Trust-Based Admission and Departure Control for Cooperative Platooning

Farah-Emma Braiteh[1,2,3]
[1] *Renault Group*
farah-emma.braiteh@renault.com

Francesca Bassi [2]
[2] *IRT SystemX*
francesca.bassi@irt-systemx.fr

Rida Khatoun [3]
[3] *Télécom Paris, IP Paris*
rida.khatoun@telecom-paris.fr

***Abstract*—Reliable data exchange is essential for safety and coordination in Cooperative Intelligent Transport Systems (C-ITS), especially within vehicular platoons. However, this requires interaction with previously unknown vehicles, introducing security risks and requiring trust evaluation prior to sharing sensitive information. This paper presents a cooperative platooning protocol with a trust management framework based on Subjective Logic to assess the trustworthiness of vehicles based on the information they share. The framework processes heterogeneous evidence types to estimate individual trust levels at different stages. A fuzzification module classifies these trust values, enabling adaptive and interpretable trust-based decision-making. The resulting trust assessments are used to determine whether to accept vehicle requests to join or leave a platoon and to detect misbehavior among existing platoon members. The complete model was thoroughly evaluated using PLEXE and SUMO simulators in dynamic and realistic platooning scenarios. Empirical results demonstrate its effectiveness in identifying faulty or malicious vehicles, thereby significantly enhancing the reliability of cooperative driving decisions.**

***Index Terms*—Cooperative Vehicular Platooning, Data Reliability, Trust Management, Subjective Logic, Fuzzy Logic**

I. Introduction

Connected vehicles exchange real-time data to coordinate maneuvers and enhance road safety and traffic efficiency. Vehicular platooning involves a group of connected vehicles traveling in close coordination and requires interaction with previously unknown vehicles to form, join, or leave a platoon [1]. In response to the need for secure and trustworthy interactions in vehicular platooning, our previous work introduced a platooning protocol that encompasses the Join and Leave procedures [2], [3], enabling a vehicle to securely create or join a platoon, as well as leave a platoon it is currently part of. The protocol was designed as cooperative mechanisms incorporating a series of security checks to assess the intentions of vehicles participating in platoon operations. Each verification phase is executed sequentially, with the next step triggered only if the current check has been successfully validated. Based on the outcome of each individual check, the vehicle's request is either accepted or rejected.

The sequential structure helped defend against several attack vectors, including data injection and Sybil attacks. The exclusion approach, where interactions are immediately halted upon a failed check, ensures the functional integrity of the platoon. To effectively secure platooning operations, security mechanisms should encompass both the integrity and accuracy of data exchanged through communication flows and physical-world verifications of vehicle driving behavior. These verifications are made possible by the utilization of on-board sensors.

A drawback in our previous approach is that the adopted security countermeasures only focus on the temporally local behavior of the agent, which can lead to unfavorable outcomes. For example, a vehicle may engage in the Join protocol to integrate the platoon, a process that requires verifying physical checks by modifying its trajectory to meet target positions within prefixed deadlines [2]. This requirement may be difficult to satisfy due to external factors, such as route conditions, which could potentially lead to the exclusion of a legitimate vehicle from the operation. Similarly, this limitation can lead to false negatives, such as when a DoS attack goes undetected at the time of evaluation, allowing a malicious vehicle to be accepted. These issues arise when decisions are made based on single interactions without considering the accumulation of prior evidence. To address this drawback, we propose an enhanced platooning protocol that employs a trust evaluation model. This model aggregates the varying degrees of vehicle's trustworthiness, its quantifiable level of reliability and confidence, observed throughout different protocol phases. Instead of making isolated binary decisions, the protocol collects trust evidence across all phases, which are compounded to support more informed and context-aware decisions about a vehicle's participation in the platoon. For instance, consider the Join procedure outlined in [2], where a platoon member interacts with a potential joiner and is ultimately responsible for granting membership. This multi-phase procedure involves collecting evidence about the joiner's behavior. The evidence is about the capability of the joiner to comply with the communication protocol, execute required physical maneuvers on the road, and provide correct kinematic information in Vehicle-to-Vehicle (V2V) messages. This platoon member maintains a trust score for the joiner that is dynamically updated as additional evidence is collected. We choose subjective logic to model this process, for its ability to represent uncertainty related to lack of evidence. This is considered a suitable formalism and has already been explored in the Connected Cooperative and Automated Mobility (CCAM) domain in the presence of heterogeneous sources of evidence [4]. The dynamic evaluation of the joiner's trust level is used by the decision process to decide whether to accept the new vehicle or not. The decision process is also dynamic and provides an updated status at each phase of the Join procedure until a final decision is reached. This framework allows to promptly exclude entities exhibiting scarce trust levels, while keeping to solicit evidence for other entities. We employ fuzzy logic in the decision process to account for epistemic uncertainty.

The main contributions of this paper are the following:

- We incorporate a multi-phase trust assessment mechanism into our platooning protocol. This mechanism employs subjective logic to compute trust scores for vehicles under evaluation. Subjective logic allows to model uncertainty related to the abundance or scarcity of collected evidence.
- We implement fuzzy logic to decide whether to accept or reject vehicles in a platoon, aiming to secure the platoon operations. Fuzzy logic is chosen to model epistemic uncertainty on the definition of trust.
- We evaluate the model and simulate scenarios using PLEXE simulator and SUMO under realistic vehicular conditions and validate its effectiveness in maintaining secure platoon formation and dynamics.

The paper is structured as follows: Section II reviews related work. Section III outlines the system architecture. Sections IV and V describe trust modeling and decision processes. Section VI reports simulation results. Section VII concludes the work.

II. Related Works

Research efforts focused on trust evaluation mechanisms to assess the trustworthiness of vehicles and detect misbehaving participants, particularly those transmitting false data, in vehicular networks. Several studies explored decentralized trust management approaches to address issues of scalability, resilience, and single points of failure. Guleng *et al.* [5] introduced a trust management framework in which vehicles estimate the trustworthiness of neighbors or indirectly observed nodes through evaluations from trusted entities. While this approach offers autonomy from centralized authorities, it assumes full visibility of packet forwarding activities and requires each vehicle to maintain trust values for all others. This assumption may constrain scalability and limit its practicality in dynamic platooning environments. Further decentralized but diverging from cooperative frameworks, Garlichs *et al.* [6] proposed a trust-based misbehavior detection mechanism targeting platoon members disseminating false vehicular dynamics. Their approach relies solely on sensor data for trust evaluation. This model may be acceptable for existing platoon members, but it is unsuitable for assessing vehicles requesting to join the platoon, as it neglects uncertainty and may yield misleading trust estimates. In contrast to decentralized approaches, other studies have proposed centralized frameworks for trust evaluation in vehicular networks, particularly in the context of vehicular platoons. Madl [7] introduced a security framework in which a C-ITS root certificate authority assigns trust values to vehicles' short-term C-ITS certificates based on peer evaluations of shared data. Building on this concept, Cheng *et al.* [8] proposed a cloud-based architecture for storing and updating trust values of vehicles within a platoon. These values, derived from behavioral assessments conducted by neighboring vehicles, are made accessible to authenticated nodes to support real-time decision-making. In a similar vein, Chen *et al.* [9] developed a trust model wherein roadside units manage and aggregate trust values submitted by individual vehicles. These values are securely stored on a blockchain for subsequent updates and future reference. Complementing these efforts, Müller *et al.* [10] proposed another centralized trust management and misbehavior detection scheme to enhance system reliability and security.

In our approach, we draw inspiration from existing trust models to incorporate a decentralized and cooperative trust evaluation mechanism into our platooning protocol. This approach enables proactive assessment of a candidate's trustworthiness before acceptance, collaboratively share this information, and update trust values within the platoon continuously. As a result, it enhances the overall scalability, robustness, and responsiveness of trust management in vehicular platoons.

III. System Overview: Cooperative Platooning with Trust Evaluation

In this section, we present the overall design of our proposed trust-enhanced platoon management system. This design integrates the protocol we previously developed [2], [3], [11] with a multi-phase trust evaluation framework that guides decision-making during vehicle admission, in-platoon driving, and departure. The interactions between different protocol components are illustrated through a sequence diagram in Fig.1. The green components correspond to the new modules integrated into the system to enable trust assessment functionality.

A. Functional Protocol

Fig. 1 describes the protocol as executed by the platoon member, the Ego, responsible for processing a join (or leave) request by a vehicle initially outside the platoon and managing its admission [2]. In this section, we review the functional steps of the protocol, focusing on the join case for simplicity. The trust evaluation process, represented by the green boxes in Fig. 1, will be introduced in the next section.

Upon reception of the join request, in the Pre-Join phase, the Ego performs preliminary functional checks, as checking that the platoon is not at its maximum capacity, and that no other operation is in execution, before granting authorization to the procedure. In Phase 1, the Ego issues physical challenges to the requesting vehicle, specifying a target inter-vehicular distance and a time constraint [2]. The requesting vehicle has to reach the designated position relative to the platoon within the specified time. Upon successful completion of the challenges, in Phase 2, the Ego sends maneuver instructions, which may include lane changes, to approach the platoon. In Phase 3, the Ego verifies the maneuver, by comparing the kinematic data reported by the requesting vehicle against locally sensed measurements. If consistency is confirmed, the vehicle is admitted into the existing platoon. The block *Add Member* in Fig. 1 corresponds in reality to a complex function triggered by the Ego and executed in a distributed manner by all the members of the platoon [2]. Phase 4 completes the enrolling of the requesting vehicle in the platoon, through the acquisition of the platoon group key by the new member [11]. The blocks *Create Master Key* and *Distribute Master Key* actually involve all the platoon members in the execution. The new member has to reconstruct the platoon group key and start to use it for producing platooning messages. The outgoing platoon messages, which include information as the platoon identifier, structural details, kinematic state of the vehicle, maneuver information, are hashed using the group key and digitally signed using individual private keys. The message receiver authenticates the sender as a platoon member by verifying the hash generated with the group key.

B. Trust Evaluation Process

The trust evaluation process is integrated to the functional protocol described in the previous section by incorporating to each Phase: i) the assessment of the trustworthiness of the requesting vehicle; ii) the decision to carry on or to interrupt the procedure based on the assessed trustworthiness. These are indicated by the green boxes in Fig. 1.

The trust assessment is based on evidence about the requesting vehicle, which is collected by the Ego during the execution of the different phases of the protocol. Evidence collection begins at the moment of the reception of the join request by the Ego and continues until the requesting vehicle is rejected or leaves the platoon. We denote this interval as the Trust Evaluation Time Window. As a consequence, trustworthiness evaluation performed at different phases of the protocol is based on different amounts of evidence, with evaluation in later stages able to rely on broader information. Intuitively, this introduces more uncertainty on the trust score evaluated in earlier phases. To represent this effect, we employ the mathematical framework of subjective logic to model trustworthiness, as detailed in Section IV.

The decision process is based on the classification of the vehicle based on its trustworthiness level. This is accomplished, as detailed in Section V, using fuzzy logic, to determine whether the vehicle is Trustworthy, Suspect or Untrustworthy. Once a vehicle is classified as Untrustworthy, it is excluded from the procedure. Conversely, a vehicle labeled as Suspect is permitted to continue, provided that this classification has not occurred in two previous phases.

C. Trust Evidence Types

In this section, we examine the evidence used by the Ego to perform trust assessment on the requesting vehicle. *Vehicle-to-Vehicle Message Verification* ensures that messages are correctly signed, comply with ETSI standards in their field construction, and contain plausible data. *Physical Challenge Verification* confirms that the vehicle is physically near the platoon by issuing position and time-deadline challenges requiring it to reach a specified location within the given time frame. *Maneuver Verification* cross-validates V2V message contents with sensor data to ensure consistency between communicated information and actual sensed conditions. *Group Key Verification* verifies that the new member has correctly reconstructed the group key upon joining and that existing members possess the updated key following any changes. These *checks* function as input evidence for the trust model, with each check corresponding to a distinct *evidence type*. A successful check is a positive evidence, whereas a failed check constitutes negative evidence. For example, a verification checking the integrity of a received message is considered as positive evidence when the message's signature is successfully verified and as negative evidence when the verification fails.

A collection of observations of evidence of the same type at a certain phase of the protocol is grouped in an *Evidence Set*. At each evaluation phase, a separate *Evidence Set* is constructed for each evidence type. Each Evidence Set consists of: (i) the number of collected positive observations, (ii) the number of collected negative observations, and (iii) the total number of expected observations of that type at this phase, including both collected and uncollected instances.

IV. Modeling Trust Using Subjective Logic

We choose to model trust using the subjective logic formalism [12], which allows to represent situations where decisions may be based on incomplete information. In the subjective logic framework trust is represented by the vector (b, d, u, a), where u is the uncertainty component, b and d are the belief and disbelief, respectively, and a is prior belief when uncertainty is maximum. In subjective logic $b + d + u = 1$, modeling the fact that high values of uncertainty must be accompanied by moderate degree of belief or disbelief. In our model, we directly tie the uncertainty value to the amount of evidence observed to provide the trust assessment. Subjective logic has been already proposed as an effective means for dynamic trust assessment in vehicular networks [4].

A. Modeling trust with subjective logic

In order to be able to anchor the value of uncertainty to the actually observed evidence, we start by defining the quantity E_{total}, representing the volume of total evidence potentially observable in the trust evaluation phase window. This is expressed as:

$$E_{\text{total}} = \varepsilon + \sum_{p=1}^{M} \sum_{i=1}^{N} \beta_i \cdot V_i^{(p)}, \quad \varepsilon > 0, \tag{1}$$

where $p \in 1, ..., M$ is an index indicating the protocol phase; $i \in \{1, ..., N\}$ is an index indicating the evidence type; β_i is a weighting factor for evidence type i; and $V_i^{(p)}$ is the maximum number of observations of evidence of type i expected during the protocol phase p.

Let $P_i^{(p)}$ denote the mass of positive evidence of type i actually observed during phase p, and $Z_i^{(p)}$ denote the mass of negative evidence:

$$P_i^{(p)} = \beta_i \cdot P, \qquad Z_i^{(p)} = \beta_i \cdot Z, \tag{2}$$

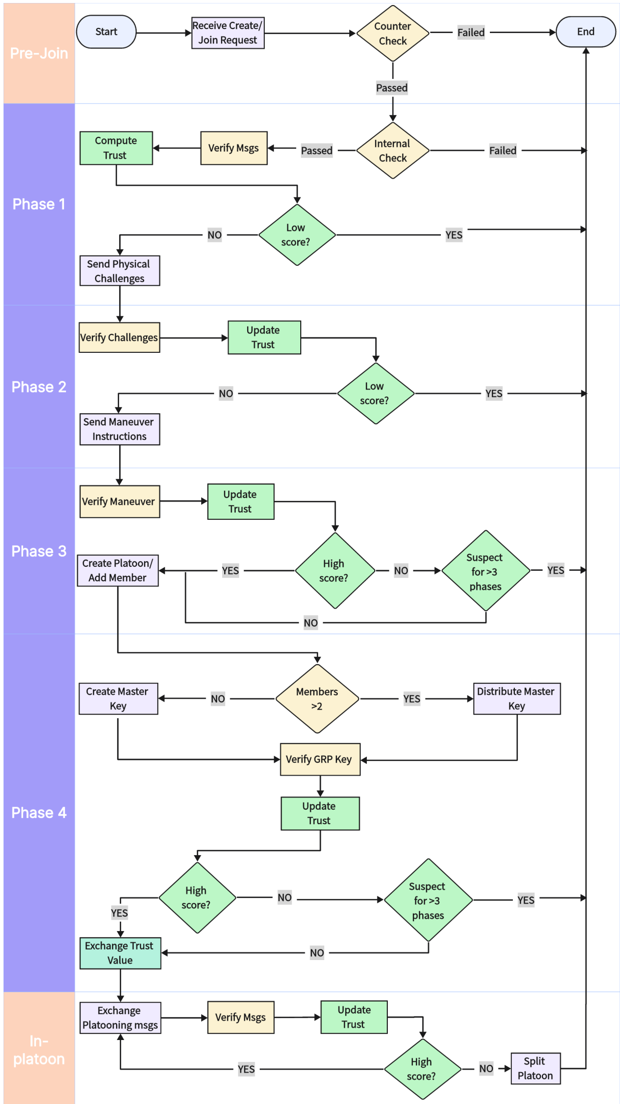

Fig. 1: Platoon Formation and Split with Trust Evaluation

where P is the number of observed checks of type i that provided a positive outcome and Z a negative outcome. If the trust evaluation is performed at the end of phase q, one can evaluate the total mass of positive and negative evidence observed so far as:

$$P^{(q)}_{\text{observed}} = \sum_{p=1}^{q} \sum_{i=1}^{N} P_i^{(p)}, \qquad Z^{(q)}_{\text{observed}} = \sum_{p=1}^{q} \sum_{i=1}^{N} Z_i^{(p)}. \tag{3}$$

Finally, the value of the uncertainty u is defined as the fraction of the potential evidence in the trust evaluation window for which there has been no actual observation:

$$u = \frac{E_{\text{total}} - P^{(q)}_{\text{observed}} - Z^{(q)}_{\text{observed}}}{E_{\text{total}}}. \tag{4}$$

The belief and disbelief are then evaluated depending on the fraction of positive and negative observed evidence:

$$b = (1-u)\frac{P^{(q)}_{\text{observed}}}{P^{(q)}_{\text{observed}} + Z^{(q)}_{\text{observed}}}, \tag{5}$$

$$d = (1-u)\frac{Z^{(q)}_{\text{observed}}}{P^{(q)}_{\text{observed}} + Z^{(q)}_{\text{observed}}}. \tag{6}$$

B. Scalar Trust Projection

To simplify the decision-making process, we project the trust opinion represented by the belief, disbelief, and uncertainty components onto a single scalar value. This scalar, known as the trust projection T provides a measure of trustworthiness and is defined as:

$$T = b + a \cdot u, \tag{7}$$

where $a \in [0,1]$ is base rate parameter that reflects prior expectation in the complete absence of evidence. In the absence of prior interactions with the vehicle under evaluation, uncertainty attains its maximum value of one, thus both belief and disbelief measures are equal to zero. Considering that vehicles participating in the ecosystem are PKI-authenticated [13], the base rate parameter a is set to 0.5 to represent a neutral prior expectation. Under these conditions, the resulting trust projection is consequently $T = 0.5$.

V. Fuzzy Classification of Trust Values and Decision Making

After computing the scalar trust value $T \in [0,1]$, the next step is to determine whether the trust in the vehicle under evaluation is acceptable. This assessment can be performed either by applying fixed numerical thresholds or through semantic categorization. In our protocol, we employ fuzzy logic [14] to better manage gray areas, thereby avoiding sharp decisions that are unsuitable for dynamic environments. Specifically, at each evaluation phase, membership functions are applied to the crisp trust value T to determine its degrees of membership in the fuzzy sets: untrustworthy, suspect, and trustworthy. Based on fuzzy inference rules, a decision is then made to either accept the vehicle and allow it to continue in the protocol, or reject it by terminating the evaluation.

A. Fuzzification Using Gaussian Membership Functions

To assign a trust value T to a qualitative category (*untrustworthy*, *suspect*, or *trustworthy*), we use Gaussian membership functions [15] centered at predefined means. The membership degree of a trust value T to a category i is defined by the Gaussian membership function, $MF(T)$:

$$MF(T; \sigma_i, \mu_i) = \exp\left(-\frac{(T-\mu_i)^2}{2\sigma_i^2}\right) \tag{8}$$

where $i \in \{untrustworthy, suspect, trustworthy\}$; μ_i is the mean trust value associated with category i; σ_i is the standard deviation of the Gaussian curve for category i. For instance, typical parameter values might be: $\mu_{\text{untrustworthy}} = 0.4$, $\mu_{\text{suspect}} = 0.6$, $\mu_{\text{trustworthy}} = 0.8$, and

$$\sigma_{\text{untrustworthy}} = 0.11, \quad \sigma_{\text{suspect}} = 0.16, \quad \sigma_{\text{trustworthy}} = 0.16$$

Using the value T, calculated in Equation 7, each category's membership degree is computed, and the final trust classification corresponds to the category with the highest membership:

$$\text{Class}(T) = \arg \max_{i \in \{\text{untrustworthy}, \text{suspect}, \text{trustworthy}\}} MF_i(T) \quad (9)$$

B. Trust-Based Decision Policy

Based on the classification obtained from Equation 9, a decision-making policy is applied to determine whether to reject, proceed with caution, or accept the vehicle under evaluation at a certain phase. Let $\text{Class}(T) \in \{\text{untrustworthy}, \text{suspect}, \text{trustworthy}\}$. The decision function, $\mathcal{D}(T)$, can be given as:

$$\mathcal{D}(T) = \begin{cases} \text{Accept}, & \text{if Class}(T) = \text{trustworthy} \\ \text{Proceed}, & \text{if Class}(T) = \text{suspect}(\leq 3 \text{ phases}) \\ \text{Reject}, & \text{otherwise} \end{cases} \quad (10)$$

VI. Trust Model Simulation Results

This section presents the simulation results of the proposed trust-based platooning management system. In the context of Join-from-behind protocol, the evaluating vehicle, being the last vehicle in the platoon, is responsible for computing the trustworthiness of a joining vehicle. This evaluation is performed based on the joiner's provided evidence, derived from its interactions. The simulated protocol includes up to five sequential security checks, presented in Section III-C, culminating in Phase 4 of the admission sequence illustrated in Fig. 1.

To test the trust evaluation mechanism, we employed the hybrid model combining Subjective Logic and a fuzzy logic-based classification and decision system. At each evaluation stage, the trust level of the joining vehicle is assessed and classified into one of three fuzzy sets: *untrustworthy*, *suspect*, or *trustworthy*. This classification relies on a Gaussian membership function with specific parameters and associated decision rules. The mean trust values for the fuzzy sets are defined as 0.4 for *untrustworthy*, 0.6 for *suspect*, and 0.8 for *trustworthy*, respectively. The simulation involved approximately 2000 joining vehicles evaluated through the multi-stage trust assessment protocol. Two separate executions were conducted to assess the impact of varying the Gaussian membership function parameters. During evaluation, fuzzy outputs determined vehicle progression. A vehicle is excluded if its membership value is classified as *untrustworthy* once or *suspect* on three occasions.

The simulation results highlight the significant impact of the standard deviation, σ, in the Gaussian membership functions on system behavior. Our objective is to avoid a hard-thresholding mechanism with minimal tolerance for uncertainty. Setting sigma values to $0.11, 0.16, 0.16$ for the respective sets produces wider Gaussian membership functions, especially for the *suspect* and *trustworthy* categories. The broader spread increases tolerance in trust evaluation, allowing vehicles with trust scores near the distribution centers to be classified more flexibly. This effect is pronounced in the *suspect* range, where trust scores cluster. Consequently, the system becomes more permissive, allowing more vehicles to progress through security checks. Under this configuration, an additional 12.8% of vehicles reached Check 5, Phase 4 in Fig. 1, compared to the case where narrower σ values were employed.

Membership Rules: Each vehicle is assigned to the fuzzy set corresponding to its highest membership value. In this simulation, an attacker rate of 5% is introduced. The results show that over 60% of vehicles were classified as *suspect*, most of which were ultimately accepted after further verification at later stages, when additional positive evidence became available, as shown in Table I.

TABLE I: Classification Results and Decision Outcomes

Total nb of simulated vehicles: 2020, Attacker rate: 5%			
Classification	**Percentage**	**Decision Outcome**	**Count (%)**
Untrustworthy	0.87%	Rejected	87 (4.31%)
Suspect	60.52%	Accepted	1933 (95.69%)
Trustworthy	38.61%		

Evolution of Trust Values: The progression of vehicle trust values across checks is illustrated in Fig. 2. The solid line represents the average trust value computed at each individual check. This average is calculated solely based on the subset of vehicles that reached the corresponding check. The density of blue dashes indicates the concentration of vehicles with similar trust values.

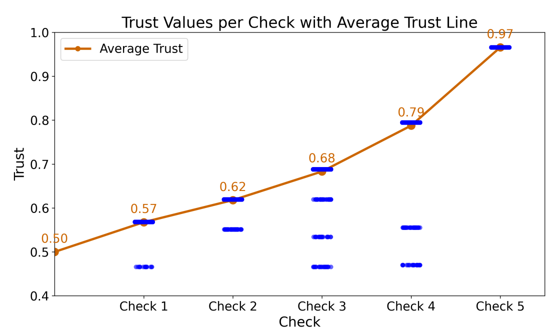

Fig. 2: *Evolution of Trust Values for Joining Vehicles*

Evaluation in Platooning Scenarios To assess the impact of the trust management system on platooning operations, we used the *Plexe* and *SUMO* simulators to replicate the scenario under realistic driving conditions. The simulated scenario involves five vehicles operating on a multi-lane road. Vehicles V_0 and V_1 are initially positioned in 'Lane 1', while V_2, V_3, and V_4 are in 'Lane 2'. At the start of the simulation, all vehicles travel independently at a speed of 110 km/h. Shortly after initialization, V_1 sends a request to join V_0. It successfully passes all five trust evaluation checks, and a platoon is formed. Subsequently, V_2 requests to join the platoon. Its trust level is evaluated by V_1, which grants admission. In the first simulation run, V_3 is also accepted by V_2 into the platoon. However, in a second simulation, V_3 is designated as an attacker and injects false data, leading to its rejection. Vehicle V_4 does not attempt to join the platoon and continues driving independently throughout the simulation.

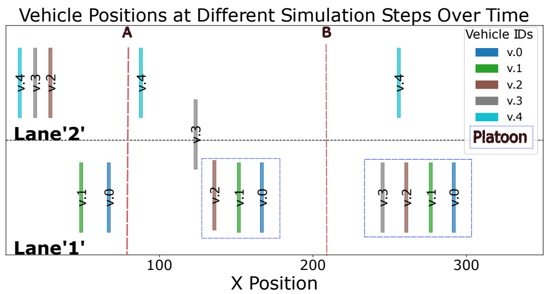

Fig. 3: *Platoon Creation and Joining*

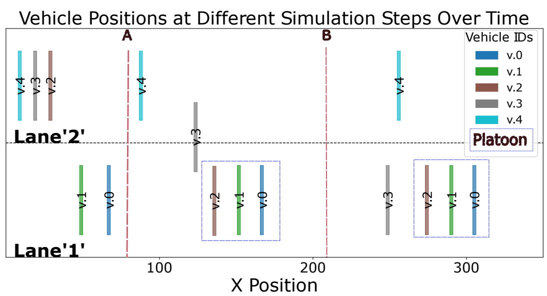

Fig. 4: *Platoon Join Rejected*

Phases **'A'** and **'B'** in Figures 3, 4 represent different time steps in the simulation timeline. The results of the first simulation, shown in Fig.3, indicate that vehicles V_0, V_1, and V_2 successfully belong to the same platoon after phase 'A'. V_3 is instructed to change lanes in order to join the platoon. Next, it is admitted into the platoon, as illustrated after phase 'B'. Once integrated, V_3 maintains the same inter-vehicle distance and speed as the other platoon members. In the second simulation, V_3 is initially classified as *suspect*, and later as *untrustworthy*, due to the detection of false evidence during the trust evaluation process. As depicted in Fig.4, V_3 is first instructed to change lanes while under *suspect* status. However, once classified as *untrustworthy*, it is rejected and denied access to the platoon. Consequently, no platooning information is shared with V_3, and it continues to drive independently behind the platoon.

VII. Conclusion

In this paper, we extended our previously tested platooning protocol that allows vehicles to join, leave or create a platoon of connected and cooperative vehicles by integrating a trust assessment model to the decision-making process. This model allows a vehicle to be evaluated for trustworthiness based on accumulated interactions over multiple protocol phases, rather than relying on isolated binary checks. With each step of the protocol, the system builds a more nuanced trust profile, enabling it to make an informed decision on whether to admit, retain or exclude a vehicle. The proposed approach provides a continuous and context-aware trust evaluation mechanism that increases the resilience of platoon operations against misbehavior and malicious activity. The simulation results obtained with rigorous experimentation using PLEXE and SUMO simulators strongly support the empirical proof of the model effectiveness and robustness for secure, adaptive and resilient platooning in dynamic C-ITS environments.

References

[1] 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*, vol. 10, no. 5, pp. 3134–3155, 2025.

[2] B. F. Braiteh, Farah-Emma and R. Khatoun, "Securing Cooperative Vehicular Platooning with a Set of Reinforced Checks," in *2025 International Wireless Communications and Mobile Computing (IWCMC)*, 2025, pp. 1027–1033.

[3] F.-E. Braiteh, D. Tse, O. Yhia, F. Bassi, and R. Khatoun, "A Secure and Cooperative Departure Protocol for Connected Automated Platoons," in *2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2025, pp. 174–182.

[4] CONNECT, "Architectural Specification of CONNECT: Trust Assessment Framework, Operation and Interaction," 2024, Accessed: 29 July 2025. [Online]. Available: https://horizon-connect.eu/wp-content/uploads/2024/04/CONNECT-D3.2-PU-M18.pdf

[5] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized trust evaluation in vehicular internet of things," *IEEE Access*, vol. 7, pp. 15 980–15 988, 2019.

[6] K. Garlichs, A. Willecke, M. Wegner, and L. C. Wolf, "Trip: Misbehavior detection for dynamic platoons using trust," in *IEEE Intelligent Transportation Systems Conference (ITSC)*, 2019, pp. 455–460.

[7] T. Madl, "Security concept with distributed trust-levels for autonomous cooperative vehicle networks," in *2021 IEEE Intelligent Vehicles Symposium (IV)*, 2021, pp. 321–328.

[8] M. Cheng, C. Yin, J. Zhang, S. Nazarian, J. Deshmukh, and P. Bogdan, "A general trust framework for multi-agent systems," in *20th Int. Conf. on Autonomous Agents and MultiAgent Systems*, 2021, pp. 332–340.

[9] H. Chen, X. Fu, Q. Yuan, Z. Zhuang, J. Kang, Z. Liu, J. Wang, and D. Niyato, "Trust model-based consensus optimization for vehicle platooning networks: A novel deep reinforcement learning approach with genai," *IEEE Trans. on Intelligent Transportation Systems*, 2025.

[10] J. Müller, T. Meuser, R. Steinmetz, and M. Buchholz, "A trust management and misbehaviour detection mechanism for multi-agent systems and its application to intelligent transportation systems," in *IEEE 15th Int. Conf. on Control and Automation (ICCA)*, 2019, pp. 325–331.

[11] F.-E. Braiteh, F. Bassi, and R. Khatoun, "Secure Group Key Dissemination Protocol in Cooperative Vehicular Platooning," in *2025 21th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2025, pp. 1–8.

[12] A. Jøsang, "Subjective Logic," University of Oslo, Tech. Rep., 2013, Accessed: 29 July 2025. [Online]. Available: http://folk.uio.no/josang/

[13] B. Lonc, F.-E. Braiteh, and F. Bassi, "Hybrid key exchange and signature design for quantum-safe c-its," in *2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2025, pp. 100–108.

[14] I. Tal and G.-M. Muntean, "Towards reasoning vehicles: A survey of fuzzy logic-based solutions in vehicular networks," *ACM Computing Surveys (CSUR)*, vol. 50, no. 6, pp. 1–37, 2017.

[15] A. Hawbani, E. Torbosh, X. Wang, P. Sincak, L. Zhao, and A. Al-Dubai, "Fuzzy-based distributed protocol for vehicle-to-vehicle communication," *IEEE Trans. on Fuzzy Systems*, vol. 29, no. 3, pp. 612–626, 2019.