other, but not with the ones of the other $N-K$ vehicles.

Therefore, the outcome of the installation phase is the sets Ω_i of vehicle identifiers such as beacons from different sets never collide with each other, which is obtained by analyzing the transmission in the first detection period. By the end of the first detection period the detector switches to normal operation.

3.3 Normal operation of the detector

Normal operation is organized in detection periods of length T. The detector listens to the channel and records the identifiers of the vehicles for which beacons have been successfully received. The decision is made by the end of each detection period as follows:

- *"Alarm"*: if there is *at least one* group among Ω_i, where *exactly one* beacon has not been received.
- *"No alarm"*: otherwise.

The underlying idea of such an approach is simple: in case of a beacon loss there should exist at least two nodes involved in the collision within the same group.

4 Performance Evaluation

4.1 Preliminaries

We study an IEEE 802.11p system with N=25 vehicles and T=0.1 s with the following parameter values (see [16], best effort MAC access category): $AIFS$=110 μs, W=16, L=400 bytes, R=3 Mbit/s, σ=13 μs, T_h=52 μs.

It is easy to check that for the above parameters, the condition (1) holds. Simulations demonstrate that the installation phase time, i.e. the time from the moment when the detector is turned on until the end of the first detection period, does not exceed 150 ms for the error-free channel and 200 ms for PER =0.01, see Fig. 4.

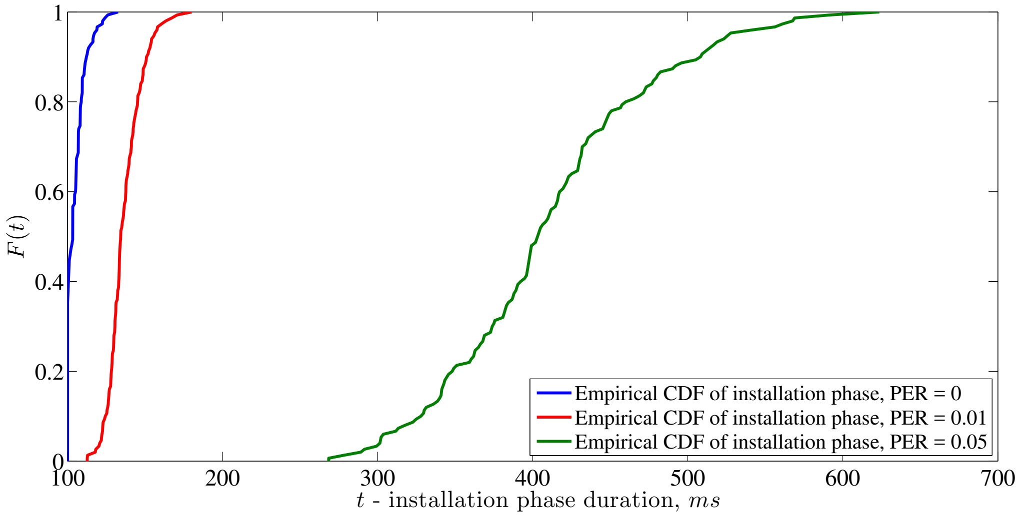


Figure 4: Cumulative distribution function (CDF) of installation phase time

Under the given set of assumptions and based on the rules of detector operation, the probability of false alarm, i.e. the probability that the alarm is triggered although no beacons have been jammed in the detection period, is zero for error-free channel and does not exceed 2% for $PER = 0.01$ $(0.1 \leq p \leq 0.5)$.

In the following subsections we study the probability of attack detection $P_{detection}$, i.e. the probability that the alarm is triggered, given that at least one successfully transmitted beacon is jammed in the detection period.

4.2 Random jamming case

For the random jamming case, the relation between the probability of attack detection and the jamming probability is depicted in Fig. 5. We average the detection probability for different initial mutual offsets of beacon generation moments. For any p value the averaged $P_{detection}$ exceeds 0.996 for error-free case and 0.993 for $PER = 0.01$. Taking into account that one detection period is $T = 0.1$ s, in most cases the attack is detected with probability close to one within a few hundred milliseconds.

The minimal value of $P_{detection}$ is observed when two beacons in average are jammed during the detection period, i.e. when $pN \approx 2$, since the probability that these two beacons belong to the same group and, therefore, the attack is not detected, is high.

The operation of the system for the error-free case can be analytically modeled using the following approximate approach.

Let us assume that the detection period is divided into M slots, such that $M = \frac{T}{\tau + AIFS + W\sigma}$. If i vehicles choose the same slot for the transmission (each with probability $1/M$), then they form one group. Due to time diversity provided by the backoff mechanism, transmissions of the group take i slots.

For such a model, the probability that a particular group of i beacons is formed ($2 \leq i \leq N$), can be computed recursively as:

$$P_i = \binom{N-(i-2)}{2} \frac{1}{M} P_{i-1} \left(1 - \frac{1}{M} P_{i-1}\right)^{N-i}, \tag{3}$$

where $P_1 = 1/M$.

Assuming for simplification that there are no collisions in the detection period and, therefore, potentially any beacon can be jammed, we calculate the probability that at least 2 beacons (out of the group with n) are corrupted by the jammer as:

$$Q(n,p) = \sum_{j=2}^{n} \binom{n}{j} p^j (1-p)^{N-j}. \tag{4}$$

Finally, taking into account the detector operation rules, which cannot detect the cases when more than one beacon is jammed in a group, we obtain:

$$P_{detection} \approx 1 - \sum_{n=2}^{N} P_n Q(n,p). \tag{5}$$

4.3 ON-OFF jamming case

For the ON-OFF jamming case ($K = 2$), the relation between the probability of attack detection and the jamming probability is depicted in Fig. 6.

In contrary to the random jamming, $P_{detection}$ in this case is an increasing function of the jamming probability. Small p values correspond to the case when exactly two subsequent (and therefore highly probable – belonging to one group), beacons are jammed, which is not detected. With the increase of p, more pairs of beacons are likely to be jammed, i.e. it is more probable, that a group of exactly one beacon is involved and, consequently, the attack is detected. Further increase of the K value also increases $P_{detection}$.

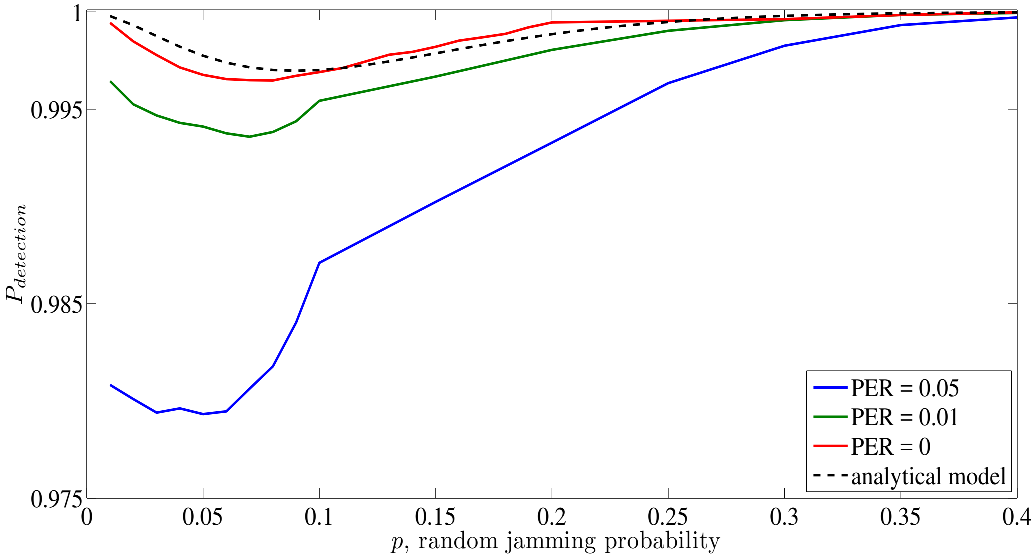


Figure 5: Attack detection probability for random jamming

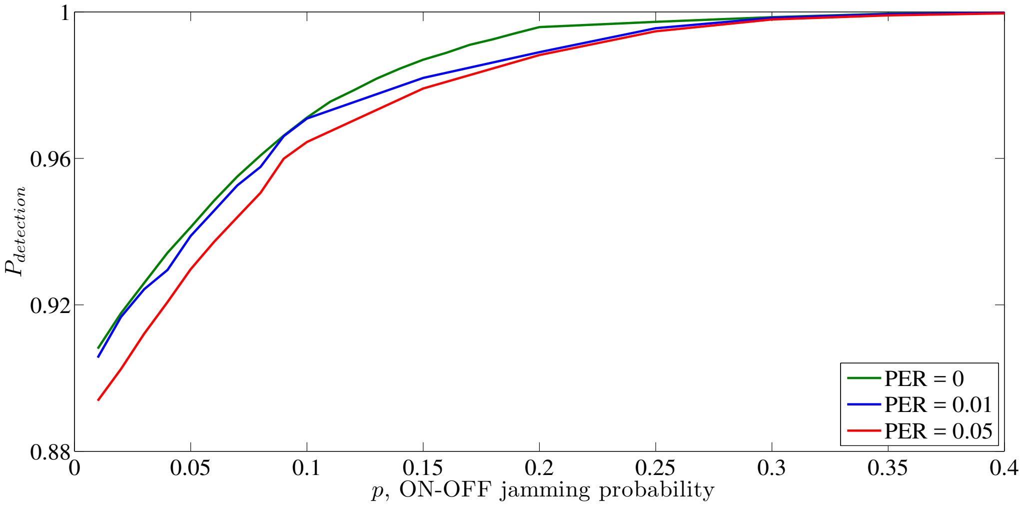


Figure 6: Attack detection probability for ON-OFF jamming ($K = 2$)

5 Conclusion and future work

We have proposed a simple algorithm for real-time detection of jamming attacks against beaconing in 802.11p vehicular networks. For the reference platooning scenario under the simplified assumptions our algorithm provides in average the probability of detection not lower than 0.9 and no false alarm for any jamming probability.

Our ongoing work is focused on relaxing the assumptions of the presented model (especially about the fixed beaconing period) and correspondingly enhancing the detector for realistic scenarios.

References

[1] "IEEE std. 802.11-2012, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std. 802.11-2012*, jun 2012.

[2] G. Karagiannis, O. Altintas, E. Ekici, G. Heijenk, B. Jarupan, K. Lin, and T. Weil, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 4, pp. 584–616, 2011.

[3] J. Ploeg, A. F. Serrarens, and G. J. Heijenk, "Connect & drive: design and evaluation of cooperative adaptive cruise control for congestion reduction," *Journal of Modern Transportation*, vol. 19, no. 3, pp. 207–213, 2011.

[4] K. Lidstrom, K. Sjoberg, U. Holmberg, J. Andersson, F. Bergh, M. Bjade, and S. Mak, "A modular cacc system integration and design," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 13, no. 3, pp. 1050–1061, 2012.

[5] E. Chan, "Overview of the sartre platooning project: technology leadership brief," SAE Technical Paper, Tech. Rep., 2012.

[6] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *ETSI EN 302 637-2 V1.3.2*, 2014.

[7] D. Committee, "Dedicated short range communications (dsrc) message set dictionary," *SAE Std. J2735*, 2009.

[8] C. Campolo and A. Molinaro, "Multichannel communications in vehicular ad hoc networks: a survey," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 158–169, May 2013.

[9] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, "Modeling prioritized broadcasting in multichannel vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, 2012.

[10] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 2, pp. 245–257, 2011.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing.* ACM, 2005, pp. 46–57.

[12] A. L. Toledo and X. Wang, "Robust detection of mac layer denial-of-service attacks in csma/ca wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 347–358, Sept 2008.

[13] A. Hamieh, J. Ben-Othman, and L. Mokdad, “Detection of radio interference attacks in vanet,” in *GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, Nov 2009, pp. 1–5.

[14] J. Tang, Y. Cheng, and W. Zhuang, “Real-time misbehavior detection in ieee 802.11-based wireless networks: An analytical approach,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 1, pp. 146–158, Jan 2014.

[15] S. Djahel, Z. Zhang, F. Nait-Abdesselam, and J. Murphy, “Fast and efficient countermeasure for mac layer misbehavior in manets,” *IEEE Wireless Communications Letters*, vol. 1, no. 5, pp. 540–543, October 2012.

[16] “IEEE std. 802.11-2012, part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications,” *IEEE Std. 802.11-2012*, 2012.

[17] A. Bohm, K. Lidstrom, M. Jonsson, and T. Larsson, “Evaluating calm m5-based vehicle-to-vehicle communication in various road settings through field trials,” in *IEEE Local Computer Network Conference*, Oct 2010, pp. 613–620.

Paper 4

AI-based malicious network traffic detection in VANETs

Authors:
Nikita Lyamin, Denis Kleyko, Quentin Delooz, Alexey Vinel

Reformatted version of paper accepted for publication in:
IEEE Networks.

AI-based malicious network traffic detection in VANETs

Nikita Lyamin, Denis Kleyko, Quentin Delooz, Alexey Vinel

Abstract

Inherent unreliability of wireless communications may have crucial consequences when safety-critical Cooperative Intelligent Transportation Systems (C-ITS) applications enabled by Vehicular Ad-Hoc Network (VANETs) are concerned. Although, natural sources of packet losses in VANETs such as network traffic congestion are handled by a Decentralized Congestion Control (DCC), losses caused by malicious interference need to be controlled too. For example, jamming Denial-of-Service (DoS) attacks on Cooperative Awareness Messages (CAMs) may endanger vehicular safety and first and foremost are to be detected in a real-time. Our first goal is to discuss key literature on jamming modeling in Vehicular Ad-Hoc Networks (VANETs) and revisit some of existing detection methods. Our second goal is to present and evaluate our own recent results on how to address real-time jamming detection problem in Vehicle-to-Everything (V2X) safety-critical scenarios with the use of Artificial Intelligence (AI). We conclude that our hybrid jamming detector, which combines statistical network traffic analysis with data mining methods, allows achieving acceptable performance even when random jitter accompanies the generation of CAMs what complicates the analysis of the reasons for their losses in VANETs. The use case of the study is a challenging platooning C-ITS application, where V2X-enabled vehicles move together at highway-speeds with short inter-vehicle gaps.

1 Introduction

Cooperative Intelligent Transportation Systems (C-ITS) integrate telecommunications, electronics and information technologies with transport engineering aiming at increased road safety, efficiency and driving comfort [1]. Dependable and secure Vehicle-to-Everything (V2X) communications to exchange status updates among road users is an important component of the C-ITS. The concept of Vehicular Ad hoc Networks (VANETs) assumes that vehicles, which encounter each other on roads, are able "to talk" in machine-to-machine (M2M) fashion [2], understand each other, and cooperate. To this end, the standardization in V2X communications is absolutely needed and has been actively carried recently worldwide. For instance, European Telecommunication Standard Institute (ETSI) delivered the first ITS-G5 release of V2X communication standards in 5.9 GHz band under European Commission Mandate M/453. ITS-G5 defines the overall vehicular communication protocol stack. Similar stack for North America is specified by IEEE

1609.x WAVE (Wireless Access in Vehicular Environment). The packets with status updates are referred to as Cooperative Awareness Messages (CAMs) in Europe and Basic Safety Messages (BSM) in USA. Both are generated with the periodicity in the order of tens messages per second by every road user and are transmitted to the surroundings in a broadcast mode.

We believe that future self-driving vehicles as well as advanced assistance applications for highly automated driving will rely on a massive deployment of V2X technologies empowered by edge [3] and fog [4] computations, which will make a theoretical concept of VANETs and Internet of Vehicles to come true. The reasonable concern, that connected vehicles could be quite easily exposed to cyberattacks via wireless as entrypoint was risen in [5]. While to prevent uploading of malicious code to vehicle through wireless there are various cryptography-based countermeasures exist, the radio jamming was not studied carefully in the literature.

V2X communication links are inherently vulnerable to different forms of losses that may endanger vehicular safety of the C-ITS. It is important to identify the sources of packet losses in critical vehicular networked control loop since a source could require a design of specific countermeasure. For example, to control the natural sources of losses (e.g., network traffic congestion) in VANETs the Decentralized Congestion Control (DCC) mechanism, which is a mandatory V2X component, was standardized for VANETs in both ETSI and IEEE frameworks. The European DCC approach is based on state machines, where in each state the controller limits parameter values that influence the channel load. At the same time, protocol parameters like CAM generation rate or MAC parameters could be adjusted to avoid performance degradation caused by CAM collisions. CAM losses caused by channel impairments may be partially mitigated by adjusting PHY parameters (e.g. decrease channel datarate, increase transmission power) or, again, adjust CAM parameters (e.g. like CAM generation rate if allowed by congestion control mechanism). However, malicious interference needs to be controlled too. Experiments in [6] demonstrated that a reactive jammer can be created with an open access wireless research platform, when located along the road it can substantially increase the packet loss ratio at V2V links of platooning vehicles up to the level of a complete blackout for few seconds. Thus, a jamming Denial-of-Service (DoS) attack on CAMs may endanger vehicular safety and first and foremost is to be detected in real-time. Moreover, none of the above mechanisms is designed for handling losses caused by malicious interference. Besides, trying aforementioned adaptations, a valuable time in safety critical application could be lost. Instead, one could design specific measures for such situation by immediately adjusting the physical part of the system (e.g. increase headway time between vehicles) to presume safety of the C-ITS application. However, no network control mechanism for malicious interference in VANETs was presumed so far. We believe, that certain steps should be undertaken in this direction.

There are few common ways to execute the Denial-of-Service (DoS) attack in vehicular scenarios. One can keep sending fake requests constantly what makes some segment of VANET busy [7]. Another form of malicious activity is an intentional corruption of the CAM/BSM packets exchanged between some of the road users. For instance, in *random* *jamming* each transmitted packet is distorted by a malicious node independently with a fixed probability. In *ON-OFF jamming*, the interference is generated to destroy a sequence of consecutive packets [8]. The need of jamming detection in VANETs is strongly justified by [6], where the authors implement different jammers and demonstrate their potentially severe impact on the performance of safety V2X applications. Therefore, an emerging problem of malicious interference monitoring, showcased in the form of a real-time jamming detection in vehicular scenarios, is a subject of this article. For a broader context of this problem in the area of wireless network security, an interested reader is referred to [9].

As a starting point to approach the problem, we notice that since both ITS-G5 and WAVE stacks assume IEEE 802.11p standard at the lower layers, we see the approaches designed to detect jammers in Wi-Fi networks as a natural choice for the V2X communications as long as they are appropriately adapted for vehicular context. The fundamental difficulty for a detection of jamming in IEEE 802.11 Medium Access Control (MAC), which adopts a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) approach, is a need to tell legitimate sources of packet losses such as channel impairments and interfering traffic from any malicious activities. Trivial metrics like Packet Delivery Ratio (PDR) are not appropriate for this purpose [10].

Seminal theoretical paper [11] on the detection of DoS attacks in IEEE 802.11 suggests monitoring different channel events and estimating their likelihood while taking into account the rules of the backoff collision resolution mechanism. The detector designed allows for a robust detection of random jamming within the delay in the order of milliseconds for IEEE 802.11b network with unicast traffic. In vehicular scenarios acceptable detection latencies which are imposed by a physical proximity of high-speed road users running C-ITS safety applications, are in the same order. Therefore, we find these results promising and apply similar approach to design a detection method [12] for a periodic broadcast traffic of CAM packets in IEEE 802.11p. Recently, this work of us is independently extended further for multi-channel WAVE framework in [13].

The strong assumption of the latter works, however, is that CAMs are arriving to the MAC layer with a fixed period. Although, in theory this assumption on a perfect CAM periodicity pattern makes sense, there are sources of jitter in real systems. For instance, there will be non-negligible random processing delays between the message generation moment and the time when actual packet is placed in the MAC-queue for the transmission [14]. Therefore, in our article we rely on Artificial Intelligence (AI) to relax this assumption and augment previously suggested statistical method [12] with the data mining approach in order to enable detection of jamming under these more complex conditions. Previously, data mining-based techniques have been already applied for jamming detection in IEEE 802.11 networks [15] and demonstrated high reliability although have not been adapted for time-critical detection in V2X safety scenarios.

The article is organized as follows. In Section II we describe the scenario of interest and assumptions adopted in our study. Section III discusses the limitations of existing VANET jamming detection methods, while our new approach is presented and evaluated in Section IV. Concluding discussions are presented in Section V.

2 Scenario and assumptions

2.1 Scenario

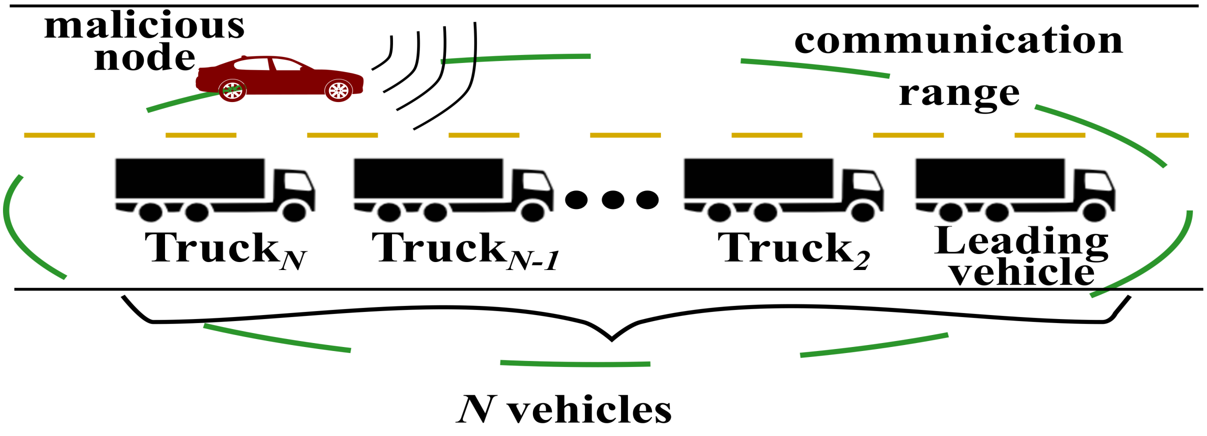


Figure 1: Reference scenario.

In this study we focus on the C-ITS use case named *platooning* [14], which is one of the applications that is assumed to be an early adopter of V2X technology. A European strategy on *"Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility"* (November 2016) highlights, that "Communication between vehicles, infrastructure and with other road users is crucial also to increase the safety of automated vehicles and their full integration into the overall transport system. Truck platooning (trucks communicating to automatically and safely follow each other at very short distance) is a good example: connectivity, cooperation and automation must all come together to make it work."

In platooning the leading vehicle is a human-driven, while others follow it automatically while relying on the information exchange of CAMs on a dedicated ITS-G5 wireless communication channel via the IEEE 802.11p protocol. Therefore, platooning is a C-ITS application where unreliability of V2X communications could negatively influence the system-level performance and even cause critical impact on road safety. It was demonstrated in [6] that jamming attacks may have a crucial impact on platooning communication performance and are easy to implement. Thus, reliable methods to detect jamming intrusion into platooning C-ITS are required. Moreover, taking into account that platooning vehicles are moving with only a few meters inter-vehicle gap, the DoS detection methods should be able to detect attack in *real time* within a fraction of a second.

We consider the following reference jamming DoS attack scenario: platoon moves on a highway, while the malicious vehicle, that implements jamming DoS attacks, drives in the proximity, for instance, on a neighboring lane, see Figure 1.

2.2 Assumptions

We assume a platoon [14] of N vehicles. Following our previous works [12, 14], we assume that all vehicles in the platoon are within each other's communication range. Indeed, since for the valid inter-vehicle distance of 7 m, which for 20–25 vehicles results in a maximum platoon size as of 300 m when the car length is 5 m, and less than 500 m when the truck size is 13 m. A recent measurement campaign (see Fig. 4, [16]) shows that in a convoy of vehicles moving on a highway, exploiting IEEE 802.11p transceivers in the 5.9 GHz band, the communication range, where the vehicles experience confident packet reception, is at least 500 m.

To enable functioning of the platooning control system, we assume each vehicle is generating and transmitting CAM messages. This process incorporates the following steps:

- According to EN 302 637-2 ETSI standard [17] CAM is generated. Each vehicle generates f messages per second (with corresponding generation period $T = \frac{1}{f}$).
- CAM experiences a random transmission *jitter* with distribution $\sim uniform[0, \delta]$ ms before the packet is placed in the MAC queue for the actual transmission.
- CAM packet is transmitted on a dedicated ITS-G5 channel in accordance with the IEEE 802.11p MAC which introduces further CSMA/CA backoff delays.

Following [12], we consider two jamming models:

- *"Random jamming"*. Each transmitted CAM is jammed independently with probability p.
- *"ON-OFF jamming"*. In the OFF state no packets are jammed, while in the ON state K subsequent CAMs are destroyed with probability one. Then the attacker switches to the OFF state. The OFF–ON transitions occur at the moments of CAMs transmission start with probability p_0.

2.3 Data description

The system model described above was used to simulate platoon communication exchange traces for the evaluation of detection methods. As a simulation tool we use our own simulation framework written in MATLAB, the same that was used in our original work in [12]. Number of vehicles in a platoon was varied in the following range $N = \{5, 10, 15, 20, 25\}$. CAM generation frequency was fixed to $f = 30$ Hz. The jitter parameter was set to $\delta = 10$ ms (jitter$\sim U(0, 10)$ ms). We also assume that the detector has information about the time of collision/jamming event in the channel. To our knowledge, there are number of methods proposed in the literature, that could enable collision detection in 802.11 systems. Thus, for example, [18] propose a method that is able to stably and in real-time detect packet collision in OFDM based 802.11 systems. The duration of simulation was fixed to 150 s. Each platoon communication exchange trace had two parts without and with jamming. The part without jamming occupied first 75% (3/4) duration of a trace (approximately 112.5 s). It served as the training data for a detection method. The jamming (either random or ON-OFF strategy) was added to the last 25% (1/4) duration of a trace (approximately 37.5 s). This part was used as the testing data to evaluate the performance of a detection method. During the jamming phase the probability of a CAM to be attacked was fixed to $p = 0.01$, $p_0 = p/K = 0.05$ ($K = 2$). Ten independent platoon communication exchange traces were simulated for each combination of jamming strategy and vehicles number N.

2.4 Performance metrics

For evaluation of detection methods, we use performance metrics commonly accepted in data mining. In particular, *a confusion matrix* is used. It is a table depicting the prediction results against the ground truth. For the purpose of jamming DoS detection, a binary confusion matrix is sufficient. It requires two data labels: positive and negative. Positive labels are given to the events of interest. In our case, these are the collisions caused by a malicious node. Respectively, the legitimate CSMA/CA collisions are marked with negative labels. The binary confusion matrix has four entries referred to as: true negatives (TN), true positives (TP), false negatives (FN), and false positives (FP). In the scope of this paper, the confusion matrix entries are interpreted as follows: *a*) True negatives (denoted as $\mathcal{C}$ for Collisions) are legitimate CSMA/CA collisions correctly identified by a detection method; *b*) True positives (denoted as $\mathcal{J}$ for Jamming) are jammed CAMs correctly identified by a detection method; *c*) False negatives (denoted as $\mathcal{M}$ for Missed detections) are jammed CAMs which were not detected, i.e., they are considered to be legitimate CSMA/CA collisions; *d*) False positives (denoted as $\mathcal{A}$ for false Alarms) are legitimate CSMA/CA collisions which were falsely detected as jammed CAMs.

The confusion matrix characterizes the performance of a detection method. It is, however, convenient to have a single numeric metric for the comparison of different detection methods. As the main focus of this paper is on jamming DoS detection, we have chosen to use F_1 *score* as the overall performance metric of a detection method. Given the confusion matrix, F_1 (denoted as F) score is calculated as follows:

$$F = \frac{2\mathcal{J}}{2\mathcal{J} + \mathcal{A} + \mathcal{M}}.$$

F_1 score of an ideal detection method is 1 while an absolutely idle detection method has F_1 score, which equals 0. In other words, a detection method with the higher F_1 score is preferable.

Two other metrics used below are true positive rate (TPR) and true negative rate (TNR). TPR (denoted as P) is a portion of jammed CAMs correctly identified by a detection method:

$$P = \frac{\mathcal{J}}{\mathcal{J} + \mathcal{M}}.$$

TNR (denoted as I) is a portion of legitimate CSMA/CA collisions correctly identified by a detection method:

$$I = \frac{\mathcal{C}}{\mathcal{C} + \mathcal{A}}.$$

3 Existing detection methods

This section introduces two reference detection methods: *a model-based* and *a data-driven*. The model-based method presented in [12] is the current state-of-the-art for the real-time detection of jamming in VANETs. It is purposefully designed for the considered problem taking into account the knowledge about the IEEE 802.11p communication protocol as well as the platooning C-ITS application and making certain simplifying assumptions, hence, it is model-based.

To enable functioning of each of the later presented detection algorithms, the detector can be envisioned as a sniffer mounted on the leading platoon vehicle.

The operation of the model-based method [12] is the following. First, during an installation phase, the model-based method should collect the statistics of the CAM transmissions in the communication channel, until it receives the sequence of $N + 1$ successfully transmitted CAMs in a row. Then, it separates all the transmissions in different groups accounting for the fact that from the CSMA/CA algorithm rules it follows that two CAMs never collide if they do not have any common slots out of the contention window size to choose. The analysis of the obtained transmitted CAMs provides the outcome of the learning phase in the form of sets of vehicles' identifiers. CAMs of vehicles from different sets never collide with each other. A detection mode is divided into independent *detection periods* (duration of which is equal to the CAM generation period T). The detector compares overheard transmission results with the sets acquired during the installation phase. The jamming is detected using the following straightforward rule: if there is at least one set among the sets formed at the installation phase where exactly one CAM has not been received, a jamming DoS attack is detected.

A data-driven approach in its extreme is completely opposite to a model-based approach. It may work without any knowledge of a system but it requires data produced by that system. Additionally, the data-driven approach requires to use a data mining method for processing the available data.

In terms of data mining, the jamming DoS scenario in this article can be treated as a problem of *anomaly detection in a discrete sequence.* It is the anomaly detection as there are two types of events in the considered system: natural collisions (legitimate CSMA/CA collisions) and anomalous collisions (jammed CAMs). Legitimate CSMA/CA collisions are possible according to the IEEE 802.11p MAC communication protocol used in V2X, hence, they are treated as natural events. Jammed CAMs, on the other hand, are not a part of the system design, they come from an unknown source and they are rather rare (jamming DoS attacks are very dangerous but not as frequently observed as legitimate CSMA/CA collisions on the overall platoon operation scale), therefore, jammed CAMs are treated as anomalies and their occurrence in the system should be detected. Hereafter, we refer to the term *collision* when the source of the CAM loss (either legitimate collision or jamming) is unknown. The type of data for the jamming DoS scenario is discrete sequence because a platoon communication exchange trace is a temporal sequence and at the level of IEEE 802.11p slots it is discrete. For an overview of other types of anomaly detection problems in discrete sequences and data mining methods, an interested reader is referred to survey [19]. For the data-driven detection approach, we use a concrete method suggested in [19] for the case of detecting anomalies in discrete sequences. It is called *the window-based method.*

On a very high conceptual level, the window-based method works in two phases: training and detection. In the training phase, it simply makes a dictionary which consists of fixed-length subsequences of the training data (hence window-based). In the detection phase, it takes a subsequence (the same length as in the dictionary), which should be evaluated. Next, it finds the most similar subsequences in the dictionary. An anomaly score is calculated using values of similarity to these subsequences. Finally, if the calculated anomaly score is above a threshold then the subsequence is considered to be an anomaly.

Performance of the reference detection methods

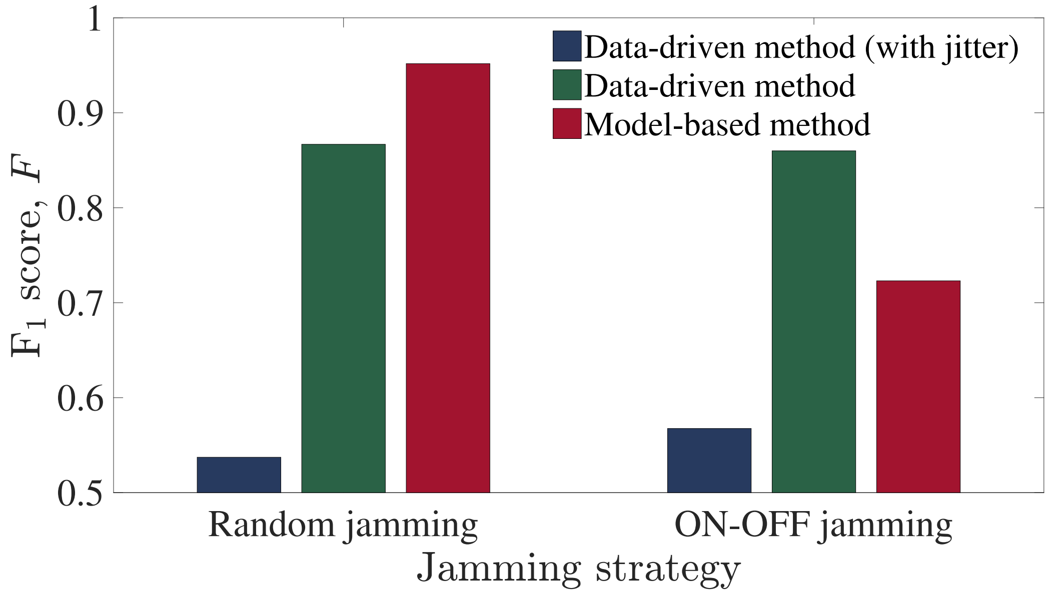


Figure 2: Performance of the reference detection methods: the model-based [12] and the window-based [19]. The number of vehicles in a simulated platoon was fixed to $N = 25$. Bars depict mean true positive rate (P) values.

Figure 2 shows F_1 scores F for the reference detection methods: the model-based [12] and the data-driven window-based method [19]. It is important to note that the the performance of the window-based method is overoptimistic. Recall that this method requires to choose an anomaly threshold, which is usually application dependent. The choice of the anomaly threshold will determine the balance between true positives and true negatives, which in turn determine the detection performance. It was found empirically, that in the data-driven method the correct choice of the anomaly is critical for achieving high detection performance. Therefore, in the absence of a threshold setting algorithm for each platoon communication exchange trace we have chosen to use a threshold that maximized F_1 score. Thus, the reported results should be treated as an optimal theoretical performance rather than a real one.

When we compare the window-based and the model-based detection methods for the case of random jamming, expectedly, the model-based detection method outperforms the data-driven one, since it was specifically designed for the given system model of platoon under specific assumptions and using the knowledge of platoon operation from communication protocol point of view. However, the model-based detection method is designed under the strong assumption, namely it assumes that CAMs are generated with deterministic period and are placed in the MAC queue immediately, although in practice there might be random delays in CAM processing. Thus, this method simply can not operate under any deviations in the moment when CAM arrives to the MAC layer. At the same time, data-driven window-based approach can still provide some detection figures even, when one introduces a jitter.

From Figure 2 it is clear that once the jitter was added the performance of the window-based detection method decreased significantly as there were many false positives in the presence of jitter. In particular, for the random jamming the mean F_1 score dropped from 0.87 to 0.54. In other words, while the window-based detection method works in the presence of jitter its overall performance is rather poor. A possible explanation of the decreased performance of the window-based detection method is based on the fact that the jitter increases the complexity of patterns present in the data. It could be that the increased amount of the training data (with jitter) would address this problem, however, it would make such a data-intensive solution for the considered problem to be impractical.

As one could see, both reference detection methods have their own disadvantages limiting their possible practical usage. Therefore, we propose to consider a hybrid approach that would take the advantages of each reference method to overcome the limitations presented above and enable reliable jamming DoS detection in V2X C-ITS.

4 Proposed detection method

A hybrid detection method combines the prior knowledge of the communication protocol operation of the platoon and the statistics collected from training data (platoon communication exchange trace) for a particular realization of vehicular communications pattern. Similar to the model-based method it operates on detection periods. Another, rather simple knowledge about the system is that in order to create a legitimate CSMA/CA collision at least two vehicles have to transmit their CAMs simultaneously. Because the number of vehicles in the platoon is known and fixed, this knowledge can be used to unequivocally detect jamming in the cases when k collisions happened during a detection period and only $N-k$ CAMs were received. In other words, there are no sources of interference other than a malicious node, hence, collisions are identified as jammed CAMs.

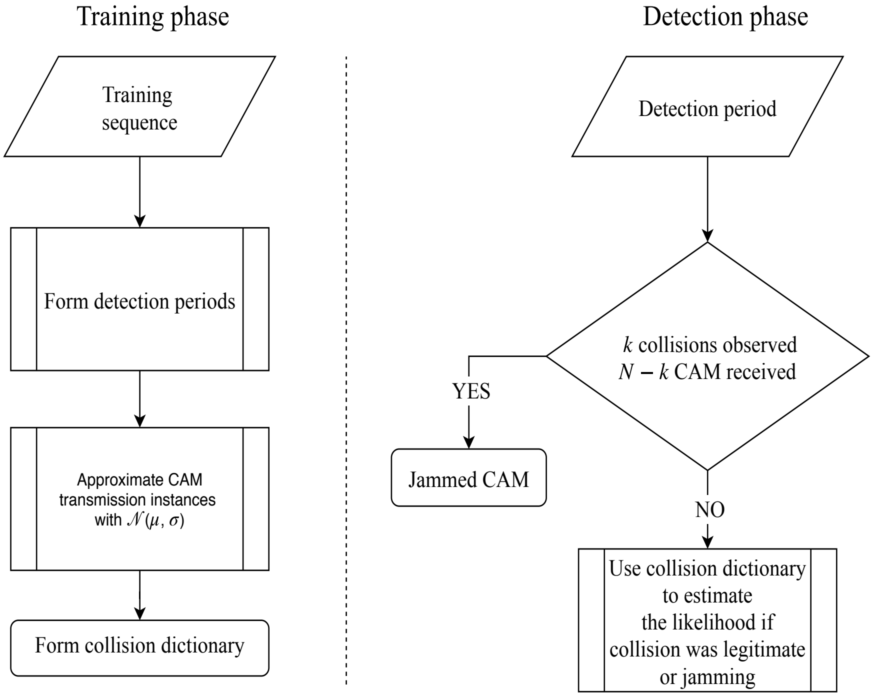


Figure 3: Flowchart of operation of the hybrid detector.

However, more complex cases cannot be treated with this knowledge alone. Therefore, additional information about the system is extracted from the training data. Recall that CAMs are generated with the constant frequency f but the actual CAM transmission time in the detection period fluctuates due to the MAC procedures and jitter. The hybrid detection method uses the training data to approximate the CAM generation time of each vehicles in a detection period using normal distribution. This information is used during a detection phase to estimate how likely particular vehicles were involved in a collision. Additionally, the hybrid detection method creates a dictionary of collisions observed in the training data. The approximations of CAM generation times are used to identify vehicles involved in these collisions.

The detection phase is done in two steps. The first step treats two cases, which can be identified using the knowledge about the system. One case was presented above. Another case is when one collision happened during a detection period and less than $N-1$ CAMs were received, then the collision is identified as the legitimate CSMA/CA collision. The second step treats all other situations using the dictionary of collisions and the approximations of CAM generation times to calculate the anomaly scores for both possible types of collisions (legitimate CSMA/CA collision or jammed CAM). A type with the higher score is assigned to the collision. The general operation of the hybrid detector is summarized as flowchart on Figure 3. It should be noted that for the model-based detector the decision on jamming presence is taken every T. For hybrid detector the decision delay does not exceed $1.5T$. Thus, both detectors are able to detect jamming in real-time and the decision delay is bounded.

Performance of the hybrid detection method

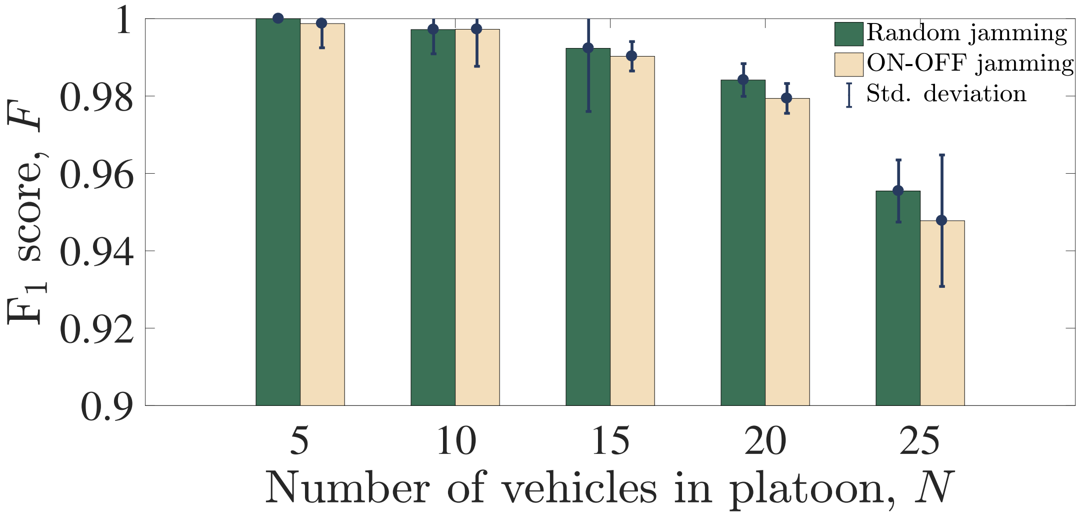


Figure 4: Performance (F_1 score) of the hybrid detection method against the number of vehicles in a platoon for random and ON-OFF jamming strategies.

Figure 4 shows the hybrid detection method performance in terms of F_1 score (both mean values and standard deviations are shown). The results are depicted for two different jamming strategies and varying number of vehicles in the platoon. There are two main findings observed. First, for the increased number of vehicles, mean F_1 score is decreasing while standard deviations are increasing. Second, the hybrid detection method performs slightly better in the case of random jamming. We conjecture that it has to do with the nature of the hybrid detection method, which performs detections within the detection periods. As the ON-OFF jamming introduces the consequent collisions, it could increase the complexity of analysis for determining the nature of each collision.

Table 1 provides mean values of P (TRP) and I (TNR) for the hybrid detection method in the considered range of vehicles in the platoon. The upper part of the table shows the results for the random jamming while the lower part of the table shows the results for the ON-OFF jamming. The results show that the efficiency of jamming detection is similar for both jamming strategies. It mostly depends on the number of vehicles participating in the platoon. Similar, to the Figure 4 both performance metrics decrease with the increased number of vehicles in a platoon. However, even when the number of

Table 1: Detection performance.

Random jamming					
N	5	10	15	20	25
TNR, I	1.000	0.992	0.986	0.983	0.978
TPR, P	1.000	0.997	0.993	0.985	0.956
ON-OFF jamming					
N	5	10	15	20	25
TNR, I	1.000	0.990	0.982	0.977	0.973
TPR, P	0.998	0.997	0.991	0.981	0.950

vehicles is large ($N = 25$) both metrics have high values, especially when compared to the performance of the alternative method (cf. Figure 2).

5 Discussions

Based on the results of the performance evaluation, one could conclude, that for both random and ON-OFF jamming strategies, the hybrid detection method demonstrated a high detection performance keeping false positive rate $(1 - I)$ and false negative rate $(1 - P)$ at quite low levels. It is important to note here, that the hybrid detection method was tested in the scenario system with jitter, which the two considered reference detection methods were not able to deal with.

In contrast to the reference detection methods, the nature of the proposed detection method is hybrid. It takes into account the knowledge about the platoon from the communication protocol point of view (as the model-based method [12]) but it also uses a communication exchange trace produced by a platoon (as the window-based method). Thus, the hybrid detection method tries to avoid the drawbacks of each reference approach: it works in the presence on jitter (in contrast to the model-based [12]) and shows much higher detection performance in the presence of jitter in contrast to the data-driven window-based method [19].

While the performance of the data-driven method considered in this article is not high, one should not infer that there are no existing data mining algorithms which can deal with the problem of interest. However, we presented that the baseline method for anomaly detection in a discrete sequence suggested in the literature [19] did not achieve satisfactory results. Therefore, we conclude that it is not trivial to simply apply data mining methods to this problem without using the prior knowledge about the nature of the system.

Another aspect of applying data mining methods is the usage of Deep Learning (DL), which is the dominating AI paradigm in many application areas. In relation to the considered problem, there are two challenges for the DL. First, it requires a significant amount of data. Currently, it does not seem feasible to train a detection method for a general case (arbitrary vehicular communications pattern in a platoon). It implies that one cannot train a detection method using, for example, simulated data and then deploy the trained method in a real system. Instead, the data from a particular realization of inter-vehicular communications pattern is needed but the amount of this data should not be large otherwise a method becomes impractical. A possible way to overcome this challenge could be the use of the transfer learning approach when a detection method would be trained, e.g., with simulated data. This initially trained method would then be used to adjust to a particular inter-vehicular communications pattern. The second challenge is in

the nature of problems solved by the DL. Up to this day, most of the DL methods require the supervised (annotated) data while the considered problem belongs to a class of anomaly detection (see Section 3) where anomalous events are not available in the training data.

Nevertheless, we conclude that AI-powered jamming DoS detection methods allow handling realistic IEEE 802.11p V2X protocol behavior with uncertain time components accompanying CAM generation, processing, and transmission processes. The later could become an enabler for detection methods that would account for varying period CAM generation strategies, for instance, mobility-dependent CAM triggering approaches [20] or for a stochastic nature of CAM losses due to the impairments in the wireless channel. From the network traffic control perspective, as soon as the DoS attack has been detected in VANET, the next step is to apply a countermeasure, whose design we leave for future work.

Acknowledgement

The authors wish to thank the anonymous reviewers for their helpful comments. The research leading to the results reported in this work has received funding from the Knowledge Foundation in the framework of AstaMoCA "Model-based Communication Architecture for the AstaZero Automotive Safety" project (2017–2019) and from the ELLIIT Strategic Research Network.

References

[1] K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier, “Cooperative intelligent transport systems in europe: Current deployment status and outlook,” *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 89–97, June 2017.

[2] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, “Home m2m networks: Architectures, standards, and qos improvement,” *IEEE Communications Magazine*, vol. 49, no. 4, pp. 44–52, April 2011.

[3] H. Liu, Y. Zhang, and T. Yang, “Blockchain-enabled security in electric vehicles cloud and edge computing,” *IEEE Network*, vol. 32, no. 3, pp. 78–83, May 2018.

[4] J. Kang, R. Yu, X. Huang, and Y. Zhang, “Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–11, 2017.

[5] M. H. Eiza and Q. Ni, “Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity,” *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, June 2017.

[6] O. Punal, C. Pereira, A. Aguiar, and J. Gross, “Experimental characterization and modeling of RF jamming attacks on VANETs,” *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, February 2015.

[7] Z. A. Biron, S. Dey, and P. Pisu, “Real-time detection and estimation of denial of service attack in connected vehicle systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. PP, no. 99, pp. 1–10, 2018.

[8] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” *IEEE Communications Surveys Tutorials*, vol. 13, no. 2, pp. 245–257, 2011.

[9] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: Technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, September 2016.

[10] L. Mokdad, J. Ben-Othman, and A. T. Nguyen, “DJAVAN: Detecting jamming attacks in vehicle ad hoc networks,” *Performance Evaluation*, vol. 87, pp. 47 – 59, 2015, special Issue: Recent Advances in Modeling and Performance Evaluation in Wireless and Mobile Systems. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0166531615000048

[11] A. L. Toledo and X. Wang, “Robust detection of mac layer denial-of-service attacks in csma/ca wireless networks,” *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 347–358, Sept 2008.

[12] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, “Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks,” *IEEE Communications Letters*, vol. 18, no. 1, pp. 110–113, January 2014.

[13] A. Benslimane and H. Nguyen-Minh, “Jamming attack model and detection method for beacons under multichannel operation in vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 7, pp. 6475–6488, July 2017.

[14] A. Vinel, L. Lan, and N. Lyamin, “Vehicle-to-vehicle communication in C-ACC/platooning scenarios,” *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[15] O. Punal, I. Aktas, C. J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," in *Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014*, June 2014, pp. 1–10.

[16] M. G. Nilsson, D. Vlastaras, T. Abbas, B. Bergqvist, and F. Tufvesson, "On multilink shadowing effects in measured V2V channels on highway," in *2015 9th European Conference on Antennas and Propagation (EuCAP)*, May 2015, pp. 1–5.

[17] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service," *ETSI EN 302 637-2 V1.3.2*, 2014.

[18] T. Zhou, X. Wang, and W. Hou, "A fast collision detection algorithm in ieee 802.11 through physical layer sinr monitoring," in *2011 IEEE 73rd Vehicular Technology Conference (VTC Spring)*, May 2011, pp. 1–5.

[19] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection for discrete sequences: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 5, pp. 823–839, May 2012.

[20] C. Campolo, A. Molinaro, A. Vinel, and Y. Zhang, "Modeling prioritized broadcasting in multichannel vehicular networks," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 2, pp. 687–701, 2012.

Paper 5

Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining

Authors:
Nikita Lyamin, Denis Kleyko, Quentin Delooz, Alexey Vinel

Reformatted version of paper submitted to:
IEEE Communications Letters

Real-time jamming DoS detection in safety-critical V2V C-ITS using data mining

Nikita Lyamin, Denis Kleyko, Quentin Delooz, Alexey Vinel

Abstract

A data mining-based method for real-time detection of radio jamming Denial-of-Service (DoS) attacks in IEEE 802.11p vehicle-to-vehicle (V2V) communications is proposed. The method aims at understanding reasons of losses of periodic cooperative awareness messages (CAM) exchanged by vehicles in a platoon. The detection relies on the knowledge of IEEE 802.11p protocols rules as well as on historical observation of events in the V2V channel. In comparison to the state-of-the-art method, the proposed method allows operating under the realistic assumption of random jitter accompanying every CAM transmission. The method is evaluated for two jamming models: random and ON-OFF.

1 Introduction

Cooperative ITS (C-ITS) is a promising extension of Intelligent Transport Systems (ITS) when together with recent electronic advancements, the connectivity between road users is introduced. Overall, C-ITS aims at improving road safety and vehicle fleet management, decrease congestion, and reduce energy use. Vehicle-to-Vehicle (V2V) communications in Vehicular Ad-hoc Networks (VANETs) are expected to be a major enabler of such a connectivity in C-ITS [1].

Different novel C-ITS applications can be enabled by V2V communications [2]. Our focus is on a *platooning*, where a caravan of vehicles automatically follows a human-driven leading one, which is one of the applications that is assumed to be an early adopter of VANETs [3].

The automatic control of a platoon relies, particularly, on the information in cooperative awareness messages (CAMs) transmitted on a dedicated DSRC/ITS-G5 wireless communication channel via the IEEE 802.11p protocol. Therefore, platooning is a C-ITS application where unreliability of V2V communications could seriously deteriorate the system-level performance and even cause critical impact on road safety.

Packet losses in VANETs may be caused not only by legitimate IEEE 802.11p CSMA/CA collisions or ITS-G5/DSRC channel impairments, but also by malicious interference originated from a radio transmitter located in the vicinity of communicating vehicles.

Experiments in [4] demonstrated that Denial-of-Service (DoS) attacks via jamming of CAMs are easy to implement and may have a crucial impact on the platooning performance. Specifically, jammer with the reaction time in order of tens microseconds can be created with an open access wireless research platform. When located along the road, such a reactive jammer can substantially increase the packet loss ratio at V2V links of platooning vehicles up to the level of a complete blackout for few seconds.

The simulation study in [5] demonstrated that the platoon system is highly sensitive to jamming attacks and its performance can be compromised by a reactive jammer, in particular it was shown that the presence of reactive jammer may lead to string instability phenomena. In [6] authors perform a simulation experiment for radio jamming countermeasures effectiveness, i.e. beamforming. Results demonstrate that in static configuration of nodes like platooning beamforming may reduce the harmful influence of radio jamming on platooning performance. However, no jamming detection technique was proposed in study to identify the presence of jammer, also the power of the jammer was limited, which make efficiency of beamforming questionable under stronger jamming signal.

Thus, reliable methods to detect radio jamming DoS intrusion into platooning C-ITS are required. Moreover, taking into account that platooning vehicles are moving with only a few meters inter-vehicle gap, the jamming DoS detection methods should be able to detect an attack in *real-time* within a fraction of second.

This letter enhances the model-based detector presented in [7] by relaxing one of its key assumptions. Namely, [7] assumes fixed CAM generation period and is not designed to operate under its random deviations inherent to practical DSRC/ITS-G5 implementations [3].

The letter is organized as follows. Section 2 describes the scenario of interest and the adopted assumptions. The proposed detector is presented in Section 3. Performance of detectors is evaluated in Section 4. Section 5 concludes the letter.

2 Scenario & System model

2.1 Reference scenario

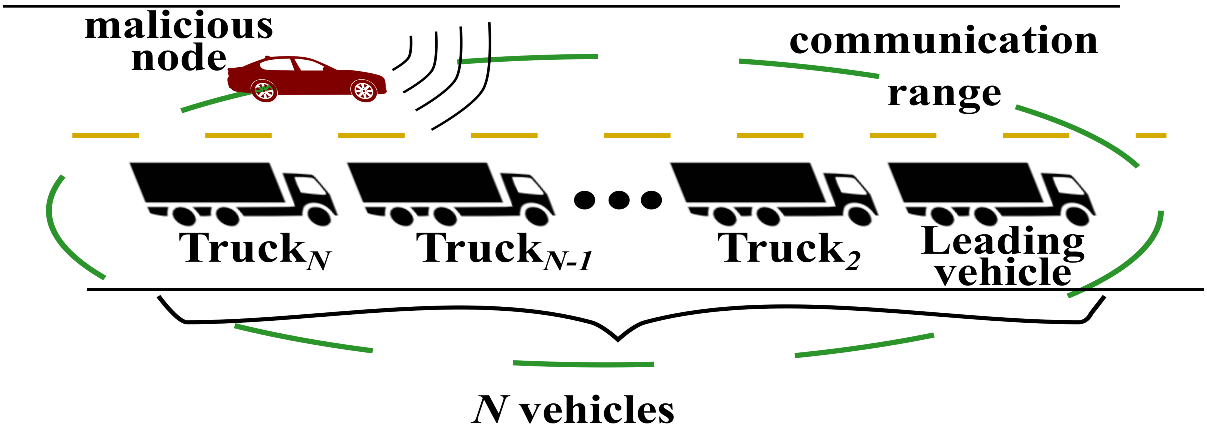


Figure 1: Reference scenario.

We consider the following reference jamming DoS attack scenario: platoon moves on a highway, while the malicious vehicle, that implements jamming DoS attacks, drives in the proximity, for instance, on a neighboring lane, see Figure 1.

2.2 Assumptions

We assume a platoon of N vehicles. Following our previous works [7, 3], we assume that all vehicles in the platoon are within each other's communication range.

To enable functioning of the platooning automatic control system, we assume each vehicle is generating and transmitting CAM messages. This process incorporates the following steps:

- EN 302 637-2 CAM [8] is generated. Each vehicle generates f messages per second (with corresponding generation period $T = \frac{1}{f}$).
- CAM experiences a random transmission *jitter* with distribution $\sim U[0, \delta]$ ms before the packet is placed in the Medium Access Control (MAC) queue for the actual transmission. In our previous work [7] no jitter was assumed. Although, in theory this assumption on a perfect CAM periodicity pattern makes sense, there are sources of jitter in real systems. For instance, there will be non-negligible random processing delays between the message generation moment and the time when actual packet is placed in the MAC-queue for the transmission [3].
- CAM packet is transmitted on a *dedicated* ITS-G5 channel in accordance with the IEEE 802.11p MAC which introduces further CSMA/CA backoff delays.
- The communication channel is assumed to be error-prone with independent CAM losses and fixed packet error rate (PER).

Following [7], we focus on the two following jamming models:

- *"Random jamming"*. Each transmitted CAM is jammed randomly and independently with probability p.
- *"ON-OFF jamming"*. In the OFF state no packets are jammed, while in the ON state K subsequent CAMs are destroyed. Then the attacker switches to the OFF state. The OFF–ON transitions occur at the moments of CAMs transmission start with probability $p_0 = p/K$.

To enable functioning of the jamming DoS detector, we assume the leading vehicle in the platoon is equipped with ITS-G5 communication device and able to *sniff* communication exchange between platoon members and implement the detection algorithm. Also, we consider that platoon leader is always aware of the current platoon configuration (number of vehicles N, adopted CAM generation period T) [3].

The detectors were evaluated using platoon communication exchange traces. Traces were obtained via the simulations of the system described above. Table 1 presents the parameters of simulations. Training sequences were not exposed to jamming.

Table 1: Summary of data parameters (unless stated differently)

Parameter	Values	Parameter	Values
Trace duration	150 s	CAM frequency	$f = 30$ Hz
Training sequence	first 75%	ON-OFF jamming par.	$K = 2$
Testing sequence	last 25%	Jitter par.	$\delta = 10$ ms
# of traces[1]	10	Error rate, PER	0.1

3 Detection methods

3.1 Model-based detector

The operation of the model-based detector [7] is divided into training and detection phase[2]. During training phase method collects statistics of $N + 1$ successfully received in a row CAM transmissions and subsequently classify them in the *groups* following the rule: only CAM messages that could potentially collide from the CSMA/CA standpoint are placed in the same group. A detection mode operates on the independent *detection periods* (duration of which is fixed and equals to CAM generation period T). During detection phase the alarm is raised when exactly one CAM from the group formed in the training phase is not received. Due to the space limitation, we omit the technical details of the model-based detector operation, interested reader is kindly referred to original publication [7].

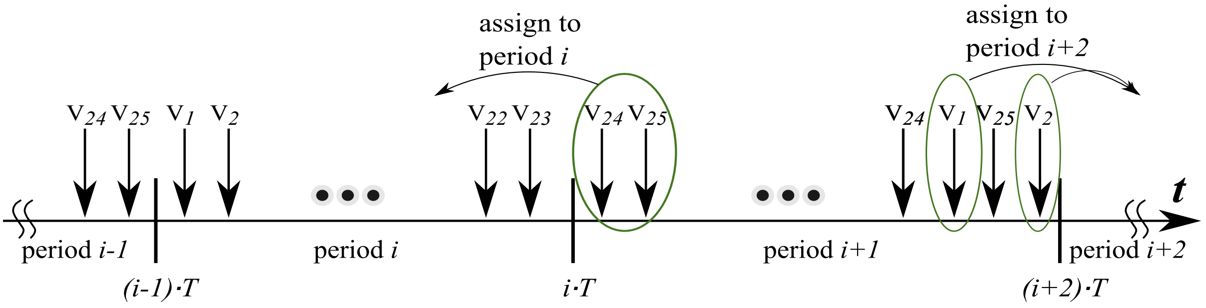


Figure 2: Detection sets.

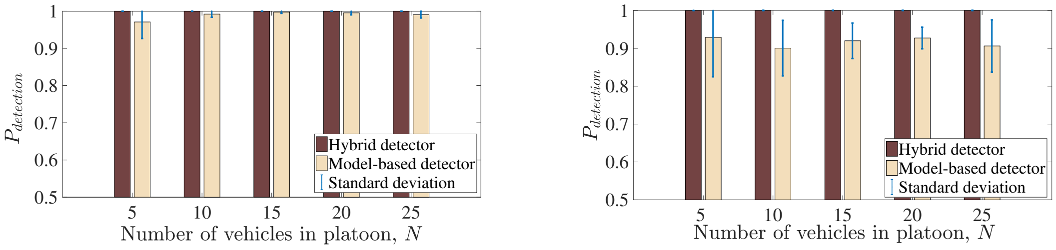
3.2 Hybrid detector

In terms of data mining, the jamming DoS scenario in this letter can be treated as a problem of *anomaly detection in a discrete sequence* [9].

There are two types of events in the considered system: natural collisions (legitimate CSMA/CA collisions) and anomalous collisions (jammed CAMs). The proposed method

---

[2] In the original manuscript [7] the training phase was referred to as *installation phase*, while detection phase had a notion of *normal operation*.



(a) Random jamming **(b)** ON-OFF jamming, $K = 2$

Figure 3: Probabilities of attack detection for the model-based and hybrid detectors against the number of vehicles in a platoon in the absence of jitter ($\delta = 0$) and noise-free channel for $p = 0.4$. Plots depict mean and standard deviation values.

has a hybrid nature. Following data mining approach, it uses historical data of platoon communications. At the same time, the a priori knowledge about a platoon is used in the method.

The detector observes the transmissions of CAMs from different vehicles as well as the collisions. The overall outline of jamming detector is presented in the form of a flowchart in Fig. 4.

Training phase

Our initial target is to try grouping received CAMs, which are closely located on the time axis, into *detection sets* in such a way that each set contains N received CAMs (one from each vehicle). Our heuristic approach tries to do so.

First, we find N subsequently successfully received CAMs from different vehicles and assign the identifiers V to these CAMs (or respective vehicles) via their enumeration in the ascending order from 1 to N. An interval of duration T which starts from the transmission time of the first CAM in this sequence will be referred to as the *detection period*. We use this initially identified period to further slot the entire time axis into detection periods.

Second, for each detection period i, we create *detection sets* $\mathcal{R}_i$ of pairs {CAM id, CAM transmission time} as follows. In each detection period we track the last highest CAM id received (denoted as $lastHighestid$). We use the parameter $k = N/2$. When a collision is observed $lastHighestid$ is also incremented by one. Let us denote the identifier of the CAM under consideration as id. If the $id > lastHighestid + k$ we assign CAM to the previous detection period, if $id < lastHighestid - k$ we assign CAM to the next detection period, else we assign CAM to the current detection period. The illustration of this process is shown on Fig. 2. CAM transmission time is measured from the beginning of the detection period it belongs to.

Our next target is to "make a guess" which CAMs could have been involved into each collision. For each detection period i and respective detection set $\mathcal{R}_i$ we consider time intervals from the beginning of the period till CAM transmission times. For every vehicle V we average the data from different detection periods and compute the mean μ_V and the standard deviation σ_V of these intervals durations. As a result we get intervals of highly probable transmission starting times of each vehicle V: $\tau_V = [\mu_V - \sigma_V, \mu_V + \sigma_V]$.

Detection phase

During the detection phase, the detector keeps operating on the detection periods of length T and uses intervals of most probable transmissions τ_V for all the vehicles from 1 to N obtained at the learning phase. Moreover, for each detection period i the detector builds a detection set $\mathcal{R}_i$, which is constructed by the middle of detection period $i+1$ as explained above.

We analyze each observed collision. On every detection interval i for each collision c with starting time t_c we try to "make a guess" on which CAMs could create it and make a set $\mathbf{M}_c$ consisting of their ids. To this end we consider all the CAMs with ids V, which are *not* in the detection set $\mathcal{R}_i$ and if t_c falls into interval τ_V, then V is added into set $\mathbf{M}_c$. Also the set $\mathbf{C}_c$ with an only element - collision identifier c - is created.

Next, we try to find CAMs which could be involved in several collisions. For all possible pairs of $\mathbf{M}_i$ and $\mathbf{M}_j$ $(i \neq j)$ we check if there is a CAM id V exists which is included in both of them. If found, we merge $\mathbf{M}_i$ with $\mathbf{M}_j$ and $\mathbf{C}_i$ with $\mathbf{C}_j$. The process is repeated until we cannot find such CAM V any longer.

Finally, for each detection period we construct *dependent collision set* $\mathbf{C} = \{\mathbf{C}_1, \ldots, \mathbf{C}_k\}$ and *involved vehicles set* $\mathbf{M} = \{\mathbf{M}_1, \ldots, \mathbf{M}_k\}$, which both consists of subsets from the previous step. The jamming detection is built on the basic knowledge about the system: *in order to create a legitimate CSMA/CA collision at least two vehicles have to transmit their CAMs simultaneously*, what enables the decision on raising the alarm jamming if inequality $|\mathbf{M}_j| \geq 2|\mathbf{C}_j|$ does not hold for at least one pair of subsets $\mathbf{M}_j$ and $\mathbf{C}_j$.

4 Performance evaluation

In this section the detectors are studied from two angles. First, we conduct their performance comparison in the absence of jitter. Second, since the model-based detector is brittle to jitter, we introduce jitter in our experiments and focus on a performance of the hybrid detector only.

We are interested in the following performance metrics:

- *Upper bound on decision delay.* For model-based detector the decision on jamming presence is taken every T. Since the operation of hybrid detector is based on the construction of detection sets $\mathcal{R}_i$, the decision delay does not exceed $1.5T$. Thus, both detectors are able to detect jamming in real-time and the decision delay is bounded. For our numerical values it does not exceed 50 ms.

- *Probability of attack detection.* We inherit approach used in [7] and in the following subsections we use the probability of attack detection $P_{detection}$, i.e. the probability that the alarm is triggered, given that at least one successfully transmitted beacon is jammed in the detection set[3].

---

[3] Under the given set of assumptions and based on the rules of detector operation, the probability of

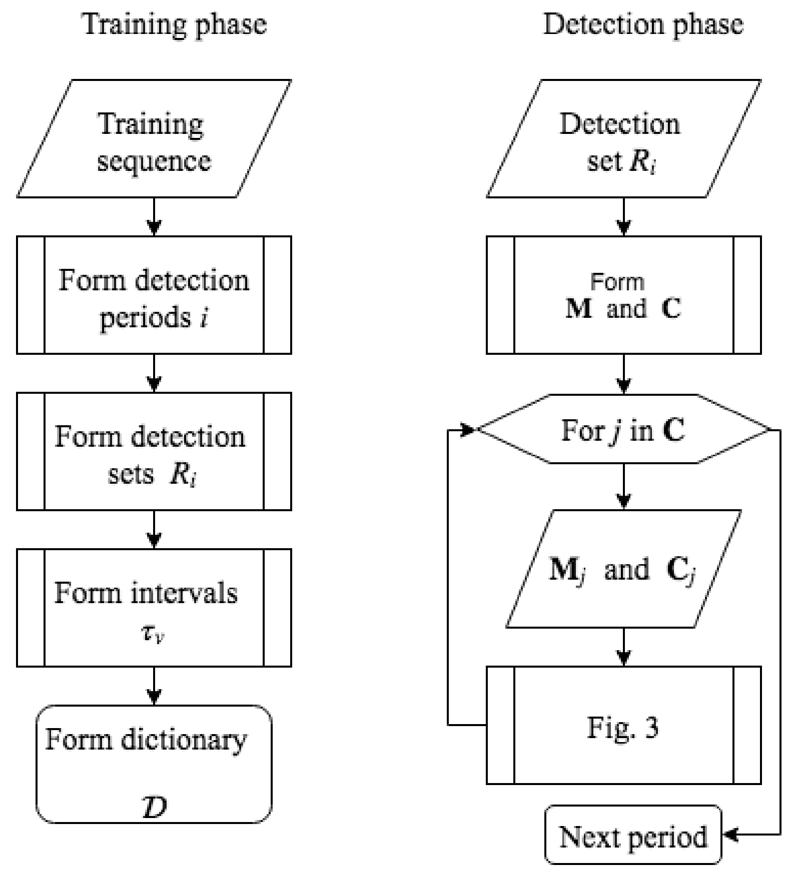
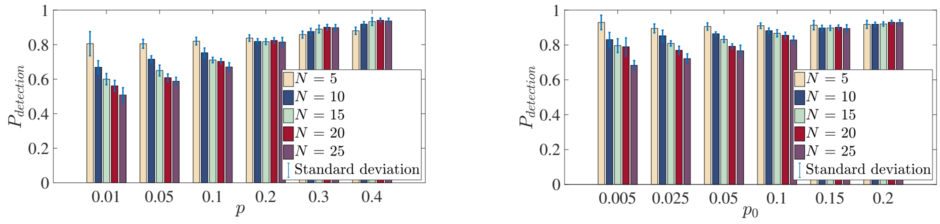


Figure 4: Flowchart summarizing the operation of the proposed detector.



(a) Random jamming **(b)** ON-OFF jamming, $K = 2$

Figure 5: Probabilities of attack detection of the hybrid detector against the number of vehicles in a platoon in the presence of jitter and packet looses. Plot depicts mean and standard deviation values.

4.1 Performance comparison of two detectors

Fig. 3 compares both detectors in terms of $P_{detection}$ against varying number of vehicles in a platoon when there is no jitter in CAM transmissions and noise-free channel assumption. From Fig. 3 one can see, that the performance of model-based detector is decreasing under ON-OFF jamming strategy. The reason is the design of detection algorithm.

---

false alarm, i.e. the probability that the alarm is triggered although no beacons have been jammed in the detection period, does not exceed 1% for presented experiments.

When one increases the number of vehicles N, the probability of groups in detection period of model-based detector with more than one CAM is increasing. Thus, when several of jammed CAMs or a jammed CAM together with natural legitimate collision are appearing in the same group, model-based detector is unable to detect it, which can contribute visibly to the decrease in true positives $P_{detection}$. The same principle applies to the increase of CAM generation frequency [4]: with the decrease of time diversity within a detection period, more large groups are formed during training phase which leads to the decrease of $P_{detection}$ under same jamming probabilities p. One can conclude that the performance of hybrid detector outperforms that of model-based one.

4.2 Performance of hybrid detector

Fig. 5 and 6 evaluate the hybrid detector in terms of $P_{detection}$ when jitter is added to CAM transmissions and also packet losses are introduced. Overall, the hybrid detector demonstrates better performance under ON-OFF jamming. The performance of hybrid detector decreased in the presence of jitter and packet loss but the lowest $P_{detection}$ is still higher than 0.7 (for N=25, p=0.1).

Also, the results show that the hybrid detector does not require long training sequence for approaching its best performance. In fact, even for short training sequences (5 s) $P_{detection}$ are identical to the values achieved for, e.g., 100 s. Moreover, the performance for short training sequences is as stable as for long training sequences as standard deviations are comparable. These results allow conjecturing that the hybrid detector can be easily retrained if necessary, for example, when the number of vehicles in a platoon has changed. Let us note here that a platoon configuration is rather static and does not change in the time scale of minutes or even hours: new members join/leave platoon relatively rarely. Moreover, even when platoon configuration changes, the hybrid detector could be retrained for further deployment in 1-5 seconds.

5 Conclusion & Future work

In this letter, we presented a new method of radio jamming DoS attacks detection in IEEE 802.11p VANETs. The simulation experiments showed that the performance of the proposed method was comparable to the existing method in ideal conditions of constant packets transmission interval, while it also demonstrated high performance in the presence of its jitter. Moreover, the proposed method does not require a large amount of historical data which makes it suitable for a practical deployment.

In our future work, we are going to perform a detailed study of additional performance dimensions of the proposed method such as varying parameters of jitter distribution. We also plan to include additional jamming models and known data mining techniques [9]. We also aim to proof the performance of the proposed DoS detections approach on the real measurement data (e.g. logs from C-ITS and platooning trial projects) and fine-tune

---

[4] It should be noted here, that in [7] the value of f was set to 10 Hz, while it is 30 Hz in the current study. This fact explains the variation in model-based detector result, compared to figures 5 and 6 presented in [7].

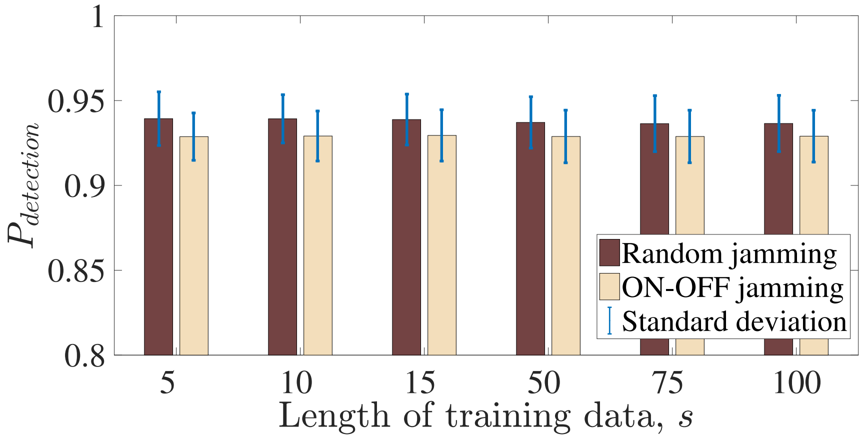


Figure 6: Probabilities of attack detection of the hybrid detector against the length of the training sequence for random and ON-OFF jamming strategies. Plot depicts mean and standard deviation values. The number of vehicles in a platoon is fixed to $N = 25$, $p = 0.4$.

the detecting capabilities (e.g. adjustment of the operation for practical receiver, initial calibration and real-time adaptations to the observed channel quality).

References

[1] K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier, "Cooperative intelligent transport systems in europe: Current deployment status and outlook," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 89–97, June 2017.

[2] C. Englund et al., "Future applications of vanets," *In: C. Campolo et al. (eds) Vehicular ad hoc Networks. Springer*, 2015.

[3] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-vehicle communication in C-ACC/platooning scenarios," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[4] O. Punal, C. Pereira, A. Aguiar, and J. Gross, "Experimental characterization and modeling of RF jamming attacks on VANETs," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 524–540, February 2015.

[5] A. Alipour-Fanid et al., "String stability analysis of cooperative adaptive cruise control under jamming attacks," in *2017 IEEE 18th Int. Symp. on High Assurance Systems Engineering*, 2017, pp. 157–162.

[6] G. Patounas et al., "Evaluating defence schemes against jamming in vehicle platoon networks," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, 2015, pp. 2153–2158.

[7] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo, “Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks,” *IEEE Communications Letters*, vol. 18, no. 1, pp. 110–113, January 2014.

[8] “Intelligent transport systems (ITS); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service,” *ETSI EN 302 637-2 V1.3.2*, 2014.

[9] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection for discrete sequences: A survey,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 5, pp. 823–839, May 2012.