Modeling and Evaluating the Effects of Jamming Attacks on Connected Automated Road Vehicles

Mehdi Maleki*, Mateen Malik*, Peter Folkesson*, Behrooz Sangchoolie*, Johan Karlsson†
*Dependable Transport Systems, RISE Research Institutes of Sweden, Borås, Sweden
{mehdi.maleki, mateen.malik, peter.folkesson, behrooz.sangchoolie}@ri.se
† Department of Computer Science and Engineering, Chalmers University of Technology, Göteborg, Sweden
johan@chalmers.se

***Abstract*—In this work, we evaluate the safety of a platoon of four vehicles under jamming attacks. The platooning application is provided by Plexe-veins, which is a cooperative driving framework, and the vehicles in the platoon are equipped with cooperative adaptive cruise control controllers to represent the vehicles' behavior. The jamming attacks investigated are modeled by extending ComFASE (a Communication Fault and Attack Simulation Engine) and represent three real-world attacks, namely, *destructive interference*, *barrage jamming*, and *deceptive jamming*. The attacks are injected in the physical layer of the IEEE 802.11p communication protocol simulated in Veins (a vehicular network simulator). To evaluate the safety implications of the injected attacks, the experimental results are classified by using the *deceleration profiles* and *collision incidents* of the vehicles. The results of our experiments show that jamming attacks on the communication can jeopardize vehicle safety, causing emergency braking and collision incidents. Moreover, we describe the impact of different attack injection parameters (such as, attack start time, attack duration and attack value) on the behavior of the vehicles subjected to the attacks.**

***Index Terms*—attack injection, jamming, V2V communication, platooning, simulation-based system**

I. Introduction

Modern road vehicles have become interconnected cyber-physical machines that offer tremendous opportunities for enhanced safety, fuel efficiency, driver support and passenger comfort. Wireless vehicle-to-vehicle (V2V) technology enables modern road vehicles to exchange information about their position, speed and acceleration, as well as sensor data about the surrounding environment and current road conditions [1]. This information may be used in various safety-related applications such as early threat detection, minimizing safety hazards, and trajectory planning [2], [3].

Like most communication protocols, the V2V communication protocols are divided into several layers, including the application, Media Access Control (MAC) and physical (PHY) layers together with security and management layers. These layers are used to process and deliver the information between the vehicles. Among them, the PHY layer is responsible for sending and receiving electromagnetic radio signals over a wireless channel (i.e., the air medium between the interconnected vehicles). In the wireless channel no safety and security mechanisms are applicable, hence, the radio signals are susceptible to jamming attacks.

In a jamming attack, an attacker may block the signals by modulating an Radio Frequency (RF) carrier with random frequencies and amplitudes (i.e., *noise*) and transmit that malicious signal towards a target receiver to corrupt the legitimate signal. This type of security attacks may potentially compromise the ability of the connected and automated driving applications to perform their functions properly, and could thereby jeopardize vehicle safety [4]. Therefore, it is imperative to test, verify and validate the resiliency of such applications, as well as the communication system, against these jamming attacks.

In this paper, we introduce and investigate attack models for three types of jamming attacks: *destructive interference* [5], *barrage jamming* [6], and *deceptive jamming* [7]. In a simulation environment, we use these attack models to investigate the effects of jamming attacks on a platooning application. To this end, we use and extend ComFASE, a simulation-based fault and attack injection tool developed in our research group [8].

ComFASE combines several simulators, including a network simulator, an application simulator and a traffic environment simulator. This allows us to study the severity of cyberphysical attacks on vehicle movements in realistic traffic situations. To characterize the impact of the attacks on vehicle behavior, we use *deceleration profile* (i.e., the amount of braking) and *collision incidents* collected from the traffic scenario simulator. *To the best of our knowledge, we are the first to model and implement jamming attacks on physical layer of a realistic V2V communication model and evaluate their impact on vehicle behavior.*

In summary, this paper makes the following contributions:

1) We introduce simulation-based attack models for three types of jamming attacks: *destructive interference*, *barrage jamming*, and *deceptive jamming*.
2) By means of simulations, we evaluate the safety implications of these jamming attacks on a platooning application consisting of 4 vehicles.
3) We study the impact of different attack injection parameters namely, *target vehicle*, *attack model*, *attack start*

time, *attack duration*, and *amount of attack values* on the safety of the target vehicle(s). This knowledge could help testers to build effective attack injection campaigns for early system testing in a simulation environment.

II. Background

A. Related Work

Growing challenges of cybersecurity threats and the importance of information security in V2V communication systems have been recognized and studied by researchers of this field [4], [9]–[12]. There are previous studies that investigated the impacts of jamming attacks on wireless networks. However, there are relatively few publications on *signal cancellation attacks* on wireless channels as compared to other jamming attacks. In this section, we briefly present these studies.

Moser et al. [5] studied the impact of signal cancellation attacks where the attacker's signal interfere destructively with the legitimate signal. As a result, the affected signal frequencies are removed from the frequency spectrum in the ideal case. The researchers in this study considered Software-Defined Radio (SDR) device to analyse the system requirements to launch such attacks. Moreover, they demonstrated that, the signal cancellation attack could effectively attenuate the signals up to $40\ dB$ in the air, or even lower than the receivers sensitivity threshold.

Clancy [13] studied the performance of Orthogonal Frequency Division Multiplexing (OFDM) transmission which is under *pilot jamming* and *pilot nulling* attacks. In pilot jamming attacks, the pilot symbols are the main target of the attackers to compromise the performance of the channel equalization. In this research the author conducted experiments in simulations and concluded that, the pilot nulling attack on OFDM transmission with Quadrature Phase Shift Keying (QPSK) modulation is capable of cancelling target signals with $4\ dB$ of signal-to-jamming ratio. Clancy's work resembles our work presented in this paper, as we also injected *destructive interference* jamming attacks on OFDM based transmission signals with QPSK modulation.

There are other types of jamming attacks, where researchers have studied the performance of IEEE 802.11 communication protocol. For instance, Bayraktaroglu et al. have measured the performance of IEEE 802.11 protocol under reactive jamming attacks [14]. They have used GNU radio [15] and Universal Software Radio Peripheral (USRP) platform [16] to build a jamming prototype for real world experimentation.

Alipour-Fanid et al. [12] investigated effects of attacker's location when performing jamming attack on cooperative driving. They used a high-level model of IEEE $802.11p$ protocol to study the impact of jamming attacks on the CACC controller implemented in Matlab. They showed that targeting the vehicle behind the lead vehicle is the most effective location for an attacker.

The work presented in this paper is different from the previous research, as we have modeled and injected different realistic jamming attacks on the physical layer of the V2V communication system and evaluated their impact on the safety of the vehicle behavior. Moreover, we ran the attack injection campaigns in the simulation environment which gave us the possibility to re-run many experiments without jeopardizing safety of passengers and the environment.

B. Simulation Environment

To verify and validate the communication system of interconnected automated vehicles, fault and attack injection testing technique can be used either in real-world or in simulation-based environment. Real-world testing is often unsafe, costly and difficult to reproduce. On the other hand, some benefits of the simulation-based testing are, *(i)* low cost, *(ii)* reproducibility *(iii)* test automation, *(iv)* verification of the system with respect to edge cases without any safety concerns, and *(v)* revealing weaknesses in the system design at the early stages of development process [17], [18]. However, the quality of the results obtained from the simulation testing are tightly connected to the fidelity of the models w.r.t the actual system.

In this paper, we use and extend ComFASE [8], [19], that is an open source tool suitable to model and inject attacks in the communication system of connected vehicles. ComFASE is a simulation-based attack injection tool, where it integrates several simulators for network and traffic simulations. The simulators which are part of the ComFASE simulation environment includes, *(i)* OMNeT++ (a network simulator) [20], *(ii)* Veins (a vehicular network simulator) to simulate the V2V communication [21] , *(iii)* SUMO (a traffic simulator) to design, simulate traffic, and study traffic behavior [22] and *(iv)* Plexe-veins (a cooperative driving framework), which provides a platooning scenario [23].

ComFASE is flexible in targeting different layers of the V2V communication system (such as application, MAC, PHY) by adding new attack models. In addition, the tool allows us to record attack injection and traffic simulation data, which could be used to study and evaluate the safety implications of the cybersecurity attacks on the connected vehicles. In this paper however, we extend ComFASE to model three jamming attacks on the communication system (see §III).

C. WAVE Communication Protocol

Wireless Access in Vehicular Environment (WAVE) [24], [25] is an application of Dedicted Short Range Communication (DSRC) technology that defines the protocols used for constructing different communication layers of the V2V communication. These communication layers are such as, IEEE 1609.1 that defines the application layer, IEEE 1609.4 defines the media access control layer and IEEE $802.11p$ defines the physical layer protocol layer links [26]. A realistic model of WAVE communication protocol is implemented in the Veins simulator [21] which we have used to inject the jamming attacks.

Our main research objective in this paper is to observe and evaluate the impact of jamming attacks (see §III) on the behavior of the target system. The attacks are injected on the physical layer model of the WAVE protocol implemented as IEEE $802.11p$ in Veins. Therefore, in §II-D, we provide the

reader with a brief description of the information flow from the physical layer of the transmitter vehicle to the receiving vehicle (see Fig. 1). Note that, we consider the wireless channel (see §II-D3) as part of the physical layer as the impact of any attacks on the wireless channel is propagated to the physical layer of the communication system and could affect the behavior of the system.

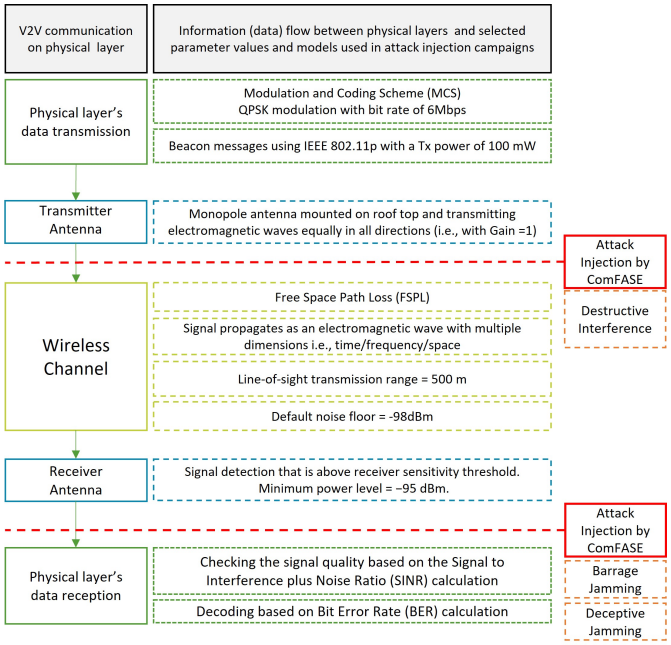


Fig. 1: V2V communication between physical layers and information flow from physical layer of transmitter vehicle to physical layer of receiver vehicle and parameter values used for attack injection campaign configuration.

D. V2V Physical Layer's Communication

1) Physical Layer's Transmission and Reception:

a) Transmission: To transmit the data towards the receiver, the physical layer is responsible for tasks such as, frequency selection, carrier frequency generation and modulation. For wireless transmission, the data is converted to a waveform (i.e., a *modulating signal*). The *modulating signal* contains actual data to be transmitted.

QPSK is one such scheme of modulation used in OFDM transmission for the WAVE communication protocol [27], that is used for V2V communication [28]. The *modulation signal* is then amplified at high frequencies (i.e., *carrier modulation*) to make it suitable for wireless transmission (i.e., *modulated signal*) in the form of electromagnetic waves [29]. Note that, from here on we call the *modulated signal* as signal when it is propagating in the wireless channel. The wireless transmission of signals is carried out by using an antenna (see §II-D2).

b) Reception: After the signal is received at the physical layer of the receiver vehicle, the Bit Error Rate (BER) is calculated using a BER calculation model. Moreover, the BER calculation model needs Signal to Interference and Noise Ratio (SINR) value as an input to calculate the bit errors. On the basis of the BER calculation result, either the data is discarded due to poor quality or it is sent to the upper layers (i.e., media access control) for further processing. SINR is used to determine the quality of the signal received. It is the ratio between the legitimate signal and unwanted noise (i.e., channel noise, parasitic noise and interference from the neighbouring channels transmitting with same frequencies). The SINR in Veins implemented according to Eq. 1.

$$SINR = \frac{SignalPower}{InterferencePower + NoisePower} \quad (1)$$

BER, on the other hand, is used to predict the errors in the communication data bits that are transmitted over the wireless channel. It is the ratio between the number of bit errors occurred and the total number of bits transmitted over the wireless channel. The BER calculation model varies depending on the modulation scheme used in the wireless communication system. We used QPSK modulation scheme implemented in the Veins simulator, while performing the experimentation [21].

2) Antenna: The antenna is a metallic structure that is able to transmit or receive electromagnetic waves to and from the wireless channel. There are different types of *antennas* (such as, *monopole* and *directional* antennas [30]), that could be used to transmit and receive the data from the wireless channel. The monopole antenna transmits the electromagnetic waves equally in all directions whereas in case of directional antenna, the concentration of electromagnetic waves are in one direction [30]. In the platooning application model, that is part of our simulation environment (see §II-B), all vehicles are equipped with monopole antennas to transmit-receive signals [31] (see Fig. 1). If the received signal power is above the antenna's sensitivity threshold, the signals are then sent to the physical layer for processing [21], [32]. The default threshold value in Veins is, $-95\ dBm$ (see Fig. 1).

3) Wireless Channel: In this study, the wireless channel refers to the *air medium* between transmitter–receiver link in which the electromagnetic waves propagate. In the wireless channel, the signal is affected by factors such as, *(i)* the signal's electromagnetic waves property, i.e., the wave becomes weaker as it travels through the air, *(ii)* the transmitter–receiver distance *'d'*, *(iii)* the sensitivity of the receiver to sense and decode a weak signal, *(iv)* the wavelength (λ) of the transmitting frequency and *(v)* reflections from objects in the environment such as, buildings, vehicles, roads, pedestrians.

The attenuation (i.e., the degradation in the signal power) caused only due to distance $'d'$, wavelength (λ) of the transmitting frequency, and sensitivity of the receiver is called *Free Space Path Loss (FSPL)* [33]. The mathematical representation of *FSPL* is called the *friis transmission equation* as shown in Eq. 2. In this equation, the received power i.e., *Pr* (dBm) could be calculated based on the transmitted power *Pt* (dBm) that is delivered to the transmitting antenna, *Gt* (dB) and *Gr* (dB) are the transmitter and receiver antenna gains, respec-

tively, and $\sum Lx$ (dB) represent the total losses caused by the environment.

$$Pr[dBm] = Pt[dBm] + Gt[dB] + Gr[dB] - \sum Lx[dB] \quad (2)$$

In the Veins simulator, there are few environmental models implemented such as, *Two-Ray Interference Model*, *Obstacle Shadowing* and *FSPL* models [34], [35]. We have used the *FSPL* model to represent the environment for our experimentation [33].

E. Jamming Attacks on the Physical Layer

The physical layer is the lowest layer of V2V communication systems and also vulnerable to attacks. This is because it deals with various interfaces such as, electrical, mechanical and timing interfaces. Moreover, the transmission medium (i.e., wireless channel) has a direct interface with the physical layer. The wireless channel is beyond the safety and security mechanisms of the physical layer. Therefore any intention to interfere or obstruct the signal, could have direct impact on the functionality (i.e. the ability to filter and correctly process the data) of the physical layer. Jamming attacks are one way to disturb the signals in the wireless channel. The term jamming could refer to as, blocking the legitimate signals by interfering with the legitimate signal or adding noise to it. In related work section (see §II-A) we presented some previous studies where, researchers have injected and studied the impact of different types of jamming attacks on the wireless network.

III. Attack Model Implementation

This section presents three real-world jamming attacks that can be carried out on V2V communication systems, and describes how we model the impact of such attacks in our simulation environment. These attacks belongs to a category which could effect the system functionality by either degrading the quality of the legitimate signal (such as power) or deceiving the system by sending identical malicious signals with no real information.

A. Destructive Interference

Destructive interference is a type of jamming where an attacker sends malicious signals directed towards the target vehicle to affect the power of the legitimate signal destructively [5], [6]. To launch this attack successfully, the attacker must have the information of the target vehicle's communication protocol. These types of attacks are also known as *protocol-aware jamming* [6].

Fig. 2 has three cases of phase shifts that can be performed by an attacker to show basic principle of *destructive interference*. To explain *destructive interference* attack, we consider a single signal and elaborate on how the attack works. The attacker's signal is an inverted version of the legitimate signal, which is to be received. In order words, the attacker's signal has the same frequency and amplitude of the legitimate signal with some degrees of phase shift (i.e., in between 120° to 180°) to achieve different levels of destructiveness [5]. The phase shift defines the level of destructiveness 'D' that an attacker can achieve, where higher phase shift results into more destructiveness of the legitimate signal.

At the receiver's antenna, the signals interfere destructively with each other and, as a result, the legitimate signal is either annihilated or received with a very low power due to signal cancellation (see Fig. 2). Once the legitimate signal is affected by the destructive interference, the quality of the received signal is reduced drastically. This results into one of the following two cases, *(i)* the signal cannot be detected by the receiver's antenna as the received signal power is lower than the antenna sensitivity threshold. [32], *(ii)* the signal power is higher than the antenna's sensitivity threshold (see Fig. 1), but it is received with very low SINR value due to the weak reception, which results into a high BER, and therefore the signal is categorized as *noise* (see §II-D1b).

Perfect *destructive interference* (a.k.a nulling [6]) occurs when the legitimate signal power is reduced to zero at the receiver end. In order to achieve this, the attacker must generate an accurate inverted signal (i.e., 180° phase shift) in real time. Technically, this is a challenging task since the inverted signal must arrive at the receiver's antenna at the same time as the legitimate signal. However, a recent study has revealed that the signal cancellation attacks can in fact manage to attenuate up to 40 dB of the legitimate signal in GPS based wireless communication systems [5].

Similarly, perfect *destructive interference* is hard or even infeasible to achieve in the case of V2V communication. This is due to the wireless channels' varying nature (e.g., the signal delay varies over time). Factors that contribute to the signal delay include, buildings, roads and vehicles.

Therefore, we model the attacker according to Eq. 3 where the attacker may achieve negligible to complete destructiveness $'D'$ of the signal over the period of time while the attack is active. In Fig. 2, the minimum (when $D = 0$) and maximum (when $D = 1$) effect of destructive interference that can be achieved is shown.

$$P_r^{'} = P_r(1 - D) \quad (3)$$

The parameters P_r and $P_r^{'}$ represent power of the legitimate and superimposed signals. Moreover, the parameter 'P_r' is part of *analogue model* implemented in the Veins simulator, where, the *analogue model* refers to wireless communication channel. Fig. 1 shows where in the hierarchy of the communication chain the received power parameter is manipulated to model the impact of the *destructive interference* attack.

B. Barrage Jamming

In *Barrage jamming*, the attacker continuously transmits noise-like energy across the entire frequency spectrum of the communication channels [36]. The *barrage jamming* attacks are categorized as *non–protocol aware jamming* [6], [9] since the attacker does not require any prior knowledge about the communication protocol to be able to conduct the attacks.

We model the impact of *barrage jamming* by using the *noise* parameter, that is implemented in Veins. The *noise* parameter is originally used to model the impact of various source of

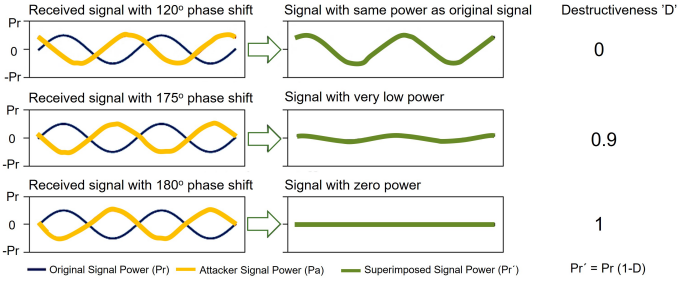


Fig. 2: Examples of the impact of the destructive interference attack on the legitimate signal, along with the destructiveness 'D' used for modeling the attack with ComFASE.

noise that may affect the received signal such as channel noise and system circuitry noise, while processing the legitimate signal. This parameter is used in SINR calculation (see Eq. 1) to determine the quality of the signal. Fig. 1 shows where in the hierarchy of communication chain the noise parameter is manipulated to model the impact of the *barrage jamming*.

C. Deceptive Jamming

Deceptive jamming is a technique where the attacker generates a fake signal, which possesses the same characteristics (such as, frequency and power) as a legitimate signal. The purpose of this attack is to trick the receiver into receiving and processing the attacker's signal instead of the legitimate signal [6].

We model the impact of *deceptive jamming* attack by using a parameter called *interference*, which is implemented in Veins. This parameter is originally used to map the effects of interfering signals on the quality of the legitimate signal used for SINR calculation (see Eq. 1). Fig. 1 shows where the interference parameter is located within the V2V communication hierarchy.

D. Existing Jamming Tools and Techniques

With modern commercial and off-the-shelf software and hardware tools and techniques, attackers are able to launch various jamming attacks on interconnected vehicles. In the following subsections we will present a few of these tools and techniques,

a) Software Defined Radio (SDR) devices: SDR devices are easily accessible in the open market and can be used to launch jamming attacks. They can generate a wide range of radio signals over a broad spectrum of frequencies, making them capable of jamming of many wireless communication protocols, including GPS and IEEE 802.11p. Two examples of SDR based devices are, *(i) Lime SDR* is capable of simultaneously transmitting/receiving radio frequencies within the range of 10 MHz to 3.5 GHz with a bandwidth of up to 30.72 MHz [37] and, *(ii) USRP B200/B210* is a high performance scalable software-defined radio platform with a possibility of generating frequency range between 70 MHz to 6 GHz with maximum bandwidth of 56 MHz [38].

These frequencies can be transmitted towards the target receiver by using different types of advanced antennas such as omnidirectional and directional antennas with beam-forming ability [39].

b) Machine Learning (ML) based techniques: ML based techniques can be used for analyzing the data exchanged between the target vehicles to understand the characteristics and behaviour of the signals in a wireless channel to launch jamming attacks [40]. For instance, based on these techniques, it is possible to launch an attack when the energy is detected at the receiver's antenna of the target vehicle. This type of attacks is known as *reactive jamming* [11].

c) Direct Digital Synthesis (DDS): This technique is used to generate analog waveforms of different frequencies much easier and faster in real-time. This is done usually by generating a digital time-varying signal, which is later transformed into an analog waveform by performing a digital-to-analog conversion. Due to the DDS's device digital nature, it is easier to generate broad spectrum of frequencies ranging from 1 Hz to 400 MHz and fast switching between these output frequencies [41]. Moreover, DDS devices are compact, low power and accessible at low cost.

It is to be noted that according to EU directives, it is generally illegal to manufacture or use any sort of jammers to deliberately interfere with radio communication under public use [42]–[44]. Even jamming radio signals (such as mobile phone communication) for testing purposes are prohibited and require special permit (requirements specific to each country) to conduct tests in the open environment or test chambers.

Considering these limitations, executing attack injection campaigns on a wireless communication protocols in a simulation environment is advantageous. Moreover, it provides an opportunity to perform initial testing with regards to resilience of safety critical systems (or system models) and intrusion detection systems against different types of jamming attacks without worrying about the license issues.

IV. Attack Injection Experimental Setup

A. Traffic Scenario

We have used the platooning application provided by Plexe-veins [23] to evaluate the impact of jamming attacks on vehicle behaviour. We conducted all experiments with a platoon of 4 identical vehicles, which are driving on a highway (see Fig. 3) according to a sinusoidal driving pattern (see Fig. 4). This means that the vehicles in the platoon are constantly accelerating and decelerating with the oscillating frequency of 0.2 Hz and amplitude of 5.0 km/h. We use this driving pattern to observe the impact of the attacks on vehicles while they are accelerating or decelerating. The maximum speed that the lead vehicle can achieve (vehicle 1 in Fig. 3) is set to 100 km/h and all the vehicles are controlled by the Cooperative Adaptive Cruise Control (CACC) controller [45]. We selected the CACC controller as a vehicle equipped with this controller uses its own data, the data transmitted from the vehicle in front and the platoon leader. This allows us to

evaluate the safety implications of the jamming attacks on the interconnected vehicles in the platoon.

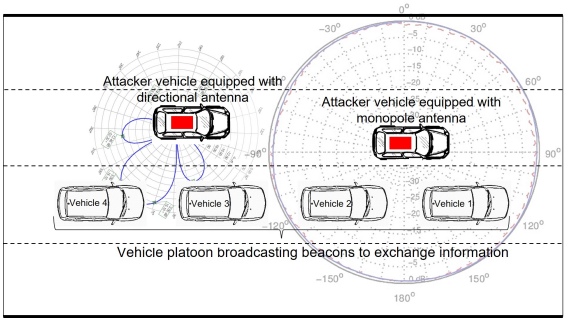


Fig. 3: A four-vehicle platooning scenario. The attacker vehicles illustrate the use of a *monopole antenna* to conduct *barrage jamming* and a *directional antenna* to conduct *destructive interference* and *deceptive jamming*.

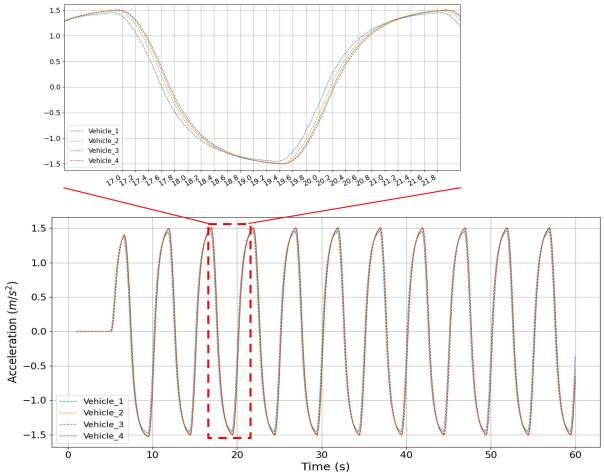


Fig. 4: Acceleration profiles of all vehicles in the platoon. NB: the dashed area marks the selected attack start time period.

B. Communication Model and Wireless Channel Model

We have used the WAVE communication model (see §II-C) and the wireless channel model (see §II-D3) implemented in Veins [21]. We used the default parameter values of the communication model and the wireless channel model included in Veins, which are presented below:

Communication model parameters: We use a data packet of 200 bits for transmission with beaconing time of 10 Hz (0.1 s). To send the data with the rate of 6 $Mbps$ we use the QPSK Modulation and Coding Scheme (MCS). Each vehicle in the platoon is equipped with a monopole antenna mounted on the roof top that transmits the data with the transmission power of 100 mW. The default noise floor of the messages received at the receiver's antenna is set to -95 dBm. Moreover, the antenna sensitivity level is -94 dBm for data reception, which is a high sensitivity level often used for safety-critical applications.

Wireless channel model parameters: We use the default *Free Space Path Loss (FSPL)* model to represent the impact of the environment on the communication signal (see §II-D3). The central frequency of the signal is 5.85 GHz as defined by the 802.11p protocol [46].

C. Attack Injection Campaign Setup

We target signals by modeling each of the jamming attacks explained in §III. Table I presents the parameters manipulated in Veins to model the impact of the jamming attacks. The table also includes the span of points in time when the attacks start, and the range of the attack duration.

For attack start time, we target the third cycle of the platoon sinusoidal maneuver that spans from 17.0 s to 21.8 s (see Fig. 4). This cycle is selected as the platoon becomes stable (i.e., the vehicles achieve the desired driving pattern) from that cycle until the end of the simulation run (i.e. 60 s). Moreover, this cycle is chosen to be able to observe the impact of the injected attacks before the simulation ends. Note that, the attack start time values chosen within this driving cycle are 0.2 s apart, resulting in a total of 25 cases.

For each attack start time, we run 30 experiments that lasts from 1 s to 30 s, corresponding to the duration of attacks. The attack with the start time of 21.8 s and duration of 30 s ended at 51.8 s, where the total simulation time was 60 s. Thus the attack duration of 30 s was selected for a better resolution of the experimental results, that is, to observe the optimal impact of the attacks before the simulation ends (i.e., 60 s). This corresponds to 750 experiments (25 *attack start times**30 *attack end times*).

When modeling the *destructive interference* attack, we reduced the received signal power 'Pr' dramatically to between 0.08052% and 0.0% of the original power, in steps of 0.00183%. This corresponds to a range of destructiveness values between 99.91948% and 100%. We selected this range of destructiveness values based on observations that experiments with lower destructiveness values than 99.91948% had no impact on the behavior of the platoon compared to the golden run. This is due to the high sensitivity of the antenna (i.e., -94 dBm) which enables the receiver to receive and process extremely low power signals. The step size of 0.00183% results in 45 attack values. Hence, the total number of experiments for this attack injection campaign is 33750 (25 *attack start times**30 *attack end times**45 *attack values*).

When modeling the *barrage jamming* attack, we vary the noise signal power from 0 to $1*10^{-5}$ mW, where every experiment is $0.01*10^{-5}$ mW apart, resulting in 100 experiments. Hence, the total number of experiments for this attack model is 75000 (25 *attack start times**30 *attack end times**100 *attack values*).

Note that when modeling the *deceptive jamming* attack, the range that we have selected for the interference signal power is also the same as the one chosen for the noise signal power when modeling the *barrage jamming* attack. This is due to the fact that the *noise* and *interference* parameters

TABLE I: Parameters & values used to setup the attack injection campaigns.

Attack type	Target parameter	Selected valueRange	Selected attackStartTimes	Selected attackEndTimes
Destructive Interference	Received signal power	99.91948% to 100% with 0.00183% steps	$17.0s$ to $21.8s$ with $0.2s$ steps	attackStartTime $+(1s$ to $30s)$ with $1s$ steps
Barrage Jamming	Noise signal power	(0.0 to 1.0)$*10^{-5}mW$ with $0.01*10^{-5}mW$ steps		
Deceptive Jamming	Interference signal power			

affect the SINR of the received signal in the same way as according to Eq. 1. Also note that we limit the upper bound of noise and interference parameters to $1 * 10^{-5}\ mW$ as for greater values, we did not observe significant differences in result classification when compared to those obtained for $1 * 10^{-5}\ mW$.

D. Result Classification

Results of the attack injection experiments are classified into four categories based on the deceleration profiles and collision events of the vehicles. The four categories are, *(i) non-effective*: identical deceleration profiles as the golden run, *(ii) negligible*: the recorded maximum deceleration is less than or equal to $1.53\ m/s^2$ (i.e., the maximum deceleration recorded in the golden run), *(iii) benign*: the recorded maximum deceleration is greater than $1.53\ m/s^2$ and less than or equal to $5\ m/s^2$ (i.e., the maximum comfortable braking value defined), and *(iv) severe*: the recorded maximum deceleration is greater than $5\ m/s^2$, or a collision occurred.

V. Experimental Results and Evaluation

In total, we describe results from 5 attack injection campaigns. Three of them for destructive jamming, and one each for barrage jamming and deceptive jamming. A summary of the results for each campaign is shown in Table II.

A. Destructive Interference

We conducted three attack injection campaigns to evaluate the overall impact of *destructive interference* attacks on the reception capability of the vehicles that are on different positions in a platoon (see Fig. 3). The overall impact is evaluated in terms of the behavior of the vehicle under attack and the impact of the attack on the entire platoon. The attack injection campaigns are divided into three subsets of campaigns that is when, *(i)* only vehicle 2 is targeted, *(ii)* only vehicle 4 is targeted, and *(iii)* all vehicles in the platoon are under attack.

1) First campaign: In the first attack injection campaign, we target vehicle 2, that is the vehicle driving behind the lead vehicle (i.e., vehicle 1). As shown in Table II, 7.2% of a total 33750 attacks resulted in severe collisions. Around 3.7% of the total attacks had a benign or negligible impact, while 89.1% had no impact at all. This shows the effectiveness of attacks in revealing the weaknesses of the system under test.

TABLE II: Attack injection results.

Campaign #	Target Vehicle(s)	Non-Effective	Negligible	Benign	Severe	Total
Destructive Interference						
1	V2	30060	854	403	2433	33750
2	V4	4351	7209	13363	8827	33750
3	all vehicles	4012	7713	12747	9278	33750
Barrage Jamming						
4	all vehicles	3042	5424	30788	35746	75000
Deceptive Jamming						
5	all vehicles	3042	5433	30768	35757	75000

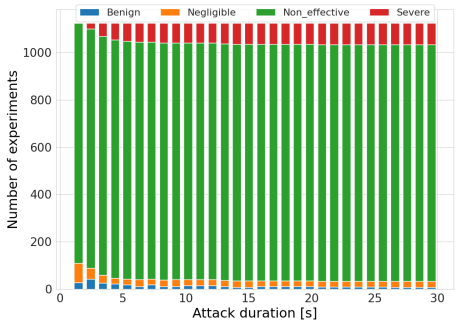
2) Second campaign: In the second campaign, the attacks were directed towards vehicle 4, which is the last vehicle in the platoon. 26.1% of total attacks on this vehicle resulted in severe collisions which is more than three times higher than the corresponding results obtained for when targeting vehicle 2. Furthermore, 39.5% of the total attacks were benign, 21.0% negligible and 13.4% had no impact at all.

So why is vehicle 4 much more vulnerable to *destructive interference* attacks than vehicle 2? That is because in the *FSPL* environment model chosen in this study, the attenuation of signals is tightly connected to the distance between the transmitter and receiver vehicles (see §II-D3). In the case of our chosen traffic scenario, vehicle 4 receives a more attenuated signal as it is farthest from vehicle 1 (see Fig.3), resulting in vehicle 4 to be highly vulnerable to the attacks injected. This shows the importance of the chosen traffic scenario and the environmental models in the results obtained.

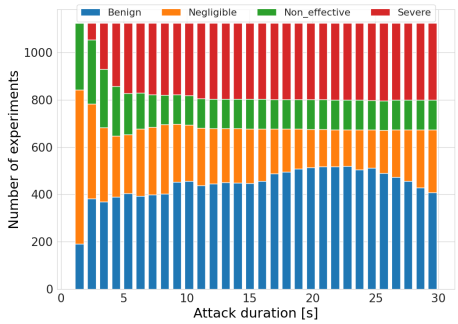
3) Comparison of the results obtained from the first and second campaigns: In Fig. 5, we present a classification of the results obtained from the first and second campaigns. Fig. 5a and 5b show how the duration of an attack affects the results for vehicle 2 and vehicle 4, respectively. These figures show that, the number of severe cases increases up to attack duration of $5\ s$. However, exposing the target vehicles to the attack for more than $5\ s$ results in approximately the same number of severe cases as obtained for when exposing the vehicles to the attack for $5\ s$. This confirms the findings of previous study that drew the same conclusion when targeting vehicles in a platoon with delay attacks [8].

Fig. 5c and 5d illustrate the experimental results classified according to the *attack start time*. The results presented in these figures could be better explained by knowing if an attack has been active during a vehicle's acceleration or deceleration times. Therefore, we consider four cases as below;

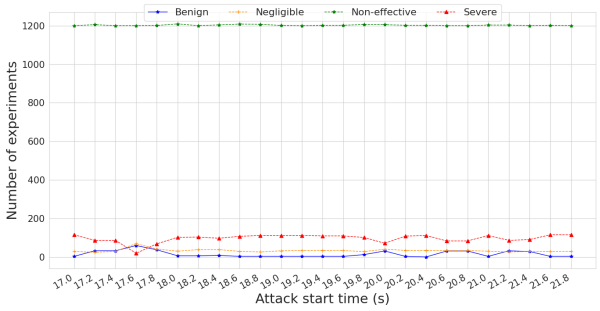
Case 1: The attack starts while the vehicles are accelerating



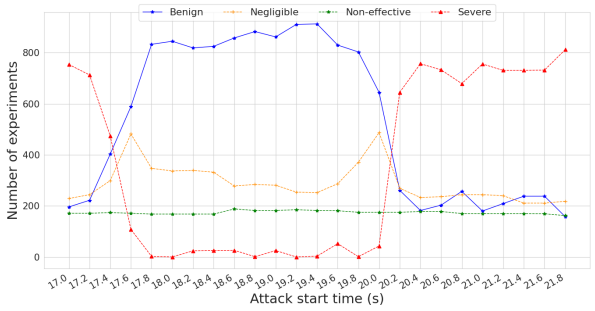
(a) Classification of results for vehicle 2 w.r.t. the *attack duration*.



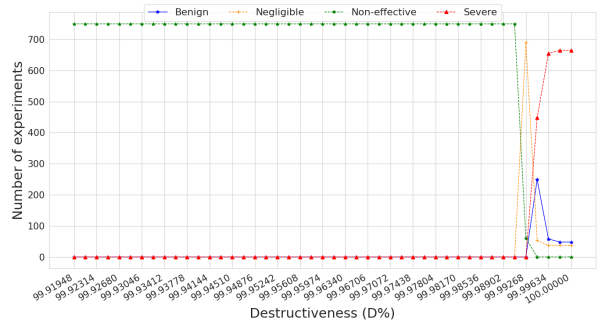
(b) Classification of results for vehicle 4 w.r.t. the *attack duration*.



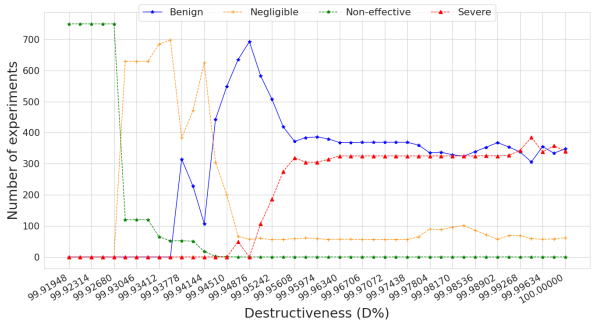
(c) Classification of results for vehicle 2 w.r.t. the *attack start times*.



(d) Classification of results for vehicle 4 w.r.t. the *attack start times*.



(e) Classification of results for vehicle 2 w.r.t. the *'D'* values.



(f) Classification of results for vehicle 4 w.r.t. the *'D'* values.

Fig. 5: Classification of the results obtained for campaigns 1 and 2 of the destructive interference attacks.

and ends before they start decelerating.
Case 2: The attack starts while the vehicles are decelerating and ends before they start accelerating.
Case 3: The attack starts while the vehicles are accelerating and ends while the vehicles are decelerating or even continues further, depending on the duration of the attack.
Case 4: The attack starts while the vehicles are decelerating and ends while the vehicles are accelerating or even continues further, depending on the duration of the attack (see Fig. 4).

For these campaigns, the majority of the experiments (i.e., with duration of 3 s or more) belong to either *case* 3 or *case* 4 (see Fig. 4). In *case* 3, if the injected attack leads to a communication loss, the target vehicle will keep accelerating. Therefore, its distance to the vehicle in front will decrease, depending on the acceleration amount and duration of the attack can eventually lead to a collision with the front vehicle. In *case* 4, if the injected attack leads to a communication loss, the target vehicle will keep decelerating. Therefore, its distance with the following vehicle will decrease, depending on the deceleration amount and duration of the attack can eventually lead to a rear-end collision.

In Fig. 5c, the target vehicle is 2, in which the *case* 3 applies to the time period of 17.0 s - 17.6 s and 20.2 s - 21.8 s, where the majority of severe attacks led to a frontal collision of target vehicle with vehicle 1. And the *case* 4 applies to the time period of 17.8 s - 20.0 s, where majority of the severe attacks

resulted in rear-end collision with vehicle 3. Fig. 5d shows that when targeting vehicle 4, as there is no following vehicle to cause a rear-end collision, the majority of the collisions happened in *case* 3 (i.e., from 17.0 s to 17.6 s and from 20.2 s to 21.8 s) which led to frontal collision with vehicle 3.

Fig. 5e and 5f demonstrate the impact of the level of destructiveness $'D'$ when targeting vehicle 2 and vehicle 4, respectively. Fig. 5e shows that, to be able to cause collisions as a result of a *destructive interference* attack on vehicle 2, the attacker would need to destroy the signal's power by more than 99.99268%. This is due to the close proximity of vehicle 2 and the leader of the platoon. In the case where vehicle 4 is the target of the attack, the high number of *severe* cases occur already for when the destructiveness parameter is around 99.94693 percentage points. Therefore, the far proximity of vehicle 4 with the leader of the platoon could be a motivating factor for an attacker to target this vehicle.

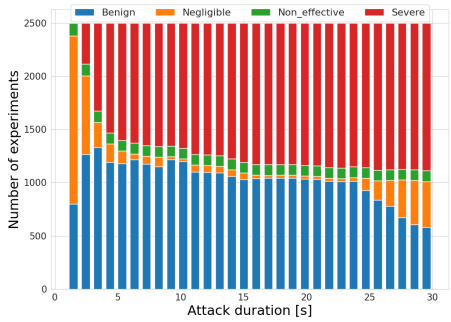
4) Third campaign: To further investigate the impact of *destructive interference* attacks, we targeted all the vehicles in the platoon. As shown in Table II, the number of *severe* cases is slightly higher than that obtained for campaigns 1 and 2. This indicates that by targeting multiple vehicles which are at different positions in the platoon, an attacker could reveal weaknesses of the target system which would otherwise be difficult if only a single vehicle is targeted.

For all three campaigns presented in this section, we also study the impact of the injected attacks on the entire platoon. This was achieved by looking further into the *severe* results where the injected attacks led to a collision, to identify the collider vehicle (i.e., the vehicle responsible for collision) based on data collected from SUMO traffic simulator [47]. In campaign 1, where we targeted vehicle 2, out of the 2433 severe cases 54% and 46% were caused by vehicles 2 and 3, respectively. In campaign 2, where vehicle 4 was targeted, all the collision cases were caused by vehicle 4. Finally in campaign 3, where we targeted all the vehicles in the platoon, out of the 92784 *severe* cases, 13% were caused by vehicle 2, 31% by vehicle 3 and 56% by vehicle 4.

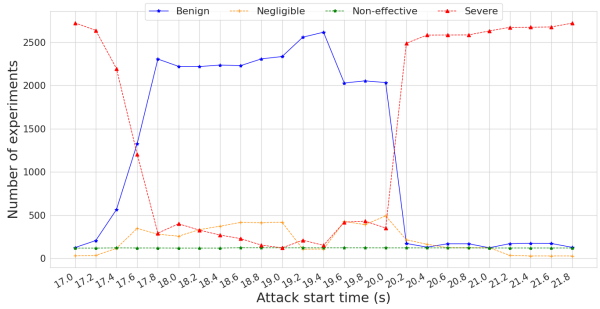
B. Barrage Jamming

In the 4^{th} attack injection campaign, we investigated the impact of *barrage jamming* on the platoon vehicles. To do so, 75000 experiments are conducted, out of which 35746 are classified as *severe* causing vehicular collisions. The results of the experiments are summarized in Table II. Fig. 6 shows the overall classification of the experimental results for the *barrage jamming* attacks.

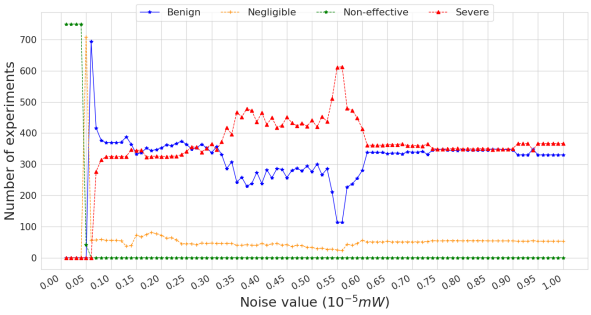
Fig. 6a shows the classification of the results w.r.t the attack duration. Here we observed that the number of *severe* cases are higher for attacks with longer duration times. However, exposing vehicles to the *barrage jamming* attacks for more than 10 s result in approximately the same number of severe cases as obtained for duration of 10 s. This observation is similar to that observed for the destructive interference attacks. That is, the proportion of severe outcomes tends to become



(a) Classification of results w.r.t. the *duration* in which all vehicles are targeted.



(b) Classification of results w.r.t. the *attack start times* in which all vehicles are targeted.



(c) Classification of results w.r.t. the *noise* values chosen to target all vehicles.

Fig. 6: Classification of the results obtained for the barrage jamming attacks.

approximately constant for attack duration times longer than a certain threshold value.

Fig. 6b shows the distribution of outcomes w.r.t. the *attack start time*. Again, we need to consider the four cases describing the occurrence of the attacks in relation to the sinusoidal driving pattern (see Fig. 4), which we introduced in §V-A3 for the *destructive interference* attacks. We observe a similar impact of the *barrage jamming* attacks, as we described for case 3 and case 4 for the *destructive interference* attacks.

Fig 6c shows the experimental results when injecting dif-

ferent *barrage jamming* attack values through manipulation of the *noise signal power* parameter. This parameter is used in the SINR calculation (see Eq. 1) to determine the quality of the signal. As the noise increases, the SINR decreases, which eventually leads to communication loss of all vehicles in the platoon. For experiments with attack values lower than $0.04 * 10^{-5}\ mW$, all injections are classified as *non-effective*. However, higher *noise signal powers* result in a large number of experiments to be classified as *severe*. For noise values higher than $0.61 * 10^{-5}\ mW$, the number of *severe* cases are almost the same as the one resulted when using this value. This is due to the fact that, when the *noise* value is as high as this value (i.e., $0.61 * 10^{-5}\ mW$), a complete communication loss occurs, which consequently result in all vehicles to keep consuming old data as modeled in the Veins network simulator.

For this campaign, we also identify the responsible vehicle for collision, to study the impact of the injected attack on the entire platoon. Out of the 35746 *severe* cases, 41%, 43% and 16% were caused by vehicles 2, 3 and 4, respectively.

C. Deceptive Jamming

We conduct one attack injection campaign comprising of 75000 experiments to study the impact of *deceptive jamming*. A total of 35757 experiments within this campaign resulted in vehicle collisions. As can be seen in Table II, this result is comparable with that obtained for *barrage jamming*. This is due to the fact that both attack types are carried out at the receiving antenna, and thus affect the SINR in a similar way (see Eq. 1). Note that, the similarity of the results obtained was also evident when plotting the results of the *deceptive jamming* and comparing them with those presented in Fig. 6 for the *barrage jamming* attacks. Because of this similarity, we decided not to include such plots in the paper.

VI. Discussion and Future Work

Our study shows that the platooning application provided in Veins, which is based on the CACC controller, is highly vulnerable to message losses caused by jamming attacks. For both *barrage jamming* and *deceptive jamming*, our results show that close to 48% of the attacks resulted in severe outcomes, of which most were collisions. For *destructive jamming*, the proportion of attacks resulting in severe outcomes varies from 7.2% to 27%, depending on whether one vehicle or all vehicles in the platoon was subjected to the attacks.

From these results it is evident that the CACC controller, as implemented in the Veins, has not been designed to tolerate message losses. The reason for this is most likely that the individuals who implemented the CACC controller were mainly interested in providing an effective platooning controller for normal fault-free operations. Clearly, if the CACC controller is to be used in a real system it must be provided with mechanisms that makes it tolerate message losses.

Although our experiments were conducted with a platooning application that is highly vulnerable to message losses, and therefore can be considered unrealistic to use in a real system, we believe that our result provide valuable insights for researchers and engineers who design and validate platooning applications. One obvious observation is of course that a platooning system must be made highly resilient to message losses. Another interesting observation is that the vulnerability to jamming attacks may vary for different vehicles within a platoon. Whether this is true also for other implementations of platooning systems is an open question that needs to be answered by further research.

We have developed the ComFASE tool to address the needs of the automotive industry to reduce the cost of real-world testing by replacing such tests with simulation-based tests [17]. To enable studies of how attacks and faults may affect vehicles in realistic traffic situations, ComFASE combines several simulators, including a network, an application, and a traffic simulator. The validation of whether these simulators jointly can provide accurate representations of real-world systems constitutes a demanding challenge that we currently don't have financial resources to address, since this would involve comparing the simulation results with results conducted with a real-world system.

However, to build confidence in our simulation results we plan to conduct experiments where we investigate how variations in the network model parameters will affect the outcome distributions. In addition, we plan to conduct experiments with more advanced wireless channel models, such as *Two-Ray Interference Model* and *Obstacle Shadowing*. Moreover, we plan to investigate alternative modulation schemes for V2V communication based on the WAVE protocols suit. Our plans for future research also include evaluations of other systems, including a teleoperation application for remote driving.

VII. Conclusions

In this paper, we propose and use simulation models for three types of jamming attacks: *destructive interference*, *barrage* and *deceptive* jamming. We apply these models in simulations to investigate the vulnerability of a platooning application to jamming attacks. The platooning application is based on the CACC controller and was implemented in the Veins. To be able to investigate the impact of the attacks on the behaviour of the vehicles in the platoon, we have integrated Veins [21] and SUMO [22] in a tool called ComFASE [8], which has been developed in our research group. We report results from 5 attack injections campaigns, which in total consists of 251250 attack experiments. The results show that the evaluated platooning application was highly vulnerable to the jamming attacks; the proportion of attacks that had severe outcomes (mostly collisions) varied from 7.2% to 48% among the different campaigns. Due to these high proportions of severe outcomes, we conclude that the tested implementation of the CACC controller is not sufficiently protected against jamming attacks. Our future research will therefore address techniques for making platooning applications, as well as other applications for autonomous driving, resilient to jamming attacks.

ACKNOWLEDGMENT

This work was supported by VALU3S project, which has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876852. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey.

REFERENCES

[1] What is vehicle-to-vehicle (V2V) communication? https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication/. (accessed: 17.06.2022).

[2] Volvo models warn each other of slippery roads and hazards. https://www.media.volvocars.com/global/en-gb/media/pressreleases/251381/. (accessed: 17.06.2022).

[3] C. Wuthishuwong, A. Traechtler, and T. Bruns, "Safe trajectory planning for autonomous intersection management by using vehicle to infrastructure communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, pp. 1–12, 2015.

[4] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

[5] D. Moser, V. Lenders, and S. Capkun, "Digital radio signal cancellation attacks: An experimental evaluation," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 23–33. [Online]. Available: https://doi.org/10.1145/3317549.3319720

[6] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security and Privacy*, vol. 14, no. 1, pp. 47–54, 2016.

[7] 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*, ser. MobiHoc '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 46–57. [Online]. Available: https://doi.org/10.1145/1062689.1062697

[8] M. Malik, M. Maleki, P. Folkesson, B. Sangchoolie, and J. Karlsson, "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)*, 2022.

[9] W. Fang, F. Li, Y. Sun, L. Shan, S. Chen, C. Chen, and M. Li, "Information security of phy layer in wireless networks," *Journal of Sensors*, vol. 2016, 2016.

[10] B. Sangchoolie, P. Folkesson, P. Kleberger, and J. Vinter, "Analysis of cybersecurity mechanisms with respect to dependability and security attributes," in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2020, pp. 94–101.

[11] D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. Schmitt, "Gaining insight on friendly jamming in a real-world ieee 802.11 network," in *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 105–116. [Online]. Available: https://doi.org/10.1145/2627393.2627403

[12] A. Alipour-Fanid, M. Dabaghchian, and K. Zeng, "Impact of Jamming Attacks on Vehicular Cooperative Adaptive Cruise Control Systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 12 679–12 693, 2020.

[13] T. C. Clancy, "Efficient ofdm denial: Pilot jamming and pilot nulling," in *2011 IEEE International Conference on Communications (ICC)*, 2011, pp. 1–5.

[14] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "Performance of ieee 802.11 under jamming," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 678–696, 2013.

[15] gnuradio. The free and open source software radio ecosystem webpage. https://www.gnuradio.org/. (accessed: 25.07.2022).

[16] USRP software-defined radio platform. https://www.ettus.com/products/. (accessed: 25.07.2022).

[17] M. F. Drechsler, G. Seifert, J. Peintner, F. Reway, A. Riener, and W. Huber, "How simulation based test methods will substitute the proving ground testing?" in *2022 IEEE Intelligent Vehicles Symposium (IV)*, 2022, pp. 903–908.

[18] R. Donà and B. Ciuffo, "Virtual testing of automated driving systems. a survey on validation methods," *IEEE Access*, vol. 10, pp. 24 349–24 367, 2022.

[19] ComFASE Github repository for code access. https://github.com/RISE-Dependable-Transport-Systems/ComFASE/. (accessed: 27.07.2022).

[20] omnetpp.org. OMNet++ simulation models and tools. https://omnetpp.org/.

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

[22] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic Traffic Simulation using SUMO," in *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, 2018. [Online]. Available: https://elib.dlr.de/124092/

[23] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. L. Cigno, "Plexe: A platooning extension for Veins," in *2014 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2014, pp. 53–60.

[24] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation," *IEEE Std 1609.4-2006*, pp. 1–82, 2006.

[25] Y. J. Li, "An overview of the dsrc/wave technology," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, X. Zhang and D. Qiao, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 544–558.

[26] M. N. Tahir and M. Katz, "Performance evaluation of IEEE 802.11p, LTE and 5G in connected vehicles for cooperative awareness," *Engineering Reports*, vol. n/a, no. n/a, p. e12467. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/eng2.12467

[27] K.-Y. Ho, P.-C. Kang, C.-H. Hsu, and C.-H. Lin, "Implementation of wave/dsrc devices for vehicular communications," in *2010 International Symposium on Computer, Communication, Control and Automation (3CA)*, vol. 2, 2010, pp. 522–525.

[28] A. B. Al-Khalil, A. Al-Sherbaz, and S. J. Turner, "Enhancing the physical layer in v2v communication using ofdm-mimo techniques," 2013.

[29] OFDM transmitter and OFDM receiver. http://telcosought.com/4g-ran/ofdm-transmitter-ofdm-receiver/. (accessed: 18.07.2022).

[30] Antenna types. http://www.antenna.be/vm.html. (accessed: 18.07.2022).

[31] D. Eckhoff, A. Brummer, and C. Sommer, "On the impact of antenna patterns on vanet simulation," in *2016 IEEE Vehicular Networking Conference (VNC)*, 2016, pp. 1–4.

[32] sharetechnote. RF sensitivity webpage. https://www.sharetechnote.com/html/RF_Handbook_Sensitivity.html/. (accessed: 18.07.2022).

[33] J. Speiran and E. M. Shakshuki, "Understanding the effect of physical parameters on packet loss in veins vanet simulator," *Procedia Computer Science*, vol. 201, pp. 359–367, 2022.

[34] C. Sommer, S. Joerer, and F. Dressler, "On the applicability of two-ray path loss models for vehicular network simulation," in *2012 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2012, pp. 64–69.

[35] C. Sommer, D. Eckhoff, R. German, and F. Dressler, "A computationally inexpensive empirical model of ieee 802.11p radio shadowing in urban environments," in *2011 Eighth International Conference on Wireless On-Demand Network Systems and Services*, 2011, pp. 84–90.

[36] A. Jirjees, "Vehicular ad hoc networks: Growth and survey for three layers," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7, p. 271 284, 02 2017.

[37] New generation SDR device. https://www.crowdsupply.com/lime-micro/limesdr/. (accessed: 24.07.2022).

[38] A high performance and scalable software- defined radio platform. https://www.ettus.com/all-products/usrp-b200-enclosure/. (accessed: 24.07.2022).

[39] Antenna beamforming techniques. https://www.electronics-notes.com/articles/antennas-propagation/phased-array-antennas/beamforming-beamsteering-antenna-basics.php/. (accessed: 24.07.2022).

[40] T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep learning for launching and mitigating wireless jamming attacks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 1, pp. 2–14, 2018.
[41] Direct Digital Synthesis (DDS): A method used for analog waveform generation. https://www.analog.com/en/analog-dialogue/articles/all-about-direct-digital-synthesis.html/. (accessed: 24.07.2022).
[42] RTTE $(1999/5/EC)$. https://www.eur-lex.europa.eu/legal-content/EN/ALL. (accessed: 24.07.2022).
[43] 89/336/EEC EMC. https://www.standards.iteh.ai/catalog/directive/f8bf5af6-f6d2-4c50-967c-7e09c88e282e/89-336-eec. (accessed: 24.07.2022).
[44] Radio equipment directives $(2014/52/EU)$. https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en. (accessed: 24.07.2022).
[45] V. Milanés and S. E. Shladover, "Modeling cooperative and autonomous adaptive cruise control dynamic responses using experimental data," *Transportation Research Part C: Emerging Technologies*, vol. 48, pp. 285–300, 2014.
[46] D. Jiang and L. Delgrossi, "Ieee 802.11p: Towards an international standard for wireless access in vehicular environments," 06 2008, pp. 2036 – 2040.
[47] SUMO Collisions Outputs. https://sumo.dlr.de/docs/Simulation/Output/Collisions.html. (accessed: 09.12.2021).