A Blockchain-based Reputation System for Data Credibility Assessment in Vehicular Networks

Zhe Yang*, Kan Zheng*, Kan Yang†, and Victor C. M. Leung‡
*Intelligent Computing and Communication (IC^2) Lab,
Key Laboratory of Universal Wireless Communication, Ministry of Education,
Beijing University of Posts and Telecommunications (BUPT), Beijing, 100876, China.
†Department of Computer Science,
University of Memphis, Memphis, TN 38152, USA.
‡Department of Electrical and Computer Engineering,
The University of British Columbia, Vancouver, BC, Canada V6T 1Z4.
Email: yangzhe077@bupt.edu.cn

***Abstract*—The security of vehicular networks has been paid increasing attention to with the rapid development of automobile industry and Internet of Things (IoT). However, existing approaches mainly focus on ensuring data authentication and integrity, which are not sufficient to assess the credibility of received messages. Recently, reputation systems are proved to be effective approaches to solve the above problem. This paper proposes a new reputation system for data credibility assessment based on the blockchain techniques. In this system, vehicles rate the received messages based on observations of traffic environments and pack these ratings into a "block". Each block is "chained" to the previous one by storing the hash value of the previous block. Then, a temporary center node is elected from vehicles and it is responsible for broadcasting its rating block to others. Based on ratings stored in the blockchain, vehicles are able to calculate the reputation value of the message sender and then evaluate the credibility of the message. Simulation results reveal that the proposed system is reliable in collecting, validating, and storing reputation information in vehicular networks.**

***Index Terms*—Blockchain, reputation system, vehicular networks, data credibility.**

I. Introduction

Recently, vehicles have been given increasing autonomy with the help of various sensing, communications, and data analysis techniques. Gathered by onboard sensors, both internal and external information about a vehicle can be sent to base stations or nearby vehicles through wireless channels. Due to the open environments, security is usually regarded as a vital issue in wireless communication systems, especially for vehicular networks whose environments are much more complex and fast-changing. Therefore, without effective approaches, attackers may forge or manipulate important messages and eventually harm the security or efficiency of vehicular networks.

978-1-5386-3531-5/17/$31.00 © 2017 IEEE

Generally, a secure communications environment in vehicular networks usually means that 1) messages are sourced from legitimate vehicles or infrastructures; 2) messages have not been tampered with; and 3) the information provided by the message is credible and authentic [1]. Several techniques have been widely studied in order to achieve the first two goals, such as identity authentication, digital signature, and data encryption [2]. However, researches for the third goal, i.e., data credibility, are much more deficient [3]. In fact, once the content of a message is incredible, efforts for both identity authentication and data integrity may be in vain.

Thanks to reputation systems, data credibility can be effectively assessed according to past behaviors of data generators. In vehicular networks, reputation is usually regarded as the public knowledge and aggregated opinion of a certain vehicle [4]. Several reputation-based systems have already been presented in previous studies [5]–[7]. Among all these researches, a centralized authority is usually needed in order to collect feedbacks and calculate reputation values. However, due to the wide range and high variability of spatial distribution, vehicles cannot always be covered by a center node, e.g., the base stations. Therefore, how to transmit, calculate, and store reputation information in a decentralized manner is still a problem needed to be solved urgently.

It is believed that blockchain has the potential to cope with the above problems in vehicular networks and eventually revolutionize the Internet of Things (IoT) [8]. Known as one of the disruptive technologies in financial industry, blockchain enables distributed nodes to trade with each other and maintain a consistent ledger without a centralized bank. Based on the basic ideas of blockchain, we propose a decentralized reputation system in vehicular networks. Specifically, a certain vehicle

elected from the crowds rates the received messages and then broadcasts its rating block. Other vehicles can validate the received block using their local knowledges and decide whether to add it to the blockchain or not. Thus, ratings stored in the blockchain are validated by the majority of vehicles and are known as reliable to a large extent.

The reminder of this paper is organized as follows. Section II presents an overview of the blockchain techniques. The detailed designs of the proposed system is introduced in Section III, which includes entities and main procedures. In Section IV, we conduct several tests in order to verify the effectiveness and reliability of the proposed system. Finally, Section V concludes this paper.

II. Overview of blockchain techniques

Blockchain is usually regarded as a series of techniques utilized in decentralized networks so as to maintain a consistent database among all members. It is firstly proposed by Satoshi Nakamoto in order to abstract the core techniques of the well-known digital currency, i.e., the Bitcoin [10]. Different from the traditional centralized network structure, there are no fixed center nodes in blockchain-based networks. All members in the network have relatively equal positions and store the same copy of blockchain. Due to the high security and reliability, blockchain has been applied in a plenty of application scenarios and is regarded as one of the key techniques to promote the development of world.

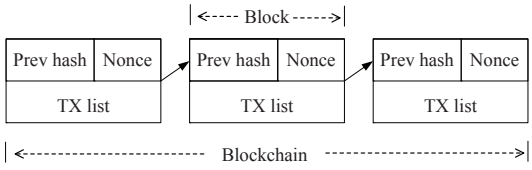

Fig. 1. Typical structure of blockchain.

As depicted in Fig. 1, a blockchain is an ordered list of blocks, where each block stores certain numbers of historical transactions (TXs). These TXs are generated by traders and are broadcast through the entire network. Each block is "chained" to the previous one, by keeping a digest (i.e., the hash value) of the previous block. Thus, any change on a specific block would inevitably destroy the integrity of the chain. In addition, a nonce is usually included in each block, which is the answer of a mathematical problem. The node who firstly solves the problem is elected as a temporary center node, i.e., the miner and broadcasts its block to others. Several miner election schemes have been proposed in recent blockchain-based systems, e.g., the proof-of-work, proof-of-stake, and proof-of-capacity [10], under which nodes with higher computing power, capital, and storage capacity are more likely to win the election. Consequently, blockchain has provided a feasible way to keep data integrity and consistency in decentralized networks.

III. Blockchain-based reputation system

Benefit from the consistency and security, a blockchain-based reputation system is designed to improve the evaluation accuracy of message credibility in vehicular networks. Since the behaviors of a specific vehicle can hardly affect vehicles far away from it, the blockchain only needs to store ratings of nearby vehicles. In this system, all neighboring vehicles traveling together consist the vehicle cluster (VC), in which all members maintain a blockchain and try to reach a consensus of reputation information. A detailed introduction to the system is provided in the following parts, which includes entities and main procedures.

A. Entities

The proposed system mainly contains four types of entities, i.e., the trusted authority (TA), ordinary vehicle (OV), malicious vehicle (MV), and miner.

1) TA: In the blockchain-based reputation system, TA mainly has the following two functions:

- **Vehicle registration:** Vehicles need to register in TA before joining into the vehicular network. TA records the basic information of the vehicle and then allocates an ID and a pair of keys (i.e., the private key and public key) to it. The key pair is used to encrypt and decrypt messages in order to prevent malicious eavesdropping or manipulating.
- **Capacity certification:** Apart from the registration, TA also needs to quantify and certificate the sensing capacity of each vehicle, e.g., the ranges and accuracies of on-board sensors. It is evident that vehicles with higher sensing capacity are able to obtain more accurate environmental information and generate more reliable ratings for the received messages.

Note that TA is only used for registration and certification in the proposed system, which is not included in the generation, transmission, and storage of reputation data.

2) OV: OVs make up the bulk of the VC. Every vehicle joining into the VC can be regarded as an OV until it is elected as the miner. OVs are able to broadcast and receive messages, generate ratings, and receive validated rating packages (i.e., the blocks) from the miner.

3) MV: Sometimes a number of malicious vehicles may exist in vehicular networks. They usually have specific motivations and try to interfere with the normal operation of the network. In this system, it is assumed that MVs mainly have two kinds of malicious behaviors, i.e.,

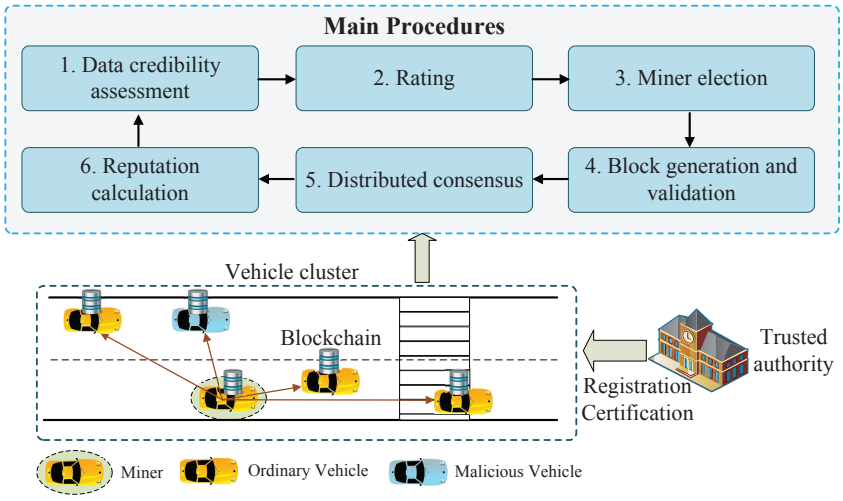

Fig. 2. Architecture of the blockchain-based reputation system.

- Broadcasting fake messages deliberately in order to degrade the traffic security or efficiency;
- Broadcasting fake ratings deliberately in order to degrade the reliability of the reputation system.

4) Miner: Miner is elected from vehicles through specific rules. It can be regarded as a temporary center node which is responsible for generating rating block and broadcasting the block to other vehicles.

B. Main procedures

Main procedures of the proposed system are demonstrated in Fig. 2, i.e.,

1) Data credibility assessment: Vehicles are able to broadcast sensed data about the traffic environment, e.g., messages for traffic accidents or road conditions. Once a certain vehicle has received a message from other vehicles, it can assess the message's credibility based on the reputation value of the sender. Specifically, when the sender's reputation value is higher than a preset threshold, the receiver would take the message as credible and accept it.

2) Rating: Reputation only represents historical behaviors of a certain vehicle, which needs to be timely updated through specific rating mechanisms. After gathering enough information about the received message's credibility using on-board sensing devices, vehicles are able to generate a rating on it, i.e., 1 (for credible messages) or -1 (for incredible messages). However, limited by the message's timeliness and vehicle's sensing capacity, these posteriori ratings may have some mistakes.

3) Miner election: Due to the existence of incorrect ratings, a temporary center node, i.e., the miner, is needed to be elected to broadcast its ratings and try to reach a consensus. The proposed miner election scheme is:

$$\mathrm{Hash}(\mathrm{ID}, \mathrm{time}, \mathrm{PreHash}) < C, \tag{1}$$

where C is the hash threshold representing the quantized sensing capacity certificated by the TA. Several hash functions can be utilized in the proposed system, such as the SHA-256 algorithm. Vehicles calculate the hash value of its ID, current time, and the hash value of the previous block and then compare the results with their C values. The first one to satisfy Eq. (1) is elected as the miner. It is clear that vehicles with stronger sensing capacities have higher probability to win the election.

4) Block generation and validation: After wining the election, the miner packs its ratings into a block and distributes it to all the OVs. OVs would accept the received block and add it to the blockchain if 1) the miner satisfy Eq. (1); 2) ratings recorded in the block can pass the signature validation; and 3) ratings recorded in the block do not conflict with their local ratings. Otherwise, they would ignore the block and elect another miner.

5) Distributed consensus: Owing to the possible incorrect ratings, vehicle's local ratings may conflict with the ratings stored in the received block. Therefore, the blockchain is likely to fork, as depicted in Fig. 3. Obviously, the fork acknowledged by the majority of

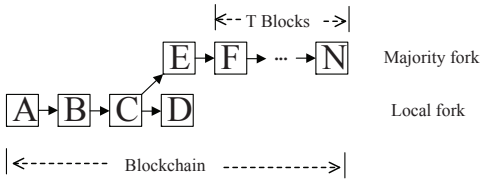

Fig. 3. Blockchain forks.

the VC grows faster than others. When the majority fork is T blocks longer than the local fork, vehicles need to switch to the majority fork, where T is a preset parameter of the system which is called the switch

TABLE I
KEY PARAMETERS OF THE BLOCKCHAIN-BASED REPUTATION SYSTEM.

Parameters	Values
Total number of vehicles	20
Number of malicious vehicles	5
Rating values	1 for credible messages; -1 for incredible messages
Probability of generating mistake ratings	10% for 1/3 OVs; 20% for 1/3 OVs; 30% for 1/3 OVs; 100% for MVs
Switch threshold	3
Number of ratings per block	4
Message generation interval	Poisson distribution with an average of 10 seconds

threshold. Consequently, ratings in the blockchain are validated by the majority of the VC.

6) Reputation calculation: Using the validated ratings stored in the blockchain, a vehicle is able to accumulate these ratings and update the reputation values of other vehicles. Moreover, the rating blockchain can be uploaded to the TA regularly. Based on the data stored in the blockchain, TA is able to reward the vehicles with good reputations in specific rules, such as decreasing the tolls or insurance costs.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental configurations

In order to validate the effectiveness of the proposed system, several experiments are conducted using the Matlab platform. In these experiments both messages and ratings are transmitted through vehicle-to-vehicle (V2V) communications channels [11]–[13]. It is assumed that all data packets can be timely delivered to the destination.

Message detection accuracy (MDA) is used as the performance metric in this paper, which is defined as,

$$MDA = \frac{TP + TN}{TP + FN + FP + TN}, \tag{2}$$

where TP represents the number of true messages being regarded as true ones (true positive); TN represents the number of fake messages being regarded as fake ones (true negative); FP represents the number of fake messages being regarded as true ones (false positive); FN represents the number of true messages being regarded as fake ones (false negative). It is clear that a higher MDA means more accurate detection of message credibility. Key parameters of the blockchain-based reputation system is presented in Table I.

B. Results and analysis

This paper mainly tests and compares two reputation systems, i.e.,

- **Blockchain-based**: The proposed system introduced in Section III;
- **Individually-detect**: Vehicles rate received messages based on the direct observations of the environment and generate reputation values individually [9].

The impacts of three variables on MDA are studied as follows, i.e., the ratio of malicious capacity (ROM), reputation threshold (RTH) and number of zero bits at the beginning of hash threshold (NOZ). ROM is defined by Eq. (3).

$$\text{ROM} = \sum_{i \in M} C_i \Big/ \sum_{j \in A} C_j, \tag{3}$$

where M is the set of malicious vehicles and A is the set of all vehicles.

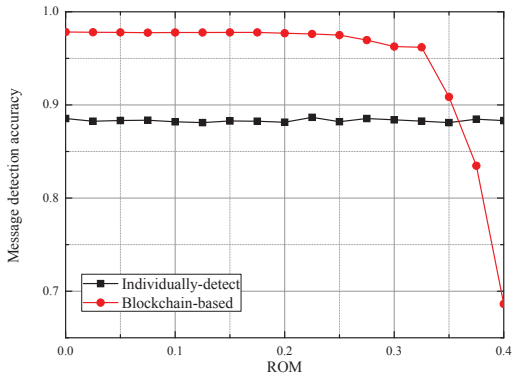

Fig. 4. Message detection accuracy versus ROM.

Fig. 4 plots the impact of ROM on MDA. It is evident that the MDA of individually-detect scheme remains stable with the growth of ROM. This is because under this scheme, vehicles use their own sensors to collect the environmental information and calculate the reputation values individually, which can not be influenced by the mistake ratings generated by malicious attackers. However, ROM has a vital impact on the performance of blockchain-based scheme. It can be observed that the MDA of blockchain-based scheme drops rapidly when the ROM exceeds 0.325. This is because the growing capacity of malicious vehicles may corrupt the consensus reached in the network and add unfair ratings into the blockchain. Therefore, the blockchain-based scheme outperforms the individually-detect one when there is a small proportion of adversaries compared with the entire population of vehicles, which is a common assumption in existing studies [1].

RTH is a threshold value which vehicles used to assess the credibility of received messages. Messages from senders whose reputation values are higher than RTH are trusted by receivers. As depicted in Fig. 5, RTH also has a significant impact on the performances of reputation systems. It is evident that the trends of the two lines well coincide. The MDA rises with the

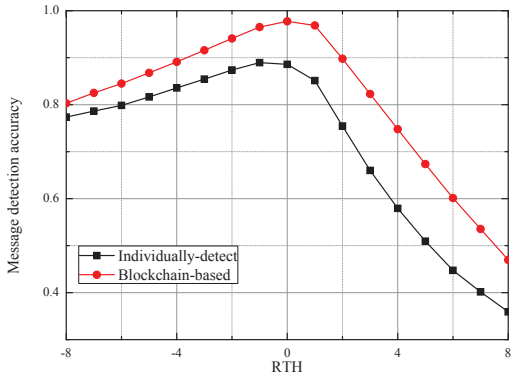

Fig. 5. Message detection accuracy versus RTH.

increase of RTH before it reaches the peak and then drops gradually when the RTH exceeds 0. Hence there exists an optimal RTH value which makes the reputation system perform best. This is because a lower RTH may overlook some fake messages while a higher RTH may mistake true messages for fake ones, both of which have negative effects on the message detection accuracy.

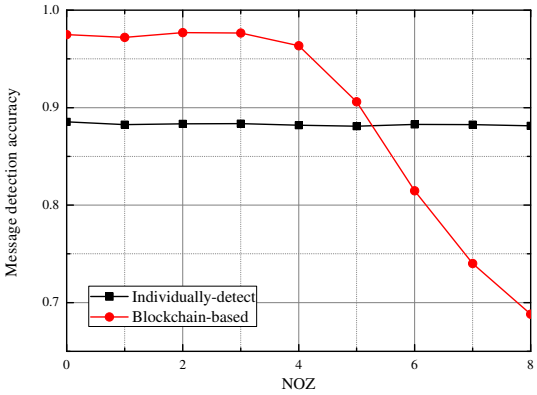

Fig. 6. Message detection accuracy versus NOZ.

NOZ is the number of zero bits at the beginning of the hash threshold. The miner should obtain the hash value smaller than the threshold before broadcasting the rating block. Thus, NOZ represents the difficulty of generating new blocks, which has vital impacts on the update speed of reputations. The impact of NOZ on MDA is depicted in Fig. 6. It is can be observed that once the NOZ exceeds a proper range, it may restrict the update rate of vehicle reputations and finally degrade the MDA.

V. Conclusion

In this paper, we proposed a blockchain-based reputation system in vehicular networks. With the aid of this system, vehicles are able to judge the received messages as ether true or false based on the senders' reputation values. Reputation value is calculated from ratings on the historical messages a certain vehicle has ever broadcast. These ratings are generated by a temporary center node, validated by the majority of vehicles, and finally stored in the blockchain. Therefore, ratings stored in the blockchain represent the consensus of crowds on each vehicle's reputation. A number of experiments are carried out in order to verify the reliability of the entire system. Experimental results demonstrate that the system can play a vital role in the assessment of data credibility and finally improve the security of vehicular networks.

VI. Acknowledgment

This work was supported by the China Natural Science Funding (NSF) under Grant 61331009, the Fundamental Research Funds for the Central Universities under Grant 2014ZD03-02, the BUPT Excellent Ph.D. Students Foundation under Grant CX2016208, and China Unicom Project.

References

[1] Q. Li *et al.*, "A reputation-based announcement scheme for VANETs," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 9, pp. 4095-4108, Nov. 2012.

[2] A. Wasef *et al.*, "Complementing public key infrastructure to secure vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 17, no. 5, pp. 22-28, Oct. 2010.

[3] T. Roosta *et al.*, "Distributed reputation system for tracking applications in sensor networks," in *Proc. 3rd Annual International Conference on Mobile and Ubiquitous Systems*, San Jose, USA, July 2006, pp. 17-21.

[4] S. Li *et al.*, "Quickest attack detection in multi-agent reputation systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 4, pp. 653-666, Aug. 2014.

[5] M. Mahmoud *et al.*, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 8, pp. 3947-3962, Oct. 2011.

[6] K. Zheng *et al.*, "Stochastic performance analysis of a wireless finite-state Markov channel," *IEEE Transactions on Wireless Communications*, vol. 62, no. 4, pp. 1450-1458, Feb. 2013.

[7] C. Lai *et al.*, "SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1559-1574, June 2017.

[8] K. Christidis *et al.*, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, May 2016.

[9] H. Yu *et al* "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, no. 10, pp. 1755-1772, Oct. 2010.

[10] F. Tschorsch *et al.*, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084-2123, thirdquarter 2016.

[11] J.B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162-1182, July 2011.

[12] F. Liu *et al.*, "Design and performance analysis of an energy-efficient uplink carrier aggregation scheme," *IEEE Journal on Selected Areas in Communication*, vol. 32, no. 2, pp. 197-207, Feb. 2014.

[13] K. Zheng *et al.*, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2377-2396, Fourthquarter 2015.