Blockchain-Based Trust Management Using Multi-Criteria Decision-Making Model for VANETs

SUBMISSION DATE / POSTED DATE

17-10-2020 / 29-10-2020

CITATION

Pu, Cong (2020): Blockchain-Based Trust Management Using Multi-Criteria Decision-Making Model for VANETs. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.13106876.v2

DOI

10.36227/techrxiv.13106876.v2

Blockchain-Based Trust Management Using Multi-Criteria Decision-Making Model for VANETs

Cong Pu
Department of Computer Sciences and Electrical Engineering
Marshall University, Huntington, WV 25755
Email: puc@marshall.edu

***Abstract*—Recent advancements in embedded sensing system, wireless communication technologies, big data, and artificial intelligence have fueled the development of Internet of Vehicles (IoV), where vehicles, road side unit (RSUs), and smart devices seamlessly interact with each other to enable the gathering and sharing of information on vehicles, roads, and their surrounds. As a fundamental component of IoV, vehicular networks (VANETs) are playing a critical role in processing, computing, and sharing travel-related information, which can help vehicles timely be aware of traffic situation and finally improve road safety and travel experience. However, due to the unique characteristics of vehicles, such as high mobility and sparse deployment making neighbor vehicles unacquainted and unknown to each other, VANETs are facing the challenge of evaluating the credibility of road safety messages. In this paper, we propose a blockchain-based trust management system using multi-criteria decision-making model, also referred to as $Trust^{Block}_{MCDM}$, in VANETs. In the $Trust^{Block}_{MCDM}$, each vehicle evaluates the credibility of received road safety message and generates the trust value of message originator. Due to the limited storage capacity, each vehicle periodically uploads the trust value to a nearby RSU. After receiving various trust values from vehicles, the RSU calculates the reputation value of message originator of road safety message using multi-criteria decision-making model, packs the reputation value into a block, and competes to add the block into blockchain. We evaluate the proposed $Trust^{Block}_{MCDM}$ approach through simulation experiments using OMNeT++ and compare its performance with prior blockchain-based decentralized trust management approach. The simulation results indicate that the proposed $Trust^{Block}_{MCDM}$ approach can not only improve fictitious message detection rate and malicious vehicle detection rate, but also can increase the number of dropped fictitious messages.**

***Index Terms*—Blockchain, Multi-Criteria Decision Making Model, Trust Management, Vehicular Networks**

I. Introduction

As one of the most important evolution of vehicular networks (VANETs) and Internet of Things (IoT), Internet of Vehicles (IoV) has emerged as a promising technology to address the grand challenges of modern transportation. In the IoV, vehicles, road side units (RSUs), and smart devices smoothly interact with each other through Vehicle-to-Everything (V2X) communications to achieve the goals of Intelligent Transportation Systems (ITSs), such as improving the safety, efficiency, and sustainability of transportation networks, reducing traffic congestion, and enhancing drivers' experiences [1]. It is expected that the number of passengers and commercial vehicles used worldwide is about to reach 2 billion by 2035 [2], and there will be 20.8 millions autonomous vehicles in operation in the U.S. by 20230 [3]. Moreover, the McKinsey & Company Global Institute predicts that the potential economic value of IoV will be between $210 billion and $740 billion in the year 2025 [4]. However, IoV is fast becoming a double edged sword: while it is improving our life, it also bring many other problems. The explosive growth in the number of vehicles has potentially caused and even worsened traffic congestion and vehicle accidents on the roads. According to the annual global road crash statistics from Association for Safe International Road Travel [5], nearly 1.25 million people die in road crashes each year, on average 3,287 deaths a day.

As a major enabler of IoV, VANETs provide a platform where traffic-related information, e.g., road conditions, traffic congestion, or even vehicle accidents, can be gathered and shared with neighboring vehicles, which help vehicles timely be aware of traffic situations and finally improve the road safety and travel experience [6]. Both in-vehicle technologies and infrastructure-based safety systems can help prevent crashes before they happen, with technologies like automatic crash notification, emergency vehicle preemption at intersections, and real-time data sharing all helping to speed recovery after an incident occurs [7]. However, due to the high mobility of vehicles and the openness of wireless communications, VANETs are vulnerable to various kinds of security attacks. For example, malicious vehicles may intercept, relay, and even tamper the transmitted traffic-related messages [8]. The problem becomes more serious when malicious vehicle reports fraudulent or incredible traffic information, e.g., the road is clear while there is a traffic accident or congestion actually, which can significantly affect transportation system safety and traffic efficiency.

Trust management is treated as an effective measure to ensure vehicles, without any previous interactions, desire to establish communications with an acceptable level of trust relationships among themselves [9]. In trust management system, each vehicle assesses various behaviors of each interacting vehicle and builds a reputation for each of them based on the behavior assessment, which can help it decide which interacting vehicle is the best option to cooperate with. The existing trust management systems can be categorized into centralized and decentralized approaches [10]. In centralized

approaches, a centralized server collects assessment of vehicles and calculates reputation value for each vehicle. However, the centralized server is easy to become the target of cyber attack and suffers from a single point of failure. In decentralized approaches, trust management system is running on multiple RSUs and each vehicle can retrieve reputation value of other vehicles from the nearest RSU. Nonetheless, how to maintain the consistency of reputation values among multiple RSUs at the real-time is a nontrivial problem. Blockchain, which is designed to achieve peer-to-peer electronic payments directly without participation of a trusted third party [11], is considered to be a feasible approach to cope with the problems existing in the centralized and decentralized trust management approaches. First, the decentralized nature of blockchain allows trust management to run among distributed RSUs, which can successfully avoid the single point of failure. Second, blockchain enables multiple RSUs to cooperate together to maintain a consistent and tamper-proof reputation database without a centralized server.

In light of these, we propose a novel trust management system to enable vehicle to access the reputation of interacting vehicles and evaluate the credibility of received road safety messages in VANETs. Our major contribution is briefly summarized below:

- We propose a blockchain-based trust management system using multi-criteria decision-making model, also referred to as $Trust_{MCDM}^{Block}$, in VANETs, where each vehicle evaluates the credibility of received road safety message, generates the trust value of message originator, and periodically uploads the trust value to the nearby RSU. Then, the RSU calculates the reputation value of message originator using multi-criteria decision-making model, packs the reputation value into a block, and competes to add the block into blockchain.
- We develop a customized discrete event-driven simulation framework by using OMNeT++ [12] and evaluate its performance through simulation experiments. We also revisit prior decentralized trust management approach [13] and modify it to work in the framework for performance comparison and analysis.

The simulation results indicate that the proposed $Trust_{MCDM}^{Block}$ approach can not only improve fictitious message detection rate and malicious vehicle detection rate, but also can increase the number of dropped fictitious messages, indicating a viable trust management system in VANETs.

The rest of the paper is organized as follows. An overview of existing and relevant literature is provided in Section II. Section III focuses on the proposed blockchain-based trust management system. Extensive simulation experiments and their analysis are provided in Section IV. Finally, concluding remarks are provided in Section V.

II. Related Work

In this section, we categorize, present, and analyze existing trust management systems in terms of centralized, decentralized, and blockchain-based approaches in VANETs and similar environments.

Centralized Trust Management Systems: The [14] proposes a software-defined trust based deep reinforcement learning framework, where a deep Q-learning algorithm is deployed into a logically centralized controller of software-defined networking (SDN). The basic idea is that the SDN controller is used as an agent to learn the highest routing path trust value of a vehicular network environment by convolution neural network, where the trust model is designed to evaluate neighbor vehicle's behavior of forwarding packets. If the trust value is greater than or equal to the threshold, the vehicle is trusted. Otherwise, the vehicle is considered as malicious vehicle. In [15], an anti-attack trust management scheme is proposed to evaluate trustworthiness of vehicles in vehicular networks. A Bayesian inference based method and TrustRank based algorithm is utilized to calculate local trust value and global trust value of vehicles respectively, which indicates the local and global trust relationships among vehicles. In order to prevent a vehicle's trust value from rising rapidly and allow it to drop quickly, an adaptive forgetting factor and an adoptive decay factor are used to update local and global trust values.

Decentralized Trust Management Systems: In [13], a decentralized trust management scheme is proposed for vehicular networks. To evaluate the direct trust of one-hop neighbor vehicles based on its behavior and other neighbors' reports, a fuzzy logic-based approach is proposed by taking into account cooperativeness, honestness, and responsibility factors. In addition, a Q-learning approach is proposed to evaluate indirect trust of vehicles that are not directly connected to a evaluator, where an evaluation is conducted by averaging the evaluation reports from multiple vehicles. The [16] presents a framework for computing and updating the trustworthiness of participants in the social IoT network in a self-enforcing manner without relying on any trusted third party. The privacy of the participants in the social IoT network is protected by using homomorphic cryptographic techniques with efficient zero-knowledge proof methods in the decentralized setting. To achieve the properties of self-enforcement, the trust score of each device is automatically updated based on its previous trust score and the up-to-date tally of the votes by its peers in the network with zero-knowledge proofs to enforce that every participant follows the protocol honestly.

Blockchain-Based Trust Management Systems: The [17] proposes a traffic event validation and trust verification mechanism based on the decentralized nature of blockchain in vehicular networks, where the RSUs first use the cooperative traffic information from vehicles and initiate the proposed Proof-of-Event (PoE) consensus algorithm among passing vehicles once the collected data meets the corresponding threshold. If the result of PoE is confirmed to be an incident, the vehicles in the adjacent area are going to be notified through the broadcast from the RSU, and the event stored on the blockchain will be permanently retained for public access. In [18], a blockchain-based trusted data management scheme is investigated to solve the issues of data trust and

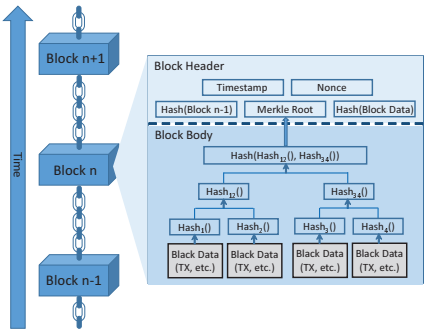


Fig. 1. Generic chain of blocks.

security in edge computing environment, where a flexible and configurable blockchain architecture that includes mutual authentication protocol, flexible consensus, smart contract, block and transaction data management, blockchain nodes management, and deployment is proposed. The [19] provides trust management in vehicular networks by proposing a trustless system model using blockchain and a certificate authority for registering vehicles as well as revoking their registration if needed. In addition, the proposed approach assigns each vehicle a unique crypto fingerprint using a PUF to provide the root of trust. The [20] provides a comprehensive survey and aims at analyzing and assessing the use of blockchain in the context of distributed trust and reputation management systems, with a specific focus on the identification of the relevant emerging features that could represent main drivers for the next generation of distributed trust and reputation management system.

III. The Proposed Blockchain-Based Trust Management System

A. Overview of Blockchain

Blockchain became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. Blockchain is tamper-proof and unforgeable distributed database that generates blocks of cryptographically signed transactions in chronological order and adds them into a specific chain structure without the involvement of a central authority (i.e., a bank, company or government) [21], [22]. As shown in Fig. 1, blocks are chained together through each block containing the hash digest of the previous block's header, which forms the blockchain. The block is composed of block header and block body. The block header contains metadata, such as the previous block header's hash value, a timestamp, the nonce value, a Merkle root, and a hash representation of the block body. The block body consists of a Merkle tree structure [23], where the value of each leaf node is the hash of a transaction record and the value of each non-leaf node is the hash of its child nodes. The Merkle tree is used to store a list of validated and authentic transactions submitted to the blockchain network. If a previously published block were changed, it would have a different hash. This in turn would cause all subsequent blocks to also have different hashes since they include the hash of the previous block, which makes it possible to easily detect and reject altered blocks.

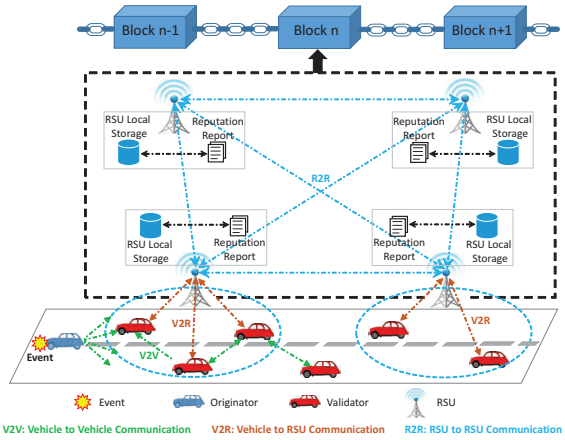


Fig. 2. Overview of the proposed $Trust^{Block}_{MCDM}$ approach.

Thus, blockchain has provided a feasible way to ensure data security and consistency in decentralized networks.

B. System and Adversary Models

A system model of the proposed blockchain-based trust management approach $Trust^{Block}_{MCDM}$ is shown in Fig. 2. Each vehicle is installed with an on-board unit (OBU) which permits it to communicate with other vehicles and RSUs via vehicle-to-vehicle (V2V) and vehicle-to-roadside (V2R) communications [24], respectively. With the assistance of OBU and driving event detection system [25], the vehicle who first detects the traffic-related event (e.g., car accident) can communicate with other vehicles to share event information. However, a malicious vehicle can forge traffic-related event information to deceive other vehicles, which may lead to injuries and even deaths. For example, a malicious vehicle detects a traffic accident on the road, however, it broadcasts a message claiming ''The road is clear.'' to nearby vehicles. Thus, when receiving the road safety message, each vehicle needs to evaluate the credibility of message and generates the trust value of message originator. If the trust value of message originator is larger than a predefined threshold, the vehicle will rebroadcast the received road safety message to neighboring vehicles. Otherwise, it simply discards the received road safety message. Due to the limited storage capacity of OBU, the trust values of message originators cannot be stored locally for a long period. Therefore, each vehicle needs to upload the trust values of message originators to a nearby RSU periodically. RSU is responsible for collecting the trust values of message originators from vehicles and calculating the reputation values of message initiators. And then, the RSU will pack the reputation values of message initiators into a block and compete to be elected as the miner to add the block into the blockchain. Once being added, the reputation value of each vehicle can be accessed by other vehicles whenever it is needed.

C. Blockchain-Based Trust Management System

First, when a vehicle n_i (referred to as originator) detects a traffic-related event, it immediately generates and broadcasts a message, $msg[seq,id,meta,sig^{id}]$, regarding the traffic-related

event to nearby vehicles. The traffic-related event message consists of message sequence number (*seq*), vehicle id (*id*), meta-information (*meta*) such as event type, message originator's location, event location, etc., and a digital signature (sig^{id}) generated using its private key. In this paper, we implicitly assume that the traffic-related event message is only propagated to the vehicles who haven't passed the location of event area. Once a vehicle n_v (referred to as validator) receives the message, it validates the credibility of message based on the opinion from neighboring validators, the reputation value of message initiator, as well as its own confidence to the event, and then generates the trust value of message originator n_i according to

$$Trust_v^i = Opn_v^* \times Rep_v^i \times Conf_v^{msg}. \tag{1}$$

Here, Opn_v^* is the opinion from n_v's neighboring validators, Rep_v^i is the current reputation value of message initiator n_i, and $Conf_v^{msg}$ is n_v's confidence to the event. The opinion from n_v's neighboring validators Opn_v^* is calculated as

$$Opn_v^* = \frac{N_v^{msg}}{N_v^{neighb}}, \tag{2}$$

where N_v^{msg} is the number of rebroadcasted event messages by n_v's neighboring validators and N_v^{neighb} is the total number of n_v's neighboring validators. In addition, n_v's confidence to the event $Conf_v^{msg}$ is observed through

$$Conf_v^{msg} = \eta + e^{-\delta \cdot d_v^i}, \tag{3}$$

where η and δ is the system parameter to control the lower bound and the change rate of confidence, respectively. d_v^i is the distance between message validator n_v and message initiator n_i. The current reputation value of message initiator n_i can be periodically queried from nearby RSUs. If the calculated trust value $Trust_v^i$ is larger than a predefined threshold, validator n_v rebroadcasts the message to neighboring vehicles. Otherwise, it simply discards the message. Finally, validator n_v uploads the trust value of message originator n_i to a nearby RSU.

Second, when the RSU receives various trust values of message originator n_i from different validators, it can calculate the reputation value of message originator n_i by using multi-criteria decision-making model. The RSU first establishes a matrix with the uploaded trust values of message originator and validators' own reputation values. The structure of the matrix is shown as follows:

$$M = \begin{array}{c} \\ R_1 \\ R_2 \\ \vdots \\ R_v \\ \vdots \\ R_m \end{array} \begin{array}{c} \begin{array}{cc} F_1 & F_2 \end{array} \\ \begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \\ \vdots & \vdots \\ f_{v1} & f_{v2} \\ \vdots & \vdots \\ f_{m1} & f_{m2} \end{pmatrix} \end{array},$$

where the row R_v denotes validator n_v who uploaded the trust value; F_1 and F_2 represents the uploaded trust value of message originator n_i from validator and the reputation value of validator, respectively. In order to transform the various scale into a comparable scale, the RSU needs to generate a normalized matrix M^{Norm} (=$[r_{xy}]$), which is calculated as

$$r_{xy} = \frac{f_{xy}}{\sqrt{\sum_{y=1}^{2} f_{xy}^2}}, \quad x = 1, 2, \ldots, m; y = 1, 2. \tag{4}$$

After that, the RSU calculates the weighted normalized matrix M^* (=$[r_{xy}^*]$) by multiplying the normalized matrix M^{Norm} by its associated weights. The weighted normalized value r_{xy}^* is calculated as:

$$r_{xy}^* = w_y \times r_{xy}, \quad x = 1, 2, \ldots, m; y = 1, 2. \tag{5}$$

Here, w_y is the weight used to control the value range of the F_y criterion, and $\sum_{y=1}^{2} w_y = 1.0$. The rationale behind the design of w_y is to adjust the effect of the F_y criterion for subjective preference. Then, the RSU calculates the separation measures using *m*-dimensional Euclidean distance. The separation between each validator's trust value to message initiator and positive-ideal trust value (S_x^+) is given as

$$S_x^+ = \sqrt{\sum_{y=1}^{2} (r_{xy}^* - max(F_y))^2}, \quad x = 1, 2, \ldots, m. \tag{6}$$

Similarly, the separation between each validator's trust value to message initiator and negative-ideal trust value (S_x^-) is as follows:

$$S_x^- = \sqrt{\sum_{y=1}^{2} (r_{xy}^* - min(F_y))^2}, \quad x = 1, 2, \ldots, m. \tag{7}$$

With the results of separation measures, the RSU can calculate a reputation index of message originator n_i based on each validator's own reputation value and uploaded trust value according to

$$\mathbb{I}_x = \frac{S_x^-}{S_x^- + S_x^+}, \quad x = 1, 2, \ldots, m. \tag{8}$$

Here, the value of reputation index $\mathbb{I}_x$ lies between 0 and 1. A larger reputation index value means that the message initiator n_i gets a higher reputation value based on the validator n_x's reputation value and uploaded trust value. Finally, the RSU uses the average of all reputation index values to update the reputation value of message initiator n_i through the low-pass filter with a filter gain constant α,

$$Rep^i = \alpha \cdot \frac{\sum_{x=1}^{m} \mathbb{I}_x}{m} + (1 - \alpha) \cdot Rep^{i,old}. \tag{9}$$

Here, $Rep^{i,old}$ is the previous reputation value of message initiator n_i.

Third, after generating the reputation value of message initiator, the RSU puts the updated reputation value into a block and tries to add it into the blockchain. Since many RSUs may try to add a new block into the blockchain concurrently, a miner should be elected from all these RSUs competitively. To be elected as the miner, a RSU must find a hash value

meeting the following target criterion (known as the difficulty level)

$$Hash(timestamp, prevHash, nonce) < C, \tag{10}$$

where the current system time, *timestamp*, the hash value of previous block, *prevHash*, as well as the *nonce* are used to compute the hash value of its block. Here, C is the hash threshold and can be adjusted by the system to control the difficulty level or the block generation speed. The RSU who first finds a *nonce* to satisfy the above target criterion will be elected as the miner to add its block into the blockchain. The miner packs the reputation values of message initiators along with its digital signature into a block and distributes it to all other RSUs. Other RSUs would accept the newly generated block and add it into their blockchains if the new block fulfills the target criterion Eq. (10) and the attached digital signature can be verified. Otherwise, they just simply discard the block and try to choose another miner. If a RSU receives multiple blocks at the same time, the blockchain starts to fork. In this paper, we adopt the proposed distributed consensus in [26], where each RSU chooses one fork and continues to add new blocks after it. As time elapses, the fork acknowledged by the largest number of RSUs grows faster than others. Finally, the longest one becomes the distributed consensus of the network, while other forks are discarded.

IV. Performance Evaluation

We conduct simulation experiments using OMNeT++ [12] for performance evaluation and analysis. A 2,000 $\times$ 2,000 m^2 square network area is divided into 4 $\times$ 4 square-shaped grids, also referred to as Manhattan-grid map topology [27], where line segment and line segment intersection represents road and traffic intersection, respectively. Before beginning the simulation, 100 to 200 legitimate vehicles are randomly distributed on the roads. The communication range of each vehicle is 200 meters. Each vehicle is traveling along the road with a speed of 10 to 25 meter/sec, and randomly changes direction at the intersection with a zero pause time. There are 5 to 30 malicious vehicles, and the fictitious message rate is set to 0.2 to 1.2 msg/sec. 15 RUSs are randomly distributed along the roads in the network. The total simulation time is 1000 seconds, and each simulation scenario is repeated 10 times with different randomly generated seeds to obtain steady state performance metrics. We measure the performance in terms of fictitious message detection rate, malicious vehicle detection latency, number of dropped fictitious messages, and average of trust value. We also revisit prior decentralized trust management approach $Decen^{Trust}$ [13], and modify it to work in the framework for performance comparison.

First, we measure the fictitious message detection rate by changing the number of malicious vehicles in Subfig. 3(a). The fictitious message can be detected when the calculated trust value of malicious vehicle is less than a threshold value. Broadly speaking, as the number of malicious vehicles increases in the network, the fictitious message detection rate of both $Trust^{Block}_{MCDM}$ and $Decen^{Trust}$ decrease. This is

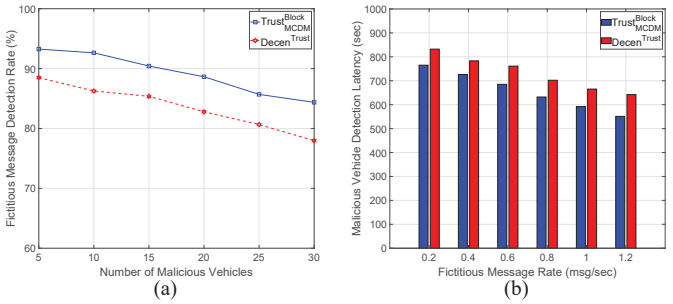
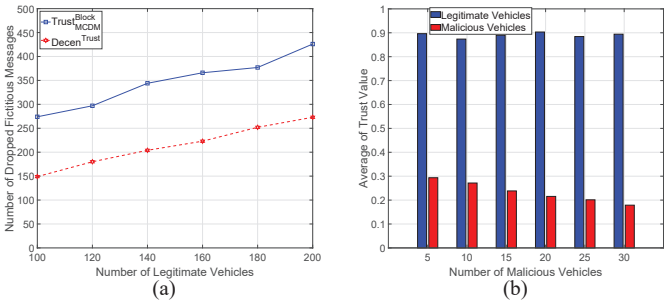


Fig. 3. The performance of fictitious message detection rate and malicious vehicle detection latency.

because more malicious vehicles can collaborate together and rebroadcast the fictitious messages, and the calculated trust value of malicious vehicle can be increased. As a result, a higher trust value of malicious vehicle is uploaded to the RSU and the reputation value of malicious vehicle will be increased. Thus, a less number of fictitious messages can be detected by comparing with a predefined threshold value. However, the $Trust^{Block}_{MCDM}$ outperforms the $Decen^{Trust}$ because each message validator also relies on both reputation value of message initiator and its own confidence to the event to calculate the trust value of message initiator in the $Trust^{Block}_{MCDM}$. The collaboration of malicious vehicles has less effect on the calculated trust value of malicious vehicle, thus, more fictitious messages can be detected.

Second, we observe the performance of malicious vehicle detection latency by varying the fictitious message rate in Subfig. 3(b). When the fictitious message rate increases, the malicious vehicle detection latency of $Trust^{Block}_{MCDM}$ and $Decen^{Trust}$ decrease. With a larger fictitious message rate, the malicious vehicle generates and broadcasts more fictitious messages. Thus, the legitimate vehicles have more chances to validate the fictitious messages from malicious vehicle and generate more lower trust values of malicious vehicle. As a result, the reputation value of malicious vehicle will decrease quickly, and the malicious vehicle can be detected more quickly. The $Trust^{Block}_{MCDM}$ shows a lower malicious vehicle detection latency compared to that of the $Decen^{Trust}$ because more fictitious messages from malicious vehicle can be detected and the reputation value of malicious vehicle drops much more faster. Thus, the malicious vehicle can be detected earlier than that of the $Decen^{Trust}$.

Third, the number of dropped fictitious messages against the number of legitimate vehicles is shown in Subfig. 4(a). Overall, as the number of legitimate vehicles increases, the number of dropped fictitious messages increases. For the $Decen^{Trust}$, since more legitimate vehicles can receive and validate the fictitious message, a lower trust value of malicious message initiator can be obtained and uploaded to the RSU. As a result, more fictitious messages can be dropped by the legitimate vehicles when the reputation value of malicious message initiator is lower than a threshold value. However, a larger number of fictitious messages can be dropped by the $Trust^{Block}_{MCDM}$ than that of the $Decen^{Trust}$. This is because the $Trust^{Block}_{MCDM}$ compares the calculated trust value of malicious



(a) (b)

Fig. 4. The performance of the number of dropped fictitious messages and average of trust value.

message initiator with a threshold value to decide whether to rebroadcast the received message. If the trust value is lower than a predefined threshold, the validator simply discards the message without rebroadcasting. However, in the $Decen^{Trust}$, each vehicle only drops the received message only if the RSU marks the message initiator as a malicious vehicle.

Last, for the proposed $Trust^{Block}_{MCDM}$, we obtain the average of trust value of legitimate and malicious vehicles in Subfig. 4(b). Please note that we do not consider the bad mouth attack in this paper. As the number of malicious vehicles increases, the average of trust value of legitimate vehicles is not changing significantly. However, the average of trust value of malicious vehicles is decreasing linearly as the number of malicious vehicles increases. Since more malicious vehicles will generate and broadcast more fictitious messages, more lower trust values will be generated and uploaded into the RSUs, which causes the reputation values of malicious vehicles decrease. As a result, the overall trust value of malicious vehicles decreases.

V. Concluding Remarks

In this paper, a blockchain-based trust management system using multi-criteria decision-making model is proposed to enable vehicle to access the reputation of interacting vehicles and evaluate the credibility of received road safety messages in VANETs. After evaluating the credibility of received road safety message and generating the corresponding trust value of message originator, each vehicle uploads the trust value to the nearby RSU. After the RSU receives various trust values uploaded from vehicles, it can calculate the reputation value of message originator using multi-criteria decision-making model, packs the reputation value into a block, and competes to add the block into blockchain. We also develop a customized discrete event driven simulation framework by using OMNeT++ and evaluate its performance through simulation experiments in terms of fictitious message detection rate, malicious vehicle detection latency, number of dropped fictitious messages, and average of trust value. The simulation results indicate that the proposed blockchain-based trust management system using multi-criteria decision-making model is a viable trust management system in VANETs.

References

[1] X. Shen, R. Fantacci, and S. Chen, "Internet of Vehicles," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 242–245, 2020.

[2] J. Contreras-Castillo, S. Zeadally, and J. Guerrero-Ibañez, "Internet of Vehicles: Architecture, Protocols, and Security," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3701–3709, 2018.

[3] *Autonomous Vehicles Operating in U.S. 2025/2030*, https://www.statista.com/statistics/750149/us-autonomous-vehicles-in-operation-forecast/.

[4] *Internet of Things for Vehicles is Driving Business*, https://www.raconteur.net/business-innovation/internet-of-things-for-vehicles-is-driving-business.

[5] *Annual Global Road Crash Statistics*, https://www.asirt.org/safe-travel/road-safety-facts/.

[6] W. Benrhaiem, A. Hafid, and P. Sahu, "Reliable Emergency Message Dissemination Scheme for Urban Vehicular Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 1154–1166, 2020.

[7] "Intelligent Transportation Systems-Safety Solutions: Preventing Crashes and Saving Lives," *Office of The Assistant Secretary for Research And Technology*, 2018.

[8] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey," *Vehicular Communications*, vol. 16, pp. 45–61, 2019.

[9] A. Malhi, S. Batra, and H. Pannu, "Security of Vehicular Ad-hoc Networks: A Comprehensive Survey," *Computers & Security*, vol. 89, p. 101664, 2019.

[10] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet Things J. (Early Access)*, pp. 1–1, 2019.

[11] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf.

[12] A. Varga, *OMNeT++*, 2014, http://www.omnetpp.org/.

[13] S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, "Decentralized Trust Evaluation in Vehicular Internet of Things," *IEEE Access*, vol. 7, pp. 15 980–15 988, 2019.

[14] D. Zhang, F. Yu, and R. Yang, "A Machine Learning Approach for Software-Defined Vehicular Ad Hoc Networks with Trust Management," in *Proc. IEEE GLOBECOM*, 2018, pp. 1–6.

[15] J. Zhang, K. Zheng, D. Zhang, and B. Yan, "AATMS: An Anti-Attack Trust Management Scheme in VANET," *IEEE Access*, vol. 8, pp. 21 077–21 090, 2020.

[16] M. Azad, S. Bag, F. Hao, and A. Shalaginov, "Decentralized Self-enforcing Trust Management System for Social Internet of Things," *IEEE Internet Things J. (Early Access)*, pp. 1–1, 2020.

[17] Y. Yang, L. Chou, C. Tseng, F. Tseng, and C. Liu, "Blockchain-Based Traffic Event Validation and Trust Verification for VANETs," *IEEE Access*, vol. 7, pp. 30 868–30 877, 2019.

[18] M. Zhaofeng, W. Xiaochang, D. Jain, H. Khan, G. Hongmin, and W. Zhen, "A Blockchain-based Trusted Data Management Scheme in Edge Computing," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2013–2021, 2020.

[19] U. Javaid, M. Aman, and B. Sikdar, "DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts," in *Proc. IEEE VTC*, 2019, pp. 1–5.

[20] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based Distributed Trust and Reputation Management Systems: A Survey," *IEEE Access*, vol. 8, pp. 21 127–211 517, 2020.

[21] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," *National Institute of Standards and Technology Internal Report*, 2019.

[22] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[23] D. Morrison, "PATRICIA—Practical Algorithm To Retrieve Information Coded in Alphanumeric," *Journal of the ACM*, vol. 15, no. 4, pp. 514–534, 1968.

[24] X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," *IEEE Access*, vol. 7, pp. 58 241–58 254, 2019.

[25] P. Brombacher, J. Masino, M. Frey, and F. Gauterin, "Driving Event Detection and Driving Style Classification using Artificial Neural Networks," in *Proc. IEEE ICIT*, 2017, pp. 997–1002.

[26] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, 2018.

[27] J. Harri, F. Filali, and C. Bonnet, "Mobility Models for Vehicular Ad Hoc Networks: A Survey and Taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 19–41, 2009.