Blockchain-Based Collaborative Decision-Making in Vehicular Networks

Dezhen Wang[1], Rongqing Zhang[1,2,*], Shengjie Zhao[1,*]
{wdztju@163.com, rongqingz@tongji.edu.cn, shengjiezhao@tongji.edu.cn}

School of Software Engineering, Tongji University, Shanghai 201804, China[1]
Shandong Provincial Key Laboratory of Wireless Communication Technologies, Shandong University, China[2]

Abstract. Collaborative decision-making (CDM) in vehicular networks can greatly improve the driving efficiency of vehicles. However, vehicle clusters often have serious security threats. To solve this issue, we propose a blockchain-based collaborative decision-making (BCDM) model, which is divided into two parts: the architecture level and the algorithm level. At the architectural level, we employ blockchain into vehicular networks and propose a layered blockchain network architecture (LBNA) that not only eases the data calculation and storage pressure of vehicular networks, but also further guarantees the security of the system. At the algorithm level, a BCDM algorithm combining direct trust and indirect trust is provided to determine the occurrence of traffic events and identify false messages. Simulation results reveal that the proposed system is effective and feasible in processing and storing trust information in vehicular networks.

Keywords: Blockchain, collaborative decision-making, vehicular networks, data credibility.

1 Introduction

In the field of vehicular networks, the development of communication technology among vehicles has achieved great results. In an increasingly complex road environment, vehicular networks need to face a variety of traffic events [1], [2]. The *Traffic Incident Management Handbook* [3] defines an event as "any non-recurring event that causes a reduction of roadway capacity or an abnormal increase in demand." The *2000 Highway Capacity* [4] defines an event as being "any occurrence on a roadway that impedes normal traffic flow." In order to take safe and efficient driving actions according to different traffic events, cooperative decision-making (CDM) is regarded as a promising solution for connected and intelligent vehicles in vehicular networks. In the process of CDM, there are many security threats such as in-vehicle sensor recognition errors and malicious vehicles' false information pouring. In the case of limited hardware, software, and energy resources of vehicular networks, enhancing vehicle safety and proposing effective solutions to potential safety hazards are major challenges [5].

At the level of the event discrimination algorithm, Ahmad *et al*. [6] summarized several trust models (TMs) applicable to vehicular networks, which can be divided into three categories: Entity-oriented Trust Models (ETM), Data-oriented Trust Models (DTM), and Hybrid Trust Models (HTM). Kerrache *et al*. [7] proposed an opportunistic alert dissemination mechanism

* Corresponding authors: Rongqing Zhang and Shengjie Zhao.

EAI MOBIMEDIA 2020, August 27-28, Harbin, People's Republic of China

DOI 10.4108/eai.27-8-2020.2294370

based on trust relationships between vehicles. Chen *et al*. [8] proposed a security scheme for evidence combination in CDM. This scheme can combine the direct trust value from local data with the indirect trust value from neighboring vehicles to obtain traffic incident decision results. Li *et al*. [9] proposed an Attack-Resistant Trust (ART) management scheme. This scheme can detect malicious attacks, evaluate the credibility of data and mobile nodes in vehicular networks.

However, with the development of information technology, algorithm-level security solutions are no longer sufficient to ensure the reliability and robustness of vehicular networks. Therefore, we propose to exploit blockchain to adjust and optimize the vehicular network architecture [10]. The blockchain has inherent characteristics such as fault tolerance, transparency, tamper resistance, and traceability. Based on this, Kang *et al*. [11], [12] proposed that blockchain technology can ensure secure data sharing in vehicular edge computing and networks (VECONs). What's more, blockchain-enabled Internet of Vehicles (BIoV) can enhance soft security performance through miner selection and block verification. Ali *et al*. [13] proposed a multi-tier blockchain network architecture, which has good horizontal extensibility. Yang *et al*. [14] proposed a Blockchain-based Traffic Event Validation (BTEV) framework, which collects traffic data by roadside units (RSUs), and vehicles can use these data to verify the occurrence of traffic incidents. Yang *et al*. [15] proposed a decentralized management system for vehicular networks based on blockchain technology. In this system, vehicles can use Bayesian inference models to verify messages received from neighboring vehicles. Besides, each vehicle that sends a message will get a corresponding trust value, and these values will be stored in the blockchain network formed by RSUs.

Therefore, in this paper, we propose a Blockchain-based Collaborative Decision-Making (BCDM) model applied to vehicular networks. At the network level, the BCDM model includes an innovative layered blockchain network architecture (LBNA), which can protect the system's security while avoiding on-board memory and computing resources that are occupied by blockchain data. At the algorithm level, we further propose a BCDM algorithm for vehicle clusters based on hierarchical events. The algorithm has the functions of event determination, malicious node identification, and reputation rating, which can be perfectly integrated with the blockchain network architecture.

The remainder of this paper is organized as follows. Section 2 describes the system model of BCDM. In Section 3, we propose a BCDM algorithm combining direct trust, indirect trust, and reputation rating. The numerical results and conclusions are drawn in Section 4 and Section 5, respectively.

2 System model

2.1 Network architecture model

As illustrated in **Figure 1**, the LBNA is divided into two layers, namely the center-layer and the edge-layer.

The edge-layer includes multiple groups of temporary blockchain networks (TBN), and each group is composed of vehicles in the same traffic environment. Because the vehicle itself has inherent characteristics such as high mobility, relatively small on-board memory, and relatively low on-board computing power, the TBN will not exist for a long time. Before the TBN disintegrates, its last miner node will upload the necessary data for the entire chain to the center-layer.

The center-layer is a permanent blockchain network (PBN), which is composed of RSUs, base stations, and databases in a large geographical area. These nodes have stronger computing and data storage capabilities, which can process and save massive data from edge-layer in order to query historical records or trace information sources when necessary. In addition, the PBN will perform statistics and analysis on the historical quality of messages broadcast by each vehicle, and thereby identify malicious vehicles. Identified malicious vehicles will be notified online for criticism and punished by prohibiting them from broadcasting messages.

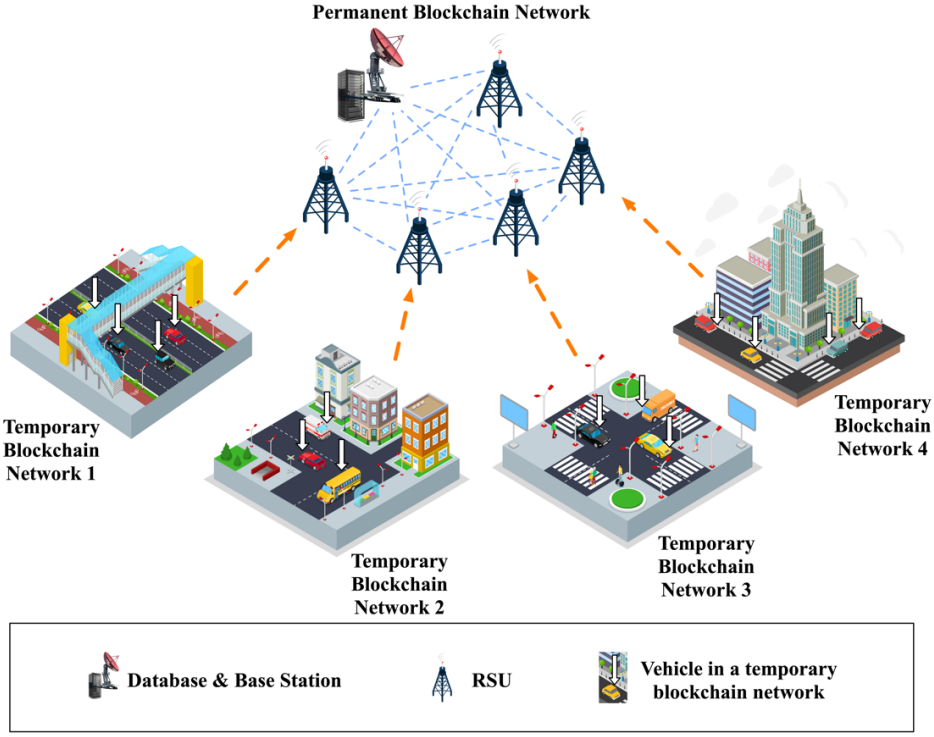

Fig. 1. The layered blockchain network architecture (LBNA) in vehicular networks.

2.2 Event model

While driving, vehicles often face a variety of complex traffic events, such as road construction, road congestion, or different types of traffic accidents. These traffic events make up the collection: $Event = \{E_1, E_2, \ldots, E_j, \ldots\}$. In this paper, it is assumed that traffic events have been pre-classified, and each type of traffic event is divided into different levels. Each level is independent of each other and all levels together constitute a complete set representing the corresponding event. For example, road congestion can be divided into five levels: (I) roads are clear, (II) lightly congested, (III) moderately congested, (IV) severely congested, and (V) impassable.

In addition, the BCDM model will set a corresponding prior probability for each level of a specific event based on empirical statistics on traffic big data: $Priori = \{pr_1, pr_2, \ldots, pr_\omega\}$. Where, Pr_1 represents the prior probability of level (I) in E_j, ω represents the total number of levels included in E_j.

During the driving process, the surrounding environment will be detected by on-board sensors. Once a specific traffic event is observed, the event will be evaluated according to the preset event levels, and a cooperative awareness message (CAM) will be generated based on this assessment result. Each CAM will contain the identity of the sender, the generation time, and a level recommendation for a certain traffic event. It will be broadcast to other vehicles in the same TBN.

2.3 Test model

All the CAMs received by a vehicle V_m constitute a set $CAM = \{cam_1, \ldots, cam_j, \ldots\}$. This set may contain false contents from malicious vehicles or untrusted vehicles. Malicious vehicles are vehicles that intentionally broadcast false CAMs, whereas untrusted vehicles are vehicles that accidentally broadcast an error CAM because they are far away from where the event occurred. In the hypothesis of our paper, only a few of benign vehicles become untrusted due to occasional errors. Among them, $cam_j = \{cam_j^1, \ldots, cam_j^k, \ldots\}$ refers to the set of all CAMs related to E_j received by V_m. cam_j^k in the set denotes the CAM that V_k broadcasts to V_m about E_j.

Each vehicle in the TBN will infer and judge the true situation of events based on two principles of direct confidence T_{dir} and indirect confidence T_{ind}. The calculation of T_{dir} is based on the trustworthiness of CAMs received by the vehicle. The calculation of T_{ind} is based on the historical reputation records of the vehicle that issued the CAM. The historical reputation record is the quality judgment of all CAMs that the vehicle has ever issued. The vehicle receiving the message, V_m, will calculate the comprehensive trust T_{com} for the broadcast vehicle V_k based on T_{dir} and T_{ind}.

In the end, V_m uses Dempster-Shafer theory (DST) to fuse all comprehensive trusts about E_j, and obtains the event's final discrimination result, T_{final}. Meanwhile, V_m will give a reputation score to the broadcast vehicle V_k based on T_{final}. If T_{final} proves the CAM is false, the corresponding vehicle V_k is given a negative reputation score (-1). This reputation score will affect the vehicle's T_{ind} and further affect the determination of whether the vehicle is malicious.

3 The proposed algorithms

3.1 The BCDM algorithm

Step 1 Direct trust. The vehicle's direct trust T_{dir} is an assessment of the reliability of vehicles' broadcast CAMs.

The closer the vehicle is to the event, the more reliable the information it detects. Therefore, the distance trust of a certain CAM is defined as follows:

$$d_j^k = e^{-\alpha \cdot l_j^k} + \beta \tag{1}$$

where d_j^k is the distance trust of cam_j^k sent by vehicle V_k. l_j^k is the distance between V_k and the event location. α and β are two present parameters, which respectively control the change rate and lower bound of the distance trust.

Suppose that the total number of CAMs received by V_m for a certain event E_j is N, that is, vehicle V_m has a distance trust set for E_j:

$$Tot = \left\{d_j^1, d_j^2, \dots, d_j^N\right\}. \tag{2}$$

In the set Tot, there are M CAMs of the same level as cam_j^k about E_j, which will form a subset:

$$Sub = \left\{d_j^{(1)}, d_j^{(2)}, \dots, d_j^{(M)}\right\}. \tag{3}$$

Each element in the set Sub also belongs to the set Tot.

Therefore, the direct trust of the CAM about E_j, which received by V_m from V_k is defined as follows:

$$T_{dir} = \frac{\sum_{i=1}^{M} d_j^{(i)}}{M}. \tag{4}$$

Step 2 Indirect trust. The vehicle's indirect trust T_{ind} is calculated based on its own historical reputation.

The historical reputation $T_k^{b_i}$ is the accuracy of all the CAMs V_k has broadcast when it joined the TBN for the $i-th$ time.

$$T_k^{b_i} = \frac{Reliable_k^{b_i}}{Reliable_k^{b_i} + Unreliable_k^{b_i}} \tag{5}$$

where $Reliable_k^{b_i}$ is the number of reliable CAMs that V_k have been broadcasted in its $i-th$ TBN, while $Unreliable_k^{b_i}$ is the number of unreliable CAMs.

In order to ensure the reasonableness of the historical reputation evaluation of vehicles, we will focus on examining the performance of CAMs when vehicles join in the TBN this or the penultimate time. Therefore, the weighted aggregation method is used to calculate the indirect trust of V_k:

$$T_{ind} = \begin{cases} \dfrac{\sigma \cdot \left[\dfrac{\sum_{i=1}^{H-2} T_k^{b_i}}{H-2}\right] + T_k^{b_{H-1}}}{\sigma + 1}, num \le \delta \\ \dfrac{\sigma \cdot \left[\dfrac{\sum_{i=1}^{H-1} T_k^{b_i}}{H-1}\right] + T_k^{b_H}}{\sigma + 1}, num > \delta \end{cases} \tag{6}$$

where H is the total number of times V_k has added to the TBN, $T_k^{b_H}$ is the historical reputation of V_k joining in TBN this time, num is the number of times V_k broadcasted in the current TBN,

δ is a positive integer parameter which denotes the threshold for switching formulas, σ is the factor between 0 and 1 which denotes the weight given to the previous TBN's historical reputation.

Step 3 Comprehensive trust. Based on the step 1∼2, the comprehensive trust of the CAM from V_k to V_m is:

$$T_{com} = \gamma \cdot T_{dir} + \eta \cdot T_{ind}\ ,\ \gamma + \eta = 1 \tag{7}$$

where γ and η are the weights of T_{dir} and T_{ind}, respectively.

Step 4 Final trust. In this work, Dempster-Shafer theory (DST) is able to fuse T_{com} of multiple vehicles on the event E_j, and even if there are non-true discrimination results among them, accurate final judgment can be obtained. In DST, the recognition frame Ω of E_j is composed of all its levels:

$$\Omega = \{r_1, r_2, \dots, r_x, \dots r_\omega\} \tag{8}$$

where r_1 indicates that the level of E_j is (I), and ω indicates the total number of levels in E_j.

When V_m receives the CAMs sent by any other vehicle about E_j, it can calculate the corresponding comprehensive trust and obtain the set $\{T_{com}^1, \dots, T_{com}^N\}$. Based on this set, the basic probability assignment (BPA) for each level in Ω can be completely obtained.

Here are the examples: suppose that V_k judges E_j as level r_x, and V_m gets the corresponding $T_{com}^k(r_x) = m_k(x)$. According to the prior probability set $Priori = \{pr_1, pr_2, \dots, pr_\omega\}$, other levels of BPA in Ω can be calculated:

$$m_k(y) = \frac{pr_y \cdot [1 - m_k(x)]}{1 - pr_x} \qquad r_y \in Priori, y \neq x\ . \tag{9}$$

In DST, the probability is replaced by an uncertainty interval bounded by belief (bel) and plausibility (pl). bel is the lower bound of this interval and represents the supporting evidence. pl is the upper bound of this interval and represents non-denied evidence. Trust interval $[bel(r_x), pl(r_x)]$ represents the value range of T_{final}, while $pl(r_x) - bel(r_x)$ represents the uncertainty of the judgement about r_x. When $pl(r_x) - bel(r_x) = 0$, it means that the degree of trust in the judgement about r_x is completely determined.

The belief function and plausibility function with regard to the level r_x of E_j obtained by V_m are calculated as follows:

$$bel(r_x) = \sum_{r_z \in r_x} mass(r_z) \tag{10}$$

and

$$pl(r_x) = \sum_{r_z \cap r_x \neq \emptyset} mass(r_x) = 1 - bel(\bar{r}_x)\ . \tag{11}$$

Here r_z are all the basic elements that compose the level r_x. Since levels of E_j in our hypothesis are single-element propositions and mutually exclusive, we have the following formulas:

$$bel(r_x) = pl(r_x) = mass(r_x) \quad \forall r_x \subseteq \Omega \,. \tag{12}$$

$$mass(r_x) = \bigoplus_{n=1}^{N} m_n\,(r_x) \,. \tag{13}$$

Here $mass(r_x)$ denotes the fusion of discrimination results about r_x for a total of N broadcast vehicles. We can combine these discrimination results by applying the Dempster's rule, which is defined as follows:

$$m_1(r_x) \oplus m_2(r_x) = \frac{\sum_{a,b:R_a \cap R_b = r_x} m_1(R_a) \cdot m_2(R_b)}{1 - \sum_{a,b:R_a \cap R_b = \emptyset} m_1(R_a) \cdot m_2(R_b)} \,. \tag{14}$$

The final result of a particular level r_x about E_j is:

$$T_{final}(r_x) = bel(r_x) = pl(r_x) \,. \tag{15}$$

3.2 Distributed consensus algorithm

Vehicle clusters store data in the BCDM process through a TBN. As a decentralized system, the TBN needs to choose an appropriate consensus mechanism to ensure that all vehicles can follow the established protocol rules. We choose to adopt the proof-of-stake (PoS) miner election method. Compared with proof-of-work (PoW), PoS is more suitable for applications in the field of vehicular networks, it can greatly shorten the time to reach consensus in each block, and does not require energy consumption for mining [16], [17]. In PoS protocols, instead of computational power resources, miners are selected based on their stakes:

$$P_i = \frac{s_i}{\sum_{j=1}^{N} s_j} \,. \tag{16}$$

In our research, the weight of a vehicle s_i is the number of false CAMs it receives. In this way, most false CAMs and related data can be stored in TBN promptly, thereby ensuring the rapid identification of malicious nodes.

Considering the scalability of the entire architecture model, the PBN will use the PoW algorithm to be publicly deployed in a permissionless manner so that TBN in the edge layer can upload data freely.

3.3 Identification and punishment mechanism of malicious vehicles

The BCDM model will identify and punish malicious vehicles based on the data stored in the blockchain. The specific execution rule is to calculate the proportion of false CAMs to the total CAMs broadcasted by each vehicle in the current TBN. If the proportion of false CAMs exceeds the threshold Thr_1, the corresponding vehicle will be warned by broadcast. If the proportion of false CAMs exceeds the threshold Thr_2 $(Thr_2 > Thr_1)$, the corresponding vehicle will be punished by banning broadcast CAMs.

4 Simulation results

In order to evaluate the efficiency of the proposed BCDM model, we conduct the simulations based on MATLAB. The configurations of key parameters are listed in Table 1. We classify all vehicles into three categories: trusted, untrusted, and malicious vehicles. Malicious vehicles are vehicles that intentionally broadcast false CAMs. Untrusted vehicles are vehicles that accidentally broadcast an error CAM because they are far away from where the event occurred. In order to simulate a real traffic scene, a certain percentage (broadcast ratio) of random vehicles will detect traffic events and broadcast them during each iteration. The number of iterations is 150 in the simulation.

Experimental strategies in the simulations: In the simulations, we evaluate the performance of the BCDM model by event discrimination accuracy, Precision (P) and Recall (R).

Table 1. Simulation parameters.

Parameters	Settings
ω	4
$Priori$	$pr_1 = pr_2 = pr_3 = pr_4 = 0.25$
N	50
trusted to untrusted vehicle ratio	8:1
broadcast ratio	0.6
α	0.015
β	0.0723
σ	0.7

4.1 Event discrimination accuracy

We compare our accuracy performance with Yang *et al*. [15], in which they calculated the credibility of the vehicle broadcast message through Bayesian Inference (BI) to determine whether the event occurred. **Figure 2** shows the impact of malicious vehicles on accuracy.

From Figure 2, we can see that as the proportion of malicious vehicles gradually increases, the accuracy of our BCDM algorithm is always higher than the scheme in [15], and when the proportion of malicious vehicles is less than 55%, the BCDM algorithm can keep the discrimination accuracy as 100%.

4.2 Precision and Recall

We use Precision and Recall as evaluation parameters, which are widely used in the CDM scenario.

In this paper, P and its $baseline$ are defined as follows:

$$P = \frac{malicious\ vehicles\ detected}{wrong\ broadcast\ vehicles\ detected} \tag{17}$$

$$baseline = \frac{real\ malicious\ vehicles}{real\ wrong\ broadcast\ vehicles} \tag{18}$$

where *wrong broadcast vehicles* means malicious vehicles and untrusted vehicles. **Figure 3** shows the impact of malicious vehicles on Precision. When the proportion of malicious vehicles is 65% or less, the Precision of BCDM exactly matches the *baseline*.

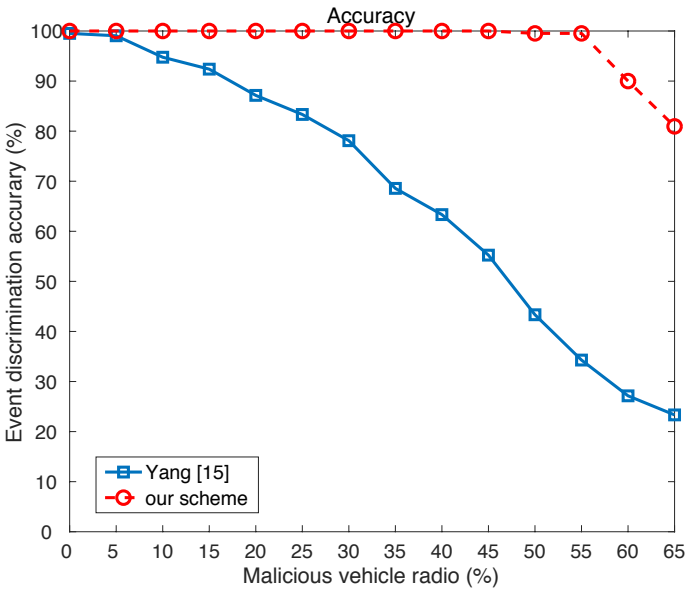

Fig. 2. The impact of malicious vehicles on Accuracy.

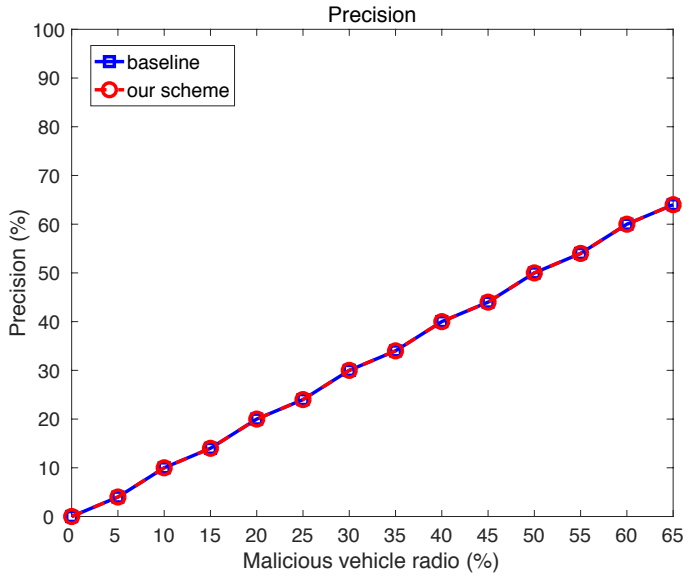

Fig. 3. The impact of malicious vehicles on Precision.

In this paper, R is defined as follows:

$$R = \frac{malicious\ vehicles\ detected}{real\ malicious\ vehicles}\ . \tag{19}$$

Figure 4 shows the impact of malicious vehicles on Recall with different proportions of T_{dir}. In T_{com}, the more malicious vehicles in TBN leads to the smaller proportion of T_{dir} and the better Recall performance. However, T_{dir} can measure the trustworthiness of CAM itself and play an indispensable role in the BCDM model when there are fewer malicious vehicles. Therefore, the proportion of T_{dir} in T_{com} cannot be too small in practical applications.

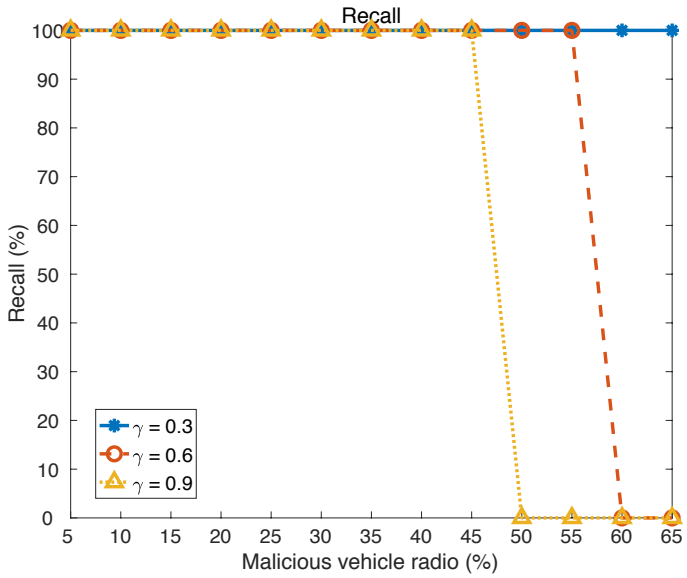

Fig. 4. The impact of malicious vehicles on Recall.

5 Conclusions

In this paper, we proposed a BCDM model. With this model, vehicles can collect CAMs in the same TBN, and process the information according to both direct and indirect trust. The BCDM model will discriminate events based on the processing results and score each vehicle's reputation. These results and scores will be stored in the TBN at the edge layer and uploaded to the PBN before it disintegrates. Architecture analysis and simulation results show that our proposed model has better decision-making performance, and also makes practical contributions to the innovation of cooperaive vehicular network architecture.

Acknowledgments. This work is supported in part by the National Key Research and Development Project under Grant 2017YFE0119300, 2019YFB2102300 and 2019YFB2102301, in part by the National Natural Science Foundation of China under Grant 61936014 and 61901302, in part by the Scientific Research Project of Shanghai Science and Technology Committee under Grant 19511103302, in part by the open research fund from Shandong Provincial Key Laboratory of Wireless Communication Technologies (No. SDKLWCT-2019-02), and in part by the Fundamental Research Funds for the Central Universities (China).

References

[1] Zhou, H.; Liu, B.; Hou, F.; *et al*.: Chaincluster: Engineering a cooperative content distribution framework for highway vehicular communications. IEEE transactions on intelligent transportation systems. vol. 15, no. 6, pp. 2644-2657 (2014)

[2] Alam, K. M.; Saini, M.; *et al*.: VeDi: A vehicular crowd-sourced video social network for VANETs. 39th Annual IEEE Conference on Local Computer Networks Workshops (2014)

[3] Farradyne, P. B.: Traffic incident management handbook. Prepared for Federal Highway Administration. Office of Travel Management (2000)

[4] Manual, H. C.: Highway capacity manual. Highway Capacity. Washington, DC (2000)

[5] Kleberger, P.; Olovsson, T. and Jonsson, E.: Security aspects of the in-vehicle network in the connected car. IEEE Intelligent Vehicles Symposium (IV) (2011)

[6] Ahmad, F.; Adnane, A.; *et al*.: A comparative analysis of trust models for safety applications in IoT-enabled vehicular networks. 2019 Wireless Days (WD) (2019)

[7] Kerrache, C. A.; *et al*.: Trust-aware opportunistic dissemination scheme for VANET safety applications. 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld) (2016)

[8] Chen, J.; Li, T. and Panneerselvam, J.: TMEC: a trust management based on evidence combination on attack-resistant and collaborative internet of vehicles. IEEE Access. vol. 7, pp. 148913-148922 (2018)

[9] Li, W. and Song, H.: ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems. vol. 17, no. 4, pp. 960-969 (2015)

[10] Xiong, Z.; *et al*.: When mobile blockchain meets edge computing. IEEE Communications Magazine. vol. 56, no. 8, pp. 33-39 (2018)

[11] Kang, J.; *et al*.: Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal. vol. 6, no. 3, pp. 4660-4670 (2018)

[12] Kang, J.; *et al*.: Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology. vol. 68, no. 3, pp. 2906-2920 (2019)

[13] Ali, M.; Vecchio, M. and Antonelli, F.: Enabling a Blockchain-Based IoT Edge. IEEE Internet of Things Magazine. vol. 1, no. 2, pp. 24-29 (2018)

[14] Yang, Y.; *et al*.: Blockchain-based traffic event validation and trust verification for VANETs. IEEE Access. vol. 7, pp. 30868-30877 (2019)

[15] Yang, Z.; *et al*.: Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal. vol. 6, no. 2, pp. 1495-1505 (2018)

[16] Nguyen, C. T.; Hoang, D. T.; *et al*.: Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access. vol. 7, pp. 85727-85745 (2019)

[17] Ribera, E. G.: Design and Implementation of a Proof-of-Stake Consensus Algorithm for Blockchain. BS thesis. Universitat Politècnica de Catalunya (2018)