Reputation-based Security for IoV Environment

Nozha Dhibi, Amel Meddeb Makhlouf, Faouzi Zerai

***Abstract*—The Internet of Vehicles (eV) networks provide communications between vehicles. They become interconnected and interactive. Their objective is to provide services for drivers and to make driving safer and more comfortable. Our prior focus in this project work is on the safety feature; this suggested solution guarantees the greatest protection and safety to drivers and vehicles on the roads through the transmission of essential information and safety warnings. Indeed, due to the special requirements of road networks, it has become a target for complex attacks. Our solution has the ability to detect attacks at an early stage regarded to the vehicle and driver behavior along with the network state.The selected measures include incorrect alerts, vehicle speed and information weakness caused by the wireless link. These metrics are used with previously collected behavior of the vehicle to compute a reputation managed by the Edge server to secure IoVs. Based on its reputation, a vehicle is known as trustworthy. Following analysis, it is found that reputation decreases with an increase in vehicle speed. Furthermore, the calculated delay of 4.2 ms does not disrupt network communications, which is notable for the security features introduced.**

***Index Terms*—Internet of Vehicles (IoV), attack, security, trust, reputation**

I. Introduction

NEWLY due to the rapid evolution of movable vehicles in the Internet of Vehicles (IoV), vehicles become interconnected and interactive with each other [1] [2]. The IoV that integrates the inter-cluster and the inter-vehicle network can perceive information related to vehicle status and environment [3]. Recently, automotive vehicles have represented an important part of the market. [4]. This technology allows drivers to be more vigilant about road conditions and makes the strategy of transport networks more structured and healthy. [5] [6]. In fact, they let road partners have information about their road conditions, meteorological conditions[7], and access to the net in real time. This platform offers a wide range of comfort and entertainment, including multimedia data transfer and tourist information [8] [9]. IoVs are created when various vehicles connect with each other with or without infrastructure [10][11]. In certain circumstances, the absence of infrastructure is a benefit, but it also brings about several challenges that must have an impact on the road [12]. The biggest challenge of these networks is security, where more complex attacks endanger these networks due to vehicle movement, causing numerous changes in topology [13] [14]. In practice, given the specific needs of vehicle networks, due to the openness and vitality of the network, it has become susceptible to manipulation and created new vulnerabilities [15] [16]. Information failure, incorrect warning messages, and vehicle speed due to wireless connection are several of the issues that impact road safety. To solve the above problems, we suggest a reputation management schema that rejects fake vehicles and warns neighbors to get trusted vehicles to communicate securely and save communication bandwidth [17][18] [19]. The proposed approach analyzes vehicles in the edge server area to assign and update a keep score. Based on this, communicating vehicles can be accepted or rejected [20]. We mainly aim to suggest an effective cooperative reputation management framework in the IoV domain by identifying intruders, where the main contributions of our work are:

-Cooperating nodes to evaluate vehicle reputations

-Compute and update the reputation score to trust or not vehicles and communications

-Monitor the network/vehicles to continuously update reputation to maintain trust in the network

The remainder of this paper is organized as follows. Section 2 briefly presents the associated work. We introduce some preliminaries knowledge on the architecture of the suggested reputation schema and the algorithm for computing the reputation score will be introduced in Section 3. An extensive simulation will be conducted and will be discussed in Section 4. In Section 5, a comparative analysis is performed. Finally, we complete this study in Section 6.

II. Related work

Several searches were proposed to offer safe roads by detecting attacks based on the calculation of a trust or a reputation metric. Indeed, Vishal Venkatraman et al. [21] presented a conceptual framework for managing trust under uncertainty for smart vehicle networks, In this context, the measure of trust is founded on the level of uncertainty present in the source data. In their work, the level of trust in an Internet of Things (IoT) network is related regarding the volume of uncertainty produced by various factors, Among the network stability issues, conflicts, and the type of data transmitted across entities. As an extension of this work and to manage vehicle trust, Guntur Dharma Putra *et al.* [22] proposed a blockchain-based trust and reputation management for reliable 6G networks. Trust and Reputation Management (TRM) is suggested as a mechanism to continuously assess the credibility of each participant by collecting and analyzing evidence of interactions with other points and the infrastructure. To enhance trust computing, Fan N. *et al.* [23] proposed a hybrid model based on communication and social security for vehicle social networks that takes into account both communication trust and social trust. In the suggested plan,They first designed a communication trust model to evaluate the value of trust based on interactions across vehicles. Then, they designed a social trust model to measure mutual trust based on the social attributes of

Manuscript received July 4, 2024; revised February 3, 2025.

Nozha Dhibi is a member of the NTS'COM Research unit, University of Sfax, Tunisia (Phone: +2165308678; e-mail: dhibi.nozha@gmail.com).

Amel Makhlouf is a member of the NTS'COM Research Unit, University of Sfax, Tunisia (Phone: +21698630994; e-mail: amel.makhlouf@enetcom.usf.tn).

Faouzi Zerai is a member of the NTS'COM Research Unit, University of Sfax, Tunisia (Phone: +21697244802; e-mail: faouzi.zerai@enetcom.usf.tn).

automobile drivers. Based on these two trust models, they calculate the combined trust evaluation of a vehicle core in automobile social networks. Because of the huge amount of managed data, D. Rajavel *et al.* [24] presented a trust-based pricing scheme for the edge sensory mobile cloud for IoT vehicles. It proposes a mobility-oriented trust model based on transferable belief, which exploits various kinds of information gathered by devices to estimate confidence values. The trust model suggested in this work is based on three categories of beliefs: device-to-device (D2D), infrastructure-to-device (I2D), and cloud-to-infrastructure (C2I). A trust calculation and reasoning method is proposed by J. Bai *et al.* [25] In order to assess the value of the network trust and divide it into different segments with different trust values, the Unmanned Aerial Vehicle (UAV) heads towards the segments increased confidence value to increase the rate of task completion and minimize delays. Therefore, they mainly introduce the trust value update, which is usually divided into a calculation of the trust area and a suspicious area. To simplify the calculation of the trust of the network area, authors calculate the trust of the virtual grid. The trust value for each group is initially the same, the trust value remains unchanged adjusted as the UAV engages with the devices. Moreover, trust-based mechanisms are generally crucial to ensure communications in IoT networks. However, it is rare to achieve both safety and efficiency simultaneously. Then, Li, T. *et al.* [26] reliable data collection via vehicles associated with autonomous aerial vehicles in the intelligent context of the Internet of Things. Their goal is to optimize the security problem by choosing trusted cars as mobile stationary. A key aspect of trust is that vehicle trajectories are designed based on anticipated circumstances. It can be observed that this vehicle is more trustworthy, Considering cars without such spots. Additionally, if a vehicle is parked at defined spot every day, drones can easily retrieve the information stored in this vehicle. Obviously, cars with regular routes are chosen as trust-based mobile stations, they exhibit an increase in trust level. Thus, Check if a vehicle has a fixed parking space spot, they analyzed its routes. The vehicle's trust level is analyzed based on past routes. the researchers in [27] proposed a reputation-based service provisioning system, as well as a reputation management system including decentralized reputation update and Global reputation sync. The goal is to stop fog vehicles from providing Poor service by optimizing reputation. gained by all servers during the optimization period. When a fog vehicle is completed to meet the requested service, RSU assigns it a score to evaluate its performance during service provisioning. This evaluation considered various things like prints from IoT devices and RSUs. Usually, the drone that provides low-quality service will be reprimanded while the quality of service will be rewarded.. similarly at work [28] suggested a method based on task-based experience (TER), this is a testament to the vehicle's reputation for specific performance. In conclusion, they pointed out the problem of two commonly employed confidence updating methods and suggest using the concept of TER to be resolved this problem. [28] Optimizes message transmission and vehicle work in the face of experience-based models. In VANET, Primarily, the management of the Trust emphasizes a direct assessment between individuals without considering the type of task. Some tasks have an impact on road safety, such as providing misleading advice. Furthermore, tasks that have no impact on road safety, such as events, add to the overall value of the vehicle. Thus in [28], All experiments were evaluated depending on the kind of task the node is performing. Thus, they have the possibility to choose a specific core intended for specific task, the realization of this work is based on its TER. Furthermore, they notice the boredom of calculating the reputation value while ignorant the gender of task. What's more illustrate how this concern influences trust management and security on roadways. In [29] a centralized reputation management system is suggested to detect malicious points on the road network. It operates on centralized and local servers. When a vehicle enters the control zone of a server room, the local server retrieves vehicle reference information from the central server and acquires this information as the vehicle moves in the zone. When the local server receives a validation report, it updates the reputation list of the corresponding cars in the next incidents. First, the local server determines the trustworthiness of all vehicle founded on its existing reputation through normalization. The local server analyzes the newly received validation tests and checks the credibility of the validation report to determine check if the vehicle is valid produces a spurious message or not. If the validation tests indicate a normal message, we increase the reputation of the validated vehicle. Otherwise, we decrease the reputation of the vehicle validated by a some percentage that increases exponentially depending on the number of false information transmitted. In summary and after analyzing several existing approaches, we notice that the reputation calculation is always non-distributed and the nodes are non cooperative, i.e., only one level of computation performed and an only one type of used reputation. Moreover, most solutions supervise one metric for the reputation computation, which is not sufficient to be sure about the trustworthiness of the vehicle based on the reputation score. Indeed Li. T and al. [26] only use parking history to identify malicious vehicles, where works in [21] [24] [25] [27] [28] [29] highlight the interactions with neighboring nodes, where the exchanged messages are factors for the estimation of trust score, which cannot be enough to identify dishonest nodes. Moreover, through the social relationship between drivers, Fan N et al. [23] calculate the social reputation score but we think that more parameters can be more efficient to identify the malicious behavior of the vehicles. Table 1 features a contrast between studied works in terms of used metrics to decide about the reputation of the vehicle/node.

Table I
COMPARISON OF RELATED WORKS

	PDR	Identity	Speed	Delay	History
V. V and al.[21]	√	×	×	×	×
G. P and al.[22]	√	√	×	×	×
F. N and al[23]	√	√	×	×	√
D. R and al.[24]	√	×	×	×	×
J. B and al.[25]	√	×	×	×	×
L. T and al[26]	×	×	×	×	√
ch. T and al[27]	√	×	×	×	√
R. J and al[28]	√	×	×	×	×
S. Su and al[29]	√	×	×	×	√

III. Proposed Reputation Management Approach

To overcome current constraints approaches by (1) co-operating vehicles and RSU in the process of calculating the reputation and (2) using different collected metrics to calculate and update the reputation, we suggest in this paper a distributed reputation management method that performs three stages of computation. (1) Initial study of the reputation calculation at the edge level that computes the first score and executes the authentication process based on vehicle identifier, vehicle speed variation, and exchanged messages through neighboring RSUs connected to the edge server. (2) Reputation update analysis at the RSU level that introduces reputation update, authentication, and clustering processes. (3) Final computational analysis at the cloud level, the reputation of genuine vehicles is stored in the database for updating. The last-keep assessment is sent to adjacent vehicles to mark the right assessment to accept or reject intrusive vehicles that include that vehicle. With this reputation result system, every vehicle with down reputation should be eliminated from the network and the one with capable reputation becomes a communication collaborator. Fig.1 illustrates the edge-based planning of our reputation calculation structure with these two stages, where several components are introduced, such as the Edge server, which does vehicle registration, authentication process, and initial and final reputation calculation. Thus, the RSU executes the clustering of a set of vehicles in its coverage area, the authentication, and the update of the reputation. Table 2 presents the descriptions of terms used in the rest of the document.

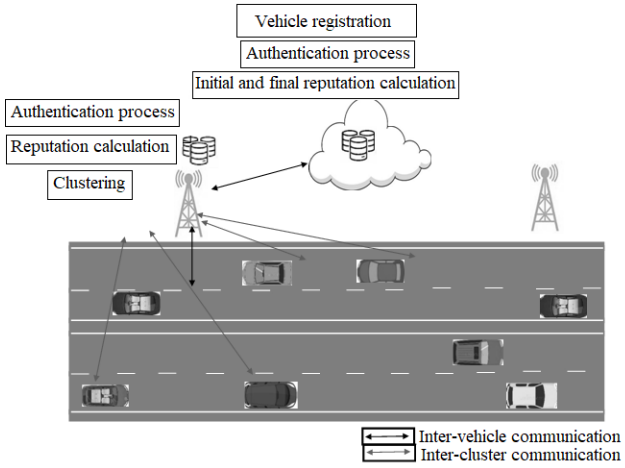

Figure 1. Cloud-based architecture of two levels reputation calculations

A. First level: Inter-vehicle reputation

The reputation calculation method is performed through two points (RSU and Edge server), where the reputation is updated by precise vehicle level parameters. As indicated in Fig.2, the reputation score algorithm is separated into various parts: the Packet Delivery Ratio (PDR) verification process, the speed difference function, the unique identifier usage verification process, the response delay verification process, and the parameter combination module for reputation score management, in addition to the preceding RSU-based reputations, which are stored in a data list, containing the coordinates of the authenticated vehicles with RSU.

Table II
Notations

Notation	Description
PDR/PLR	Packet delivery ratio/ packet loss ratio
ID_v	Identity of vehicle
ID_rsu	Identity of RSU
M_1	Parameter to check PDR
M_2	Speed difference function
M_3	Checking the unique use of the identifier
M_4	Response time check
V	Vehicle Speed
V_m	Vehicle Average speed
R_i	Initial reputation
R_j	Reputation update
R_f	Final reputation
R	Current reputation
m	Number of vehicles
n	Number of RSU
k	variable

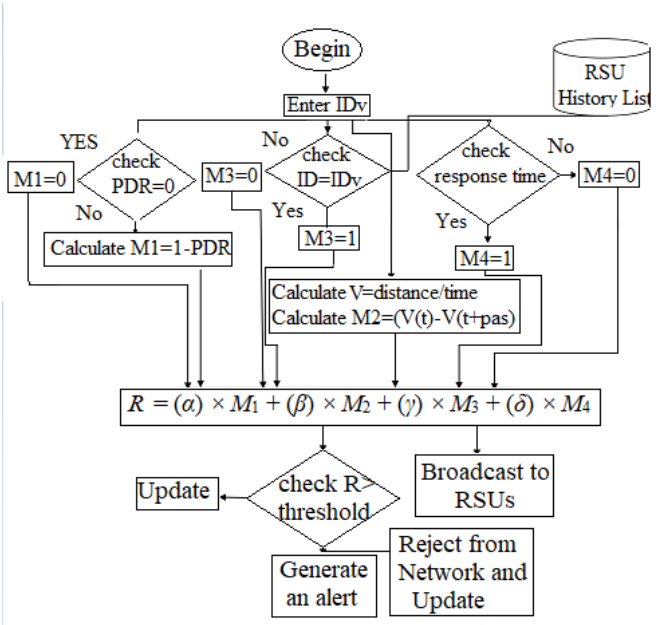

Figure 2. Reputation calculations process

1) Packet Delivery Ratio (PDR) check: Previous research has discovered various types of attacks. H. M. and al. in [24] warned about sophisticated attacks by message injection to control the vehicle. The Packet Delivery Ratio (PDR) evaluation handles these attacks, where the verification process involves the proportion of data packets that were received by the destination node compared to those produced by the source. If PDR equals zero, it means that the number of packets received equals zero and therefore the first parameter M_1 equals zero if not M_1 depends on PLR.

$$M_1 = 1 - PLR \tag{1}$$

2) Speed difference check: The speed V is applied as a factor to monitor the conduct of the vehicle. We study that a malicious node performs most of the nodes in its environment, it turns at a steady standard speed. If the speed $V(t)$ at a time t increases irregularly, it will turn malevolent. Shifting at a speed deviation that is external the accepted

speed deviation limit, it is turned malicious, which decreases its reputation. However, if the node is within the limit, the setting M_2 results in 1.

$$M_2 = V(t) - V(t + step) \quad (2)$$

3) Identity check for authentication: Vehicle communications integrity is vulnerable to various threats [25] especially spoofing attacks. Thus, we checked the identity of each partner. The process of checking *Idi = Idj* or checking the only use of the identifier. This scan is performed to check whether the vehicle identifier is exploited by different nodes in the RSU or not. If the identifier is used by another vehicle in the RSU, a result of 1 is allocated to the parameter M_3. If not, a result of 0 is assigned to the parameter M_3.

4) Response time check: The delay time is determined when a message arrives at a receiving node after being transmitted by a transmitting node. DoS attack messages aim to occupy the network [26]. They are injected between request and response messages, and they inevitably delay receipt of the response. Since all nodes are sharing on the network, increased network occupancy can produce latency for other messages and lead to availability threats without driver response. The process of checking the response time, the delay increases when the response time increases, which generates a time squandering and therefore it exceeds the predefined threshold.

5) Reputation aggregation module: The aforementioned metrics are used to detect attackers among vehicles on the road by computing the reputation and updating it if it exists. Thus, the reputation aggregation function aims to combine up all the elements determined by the several variable to find the reputation score, as follows:

$$R = (\alpha) \times M_1 + (\beta) \times M_2 + (\gamma) \times M_3 + (\delta) \times M_4 \quad (3)$$

6) RSU History List to update reputation: This list includes all the details of the vehicles authenticated with RSU. [The identifier] All the identifiers of the authenticated vehicles with different RSUs are stored on the Edge server.
[Speed check] The difference in speed between two well-determined instants is calculated and sent to the RSU BD with the following equation:

$$V = Distance/time \quad (4)$$

$$D_v = V(t) - V(t + step) \quad (5)$$

[Average Speed] The average speed of a set of vehicles in a cluster.

$$V_m = (V_1 + \ldots + V_n)/n \quad (6)$$

[Number of messages] The total number of messages sent and received is stored in the RSU database.
[Reputation] The initial and final reputation scores are stored in the RSU data base

B. Second Level: Reputation calculation at the edge and RSU level

The calculation of the reputation score at the cloud and RSU level comprises several procedures. The authentication process is used to verify the identity of vehicles detected by a specific RSU, named (RSUi). When the vehicle and RSU send these IDs (ID_V and ID_RSU), the edge server checks its database, once ID_V does not exist in its database, an alert is sent to the vehicle to request's registration, once the registration is completed, the vehicle requests authentication. After verification, the edge server authenticates ID_V. Then, it calculates the initial reputation score using the parameters related to the vehicle and networks simultaneously. Finally, this initial reputation score must be sent to the RSUs as shown in the initialization sequence diagram (Fig.3). Once ID_V exists in the database, the vehicle requests authentication, after verification the vehicle authenticates *n* times and the reputation score is updated at the RSU level. After that, the new reputation score is sent to the edge server for final calculation and then broadcast to RSUs as shown in the update diagram of Fig.4. After registering vehicles, an initial reputation score is computed and then monitored and updated, as presented in the following sections.

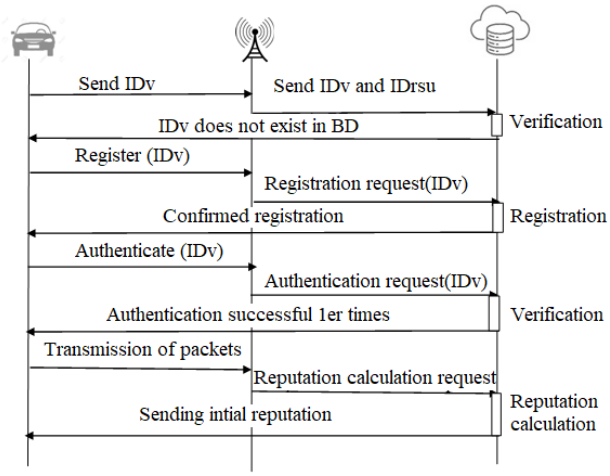

Figure 3. Initialization Sequence Diagram

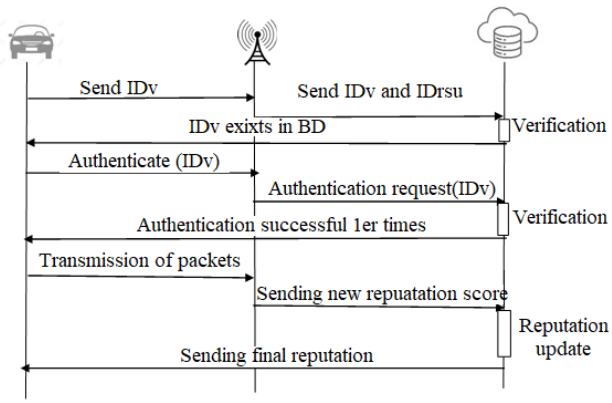

Figure 4. Update Sequence Diagram

1) Initial calculation of the reputation score at the cloud level: As shown in Fig.5, the initial calculation of the Edge-level reputation score includes various processes, starting with verification of the vehicle identity (authentication) after retrieving this information from the RSU. If the vehicle is not valid in the RSUi, it is excluded from the network. If the vehicle is authenticated by RSUi, the reputation score is determined and transmitted to RSU. Reputation verification

analysis is used to verify if the reputation score exceeds a predefined threshold. If this Rau score surpasses S, a warning is created to reject this vehicle out of the network.

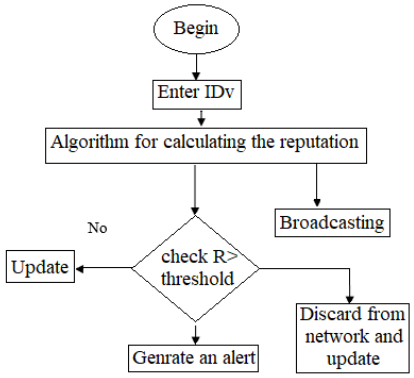

Figure 5. Initial calculation of the reputation score at the cloud level

2) Reputation update at the RSU level: The reputation score is renewed at the RSU level. Afterwards, selecting several vehicles m and verifying, the reputation score is renewed with the processes of the initial calculation but at the RSU level and then with the primary reputation score R_i and the current reputation score Rau. We determine the updated reputation score and send it to the cloud via the Edge server using Equation (7).

$$R_j = (R_i + R)/k \tag{7}$$

As shown in Fig.6, the reputation score R_j is calculated to be verified. If it exceeds a limit, a notification is created and send to the Edge server and then to the cloud.

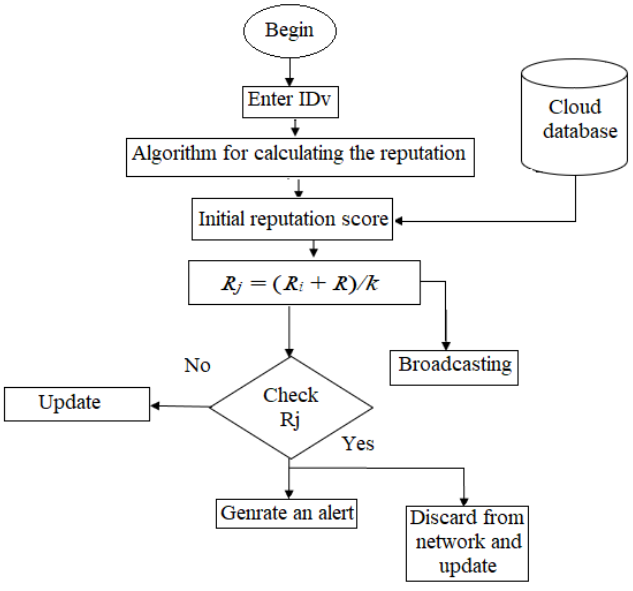

Figure 6. Reputation update at the RSU level.

3) Calculation of the final reputation at the Edge server level: At the edge level, the final reputation is calculated based on the RSUs, Authenticating the vehicle V. The edge server supervises n RSUs, the reputation update R_j where each RSU saves the reputation of the authenticated vehicle. Then, with the current reputation Rau and the updated reputation R_j we determine the final reputation. Finally, the result is evaluated using a threshold to decide if the vehicle will be rejected from the network or not (Fig.7).

$$R_f = (R_j + R)/k \tag{8}$$

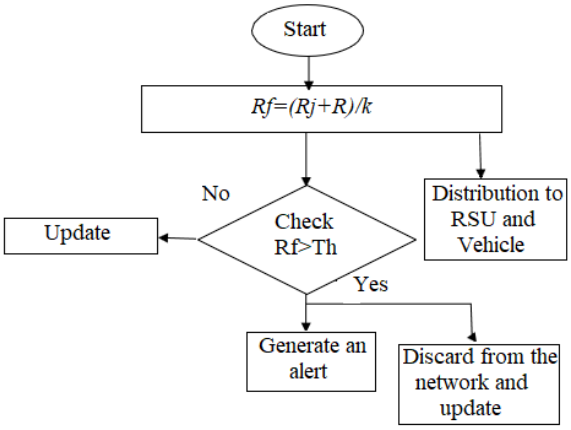

Figure 7. Final reputation at the cloud level.

IV. Evaluation Results

In this section, we execute the approach assessment to estimate its efficiency and evaluate network overhead after executing our reputation management process. Our objective in this analysis is to demonstrate that our approach is running, i.e. that it be able to detect misbehavior's vehicles. In this part, we illustrate various evaluation functions in which several metrics are used. If the vehicle identifier exists in the Edge server, we indicate that this vehicle is verified and we progress to reputation calculations. If not, it requests registration and authentication, and we proceed to reputation calculations. Clearly, if vehicle ID exists in the cloud database, we proceed to the evaluation based on four factors (M_1, M_2, M_3, M_4). The simulation environment is shown in Table 3. In this section, we study the following setting:

Table III
Simulation conditions for inter-cluster reputation.

Simulation Parameter Name	Value
Total number of messages	1000
Number of erroneous messages	30,20,40,15,80,240,30,150,9 0
Average vehicle speed	60
Accelerations	0,2,1,1,4,6,3,5,2,4,6,3
Authentication with RSU	Yes
Number of vehicles	10

identifier analysis, speed difference, PDR and response time verification. Lastly, we assess the reputation result. For each assessment, we prove and review the results to estimate the overhead of our suggested reputation management approach. Simulation assessments for inter-cluster reputation, inter-vehicle reputation, authentication study with RSUi, ID authentication, speed change analysis, PDR and response time are settings, used to estimate the execution of our solution.

A. Inter-cluster reputation

As explained in Fig.8, we designed the inter-cluster reputation results for 10 neighbor vehicles separately, where the reputation probabilities are too high, because of the specific simulation conditions. This simulation allows us to represent

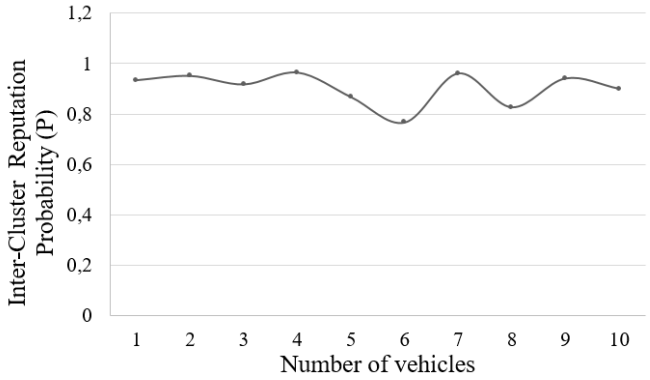

Figure 8. Inter-cluster reputation according to the number of communicating vehicles

the global reputation state of the edge server underneath precise situations, where we establish that the reputation ranges but is still an overhead of *0.7667*, which demonstrates that our result works properly with a correct inter-cluster reputation.

1) Authentication analysis: In this section, we check the authenticity of the vehicle along with the RSU on the cloud network. If the vehicle is not authenticated with separate RSUs, the reputation progressively decreases up to it reaches 0. Fig.9 illustrates the authentication of a vehicle as a function of the number of connected vehicles. We suppose that if the vehicle is authenticated per the RSU, auth=1; Else auth=0. We found that if the vehicle loses the connection

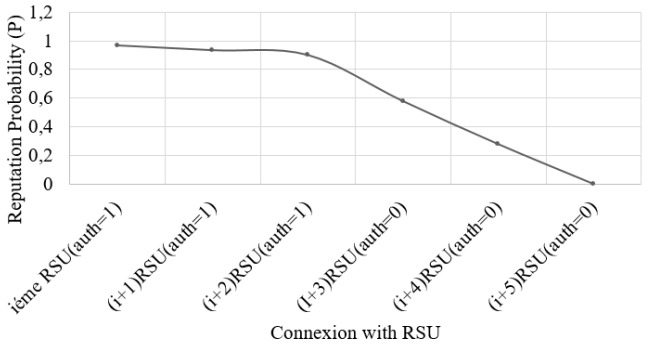

Figure 9. Vehicle authentication results with RSU

with RSUi, the reputation value will quickly decrease to 0. This is due to the number of wrong attempts allowed by our algorithm (Threshold =k).

2) verification of the identifier: In this evaluation, we are assessing the identifier of a vehicle authenticated by RSUi with the identifiers of the nearest RSUj in the edge server. If a vehicle ID is used by a neighbor in a previous interaction, we assess the number of authentication these vehicles have with RSU. If this vehicle gets further authentication than the others, a grade of 1 is allocated to M_3. Otherwise, a grade of 0 is assigned. If this identifier is not used by any neighbors, a grade of 1 is assigned to M_3. As demonstrated in Table 4, we have signified our assessment of the identifier, when ID1 is used by two vehicles, the first is authenticated twice and the next five times, this is why the reputation of the first decreases and the second remains constant. Same as ID2.

Table IV
ANALYSIS OF THE IDENTIFIER

Identifier	Id1	Id1	Id2	Id2
Nbr of auth with RSU	2	5	6	1
Initial reputation	0,9333	0,9667	0,9333	0,9667
Final reputation	0,6	0,9667	0,9333	0,6333

3) Speed difference analysis: The speed evaluation depends on the change of the vehicle's speed at two separate times. If the vehicle does not exceed its expected speed difference, the speed assessment would result in a low score for the M_2 variable. If this velocity gap is consistent with that anticipated by the node, a good mark is allocated to the M_2 variable. This result is calculated by a well-defined equation. Whenever the speed increases, the M_2 score reduces until it reaches 0. In this evaluation, we ignored the number of wrong communications, whenever our node is authenticated with RSUs. We utilized an identifier that was not used by any neighbor. In Fig.10, we assess the reputation value of a vehicle by growing the speed and time until a predetermined threshold is attained. From the out-coming results, we notice

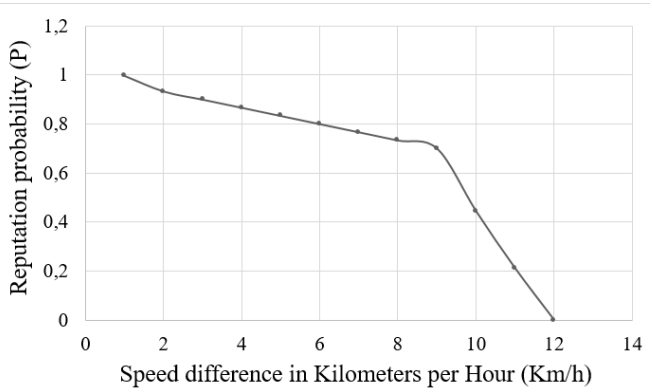

Figure 10. Speed difference analysis

that the score of reputation is reduced with the increase of the speed until reaching the threshold. If the threshold is affected, the reputation decreases quickly. In our situation, the threshold is K. If the speed gets beyond this limit, our vehicle is riskier and added classified as an aggressor on the route.

4) PDR Analysis: From the evaluation of the switched messages, we decide the packet loss ratio (PLR) and the packet delivery ratio (PDR). The acceleration speed is set within a precise range so that the speed does not reach our limit. Each time, the observed node is authenticated to the RSUs. As illustrated in Fig.11, we assess the reputation score of a vehicle by growing the PLR all time until a predefined limit is attained. We observe that when the PLR increases, the reputation decreases, which is logical since the more wrong messages the node forwards on the network, the less reputable the vehicle is on the network.

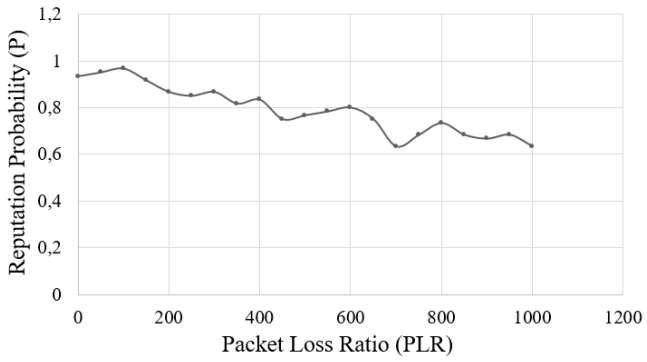

Figure 11. PDR Analysis

B. Response time

In this part, we estimate the delay in each evaluation. We employ the tic toc operate to assess the above delay. Before evaluating the inter-vehicle reputation value, the algorithm runs an authentication check through RSUi. We obtained that the delay grows when the node is not authenticated per RSUi, which creates a time loss that can lead to a DoS attack.

1) Inter-cluster reputation period: From the inter-cluster evaluation, we assess the inter-cluster delay in the network. From the results obtained in Fig.12, we notice that the delay differs between *1.4ms* and *2.5ms*, which is reasonable considering the number of additional checks.

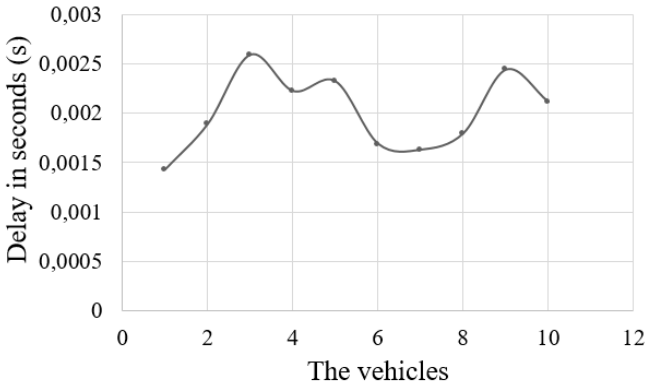

Figure 12. Inter-cluster reputation delay

2) Message analysis time: For the message checking, we assess the message scan time. We set the increase in speed in a definite range so that the speed does not affect our limit. The node is authenticated by the RSUi with an identifier that is not operated by any other neighbor. From the results obtained in Fig.13, we found that the delay increases by *0.3 ms* to 4.5 ms. The delay grows when the number of wrong messages grows, by assuming the time failure associated with the diffusion of wrong messages.

3) Speed assessment time: From the evaluated speed, previously estimated in the previous part, we estimate the delay of the speed evaluation. From Fig.14, we found that the delay ranges from *0.834 ms* to *4.27 ms*. The delay grows as the speed difference increases.

4) Study of the cases: In this part, we estimate the delay introduced by the speed evaluation process in urban and rural areas.

Case 1: Urban area From the speed evaluation in the urban area, we notice that the delay varies between *0.2 ms* and *0.3 ms* in Fig. 15, which is reasonable as long as the speed is within the standards.

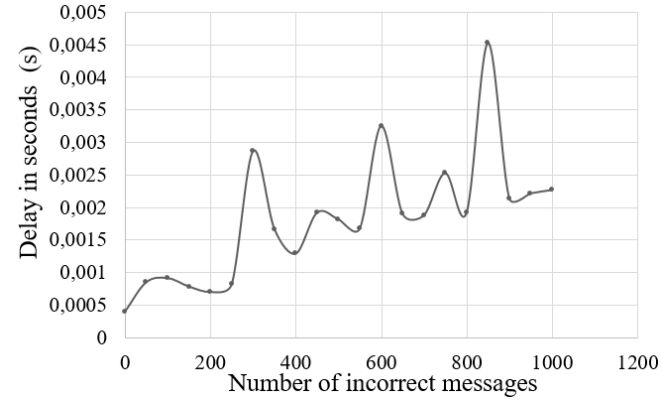

Figure 13. Message scan delay

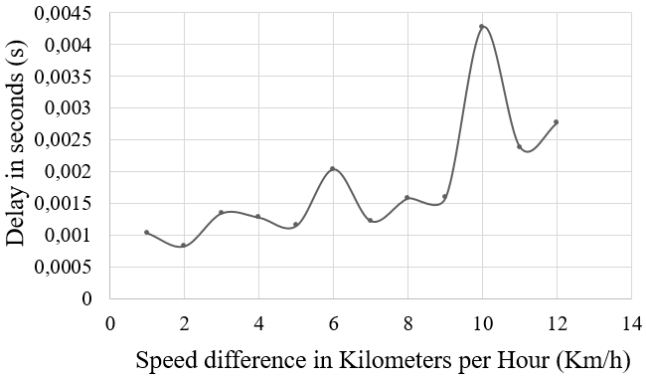

Figure 14. Speed difference scan delay

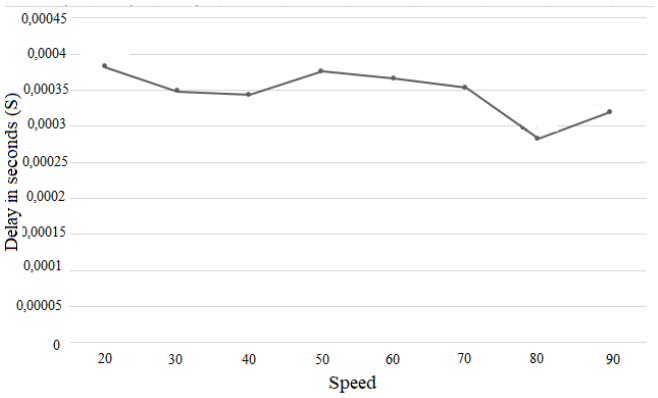

Figure 15. Delay of the speed evaluation in the urban area

Case 2: Rural area : In rural areas, we found that the delay increases compared to urban areas but still remains between *1 ms* and *2 ms* as shown in Fig. 16.

V. Discussion

In this part, we confront some existing work with related works, in terms of the metrics shown in Table 5. For the sake of comparison, we evaluate our approach against similar ones, such as the approach proposed in [27], named ”Procedure for Fog Node Determination and Resource Distribution (PDD)”. This method suggests a reputation-based service

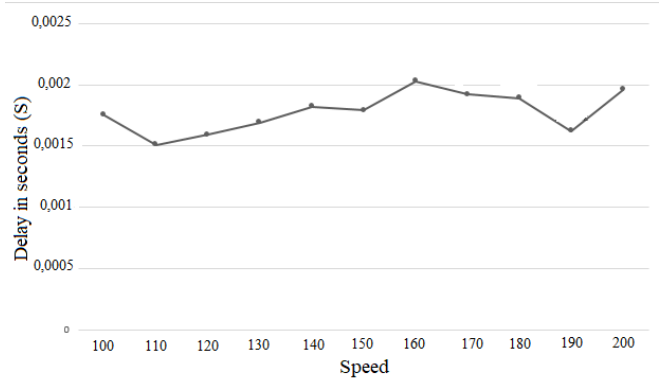

Figure 16. Delay of the speed evaluation in the rural area

strategy and reputation management plan, including updating the decentralized reputation and the global synchronization of reputation in the architecture of the Cloud Vehicular. The objective is to prevent fog vehicles from providing poor quality IT services by optimizing the reputation acquired by all fog vehicles in service during the ideal period.

Table V
COMPARATIVE ANALYSIS

	Id	PDR	Speed	Delay	Inter-cl	Intra-cl
V. V [21]	×	√	×	×	√	×
G. P [22]	√	√	×	×	×	×
F. N [23]	√	√	×	×	×	×
D. R[24]	√	×	×	×	×	×
J. B[25]	√	×	×	×	×	×
L. T[26]	×	×	×	×	√	×
ch. T [27]	×	√	×	×	√	×
R. J [28]	×	√	×	×	√	×
S. Su [29]	×	√	×	×	√	×
This work	√	√	√	√	√	√

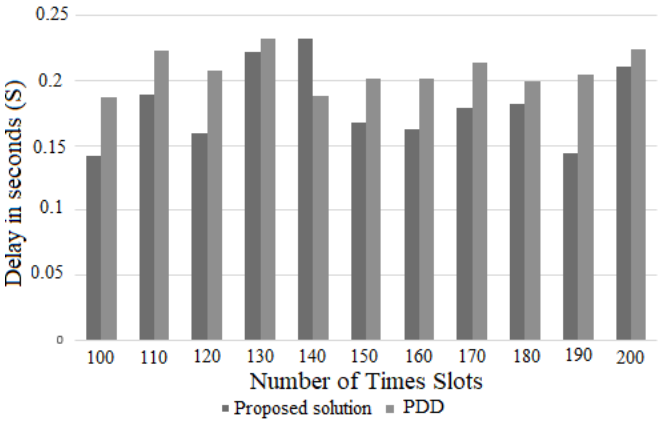

Figure 17. Performance comparison with PDD w.r.t. the response delay

Furthermore, in [28], the "Task-Based Experience Reputation (TER)" method assigns different values to different tasks to determine their urgency and significance. Reputation is calculated on the basis of the distance from previous reputation values. Furthermore, we conducted a series of additional experiments to compare our approach with the one proposed in [29], named Iterative Reputation Management (IRM). This iterative method controls the reputation of a vehicle, taking

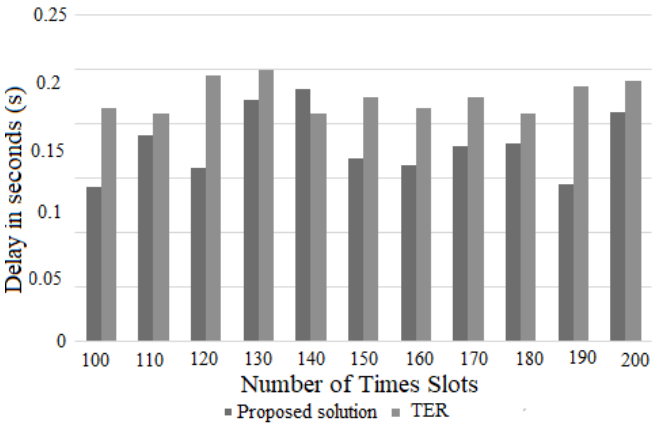

Figure 18. Performance comparison with TER w.r.t. the response delay

into account the constant ratio that is formed during each iteration. Figures 17 and 19 present the results, where the y-coordinate indicates the response time. In these simulations,

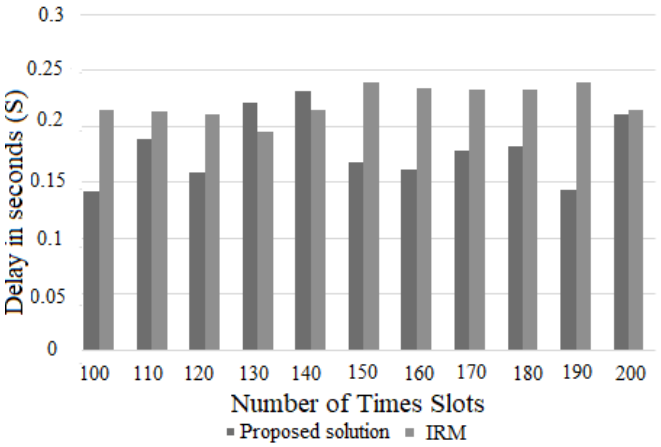

Figure 19. Performance comparison with IRM w.r.t. the response delay

the number of periods is adjusted between 100 and 200, which means that hundreds of service requests are waiting to be processed. From Fig.17, we can see that our method significantly outperforms PDD in terms of response time. Exactly like the TER and IRM approach presented in Figures 18 and 19.

Furthermore, we conducted a second set of experiments to compare our method with the recommendations presented in [27], [28], and [29]. Fig. 20 highlights that our reputation values are generally higher than those of the PDD. Over time, the reputation values exceed the reputation threshold. This is because all reputation values are correctly evaluated by various factors, which allows vehicles to instinctively choose vehicles with a better reputation when sharing information. This also demonstrates that although malicious cars quickly lose their reputation, the proposed algorithm remains effective in estimating the reputation of the vehicle.

The simulation results are shown in Figures 21 and 22, respectively. It is worth noting that in the simulation we made a separate comparison between our approach and TER. In fact, when comparing our solution with TER, we are consistently above the reputation threshold, while TER fails to achieve this goal. Thus, our method outperforms TER in

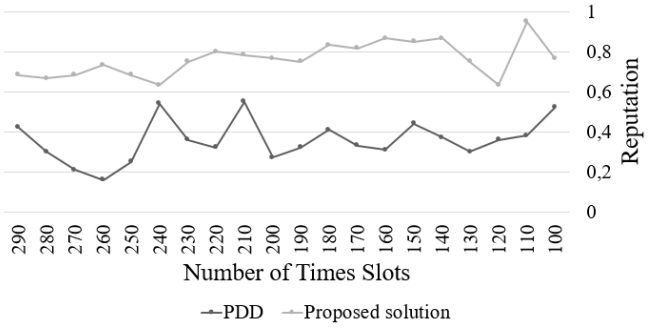

Figure 20. Performance comparison with PDD w.r.t. reputation

terms of the reputation values obtained. Similarly, with IRM, the reputation values of our solution are generally found to be more effective than those of IRM, as shown in Figure 22.

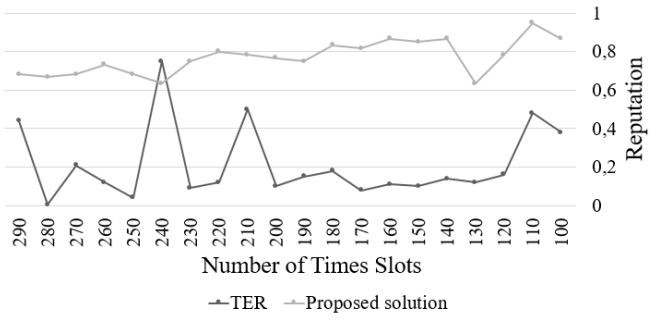

Figure 21. Performance comparison with TER w.r.t. reputation

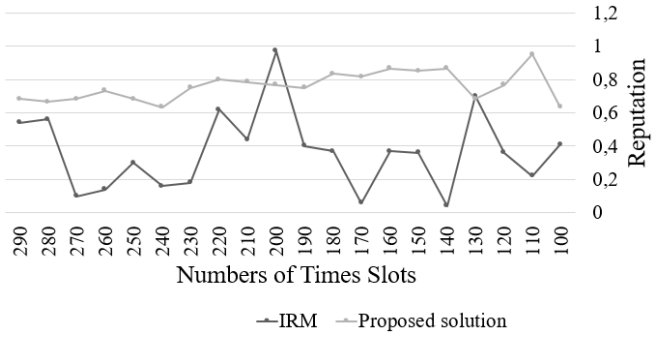

Figure 22. Performance comparison with IRM w.r.t. reputation

VI. Conclusion

Security is an important issue in IoV networks, where we suggest in this paper a reputation management process that separates out mischievous vehicles, i.e., vehicles that have given mistaken information, enormous speed, and fake identities. Vehicles have the ability to transmit information to other neighbors based on their metric value of renewed reputation. As future work, we offer to apply a deep learning algorithm to add intelligence in detecting attacks and to add additional network-based simulators to permit the insertion of other QoS limits such as throughput as reputation assessment conditions.

References

[1] Huy Kang Kim Hyun Min Song, Jiyoung Woo : In-vehicle network intrusion detection using deep convolutional neural network. *Vehicular Communications*, 21(100198):2214–2096, 2020.

[2] Xiao Chen Zhenxiang Chen. Lijun Sun, Qian Yang : Rc-chain: Reputation-based crowdsourcing blockchain for vejournal of network and computer applications,hicular networks. 176:1084–8045, 2021.

[3] AU Rahman S. Iqbal SS Shah, AW Malik et SU Khan : Time barrier-based emergency message dissemination in vehicular ad-hoc networks. *IEEE Access.*, 169(7):16494–16503, 2019.

[4] Mohammad Zulkernine Anika Anwar, Talal Halabi : A coalitional security game against data integrity attacks in autonomous vehicle networks. *Vehicular Communications*, 37(100517):2214–2096, 2020.

[5] SH Jeong et HK Kim H. Lee : Otids : A novel intrusion detection system for in-vehicle network by using remote frame, 2017. I15e conférence annuelle sur la confidentialité, la sécurité et la confiance (PST) , Calgary, AB, Canada, 2017.

[6] Xiewen Wu Mingyang Liu Jiazhen Li Xin Jian Derong Du, Lingqian Wu et Xiaoping Zeng : A novel adaptive clustering algorithm in 3d comp communication for the internet of vehicles. *Engineering Letters*, 32(1):129–135, 2024.

[7] Chenning Liu Shixiang Wan Keqiang Yang Zunzun Hou, Ruichun He et Cunjie Dai : Optimization of passenger and freight collaborative transportation for urban rail transit under virtual coupling condition. *Engineering Letters*, 32(1):179–192, 2024.

[8] Yahui Wang Lingzhi Yi, Yu Yi et Jianlin Li : Speed tracking and train anti-slip control based on active disturbance rejection for freight trains with large inertia. *Engineering Letters*, 32(1):101–111, 2024.

[9] AM Makhlouf et F. Zerai N. Dhibi : Reputation management for trusted vcc architecture, 2020. Paper presented in International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia,https://doi: 10.1109/IWCMC55113.2022.9824735. .

[10] Husanbir Singh Pannu Avleen Kaur Malhi, Shalini Batra : Security of vehicular ad-hoc networks: A comprehensive survey. *Computers Security*, 89(100199):0167–4048, 2020.

[11] Zhaolong Ning Amr Tolba Mubarak Alrashoud Feng Xia Noor Ullah, Xiangjie Kong : Emergency warning messages dissemination in vehicular social networks: A trust based scheme. *Vehicular Communications*, 22(100199):2214–2096, 2020.

[12] Y. Kwang Hooi M. Aasim Qureshi T. Duc Chung A. Rehman, M. Fadzil Hassan et al. : Context and machine learning based trust management framework for internet of vehicles,. *Computers, Materials Continua*, 68(3):4125–4142, 2021.

[13] Deepak Puthal Hesham El Sayed, Sherali Zeadally : Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks,. *Vehicular Communications*, 24(100227):2214–2096, 2020.

[14] S. He et Q. Yang Z. Shen : Quickwalk : Quick trust assessment for vehicular social networks, 2020. Conférence IEEE sur les ateliers de communications informatiques (INFOCOM WKSHPS) , Toronto, ON, Canada.

[15] Liu J. Wang L. et al. Deng, X. : A trust evaluation system based on reputation data in mobile edge computing network. *Peer-to-Peer Networking and Applications*, 13(100227):1744–1755, 2020.

[16] Hui Y. Luan T.H. Liu Q. Xing R. Su, Z. : Reputation based content delivery in information centric vehicular networks. *In* Yilong Hui et Tom H. Luan, éditeurs : *The Next Generation Vehicular Networks, Modeling, Algorithm and Applications.*, page 29–47. Springer, 2020.

[17] Farzaneh N. Behzad, D. : A novel trust management method to preserve privacy in vehicular ad-hoc networks. *Peer-to-Peer Networking and Applications*, 14:1118–1131, 2021.

[18] Xu Y. Su Z. Zhu, Z. : A reputation-based cooperative content delivery with parking vehicles in vehicular ad-hoc networks. *Peer-to-Peer Networking and Applications*, 14:1531–1547, 2021.

[19] Nadia B.A. Lamjed B.S. Ouechtati, H. : A fuzzy logic-based model for filtering dishonest recommendations in the social internet of things. *Journal of Ambient Intelligence and Humanized Computing*, 14:6181–6200, 2023.

[20] A. Rachini et L. Khoukhi Y. Begriche, R. Khatoun : A reputation system using a bayesian statistical filter in vehicular networks, 2020. Sixième conférence internationale 2020 sur les services mobiles et sécurisés (MobiSecServ) , Miami Beach, FL, États-Unis, 2020, pp. 1-7.

[21] Z. Jadidi V. Venkatraman, S. Pal et A. Jolfaei : A conceptual trust management framework under uncertainty for smart vehicular networks, 2022. IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2022, pp. 1-7.

[22] S. S. Kanhere G. D. PUTRA, V. Dedeoglu et R. JURDAK : Toward blockchain-based trust and reputation management for trustworthy 6g networks. *IEEE Network*, 36(4):112–119, 2022.

[23] Shen S. Wu C. Q. Yao J. FAN, N. : A hybrid trust model based on communication and social trust for vehicular social networks. *International Journal of Distributed Sensor Networks,*, 18(5), 2022.

[24] A. Chakraborty D. RAJAVEL et S. MISRA : Mobitrust: Trust-aware pricing scheme for edge-based mobile sensor-cloud for vehicular iot. *IEEE Transactions on Vehicular Technology*, 71(9):10033–10043, 2022.

[25] T. Wang S. Zhang N. N. Xiong J. BAI, Z. Zeng et A. LIU : Tanto: An effective trust-based unmanned aerial vehicle computing system for the internet of things. *IEEE Internet of Things Journal*, 10(7):5644–5661, 2023.

[26] Wang T Ming Z Li X Ma M. LI T, Liu W : Trust data collections via vehicles joint with unmanned aerial vehicles in the smart internet of things. *Transactions on Emerging Telecommunications Technologies*, 2020.

[27] Chaogang TANG et Huaming WU : Reputation-based service provisioning for vehicular fog computing. *Journal of Systems Architecture*, 131(102735):1383–7621, 2022.

[28] P. Flocchini RJ ATWA et A. NAYAK : A fog-based reputation evaluation model for vanets, 2021. Paper presented at the International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1-7.

[29] S. Liang S. Li S. Du S. SU, Z. Tian et N. GUIZANI : Reputation management scheme for efficient malicious vehicle identification over 5g networks, 2020. Paper presented in IEEE Wireless Communications https://doi: 10.1109/MWC.001.1900456. .