A Secure and Cooperative Departure Protocol for Connected Automated Platoons

Farah-Emma Braiteh, Davy Tse, Ounas Yhia, Francesca Bassi, Rida Khatoun

A Secure and Cooperative Departure Protocol for Connected Automated Platoons

Farah-Emma Braiteh[1,3,4], Davy Tse[2], Ounas Yhia[2], Francesca Bassi[3], and Rida Khatoun[4]

[1]farah-emma.braiteh@ampere.cars
[2]{davy.tse, ounas.yhia}@etu.sorbonne-universite.fr
[3]{francesca.bassi, farah-emma.braiteh}@irt-systemx.fr
[4]{rida.khatoun, farah-emma.braiteh}@telecom-paris.fr

***Abstract*—Cooperative and automated vehicular platoons enhance road safety and reduce traffic congestion by enabling vehicles to travel closely together and maneuver in a synchronized manner. This synchronization relies on vehicle-to-vehicle (V2V) communications, which, while beneficial, also introduce vulnerabilities to potential cyberattacks. In this paper, we introduce a new cooperative and secure protocol for platoon departures, focusing specifically on the departure phase. We demonstrate that, without security measures, a vehicle attempting to leave the platoon could exploit the leave messages of the platoon protocol and introduce attacks that may disrupt the formation of the platoon or even jeopardize its stability. To mitigate this risk, we propose data consistency measures that protect both the stability and integrity of the platoon. Simulations conducted using Plexe simulator validate the security of the proposed protocol through rigorous security assessments.**

***Index Terms*—CACC, Cooperative platooning, Leave Platoon Maneuver, Misbehavior detection and reaction, V2V.**

I. Introduction

Connected and automated vehicles (CAVs) are reshaping transportation through real-time communication and coordination, enhancing safety, efficiency, and traffic flow. This technological shift is driving rapid adoption, with the U.S. connected car fleet growing from 84 million in 2021 to a projected 305 million by 2035, making it the world's largest market for these vehicles [1]. A cooperative vehicular platoon consists of a group of CAVs that travel together in a coordinated manner, forming a string of closely spaced vehicles. These vehicles cooperate by exchanging V2V messages to ensure synchronized operations. Each vehicle in the platoon is equipped with Cooperative Adaptive Cruise Control (CACC) [2], an advancement of Adaptive Cruise Control (ACC) [3]. CACC leverages both V2V communication and sensor data to perceive the environment, enabling vehicles to autonomously manage their longitudinal and lateral movements. This coordination allows for tight spacing between vehicles and facilitates complex group maneuvers.

By maintaining close distances, the platoon achieves reduced air resistance for trailing vehicles, which enhances fuel efficiency. Additionally, synchronized braking and acceleration improve road safety by decreasing the likelihood of accidents. As a result, cooperative vehicular platoons offer significant benefits, including energy savings and safer roadways.

The cooperative platooning service relies on several key functions, as outlined in [4], which can be classified into three main phases: enrollment phase functions facilitate the creation of the platoon and the integration of new members [5], drive-in phase functions ensure the stable operation of a platoon with fixed members, and departure phase functions enable a vehicle to exit the platoon without compromising its integrity. All of these functions depend on the continuous exchange of V2V data to maintain the cohesion and coordination of the platoon, making secure communication between vehicles essential.

CAVs are authenticated through a Public Key Infrastructure (PKI) [6], which enables them to exchange signed V2V messages containing kinematic data and maneuver intentions. This authentication ensures that only verified vehicles can participate in cooperative activities within the platoon. While the platoon is safeguarded against cyberattacks from non-PKI-authenticated vehicles, it remains susceptible to threats posed by authenticated but malicious vehicles. Such vehicles can inject false data into signed V2V messages or perform unauthorized maneuvers, potentially jeopardizing the safety and stability of the platoon.

Upon reviewing the literature, we found that despite advancements in connected and automated vehicle technology, there is a lack of robust cooperative platooning protocols to securely address critical scenarios, such as a vehicle's departure from the platoon. A decentralized cooperative departure protocol would enable a vehicle to communicate its intention to exit the platoon and change lane, immediately or after a brief delay [7], allowing other members to prepare accordingly and reorganize the platoon's formation after the departure. If the vehicle chooses to exit and change lanes, the remaining vehicles would need to adjust their gaps after the departure. In [4], we presented various types of attacks that can impact a platoon, including false information exchange, false in-platooning information, false V2X data injection, velocity and position falsification, DoS jamming, and Sybil attacks [8]. In this paper, we focus on attacks carried out by authorized vehicles already in the platoon during the execution of the leave protocol, which could have serious consequences on the platoon's formation and operations. We define the platoon formation as the organizational structure of the platoon, comprising a specified list of authorized members capable

of exchanging platooning-related information. Modifying the formation involves adding or removing vehicles from the group of authorized CAVs within the platoon.

Contribution: In our work, we primarily focus on the function that enables a platoon member to leave the group and change lanes. We address a particular type of attacker: PKI-authenticated platoon members who send signed messages, followed a procedure to join the platoon, and have been driving without issues within the platoon. Our study yields several original contributions:

- We develop a decentralized communication protocol that facilitates a vehicle's exit without disrupting the platoon's formation.
- We identify vulnerabilities, particularly the risk of fake requests or maneuvers that could destabilize the platoon's formation.
- We design security measures to mitigate the potential impact of such risks.
- We validate the protocol by simulations across various scenarios, proposing platoon reactions to respond to misbehavior to ensure its proper operation.

While our analysis primarily focuses on the scenario where a vehicle attempts to leave from the middle of the platoon, the proposed solutions are broadly applicable, extending to the simpler case of a vehicle leaving from the rear of the platoon.

The remainder of the paper is structured as follows: Section II offers an overview of the V2V communication protocols relevant to our research; Section III explains the Leave Protocol, along with the types of messages exchanged; Section IV presents the attack models relevant to the departure phase; Section V outlines the security measures we have implemented to detect these attacks; Section VI demonstrates the impact of the attacks and the improvements to the platoon's operation after integrating the security checks; and Section VII concludes the paper and suggests potential improvements and directions for further work.

II. Related Works

In this paper, we develop a cooperative decentralized leave protocol. To the best of our knowledge, existing communication protocols are either non-cooperative, lacking V2V data exchange, or centralized. The non-cooperative protocols are outside the scope of this work as they only rely on sensor data to adjust the movements of vehicles in the platoon. In centralized protocols, whether cooperative or not, a single entity, such as the platoon leading vehicle or a server, is responsible for initiating and approving maneuvers, as well as issuing instructions to platoon members for their execution. Allowing a single entity to manage the entire platoon introduces a significant vulnerability, as it creates a single point of failure. Details on the differences between centralized and decentralized approaches are discussed in [9], where the authors focus on platooning protocols for merging and splitting operations. The literature contains numerous examples of cooperative approaches. For example, Farag et *al.* [10] introduced cooperative protocols for joining and leaving a platoon but did not provide details on the V2V messages or their content. Additionally, they assigned the responsibility of managing maneuver requests and issuing instructions to the platoon leader. The authors in [11] presented an interesting protocol to manage long platoons, where vehicles may fall outside the communication range of the leader. In such cases, they suggest selecting a new virtual leader, within the DSRC range, to manage the platoon. Maiti et *al.* [12] presented an algorithm for platoon splitting, where the leader decides when and where to split the platoon. The leader is also responsible for updating the list of members when the platoon formation changes. In [13], the exit maneuver is also coordinated by the platoon leader. This vehicle is responsible for receiving and processing exit requests, preparing instructions for the departing vehicle and the remaining members, and ultimately updating the platoon. These studies indicate that a significant number of cooperative protocols are centralized, relying on the leader for coordination.

Due to the limited number of cooperative platooning protocols, there is a notable lack of cybersecurity studies addressing them to date. Petrillo *et al.* [14] studied false position injection attacks in platooning. They compare the real inter-distance between vehicles, calculated using V2V data, to an expected value based on the leader's velocity. If discrepancies are detected, the suspicious vehicle's data is excluded from control calculations. In their model, the leader's kinematic data is used as a reference. Biroon *et al.* [15] explored false data injection attacks in CACC and propose a detection model operated by the platoon leader. This model identifies ghost vehicles, attackers pretending to be platoon members, that alter inter-vehicle distances to either split the platoon or trigger collisions. The leader compares estimated and observed velocity and acceleration values of platoon members to identify an attack. These studies, along with others we've discussed in [4], demonstrate that the few existing platooning protocols addressing cybersecurity rely on the leading vehicle or its kinematic data to detect attackers, resulting in a centralized and therefore vulnerable security approach.

In [16] the authors analyze resilient control in Vehicle Cooperative Platooning Systems (VCPSs) under Denial of Service (DoS) attacks. Their method improves robustness against cyber threats while preserving operational integrity. An optimization problem is formulated to set limits on DoS attack duration and frequency, ensuring safe and effective operation. However, challenges include implementation complexity, estimation errors, and scalability issues. The authors in [17] analyze vehicular platooning challenges under uncertainties and attacks, proposing a resilient control framework with a logical data processor for DoS detection. However, assumptions about vehicle dynamics, unknown nonlinearities, and V2V communication limitations may compromise overall performance, potentially leading to instability and delays in real-world scenarios. In [18] the authors present a novel method for detecting internal attacks in vehicular platoons under dynamic conditions. The method's effectiveness in real-time is not guaranteed, as processing or communication delays could

hinder timely attack detection, risking safety. The authors in [19] examine the detection and estimation of position sensor deception attacks in vehicular platoons, emphasizing the risks posed by external information sources such as compromised GPS and camera data. They introduce a linearized model for vehicle longitudinal dynamics and validate their detection method through analysis and simulations, demonstrating its potential to enhance platoon resilience. However, the model may oversimplify complex behaviors of real-world vehicle dynamics. This can limit its effectiveness in diverse or extreme driving conditions and lower attack detection accuracy in practical applications.

These platooning research works highlight the need for further research and testing to propose decentralized and cooperative protocols, while also enhancing the security and robustness of platooning protocols and solutions.

III. Leave Protocol: Initial Design

The novelty of our protocol lies in its decentralized, secure, and cooperative approach. The protocol is formulated based on the following scenario: A platoon of N authenticated and authorized CAVs has already been formed and has been operating in close formation for an extended period. At a given moment, one of the platoon members, regardless of its position within the platoon, decides to exit the platoon and transition to the leftmost lane as shown in Fig.1.

We define as Leader the first vehicle in the platoon, at a considered moment. Our leave protocol is illustrated in Fig. 2 for departures from the middle. The complete protocol is composed of two parts, the Leave Procedure and the Update Platoon Formation Procedure, described in Sections III-B and III-C, respectively. Notice that once the protocol begins, the platoon considers itself engaged in an ongoing cooperative operation until the Update Platoon Formation Procedure is completed.

A. V2V Data Types Customized for Platooning Operations

All vehicles exchange Cooperative Awareness Messages (CAM) [20] mainly containing vehicle kinematic data (position, velocity, etc). Since the standard CAM is not specifically designed for platooning, we have incorporated an additional container to notify nearby vehicles about the presence of the platoon. Similar to the standard CAM, the extended version is broadcast. To ensure effective communication, we have opted to broadcast these messages at a high frequency.

The standardized V2V message types lack adaptability for platooning operations. Therefore, we have developed several types of messages specifically tailored for platooning operations:

- Platooning messages: While operating within the platoon, vehicles multicast platooning messages to one another. These messages include critical information about the platoon, such as its ID, velocity, number of members, maximum capacity, and details related to each member, including their position and role within the platoon.

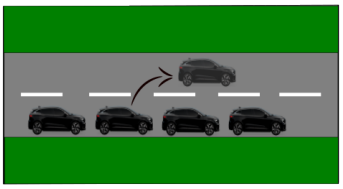


Fig. 1: Leave and Change Lane

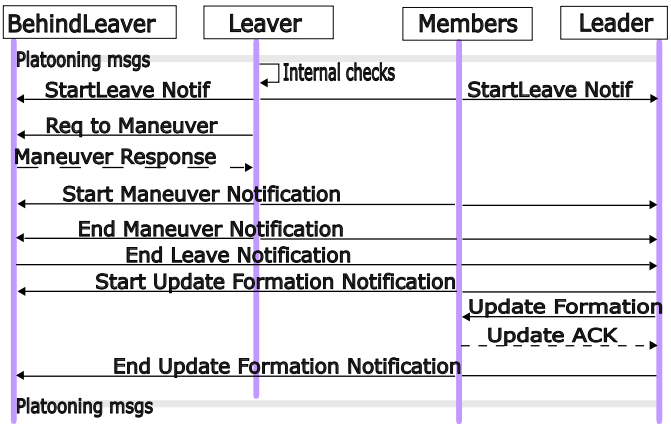


Fig. 2: Leave From the Middle

- Notification messages: These messages are multicast to announce the initiation or completion of a platooning procedure, such as Leave, Update, Join, and others.
- Maneuver messages: Unicast messages sent between members to initiate a maneuver request or to respond to an incoming maneuver request.
- Update messages: Unicast messages exchanged between individual members of the platoon to request or confirm the platoon formation update.

B. Leave Procedure

In the platoon, vehicles exchange platooning messages to coordinate their actions. When a vehicle, the Leaver, decides to exit the platoon, it first verifies that the platoon is not already engaged in any other maneuver, update, or other operation. If this condition is satisfied, the Leaver multicasts a *Start Leave* notification to all platoon members, indicating its intention to depart.

We first examine a scenario where the Leaver is not the last vehicle in the platoon. The Leaver has to exit and change lanes: it sends a *Leave Maneuver* request to the vehicle directly following (BehindLeaver in Fig. 2). When the BehindLeaver is prepared to adjust its position and driving behavior to facilitate the maneuver, it responds affirmatively to the request. Upon receiving a positive response, the Leaver announces the initiation of its maneuver. As soon as the Leaver moves to the adjacent lane, it multicasts the *End Maneuver Notification*. Then, the BehindLeave notifies the end of the leave procedure.

All remaining platoon members update their member list by removing the departing vehicle, following the procedure detailed in III-C.

At this point, the gap closure occurs automatically as it is based on sensor data. Consequently, whenever a vehicle leaves the platoon, the following vehicles close the gap to maintain a consistent time gap, and thus inter-vehicle distance, between one another. The pseudo code for the Leave from the Middle Procedure is presented in Algorithm 1.

This procedure can be straightforwardly adapted to the case when the Leaver is the last vehicle in the platoon. In this case, there is no *Request to Maneuver* and the Leaver sends the *Start Maneuver Notification* just after the *Start Leave Notification*. After completing the lane change, the Leaver notifies all platoon members of the maneuver's conclusion. At this point, the vehicle immediately in front (FrontLeaver) sends the *End Leave Notification.*

C. Update Platoon Formation Procedure

Upon completion of the leave procedure, the platoon readjusts its formation. To ensure that each vehicle updates its member list, the Leader notifies all platoon members of the formation update by sending an *Update formation* message to every vehicle in the platoon and waits for its confirmation (*Update ACK*). Once all members have issued valid confirmations, the Leader declares the update complete and the leave protocol concludes.

Note that, although in our scenario we have designated the Leader as the vehicle responsible for verifying the formation update, this role may alternatively be assumed by the preceding vehicle in the case of a departure from the end, or by the following vehicle in the case of a departure from the middle.

During the update procedure, all members are assumed honest and without any intent to deliberately update the formation incorrectly. Additionally, this work does not address scenarios involving communication failures. The update procedure pseudo code is shown in Algorithm 2.

IV. Protocol Vulnerabilities and Attack Models

We focus on identifying potential internal attacks that may originate from the actions of the departing vehicle, through a systematic vulnerability analysis of the leave procedure. Other platoon members are presumed trustworthy.

Based on the Leaver's expected state transitions, illustrated in Fig. 3, we analyze the sequence of messages exchanged, the alignment between the Leaver's actions and these messages, and any potential deviations the vehicle might exploit.

A. Unauthorized Maneuver

This type of attack occurs when the departing vehicle changes lanes without completing the established Leave protocol described in Section III. Such an attack can manifest in several ways: the departing vehicle may bypass the leave procedure entirely, abruptly leave the platoon without following the required steps, or fail to adhere to the conditions stipulated in the protocol. For instance, the vehicle may depart even

Algorithm 1 LeaveFromMiddle

Input: Platoon information, member list, member data
Output: Updated platoon formation with Leaver removed
//Internal Check and Announce Departure
if $isEngagedInManeuver \neq 1$ **then**
    multicastToPlatoon("StartLeaveNotification", Leaver_ID)
else
    return "Platoon is engaged in another operation"
    wait()
end if
//Leave Maneuver Request
sendMessage("RequestToLeave", Leaver_ID, BehindLeaver_ID)
Wait for Response, Initiate Maneuver
response ← receiveMessage("Leave.ACK", BehindLeaver_ID, Leaver_ID)
if response = "ACK" **then**
    multicastToPlatoon("StartManeuverNotification", Leaver_ID)
    $isEngagedInManeuver \leftarrow 1$
else
    return "Maneuver denied. Leaving deferred."
    wait()
end if
//Perform Maneuver
Leaver.performLaneChange("LeftLane")
multicastToPlatoon("EndManeuverNotification", Leaver_ID)
closeGapAutomatically()
//Complete Maneuver and Update Member Lists
multicastToPlatoon("EndLeaveNotification", BehindLeaver_ID)
for all member in Platoon.Members **do**
    if $member \neq Leaver$ **then**
        member.removePlatoonMember(Leaver)
        member.updateFormation()
    end if
end for
Platoon.decreasePlatoonMemberCount()

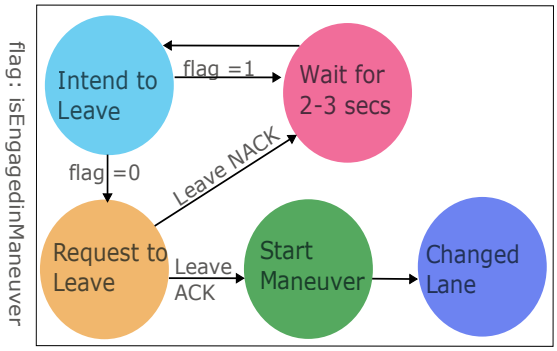


Fig. 3: Leaver State Transition Diagram

Algorithm 2 UpdateFormationCheck

```
1: Input: Platoon
2: Output: Updated platoon formation with Leaver removed
3: //Start confirming the update from the first member
4: multicastToPlatoon("StartUpdateFormationNotification", Leader_ID)
5: sendMessage("RequestToUpdateFormation", Leader_ID, Platoon.Members[1])
6: //Propagate the request to the next members
7: currentMemberIndex ← 1
8: while currentMemberIndex ≤ Platoon.Members.count do
9:    response ← receiveMessage("UpdateFormation.ACK", Platoon.Members[currentMemberIndex], Leader_ID)
10:   if response = "ACK" then
11:      //Send request to the next member
12:      currentMemberIndex ← currentMemberIndex + 1
13:      if currentMemberIndex ≤ Platoon.Members.count then
14:         sendMessage("RequestToUpdateFormation", Leader_ID, Platoon.Members[currentMemberIndex])
15:      else
16:         //Finish the process
17:         multicastToPlatoon("EndUpdateFormation", Leader_ID)
18:      end if
19:   else
20:      //Retry sending the request to the same member
21:      sendMessage("RequestToUpdateFormation", Leader_ID, Platoon.Members[currentMemberIndex])
22:   end if
23: end while
```

when the platoon is engaged in another operation, or when the following vehicle is not prepared to accommodate the maneuver. This disrupts the orderly execution of the leave procedure and poses a significant threat to the stability and safety of the platoon.

Impact of the attack: This disrupts the platoon formation, as the members remain unaware of the vehicle's departure and, as a result, fail to update their member list. An extra, non-existent member will be included in the calculations. If the departing vehicle remains nearby, it will continue receiving the multicast messages, assuming it doesn't change its certificate during this time.

B. Fake Maneuver

Through vulnerability analysis, we identify that the protocol is most vulnerable at the critical step, which occurs while awaiting the *EndManeuver* Notification from the departing vehicle.

1) Fake Leave Maneuver: The first variant of the attack occurs when the departing vehicle announces its departure then its lane change by sending the *EndManeuver* Notification, while physically remaining within the platoon.

Impact of the attack: Once the vehicle sends the *EndManeuver* Notification, it is no longer considered a platoon member and will eventually be removed from the member list. While vehicles are equipped with CACC, the vehicle's continued physical presence may still lead to incorrect calculations and subsequent errors in movement adjustments. Additionally, it could pose a risk by manipulating other platoon members or potentially hijacking the role of another vehicle.

2) Malicious Leave Maneuver and Denial of Service (DoS): In this attack, the departing vehicle falsely announces the start of the maneuver, triggering the platoon's *isEngagedInManeuver* flag to be set to '1'. However, the vehicle stays in the platoon and never sends the *EndManeuver* Notification. After a predefined interval of time, the platoon reinitializes the *isEngagedInManeuver* flag. Once the platoon recovers from this state, the Leaver inadvertently repeats the same procedure of false announcement.

Impact of the attack: The ongoing false state can lead to further disrupting the platoon's operations. All other operations will be automatically rejected, as the platoon is mistakenly engaged in an ongoing maneuver. Meanwhile, the malicious vehicle remains within the platoon and is still considered a legitimate member. It can influence critical decisions or even impersonate other vehicles, further destabilizing the platoon and compromising its safety and coordination.

V. Enhancing Protocol Security with Countermeasures

After analyzing the vulnerabilities of our protocol to the attacks outlined in Section IV, we enhanced its security by incorporating multiple validation checks at various stages of the protocol.

A. Sensor Data Verification

Given that the vehicles are equipped with CACC, we incorporated a periodic sensor data verification to our protocol. Each vehicle continuously monitors the distance to the preceding vehicle and, when equipped with rear sensors, also evaluates the distance to the following vehicle.

Because of the CACC control, the unplanned displacement of a platoon member on the adjacent lane, as in the case of the unauthorized maneuver attack described in Section IV-A, will result in the appearance of an unexpected gap in the platoon formation. If a vehicle detects a gap, in front or behind, that equals or exceeds the platoon's interdistance plus the vehicle's length, it concludes that a member has departed. It then alerts the rest of the platoon to start the update procedure.

As mentioned earlier, this work defends the platoon against departing vehicles, assuming that the remaining vehicles are innocent and not compromised.

B. V2V and Sensor Data Consistency Verification

Whenever a vehicle requests to leave, the following vehicle and/or the preceding vehicle conduct V2V and sensor data consistency checks from the moment the departure is announced until the maneuver is completed.

If the vehicle departs without confirming the maneuver's conclusion, the vehicles performing the consistency checks will detect the discrepancy and promptly notify the platoon to update its formation accordingly. However, if the vehicle remains in the lane but incorrectly announces the end of the maneuver, the platoon will split into two separate platoons at the leaver's position. The Leader of the second platoon will be the vehicle immediately following the misbehaving leaver.

C. Limit on Departure Attempts

In addition to the two verification measures described in this section, we imposed a limit of three departure attempts within a short time window of 5 seconds. If the vehicle exceeds this limit, it is classified as misbehaving. This limit applies to other platooning operations as well.

The platoon reacts to this situation based on the vehicle's position; if the vehicle remains in the lane, the platoon will be split into two parts. However, if sensor data confirm that the vehicle has changed lanes, it will be removed from the platoon formation.

VI. Simulation Results and Analysis

To evaluate our leave protocol, (see Section III), and the effectiveness of the security verifications, (see Section V), we simulated a series of scenarios in the order provided in Table I. This table summarizes the impact of the attacks on the platoon's functionality, first in the absence of countermeasures, and then with the countermeasures implemented. The platooning protocol and the countermeasures were implemented using the Plexe-API and simulated with SUMO. We simulated a platoon of five vehicles, where v_0 serves as the Leader, v_2 as the attacker, and v_4 as the tail. The simulation parameters are provided in Table II.

TABLE II: Simulation Parameters

Parameter	Value	Parameter	Value
N members	5	Controllers	CACC
N max	10	Lane width	3.3 m
Speed	110 km/h	Radar resolution	1

A successful attack is defined as one that destabilizes the platoon's formation relative to the real configuration or disrupts the normal operation of the platoon.

The departure phases are detailed in Table III and illustrated in Figures 4, 5, and 6. The simulation results are discussed in the following subsections.

TABLE III: Overview of Departure Phases in Figures 4, 5, 6

Phase	Event	Key Actions in the Leave Protocol
`A`	Maneuver initiation	The leaving vehicle initiates the lane change and is expected to send a StartManeuver Notification.
`B`	Maneuver completion and gap closure initiation	The leaving vehicle is expected to complete the lane change and send an EndManeuver Notification. The platoon begins the gap closure and updates its formation.
`C`	Gap closure and formation update	The gap is fully closed, and the platoon formation is updated.

A. Unauthorized Leave Maneuver

Vehicle v_2 executes an unannounced departure from the platoon. It changes lanes, as depicted in Fig. 4, without notifying the platoon of its departure. As described in Table III, the maneuver is initiated at ``A'' and completed at ``B''. The results of the simulation at ``C'' show that:

- Without Security Checks: While the platoon successfully closed the gap created by v_2's departure using CACC, it failed to update its formation to reflect the change. Although v_2 departed and changed lanes, the set of platooning members participating in message exchanges remained consistent before and after the attack, as shown in Fig. 4a. As a result, v_2 remained involved in platooning decisions and operations, creating inconsistencies and potential vulnerabilities in the system.
- With Sensor Data Verification enabled: Vehicle v_3 detected v_2's departure when the distance between v_3 and its preceding vehicle (v_1 now) exceeded the platoon's interdistance and the length of v_2 (5m + 3m). In response, v_3 announced v_2's End of Leave and initiated a request to update the platoon formation. Following the formation update, the set of platooning members involved in message exchanges reflects the corrected formation, as shown in Fig. 4b, ensuring that v_2 no longer participates in operational decisions.

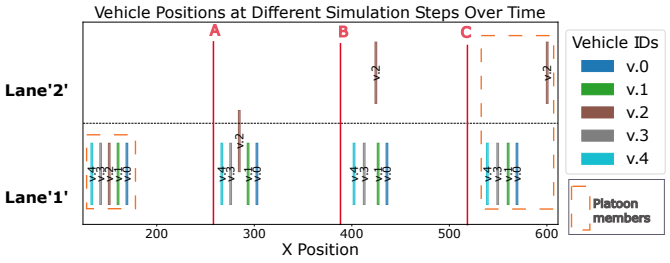
B. Fake Leave Maneuver

Vehicle v_2 follows Leave protocol to announce its departure and sends the Maneuver Notifications; however, it physically stays in the platoon and doesn't change lanes as shown in Fig. 5. As described in Table III, the maneuver is expected to be initiated at ``A'' and completed at ``B''. At ``C'', the simulation results were as follows:

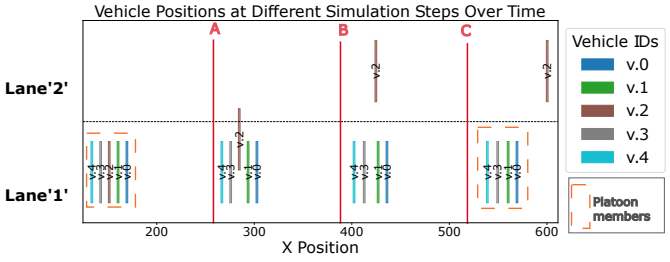
- Without Security Checks: Following the EndManeuver notification sent by v_2, the update procedure was executed, removing v_2 from the list of members, as depicted in Fig. 5a. However, v_2 didn't change lanes and remained within the platoon, posing a significant risk as it could disrupt the coordinated movement. The platoon now consists of four vehicles, but an intruder vehicle, v_2, remains among them.
- With V2V and sensor data consistency enabled: Vehicle v_3 detected an inconsistency in the CAM data and End of Maneuver announced by v_2. Specifically, the reported

TABLE I: Attack Scenarios and Their Impact on the Platoon

Attack Name	Description	Countermeasures	Impact on the Platoon	Attack Result
Unauthorized Leave Maneuver	The attacker leaves the platoon and changes lane without announcing its intention of departure.	None	Platoon closes the gap using CACC without performing the update procedure. The platoon formation becomes inconsistent with the list of physically present members.	Success
		Sensor Data Verification	The departure is detected, prompting the closure of the gap and the reconfiguration of the platoon formation.	Failure
Fake Leave Maneuver	The attacker announces its departure and sends End Maneuver Notification; however, it physically stays in the platoon.	None	The platoon members update the formation, but an intruder vehicle — the leaver — is still present between them. The interdistance between platoon members becomes inconsistent.	Success
		V2V and Sensor Data Consistency Verification	The attack is detected. The platoon splits into two smaller platoons, effectively disregarding the presence of the attacker positioned between them.	Failure
Malicious Leave and Denial of Service	The attacker announces its departure but doesn't transmit an EndManeuver Notification. This behavior is repeated multiple times, disrupting normal operations.	None	The platoon remains continuously engaged in its current operation; consequently, any other platooning operation, such as joining, are automatically rejected.	Success
		Data Consistency and Departure Attempts Limit Verification	The false state is detected. The platoon recovers its initial state within 3 seconds after the departure announcement, a join request can be accepted. After three unsuccessful exit attempts, the platoon splits into two smaller platoons, disregarding the attacker positioned in between.	Failure

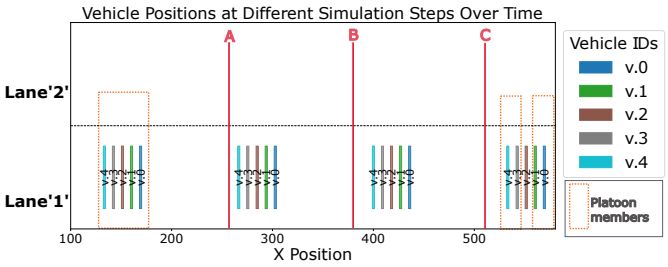


(a) v.2's Unauthorized Maneuver - Without Any Checks

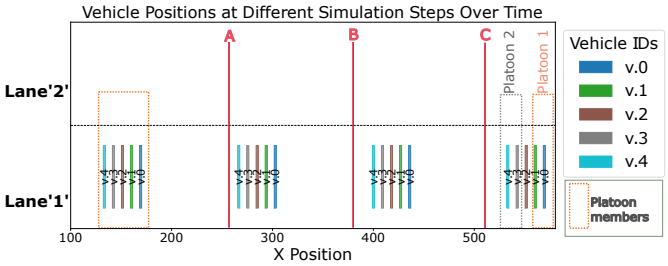


(b) v.2's Unauthorized Maneuver - With Sensor Data Verification

Fig. 4: Unauthorized Maneuver



(a) v.2's Fake Maneuver - Without Any Checks



(b) v.2's Fake Maneuver - With V2V and Sensor Data Consistency Verification

Fig. 5: Fake Maneuver

y-positions before and after the End of Maneuver notification correspond to the same lane, and no significant gap was detected following the announcement. In response, v_3 initiated a request to split the platoon at the position of v_2. As a result, the platoon was split into two separate formations: the first one before v_2, and the second one after v_2, as shown in Fig.5b. This ensures isolating the attacker, v_2, and maintaining the operational integrity of the platoons.

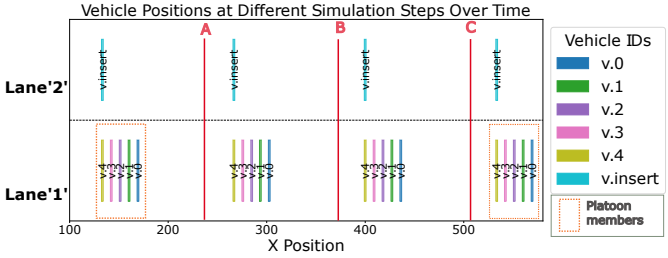
C. Malicious Leave and DoS

Vehicle v_2 announces the beginning of a Leave Maneuver, without transmitting the End of the Maneuver Notification. It waits for a few seconds and repeats the same process.

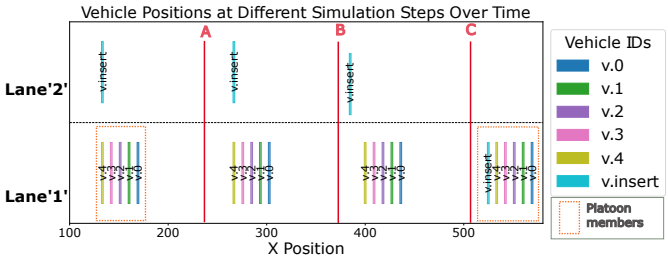
- Without Checks: Upon receiving the StartManeuver notification, the platoon set its `isEngagedInManeuver` flag to '1'and kept it set to '1'with every subsequent leave attempt announced by v_2. As a result, when a

nearby vehicle $v_{.insert}$ tried to join the platoon, its request was immediately rejected, preventing it from joining, as shown in Fig. 6a.

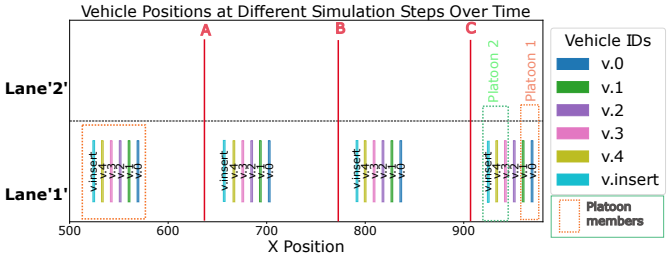
- With Data Consistency and Departure Attempts limit enabled: A few seconds after not receiving the End-Maneuver notification and detecting the presence of v_2 in the platoon through its CAM position and sensor data of platoon members, the platoon reset its `isEngagedInManeuver` flag to '0'. When $v_{.insert}$ repeated its join request shortly afterward, the request was accepted, and it joined the platoon, as shown in Fig. 6b. Subsequently, v_2 repeated this process more than three times, leading the platoon to remove v_2 from its formation. The platoon was then split into two separate platoons, as demonstrated in Fig. 6c.



(a) Without any Checks



(b) With Data Consistency Check



(c) With Departure Limit Check

Fig. 6: Fake Maneuver and DoS

VII. Conclusion and Future Work

We presented a cooperative and leader-independent Leave protocol and analyzed various attacks, including unauthorized, fake, and malicious maneuvers, which compromise the platoon's formation and operations. In response, we introduced countermeasures that strengthen the protocol's formation and operations security by mitigating attacks and preserving the platoon's integrity. Through simulations, we demonstrated that integrating these countermeasures into the protocol effectively detects attacks, allows the platoon to recover from false states, and supports the implementation of corrective actions.

Our findings underscore the critical role of real-time security checks to ensure a secure and functional platooning system, even in the presence of malicious actors. However, the proposed protocol operates under the assumption that all platoon members, except for the leaver, are trustworthy. Future research will focus on addressing this assumption to evaluate trust in members and protect the platoon against internal attacks. Another important area for future exploration would be conducting a comprehensive performance evaluation to assess the scalability of the protocol, considering factors such as the system's ability to efficiently handle an increasing number of platoon members and maintain security and operational integrity under varying conditions.

Acknowledgments

This work has been supported by the French government under the "France 2030" program, as part of the Cybersecurity for Trusted Mobility (CTM) project at the SystemX Technological Research Institute.

References

[1] Statista. Global Connected Car Fleet by Market. Accessed: March 2025. [Online]. Available: https://www.statista.com/statistics/1155517/global-connected-car-fleet-by-market/

[2] "Intelligent Transport Syst. (ITS); Cooperative Adaptive Cruise Control (CACC); Pre-standardization study," ETSI TR 103 299 V2.1.1, Tech. Rep., 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_tr/103200_103299/103299/02.01.01_60/tr_103299v020101p.pdf

[3] ISO 15622, "Intelligent transport systems — Adaptive cruise control systems — Performance requirements and test procedures," 2018.

[4] F.-E. Braiteh, F. Bassi, and R. Khatoun, "Platooning in Connected Vehicles: A Review of Current Solutions, Standardization Activities, Cybersecurity, and Research Opportunities," *IEEE Transactions on Intelligent Vehicles*, early access, August 22, 2024.

[5] F.-E. Braiteh, F. Bassi, and R. Khatoun, "Securing Cooperative Vehicular Platooning with a Set of Reinforced Checks," in *IEEE International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2025, Accepted.

[6] "Intelligent Transport Systems (ITS); ITS communications security architecture and security management," ETSI TS 102 940 V2.1.1, Release 2, Tech. Rep., 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/02.01.01_60/ts_102940v020101p.pdf

[7] S. Badnava, N. Meskin, A. Gastli, M. A. Al-Hitmi, J. Ghommam, M. Mesbah, and F. Mnif, "Platoon transitional maneuver control system: A review," *IEEE Access*, vol. 9, pp. 88 327–88 347, 2021.

[8] B. Hammi, Y. M. Idir, S. Zeadally, R. Khatoun, and J. Nebhen, "Is it really easy to detect sybil attacks in c-its environments: A position paper," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 18 273–18 287, 2022.

[9] Q. Li, Z. Chen, and X. Li, "A review of connected and automated vehicle platoon merging and splitting operations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 22 790–22 806, 2022.

[10] A. Farag, D. M. Mahfouz, O. M. Shehata, and E. I. Morgan, "A novel ros-based joining and leaving protocols for platoon management," pp. 1–6, 2019.

[11] M. Won, "L-Platooning: A Protocol for Managing a Long Platoon with DSRC," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 6, pp. 5777–5790, 2021.

[12] S. Maiti, S. Winter, and L. Kulik, "A conceptualization of vehicle platoons and platoon operations," *Transportation Research Part C: Emerging Technologies*, vol. 80, pp. 1–19, 2017.

[13] S. Graffione, C. Bersani, R. Sacile, and E. Zero, "Model predictive control for cooperative insertion or exit of a vehicle in a platoon." in *Proc. of the 17th Int. Conf. on Informatics in Control, Automation and Robotics (ICINCO)*, 2020, pp. 352–359.

[14] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks," *Proc. of the 5th IEEE Int. Conf. on Models and Technologies for Intell. Transp. Syst. (MT-ITS)*, pp. 110–115, 2017.

[15] R. A. Biroon, Z. A. Biron, and P. Pisu, "False data injection attack in a platoon of cacc: real-time detection and isolation with a pde approach," *IEEE Trans. on Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8692–8703, 2021.

[16] S. Khodadadi, T. K. Tasooji, and H. J. Marquez, "Observer-based secure control for vehicular platooning under dos attacks," *IEEE Access*, vol. 11, pp. 20 542–20 552, 2023.

[17] S. Xiao, X. Ge, Q.-L. Han, and Y. Zhang, "Secure distributed adaptive platooning control of automated vehicles over vehicular ad-hoc networks under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 52, no. 11, pp. 12 003–12 015, 2021.

[18] B. Ko and S. H. Son, "An approach to detecting malicious information attacks for platoon safety," *IEEE Access*, vol. 9, pp. 101 289–101 299, 2021.

[19] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified ufir estimator," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3693–3705, 2020.

[20] "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," ETSI TS 102 637-2 v1. 2.1, Tech. Rep., 2011. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/102600_102699/10263702/01.02.01_60/ts_10263702v010201p.pdf