# Trustworthiness Determination for a Distributed Reputation Management System in VANETs

Samira Chouikhi, Lyes Khoukhi, Abdelhakim Senhaji Hafid, Christophe Rosenberger

# Trustworthiness Determination for a Distributed Reputation Management System in VANETs

Samira Chouikhi
LIS3TN Laboratory, University of Technology of Troyes
Troyes, France
samira.chouikhi@univ-paris-est.fr

Lyes Khoukhi
Normandie Univ, ENSICAEN, UNICAEN, CNRS, CREYG
Caen, France
lyes.khoukhi@ensicaen.fr

Abdelhakim Senhaji Hafid
University of Montreal
Montreal, Canada
ahafid@iro.umontreal.ca

Christophe Rosenberger
Normandie Univ, ENSICAEN, UNICAEN, CNRS, CREYG
Caen, France
christophe.rosenberger@ensicean.fr

## ABSTRACT

In vehicular networks, the vehicles should act positively regarding the collaborative and cooperative tasks to ensure the best performance of the network. Unfortunately, there are always some selfish and non-cooperative vehicles that profit from the network without contributing to its operation. They may cause the waste of the network resources and time when assigned tasks that they will not fulfill. Hence, the identification of such vehicles becomes crucial to enhance network performance. In this paper, we propose a reputation model based on vehicle credibility and trustworthiness to improve the resistance of vehicular networks against non-cooperative vehicles for information routing tasks. The proposed distributed reputation management system consists of a model for reputation calculation. The reputation score or value reflects the behavior of a vehicle (i.e., cooperative or non-cooperative) regarding data routing within the network. This score is given to the vehicle by other network members. The trustworthiness of vehicles is used also to reinforce the efficiency of the system. We first describe how the reputation score of each vehicle is determined, aggregated, and disseminated. We then propose a dynamically adapted scheme for the computation of trustworthiness of vehicles and the selection of trustworthy ones. The effectiveness of the proposed models is demonstrated through extensive simulations.

## CCS CONCEPTS

• **Networks → Mobile and wireless security**.

## KEYWORDS

Vehicular networks, reputation and trust management, trustworthiness, wireless network security

## 1 INTRODUCTION

Since Vehicular Ad-hoc NETworks (VANETs) play crucial role in road safety, traffic management and driving experience, the reinforcement of their efficiency become of central importance. As a member of the network, each vehicle must ensure an efficient network operation by cooperating and collaborating with other members to achieve various network tasks, like detecting events, collecting and routing data, etc. Unfortunately, some vehicles prefer not to contribute to the network tasks but still benefit from its services because of selfishness and/or laziness. The network may lose in terms of resources and latency when it assigns some tasks to these vehicles that will never fulfill them. Hence, the system requires the integration of some mechanisms that allow the identification of non-cooperative vehicles to better manage the distribution of its tasks and improve its operation.

The developed solutions are generally behavior-based, where a vehicle is evaluated regarding its monitored behavior information. Hence, concepts like trustworthiness, credibility, and reputation are introduced to evaluate the vehicle behavior and several works have investigated the reputation and trust problem. In [1] a decentralized collaboration scheme has been developed to improve the resistance of vehicles regarding data integrity attacks in an Internet of Vehicles (IoV) environment. The authors introduced a hedonic cooperative game to prevent misbehaving and malicious vehicles from joining normal vehicles' communities. Begriche et al. [2] proposed a Bayesian statistical filter-based reputation system. The presented approach uses vehicles' collaboration to detect malicious vehicles and prevent them from spoiling the network operation.

A game theory-based trust model for VANETs was presented in [3]. The proposed game was defined as an attacker-defender security game to identify and isolate the malicious vehicles. The players' strategies considered the majority opinion and the node density as parameters. In [4], a security-aware content delivery scheme based on bargaining game was proposed. The game pricing model is introduced to encourage the vehicles and RSUs to act more positively regarding the content delivery. In [5], the authors introduced a reputation system using a cooperative game to identify selfish and malicious nodes. Gyawali et al. [6] proposed a misbehavior detection system (MDS) based on machine learning and reputation. The reputation score is used in Dempster-Shafer theory-based collaborative misbehavior detection system. In [7], a novel software-defined trust based VANET architecture was proposed. The trust of each vehicle and the reverse delivery ratio are considered in a joint optimization problem, which is modeled as a Markov decision process with state space, action space, and reward function.

In our work, we focus on an efficient reputation management system for isolation of non-cooperative vehicles during data routing. These vehicles disrupt the data transmission, which leads to severe network operation deterioration. Reputation management provides tools to reward the cooperative vehicles and punish the

non-cooperative ones. To support the increasing number of vehicles, we prefer a distributed management model, where the reputation of an individual is determined and updated based on the evaluation given by others towards this individual and aggregated locally. Hence, a vehicle reputation should aggregate the collected reputation scores given by other vehicles regarding their opinions towards the vehicle behavior. Moreover, the reputation management system must consider the quality of each reputation score based on the evaluating vehicle. Thus, the scores need to be well weighted to increase the reputation accuracy. In addition, we use some trustworthy vehicles to improve the accuracy of reputation and credibility values. The determination of vehicles' trustworthiness and the selection of trustworthy vehicles are investigated.

The rest of this paper is organized as follows: in Section 2, we propose a distributed reputation system model. In Section 3, we detail the determination of vehicles' trustworthiness and the selection of trustworthy vehicles. Section 4 is dedicated to the performance evaluation. Finally, Section 5 concludes the paper.

# 2 REPUTATION MANAGEMENT SYSTEM

## 2.1 Basic Concepts

In this section, we define the concepts and terms used for the reputation management model in vehicular network.

*2.1.1 Reputation.* The reputation is defined as the notoriety of a vehicle for some specific tasks such as events detection and warning, data routing participation, etc. The reputation of a vehicle is computed based on the behavior of this vehicle observed by its peers within the network. This concept allows the classification of the vehicles into two groups: Well behaving vehicles, and misbehaving vehicles.

*2.1.2 Trustworthiness.* The trustworthiness depicts whether a vehicle is worthy of being trusted, honest and reliable, or not. When a vehicle is considered trustworthy, other vehicles can blindly trust it any networking task. This vehicle has a high degree of security so any information coming from it is considered correct without any doubt. However, when we classify a vehicle as not trustworthy, it does not mean that the vehicle is misbehaving or malicious. It just means that it is a common vehicle that cannot be trusted at 100%.

*2.1.3 Credibility.* The credibility identifies a vehicle as credible/honest when it returns correct reputation scores, and incredible/dishonest otherwise. We assume that only malicious vehicles could be dishonest which means that a misbehaving vehicle is honest if it is not malicious.

## 2.2 Network Model

We consider a VANET including $N$ nodes and a Road Side Unit (RSU). We assume that the network is within an urban environment where vehicles move with low speed and there are many road intersections. The velocity limitation is guaranteed generally by strict policies. The set of vehicles at a time period $t$ is defined as $\mathcal{V}^t$; while the set of trustworthy nodes is denoted $\mathcal{TV}^t \subset \mathcal{V}^t \cup \{RSU\}$. We denote by $\mathcal{N}^t(i) \subset \mathcal{V}^t$ the set including the vehicles interacting with vehicle $i$. We assign the responsibility of reputation aggregation and manifestation to the trustworthy vehicles. We assume that they use multicast communication to exchange messages. Moreover, each trustworthy vehicle keeps a history table to truck the reputation and credibility of vehicles within its communication range. The other vehicles save only the present reputation scores of all neighbors. Some of the existing vehicles may be malicious with bad intentions.

The privacy of vehicles is preserved using different pseudonyms instead of their true identities. Only the RSUs know the association pseudonym-identity; the other nodes know only the present pseudonym. We use the genetic algorithm-based approach proposed in [8] to generate the pseudonym sets. Indeed, the evaluation of a vehicle reputation becomes challenging since the evaluation requires the history of the vehicle behavior. The proposed reputation management system includes four mechanisms: reputation aggregation mechanism, reputation notification & delegation mechanism, credibility computation mechanism, and trustworthiness management mechanism.

## 2.3 Reputation Aggregation

The reputation score is calculated based on three factors: i) previous experience based on direct interaction with the target vehicle, ii) recommendations from other surrounding vehicles, and iii) recommendations from trustworthy vehicles. The reputation aggregation is performed as follows. At the end of a time slot, each node $j \in \mathcal{V}^t$ (including the trustworthy vehicles) gives a reputation score $R^t_{j,i} \in [-1, 1]$ for each neighbor vehicle $i \in \mathcal{N}^t(j)$. This score reflects the cooperative behavior of $i$ regarding the events occurring within the network. $R^t_{j,i}$ is forwarded to the nearest trustworthy node $v \in \mathcal{TV}^t$. This latter calculates the partial reputation $R^t_{v,i}$ as a weighted sum of the scores given by all the vehicles belonging to $\mathcal{N}^t(i)$:

$$R^t_{v,i} = \frac{1}{N^t_i} \sum_{j \in \mathcal{N}^t(i)} c^t_{j,i} R^t_{j,i} \tag{1}$$

where $c^t_{j,i} \in [0, 1]$ denotes the credibility of $j$ regarding the reputation score given to $i$. $N^t_i$ is the number of vehicles interacting with $i$ at time slot $t$. The determination of credibility coefficients of common vehicles is the same as in [9], while all the credibility degrees of trustworthy vehicles are set to 1.

The trustworthy nodes exchange $R^t_{v,i}$ to determine the global reputation score $R_i$ defined as:

$$R^t_i = \alpha R^{t-1}_i + \frac{\alpha^t_i}{n^t_i} \sum_{v \in \mathcal{TV}^t_i} R^t_{v,i} \tag{2}$$

where $\mathcal{TV}^t_i \in \mathcal{TV}^t$ (with $n^t_i = \|\mathcal{TV}^t_i\|$) represents the set of trustworthy vehicles participating in vehicle $i$'s reputation aggregation at time slot $t$. $\alpha \in [0, 1]$ and $\alpha^t_i \in [0, 1]$ are the weights of the two reputation scores, with $\alpha < \alpha^t_i$ and $\alpha + \alpha^t_i = 1$. Like humans, one vehicle establishes reputation through a long process, but may quickly lose such reputation due to a misbehavior. Then, $\alpha^t_i$ is inversely proportional to $\frac{1}{n} \sum_{v \in \mathcal{TV}^t_i} R^t_{v,i}$. Finally, the trustworthy vehicles disseminate $R_i$ into the network, update the credibility degree $c_{j,i}$, and send it to $j$. If $R_i \leq 0$, the vehicle is considered malicious, while the vehicle is considered as selfish if $0 < R_i \leq R_{th}$, where $R_{th}$ is a predetermined threshold. Algorithm 1 summarizes the reputation aggregation process.

## 2.4 Reputation Notification & Delegation

Reputation notification is required if i) two vehicles meet each other, ii) a vehicle enters a new zone, iii) a vehicle changes its pseudonym, or iv) a new trustworthy vehicle is selected. Since each vehicle $i$ checks its neighbors periodically, it can detect if there is a neighbor $j$ that $i$ did not learn its reputation. If it is the case, the reputation notification performs as follows:

- $i$ triggers a timer and overhears the communications.
- If it hears $R_j^t$ before the timer expires, it saves it in its table and cancels the timer;
- Else, it broadcasts a request;
- If a vehicle $k$ receives the request, it waits for a back-off time. If it overhears that another vehicle responds, it drops the request;
- Else, $k$ sends $R_j^t$ to $i$;
- If none of the vehicles had the reputation score, $j$ is considered as a new vehicle and all the vehicles wait to receive the score from the RSU.
- If $j$ is new (i.e., old neighbor changing its pseudo or new vehicle entering the zone), the RSU forwards the history table to the trustworthy vehicles, which is their turn forwarded $R_j^t$ to the vehicles;
- If $i$ is newly elected as a trustworthy vehicle, it requests all the information from the old trustworthy vehicles.

Reputation delegation is necessary when a node $i$ enters a new zone. The RSU of the old zone collects the history tables of $i$ from the trustworthy vehicles and passes them to the RSU of the new zone. The new RSU forwards the table to the trustworthy vehicles.

Since vehicular networks are prone to attacks, malicious vehicles may use the reputation scores to spoil the system operation. Hence, we use credibility to protect honest vehicles from falsified reputation scores calculated by malicious vehicles. For instance, the latter can cooperate to deteriorate the reputation of honest vehicles whilst increasing their scores to hijack the packets and misuse the included information and/or prevent emergency messages from reaching their destinations. In the same way, malicious vehicles can maximize the reputation of some vehicles to increase the probability of using them for packets routing and hence, causing congestion within some network segments. To deal with this behavior, we use a non-cooperative game with a reward/penalty mechanism based on feedback information to determine the credibility degree$c_{j,i}^t$ as in [9].

**Algorithm 1** Aggregation of vehicle $i$'s reputation

```
Initialize R_i(0), and t = 1;
while 1 do
  for each j ∈ N^t(i) do
    calculate R^t_{j,i} ;
    send R^t_{j,i} to the adequate v ∈ TV^t;
  end for
  for each v ∈ TV^t_i do
    calculate R^t_{v,i};
    send R^t_{v,i} to ∀v' ∈ TV^t;
    receive R^t_{v'',i} from ∀v' ∈ TV^t_i
    disseminate R_i
    update c^{t+1}_{j,i};
    t = t + 1;
  end for
  for each j ∈ N^t(i) do
    update R^t_i
  end for
end while
```

## 3 TRUSTWORTHY VEHICLES' SELECTION

Considering the important role of trustworthy vehicles, the selection of them follows a strict process. The vehicles are classified into three categories: authority vehicles (e.g., police, military, and firefighter vehicles), service vehicles (e.g., buses, ambulances, ...), and finally, common vehicles. The vehicles belonging to the first category are considered as trustworthy by nature just like the RSU that is responsible for the determination of trustworthy vehicles' set $\mathcal{TV}^t$. In the same way with the reputation, the RSU keeps three history tables for the vehicles' trustworthiness: trustworthy vehicles, blacklist vehicles, and neutral vehicles. Based on the trustworthiness degree, a vehicle will belong to one of the tables. A trustworthy vehicle can become a neutral vehicle and vice versa. If it was or became a blacklist vehicle, it can never be a trustworthy or neutral vehicle again. When forming the set of trustworthy vehicles, the RSU use three factors: its familiarity and experience with the vehicle, the recommendation of other RSUs, and the behavior of the vehicle.

**Algorithm 2** Reputation notification

```
broadcast msg(hello);
collect msg(hello) from neighbors
if ∃j|R^t_j = −∞ then
  set timer T
  while T do
    overhear medium ;
    if msg(R^t_j)=true then
      cancel T;
      go to Rep
    end if
  end while
  broadcast msg(reputation_request, j);
  if k receives msg(reputation_request, j) and R^t_j ≠ −∞ then
    wait(back − off)
    while back − off do
      overhear medium
      if msg(R^t_j)=true then
        cancel back − off;
        go to Rep
      end if
    end while
    send msg(R^t_j) to i
  end if
  Rep: R^t_j = msg(R^t_j)
end if
```

When a vehicle $i$ enters the communication range of the RSU, it checks $i$'s identity to decide its move:

- Vehicle $i$ is an authority vehicle. The, $i$ is tagged as trustworthy.
- The RSU is familiar with $i$. The RSU checks its tables to distinguish one of three cases:
  - **case 1**: If $i$ belongs to the trustworthy table, it is very likely that $i$ will be trustworthy for the current period. However, to be more assured, the RSU checks other RSUs' recommendation to decide if $i$ will be added to $\mathcal{TV}^t$. The recommendation describes the vehicle either trustworthy, blacklist, or neutral. In the two first scenarios, the RSU considers $i$ as recommended (i.e., trustworthy or blacklist). For the third scenario, the same processing described in **case 3** is applied.
  - **case 2**: If $i$ belongs to the black list, it is still black listed.
  - **case 3**: If $i$ is a neutral vehicle, then, if $i$ is a common vehicle and the number of trustworthy vehicles is below a predefined value, or $i$ is a service vehicle, the RSU proceeds to the trustworthiness degree determination to classify $i$ as it will be described.
- The RSU sees $i$ for the first time. The same processing described in **case 3** is applied.

As we said before, the trustworthiness degree of vehicle $i$ is determined based on three aspects: familiarity and experience with $i$, the recommendation of other RSUs, and the behavior of the vehicle. The aspects are described as follows:

- *Familiarity and experience*: The familiarity factor reflects how much the RSU is familiar with vehicle $i$; while the experience reflects the trustworthiness history of $i$. A high degree of familiarity means that $i$ appears usually in the RSU communication vicinity; while a low degree means that the RSU rarely or never sees $i$. The previous trustworthiness degree logged by the RSU is also used to determine the current trustworthiness status of $i$. The familiarity degree is calculated as follows:

$$f_i = \frac{a_i^f}{t-1} nb_i + a_i^e T_i^e \tag{3}$$

  where $nb_i$ and $T_i^e$ represent, respectively, the number of times the RSU sees $i$ and the logged trustworthiness degree at the current time period $t$. $a_i^f$ and $a_i^e$ ($a_i^f + a_i^e = 1$) denote the coefficients that reflects the importance of familiarity and experience.
- *Recommendation*: When a vehicle $i$ travel from an old vicinity to a new vicinity, the old RSU removes $i$ from the trustworthy set, but not from its trustworthy table, and forwards the trustworthiness degree $Tr_i$ to the new vicinity.
- *Behavior*: The behavior of vehicle $i$ within the network is reflected by its reputation and credibility. However, to reduce the impact of malicious vehicles on the trustworthiness determination, only reputation scores given by trustworthy vehicles are taken in account. The behavior degree is defined as follows:

$$B_i = b_i^r r_i + b_i^c c_i \tag{4}$$

  where $r_i \in [-1, 1]$ and $c_i$ represent the aggregated reputation score given by trustworthy vehicles and the credibility degree of vehicle $i$, respectively. $b_i^r$ and $b_i^c$ are the importance coefficients ($b_i^r + b_i^c = 1$). The credibility is calculated over all the nodes and expressed as:

$$c_i = \frac{1}{N-1} \sum_{j \in \mathcal{V}^t \setminus \{i\}} c_{i,j}^t \tag{5}$$

  $c_{i,j}^t$ is the credibility degree of $i$ towards vehicle $j$.

The trustworthiness degree $T_i \in [-1, 1]$ is the combination of the three factors:

$$T_i = \beta_i^f f_i + \beta_i^T Tr_i + \beta_i^c c_i \tag{6}$$

where $\beta_i^f + \beta_i^T + \beta_i^c + 1$. When the RSU sees the $i$ for the first time $\beta_i^f = \beta_i^c = 0$. If in addition to the previous condition no other RSU sees $i$, $T_i = T_{min}$. The vehicle is considered trustworthy if $T_i \geq T_{max}$ and distrustful if $T_i < T_{min}$. Otherwise (i.e., $T_{min} \leq T_i < T_{max}$), $i$ is neutral. $T_{min}$ and $T_{max}$ are predefined thresholds.

**Algorithm 3** Trustworthiness algorithm

```
Initialize t to 1;
while 1 do
  if i enters the system then
    if i is an authority vehicle then
      TV^t=TV^t. added(i)
    else if The RSU sees i for the first time then
      Calculate T_i
    else if i ∈ trust_table then
      if Tr_i < T_min then
        black_list=black_list.added(i)
      else if Tr_i ≥ T_max then
        TV^t=TV^t. added(i)
      else
        if i is a service vehicle or |TV^t|< th_nb then
          Calculate T_i
        end if
      else if i ∈ neutral_table then
        if i is a service vehicle or |TV^t|< th_nb then
          Calculate T_i
        end if
      end if
    end if
  end if
  if i leaves the system then
    forward T_i to next RSU
  end if
  update history tables and TV^t;
end while
```

Unlike the reputation and credibility, that are calculated at each time slot, the trustworthy set and history tables update is performed only when a vehicle enters or leaves the system. However, the RSU control periodically the trustworthy vehicles to ensures that no

**Table 1: Simulation Parameters**

| Parameter | Value |
|---|---|
| Simulation area | $5 \times 5$ km$^2$ |
| Time period length | 60 s |
| Number of vehicles | from 50 to 300 |
| Maximum transmission range | 300 m |
| Maximum percentage of vehicles | 50% |

vehicle change its status. Moreover, the trustworthiness degree determination is executed only for some vehicles by using the history tables and the recommendation mechanism. This strategy optimizes the complexity and time of the trustworthiness process.

## 4 PERFORMANCE EVALUATION

To evaluate the proposed reputation management model, we implement a VANET in Matlab on a 64-bit Windows 7 machine equipped with Intel Core i7-7567U CPU (2 cores) at 3.9 GHz-4 GHz, with 32 GB of memory (4 MB cache), 2.7 MHz of RAM speed. We recreate a realistic vehicular network for Troyes city (Grand-Est region, France) using vehicles' mobility model, topology, and distribution extracted from the two road traffic data sets TMJA_2018 [10] and TMJA_2018_R44 [11]. The goal of the realized extensive simulation is to evaluate the efficiency of the proposed model to detect misbehaving vehicles. As malicious vehicles may give falsified values to deteriorate the network, we use them to evaluate the robustness of our approach regarding the manipulation of reputation scores. Each point is the average of at least forty runs. Table 1 shows the simulation parameters.

In Fig. 1, we measure the false alarm ratio (FAR) in function of the percentage of misbehaving vehicles in a vehicular network with 300 vehicles. FAR is defined as the percentage of cooperative vehicles identified as misbehaving ones from all the identified misbehaving vehicles. We compare three percentages of trustworthy vehicles: 20%, 10%, and 5%. Fig. 1 shows that FAR is still below 20% even with a large number of malicious vehicles and small number of trustworthy vehicles. We notice that when the percentage of malicious vehicles reaches 40%, FAR increases faster. However, these ratios have small effect on the network efficiency regarding the number of well cooperative nodes and the large misbehavior detection ratio deduced from the small missed detection ratio or false negatives (MDR) illustrated by Fig. 2.

The missed detection ratio depicted in Fig. 2 denotes the ratio of misbehaving vehicles not detected and considered as cooperative ones. MDR is evaluated in function of the number of malicious vehicles in a 300 vehicles' network. Unlike FAR, this parameter has a considerable impact on the operation of the network. Thus, it must be kept as small as possible since the non-detected misbehaving vehicles deteriorate the network efficiency. The proposed reputation model achieves good results since MDR is still below 10% even when the percentage of malicious vehicles becomes very large. The proposed model can even detect 100% of the misbehaving nodes if the number of trustworthy vehicles is sufficient.

Fig. 3 shows the evolution of the reputation of two nodes over the time. The total number of vehicles is 200 vehicles, among them 20% are trustworthy and 40% are malicious. We choose $R_{th} = 0.4$,

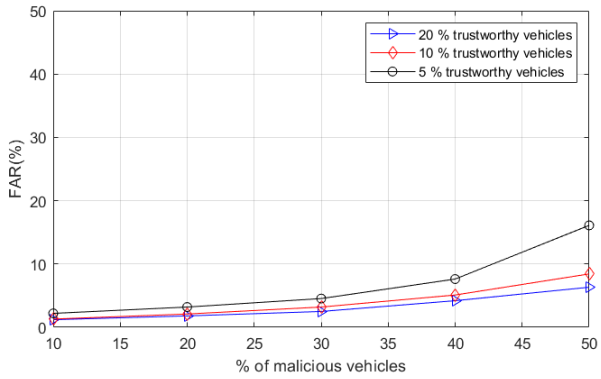


**Figure 1: The percentage of false alarms vs. the percentage of misbehaving vehicles.**

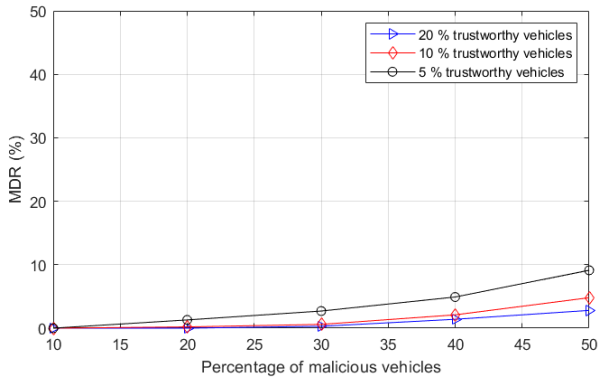


**Figure 2: The missed detection ratio vs. the percentage of misbehaving vehicles.**

$\alpha = 0.3$, and $\alpha_i^t = 0.7, \forall t, \forall i$. We generate an attack where malicious vehicles collaborate in the aim of spoiling the reputation of a cooperative and contributing vehicle and increasing the reputation of a malicious vehicle. We assume that the latter has a reputation score of 0.5 during a previous execution of the algorithm. This score is used as initial score in the current algorithm execution. As we can notice, during the first rounds, the reputation of the well-behaving vehicle decreases while that of malicious vehicle increases. Since the credibility degrees are not stable yet, the malicious vehicles affect the reputation score. Fortunately, the impact is not as drastic as it could be since the trustworthy nodes are more influential. From round 5, the victim vehicle begins to regain its reputation, while the malicious vehicle loses it. This is explained by the fact that the credibility degrees of attackers, towards the victim and the malicious vehicles, are deteriorated quickly by the trustworthy nodes using the reward/penalty mechanism. Furthermore, the malicious vehicle is detected before round 10 and loses its reputation totally. Contrarily, the cooperative vehicle regains its reputation slowly but surely since the trustworthy vehicle are more careful when giving reputation than taking it away.

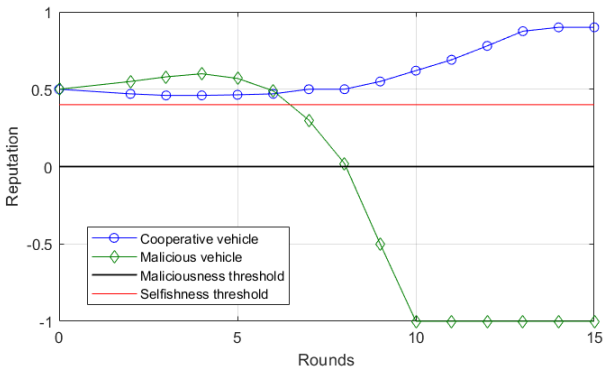


**Figure 3: Comparison of reputation evolution for two vehicles**

Fig. 4 shows the convergence time of the reputation determination algorithm vs. the number of vehicles in the network. The percentage of trustworthy vehicles and malicious ones are set to 10% and 20%, respectively. The obtained results are reasonable with the time period set to 60 seconds. It is true that the convergence speed increases when the number of vehicles exceeds 200, but it is still inferior to 3 seconds even with 300 vehicles. When the number of vehicles increases, the number of exchanged messages increases even with a distributed data processing. In addition, the interference ratio increases which leads to more packets' retransmissions. Hence, despite the distributed reputation management, the convergences time will increase, but still represents a small fraction of the time period length.

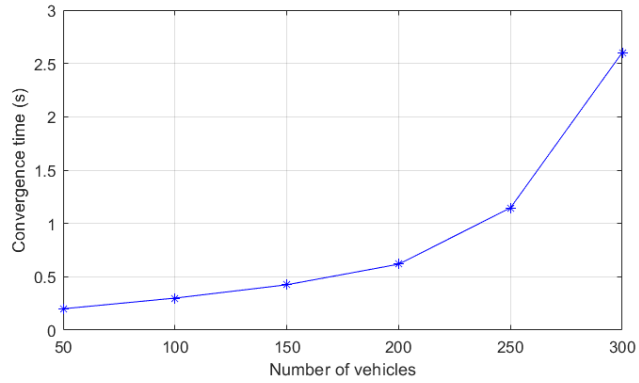


**Figure 4: Convergence time of the trustworthiness process**

## 5 CONCLUSION

The cooperation and collaboration of vehicles, while executing tasks such as event detection and data routing, have a considerable impact on the efficiency of services offered by vehicular networks. Unfortunately, some vehicles misbehave by not participating to collaborative tasks which deteriorate the network operation. Hence, to identify these vehicles, the reputation concept is integrated within vehicular networks. The reputation is the metric that allows us evaluating vehicles' behavior. When the system identifies the misbehaving vehicles, it saves time and resources by not assigning tasks to these vehicles since it knows they will not fulfill them. In this paper, we focused on the proposition of a robust reputation model to improve the operation of the network and prevent any selfish or misbehaving node from spoiling its operation. In the proposed model, the reputation of a vehicle, determined by its neighbors, depends on its cooperative behavior within the network. However, since some malicious vehicles could be part of the network, they participate in the reputation calculation, and this may lead to falsified reputation scores. To deal with the problem, we used some trustworthy nodes to attenuate the influence of malicious nodes. We developed a novel scheme for vehicle trustworthiness computation and trustworthy vehicles' selection. This scheme dynamically elects the trustworthy vehicles and updates them periodically. The simulation results showed that the proposed model achieves reasonable results regarding the efficiency of misbehavior detection and prevention. As a future work, we intend to integrate some clustering methods to improve the efficiency of reputation, credibility and trustworthiness models.

## REFERENCES

[1] T. Halabi, and M. Zulkernine , "Trust-based Cooperative Game Model for Secure Collaboration in the Internet of Vehicles," IEEE International Conference on Communications (ICC), 2019.
[2] Y. Begriche, R. Khatoun, A. Rachini, and L. Khoukhi, "A Reputation System Using a Bayesian Statistical Filter in Vehicular Networks," Sixth International Conference on Mobile And Secure Services (MobiSecServ), 2020.
[3] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for Vehicular Ad hoc Networks (VANETs)," Computer Networks, vol. 121, pp. 152-172, 2017.
[4] J. Li, R. Xing, Z. Su, N. Zhang, Y. Hui, T. H. Luan, H. Shan , "Trust Based Secure Content Delivery in Vehicular Networks: A Bargaining Game Theoretical Approach," IEEE Trans. on Veh. Technol., vol. 69, no. 3, pp. 3267-3279, 2020.
[5] A. M. B. C. Quevedo, C. H. O. O. Quevedo, R. L. Gomes, S. F. Camara, and J. Celestino , "A Reputation and Security Mechanism for Heterogeneous Vehicular Networks," IEEE Symposium on Computers and Communications (ISCC), 2022.
[6] S. Gyawali, Y. Qian, and R. Q. Hu , "Machine Learning and Reputation based Misbehavior Detection in Vehicular Communication Networks," IEEE Trans. on Veh. Technol. vol. 23, no. 2, pp. 1400-1414, 2022.
[7] D. Zhang, F. R. Yu, R. Yang and L. Zhu , "Software-Defined Vehicular Networks With Trust Management: A Deep Reinforcement Learning Approach," IEEE Transactions on Intelligent Transportation Systems, 2020.
[8] B. Chaudhary, and K. Singh, "Pseudonym generation using genetic algorithm in vehicular ad hoc networks," Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, no. 4, pp. 661-677, 2019.
[9] S. Chouikhi, L. Khoukhi, S. Ayed, and M. Lemercier, "An Efficient Reputation Management Model based on Game Theory for Vehicular Networks," IEEE Conference on Local Computer Networks (LCN), 2020.
[10] Online: "https://www.data.gouv.fr/en/datasets/trafic-moyen-journalier-annuel-sur-le-reseau-routier-national/. " [Accessed: July 2022].
[11] Online: "https://www.data.gouv.fr/en/datasets/trafic-moyen-journalier-annuel-sur-le-reseau-routier-national/. " [Accessed: July 2022].

Received 24 November 2023