



[This is not an article, chapter, of conference paper!]

Vulnerability Analysis of Vehicular Coordinated Maneuvers

Konstantinos Kalogiannis
Networked Systems Security Group
KTH Royal Institute of Technology
konkal@kth.se

Andreas Henriksson
Networked Systems Security Group
KTH Royal Institute of Technology
anhenri@kth.se

Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology
papadim@kth.se

Abstract - Intelligent Transport Systems (ITS) latest standardization efforts focus on a Maneuver Coordination Service (MCS), for automated vehicles to cooperatively perform maneuvers. The goal is to avoid degrading to lower levels of automation, i.e., human input for maneuvering, e.g., when an obstacle ahead needs to be avoided. MCS-equipped vehicles communicate with nearby vehicles that are possibly affected by the impending maneuver, to establish that a maneuver can safely take place. An MCS-equipped vehicle that misbehaves can be catastrophic: transmitting falsified MCS messages or preventing their reception can mislead victim vehicles into aborting a maneuver, being delayed and, worse even, collide. In this work, we investigate the robustness of existing Maneuver Coordination Protocols (MCPs) and analyze the effect of falsification and jamming attacks. Our analysis shows an increased probability for neck injuries, i.e., whiplash, and potentially more severe injuries. As a first step towards thwarting attacks targeting MCPs, we extend MCPs to take into account on-board vehicle sensors, along with MCP messaging, before committing to a maneuver. Our results demonstrate the MCP vulnerability, the improvement thanks to the sensors, and the need to further improve MCP security. We conclude with a road-map towards a resilient MCS.

1 Introduction

Automated Driving (AD) is increasingly adopted: car manufacturers strive to introduce better systems that support not only driver-assisting systems but services based on connected vehicles that automate transportation. Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs) are exchanged by connected vehicles, facilitated by Roadside Units (RSUs). The benefits are: improved road safety, reduced emissions [38] and better traffic management [32]. Efforts by various projects (e.g., TransAID [37] and Imagine [14]) and the European Telecommunications Standards Institute (ETSI) [10, 11] introduced a Maneuver Coordination Service (MCS) and related Maneuver Coordination Protocols (MCPs). In Fig. 1 we illustrate potential scenarios for MCS deployment, where vehicles enter the so-called Transition Area (TA), e.g., a highway-ramp, and coordinate to safely merge in an automated way.

Each vehicle broadcasts its *planned* trajectory, a Maneuver Coordination Message (MCM), that follows the “right-of-way” traffic rules. When a maneuver needs to take place, the vehicle that needs to maneuver sends an MCM with a *desired* trajectory, essentially informing if that trajectory intersects with already planned trajectories of nearby vehicles. The

desired trajectory, in other words the requested maneuver, can be accepted or denied based on the MCM-receiving vehicle’s own needs, e.g., by taking into account passenger comfort or planned arrival time. When a desired trajectory is accepted, both the requesting and accepting vehicles take action: the initiator changes its planned trajectory according to the now accepted desired one, while the other vehicles adjust (e.g., slow down) to follow their new non-interfering planned trajectories. If proven feasible, MCS could also expand to cover other Advanced Driver Assistance Systems (ADAS) services, such as Cooperative Automated Overtaking [5].

Any MCS-ready vehicle can deviate from the prescribed functionality of the MCPs, while network impairments or deliberate attacks, such as jamming, can erase MCP messages. Wrong or badly timed information, or loss of information, can be critical for the maneuver execution and the vehicle and passenger safety. Planned or desired trajectories could be misrepresented, deliberately, to block maneuvers (e.g., preventing a legitimately needed maneuver to merge in a lane or avoid an obstacle), or mislead a victim vehicle to initiate inappropriate, unsafe maneuvers. The consequences can be dire: vehicles could be delayed, their passengers be discomforted by erratic maneuvering or lack thereof, or, worse even, victim vehicles could collide. To further strengthen the adversarial impact, such MCP manipulation can be combined with jamming or other clogging denial of service attacks [17].

Towards thwarting attacks, security for Vehicular Communication (VC) systems has received significant attention, developing a standard approach ([9, 11, 16]) that relies on public key cryptography ([22, 44]). While authenticity and non-repudiation can be valuable in attributing misbehavior, they cannot prevent attacks against MCPs by insiders, i.e., vehicles that have the appropriate credentials but are deliberately modified or compromised by malware. Clearly, external adversaries can, for example, jam too. The challenge is that attackers can manipulate disseminated trajectories to create a false perception of the vehicle neighborhood dynamics. More important, the vulnerability of MCPs is largely unexplored.

Works that validate Cooperative Awareness Messages and verify position neighborhood [12, 13] rely on safety beacons (CAMs) but do not cover trajectories and MCS functionality and needs. Another type of AD, platooning, has received attention: the impact of misbehavior during platoon joins and exits and misbehavior detection were recently investigated [19]. Work for platooning is relevant but it does not address MCS challenges: MCS supports a much broader gamut of situations, maneuvers, and differs significantly in terms of message exchange and execution. None of the ongoing efforts (surveyed in Sec. 2) developing MCPs investigates the impact that attacks

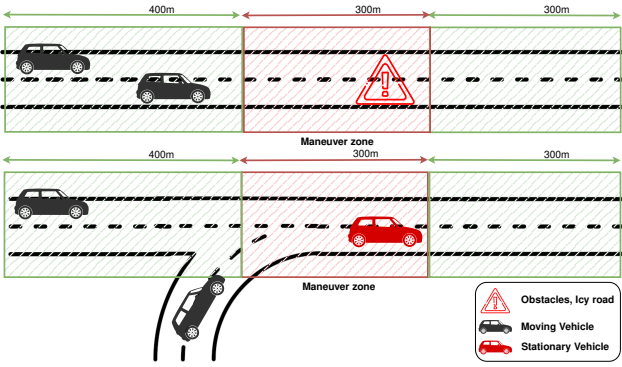


Figure 1: MCP scenarios on the road.

can have on MCS and MCPs.

This is the gap in the literature this paper strives to contribute closing. We show, with the help of detailed cyber-physical simulations, the dangers that can arise for MCS: we perform falsification attacks that manipulate the speed, position and acceleration values embedded in the trajectories; we jam the communication channel during the execution of the MCPs; and we show the effects of packet loss (or of an intelligent jammer) on their performance. We quantify these results by measuring the speed difference during collisions, the safety gap violations that occur during an attack and the lost time for each vehicle on the road.

Given that MCP standardization is work in progress, we explore the common protocol characteristics and how misbehavior attacks affects them. This paper is a first systematic investigation of MCP vulnerability and aspires to help standardization efforts to craft robust protocols and misbehavior detection and mitigation techniques tailored to MCP. It is important to combine accurate sensory data and Misbehavior Detection Schemes (MDSs). Furthermore, short-term monitoring of the actual maneuvers is needed to alleviate a “denial-of-road” misbehavior.

In the rest of the paper, we describe MCS/MCPs and related work (Sec. 2) and we provide the system and adversary model (Sec. 3). These are followed by the overall vulnerability evaluation framework, the metrics we used and the experimental evaluation (Sec. 4). Finally, we provide a road-map for future MCP developments based on our insights (Sec. 5) before concluding (Sec. 6).

2 Background and Related Work

2.1 Background

TransAID [37], delved into the problems that can arise in TAs where Transition of Control (ToC) is required: it identified critical transport safety issues and studied the feasibility of MCPs in different traffic scenarios. In the same project, [6] investigated appropriate MCM generation rules and their expansion from Vehicle-to-Vehicle (V2V) to Vehicle-to-Infrastructure (V2I) communication, termed vehicle to everything (V2X). The standardization of the MCS is not yet concluded thus several proposals are available.

Spatial Time Reservation Procedure (STRP) [31] utilizes reservation shapes, i.e., a road segment needed by the vehicle for a short amount of time, in order to perform a maneuver such as a lane change, lane merge or overtaking. A vehicle that intends to perform a maneuver checks its surroundings with its own sensors, to detect whether there is a conflict, that is, a movement of another vehicle in its intended path. If so, it transmits its reserved road segment. The vehicles only advertise their reserved shapes (or trajectories) when a maneuver needs to take place. This, however, can result in delayed MCP initiation and reduced neighborhood awareness affecting the safety of the ecosystem.

Another proposal investigated the use of Frenet frames [43] as part of a generic MCP that allows lane changes and left and right turns [23]; Frenet frames describe vehicular movements with two polynomials based on the shape of the lane and the relative position of the vehicle in it. An extension allows the coordination of a maneuver among several vehicles when more than one cars need to perform an action [45]. As each vehicle constructs its own global view of the planned trajectories based on the disseminated trajectories, it is possible that several global plans exist in parallel; the solution is to introduce time-out periods when a plan is confirmed. However, all these interactions increase the complexity, as all vehicles need to agree on the maneuver [24].

AutoMCM proposes a seven-message approach for the completion of the MCP [28]. Thanks to acknowledgments and message retransmissions, the protocol is robust to benign packet loss. On the other hand, trajectories are broadcasted only when needed; the result is (for both AutoMCM and STRP) reduced safety. Opel Core [27] allows lane changes that support successive protocol negotiations. When non-communicating vehicles are present, their trajectories are inferred based on the vehicle own (termed hereafter *ego*) sensors. Opel Core also provides an assessment on the impact of maneuver coordination on traffic quality. With the exception of STRP, all the protocols rely on the V2V and V2I (V2X) received information to make a decision. As it will be motivated by our findings, we identify this as a shortcoming and we propose to rectify it by leveraging the ego sensors, similar to STRP, jointly with the V2X for MCP.

2.2 Related Work

Misbehavior analysis in the V2X ecosystem is not new, several works in the literature identified or proposed various types of attacks. A dataset for investigating attack effects, which aims to serve as a common starting point for future research, was proposed in [20]. However, the dataset does not contain any MCP attacks. Falsification and jamming attacks were examined for vehicular platoons [2, 19, 41]: the attack impact ranges from simple traffic delays to extended destabilization and catastrophic results. In our work, we follow a similar methodology in order to analyze attack impact on MCPs. This poses new challenges as it involves not only longitudinal, but also lateral control following the right-of-way rules. In contrast, platooning provides vehicles with a rigid structure, reducing the number of actions vehicles can take, e.g., change lane due to a non-leader request or alter their trajectories outside the formation parameters.

In the scope of maneuver coordination, the possibility of planning secure trajectories, for a robot, under a GPS spoofing attack was studied [26]. In our case, we perform a multi-

Table 1: Relevant MCP Protocols

Principle	Serial MCP	STRP	AutoMCM	Opel Core
Trajectory Structure	Frenet Frame	Reservation shape	Position in time	Gap in time
Transmission Frequency	Fixed interval	When needed	When needed	Fixed interval
Conflicts Detection	Check planned	Check vehicles' motion	Check planned	Check planned
Trajectory request	Attach desired	Send reservation shape	Scenario Advertisement	Send desired
Maneuver Acceptance	Send new planned	Send boolean commit	Send boolean message	Send new planned

tude of falsification attacks, which can be perpetrated without GPS spoofing, altering the position, speed and acceleration of the disseminated trajectories. An investigation on the impact of perception attacks (e.g., sensor blinding and insertion of ghost vehicles) on RSU-assisted highway merging was performed in [15]. The protocols we investigate, as part of the MCS, do not utilize RSUs to perform their maneuvers and our investigation provides an analysis of misbehavior impact regardless of the underlying maneuvering scenario. A high-level threat analysis on potential misbehavior avenues in the context of MCP was performed [29], categorizing attacks based on their impact or feasibility. In our investigation, we cover what is deemed high impact attacks: we expand on the potential falsification attacks (not only high speed values), and experimentally showcase their impact. Further, we investigate the impact of intermittent network connectivity in MCPs, e.g., due to jamming.

3 System and Adversarial Model

3.1 System Model and MCP

Several protocols in the literature tackled the problem of coordinated maneuvers. In this work, we investigate four different protocols to deduce common characteristics and assess them in the presence of malicious actors. In Table 1, we summarize the protocols based on: trajectory structure, transmission frequency, conflict detection, trajectory request and maneuver acceptance.

Both Frenet frames and reservation shapes include the same type of data (position, speed, acceleration). Despite the MCMs format differences, or the steps required to accept a maneuver, all four protocols ultimately require accurate data to function nominally; the structure of the message does not affect the decision-making process. Our investigation considers the impact of the attacks, not the comparison of the protocols themselves. STRP calculates the trajectories of its neighborhood based on sensor data, while all other protocols require each vehicle to disseminate its planned trajectory to its neighborhood. Considering the requirement for constantly disseminating planned trajectories ([10,40]) and their ability to detect conflicts in the available trajectories, we chose Serial MCP and STRP as the basis for our protocol implementation. While the Serial MCP follows the ETSI guidelines, it does not make use of any sensor data.

In order to bridge this gap, we utilize the functionality provided by STRP. Each vehicle first calculates any intersections between the disseminated trajectories and then performs the same calculation based on its own sensors (shown in Procedure 1 for vehicles ahead). Starting from line 12, each vehicle needs to make sure that the last timesteps included in the Frenet frames, in the received MCM (otherT), match the projected time in the vehicle's own trajectory (myT); thus, any network delays are compensated by predicting the missing speed, position and acceleration based on the currently available in-

Procedure 1 isIntersectingAhead

```

1: procedure ISINTERSECTING(myT, otherT)
2:   for all  $myT_{timesteps}$  do
3:     safeGap = ACCSafe(myT.speed, otherT.speed)
4:     gap = (otherT.pos) - (myT.pos)
5:     if gap < safeGap && sameLane then
6:       return true
7:     end if
8:   end for
9:   return false
10: end procedure
11: procedure CHECKVEHICLES Ahead(myT, otherT)
12:   if  $myT_{times} \neq otherT_{times}$  then
13:     PredictMissingDistances()
14:   end if
15:   found = isIntersecting(myT, otherT)
16:   if NOT found then
17:     sensorT = PredictT(Sensors, Sensorp, Sensora)
18:     found = isIntersecting(myT, sensorT)
19:   end if
20:   return found
21: end procedure

```

formation in the MCM. At this point, the vehicles check that at no future point the distances become smaller than the permitted ones dictated by the Adaptive Cruise Control (ACC) controller (in steps 1.2–1.8). The same procedure is repeated for the sensor trajectory (in steps 1.17–1.18), solely computed based on the vehicle's sensors, thus circumventing MCP data falsification. Our goal, in that regard, is to verify the safety guarantees that sensors can provide to the soon-to-be maneuvering vehicle.

Vehicles on the road are expected to follow the right-of-way rules. In addition, MCP-executing vehicles need to decide if they would allow a maneuver to take place near them or not. A vehicle may decide that the cost of changing its trajectory to enable the desired maneuver is too high (e.g., it would miss a timed rendezvous) or too uncomfortable for its passengers, or simply unsafe. For that purpose, cost functions for traversing intersections and changing maneuvers were proposed [8, 30]. Equations 1-3 apply a "penalty" for speed and acceleration in order to have a metric for the deviation from the nominal planning of the vehicles. First, for speed the cost is:

$$C_{speed} = w_{i1} \cdot (u_0(t) - u_{ref}(t))^2 \quad (1)$$

where w_{i1} is the non-negative penalty for speed, u_0 corresponds to the current speed at time t and u_{ref} corresponds to the new required speed for the maneuver.

For acceleration, the cost of sudden velocity changes, unwanted to preserve the comfort of the passengers, is:

$$C_{acc} = w_2 \cdot a(t)^2 \quad (2)$$

where w_{i2} describes the penalty value for the required acceleration, $a(t)$. The total cost is calculated as the sum of the two:

$$C_{total} = C_{speed} + C_{acc} \quad (3)$$

In an effort to position the vehicles at appropriate distances, i.e., the gap between the maneuvering vehicles and the vehicles adjusting to allow the maneuver (without loss of generality, the right and left lane vehicles accordingly), we calculate the left-lane's vehicles insertion time as:

$$t_l = t_r + \frac{l_R}{u_r} - \frac{l_R - \text{spacing} - l_v}{u_l} \quad (4)$$

where t_l and t_r correspond to the insertion times for the left and right lane respectively; l_R and l_v define the length of the first stretch of the road and the length of the vehicle; and u_r, u_l , which correspond to the traveling speeds of the vehicles for the left and right lanes respectively. Finally, spacing corresponds to the longitudinal distance between the vehicles on the left and the vehicles on the right lanes (the different values are given in Table 2).

3.2 Adversary Model

Adversaries can be either internal, i.e., vehicles on the road that possess valid certificates, or external, vehicle-, drone-mounted or road-side static devices without credentials. Internal attackers can perform falsification attacks in order to cause a disturbance or collisions. External attackers can jam or clog their neighborhood with a Denial of Service (DoS) attacks. Adversaries cannot break cryptographic algorithms. In addition to VC systems typical assumptions ([35, 36]) we take into account the rationality of the attacker: collision-induced attacks that involve the misbehaving vehicle are considered sub-optimal/unwanted, as it was introduced in [19] for vehicular platoons.

Directly related to MCS/MCPs, we perform falsification attacks on the disseminated trajectories by altering the position, speed and acceleration information contained in the MCMs. Our attacks target common characteristics in all the MCPs, mainly the kinematic values. Thus, our investigation is independent of the chosen protocol. Moreover, we take into account adversaries capable of jamming the communication medium, considering: (i) brute-force jamming, suppressing all communication and (ii) selective jamming, interfering to drop selected MCP packets (thus being harder to detect [1]). Jamming results either in outright exclusion of the victim from the MCP or it deteriorates the victim's (distorted) perception.

4 System Evaluation and Results

We first detail the simulation setup (Sec. 4.1) and the metrics (Sec. 4.2) used in our system evaluation. We summarize our results (Sec. 4.3) and then present in a detailed manner our analysis of the attack impact on safety; in terms of collisions the adversary can cause (Sec. 4.4); the resultant intra-vehicle distances and align it with the sensor integration (Sec. 4.5). We finish with the trip time effect from the falsifications (Sec. 4.6).

4.1 Simulation Setup

We implement the protocols and the attacks using Veins [33], an open source vehicular communication systems simulator based on OMNeT++ [34]. The mobility scenarios were implemented using SUMO [3]. Table 2 shows different simulation and experimental parameters used during our testing. The right and left lane speeds are consistent with speeds in real life for different traffic densities [39]. All vehicles in our tests used an ACC controller provided by SUMO and we set the frequency for the MCMs to 5 Hz. To test the viability of the protocols and examine the distances needed for the vehicles

Table 2: Simulation & Experimental Parameters

Parameters	Value	Parameters	Value
Right lane	12.5, 25 m/s	Targeted Jamming	R_0
Left lane (for right: 12.5)	16.5, 20.5, 24.5, 28.5, 32.5 m/s	Selective Jamming / drop rate	0, 25, 50, 75 %
Left lane (for right: 25)	29, 33, 37, 41 m/s	Position Attack (m)	10, -10, -30, -50, -100
Sensor range	30 (backward) and 250 (forward) m	Speed Attack (m/s)	1.1, 1.2, 1.3, 1.4, 1.5, 2
MCM Frequency	5 Hz	Acceleration Attack (m/s ²)	2.6, -4.5
Sensors	$\epsilon_p^{V2V} = 1m, \epsilon_a^{V2V} = 0.1m/s, \epsilon_a^{V2V} = 0.01m/s^2, \epsilon_p^{RAD} = 0.1m, \epsilon_s^{RAD} = 0.1m/s$	Spacing	10, 30, 50 m
Car-following model	ACC	Cost Weights (V, A, Brakes)	1, 1, 0.5

to avoid collisions, we set the vehicular sensors at a range of 30 m (backward-facing; Short-Range Radars (SRR) used for checking cross traffic) and 250 m (forward-facing; Long-Range Radars (LRR) used by ACC) [46].

In order to investigate on the role of the sensors of the maneuvering vehicles, we insert the vehicles periodically using equation 4. This allows us to not only experiment with different vehicle spacing, which could change the end results, but also to measure the effect that the sensors have on MCPs. In our experiments we assume that the rear-view sensor is clear of obstructions that could hide a vehicle and that it can correctly classify objects in range, as vehicles. Finally, to approximate real-world sensors, we introduce errors for the radar, the Global Positioning System (GPS) receiver and the wheel spin sensor.

For the attack scenarios, all falsified values (except speed) correspond to relative changes of actual kinematic values of the adversarial vehicle. For the speed attack, positive values represent a speed multiplier, whereas negative values are a speed divisor; i.e., a value of -2 corresponds to dividing the current speed by 2. All falsification attacks are performed by the first vehicle in the left lane (denoted as $L0$) for two reasons. If $L0$ behaves according to the MCS specification, the right-to-left lane-change maneuver will either be completed as planned, or, if there is no space, the right-lane vehicle would need to communicate with the next vehicle on the left ($L1$), the attacker, resulting in similar behavior as the one we will demonstrate. On the other hand, in the scenarios considered here, left-lane vehicles do not need to perform a lane change, thus right-lane MCMs are considered benign. However, in Sec. 5 we discuss possible effects of misbehavior originating from the right lane. Finally, we chose four different values for the percentage of messages dropped by a selective jammer, ranging from 0-75%, to examine the effect of different packet loss rates.

When a safety violation is identified, we perform an additional experiment where the vehicle has to perform an emergency brake. In a real-world scenario, this could be the result of a sudden appearance of an object; or of more nefarious circumstances, e.g., the result of a falsification attack on the vehicle. Finally, we set different weights for the cost function (define in Sec. 3.1): a weight of 1 for speed and acceleration; a weight of 0.5 (or 50%) for braking. Engaging the brakes in their full capacity would bring discomfort to the passengers. Breaking when a collision is imminent is handled by the ACC controller; the aforementioned weights apply only for deciding if the cost for agreeing to a maneuver is acceptable.

4.2 Metrics

Our analysis utilizes five metrics. We characterize each attack with a boolean *violation* value: if an attack results in unsafe gaps between vehicles, as perceived by the ACC controller, we mark it as a violation. To quantify the impact that collisions

have on the vehicles/passengers, we calculate the speed difference (ΔV) between the colliding vehicles. To motivate the discussion further, we annotate the speeds needed for potential injuries [4, 18]. In order to show the effects on the vehicles' trip we measure the total vehicle trip time, the time loss due to the MCP and finally, the attack impact on the nominal trip time, calculated as $ATI = \frac{Time_{attack} - Time_{nominal}}{|Time_{nominal}|} * 100$.

4.3 Summary of Findings

Our investigation produced several interesting results:

- Speed attacks can cause a significant number of violations because they are also part of the safety gap calculation performed by each vehicle (See Table 3).
- Misbehavior for spacing of 10 meters between vehicles is thwarted when the vehicles use their own sensors; however, in certain cases (See Fig. 5) it exposes the vehicle to different attacks.
- Delaying the completion of a safety-critical maneuver, by any means, can create safety violations or accidents when the maneuver finally takes place, due to the increased speed differences between the vehicles (See Figs. 5 and 6.c).
- Jamming the right-lane results in a near-perfect collision-free result when sensors are used; nonetheless it can lead to delayed or unsafe maneuvers (See Figs. 6 and 7).
- It is possible for the maneuvering vehicles to cause a "denial-of-road" on the left lane if they do not physically perform the accepted maneuver (See Fig. 8).

4.4 Collision Impact

Fig. 2 shows the collision impact for vehicles traveling at speeds 12.5 and 28.5 m/s on the right and left lane respectively. We denote with different symbols the intra-vehicle distances (square for distance of 10, circle for 30 and triangle for 50 meters) and with colors the vehicles that collided. We assign a color to each vehicle (with the first right-lane vehicle denoted as $R0$) and we define the inner color to represent the collision victim, whereas the surrounding corresponds to the collider. As part of this metric, we depict with horizontal lines the thresholds for injuries based on the ΔV of the crash. For whiplash, we set the line at 12.5 km/h; a middle point between the 10 and 15 km/h required for such an injury [4]. For rear-end collisions, the risk of serious injury becomes 10% at 55 km/h [18]. We can observe that by performing a (selective) jamming attack, a positional attack with a (relatively) negative falsified value or a (relatively) negative speed an attacker can cause more potent collisions for vehicle $R0$. $R0$ uses either outdated or falsified information when deciding to perform a maneuver. Coupled with the small vehicular distances, they lead to accidents. However, all these attacks include the attacking vehicle in the collision; a rational attacker would avoid such events in order to either preserve itself, or its compromised victim.

Fig. 3 compares the different collision results between the scenarios of one or two maneuvering vehicles. One can notice that in Fig. 3.a we do not observe any collision when the distances are over 50 meters. The vehicles have enough spacing

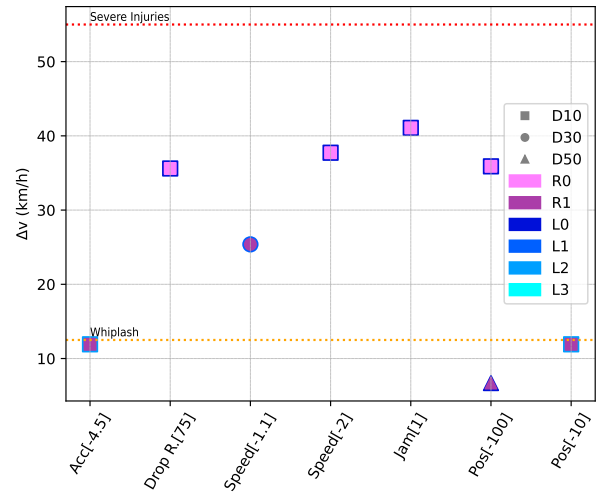


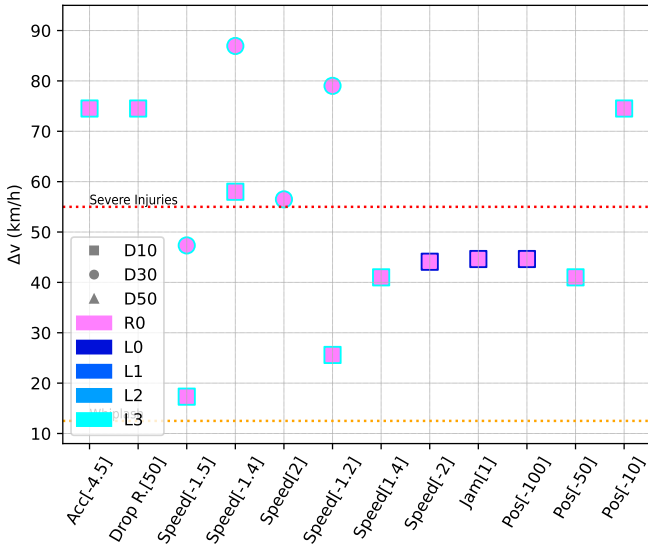
Figure 2: Collision Impact: Misbehavior at 12.5(R)/28.5(L) m/s.

between them to either complete the maneuver on their own (because their trajectories do not overlap) or to not be catastrophically affected. In contrast, when we add a single extra vehicle (Fig. 3.b), we can see that it involved in multiple collisions; some of them very potent, with a collision impact hovering at 90 km/h! Moreover, we observe that in both cases most of the collisions involve vehicles downstream, i.e., the maneuver was performed after the attacker passed, leading to optimal collisions (border color is not deep blue). The acceleration and jamming attacks produce several collisions with their severity ranging from 20-50 km/h. Finally, we can see that in Fig. 3.b most of the collisions concern vehicle $R1$ because the vehicle changes lane just after $R0$ making it the victim of $L3$.

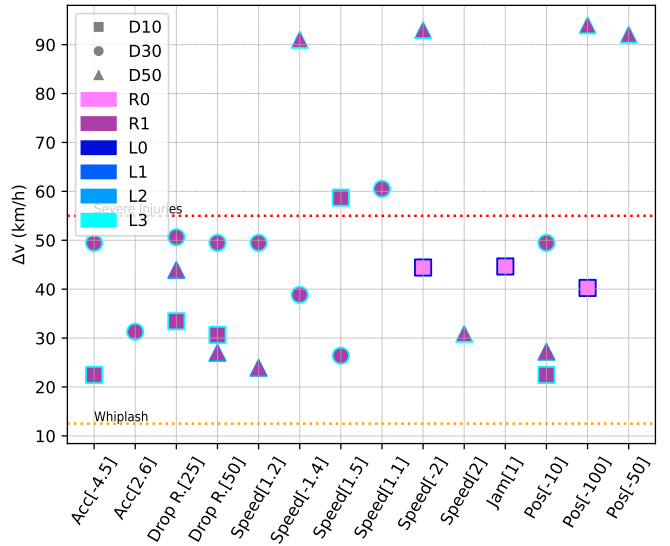
4.5 Safety and Sensors

Table 3 illustrates the effectiveness of the sensory input under all our experiments. Each column represents one type of attack with the number representing the percentage of experiments that led to a safety violation. Without sensors, 74% of them incur a safety violation to at least one of the vehicles on the road. The highest number comes from the speed falsification attack; 254 tests had a violation from a total of 324, resulting in 78%. The received speed information is crucial, as it is part of the minimum safety gap calculation performed by ACC, the other values being the speed and braking capabilities of the receiving vehicle (i.e., the vehicle's own values). Thus, smaller values affect both the received trajectory and the minimum gap required by the vehicle before performing a lane change. The position falsification also creates a substantial problem; out of the possible 135 experiments, 100 cause a violation (shown as 74% in the table). Because the positional data are used by all the protocols described in Table 1, this type of attack is deemed highly dangerous. When we utilize the sensors, all types of attacks diminish substantially with a total of 28% causing a violation. This utilization thwarts most of the attacks that occur for distances less than 30 meters, which is the range of our backward facing radar.

When we introduce a second maneuvering vehicle ($R1$), the total number of experiments that cause a violation changes to



(a) Single Maneuvering Vehicle



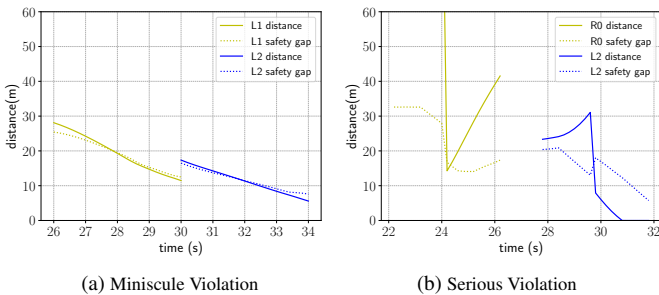
(b) Two Maneuvering Vehicles

Figure 3: Collision Impact: Maneuvering vehicles at 25(R)/41(L) m/s without sensors.

Table 3: Safety violations due to misbehavior

Sensors	Maneuvers	Jamming	Stealth Jamming	Position	Speed	Acceleration	Total
No	1	85%	69%	74%	78%	47%	74%
	2	96%	86%	90%	86%	92%	84%
Yes	1	48%	34%	17%	31%	25%	28%
	2	74%	53%	26%	48%	44%	43%

from 74% to 84% and from 28% to 43%. The former corresponds to MCP without sensors, whereas the latter uses them to avoid unsafe conditions. This increase is not abnormal, in cases where the leading right vehicle changes lane safely, its follower needs to: first wait for it to perform its maneuver, reducing the time it would take for the left lane vehicles to approach, and then slow down which increases the speed difference with the left-lane vehicles (further reducing the time). This combination, creates unsafe conditions not only for the vehicle on the right, but potentially to vehicles on the left. If the left vehicle accepts a maneuver, the speed difference can lead to excessive braking potentially affecting the vehicles downstream.



(a) Miniscule Violation

(b) Serious Violation

Figure 4: Safety Violation Intricacies: a case of 2 maneuvers under an acceleration attack.

It should be noted that the violation metric encompasses all scenarios where the safety gap is violated; however, this is not necessarily catastrophic. Fig. 4 shows the safety violation of two vehicles when maneuvers take place under an acceleration

attack. In Fig. 4.a we can see that the safety violation is triggered for vehicles L1 (approaching L0) and L2 (approaching R2). Both vehicles on the right enter the lane and trigger a safety violation for the left lane vehicles (for L1 the distance is ≈ 1.3 meters). Nonetheless, the vehicles are able to avoid a collision if their predecessor performs an emergency break. In Fig. 4.b, we can see a similar situation for R0 (approaching L0). For L2, the situation is more dire; even though an accident is averted (the distance to R1 is less than one meter), any emergency braking from its predecessor would lead to an accident.

To further demonstrate the sensor impact, in Fig. 5 we show the collision results for multiple attack scenarios when the vehicles use (or not) their sensors as part of the MCP. In Fig. 5.a most of the collisions happen for the 10 meters intra-vehicles distance; these collisions are absent when we use the MCP that utilizes the sensors. Interestingly, by enabling the use of sensors we cause two different severe-injury inducing collisions. In both cases, R0 is not able to change lane until its speed is significantly less than the left lane (and continues to decrease due to the object ahead). Remember that at the end of the maneuvering zone there is a safety-critical hazard (See Fig. 1 in Sec. 1). This speed difference ultimately leads to the collisions.

4.6 Trip Effects

Fig. 6 demonstrates the falsification attack impact on the trip completion time, for the 25 and 29 m/s right and left lane speeds, using the Attack Time Impact (ATI) metric (See Sec. 4.2). Negative impact implies two things depending on the vehicles: for right-lane vehicles, it means that the attack caused the vehicle to perform the maneuver faster (potentially causing a safety violation) thus reducing the trip time; for the left-lane vehicles it implies that the maneuver took place downstream compared to the non-attacked case leading to faster trip completion time.

In Fig. 6.a we can see that L0 is largely unaffected as the sensors do not allow a maneuver in such close distances. L1, on the other hand, gains time as the maneuver of the second

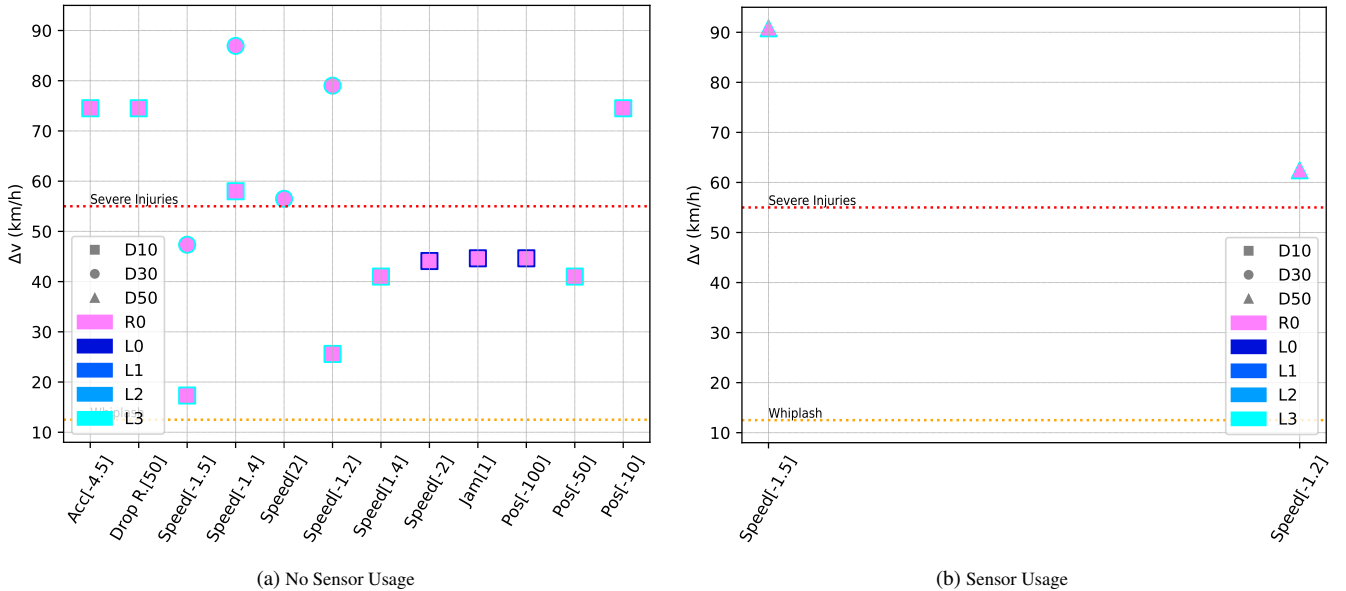


Figure 5: Collision Impact: Sensor effectiveness at 25(*R*)/41(*L*) m/s.

vehicle *R1* always takes place downstream (except for the extreme negative position and speed cases); leading also *L2* and *L3* to be delayed. Concerning the second maneuvering vehicle, all of the scenarios cause it to finish the trip later, ranging from 5-22%.

When the vehicles' spacing is 30 meters (Fig. 6.b), *R0* and *R1* both finish their trip faster. *R0* manages to maneuver in a leading position on the left lane which leads *R1* to finish ahead of *L1* gaining up to 15%; *L1* subsequently has a delay between 4-22%.

For the 50 meters distance case (Fig. 6.c), *R0* is completing most of the maneuvers on time because the left-lane vehicles are further back. The same applies for *R1* except for the negative position attacks; the left-lane trajectory covers further back on the road, yet still intersecting, forcing the car to slow down more. Similarly, the positive speeds cause *R0* to perform the maneuver later forcing the vehicles on the road to reduce their speed and increase their total trip time by 3-15%. For the positive acceleration attack we can spot an outlier in our results. For distance 50, the attack causes the right-lane vehicle to delay changing lane even further. The maneuver is accepted, but the increased acceleration forces new MCP exchanges until the speeds become low enough (where high acceleration does not translate to relatively big speed differences) for the vehicle to change lane. The total trip time lost in this case is $\approx 40\%$.

Finally, the jamming/drop rate cases also show differences between the three distances. When the distance is small, i.e., 10 meters, the dropped signals cause a slight delay resulting in *R1* to lose a place to *L1*. When the distance is 30 meters, the maneuvering vehicles finish the maneuvers faster, using only their sensor-generated trajectories, but their lane-change trigger a safety violation to the incoming vehicle. For the big intra-vehicle distance (50 meters), a complete jam or some network interference are completely ineffective. The attacks do not cause any time delays.

Fig. 7 compares the time loss for each the vehicle due to the maneuver, i.e., the time lost due to the vehicle traveling below the ideal speed. In both cases, *L0* loses the least amount

of time. In Fig. 7.a, where there is only one vehicle on the right lane, we observe that high drop rates (75%) cause an actual delay for *L0*; the network affected vehicle, *R0*, performs a maneuver immediately. The vehicles downstream (from *L1*) perform similarly. When we introduce a second maneuvering vehicle (Fig. 7), we see an immediate delay for vehicles *L2* and *L3* because a MCP is not finished from the second vehicle. When the packets are dropped and the radar-generated trajectories from the left do not intersect with its own, *R1* finishes the maneuver earlier.

5 Discussion

In an effort to steer future developments in the space of MCS we discuss several emerging key points. We group those points into four categories based on their timely appearance during a maneuver coordination.

Sensors effectiveness: Considering the straightforward, if not arguably the obvious, improvement that sensors can provide to MCS, it is important that the information they provide are as accurate as possible. Weather conditions can affect their performance [42] or vehicles can be partially hidden, by obstacles or other vehicles, making their detection and classification harder [47]. Further, trajectories generated through sensory input is bound to be less accurate; nonetheless, they should not lead to any safety violations. The topic of generating trajectory predictions in adversarial environments is actively investigated in the literature [48].

Maneuver-aware MDS: Despite the improved safety due to the utilization of sensors, further mechanisms are needed in order to avoid safety violations and collisions. Simple plausibility checks can be the first step in detecting such misbehavior [21], but more advanced MDS capable of detecting intelligently crafted attacks should be considered. However, it is important that these mechanisms function during the maneuvering process in order to avoid false blame attribution [19].

Physical maneuver completion: A vehicle can request a ma-

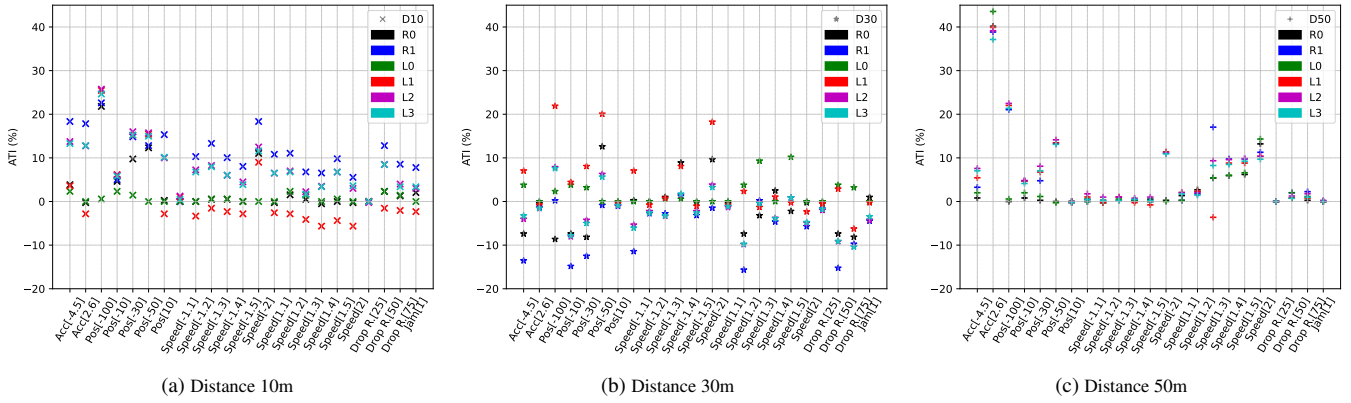


Figure 6: Travel Time Impact (%): Attacks for speeds 25(R)/29(L) m/s with sensors enabled.

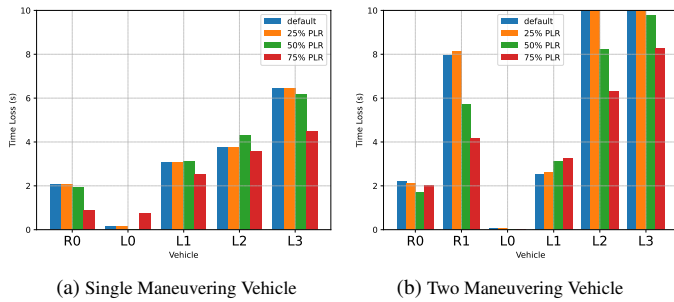


Figure 7: Packet Loss Trip Impact: 30 meters spacing at 25(R)/33(L) m/s with sensors enabled.

never and complete the protocol as expected; however, the vehicle may not physically perform the maneuver. This, not only forces its neighbors to alter their trajectory, possibly causing traffic instability, but also can lead to a type of “denial-of-road” situation as shown in Fig. 8. Fig. 8.a illustrates the position of the vehicles in each timestep, while Fig. 8.b shows their speeds. The vehicles on the left lane accept the maneuvers and start slowing down. Yet, this continues because the initiating vehicle (yellow) never physically changes lane, forcing the receiving vehicle to slow down even more due to a new MCM. The vehicles in the left lane come at, almost, a complete stop. The first vehicle on the left is stationary for ≈ 30 seconds. The lock is broken when the left lane vehicle, due to the small forward speeds, manages to reach a point ahead of the “maneuvering” vehicle.

A solution to this problem could be the introduction of a time component as part of the cost function. Delaying the trip above a threshold should cause the vehicle to reject further MCMs. Unfortunately, such a proposal could clash with safety critical maneuvers. Potential countermeasures would include the usage of sensor data to validate that an accepted maneuver actually took place or that the vehicle is moving on the disseminated path; e.g., through the use of kalman filters [25] or by requiring a physical challenge-response [7]. In the long-term detected misbehavior should be reported to the relevant authorities, as all Vehicular Ad-hoc Network (VANET) messages are signed.

Feasible overheads: Finally, potential solutions that thwart the MCP vulnerabilities need to impose little overhead due to the

time-critical nature of the scenarios. The MCS by itself requires the dissemination of multiple messages per second for each vehicle (e.g., every 200ms). Thus, it is important that any solution that mitigates the problem takes into account the required timescales and the capabilities of currently available On-Board Units (OBUs).

6 Conclusion

Automated driving solutions require a thorough experimental investigation of misbehavior that can be catastrophic. In this work, we make a first step in analyzing safety violations due to falsification and jamming attacks targeting MCPs. We also investigated the effect, in terms of time loss, that degraded network reception can have on the overall MCP functionality of MCPs. Even with the use of the ego vehicle sensors, attacks against the maneuver coordination can still cause collisions. Based on our results, we outlined a road-map towards a safe MCS. As future work, we will expand our analysis with more advanced attacks, a multitude of different driving scenarios that include an heterogeneous mix of vehicles, such as trucks, and an MCP misbehavior detection scheme towards secure and safe VC enabled AD systems.

Acknowledgments

Work supported by the Swedish Foundation for Strategic Research (SSF) SURPRISE project and the KAW Academy Fellowship Trustworthy IoT project.

References

- [1] Adnan Ahmed, Usman Ashraf, Fatima Tunio, Kamalrulnizam Abu Bakar, and Mohammed Saeed AL-Zahrani. Stealth jamming attack in wsns: Effects and countermeasure. *IEEE Sensors Journal*, 18(17):7106–7113, 2018.
- [2] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt. Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving. *IEEE Comm. Mag.*, 53(6), Jun. 2015.

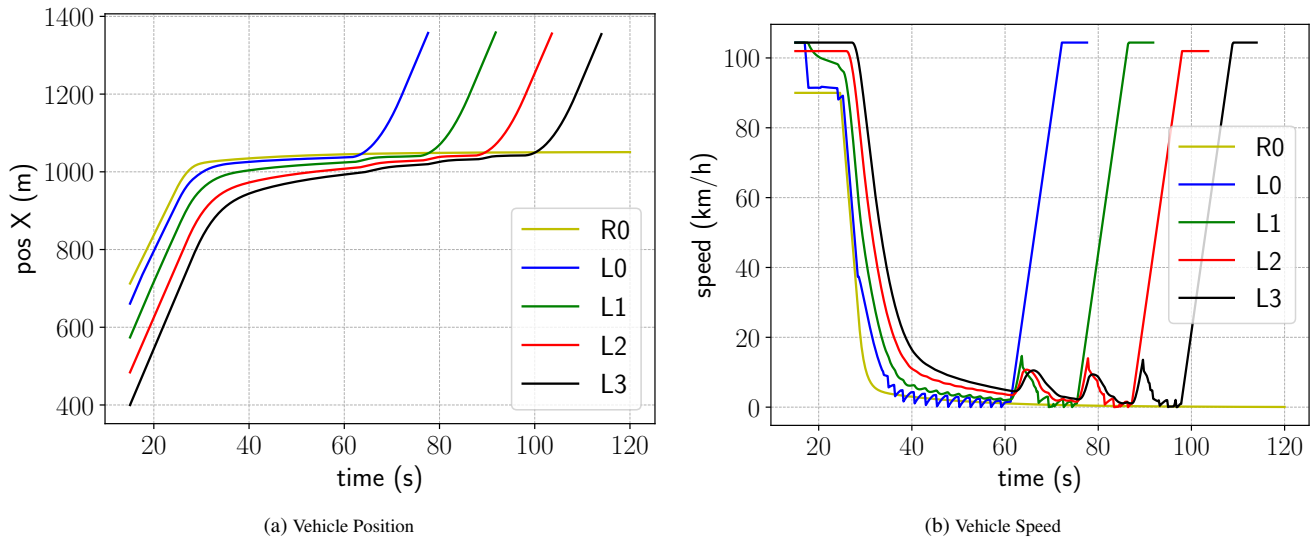


Figure 8: Road Denial by a Maneuvering Vehicle.

- [3] Michael Behrisch, Laura Bieker, Jakob Erdmann, and Daniel Krajzewicz. SUMO - Simulation of Urban Mobility: An Overview. In *The International Conference on Advances in System Simulation*, Barcelona, Spain, Oct. 2011.
- [4] WHM Castro, M Schilgen, S Meyer, M Weber, C Peuker, and K Wörtler. European spine society—the acromed prize for spinal research 1997: Do “whiplash injuries” occur in low-speed rear impacts? *European Spine Journal*, 6:366–375, 1997.
- [5] Car 2 Car Communication Consortium et al. Guidance for day 2 and beyond roadmap. *Car2Car Communication Consortium, C2CCC WP, 2072*, 2019.
- [6] Alejandro Correa, Robert Alms, Javier Gozalvez, Miguel Sepulcre, Michele Rondinone, Robbin Blokpoel, Leonhard Lücken, and Gokulnath Thandavarayan. Infrastructure support for cooperative maneuvers in connected and automated driving. In *2019 IEEE Intelligent Vehicles Symposium (IV)*, pages 20–25. IEEE, 2019.
- [7] Connor Dickey, Christopher Smith, Quentin Johnson, Jingcheng Li, Ziqi Xu, Loukas Lazos, and Ming Li. Wiggle: Physical challenge-response verification of vehicle platooning. *arXiv preprint arXiv:2209.00080*, 2022.
- [8] Tiago C. dos Santos and Denis F. Wolf. Bargaining game approach for lane change maneuvers. In *2019 19th International Conference on Advanced Robotics (ICAR)*, pages 629–634, 2019.
- [9] ETSI. Intelligent Transport Systems (ITS); Security; Stage 3 Mapping for IEEE 1609.2. https://archive.org/details/etsi_ts_102_867_v01.01.01/page/n9/mode/2up, Jun. 2012.
- [10] ETSI-TR-103-439. Intelligent Transport Systems (ITS); Intelligent Transport Systems (ITS); Multi-Channel Operation study; Release 2. Technical report, ETSI, Oct. 2021.
- [11] ETSI-TR-103-478. Intelligent Transport Systems (ITS); Vehicular Communications; Informative report for the Maneuver Coordination Service. Technical report, ETSI, Oct. 2022.
- [12] Andreas Festag, Panos Papadimitratos, and Tessa Tielert. Design and Performance of Secure Geocast for Vehicular Communication. *IEEE Transactions on Vehicular Technology (IEEE TVT)*, 59(5):2456–2471, June 2010.
- [13] M. Fiore, C. Ettore Casetti, C. F. Chiasserini, and P. Papadimitratos. Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing (IEEE TMC)*, 12(2):289–303, February 2013.
- [14] European Center for Information and Communication Technologies (EICT GmbH). Imagine, “imagine – solutions for cooperative driving”.
- [15] Mohamed Hadded, Pierre Merdrignac, Sacha Duhamel, and Oyunchimeg Shagdar. Security attacks impact for collective perception based roadside assistance: A study of a highway on-ramp merging case. In *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pages 1284–1289. IEEE, 2020.
- [16] IEEE SA. IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. *IEEE Std 1609.2*, Mar. 2016.
- [17] Hongyu Jin and Panos Papadimitratos. Dos-resilient cooperative beacon verification for vehicular communication systems. *Ad Hoc Networks*, 90:101775, 2019.
- [18] Chris Jurewicz, Amir Sobhani, Jeremy Woolley, Jeff Dutschke, and Bruce Corben. Exploration of vehicle impact speed–injury severity relationships for application in safer road design. *Transportation research procedia*, 14:4247–4256, 2016.
- [19] Konstantinos Kalogiannis, Mohammad Khodaei, Weaam Mostafa Nemr Mohamed Bayaa, and Panos Papadimi-

- tratos. Attack impact and misbehavior detection in vehicular platoons. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 45–59, 2022.
- [20] J. Kamel et al. VeReMi Extension: A Dataset for Comparable Evaluation of Misbehavior Detection in VANETs. In *IEEE ICC*, Dublin, Ireland, Jul. 2020.
- [21] Joseph Kamel, Mohammad Raashid Ansari, Jonathan Petit, Arnaud Kaiser, Ines Ben Jemaa, and Pascal Urien. Simulation framework for misbehavior detection in vehicular networks. *IEEE transactions on vehicular technology*, 69(6):6631–6643, 2020.
- [22] M. Khodaei et al. SECMAE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems. *IEEE TITS*, 19(5):1430–1444, May 2018.
- [23] Bernd Lehmann, Hendrik-Jörn Günther, and Lars Wolf. A generic approach towards maneuver coordination for automated vehicles. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 3333–3339, 2018.
- [24] Bernd Lehmann and Lars Wolf. Safety analysis of a maneuver coordination protocol. In *2020 IEEE Vehicular Networking Conference (VNC)*, pages 1–8, 2020.
- [25] Chunfeng Liu, Gang Zhang, Weisi Guo, and Ran He. Kalman prediction-based neighbor discovery and its effect on routing protocol in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 21(1):159–169, 2019.
- [26] Yin-Chen Liu, Gianluca Bianchin, and Fabio Pasqualetti. Secure trajectory planning against undetectable spoofing attacks. *Automatica*, 112:108655, 2020.
- [27] Viktor Lizenberg, Daniel Bischoff, Youssef Haridy, Ulrich Eberle, Steffen Knapp, and Frank Koester. Simulation-based evaluation of cooperative maneuver coordination and its impact on traffic quality. In *SAE WCX: World Congress Experience Digital Summit*, 2021.
- [28] Masaya Mizutani, Manabu Tsukada, and Hiroshi Esaki. Automcm: Maneuver coordination service with abstracted functions for autonomous driving. In *2021 IEEE International Intelligent Transportation Systems Conference (ITSC)*, pages 1069–1076, 2021.
- [29] Jean-Philippe Monteuis, Jonathan Petit, Mohammad Raashid Ansari, Cong Chen, and Seung Yang. V2x misbehavior in maneuver sharing and coordination service: Considerations for standardization. *arXiv preprint arXiv:2211.02579*, 2022.
- [30] Nikolce Murgovski, Gabriel Rodrigues de Campos, and Jonas Sjöberg. Convex modeling of conflict resolution at traffic intersections. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 4708–4713, 2015.
- [31] Matthias Nichting, Daniel Heß, Julian Schindler, Tobias Hesse, and Frank Köster. Space time reservation procedure (strp) for v2x-based maneuver coordination of cooperative automated vehicles in diverse conflict scenarios. In *2020 IEEE Intelligent Vehicles Symposium (IV)*, pages 502–509, 2020.
- [32] Arash Olia, Saiedeh Razavi, Baher Abdulhai, and Hossam Abdelgawad. Traffic capacity implications of automated vehicles mixed with regular vehicles. *Journal of Intelligent Transportation Systems*, 22(3):244–262, 2018.
- [33] Open Source Vehicular Network Simulation Framework. veins.car2x.org, Jul. 2019.
- [34] OpenSim Ltd. OMNeT++. <https://www.omnetpp.org/>, Jun. 2017.
- [35] Panagiotis Papadimitratos, Levente Buttyan, Tamás Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung, and Jean-Pierre Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications magazine*, 46(11):100–109, 2008.
- [36] Panagiotis Papadimitratos, Virgil Gligor, and J-P Hubaux. Securing vehicular communications-assumptions, requirements, and principles. 2006.
- [37] Julian Schindler, Baldomero Coll-Perales, Xiaoyun Zhang, Michele Rondinone, and Gokulnath Thandavarayan. Infrastructure-supported cooperative automated driving in transition areas. In *2020 IEEE Vehicular Networking Conference (VNC)*, pages 1–8, 2020.
- [38] Christos Stogios, Dena Kasraian, Matthew J Roorda, and Marianne Hatzopoulou. Simulating impacts of automated driving behavior and traffic conditions on vehicle emissions. *Transportation Research Part D: Transport and Environment*, 76:176–192, 2019.
- [39] Gokulnath Thandavarayan, Miguel Sepulcre, and Javier Gozalvez. Generation of cooperative perception messages for connected and automated vehicles. *IEEE Transactions on Vehicular Technology*, 69(12):16336–16341, 2020.
- [40] TransAID-D5.2. V2X-Based Cooperative Sensing and Driving in Transition Areas. Technical report, TransAID, Mar. 2020.
- [41] R. van der Heijden et al. Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC). In *IEEE VNC*, pages 45–52, Torino, Italy, Nov. 2017.
- [42] Jorge Vargas, Suleiman Alsweiss, Onur Toker, Rahul Razdan, and Joshua Santos. An overview of autonomous vehicles sensors and their vulnerability to weather conditions. *Sensors*, 21(16):5397, 2021.
- [43] Moritz Werling, Julius Ziegler, Sören Kammel, and Sebastian Thrun. Optimal trajectory generation for dynamic street scenarios in a frenet frame. In *2010 IEEE International Conference on Robotics and Automation*, pages 987–993. IEEE, 2010.
- [44] W. Whyte et al. A Security Credential Management System for V2V Communications. In *IEEE VNC*, pages 1–8, Boston, MA, Dec. 2013.

- [45] Wenbo Xu, Alexander Willecke, Martin Wegner, Lars Wolf, and Rüdiger Kapitza. Autonomous maneuver coordination via vehicular communication. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pages 70–77, 2019.
- [46] Chen Yan, Wenyuan Xu, and Jianhao Liu. Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *Def Con*, 24(8):109, 2016.
- [47] Masaru Yoshioka, Naoki Suganuma, Keisuke Yoneda, and Mohammad Aldibaja. Real-time object classification for autonomous vehicle using lidar. In *2017 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*, pages 210–211. IEEE, 2017.
- [48] Qingzhao Zhang, Shengtuo Hu, Jiachen Sun, Qi Alfred Chen, and Z Morley Mao. On adversarial robustness of trajectory prediction for autonomous vehicles. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 15159–15168, 2022.