Connected Automated Driving: A Model-Based Approach to the Analysis of Basic Awareness Services

Hugo Araujo[1], Ties Hoenselaar[2], Mohammad Reza Mousavi[3] and Alexey Vinel[4]

***Abstract*—Cooperative awareness basic services are key components of several Connected Autonomous Vehicles (CAV) functions. We present a rigorous approach to the analysis of cooperative awareness basic services in a CAV setup. Our approach addresses a major challenge in the traditional analysis techniques of such services, namely, coming up with effective scenarios that can meaningfully cover their various behaviours, exercise the limits of these services and come up with a quantitative means for design-space exploration.**

Our approach integrates model-based testing and search-based testing to automatically generate scenarios and steer the scenario generation process towards generating inputs that can lead to the most severe hazards. Additionally we define other objectives that maximise the coverage of the model and the diversity of the generated test inputs. The result of applying our technique to the analysis of cooperative awareness services leads to automatically generated hazardous scenarios for parameters that abide by the ETSI ITS-G5 vehicular communications standard. We show that our technique can be used as an effective design-space exploration method and can be used to design adaptive protocols that can mitigate the hazards detected through our initial analysis.

1. Introduction

Rigorous and structured validation and verification methods are pivotal for the wide-spread deployment and public acceptance of connected and autonomous vehicles. The need for such methods is intensified in the functions enabled by vehicle-to-vehicle (V2V) communication, due to the close interaction among the communication protocols, control software, and vehicle dynamics. Much of the existing (manual) analysis techniques do not scale to the huge design-space and input-space of these functions and hence, there is an increasing demand for automated validation and verification techniques to explore these huge spaces effectively.

One of the main challenges in this domain is coming up with scenarios (e.g., human driver behaviour, vehicle dynamics, road users' behaviour, and connectivity conditions) that can effectively cover the various behaviours of such systems and in particular, exercise those behaviours that are likely to lead to hazardous situations.

In this paper, we introduce an automated verification technique to automatically generate effective scenarios (test cases) to evaluate the Cooperative Awareness Services (CAS) in the context of connected automated driving. We aim to automatically generate and verify various scenarios for a convoy of autonomous vehicles following a lead vehicle with a human driver (e.g., in vehicle platoons). By generating such scenarios, our goal is to identify sets of parameters of packets generation for the state-of-the-art vehicle-to-vehicle communication protocol, specified in the ETSI EN 302 637-2 standard that can lead to hazardous situations (e.g., collisions or split convoys due to increased distance) during cooperative manoeuvres. Thus, we aim to show how these design parameters (i.e., the default recommended by ETSI and the ones we built ourselves) fare when they are verified against automatically-generated challenging scenarios that aim to identify hazardous situations and communication issues. In particular, we would like to answer the following two concrete research questions using our proposed methodology, elaborated below:

- **RQ1:** Is it possible to find hazardous behaviours caused by communication issues in scenarios abiding by the ETSI EN 302 637-2 standard?
- **RQ2:** Do the default parameter values described in the ETSI EN 302 637-2 protocol handle extreme situations better than other sets of values?

Our technique builds upon a model of ITS-G5 V2V Cooperative Awareness Basic Services at Facilities Layer that we have developed in accordance to the ETSI EN 302 637-2. The services operate on top of IEEE 802.11p Carrier-Sensing Multiple Access with Collision Avoidance (CSMA/CA) protocol. The developed model is then used as the basis for a multi-objective search technique that automatically steers the search in the scenario space (the acceleration and deceleration of the leading vehicle) in order to maximise the following objectives: 1) hazard likelihood, 2) data age, and 3) diversity. We use an adapted version of our HyConf Conformance Testing [1], [2] environment to implement and evaluate our approach.

Our results indicate that our approach, i.e., the integration of model-based testing and multi-objective search, provides an effective methodology for design-space explo-

[1]*Universidade Federal de Pernambuco* hlsa@cin.ufpe.br
[2]*TU Eindhoven* t.a.h.hoenselaar@student.tue.nl
[3]*University of Leicester* mm789@leicester.ac.uk
[4]*Halmstad University* alexey.vinel@hh.se

ration in analysing CAS. Using this methodology, we were able to generate hazardous situations (e.g., collisions) due to communication issues in vehicles that adopt reasonable kinematic functions, and thereby answer our two research questions. We discuss our approach and present the results in the remainder of the paper and subsequently, analyse the effect of changing different design parameters.

The remainder of this paper is structured as follows. In Section 2, we provide an overview of the model used for scenario generation and analyse its underlying assumptions. In Section 3, we introduce our analysis strategy. In Section 4, we explain the setup of our experiments that are designed to answer our research questions. Section 5 is dedicated to the presentation of our experimental results and their analysis. In Section 6, we present an overview of the related work in this area. Section 7 concludes the paper and presents the directions of our ongoing research.

2. Our Model and Modelling Assumptions

In this section, we explain the model that we have designed as the starting point for verification. We also specify the assumptions used in designing the abstract model and justify them for the verification task at hand.

As mentioned in the introduction, the model concerns a convoy of connected and autonomous vehicles; an overview of the modelled system is presented in Figure 1. We consider a model that comprises five vehicles: the human-controlled leader vehicle and 4 autonomous vehicles following the leader.

2.1. Vehicle dynamics and control

In order to automatically accelerate and decelerate the follower cars, an automatic controller must be in place. We use a simple controller called the Intelligent Driver Model (IDM) [13], which is further specified below. Our choice for such a simpler controller is justified, since our focus is to analyse the effect of communication protocol parameters on safety (and not to analyse and compare different control strategies).

Also for simplification, the current model only takes longitudinal movement of the car into account. We assume that the vehicles move along a long stretch of road without any drastic changes in direction. This assumption is justified by our focus on the V2V communication and its effect on safety. We expect the latitudinal manoeuvres will have similar effects and will be included in our future studies.

The input to our lead vehicle model is the acceleration and deceleration behaviour of the human driver. Once this input is provided to the lead vehicle, the following vehicles respond to the lead vehicle's behaviour using their autonomous controller. The other input parameters to our model are the design-space parameters of the CAS protocol, specified in the next section. In this model, the acceleration of the follower vehicles is described by the following function [13]:

$$a_{IDM}(s, v, \Delta v) = a \left[1 - \left(\frac{v}{v_0} \right)^{\delta} - \left(\frac{s^*(v, \Delta v)}{s} \right) \right] \quad (1)$$

$$s^*(v, \Delta v) = s_0 + \max \left(0, vT + \frac{v \Delta v}{2\sqrt{ab}} \right) \quad (2)$$

Equation 1 calculates the acceleration value based on a maximum acceleration constant a, to the acceleration exponent δ, the current and desired velocities (v and v_0, respectively) and the current and desired distance to the follower (s and $s^*(v, \Delta v)$, respectively).

Table 1 shows some typical values, obtained from domain experts, for cars and trucks, which can be used in conjunction with the IDM equation (Equation 1).

Parameter	Description	Car	Truck
v_0	Desired speed	120 km/h	80 km/h
δ	Free acceleration exponent	4	4
T	Desired time gap	1.5 s	1.7 s
s_0	Jam distance	2.0 m	2.0 m
a	Maximum acceleration	3.0 m/s^2	3.0 m/s^2
b	Desired deceleration	3.0 m/s^2	2.0 m/s^2

TABLE 1: Sensible values for IDM parameters

These parameters are further elaborated to model different traffic situations. For instance, trucks are characterised by low values for v_0, a and b. Careful drivers have higher values for the time headway T. Otherwise, aggressive drivers have a low time headway T and higher values for v_0, a and b.

2.2. V2V Communication

In the communication architecture that we use, each car communicates with the leader and the one in front of it using CAS. This assumption is justified by the particular function we studied in collaboration with design engineers. For this particular function, this assumption allows for each car to learn about the leader's manoeuvres soon after they happen and anticipate them before they are fully propagated through to the convoy.

In our model, packet collision due the channel congestion is the only modelled source of packet loss. Propagation related losses are not taken into consideration. We conjecture that the results will be similar if we consider propagation loss and plan to verify this conjecture in our future experiments. Furthermore, we assume the communication range to be of 60 meters of the leader vehicle.

We designed a model of the CAS standard [3] in the Matlab environment; we dedicate the remainder of this section to the a brief overview of this model, particularly regarding the Facilities- and Network (Datalink) layers.

2.2.1. Facilities Layer: ETSI EN 302 637-2. Our Facilities Layer vehicle-to-vehicle communication protocol is modelled based on the ETSI standard EN 302 637-2. The process of triggering CAMs is controlled by the CAS [3] and is described below.

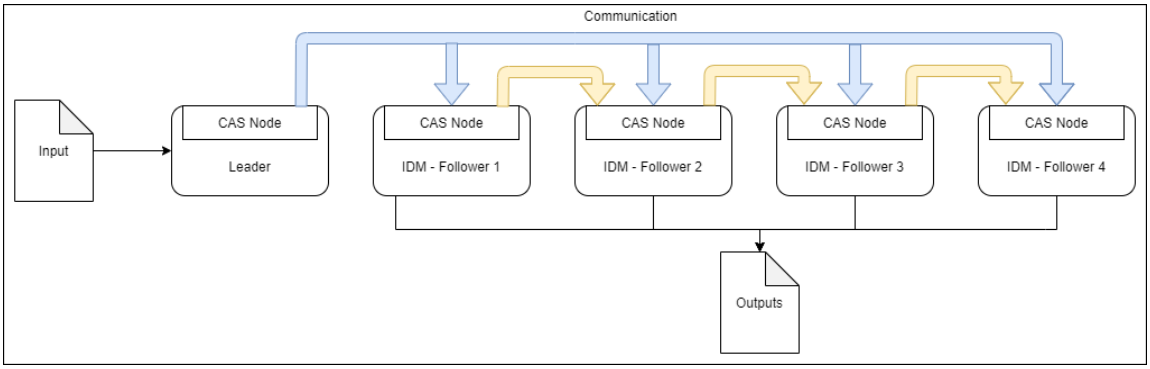


Figure 1: Overall Model Architecture

The range of the frequency of CAMs transmission are set as follows.

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

Within these limits, the CAM generation can vary depending on the vehicle's dynamics and the channel congestion status. The vehicle continuously check the variation of its current speed, coordinates and direction from the measurements that have been collected since the last triggered CAM.

The CAM is generated if one of these conditions (A or B) is satisfied:

A) The CAM shall be triggered if one of the following vehicle dynamics related conditions is given:

- The absolute difference between the current position of the vehicle and its position included in the previous CAM exceeds $d_{\min}$ = 4 m;
- The absolute difference between the current speed and the speed included in the previous CAM exceeds $v_{\min}$ = 0.5 m/s;
- The absolute difference between the current direction of the vehicle and the direction included in the previous CAM exceeds $a_{\min} = 4°$.

B) The CAM shall be triggered if the time elapsed since the last CAM generation is greater than or equal to $T_{\max}$.

The CAM transmissions occur on a dedicated ITS-G5 channel and is in accordance to CAS specification.

2.2.2. Network Layer: IEEE 802.11p CSMA/CA. As it is customary, there is a IEEE 802.11p protocol stack supporting Cooperative Awareness Services; in particular, there is a CSMA/CA scheme for managing the carrier at the Medium Access Control (MAC) sub-layer. We model this layer as it has a significant effect in our test-case generation process and the analysis of network congestion.

2.2.3. Lab package. The model and the data from our experiments are available publicly under an open source license for all purposes at https://github.com/hlsa/HyConf. The vehicles contains a CAS node for communication which is responsible for the CAM transmission. This component makes use of the CSMA/CA protocol.

3. Analysis Technique

In this section, we explain our analysis technique that explores the model and generates test inputs that push the system to its limits.

As explained in Section 2, we use the driving manoeuvres of the leading vehicle as the main input to the model. Since this input-space is inherently infinite, we need to cover it by finding inputs that are:

1) diverse enough to cover the input-space,
2) covers the models of vehicle control and V2V communication protocol, and
3) effective enough to exercise the limits of the system and maximise the possibility and severity of hazards (including collisions and convoy splits).

Defining these objectives reduces our test-case generation technique to a multi-objective optimisation problem. To this end, we use and adapt HyConf [2], which is a tool developed for conformance testing of cyber-physical systems. HyConf implements two classes of search algorithms for test-case generation: Simulated Annealing and Genetic Algorithms, which are well established probabilistic algorithms for computing global optima [4], [8].

Given an objective function f such search algorithms attempt to approximate the global maxima or minima of f by using various heuristics. However, their heuristic nature brings a certain degree of imprecision; this is mitigated by adjusting the parameters to balance accuracy and performance.

The search-based heuristics described in our past work [2] attempt to maximise 3 criteria in its strategy: 1) maximising the distance between the reference output function and that of the system under test, 2) discrete state coverage for the reference model, and 3) a diversity notion to generate

inputs that are sufficiently different from the test suite generated so far.

However, we have made some modification to the search strategy to work with our CAV model. In the present study, we use the following objectives: 1) hazard likelihood, 2) data age, and 3) diversity.

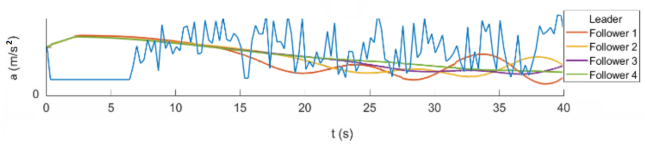
For that, the user provides a specification model and an ideal safe target that can be interpreted as a requirements specification. The requirement specification is an idealised and simplified input/output model for the vehicle convoy. In this case, the ideal follower vehicle is one that receives the acceleration input instantaneously from the leader and follows it perfectly, disregarding any kinematics in IDM or V2V communications altogether. In summary, it follows the requirement to instantaneously match the exact acceleration of the lead vehicle. By forcing our search to deviate from this ideal behaviour as much as possible, we push the convoy towards hazardous situations. This is the first search objective.

As for the second objective, we would like to maximise data age in the model. In other words, the inputs generated by our strategy, i.e., the leader acceleration pattern, aims to maximise data age in the communication protocol, which could in turn lead to hazardous behaviour.

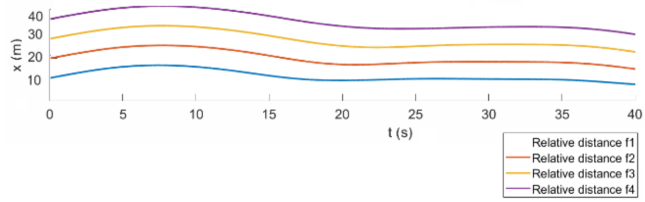
Finally, in order to cover as many different situations as possible, we have also built in a notion of diversity as our third objective: once an effective scenarios is generated, the next scenario is sought to be be as far apart as possible from the previously generated ones and cover the different areas of the input space.

Thus, we have built an ideal model of a following vehicle that behaves perfectly. We use this model only to generate inputs. Subsequently, we built more realistic models of the follower that triggers CAMs, which uses an abstract communication protocol based on ETSI ITS-G5 standard for inter-vehicular communication [6]. This model takes packet collisions and communication delays of CSMA/CA protocol into account.

Figure 2 shows examples of inputs and outputs generated by our strategy. The blue, erratic, line on Figure 2a is the leading car acceleration obtained by the search algorithm. The other, smoother, trajectories are the followers trying to keep up. Figure 2b shows the relative distance of each follower compared to the leading car.



(a) Input generated by the search heuristic.



(b) Ouput yielded by the input

Figure 2: Model input and outputs.

4. Experiment design

In this section, we give a detailed description of our experiment design. In Section 4.1, we present our research questions. In Section 4.2, we describe the steps that were carried out in the experiment. Finally, in Section 4.3 we detail the hypotheses and metrics that we collect to answer the research questions.

4.1. Research questions

The main goal of this study is the evaluation of the ITS-G5 Cooperative Awareness Basic Service according ETSI EN 302 637-2 standard; we develop an automated way of exploring the design-space regarding the frequency rules in the ETSI standard and evaluate how the awareness services fare in our model. Thus, we assess whether it is possible to find instances of hazardous behaviour in our model when we apply our search-based strategy. In summary, we make use of different sets of parameters of packets generation (the default recommended by ETSI and the ones we built ourselves) and analyse how they fare against inputs that aim to create hazardous situations and communication issues. In summary, we aim to answer the following research questions (RQs):

- **RQ1:** Is it possible to find hazardous behaviours caused by communication issues in scenarios abiding by the ETSI EN 302 637-2 standard?
- **RQ2:** Do the default parameter values described in the ETSI EN 302 637-2 protocol handle extreme situations better than other sets of values?

The hazardous behaviour that we are looking for are longitudinal distance deviation related to data age. In other words, we search for scenarios in which the vehicles in the platoon get too close or too far apart from each other due to outdated information; the former type of deviation is certainly more interesting from the safety analysis viewpoint.

4.2. Experiment methodology

To answer the research questions, we have identified the design-space parameters in the communication protocol and in our model that can affect the frequency of CAM transmission. Then, we have defined different sets of value for theses parameters; they will be compared against the default values specified in the ETSI standard.

For the communication protocol, the identified parameters are $T_{\min}$, $T_{\max}$, $d_{\min}$, and $v_{\min}$. The first two, i.e., $T_{\min}$ and $T_{\max}$, respectively represent the minimum and maximum time difference allowed by the standard for CAM packet transmission. The parameters $d_{\min}$, and $v_{\min}$ are related to the vehicles and they determine that a packet

should be sent whenever the difference in speed or distance, respectively, since the last sent packet, is greater than these values. The parameter sets are detailed in Table 2.

	$T_{\min}$	$T_{\max}$	$d_{\min}$	$v_{\min}$
Default	100	1000	4	0.5
Increased Frequency 1	50	500	2	0.25
Increased Frequency 2	75	750	3	0.425
Decreased Frequency 1	125	1250	5	0.625
Decreased Frequency 2	150	1500	6	0.75

TABLE 2: ETSI 302 637-2 CAM triggering parameters

Besides the default parameters shown in the first row of Table 2, we have defined an additional 4 sets of parameter values, depicted in rows 2 to 5. The values have been set in such a way to increase or decrease the frequency of the messages sent. Increasing or decreasing packet transmission frequency directly affects data age. Lower frequencies usually result in higher data age, however, higher frequencies can lead to packet collision, which increases data age as well.

As for IDM parameters, we consider *maximum acceleration* and *maximum deceleration*. What we show is that the communication parameters yield better or worse results depending on the maximum allowed acceleration and deceleration. The chosen values for the profiles are shown in Table 3.

Decel / Accel	-1 m/s^2	-5 m/s^2
1 m/s^2	Profile A	Profile B
3 m/s^2	Profile C	Profile D

TABLE 3: IDM maximum acceleration and deceleration profiles

The steps of the experiment are detailed as follows. First, we apply a Cartesian product of the parameters, ETSI (Table 2) $\times$ IDM (Table 3), to construct several different environment pre-conditions. Then, we make use of the search-based strategy presented in Section 3 to generate our input scenarios. Finally, we feed the inputs to our model and simulate it using the different sets of pre-conditions.

We next provide the details of the collected metrics and the hypothesis statements. During the simulation, we have collected the required data that was used to compute such metrics. Then, we have performed an statistical analysis to evaluate this data. Proven their significance, we answer the research questions via hypothesis acceptance/rejection.

4.3. Metrics and Hypotheses

In each execution, we collected the following metrics: average data age (ADA), maximum data age (MDA), minimum distance, maximum distance. Average data age tells us how outdated, on average, is the current information when a new packet is received. Maximum data age is the metric that tells us what is the longest time any car in the platooning has spent without having received any new packet.

Minimum and maximum distance are the closest and farthest the cars have gotten to one another; minimum distance is used to identify collisions and maximum distance is used to identify vehicles going outside communication range. Based on these metrics we can decide whether a faulty behaviour occurred, i.e., whether the vehicles get too close to-, or too far from each other.

Hypotheses A and B aim to evaluate the research questions that have been explained previously and are defined below.

- Hypothesis A

$$H_{A0} : FB_{DEF} = 0$$
$$H_{A1} : FB_{DEF} > 0$$

- Hypothesis B

$$H_{B0} : ADA_{DEF} \leq ADA_{OTH}$$
$$H_{B1} : ADA_{DEF} > ADA_{OTH}$$

Hypothesis A0 states that the number of faulty behaviours (FB) using the default parameter values (DEF) dictated by the ETSI EN 302 637-2 standard is zero. This experiment aims to reject such a hypothesis. Thus, an alternate hypothesis A1 is also defined, which has a complementary role to the null hypothesis, and can be accepted in case its counterpart hypothesis is rejected. The alternate one states that the number of faulty behaviours (FB) is greater than zero. These hypothesis will be used to answer **RQ1**.

Similarly, to answer **RQ2**, we have defined the hypotheses B0 and B1. Their goal is to compare the average data age (ADA) using default (DEF) and other parameter values (OTH). The null hypothesis, B0, states that average data age is lesser or equals to average data age when using the default values; the alternate hypothesis states the opposite.

5. Results and analysis

5.1. Results

For each pair of parameters (ETSI $\times$ IDM), we have run the experiment 50 times for statistical significance and analysed the outcome. The experiment was carried out using a computer equipped with an Intel Core i7 processor, 16GB of RAM, Windows 10 Operating System and the Matlab 2018b Framework. The platooning model used is the one presented in Section 2. The results, along with the threats to their validity, are detailed as follows.

For each IDM profile shown in Table 3 (Profiles A - D), we have grouped the 10 execution for each set of parameter pairs in Table 2 (Default values, as well as Increased and Decreased Frequency, respectively denoted by IF1, IF2, DF1 and DF2). The average data age (A.D.A) and maximum data age (M.D.A.) are shown in seconds and the minimum and maximum distance, in meters. A collision is detected when the minimum distance reaches 0 meters and we also consider distances larger than 15 meters to be faulty behaviour; we assume the followers must stay within 15 meters of the other vehicles, otherwise, there is a risk of the last vehicle(s) leaving the communication range and leading to a convoy split.

		A.D.A.	M.D.A.	Min. Dist.	Max. Dist.	Collision	Too far
Profile A	Default	0.38 s	0.79 s	4 m	6 m	No	No
	IF 1	0.42 s	0.48 s	4 m	8 m	No	No
	IF 2	0.67 s	1.02 s	2 m	6 m	No	No
	DF 1	0.41 s	0.91 s	6 m	9 m	No	No
	DF 2	0.49 s	1.01 s	7 m	11 m	No	No
Profile B	Default	0.61 s	1.08 s	4 m	16 m	No	Yes
	IF 1	0.59 s	1.12 s	3 m	15 m	No	Yes
	IF 2	0.64 s	1.36 s	6 m	17 m	No	Yes
	DF 1	0.41 s	0.95 s	4 m	11 m	No	No
	DF 2	0.89 s	1.62 s	4 m	16 m	No	Yes
Profile C	Default	0.46 s	0.87 s	1 m	8 m	No	No
	IF 1	0.47 s	0.99 s	4 m	11 m	No	No
	IF 2	0.73 s	1.18 s	4 m	15 m	No	Yes
	DF 1	0.39 s	0.85 s	3 m	7 m	No	No
	DF 2	0.52 s	1.52 s	0 m	9 m	Yes	No
Profile D	Default	0.65 s	1.18 s	0 m	8 m	Yes	No
	IF 1	0.67 s	1.02 s	2 m	6 m	No	No
	IF 2	0.72 s	1.52 s	0 m	6 m	Yes	No
	DF 1	0.71 s	1.19 s	0 m	4 m	Yes	No
	DF 2	0.89 s	1.81 s	0 m	6 m	Yes	Yes

TABLE 4: Experiment results

Finally, it is important to note that we have analysed the effects of using additional (up to ten) followers in the platooning; however, we have found that the difference in results, compared to four followers, was not statistically significant. Thus, we have decided to focus the experiment on a more realistic, smaller, number of followers. The results obtained when using one leader and four followers are shown in Table 4.

What the results show is that with high acceleration and high deceleration, such as in Profile D, there is a risk of collision. However, if the acceleration is high and the deceleration is low (Profile C), then there is the risk that the cars can get too far from each other.

Faulty behaviours were found in Profiles A and B using the default parameters. This results allow us to reject hypothesis A0 and accept its alternative, hypothesis A1. Therefore, the answer to the first research question, **RQ1**, is a positive one: we were able to find hazardous behaviour due to communication issues, in scenarios that follow the ETSI EN 302 637-2 standard.

To answer the second research question, **RQ2**, we have performed a statistical analysis on the average data age (A.D.A.) collected. We have used the "students t-test" [12] statistical technique with a p-value < 0.05 and level of confidence of 95% on the data. The results are shown in Table 5 and values above 0.05 means that, on average, the default values perform better than the alternative ones that we have defined. Therefore we cannot reject the null hypothesis B0.

	P-Value
Default v. IF 1	0.07
Default v. IF 2	0.25
Default v. DF 1	0.09
Default v. DF 2	0.22

TABLE 5: Test results (p-values)

It is evident from results that using the current default configuration can still yield undesired outcomes. We found scenarios in which different parameters resulted in less severe hazards. To maximise the benefit of different parameter sets, we can recommend to change the ETSI protocol parameters dynamically, taking in consideration the data age and (observed as well as predicted) input scenarios.

5.2. Threats to validity

What follows are the threats to experiment validity. This study only considers a relatively small example. Our platooning uses a simple kinematics model, Intelligent Driver Model, to control its behaviour, which makes it harder to generalise the outcome of this experiment. However, this allows us to isolate and focus on the communication issues, which is the goal of this study. Furthermore, it is possible that a sufficiently large number of vehicles or two-way communication would affect packet collision, and therefore, data age. We have not analysed the effects that different network architectures have on the data age, however, as for the numbers of vehicles, we have analysed up to 10 followers without any significant difference in results. Finally, the parameter values we have chosen in Tables 3 and 2 have a direct impact on the results. The values we have chosen are based on prior experiments and domain knowledge.

6. Related Work

Analysing V2V connectivity is a multi-disciplinary problem and typically involves expertise and methods from a number of areas. With respect to safety analysis through validation and verification, Meinke [7] uses Learning-Based Testing to learn models of a connected platoon while testing them against safety and fuel efficiency properties. Compared to the models used and learned by Meinke, we use a much more detailed model of the ITS-G5 protocol and use them for a quantitative analysis of the design decision trade-offs

and search for effective test cases revealing the extreme cases in such trade-offs.

As for simulation tools, some have been extended and adopted to analyse various properties of CAMs transmission, particularly in the context of connected autnomous driving. For example, the Sumo simulator has been extended with platooning concepts [10] and this extension has been used to analyse connectivity in platoons [9]. Furthermore, work on safety measures for connected autonomous driving has been conducted by Sidorenko [11]. Common to our approach, this work provides a model of V2V communications protocols with the goal to adjust vehicular distance (saving fuel and space) without compromising safety in emergency braking scenarios. Our work, however, automatically generates inputs that assess the safety of such protocols at its limits, via a search-based approach.

Thus, our novel contribution is the integration of search-based testing and model-based testing in analysing cooperative awareness service in CAV models and using these techniques for design-space exploration. Apart from the work by Meinke [7], another piece of research that uses similar principles is the work by Kamali et al. [5]. They use timed-automata-based models to analyse properties of platoons. Their approach uses formal verification for analysing protocols, rather than model-based testing. The strength of our approach is in scalability, we do not rely on state-space exploration, but rather use search-based techniques to locally search the state-space and steer the test-case generation process towards test-cases that are likely to reveal possible safety hazards.

7. Conclusions and future work

In this paper, we presented an automated and rigorous analysis method for automated vehicle functions and applied it to cooperative awareness services in CAV. Our method uses an integration of model-based and search-based testing on a model that we have developed for connected autonomous driving.

Our model uses the Intelligent Driver Model kinematics as well as the ITS-G5 inter-vehicular communication according to the ETSI EN 302 637- 2 standard for Cooperative Awareness Basic Services. These services operate on top of IEEE 802.11p, a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol. The standard allows for optimised implementations by specifying minimum and maximum packet transmission frequencies.

The main contribution of this work is the analysis method to check how our model fares in conjunction with the ETSI standard. For that, we have conducted a controlled experiment to compare the default parameters against alternatives values. In order to generate inputs for continuous systems, a search-based approach is used: we formulate a multi-objective search problem that maximises hazard likelihood, data age as well as coverage of the input space via diversity of test inputs. Our approach automatically generates test inputs that can yield hazardous situations while abiding by the standard.

Our ongoing research in this area involves a number of extensions of the present paper. First of all, we would like to add a notion of "drivability" to our test-cases to make sure that the generated test-cases represent reasonable driving scenarios. Moreover, our results indicate that a dynamic choice of parameters may lead to mitigating the discovered hazards. Hence, we would like to develop such a dynamic and adaptive scheme whereby the observed and predicted input scenarios are matched against the patterns detected during the analysis and the most appropriate set of parameters are accordingly chosen. An analysis of this adaptive scheme against static schemes will be our subsequent step.

Acknowledgments

This work was supported in part by the Knowledge Foundation in the framework of SafeSmart "Safety of Connected Intelligent Vehicles in Smart Cities" Synergy Project (2019–2023), in part by the Swedish Foundation for Strategic Research in the framework of Strategic Mobility Program (2019–2020) and the ELLIIT Strategic Research Network.

References

[1] Hugo Araujo, Gustavo Carvalho, Morteza Mohaqeqi, Mohammad Reza Mousavi, and Augusto Sampaio. Sound conformance testing for cyber-physical systems: Theory and implementation. *Science of Computer Programming*, 162:35–54, 2018.

[2] Hugo Araujo, Gustavo Carvalho, Mohammad Mousavi, and Augusto Sampaio. Multi-objective search for effective testing of cyber-physical systems. In *Proceedginds of the 17th International Conference on Software Enginnering and Formal Methods*. Springer, 2019.

[3] ETSI EN 302 637- 2; intelligent transport systems (its); vehicular communications; basic set of applications; part 2: Specification of cooperative awareness basic service. Standard, 2013.

[4] Saul B Gelfand and Sanjoy K Mitter. Analysis of simulated annealing for optimization. In *Decision and Control, 1985 24th IEEE Conference on*, volume 24, pages 779–786. IEEE, 1985.

[5] Maryam Kamali, Louise A Dennis, Owen McAree, Michael Fisher, and Sandor M Veres. Formal verification of autonomous vehicle platooning. *Science of computer programming*, 148:88–106, 2017.

[6] Nikita Lyamin, Alexey Vinel, and Magnus Jonsson. Does etsi beaconing frequency control provide cooperative awareness? In *2015 IEEE International Conference on Communication Workshop (ICCW)*, pages 2393–2398. IEEE, 2015.

[7] Karl Meinke. Learning-based testing of cyber-physical systems-of-systems: A platooning study. In *Proceedings of EPEW 2017*, 2017.

[8] Melanie Mitchell. *An introduction to genetic algorithms*. MIT press, 1998.

[9] Michele Segata. *Safe and Efficient Communication Protocols for Platooning Control*. PhD thesis, Institute of Computer Science, 2016.

[10] Michele Segata. Platooning in SUMO: An open source implementation. In *SUMO User Conference 2017*, pages 51–62, 2017.

[11] Galina Sidorenko, Johan Thunberg, Katrin Sjoberg, and Alexey Vinel. Vehicle-to-vehicle communication for safe and fuel-efficient platooning. In *2020 IEEE Intelligent Vehicles Symposium, IV 2020*. IEEE, 2020.

[12] Student. The probable error of a mean. *Biometrika*, pages 1–25, 1908.

[13] Martin Treiber, Ansgar Hennecke, and Dirk Helbing. Congested traffic states in empirical observations and microscopic simulations. *Physical review E*, 62(2):1805, 2000.