JOIN (Jurnal Online Informatika)
p-ISSN: 2528-1682, e-ISSN: 2527-9165
Volume 10 Number 2 | December 2025: 362-371
DOI: 10.15575/join.v10i2.1632

A Trust-Based Reputation System for Security in the Internet of Vehicles (IoV)

Nozha Dhibi[1], Amel Meddeb Makhlouf[2], Faouzi Zerai[3]
[1,2,3]University of Sfax, NTS'com, Sfax, Tunisia

Article Info

Article history:

Received May 09, 2025
Revised June 05, 2025
Accepted July 13, 2025
Published November 10, 2025

Keywords:

Attack
Internet of Vehicles (IoV)
Reputation
Security
Trust

ABSTRACT

The Internet of Vehicles (IoV) integrates with different nodes, like for example connected vehicles, roadside units, etc. Due to communication exchange, they are exposed to various attacks on the network, which poses a security risk. Nevertheless, security is a major concern in IoV networks, especially during data transmission. To address this issue, our team suggest an innovative approach. reputation management schema in an IoV environment to detect attacks at an early stage based on vehicle and driver behavior along with network state. Our algorithm combines direct and indirect trust with various metrics like Packet Lost Rate (PLR), vehicle speed distance between neighbors, alert content, and link quality. These metrics are used to compute a reputation score to identify malicious nodes. Based on its reputation, vehicles communicate with only trusted nodes. After assessment, we see that our solution surpassed the others solution and has demonstrated superior effectiveness in detecting abnormal vehicles. Furthermore, the computed delay, equal to 4.7 ms, does not affect the network communications, which is interesting for the introduced safety features.

Corresponding Author:

Nozha Dhibi,
University of Sfax, NTS'com, Sfax, Tunisia
El Ons City, Tunis Road, 3018, Sfax, Tunis
Email: dhibi.nozha@gmail.com

1. INTRODUCTION

Internet of Vehicles (IoV) is the branch of IoT technologies that has been implemented in vehicles [1][2]. IoV is the evolution of traditional Vehicle Ad Hoc Networks (VANETs) that introduce new technologies into intelligent connected vehicles [3]. Through various network technologies, IoV network communication is intended to support real-time data exchange on transportation between cars and infrastructures, vehicles and other vehicles, vehicles and sensors, and vehicles and everything else [4]. Important distinctions exist between IoV [5][6]. One of the primary functions of Intelligent Transportation Systems (ITS) is carried out by the Internet of Vehicles (IoV), an integrated network made up of wireless technologies, central servers, linked vehicles, and road infrastructure [7][8]. In addition, IoV provides secure transportation and control, learning, and intelligence capabilities to predict vehicle user goals. Currently, IoV focuses mainly on communication between vehicles and RSUs [9], where each vehicle collects driving information using onboard devices to be shared between automobiles and RSUs in order to increase traffic efficiency [11] [10]. Furthermore, in IoV, the way cars interact with one another reveals the information that is exchanged between them, including the vehicles' current status, including their speed., PLR (Packet Loss Rate) and distance, and is employed to determine the state of traffic on the roads. [12]. However, information interchange between vehicles is used to assess the traffic situation on the roadways, but it is a challenging process because IoV nodes are susceptible to several types of network attacks, which puts data sharing and storage at risk [13]. Attacks pointing out IoV networks result in serious consequences, such as failure of information, incorrect

warning messages, and vehicle speed due to wireless connection. Various issues that impact road safety, emphasize how urgently strict safety regulations are needed to protect against such hazards. [14][15]. The IoV uses a number of privacy-preserving techniques, including encoding, differential confidentiality, and zero-knowledge proofs, which require implementing security for users at several levels [16]. In fact, there exists a wide range of security solutions that researchers have proposed, but these existing solutions have limits when it comes to identifying mischievous vehicles on the Internet of Vehicles, and these methods require many round-trip exchanges [17]. To address these challenges, we propose a reputation management scheme for IoV by rejecting malicious vehicles and warning neighbors to allow trusted vehicles to communicate securely and save communication bandwidth [18]. The proposed scheme assigns to each vehicle's reputation score based on their speed, the Packet Loss Rate (PLR), alert content, link quality, and distance. Based on this score, vehicles can be accepted or refused to use the network [19].

The trust management system is used in different architectures, and it was proposed to secure communications and data. Several works have been published in the literature, such as Soumaya et al. [18] to present a strategy for managing trust that builds confidence between the two parties. The subjective three Value Logic Scheme (3VSL) is used to produce a direct trust score, which forms the basis of their trust system. An indirect trust score based on reputation is added to this. Their contacts with one another form the foundation of their trust. In other words, a continuous opinion space derived from two components is taken into consideration when they exchange data and seek direct trust. The first considers the evaluation prior to caching, which focuses on assessing the cache provider's credibility based on the message (request) it issued, and the second considers the quality of the service provided following caching. To compute the indirect reputation of a cache provider, they consider the following factors: The interaction frequency, the interaction freshness, and the interaction Effects. In this work, only the interactions between entities are a factor for the calculation of the reputation score. In another work [19], authors have suggested a technique called the Social Internet of Vehicles—Fuzzy-based Trustworthy Friendship Selection Algorithm—Crossover-boosted Arithmetic Optimization Algorithm (SIoV-FTFSA-CAOA) seeks to provide safe data exchange between vehicles in the SIoV network. The design of the technique consists of multiple steps, beginning with the Fuzzy-based Trustworthy Friendship Selection Algorithm (FTFSA), which determines the trust score by taking into account three input factors: social context, community reputation, and previous contacts. The trust calculation in this approach was based on the information linked by vehicle, i.e., the calculation is non-distributed.

In the same direction, the work published in [20] suggested a method that uses one parameter to calculate trust scores. Specifically, according to the accuracy of the messages sent by the vehicle to initiate or verify event messages. The confidence factor is calculated for each vehicle. A vehicle can earn reward points, which are incentives that can be used at a later time. The vehicle's previous communication with peer vehicles is discussed using the trust factor value. Moreover, the researchers in [21], to preserve the dependability of the FL (Federated Learning) process within the ITS, a decentralized and secure reputation system based on blockchain technology was proposed. This system maintains the integrity of the FL training process by managing the reputation data of individual nodes, such as vehicles. In this context, when determining a vehicle's reputation, the following elements are taken into account: Interaction with the vehicle, Event updates, and Trajectory similarity. In this work, data transmission is carried out from a new distributed architecture based on Edge, it protects ITS from newly emerging attacks using blockchain and FL. The reputation score in this approach is calculated based on the information linked by vehicle, i.e., the calculation is non-distributed.

The authors in [22] suggested an IoV-based hostile vehicle detection system that uses spatiotemporal traffic flow features under cloud fog computing. They suggested a reputation calculation mechanism, which established to score each vehicle by the fog server according to the verification of the traffic data uploaded by the vehicle and the traffic data predicted by a constructed prediction model, then it calculates the reputation score of the vehicle based on the calculated credibility, which is used to judge whether the vehicle is malicious according to its reputation score. Furthermore, a reputation management scheme was presented in [23], which proposed an enhanced method for multi-source, multi-weight subjective logic. Using the subjective logic trust model, this method combines nodes' direct and indirect opinion feedback while taking timeliness, familiarity, event validity, and trajectory similarity into account. Reputation criteria are used to identify aberrant vehicles, and vehicle reputation values are updated on a regular basis. Compared to other algorithms, the Multi-Source Multi-Weight Subjective Logic method (MSMWSL) can reduce the reputation values of misbehaving vehicles more quickly under various thresholds, allowing for a quicker distinction between aberrant and regular

vehicles. This method can enhance the security of information sharing inside a network and successfully remove possible security issues. The MSMWSL algorithm can detect odd vehicles at a high rate when the reputation threshold is less than the usual value of 0.5. This enhances the system's overall defensive capabilities against abnormal vehicles by allowing the quick identification of abnormal vehicles in each detection cycle under various reputation values. It employs a Vehicular Edge Computing (VEC) approach to address issues including task delay and constrained vehicle resources. To improve the quality of communication, as well as the reliability of vehicles based on multiple inter-vehicular interactions, a trust management model based on Additive Increase and Multiplicative Decrease (AIMD) has been suggested in [24].

Additionally, depending on how accurate the communications are, the suggested method offers rewards and penalties on the trust value. A reward and penalty mechanism make up the reputation evaluation algorithm. In order to control any harmful conduct, the reward penalty mechanism periodically determines the trust value in the IoV network for message broadcasting in the automotive environment using the AIMD approach and distributes it among the trusted authorities. Blockchain technology is used by a three-tier trust management architecture to monitor vehicle interactions and dynamically allocate reputation and trust ratings in response to such interactions. In this architecture, data transmission is carried out through the National Trust Authority (NTAs), State Trust Authority (STA), and City Trust Authority (CTA) are the trusted authorities. In the context of the Internet of Vehicles, a Tamper-Proof Device (TRD) exchanges communications with other nodes, including vehicles. System settings, keys, and pseudo-identities are among the private data that TRD protects for safe communication. In the same context and to improve the reliability of message authentication, [25] suggested a reputation evaluation system as the foundation for the Blockchain-Assisted Message Authentication Scheme (BAMAS). Additionally, a reputation evaluation technique is put forth to gauge the veracity of communications. This mechanism can be incorporated into message authentication to accomplish effective message reliability verification. In this work, only the feedback is a factor for the calculation of the reputation score. However, Table 1 allows us to identify the boundaries of its applicability and thoroughly solve the problems and shortcomings of the earlier work, including the current trust, reputation, and security procedures.

Table 1. Literature review

Author, Year	Method	Archived criteria	Limitations
Soumaya et al. [18], 2024	Utilizing a three-valued subjective logic paradigm, the trust management approach is founded on reputation value.	Credibility Service score, Interaction Frequency, Interaction Freshness, Interaction Effects	Only use interactions to calculate the reputation score
Jegatheesan, D et al. [19], 2024	Three input factors are used by the FTFSA algorithm to determine the trust score.	Past interactions, Social context, Community reputation	The trust calculation is calculated based on the information linked by vehicle i.e., the calculation is non-distributed.
Gaba, P et al. [20], 2024	Security Architecture Powered by Blockchain for a Networked Vehicle Fog Environment (B-SAFE)	The correctness of messages	Only use the accuracy of messages sent for trust score calculation
Abou El Houda A et al. [21], 2024	Blockchain-based decentralized and secure reputation system to uphold the FL's dependability and credibility	Vehicle interaction, Event updates, Trajectory similarity,	The reputation score is calculated based on the information linked by vehicle i.e., the calculation is non-distributed.
K. Gu, et al. [22], 2024	A method for detecting hostile vehicles using spatiotemporal traffic flow characteristics under cloud-fog computing-based IoVs	Traffic data	Only use the traffic data to calculate the reputation score

To overcome the limitations of the studied research works, where only intrusion features are separately considered by authors and the trust vs reputation computing is only based on traffic or on event features, we propose a reputation management system, which is founded on both direct and indirect confidence calculation, the reputation calculation is distributed on several factors such as the speed, the messages exchanged, the distance between the vehicles, the content of the messages exchanged and the quality of the links, all these parameters are taken into consideration for the reputation calculation in order to reduce the number of malicious nodes by giving the malicious vehicles a bad reputation value to exclude them from the network.

2. METHODOLOGY

We noticed that the shift to fog computing to address current issues has been prompted by the drawbacks of cloud computing and conventional VANET systems. In response, our team proposes an algorithm to calculate the reputation score for each connected vehicle. Our proposed approach addresses key requirements such as malicious vehicle detection and secure alert exchange in a reliable and privacy-friendly solution. Firstly, the process starts with the selection of vehicles authenticated with the RSUs located on the sides of the roads and gives them an initial score of reputation. Secondly, the authenticated vehicle having the ability to communicate with neighboring nodes is evaluated according to the messages exchanged between nodes, speed, and distance by the Direct Trust Score (DTS) calculation. Thirdly, the calculation of the Indirect Trust Score (ITS) uses the vehicle's environment. We verify the alerts' content and the link quality to evaluate the ITS. Fourthly, these scores are combined in the reputation aggregation module with σ1, σ2, and σ3 weighting factors, and Ri stands for the initial reputation score. The weights reflect the importance of the factor in terms of risk. Next, a predetermined threshold is compared to the new reputation score. Finally, our vehicle gets connected to the network when the score is equal to or higher than the threshold. When the score goes below the stated threshold, the vehicle is kicked out of the network, and an alert is raised. This also provides a way of keeping only trustworthy vehicles in the network to preserve its security and effectiveness. Algorithm 1 shows the proposed monitoring process, where its functions are detailed in the following sections.

Algo. 1. Monitoring process
Data: *Vi*
Result: *Rupdate "The updated reputation"*

1. **for each vehicle entering the network, g**o to algorithm 2.
2. **if** *Vi* communicate with neighbors **then**
   a. PLR ← number of lost packet/ numbers of delivered packet; T1 ← 1-PLR;
   b. Speed = $\sum_{t=0}^{n} \frac{\sqrt{(x2-x1)^2-(y2-y1)^2}}{t}$;
      if speed<th1.1 **then** T2 ← 0;
      else if speed>th1.1 and speed<th1.2 **then** T2 ← 1;
      else if speed>th1.2 **then** T2 ← 0;
      end if
      end if
      end if
   c. Distance = $\sqrt{\sum (x1(i) - x2(i))^2}$;
      if distance >th2 **then** T3 ← 1;
      else T3 ← 0;
      end if
   d. Direct trust score ← α1 × T1 + α2 × T2 + α3 × T3 ;
   e. **if** message received = message delivered **then** T4← 1; **else** T4← 0;
      end if
   f. Link quality = $\frac{SRi-min(SR)}{max(SR)-min(SR)}$;
      T5← link quality;
   g. Indirect trust score ← β1× T4 + β2 × T5 ;
3. Rupdate= σ1 × Ri + σ2 × DTS + σ3 × ITS;
   if Rupdate> th3 **then** Vehicle linked to network;
   else Reject from network and generate alert;
   end if

end if
end for

p-ISSN: 2528-1682
e-ISSN: 2527-9165

2.1. Initial Reputation Calculation

The selection of vehicles is executed in Algorithm 2. It starts with Vi, which is a vehicle authenticated by a set of selected RSUs in their zone. Each time a vehicle requests authentication with RSU, the RSU consults its DB, which contains a list of identifiers previously authenticated with RSUs if the vehicle IDVi exists in this DB so a variable Auth is incremented. If all the RSUs authenticate with Vi, an initial score of reputation Ri is equal to 1; else if no RSUs authenticate with Vi, then Ri is equal 0; else Ri is calculated according to Equation (1).

$$Ri = \frac{\sum_{j=1}^{n} Auth}{n} \quad (1)$$

```
Algo. 2.  Initial reputation calculation authentication algorithm
Data: IDVi, RSUj
Result: Ri,
for RSUj from 1 to n do
   if IDVi exist in DB then Auth ← Auth+1;
end
if Auth=n then Ri← 1;
else if Auth=0 then Ri← 0;
else
Ri calculated with Eq1;
end
end
end
```

2.2. Direct Trust Score Computing Process

The flowchart outlines our method for calculating the DTS in the network, based on three factors: PLR, Speed, and Distance. In the case of PLR, when the PLR value decrees, the first factor T1 increases, which means that the selected vehicle has more credibility in the network. For the second factor, the speed is calculated with the Equation (2) and compared with an interval. If the speed of the selected vehicle does not exceed the interval, the second factor T2 increases else T2 decreases. Lastly, the distance between vehicle Vi and the other nodes is calculated based on Equation (3). If the distance lowers a threshold predefined, the vehicle becomes dangerous and the third factor T3 equals 0. The DTS is typically calculated with Equation 4 is the sum of these three elements, with each component receiving an extra weighting factor to represent its relative significance. The weighting variables α1, α2, and α3 indicate the relative importance of each factor, as the equation illustrates. Depending on the needs of the network, these criteria are modified to assign weight to each component.

$$\text{Speed} = \sum_{t=0}^{n} \frac{\sqrt{(x2-x1)^2-(y2-y1)^2}}{t} \quad (2)$$

$$\text{Distance} = \sqrt{\sum (x1(i) - x2(i))^2} \quad (3)$$

2.2. Indirect Trust Score

A node's Indirect Trust Score is determined by using two factors: alert content and link quality. (a) Alert content: The exchanged alert messages are passed through verification tools to check if the content is useful or not. Recipient coordinates, such as the location from where the message is generated, are consistent with the location of the alert content. The gap between the arrival time of the alert and the time from where the alert is generated is measured, and if it exceeds a well-defined threshold, the content of the alert becomes dangerous and destructive. This factor reflects when the vehicle generates an alert, we verify the content of this alert, like the location and the time. If the alert content is true, the fourth factor T4 equals 1, and if the alert does not match, T4 equals 0. (b) Link quality: Equation 4

illustrates how the Received Signal Strength (RSSI) upon normalization determines the fifth factor, which indicates the signal's strength. In this case, the RSSI ith value (SRi) normalized value between 0 and 1 is the Link quality T5 of the ith data value; if the link quality value is less than Th_inf, then it is weak; if it is between Th_inf and Th_sup, then it is reasonable; and if it is above Th_sup, then it is good. The ITS is determined using Equation 5, the product of two factors, T4 and T5, with each element receiving an extra weighting factor β1 and β2 to represent its relative importance in terms of communicating with trusted vehicles and saving communication bandwidth. Based on network requirements, these criteria are modified to assign weight to each component. such as malicious vehicle detection and secure alert exchange in a reliable and privacy-friendly solution.

$$T5=\frac{SRi-min(SR)}{max(SR)-min(SR)} \quad (4)$$

$$ITS = \beta1 \times T4 + \beta2 \times T5 \quad (5)$$

2.3. Reputation Update

Based on the initial reputation score, direct and indirect trust score, we compute the reputation update score as shown in Equation (6) with an additional weighting factor σ1, σ2, and σ3 applied to every component to represent its relative significance. The total of all weighted factors must equal one, and each weighting element must have a value between 0 and 1. The particular requirements of the network and the objectives of the algorithm used to calculate the reputation score will determine the precise numbers allocated to each weighting component.

$$Rupdate= \sigma1 \times Ri + \sigma2 \times DTS + \sigma3 \times ITS \quad (6)$$

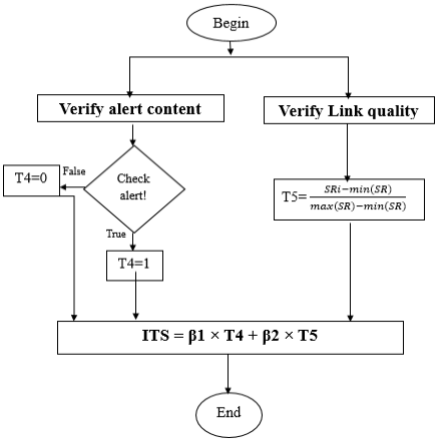

Figure 1. Indirect Trust Score computing process

3. RESULTS AND DISCUSSIONS

3.1. System Setup

In this study, a MATLAB 2024 simulator is used to assess the performance of the suggested approach. In the networks, a variety of vehicle numbers between 10 and 1000 are set up within the 100–1000 m communication range. First, emphasis is placed on the experimental configuration and parameter settings. The performance of our suggested solution is then calculated using a variety of performance criteria, including speed, distance, alert content, link quality, PDR, direct and indirect trust value, and reputation score. The suggested algorithm was contrasted with the BAMAS [16] and MSMWSL [14].

p-ISSN: 2528-1682
e-ISSN: 2527-9165

3.2. Simulations Experiment Parameters

Table 2 displays the parameters used in the simulation experiment.

Table 2. Simulation parameters

Simulation parameter	Worth
MATLAB	2024
PDR	[100…1000]
PLR	30,20,40,15,80,240,30,150,9 0
Average Vehicle Speed	[20...120]
Accelerations	0,2,1,1,4,6,3,5,2,4,6,3
Authentication with RSU	Yes
Number of Vehicle	[10...1000]
Direct Trust weight	α1=0.3, α2=0.3, α3=0.3
Indirect Trust weight	β1=0.3, β2=0.3
Reputation update weight	σ1=0.3, σ2=0.3, σ3=0.3
Reputation threshold	0.5
Minimum value of Threshold	0.3
Maximum value of Threshold	0.8
Type of attacks	Jamming attacks, False data injection attacks

3.3. Simulation Results and Discussions

As illustrated in Figure 2, we estimate the delay depending on the reputation score. For each iteration, if the reputation scores above 0.9167, the delay varies between 0.45s and 0.47s, and if the reputation is under 0.6431, the delay increases to 0.78s, which is reasonable, believing the number of added attacks as jamming or false data injection.

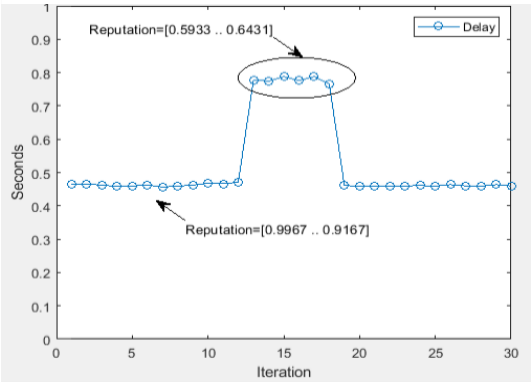

Figure 2. Delay depending on the reputation probability

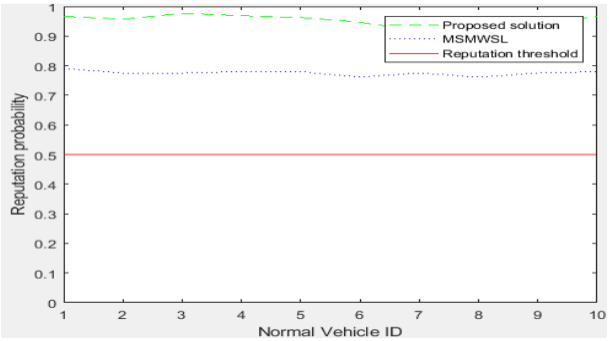

Figure 3. Comparison of the reputation probability of 10 normal vehicles

As illustrated in Figure 3, ten typical vehicles were chosen at random for reputation updates during the observation period, and each vehicle interacted with one another at random. All of the trusted

vehicles in Figure 3 have reputation values over the reputation threshold. Furthermore, the suggested algorithm's computed result is typically superior to that of the MSMWSL algorithm [14]. This is so that vehicles can choose vehicles with better reputations when exchanging information in an intuitive manner because all reputation calculation values are appropriately weighted by a variety of parameters. This demonstrates that the suggested approach still does a good job of calculating the reputation of typical vehicles even while it rapidly reduces the reputation values of harmful vehicles.

Ten malevolent vehicles were chosen for reputation updates during the observation period, as illustrated in Figure 4, and all of the vehicles engaged in random interactions with other vehicles. All malevolent vehicles had reputation values below the Reputation threshold, as seen in Figure 4. Furthermore, the harmful vehicles' reputation value under our method is smaller than that of the malicious vehicles using the MSMWSL algorithm [14]. This is due to the fact that the suggested method takes into account a number of variables, including PDR, speed, distance, warning content, and link quality. This makes it possible for the system to determine reputation more precisely, which speeds up the process of identifying malicious vehicles.

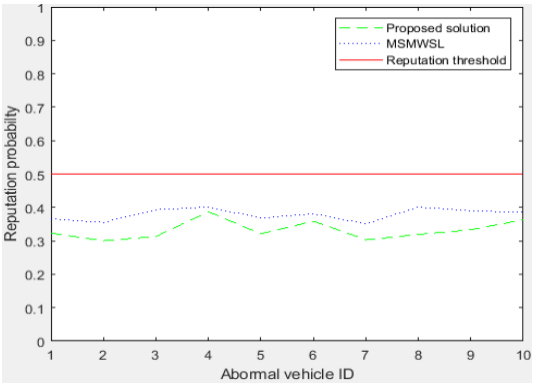

Figure 4. Comparison of reputation probability of 10 abnormal vehicles

At first, in an effort to build system confidence, this anomalous vehicle tended to give other vehicles high-quality data. However, because of anomalous behavioral occurrences, the vehicle's reputation value steadily declines during the detection window. In contrast to the MSMWSL algorithm, the reputation value of the aberrant vehicles under our system decreased noticeably more quickly, as seen in Figure 5 [14]. Following the initial detection cycle, our algorithm's value was lower than the MSMWSL algorithms, and the reputation values fell below the 0.5 reputation threshold. In the end, our algorithm's reputation value for the anomalous vehicles was substantially lower than the other algorithm's reputation value over all detection cycles. This is due to the use of multiple parameters and factors such as speed, message exchange distance, alert content, and link quality to calculate the direct and indirect trust and to evaluate the vehicles well and give accurate reputation values. Overall, the suggested method performed better than the alternative algorithm and showed increased anomalous vehicle detection efficiency.

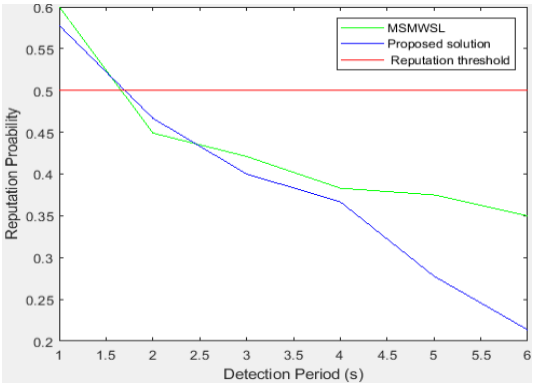

Figure 5. The anomalous vehicle reputation value's evolution over the discovery time

p-ISSN: 2528-1682
e-ISSN: 2527-9165

Figure 6 shows the results of the simulation. We can see that the average message delays of our scheme and the BAMAS scheme [16] both rise sharply as the number of vehicles increases, reaching 40 ms and 45 ms, respectively. This is likely due to the time failure associated with the diffusion of incorrect messages. Our method has a somewhat lower average message delay than BAMAS.

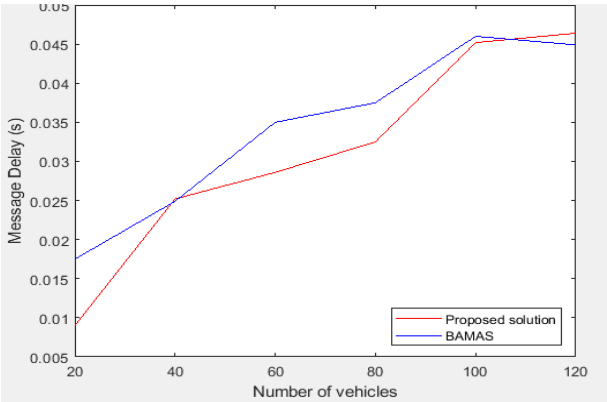

Figure 6. Comparison of average message delay

Figure 7 shows that the mes-sage loss rate is less than 0.1 when there are fewer than 30 vehicles. The message loss rate rises with the number of vehicles. The message loss rate of BAMAS [16] and our system actually increased from 0 to 0.45. Channel congestion and buffer overflow will eventually result from the increased number of vehicles and messages. It is clear that our system consistently has a lower message loss rate than BAMAS [16].

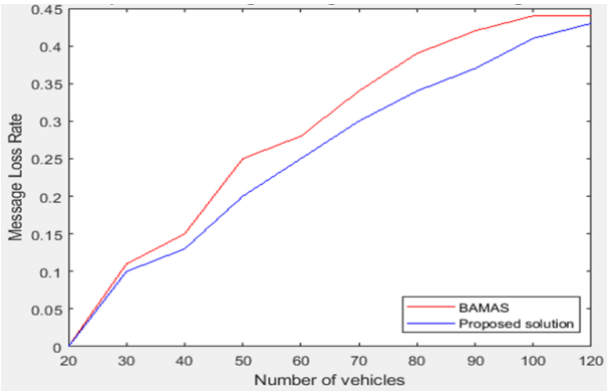

Figure 7. Comparison of average message loss rate

4. CONCLUSION

Security is an important issue in IoV networks, where we suggest in this paper a reputation Assessment to identify malicious nodes, i.e., vehicles that have given fake alert content, enormous speed, don't respect the distance between neighbors and they have low link quality. These metrics are used to compute a reputation score. Based on its reputation, vehicles communicate with only trusted nodes. We suggest using other network-based simulators in future research to enable the inclusion of additional quality of service metrics, such throughput, as reputation evaluation criterion. Additionally, the adopted cloud network security rating is not applied as a vehicle reputation criterion, which may lessen the likelihood that attackers will target this cloud network.

REFERENCES

[1] Yang, C., Ma, Y., Xie, B. et al. Multi-user covert communication in power internet of things networks. Int. J. Inf. Secur. 24,

49 (2025). https://doi.org/10.1007/s10207-024-00960-7

[2] Zainab Saadoon Naser, Hend Marouane Belguith, Ahmed Fakhfakh, (2024), Traffic Management Based on Cloud and MEC Architecture with Evolutionary Approaches towards AI: A Review, "International Journal of Online and Biomedical Engineering", pp. 19-36, https://doi.org/10.3991/ijoe.v20i12.49787

[3] Iturbe-Araya, J.I., Rifà-Pous, H. Enhancing unsupervised anomaly-based cyberattacks detection in smart homes through hyperparameter optimization. Int. J. Inf. Secur. 24, 45 (2025). https://doi.org/10.1007/s10207-024-00961-6

[4] Dhibi, N., Makhlouf, A. M., & Zerai, F. (2025). Reputation-based Security for IoV Environment. IAENG International Journal of Computer Science, 52(4).

[5] Ouechtati, H., Nadia, B.A. and Lamjed, B.S. A fuzzy logic-based model for filtering dishonest recommendations in the Social Internet of Things. J Ambient Intell Human Comput 14, 6181–6200 (2023). https://doi.org/10.1007/s12652-021-03127-7

[6] N. Dhibi, A. M. Makhlouf and F. Zerai, , (2022), " Reputation management for trusted VCC architecture," 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatiapp. 737-742, doi: 10.1109/IWCMC55113.2022.9824735.

[7] Chaogang Tang, Huaming Wu, (2022), Reputation-based service provisioning for vehicular fog computing, Journal of Systems Architecture, Volume 131, 102735, ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2022.102735.

[8] Anika Anwar, Talal Halabi, Mohammad Zulkernine, (2022), A coalitional security game against data integrity attacks in autonomous vehicle networks, Vehicular Communications, Volume 37, 100517, ISSN 2214-2096, https://doi.org/10.1016/j.vehcom.2022.100517

[9] Soumaya Bounaira, Ahmed Alioua, Ismahane Souici, Blockchain-enabled trust management for secure content caching in mobile edge computing using deep reinforcement learning, Internet of Things, Volume 25, 2024, 101081, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2024.101081.

[10] Jegatheesan, D., Arumugam, C. SIoV-FTFSA-CAOA: a fuzzy trust-based approach for enhancing security and energy efficiency in social internet of vehicles. Wireless Netw (2024). https://doi.org/10.1007/s11276-023-03626-9

[11] Gaba, P.; Raw, R.S.; Kaiwartya, O.; Aljaidi, (2024), M. B-SAFE: Blockchain-Enabled Security Architecture for Connected Vehicle Fog Environment. Sensors 2024, 24, 1515. https://doi.org/10.3390/s24051515

[12] Z. Abou El Houda, H. Moudoud, B. Brik and L. Khoukhi, "Blockchain-Enabled Federated Learning for Enhanced Collaborative Intrusion Detection in Vehicular Edge Computing," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 7, pp. 7661-7672, July 2024, doi: 10.1109/TITS.2024.3351699.

[13] K. Gu, X. Ouyang and Y. Wang, (2024), "Malicious Vehicle Detection Scheme Based on Spatio-Temporal Features of Traffic Flow Under Cloud-Fog Computing-Based IoVs," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2024.3369974.

[14] Liu, Q.; Gong, J.; Liu, Q. Blockchain-Assisted Reputation Management Scheme for Internet of Vehicles. *Sensors* 2023, *23*, 4624. https://doi.org/10.3390/s23104624

[15] Srivastava, S., Agarwal, D., Chaurasia, B.K. et al. Blockchain-based trust management for data exchange in internet of vehicle network. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-18874-w

[16] Li, H., Han, D. Blockchain-assisted secure message authentication with reputation management for VANETs. J Supercomput 79, 19903–19933 (2023). https://doi.org/10.1007/s11227-023-05394-x

[17] [17] R. Chen and Y. Guan, "Hierarchical Reputation Consensus Model for VANET," in IEEE Access, vol. 13, pp. 3521-3531, 2025, doi: 10.1109/ACCESS.2024.3525188.

[18] Shan, Y. (2025). AN EFFICIENT CROSS-DOMAIN AUTHENTICATION SCHEME FOR INTERNET OF VEHICLES (IOV) BASED ON REPUTATION. Journal of Computer Science and Electrical Engineering ISSN: 2663-1946 DOI: https://doi.org/10.61784/jcsee3040

[19] Su, Z.; Cheng, R.; Li, C.; Chen, M.; Zhu, J.; Long, Y. Federated Learning and Reputation-Based Node Selection Scheme for Internet of Vehicles. Electronics 2025, 14, 303. https://doi.org/10.3390/electronics14020303

[20] D. Mukathe, W. Di, W. Ahmed and T. Worku, "Blockchain-Powered Authenticated Key Agreement Scheme with Reputation-Incentive Mechanism for Vehicle-to-Vehicle Communication in IoV," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2025.3558278

[21] Jain, A., Kumar, A., Mahadev, Chaudhary, J. K., & Singh, S. (2025). Trust-Based Reliability Scheme for Secure Data Sharing with Internet of Vehicles Networks. Internet Technology Letters, 8(2), e70000. https://doi.org/10.1002/itl2.70000

[22] Hussain, M.; Mehmood, A.; Khan, M.A.; Khan, R.; Lloret, J. Reputation-Based Leader Selection Consensus Algorithm with Rewards for Blockchain Technology. Computers 2025, 14, 20. https://doi.org/10.3390/computers14010020.

[23] Siddiqui, S.A.; Mahmood, A.; Sheng, Q.Z.; Suzuki, H.; Ni, W. A Survey of Trust Management in the Internet of Vehicles. *Electronics* 2021, *10*, 2223. https://doi.org/10.3390/electronics10182223

[24] Muhammad Sameer Sheikh, Jun Liang, Wensong Wang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey,", Wireless Communications and Mobile Edge 2020. https://doi.org/10.1155/2020/5129620

[25] Jin, H., Khodaei, M., & Papadimitratos, P. (2017). Security and privacy in vehicular social networks. In Vehicular Social Networks (pp. 155-169). CRC Press.