A Simulation-Based Security Benchmarking Approach for Assessing Cooperative Driving Automation (CDA) Applications

Mateen Malik[1,2(✉)], Behrooz Sangchoolie[1], and Johan Karlsson[2]

[1] Dependable Transport Systems, RISE Research Institutes of Sweden, Gothenburg, Sweden
{mateen.malik,behrooz.sangchoolie}@ri.se
[2] Chalmers University of Technology, Gothenburg, Sweden
{mateenma,johan}@chalmers.se

Abstract. This paper presents our initial contributions toward defining security benchmarks for simulation-based assessment of Cooperative Driving Automation (CDA) applications. A security benchmark is a process or procedure for assessing and validating a system's ability to achieve its operational objectives in the presence of specific security attacks. This work lays the groundwork for developing security benchmarks that assess the robustness of CDA applications against jamming attacks. The *driving scenario* and the *attack model* are the core components of our proposed security benchmark. We used two scenarios *braking* and *sinusoidal* as a stimulus for evaluating the robustness of a platooning application modeled in a simulation framework called Plexe. The platooning application is equipped with a Cooperative Adaptive Cruise Control (CACC) controller. We injected *barrage* jamming attacks into the physical layer of the wireless communication system modeled by the IEEE 802.11p protocol. We demonstrate that jamming attacks can compromise safety, leading to emergency braking and collision incidents among platooning vehicles. Our findings also indicate that the severity of jamming attacks varies with the driving scenario, with the most severe impacts (i.e., collisions) occurring when the attack is injected during vehicle acceleration.

Keywords: Security benchmarks · Cooperative Driving Automation (CDA) · Simulation-based jamming attacks · Platooning system

1 Introduction

Today's road vehicles have transformed into complex interconnected cyber-physical systems, unlocking new possibilities for improved safety, fuel efficiency, driver assistance, and passenger convenience. The advent of vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) communication technology provides an

A. Kocian et al. (Eds.): INTSYS 2024, LNICST 608, pp. 244–262, 2025.
https://doi.org/10.1007/978-3-031-86370-7_15

important and necessary step towards the introduction of cooperative driving automation (CDA) [1] technologies. Although CDA is expected to increase the safety, efficiency, and reliability of automated automotive transportation systems, more research is needed to tackle the safety and security concerns that naturally occur for systems that depend on sensor data received via a wireless network.

Ensuring that a cooperative driving application is adequately protected against potential security threats is a challenging and costly task that involves many work-intensive activities [2,3]. In this paper, we address an important part of these activities: *simulation-based testing of a cooperative system's ability to cope with security attacks directed toward its wireless communication channel.*

Due to the high cost of proving ground testing and field operational tests, simulation has become the preferred method to study and validate system properties of advanced driver assistance systems (ADAS) [4] and cooperative driving applications such as platooning [5,6]. The work presented in this paper explicitly addresses simulation-based testing of a cooperative system's resilience against *barrage jamming* attacks directed toward the physical layer of the wireless communication system.

Jamming attacks constitute an important class of security threats since they are relatively easy to implement and carry out. The widespread availability of software-defined radio technology [7,8] has enabled the implementation of new types of "intelligent" jamming attacks without costly investments in expensive equipment. Jamming also requires limited knowledge about the targeted system beyond the protocol specifications for the wireless network, which normally are publicly available in open standardization documents. Relevant standards include IEEE 802.11p [9] and C-V2X [10].

This paper introduces and demonstrates a *barrage jamming* attack model for simulations. Barrage jamming is a brute-force approach in which the adversary sends noise-like energy over a broad spectrum of frequencies to block the legitimate signal. According to Lichtman et al., [11], barrage jamming can be classified as *time-uncorrelated* and *protocol-unaware*. This means that barrage jamming is uncorrelated in time concerning the targeted signal and requires no detailed information about the communication protocol. Hence, it is easy to implement and execute.

The work presented in this paper is intended as an initial contribution towards a definition of *security benchmarks* for simulation-based assessment of CDA applications concerning their ability to operate safely in the presence of jamming attacks. A security benchmark is a process or procedure for assessing, validating, or testing a system's ability to achieve its operational objectives in the presence of a given set of security attacks[1]. Work on benchmarks for assessing, testing, and evaluating essential system properties has a history of several decades. Examples include benchmarks for computing performance [12], transaction processing [13,14], dependability [15], and security [16]. In the field

[1] The terms security benchmark and security benchmarking are also used in other contexts, e.g., in the security rating of organizations.

of intelligent transportation systems, several papers have addressed simulation-based assessment of the resilience against security attacks for CDA systems, mainly for platooning systems [2,3,17–20]. However, only a few of these papers deal specifically with jamming attacks [20–23] and to the best of our knowledge, no previous paper has discussed the idea of defining security benchmarks, for simulation-based assessment of CDA applications.

To allow a simple and constructive exchange of benchmark definitions and results, we have implemented our attack models in a tool called ComFASE[2], which utilizes well-known and widely used simulation frameworks including Plexe [6], and Veins [24]. We simulate barrage jamming attacks against a platooning system consisting of four vehicles that use a cooperative adaptive cruise controller (CACC) model developed by Segata et al.[3] [6]. We consider two driving scenarios, the *sinusoidal* and *braking* scenarios available in the Plexe framework. In summary, the paper makes the following contributions:

1. A comprehensive study of the impact of barrage jamming attacks on a platooning system equipped with a CACC algorithm developed by Segata et al. [6] using two driving scenarios: *sinusoidal* and *braking*.
2. A detailed analysis of the impact of the parameters of the attack model, including 'attack start time', 'attack duration', and 'attack value', on the outcome of the simulation results.
3. A conceptual discussion and proposals for the future development of security benchmarks for platooning and other CDA systems.

2 Background

2.1 Platooning Application

Platooning is a cooperative driving technology in which a group of vehicles, known as a platoon, travels closely together at high speeds, maintaining a small distance between each other. The vehicles in a platoon are equipped with advanced communication systems and cooperative adaptive cruise controllers that allow them to share information and coordinate their movements.

In the CACC controller investigated in this paper, each vehicle receives information from the lead vehicle and the preceding vehicle in the platoon via the wireless network. This information includes the controller's desired acceleration, the vehicle's actual acceleration, speed, position, and the time at which the data has been measured. Further details about setting the controller parameters, such as engine and driver parameters, can be found in the API section of the Plexe webpage [26].

[2] The ComFASE tool has been developed in our research group and is available for download at [27].

[3] In addition to this controller, another three controllers are included in the Plexe simulation environment:'Flatbed' [29], 'Ploeg' [30], and 'Consensus' [31].

2.2 ComFASE: A Fault and Attack Injection Tool

ComFASE [27,32] is an open-source simulation-based fault and attack injection tool built on top of Veins, a network simulation framework [24]. ComFASE injects attacks on the IEEE 802.11p physical layer model in Veins. Moreover, various types of jamming attacks can be modeled in ComFASE, such as *delay attacks*, *denial-of-service (DoS) attacks* [32], *barrage jamming*, *deceptive* and *destructive interference* [28]. The simulation frameworks that are utilized by the ComFASE simulation environment are *(i)* OMNeT++ *v. 5.6.2* (a network simulator) [33], *(ii)* Veins *v. 5.1* (a vehicular network simulator) to simulate the V2V communication [24], *(iii)* SUMO *v. 1.9.2* (a traffic simulator) to design, simulate traffic, and study traffic behavior [34] and *(iv)* Plexe *v. 3.0a2* (a cooperative driving framework) that enables realistic platooning application simulation [6].

Barrage Jamming Attack Modeling in ComFASE. *Barrage jamming* is a physical layer attack where an attacker continuously transmits noise-like energy across the entire frequency spectrum of the communication channels [35] to reduce the quality of the legitimate signal in terms of Signal to Interference & Noise Ratio (SINR). *Barrage jamming* attacks are categorized as *non-protocol aware jamming* [11] since the attacker does not require any prior in-depth knowledge about the communication protocol to be able to conduct the attacks.

In ComFASE, we model the impact of *barrage jamming* by manipulating the 'noise power' parameter originally used for SINR calculations in the Veins simulator. The noise power parameter is used to model the impact of various sources of *noise* that can affect the received signal, such as channel noise. Our *barrage jamming* attack model targets a broad range of frequencies and simultaneously affects the sending and receiving capabilities of the platooning vehicles. We considered the impact of uniform noise power across all frequencies in a given frequency spectrum, which can be used to model white and broadband noises.

Our model for *barrage jamming* attacks involves injecting equal amounts of noise into all vehicles within a platoon simultaneously. However, the effect of this noise differs among the vehicles due to variations in legitimate signal strength, which is influenced by the distance from each vehicle to the lead vehicle. As a result, the noise can lead to asymmetrical message losses, impacting the communication effectiveness within the platoon. Asymmetric message losses refer to an unequal loss of messages across different vehicles. The distance between each vehicle and the platoon leader varies, leading to differences in how effectively the jamming noise disrupts communication. Apart from distance, other factors, such as interference level, impact the signal strength and could cause asymmetric message losses.

2.3 Related Work

Security Benchmarks. Researchers have proposed security benchmarking frameworks for various cybersecurity domains. Oliveira et al. [16] introduced a

two-phase benchmarking framework for web service frameworks (WSFs), focusing on security qualification and trustworthiness assessment. Similarly, Anisetti et al. [36] developed a security benchmark for assessing the security assurance of OpenStack, an open-source cloud infrastructure. Braun et al. also presented NETCARBENCH [37], a benchmark for assessing and comparing techniques and tools used to design in-vehicle communication networks. Despite these advancements, to the best of our knowledge, no previous work has focused on defining security benchmarks for simulation-based assessment of Cooperative Driving Automation (CDA) applications.

Jamming Techniques. Previous studies have explored various jamming techniques capable of partially or entirely disrupting wireless communication. Moser et al. [21] studied the impact of signal cancellation attacks against wireless communication systems such as GPS, where the attacker's signal interferes destructively with the legitimate signal. Mahal et al. [23] designed jammer to emulate the effects of jamming and nulling on the CP (Cyclic Prefix), which involves adding a copy of the end of a signal to the beginning of the signal. In these attacks, the attacker's objective is to partially or entirely cancel the legitimate signal frequency to cause a denial of service. Nulling or cancellation attacks are usually considered challenging and even infeasible to realize, as argued by Lichtman et al. [11]. Clancy et al. studied the performance of wireless transmission under jamming attacks, i.e., *pilot jamming* and *pilot nulling* [22]. Pilot symbols are inserted at specific subcarriers or time slots and help the receiver estimate the channel's frequency response to carry out synchronization and equalization. Our study assesses the impact of barrage jamming, which covers a broader frequency range than other types of jamming, such as pilot jamming and nulling.

Impact of Jamming Attacks on Platoons. Several previous studies have investigated the consequences of jamming attacks on platooning systems. Hu et al. [38] studied the impact of jamming attacks on platoon stability. They used software-defined radios and the Plexe simulator to demonstrate the feasibility of their attacks. Segata et al. [17] simulate jamming attacks using the Plexe simulation framework to demonstrate the effectiveness of fallback and recovery mechanisms that mitigate the impact of communication failures in cooperative driving applications. Van der Heijden et al. [3] proposed a general attack model which they used to evaluate the resilience of three cooperative cruise controllers implemented in Plexe. Alipour-Fanid et al. [5,19] injected jamming attacks in a simulation model of the IEEE 802.11*p* communication protocol where the string stability and the safety of the CACC controller model is evaluated.

What distinguishes our work from the others presented in this section is the way we modeled jamming attacks. We implemented a more detailed barrage jamming attack model featuring asymmetric message losses. Additionally, the granularity of the attack parameter values in our test campaigns is significantly higher; the step size of our attack model parameters is considerably smaller than those used in comparable studies.

3 Security Benchmarking

In this section, we present the details of our proposed framework for security benchmarking to evaluate the resilience of CDA applications against jamming attacks. We define a security benchmark as a well-defined procedure for assessing, validating, or testing a system's ability to achieve its operational objectives in the presence of a given set of security attacks. This work addresses security benchmarking conducted using simulations where the system under test is subjected to jamming attacks.

In general, the primary motivation for defining benchmarks for computer-based systems is to provide a widely accepted and easy-to-use procedure for evaluating or comparing system implementations, components, or design solutions. When it comes to basic concepts and main objectives, security benchmarking is akin to the closely related field of dependability benchmarking. In their work on dependability benchmarking, Kanoun et al. [39] identified "the main dimensions that are decisive for defining dependability benchmarks and the way experimentation can be conducted in practice". They are *(i)* the target system and benchmarking context, *(ii)* the measures to be evaluated, and *(iii)* the experimental conditions. We believe that these dimensions are also applicable to security benchmarking. Kanoun et al. [39] also give examples of properties that a benchmark must achieve to be successful, such as *repeatability* (at least in statistical terms), *representativeness*, *portability*, and *cost-effectiveness*.

Benchmarking has proven to be pivotal for advancing the state of the art in some fields of computer engineering, such as computer architecture [40]. However, defining a benchmark, or a benchmark suite, is a challenging undertaking that requires involvement and interaction among many groups of researchers, developers, and other stakeholders in the field of interest. Since security benchmarking is a novel topic in the context of CDA systems, we would like to emphasize that our benchmarks are intended as tentative examples of how security benchmarks for assessing the resilience of a CDA system against jamming attacks could be defined. They are not intended as final solutions but rather as a starting point for a wider effort to develop security benchmarks for CDA systems, including benchmarks for other types of security attacks than jamming attacks. In the remainder of this section we discuss the main elements of our benchmarking framework.

3.1 Driving Scenario

A driving scenario comprises specific driving conditions and parameters. The driving scenario includes road and traffic conditions, vehicle driving behavior, and their interaction. Our security benchmarks are based on *sinusoidal* and *braking* scenarios, available in Plexe.

These parameters, as well as the values selected for them, are detailed in Sect. 4.2. The sinusoidal scenario simulates an extreme driving condition and is ideal for testing a platoon's string stability. In contrast, the braking scenario is more representative of real-world situations. Additionally, for both scenarios,

a single lane on a highway with no elevation or friction is considered, and no incoming traffic or vehicles that are not a part of the platoon are considered. To further develop our proposed security benchmarking, exploring additional scenarios that reflect real-world traffic conditions would be valuable. This would offer a better evaluation of the system's resilience against the jamming attacks.

3.2 Attack Model

Selecting an appropriate attack model is critical for security benchmarking of CDA applications because it defines the type, scope, and severity of potential jamming attacks. An accurate attack model simulates real-world threats, providing insights into vulnerabilities specific to vehicle communication protocols or decision-making systems.

We implemented a barrage jamming attack model for our proposed framework of security benchmarking. Selecting the attack model parameters that produce correct results is crucial. The key parameters of our attack model include attack duration, attack value, and attack start time. In Sects. 4.1 and 4.2, we provide details about these parameters and the values selected for them.

3.3 Data Collection and Outcome Classification

A key action in creating a security benchmark is to specify the raw data that is to be collected during benchmark experiments. The raw data provides crucial information for understanding the CDA application's performance, safety, and security. It provides the foundational information to analyze vehicle behavior, assess system efficiency, and detect potential vulnerabilities. Key elements of data collection include vehicle performance data (speed, acceleration, braking), sensor data (cameras, radar, LiDAR, and other sensors that help the vehicle perceive its surroundings), communication data (data exchanged between vehicles and with infrastructure, environment data (road conditions, weather, and traffic patterns), and security data (logs of cyber events, anomalies, or intrusion attempts).

The raw data we collect from SUMO include information on vehicle speed, acceleration, deceleration, and collisions. This information can be used for the classification of the outcomes. We have specifically used vehicle acceleration and collision incidents to classify the outcomes.

3.4 Challenges

In this paper, we used two specific scenarios (i.e., *sinusoidal* and *braking*) as a stimulus for evaluating the platooning application equipped with the CACC controller. Other system components influencing the evaluation, such as the wireless communication model, wireless channel model, and the number of vehicles, are kept constant throughout the testing and evaluation process.

One of the primary challenges arises from the number of possible combinations that can be formed using the available system components, such as scenarios and attack models with their various configurations. The permutations of these combinations can be overwhelming, making it difficult to determine which elements should be tested together and how many combinations are necessary for a comprehensive evaluation. Moreover, simulations may not accurately represent all real-world conditions. Factors like unpredictable human behavior and weather conditions can introduce vulnerabilities that might not be captured in a simulated environment.

4 Experimental Setup

4.1 Attack Model

Our attack model for barrage jamming has been designed to enable a simple and constructive exchange of benchmark definitions and results. To this end, we use three basic parameters for the model: *attack start-time*, *attack duration*, and *attack value*. The attack start time defines the time when the attack starts on the timeline of the driving scenario. The attack duration defines the duration while the attack is active. Finally, the attack value defines the severity of the attack, i.e., the amount of noise injected into the communication channel.

To configure the attack injection campaigns, we vary the attack value (i.e., the noise signal power) from 0 to 1×10^{-5} mW, in steps of 0.01×10^{-5} mW, resulting in 100 experiments. We conducted tests that showed little or no difference in the results obtained for noise signal power values above 1×10^{-5} mW.

4.2 Driving Scenarios

We consider two driving scenarios in our simulations, the *sinusoidal scenario* and the *braking scenario*. These scenarios, which are available in Plexe, have been widely used by other researchers in simulation studies of platooning systems.

Sinusoidal Scenario. In this scenario, the vehicles follow a sinusoidal driving pattern where they periodically accelerate and decelerate with a frequency of 0.2 Hz and an amplitude of 5.0 km/h. The lead vehicle's maximum speed is set to 100 km/h. Using a total simulation time of 60 s (see Fig. 1), we vary the attack start time from 17.0 s to 21.8 s in increments of 0.2 s, resulting in 25 attack start times. The selected attack start times allow us to evaluate the vehicle's behavior under different situations (e.g., acceleration and deceleration). For each attack start time, we ran simulations with 30 attack durations ranging from 1 s to 30 s and 100 noise values. Thus, we conducted a total of 75000 (25 *attack start times**30 *attack end times**100 *attack values*) attack simulations for the sinusoidal scenario.

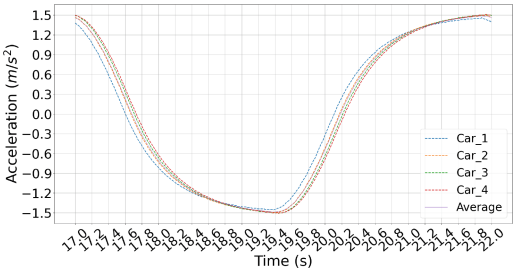


Fig. 1. Sinusoidal scenario: Acceleration profiles of all vehicles in the platoon.

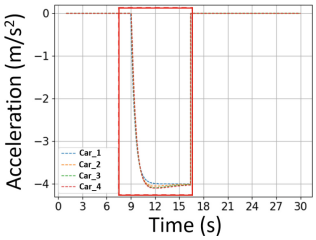


Fig. 2. Braking scenario: Deceleration profiles of all vehicles in the platoon. NB: the solid line marks the period in which the attack start times are selected.

Braking Scenario. In this scenario, the vehicles decelerate with 4 m/s^2 until a complete stop. In the first part of the scenario, the vehicles drive at a constant speed of 100 km/h. In the second part, which starts from 9 s, the vehicles brake until a complete stop.

Using a total simulation time of 30 s (see Fig. 2), we vary the attack start time from 7.0 s to 16.4 s in increments of 0.2 s, resulting in 48 cases. The selected attack start times allow us to evaluate the vehicle's behavior under different situations (e.g., constant speed and hard braking). For each attack start time, we ran simulations with 10 attack durations ranging from 1 s to 10 s and 100 noise values. Thus, we conducted a total of 48000 (48 *attack start times**10 *attack end times**100 *attack values*) attack simulations for the braking scenario.

4.3 Outcome Classification

To classify the outcomes of the simulations, we define four outcome categories based on the vehicles' deceleration profiles and collision events. These four categories are: ***Non-effective:*** The deceleration profiles of the vehicles in a attack simulation run are identical to the ones observed for the golden (attack-free) run. ***Negligible:*** The recorded maximum deceleration of the vehicles in the attack simulation run (RMD_{attack}) is less than or equal to the recorded maximum deceleration in the golden run (RMD_{golden}). ***Benign:*** The RMD_{attack} is greater than the RMD_{golden} and less than or equal to the 'maximum comfortable

Table 1. Test campaign results for sinusoidal (S1) and braking (B1) scenarios.

Campaign	Non-Effective	Negligible	Benign	Severe	Total
S1	3042 (4.0%)	5424 (7.2%)	30788 (41.0%)	35746 (47.8%)	75000
B1	9029 (18.8%)	25827 (53.8%)	2649 (5.5%)	10495 (21.9%)	48000

braking' value. ***Severe:*** RMD_{attack} is greater than the 'maximum comfortable braking' value, or a collision has occurred.

We selected the, RMD_{golden} to be 1.53 m/s^2 for the sinusoidal scenario, and 4.0 m/s^2 for the braking scenario, while the 'maximum comfortable braking' value for both scenarios was set to 5.0 m/s^2.

5 Experimental Results

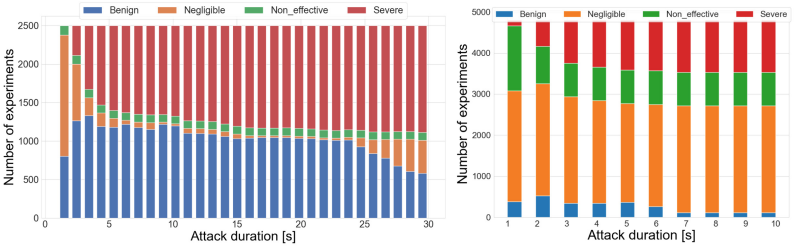
We conducted simulations with barrage jamming as described in Sect. 2.2 using the test setups for *sinusoidal* and the *braking* scenarios as presented in Sect. 4.2. The outcomes of these simulations are summarized in Table 1. As described in Sect. 4.3, the outcomes of the attack simulations are divided into four categories: non-effective, negligible, benign, and severe. Severe outcomes represent simulations resulting in collisions or emergency braking, while the other categories represent no to less significant consequences.

Table 1 shows that the outcomes vary considerably depending on the driving scenario. Notably, the severe outcomes are much more prevalent in the sinusoidal scenario than in the braking scenario. The sinusoidal scenario includes periods of acceleration and deceleration, while the braking scenario consists of periods of constant speed and deceleration. Our simulations revealed that collisions are more likely to occur if the attacks coincide with an acceleration period, which explains why severe outcomes are more prevalent in the sinusoidal scenario.

We conducted 75000 simulations in campaign **S1** and 48000 simulations in campaign **B1**. Figure 3 shows the outcomes for all simulations in campaigns S1 and B1, focusing on attack duration (Figs. 3a and 3b), attack start time (Figs. 3c and 3d), and attack (noise) value (Figs. 3e and 3f). Note that the classified results for each attack duration (see Figs. 3a and 3b) include all attack start time and noise value. Similarly, the classified results for each 'attack start time' (see Figs. 3c and 3d) include all attack duration and noise value. Finally, the classified results for each noise value (see Figs. 3e and 3f) include all attack duration and attack start time. We start our analysis by comparing the results presented in Figs. 3a (S1) and 3b (B1).

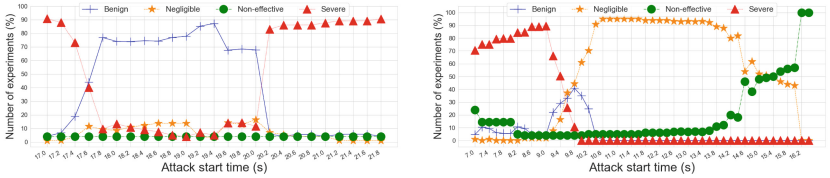
In **S1**, severe outcomes (indicated by the red bars) are the most prevalent category, comprising 47.8% of all simulations. These severe outcomes show an increasing trend as the attack duration extends. For attack durations longer than 15 s, severe outcomes account for over 50% of the total outcomes in S1.

The second-largest category of outcomes in S1 is benign outcomes (blue bars), which includes cases where the deceleration values fall between 1.53 m/s^2 and



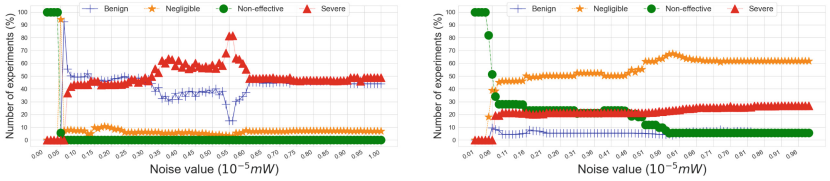
(a) Outcome distribution w.r.t. the attack duration in S1.

(b) Outcome distribution w.r.t. the attack duration in B1.



(c) Outcome distribution w.r.t the attack start times in S1.

(d) Outcome distribution w.r.t the attack start times in B1.



(e) Outcome distribution w.r.t. the noise values in S1.

(f) Outcome distribution w.r.t. the noise values chosen in B1.

Fig. 3. Outcome distribution for barrage jamming attacks on all vehicles for the sinusoidal and braking scenarios.

5.0 m/s^2, as described in Sect. 4.3. These benign outcomes make up 41.0% of the total outcomes in S1, and their percentage tends to decrease as the attack duration increases. Negligible outcomes (orange bars) account for 7.2% of the outcomes in S1. These outcomes are more prevalent for short attacks lasting less than 4 s and attacks lasting longer than 25 s. Non-effective outcomes (green bars) comprise approximately 4% of the outcomes in S1, and their distribution remains relatively consistent across all attack durations.

Turning to **B1** (Fig. 3b), we observe a different pattern compared to S1 (Fig. 3a). The percentage of severe outcomes is much lower for B1 (i.e., 21.9% and represented by red bars). In contrast, outcomes with negligible impact (orange bars) are the most frequent in B1, accounting for 53.8% of all outcomes. Their occurrence remains relatively constant across all attack durations. In contrast, B1 exhibits a lower percentage of benign outcomes (blue bars) than S1, while the percentage of non-effective simulations (green bars) is higher in B1.

There are two noteworthy observations when comparing the outcomes presented in Figs. 3a and 3b. Firstly, the impact of barrage jamming attacks can vary significantly depending on the driving scenarios. Secondly, the percentage of severe attacks (successful attacks from the attacker's perspective) tends to increase with the duration of the attack until a certain point, after which the increasing trend becomes less significant. In the tested driving scenarios, attacks lasting longer than 5 s are comparatively likely to cause severe outcomes.

We now examine the impact of the attack start times on the outcome distributions, as illustrated in Figs. 3c (S1) and 3d (B1). The data depicted in these figures strongly correlate to the acceleration and deceleration profiles of the two driving scenarios shown in Figs. 1 and 2.

In campaign **S1**, the start times range from 17.0 s to 21.8 s, where the intervals 17.0 s to 17.6 s, and 20.4 s to 21.8 s represent acceleration periods, while the interval from 17.8 s to 20.2 s represents a deceleration period. Figure 3c shows that severe outcomes dominate when the attack start times coincide with an acceleration period, as indicated by the red curve.

In contrast, attacks initiated during the deceleration period predominately result in benign outcomes (blue curve), representing around 75% of the outcomes for the attacks initiated during this period. Furthermore, the negligible outcomes (orange curve) account for around 10% of the attacks initiated during the deceleration period, while they represent less than 5% of the outcomes of the attacks initiated during the two acceleration periods. Less than 5% of the attacks in S1 result in non-effective outcomes (green curve). Interestingly, these outcomes are evenly distributed across all attack start times; hence, their percentage appears independent of the acceleration and deceleration periods.

The design of the CACC controller model explains why the platooning system is more vulnerable to attacks during an acceleration period. When utilizing this controller, the lead vehicle periodically sends acceleration and deceleration commands to the platoon's trailing vehicles. If a vehicle loses many messages, it will continue accelerating, decelerating, or keeping a constant speed according to the last received command. Consequently, if a jamming attack begins to block the communication channel during an acceleration period, the affected vehicles will continue to accelerate until the jamming attack ceases and the vehicles receive a deceleration or constant speed command from the lead vehicle, V1.

In campaign **B1**, the start times range from 7.0 s to 16.4 s, where the time interval 7.0 s to 9.0 s represents a period when the vehicles maintain a constant speed. In contrast, the time interval 9.2 s to 16.4 s represents a period when the vehicles reduce their speed rapidly until they have reached a full stop. As shown in Fig. 3d, the most severe outcomes observed in B1 occurred for attacks initiated between 7.0 s and 9.0 s. The high proportion of severe outcomes for attacks initiated in this time interval can be explained by many attacks preventing the target vehicles from receiving deceleration commands that the lead vehicle transmits between 9.0 s and 16.0 s. Thus, these attacks often result in situations where the lead vehicle decelerates while one or several other vehicles in the platoon continue at a constant speed, increasing the risk of collisions.

For attacks initiated in the interval from 10.2 s to 14.2 s, the most prevalent outcomes are those with a negligible impact (indicated by the orange curve). This time interval corresponds to a period in which all vehicles in the platoon rapidly reduce their speed. As shown in Fig. 3d, no severe outcomes (i.e., collisions) were observed for attacks initiated at 10.2 s or later. Furthermore, for attacks initiated at 14.2 s and beyond, we noticed a rapid increase in the percentage of non-effective attacks (represented by the green curve), reaching 100% at 16.4 s, which corresponds to the time when all vehicles in the platoon have come to a complete stop. One important observation we can make from Figs. 3c and 3d is that the platooning system is more vulnerable to attacks initiated during periods of acceleration and also periods of constant speed that precede a deceleration period, compared to attacks initiated during a deceleration period.

Next, we examine how the outcome distributions are affected by the attack value, as illustrated by graphs depicted in Figs. 3e (S1) and 3f (B1). As explained earlier, the attack value represents the power of the interfering noise signal. We simulate barrage jamming attacks by manipulating the noise signal power parameter, which the network simulator uses to calculate the SINR value. As the attack value increases, the SINR decreases, resulting in a complete loss of communication among all vehicles in the platoon.

In Fig. 3e, we observe a negative correlation between the 'severe' (presented by the red curve) and 'benign' (presented by the blue curve) outcomes. In other words, an increase in the percentage of severe cases comes with a decrease in the percentage of benign cases. The graph depicting the negligible outcomes (presented by the orange curve) shows a relatively even distribution across all attack values. Furthermore, for attack values below 0.04×10^{-5} mW, all the attacks are classified as non-effective (presented by the green curve), implying that these attacks do not result in any message losses.

The figure also shows that the percentage of severe outcomes remains relatively constant at approximately 42% for attack values below 0.30×10^{-5} mW and above 0.60×10^{-5} mW. However, for attack values ranging from 0.30×10^{-5} mW to 0.60×10^{-5} mW, the proportion of severe outcomes increases to an average value of approximately 60%. To explain these results, here we present Fig. 4, which illustrates the relationship between 'noise values' and 'collisions' caused by vehicle 2 (represented by the orange curve), vehicle 3 (represented by the green curve), and vehicle 4 (represented by the red curve). We remind the reader that the noise values range from 0.0 to 1.00×10^{-5} mW. To present the results illustrated in this figure, we partition the noise value range into smaller intervals and examine the collisions caused by vehicles within each interval.

Noise Value Range $[0.0 - 0.04] \times 10^{-5}$ mW**:** No collisions occur, and the platoon operates normally under this low noise level.

Noise Value Range $[0.05 - 0.15] \times 10^{-5}$ mW**:** Collisions begin to occur, primarily involving vehicle 4. This vehicle is the first in the platoon to be affected by the increasing noise. This is because this vehicle is the farthest away from the lead vehicle, causing the signal's power received, even in the attack-free run, to be the weakest compared to those received by the other vehicles. Therefore,

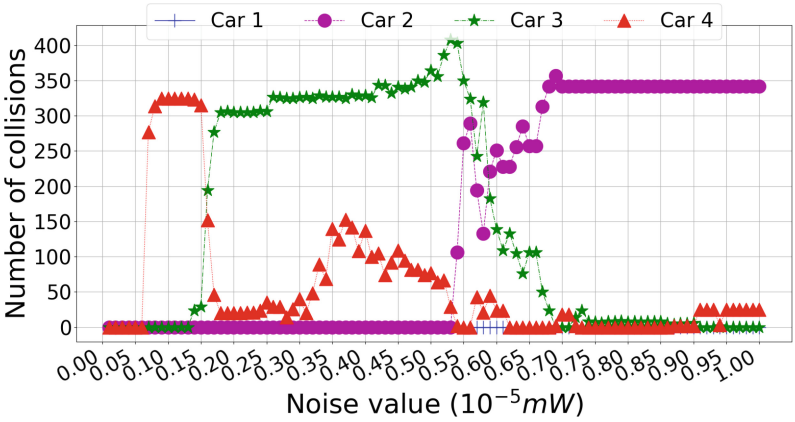


Fig. 4. Number of collisions caused by different vehicles in the platoon for different noise values.

introducing even a small amount of noise in its signals would cause this vehicle to collide. Up to 41% of the injections within this noise range caused collisions.

Noise Value Range $[0.16 - 0.30] \times 10^{-5}$ mW**:** With the increase in the noise value, vehicle 3 starts to also be affected by the noise interference, adding to the number of vehicles that could potentially cause a collision. Although the total percentage of collisions caused by these two vehicles remains the same as the one observed for the previous range, i.e., $\approx$ 41% (see Fig. 3e), the majority of the collisions are caused by vehicle 3. This is because now, vehicle 3 is the first vehicle in the platoon to be affected by the increasing noise.

Noise Value Range $[0.31 - 0.55] \times 10^{-5}$ mW**:** By increasing the noise value further, we observe a larger number of collisions caused by vehicles 3 and 4. This is not surprising as higher noise levels cause more disruptions in communication. In fact, within this range, up to around 60% of the attacks cause either of these vehicles to collide with the vehicle in front.

Noise Value Range $[0.56 - 0.60] \times 10^{-5}$ mW**:** Within this range, the noise level has reached a point where it disrupts communication of all following vehicles in a platoon. This means that now, vehicle 2, which is the closest vehicle to the lead vehicle, also starts to cause collisions. This dramatically increases the total number of collisions, comprising around 80% of the attacks using the noise values within this range.

Noise Value Range $[0.61 - 1.0] \times 10^{-5}$ mW**:** The noise levels indicated in this range are so high that as they continue to rise, we observe a complete communication loss of following vehicles with the lead vehicle. Although the initial expectation might be that the complete loss of communication should cause collisions amongst the vehicles, Fig. 3e shows that only about 41% of the injections cause collisions. The reason for this is that for the injection initiated

when the vehicles are decelerating, the complete loss of communication does not result in collisions, as the loss happens after the vehicles start to reduce their speed. Figure 4 also shows that almost all collisions are caused by vehicle 2. This is because now, vehicle 2 is the first vehicle to be affected by the increasing noise.

For the braking scenario, Fig. 3f shows that attacks with attack values below 0.04×10^{-5} mW are non-effective and cause no collisions. This is inline with our observation for the sinusoidal scenario in Fig. 3e. For attack values ranging from 0.05×10^{-5} mW to 0.11×10^{-5} mW, there is a significant increase in the proportion of benign, negligible, and severe outcomes with increasing attack values, and an equally significant drop in the non-effective outcomes. As the attack values exceed 0.11×10^{-5} mW, we observe slowly increasing values for the proportion of negligible and severe outcomes with increasing attack values. In contrast, the proportion of benign outcomes remains approximately constant. The proportion of non-effective outcomes decreases in steps until it reaches a constant value of approximately 7% for attack values above 0.61×10^{-5} mW.

In summary, Fig. 3f shows that the distribution of outcomes for the braking scenario tends to become stable (e.g., the total number of severe cases remains unchanged with the increasing noise values) for attack values above 0.61×10^{-5} mW. Our analysis of Figs. 3e and 3f shows that the correlation between the attack value and the proportion of severe outcomes is highly dependent on the number of vehicles experiencing a loss of signal as well as the driving scenario, and may exhibit unexpected and non-linear dependencies, as observed in the sinusoidal scenario.

6 Discussions

6.1 Threats to Validity

Validity refers to how accurately a test method measures its intended purpose. A test is valid when its results are closely aligned with real-world outcomes [41,42]. This section discusses internal and external threats to the validity of our results.

Internal validity can be defined as the degree of confidence that the experimental design parameters are relevant and produce meaningful results. In our benchmarking framework, the key experimental design parameters include: *(i)* the scenario and its parameters, *(ii)* the attack model and its parameters. Inaccurate or inappropriate choices of these parameters would compromise the internal validity, making the results unreliable.

External validity can be defined as the extent to which results from an experimental study can be applied to other situations. The platooning application we evaluated involves a cooperative adaptive cruise controller developed by Segata et al. [6], a sinusoidal scenario where vehicles accelerate and decelerate with a predefined frequency, a braking scenario where vehicles decelerate with a fixed deceleration rate, a wireless channel model called free space path loss (FSPL) and

the barrage jamming attack models. Altering any of these potentially yields different outcomes. For instance, consensus-based cooperative adaptive cruise controllers that maintain larger inter-vehicle distances might demonstrate greater resilience to message losses caused by jamming attacks, potentially leading to fewer severe outcomes. Similarly, employing other wireless channel models, such as two-way interference and obstacle shadowing, or scenarios like braking and constant-speed platooning could yield different outcomes. Our results are inherently tied to the experimental design and target application. Even minor variations in them can significantly impact the outcomes. Consequently, generalizing our findings to other contexts is challenging.

7 Conclusion and Future Work

To demonstrate our security benchmarking approach, we used two driving scenarios, *sinusoidal* and *braking*, for assessing the platooning application. Our benchmark approach has the potential for broad adoption. This is primarily because the simulation environment and associated tools are open-source and have already gained wide acceptance in the research for automotive use cases. Our experimental results reveal that the likelihood of a successful barrage jamming attack is notably higher when initiated during acceleration periods of a driving scenario. The attack start time is not the only factor that influences the likelihood of a collision. The attack duration is another factor; longer attacks are generally more likely to cause a collision. However, attack durations longer than a certain threshold do not significantly increase the number of severe outcomes. The higher noise values contribute to greater signal distortion, which can eventually cause communication loss. This loss significantly contributes to collisions when vehicles accelerate. We observe fewer collisions for attacks initiated when the vehicles are braking because the communication loss happens already when the vehicles have started to reduce their speed.

As part of our future work, we intend to use our proposed security benchmarking approach for evaluating other cooperative cruise controllers implemented in the Veins, such as Ploeg [30,43] and Consensus [31,44]. We plan to implement fallback mechanisms in the CACC controller developed by Segata et al. [6] that detect communication losses and activate appropriate responses. We also aim to design and implement real-world testing methodology and tools to validate simulation-based results. This approach will ensure that our simulation-based results are reliable and applicable to real-world scenarios.

Acknowledgments. The work of this paper has been partly done in the context of the SUNRISE project, funded by the European Union's Horizon Europe Research and Innovation Actions under grant agreement no. 101069573.

References

1. Cooperative Driving Automation (CDA) Committee: Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles. SAE Standard J3216_202107. https://www.sae.org/standards/content/j3216_202107/. Accessed 29 July 2024
2. El-Rewini, Z., Sadatsharan, K., Selvaraj, D.F., Plathottam, S.J., Ranganathan, P.: Cybersecurity challenges in vehicular communications. Veh. Commun. **23**, 100214 (2020)
3. Van der Heijden, R., Lukaseder, T., Kargl, F.: Analyzing attacks on cooperative adaptive cruise control (CACC). In: 2017 IEEE Vehicular Networking Conference (VNC), pp. 45–52. IEEE (2017). https://doi.org/10.1109/VNC.2017.8275598.
4. Drechsler, M. F., Seifert, G., Peintner, J., Reway, F., Riener, A., Huber, W.: How simulation based test methods will substitute the proving ground testing? In: 2022 IEEE Intelligent Vehicles Symposium (IV), pp. 903–908. IEEE (2022). https://doi.org/10.1109/IV51971.2022.9827394
5. Alipour-Fanid, A., Dabaghchian, M., Zeng, K.: Platoon stability and safety analysis of cooperative adaptive cruise control under wireless Rician fading channels and jamming attacks. arXiv preprint: arXiv:1710.08476 (2017)
6. Segata, M., Joerer, S., Bloessl, B., Sommer, C., Dressler, F., Cigno, R. L.: Plexe: a platooning extension for veins. In: 2014 IEEE Vehicular Networking Conference (VNC), pp. 53-60. IEEE (2014)
7. Ettus Research: USRP software-defined radio platform. https://www.ettus.com/products/. Accessed 25 July 2022
8. GNURadio: The free and open source software radio ecosystem webpage. https://www.gnuradio.org/. Accessed 25 July 2022
9. Jiang, D., Delgrossi, L.: IEEE 802.11p: towards an international standard for wireless access in vehicular environments. In: IEEE Vehicular Technology Conference, pp. 2036–2040. IEEE (2008). https://doi.org/10.1109/VETECS.2008.458
10. 3rd Generation Partnership Project (3GPP): Study on LTE support for V2X services. Technical Specification (TS) 22.185, Version 17.0.0 (2022). http://www.3gpp.org/ftp/Specs/archive/22_series/22.185/22185-f00.zip
11. Lichtman, M., et al.: A communications jamming taxonomy. IEEE Secur. Priv. **14**(1), 47–54 (2016)
12. Standard Performance Evaluation Corporation. https://www.spec.org/benchmarks.html. Accessed 29 July 2024
13. TPC benchmarking activities. https://www.tpc.org/. Accessed 29 July 2024
14. Gray, J., Reuter, A.: The Benchmark Handbook for Database and Transaction Systems. 2nd edn. Morgan Kaufmann (1993). ISBN: 1-55860-292-5
15. Kanoun, K.: Dependability Benchmarking for Computer Systems. Wiley-IEEE Computer Society Press (2008). https://doi.org/10.1002/9780470370506
16. Oliveira, R.A., Raga, M.M., Laranjeiro, N., Vieira, M.: An approach for benchmarking the security of web service frameworks. Futur. Gener. Comput. Syst. **110**, 833–848 (2020)
17. Segata, M., et al.: Multi-technology cooperative driving: an analysis based on PLEXE. IEEE Trans. Mob. Comput. **22**(8), 4792–4806 (2023). https://doi.org/10.1109/TMC.2022.3154643
18. Fang, W., et al.: Information security of PHY layer in wireless networks. J. Sens. **2016** (2016)

19. Alipour-Fanid, A., Dabaghchian, M., Zeng, K.: Impact of jamming attacks on vehicular cooperative adaptive cruise control systems. IEEE Trans. Veh. Technol. **69**(11), 12679–12693 (2020). https://doi.org/10.1109/TVT.2020.3030251
20. Malik, M., Aramrattana, M., Maleki, M., Folkesson, P., Sangchoolie, B., Karlsson, J.: Simulation-based evaluation of a remotely operated road vehicle under transmission delays and denial-of-service attacks. In: 2023 IEEE 28th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 23–29. IEEE (2023). https://doi.org/10.1109/PRDC59308.2023.00012.
21. Moser, D., Lenders, V., Capkun, S.: Digital radio signal cancellation attacks: an experimental evaluation. In: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2019), pp. 23–33. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3317549.3319720
22. Clancy, T. C.: Efficient OFDM denial: pilot jamming and pilot nulling. In: 2011 IEEE International Conference on Communications (ICC), pp. 1–5. IEEE (2011). https://doi.org/10.1109/icc.2011.5962467
23. Mahal, J. A., Shahriar, C., Clancy, T. C.: Emulated CP jamming and nulling attacks on SC-FDMA and two novel countermeasures. In: MILCOM 2015 - 2015 IEEE Military Communications Conference, pp. 275–280. IEEE (2015). https://doi.org/10.1109/MILCOM.2015.7357455
24. Sommer, C., German, R., Dressler, F.: Bidirectionally coupled network and road traffic simulation for improved IVC analysis. IEEE Trans. Mob. Comput. (TMC) **10**(1), 3–15 (2011). https://doi.org/10.1109/TMC.2010.133
25. Rajamani, R., Tan, H.-S., Law, B.K., Zhang, W.-B.: Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons. IEEE Trans. Control Syst. Technol. **8**(4), 695–708 (2000). https://doi.org/10.1109/87.852914
26. plexe.car2x.org: Plexe Examples - Running Plexe. https://plexe.car2x.org/tutorial/. Accessed 05 Sep 2021. Keywords: Plexe Examples - Running Plexe
27. RISE Dependable Transport Systems: ComFASE GitHub repository for code access. https://github.com/RISE-Dependable-Transport-Systems/ComFASE/. Accessed 27 July 2022
28. Maleki, M., Malik, M., Folkesson, P., Sangchoolie, B., Karlsson, J.: Modeling and evaluating the effects of jamming attacks on connected automated road vehicles. In: 2022 IEEE 27th Pacific Rim International Symposium on Dependable Computing (PRDC), pp. 12–23. IEEE Computer Society, Los Alamitos, CA, US (2022).https://doi.org/10.1109/PRDC55274.2022.00016
29. Ali, A., Garcia, G., Martinet, P.: The flatbed platoon towing model for safe and dense platooning on highways. IEEE Intell. Transp. Syst. Mag. **7**(1), 58–68 (2015). https://doi.org/10.1109/MITS.2014.2328670
30. Ploeg, J., Scheepers, B.T.M., van Nunen, E., van de Wouw, N., Nijmeijer, H.: Design and experimental evaluation of cooperative adaptive cruise control. In: 2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 260–265 (2011). https://doi.org/10.1109/ITSC.2011.6082981
31. Santini, S., Salvi, A., Valente, A.S., Pescapè, A., Segata, M., Lo Cigno, R.: A consensus-based approach for platooning with inter-vehicular communications. In: 34th IEEE Conference on Computer Communications (INFOCOM 2015), pp. 1158–1166. IEEE, Hong Kong (2015). https://doi.org/10.1109/INFOCOM.2015.7218490

32. Malik, M., Maleki, M., Folkesson, P., Sangchoolie, B., Karlsson, J.: ComFASE: a tool for evaluating the effects of V2V communication faults and attacks on automated vehicles. In: 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN2022), pp. 1–12. IEEE (2022)
33. omnetpp.org: OMNet++ Simulation Models and Tools. https://omnetpp.org/. Accessed 14 July 2021. Keywords: OMNet++, Simulation Models and Tools
34. Alvarez Lopez, P., et al.: Microscopic traffic simulation using SUMO. In: The 21st IEEE International Conference on Intelligent Transportation Systems, IEEE Intelligent Transportation Systems Conference (ITSC), pp. 1–12. IEEE (2018). https://elib.dlr.de/124092/
35. Jirjees, A.: Vehicular Ad Hoc networks: growth and survey for three layers. Int. J. Electr. Comput. Eng. (IJECE) **7**(1), 271–284 (2017)
36. Anisetti, M., Ardagna, C.A., Damiani, E., Gaudenzi, F.: A Security benchmark for OpenStack. In: Proceedings of the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), pp. 294–301 (2017). https://doi.org/10.1109/CLOUD.2017.45
37. Braun, C.: NETCARBENCH: a benchmark for techniques and tools used in the design of automotive communication systems. In: IFAC Proceedings Volumes, vol. 40, pp. 321–328 (2007). https://doi.org/10.3182/20071107-3-FR-3907.00046. ISBN: 9783902661340
38. Hu, Y., Shan, H., Dutta, R.G., Jin, Y.: Protecting platoons from stealthy jamming attack. In: 2020 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), pp. 1–6 (2020). https://doi.org/10.1109/AsianHOST51057.2020.9358269.
39. Kanoun, K.: Dependability benchmarking for computer systems (2008). https://doi.org/10.1002/9780470370506. ISBN: 047023055X
40. Conte, T.M., Hwu, W.-M.W.: Advances in benchmarking techniques: new standards and quantitative metrics. In: Zelkowitz, M., (ed.) Advances in Computers, vol. 41, pp. 231–253. Elsevier (1995). https://doi.org/10.1016/S0065-2458(08)60235-1. Available: https://www.sciencedirect.com/science/article/pii/S0065245808602351
41. Scribbr, "Internal versus External Validity," https://www.scribbr.com/methodology/internal-vs-external-validity/#:~:text=What%20is%20the%20difference%20between,be%20generalized%20to%20other%20contexts. Accessed 06 Sep 2024
42. Baldwin, L.: Internal and external validity and threats to validity. In: Research Concepts for the Practitioner of Educational Leadership, pp. 31–36, Brill (2018)
43. Ploeg, J., Semsar-Kazerooni, E., Lijster, G., van de Wouw, N., Nijmeijer, H.: Graceful degradation of CACC performance subject to unreliable wireless communication. In: 16th International IEEE Conference on Intelligent Transportation Systems (ITSC 2013), pp. 1210–1216 (2013). https://doi.org/10.1109/ITSC.2013.6728397
44. di Bernardo, M., Salvi, A., Santini, S.: Distributed consensus strategy for platooning of vehicles in the presence of time-varying heterogeneous communication delays. IEEE Trans. Intell. Transp. Syst. **16**(1), 102–112 (2015). https://doi.org/10.1109/TITS.2014.2328439