Blockchain-Based Decentralized Trust Management in Vehicular Networks

Zhe Yang, Kan Yang, *Member, IEEE*, Lei Lei, *Senior Member, IEEE*, Kan Zheng, *Senior Member, IEEE*, and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*—Vehicular networks enable vehicles to generate and broadcast messages in order to improve traffic safety and efficiency. However, due to the nontrusted environments, it is difficult for vehicles to evaluate the credibilities of received messages. In this paper, we propose a decentralized trust management system in vehicular networks based on blockchain techniques. In this system, vehicles can validate the received messages from neighboring vehicles using Bayesian Inference Model. Based on the validation result, the vehicle will generate a rating for each message source vehicle. With the ratings uploaded from vehicles, roadside units (RSUs) calculate the trust value offsets of involved vehicles and pack these data into a "block." Then, each RSU will try to add their "blocks" to the trust blockchain which is maintained by all the RSUs. By employing the joint proof-of-work (PoW) and proof-of-stake consensus mechanism, the more total value of offsets (stake) is in the block, the easier RSU can find the nonce for the hash function (PoW). In this way, all RSUs collaboratively maintain an updated, reliable, and consistent trust blockchain. Simulation results reveal that the proposed system is effective and feasible in collecting, calculating, and storing trust values in vehicular networks.**

***Index Terms*—Blockchain, data credibility, trust management, vehicular networks.**

I. Introduction

RECENTLY, vehicles have been given increasing autonomy with the help of various on-board sensing, computation, and communication devices [1], [2]. All infrastructures and smart vehicles constitute the vehicular network, which has become an important scenario of the fifth generation mobile networks [3]–[5]. Vehicular networks provide a platform for vehicles to share road-related messages with their neighbors, e.g., road conditions, traffic congestions, etc. These messages help vehicles timely be aware of traffic situations and hence improve the transportation safety and efficiency [6].

However, due to the high mobility and variability of vehicular networks, neighboring vehicles are usually strangers and cannot fully trust with each other. This problem becomes more serious when there are malicious vehicles existing in the network. These attackers may disseminate incredible messages on purpose. For example, a malicious vehicle may broadcast a message claiming that the road is clear, while there is a traffic accident or congestion actually. These misbehaviors can greatly endanger the traffic safety or efficiency of the transportation system. Therefore, how to effectively evaluate the trustworthiness of vehicles is an important problem in vehicular networks.

Trust management system enables vehicles to decide whether the received message is trustworthy or not, and also provides network operators the basis of rewards or punishments on specific vehicles [8], [9]. Usually, the trust value of a certain vehicle can be calculated using ratings on its past behaviors, which are generated by relevant nodes. Existing trust management systems can be classified into two groups, i.e., centralized and decentralized. In centralized trust management systems [10], [11], all ratings are stored and processed in a central server, e.g., cloud server. As vehicles usually have to make decisions in a quite short delay, these centralized systems cannot always satisfy the rigorous quality-of-service (QoS) requirements for vehicular networks. In decentralized trust management systems [13]–[15], trust management tasks are conducted in vehicle itself or in the roadside unit (RSU). Local management of trust values may reduce the interactions with network infrastructures. However, due to the different capacities and conditions to observe and assess the target events, ratings generated by a single vehicle cannot be always reliable. Moreover, the high variability of network topology makes it a big challenge to timely evaluate all vehicles it encounters. Some studies also utilize the RSU for trust management [15]. However, RSUs are usually distributed outside and are vulnerable to malfunctions and intrusions, which cannot provide reliable and consistent trust service for the whole vehicular network. Therefore, how to effectively conduct trust management in vehicular networks is still a problem remained to be solved urgently.

With this in mind, blockchain is considered as a feasible tool to cope with the problems above. Blockchain is initially known as one of the disruptive technologies in financial industry, which enables distributed nodes to trade with each other

Manuscript received February 1, 2018; revised April 11, 2018; accepted May 3, 2018. Date of publication May 14, 2018; date of current version May 8, 2019. This work was supported in part by the China Natural Science Funding under Grant 61731004, and in part by the BUPT Excellent Ph.D. Students Foundation under Grant CX2016208. *(Corresponding author: Kan Zheng.)*

Z. Yang and K. Zheng are with the Intelligent Computing and Communication Laboratory, Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: zkan@bupt.edu.cn).

K. Yang is with the Department of Computer Science, University of Memphis, Memphis, TN 38152 USA.

L. Lei is with the School of Science and Engineering, James Cook University, Cairns, QLD 4878, Australia.

V. C. M. Leung is with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada.

Digital Object Identifier 10.1109/JIOT.2018.2836144

and maintain a consistent and tamper-proof ledger without a centralized bank [17], [24]. Besides, due to its high security and reliability, blockchain has been widely studied and applied in nonfinancial scenarios, e.g., content delivery [26], key management [18], decentralized storage [19], [20], etc. Based on the decentralization nature of blockchain, trust management can be conducted among distributed RSUs, which can effectively avoid the problems of centralization. Moreover, blockchain enables RSUs to work together and maintain a consistent database. Even though a small portion of RSUs are compromised by attackers, the block generation speed of attackers is much slower than that of benign RSUs. Therefore, the proposed system can effectively hold the trust management tasks in vehicular networks, which enables vehicles to evaluate the trustworthiness of neighbors and assess the credibilities of received messages. The contributions of this paper can be summarized as follows.

1) We proposed a new decentralized trust management scheme for vehicular networks based on the blockchain technology, which not only enables all the RSUs to participate in updating the trust values in a decentralized manner but also provides all RSUs the trust information of all the vehicles in the vehicular networks.
2) We proposed a joint proof-of-work (PoW) and proof-of-stake consensus mechanism which enables all the RSUs to compete to update the trust, i.e., add a trust block. This captures the factor that the block containing the maximum total values of trust offset needs to be added first, as it affects the whole trust database significantly.
3) We conduct the simulation to show that our proposed blockchain-based decentralized trust management system is efficient in practical vehicular networks.

The remainder of this paper is organized as follows. Section II reviews the related works. The system model, adversary model and design goals are introduced in Section III. Section IV briefly describes the blockchain and the advantages of applying blockchain in constructing trust management system. In Section V, we introduce our blockchain-based decentralized trust management system in detail. Security analysis, performance evaluation, and further discussion about the proposed system are given in Sections VI–VIII, respectively. Finally, Section IX concludes this paper.

II. Related Work

A. Centralized Trust Management

Centralized trust management in vehicular networks has been widely studied recently. In these works [7], [10], [11], a central server is utilized to collect, calculate, and store the trust values of all vehicles. The central server is usually assumed to be a fully trusted entity, which cannot be compromised by attackers.

In [7], a reputation-based announcement scheme is presented in vehicular networks. In this paper, vehicles sense the traffic-related events and publish announcements to neighbors. The receivers need to evaluate the credibilities of messages and generate feedback reports. All feedbacks are collected by a centralized reputation server. Based on these data, the server is able to update the reputation values and issue certificates for all vehicles in the network. Moreover, Mahmoud and Shen [10] proposed a stimulation and punishment mechanism for mobile nodes. In this mechanism, a "micropayment" is used to stimulate nodes to relay packets from others. The honest nodes can earn certain amounts of credits, which can be spent when they have relay requirements. A reputation system is also designed to cope with the packet droppers. When a malicious node deliberately drops relaying packets, it will be reported by the packet receivers and finally be evicted from the network. In addition, a reputation system for reliable cooperative downloading is designed in [11], which enables vehicles to securely download and forward packets for others. When a proxy vehicle honestly finishes the task, it will obtain a virtual check from the packet receiver. Using this check, the reputation system is able to encourage cooperation and punish malicious vehicles.

All these schemes utilize a fully trusted central server for trust management. However, with the rapid development of intelligent transportation systems, it is not practical to cope with large numbers of vehicles using a centralized node. Too many requests will probably bring about high latency or even blocking, which may greatly decrease the QoS for users. Moreover, the single point of failure is also a big challenge for centralized networks.

B. Decentralized Trust Management

In order to cope with the problems of centlization mentioned above, decentralized systems are introduced for trust management. Raya *et al.* [12] proposed a data-centric trust management scheme in ad hoc networks. Once receiving data from others, the node will first calculate the trust value for each piece of data. Then, all these values are aggregated using specific algorithms. If the aggregated value exceeds a threshold, the receiver will trust the content of the data. Gurung *et al.* [13] also tried to tackle with the similar problem. This paper first analyzes the key words of messages and divides all messages into groups. Then, the trust values of all messages are calculated based on the content similarity, content conflict and routing path similarity. Besides, Li and Chigan [14] presented a mechanism which jointly considers privacy and reputation issues. Tasks of behavior evaluation, reputation aggregation and manifestation are collectively performed on each vehicle. The partially blind signature is adopted to preserve the vehicle privacy. All these schemes need individual vehicle to manage the trust values by itself, which may be inaccurate due to the limited observation conditions or possible malfunctions.

In [15] and [16], RSU is employed for trust management, where vehicles generate ratings for others and upload these ratings into the nearby RSU. They can also send requests to RSU to query the trust values of neighboring vehicles. However, the trust information stored in the distributed RSU may not be complete and consistent. Therefore, it is critical but also challenging to develop a decentralized reliable and consistent trust management system in vehicular networks.

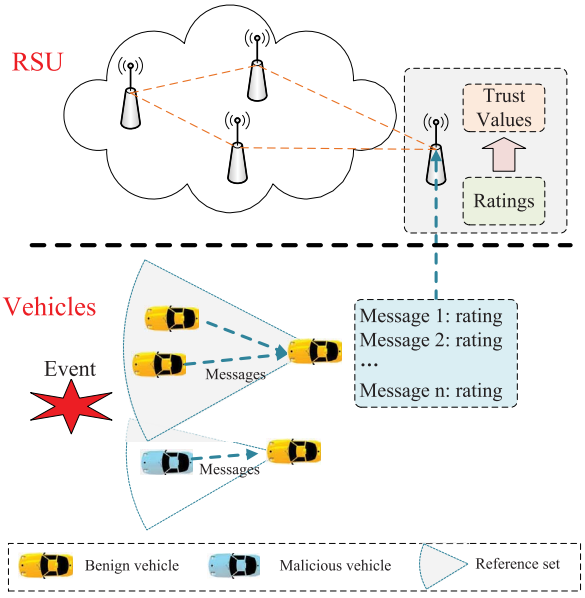


Fig. 1. System model of decentralized trust management in vehicular networks.

C. Blockchain-Based Decentralized Data Management

Blockchain has been given an increasing attention for decentralized data management. For example, Cai *et al.* [19] presented a encrypted decentralized storage system based on blockchain techniques to handle the fraudulent behaviors of clients. In this system, important information about the stored files, e.g., the digests, tokens, and metadata of integrity checking, is stored in the blockchain, which provides fair judgments for storage and search services. Moreover, Cai *et al.* [20] designed a blockchain-based distributed storage and keyword search platform. In this paper, the blockchain is used to store the public keys of well-behaved nodes, which are confirmed by the majority of the network. Therefore, due to the features of decentralization, consistence, and tamper-proofing, blockchain can be a promising technique to help cope with the trust management problems in vehicular networks.

III. Problem Definition

A. System Model

As illustrated in Fig. 1, a decentralized trust management system in vehicular networks mainly includes several connected RSUs and vehicles on the road.

1) RSU: Due to its resources and capabilities, RSU is responsible for the major tasks, i.e., rating collection and trust value management.

1) *Rating Collection:* Ratings are generated by message receivers in order to evaluate the credibilities of messages. However, they cannot be stored and managed locally in the long term, due to the fast changing traffic environments and limited capacity of on-board devices. Therefore, vehicles need to periodically upload their ratings into the nearby RSUs, which serve as the collectors and hosts for these data.

2) *Trust Value Management:* We assume that only RSUs are able to calculate the trust value for a certain vehicle based on the collected ratings. Trust value is the aggregated opinion of a vehicle, which represents the historical credibilities of messages sent by it. Once being calculated, trust values can be queried by other vehicles if needed.

2) Vehicles: Vehicles are equipped with on-board sensors, computers, and communication devices, which are used for data gathering, processing, and sharing.

With the help of on-board devices, vehicles can automatically detect traffic-related events and send warning messages to others using vehicle-to-vehicle communications standards, e.g., the long term evolution vehicle-to-vehicle or dedicated short-range communications [22]. However, not all messages are useful. For example, if a vehicle has already passed the location of a specific event, reports about this event will no longer be valuable for it. Therefore, each vehicle needs to maintain a reference set, whose members are of high relevance to the traffic safety of the target vehicle. In this system, the reference set of a certain vehicle is composed of neighboring vehicles traveling in front within certain distance, as illustrated in Fig. 1. Using messages sent from the reference set, vehicles can timely be aware of the traffic conditions and respond to possible events.

However, due to possible malfunctions or misbehaviors, messages from the reference set are not always trustworthy. Receivers need to aggregate all messages about a certain event and figure out the credible ones. Specific models are used for message aggregation, e.g., the majority rule. Then, the receiver can generate ratings for messages based on the credibilities and then upload these ratings into the RSU.

B. Adversary Model

Both vehicles and RSUs are vulnerable to probable attackers, which can severely interfere the operation of trust management systems and thus endanger the traffic safety of vehicles. Two adversaries are considered in this paper, i.e., the malicious vehicle and compromised RSU.

1) Malicious Vehicle: 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. These misbehaviors can severely endanger the traffic safety or efficiency of benign vehicles. In this paper, malicious vehicles mainly have two types of behaviors.

a) Message spoofing attack: Attackers may deliberately broadcast fake messages in order to degrade the traffic safety or efficiency. For example, a malicious vehicle may detect a traffic accident on the road, but broadcast a message claiming "The road is clear!" to nearby vehicles.

b) Bad mouthing and ballot stuffing attack: In this system, the bad mouthing (ballot stuffing) attack means that vehicles generate and upload unfair negative (positive) ratings on credible (incredible) messages. For example, after receiving a credible message, a malicious vehicle may deliberately generate a negative rating (e.g., -1) on this message and upload this rating to the RSU.

2) Compromised RSU: RSUs are distributed along the road and sometimes lack protection from the network operators. Therefore, these entities are assumed to be semitrusted, which may be compromised by the attackers. Once intruding into an RSU, the attacker is able to add, delete, and tamper the data stored in it. However, the large-scale intrusion attacks are highly unlikely due to the limited capacity of attackers. Moreover, due to the periodical security check from the network operators, the compromised RSU cannot be controlled by attackers for a long time. Based on these facts, it is assumed that attackers can only compromise a small portion of RSUs during a short period of time.

C. Design Goals

This paper focuses on assessing, recording, and disseminating the vehicle trustworthiness in vehicular networks. Thus the main objectives are that all behaviors of vehicles can be justly evaluated, and all vehicles are able to access the reliable trust values of neighbors if needed. The design of a trust management system should achieve the following goals.

1) Decentralization: With the rapid increase of smart vehicles, the centralized trust management schemes may be unpractical. Therefore, the trust management system needs to take full advantages of distributed nodes, i.e., RSUs and vehicles. Trust values are calculated by ratings uploaded from message receivers and are stored in the RSU, which can ensure the reliability and scalability of the system.

2) Tamper-Proofing: RSUs are usually distributed outside and vulnerable to be compromised by attackers. If the data stored in the compromised RSU are tampered, the reliability of trust management will be affected. However, the large scale compromising of RSUs is unlikely due to the limited capacity of attackers. Therefore, the trust management system should be resistant to a small portion of compromised RSUs.

3) Consistency: Due to the high mobility feature, vehicles usually need to travel across many RSUs. Under this scenario, how to exchange trust data among RSUs and maintain a consistent database becomes a challenging issue for decentralized trust management in vehicular networks.

4) Timeliness: Trust value indicates the overall evaluation of a certain vehicle based on its historical behaviors. This value may change over time according to the credibilities of messages sent by this vehicle recently. Hence, the trust values stored in RSUs need to be updated in time.

5) Availability: Trust values stored in the RSU need to be available for vehicles if they want to know the trustworthiness of any neighboring vehicles. Thus, an application interface (API) is required for vehicles to send query requests and receive corresponding trust values from RSUs.

IV. Methodology

A. Blockchain

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 first proposed by Satoshi Nakamoto in order to abstract the core techniques of the well-known digital currency, i.e., the bitcoin [21]. Different from the centralized network structure, there are no fixed center nodes in blockchain-based networks. All members in the network have relatively equal positions and keep the same copy of blockchain. Therefore, no one can change the data recorded in the blockchain unless he has obtained strong enough capacity to confuse the crowds. Due to the high security and reliability, blockchain has been widely studied and applied recently.

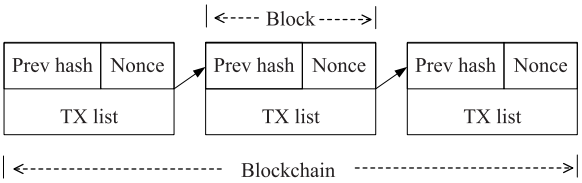


Fig. 2. Typical structure of blockchain.

As shown in Fig. 2, 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 broadcasted 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 solves the problem is elected as a temporary center node, i.e., miner and broadcasts its block to others. Several miner election schemes have been proposed in recent blockchain-based systems, e.g., the PoW, proof-of-stake, and proof-of-capacity [21], 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 security and consistency in decentralized networks.

B. Design Overview

In this paper, we explore how the blockchain can be used to keep the trust values of vehicles. First, all vehicles assess the credibilities of received messages and then generate ratings for them. The positive rating (e.g., +1) indicates a credible message, while the negative rating (e.g., -1) represents an incredible one. These ratings are uploaded into the RSU, which plays a dominant role in trust management. Compared with the vehicles, RSUs usually have more stable network topology, more reliable communications channels (i.e., wired link), and more powerful computing and storage capacities. These advantages make RSU a good choice for decentralized trust management in vehicular networks.

Based on the ratings uploaded from vehicles, RSU needs to calculate the offset of trust values for every involved vehicle using specific methods. In this system, trust value offset is between -1 and $+1$, which is positively correlated with the ratio of positive ratings. The sum of all offsets is the trust value of this vehicle. Similar with the transactions mentioned above, several offsets are packed into a candidate block by the RSU. Then the RSU tries to be elected as the miner and adds this block into the blockchain.

Miner election method is one of the most important parts in blockchain-based systems. In vehicular networks, the block containing the maximum total absolute values of trust offset needs to be added first, as it will affect the whole trust database significantly. In our design, we develop a joint PoW and proof-of-stake election scheme, which takes the sum of absolute values of offsets in the candidate block as the stake. RSUs with larger stakes are more likely to be elected as the miner. Therefore, the larger variations on trust values will be more quickly to be reflected in the blockchain, which ensures the timely update of the recorded data. By accumulating all offsets of each vehicle stored in the blockchain, RSUs are able to obtain the real-time trust values.

By contrast, the traditional proof-of-stake scheme lacks randomization, which may cause that RSUs with large stakes continuously win the election and restrict the trust value updating of RSUs with low stakes. If the RSU with large stakes is compromised by the adversary, this adversary may compromise the entire trust system. In addition, the traditional PoW scheme only takes computing capacity as the basis of miner election, which cannot distinguish high stake RSUs and low stake ones. Therefore, large variations on trust values cannot be fast reflected in the blockchain.

C. Advantages of Applying Blockchain in Trust Management

The following advantages make blockchain a promising solution for trust management in vehicular networks, which is able to achieve the design goals listed in Section III-C.

1) Decentralization: Compared with the centralized network structure, blockchain enables distributed nodes to cooperate with each other and maintain a reliable database. Every node in the network has a copy of the blockchain and is able to conduct specific operations on it, e.g., calculation and data query. Hence, the system scalability is improved to a large extent. Furthermore, the single point of failure can be effectively mitigated once using blockchain, which is always a challenging issue in centralized networks.

2) Tamper-Proofing: Due to the chain structure, malicious users attempting to modify one block stored in the blockchain, have to rebuild the whole chain after it, which exponentially increases the time cost of tampering. Moreover, all RSUs compete to be the miner in order to add their blocks. Under the assumption that most of RSUs are benign, the block generation speed of these RSUs is much larger than that of compromised ones. Therefore, the influence of small numbers of compromised RSUs on the blockchain is very limited.

3) Consistency: Blockchain enables distributed RSUs to main a consistent trust database. All RSUs contribute to the blockchain and extract data from it. Therefore, they can return the same results once being queried by vehicles.

4) Timeliness: Based on the idea of joint PoW and proof-of-stake, RSUs with larger absolute offsets are more easier to win the miner election and then add their blocks into the blockchain. This scheme makes larger changes on trust values to be faster reflected and thus ensures the timeliness of data stored in the blockchain.

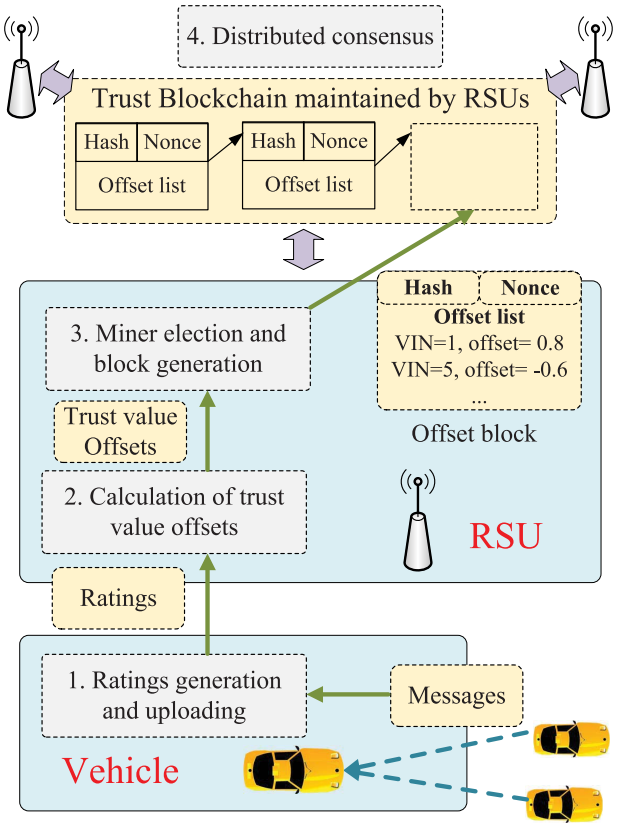


Fig. 3. System design of blockchain-based decentralized trust management.

5) Availability: Using the data stored in the blockchain, RSUs are able to accumulate all offsets about a certain vehicle and get its current trust value. Once a vehicle wants to know the trustworthiness of its neighbors, it can send request to the nearby RSU. After checking the identity of the requester, the RSU sends a response containing the trust value of the target vehicle.

V. Detailed Design of the Proposed System

A. Main Procedures

As illustrated in Fig. 3, main procedures of the blockchain-based decentralized trust management can be divided into the following steps.

1) Rating generation and uploading.
2) Calculation of trust value offsets.
3) Miner election and block generation.
4) Distributed consensus.

Step 1 (Rating Generation and Uploading): This procedure is conducted on vehicles, more specifically, the message receivers. Due to the presence of possible malfunctions or misbehaviors, messages from the reference set Ref are not always credible. Therefore, specific rules are needed for message receivers to assess the credibilities of messages and generate ratings for them. First, the receiver divides all messages into groups $\{M_1, M_2, \ldots, M_j, \ldots\}$, where M_j represents the message group reporting event e_j, e.g., "There is a traffic accident at road segment A!" However, not all messages in a same group are of equal credibility. Messages sent by vehicles near

the event location are usually more trustworthy than these from remote vehicles. Therefore, the credibility of a certain message is defined as follows:

$$c_k^j = b + e^{-\gamma \cdot d_k^j} \tag{1}$$

where c_k^j is the credibility of message in group M_j sent by vehicle k. d_k^j is the distance between the message sender and the event location. b and γ are two preset parameters, which control the lower bound and change rate of message credibility, respectively. In addition, $c_k^j = 0$ if vehicle k does not report this event. Using (1), the receiver can obtain a credibility set C^j for event e_j, where $C^j = \{c_1^j, c_2^j, \ldots\}$. Based on the credibility set C, the receiver is able to calculate the aggregated credibility of event e using Bayesian inference [12]

$$P(e/C) = \frac{P(e) \cdot \prod_{k=1}^{N} P(c_k/e)}{P(e) \cdot \prod_{k=1}^{N} P(c_k/e) + P(\bar{e}) \cdot \prod_{k=1}^{N} P(c_k/\bar{e})} \tag{2}$$

where $\bar{e}$ is the complementary event of e. $P(c_k/e) = c_k$ $P(c_k/\bar{e}) = 1 - c_k$. $P(e)$ is the prior probability of event e. $P(e/C) \in [0, 1]$. Once $P(e/C)$ exceeds a preset threshold Thr, the receiver regards this event as true and generates positive ratings (i.e., +1) on messages correctly reporting this event. Otherwise, it will generate negative ratings (i.e., -1) on them.

Finally, vehicles periodically upload the ratings to the RSU nearby for further use. The format of a rating is (VIN_i, VIN_j, m_k, $rating$), where VIN_i and VIN_j are the vehicle identity numbers of message receiver and sender, respectively; m_k is the identifier of the message; and $rating$ is either -1 (for incredible messages) or $+1$ (for credible messages).

Step 2 (Calculation of Trust Value Offsets): The RSU may get conflicting ratings about a specific message, e.g., seven positive ratings and three negative ratings. The former is the majority group and the latter is the minority group. In the proposed system, weighted aggregation is used on these ratings to obtain the offset of trust value. The offset is between -1 and $+1$, which is positively correlated with the ratio of positive ratings on this message. The calculation of trust value offset is shown as follows:

$$o_k^j = \frac{\theta_1 \cdot m - \theta_2 \cdot n}{m + n} \tag{3}$$

where o_k^j is the trust value offset of vehicle k based on message j and $o_k^j \in [-1, 1]$. m and n are the number of positive ($+1$) and negative (-1) ratings, whose weights are θ_1 and θ_2, respectively. θ_1 and θ_2 are calculated using the following equation:

$$\theta_1 = \frac{F(m)}{F(m) + F(n)} \qquad \theta_2 = \frac{F(n)}{F(m) + F(n)} \tag{4}$$

where $F(.)$ controls the sensitivity to the minority group of ratings. For example, the aggregated offset with $F(x) = x^2$ is less sensitive to the minority group of ratings compared with $F(x) = x$. Under the assumption that attackers cannot control a large portion of vehicles, the majority groups of ratings are more likely to be fair ratings. Therefore, the proposed weighted aggregation is able to improve the reliability of trust value offsets. Finally, the RSU puts all these offsets into the set O and tries to add it into the blockchain.

Step 3 (Miner Election and Block Generation): Due to the decentralized network structure, there is no constant center node to manage the blockchain. Therefore, a miner is periodically elected from all RSUs in order to generate new offset blocks. Miner election method based on PoW is usually used in blockchain-based systems, e.g., the bitcoin. In these systems, all nodes continuously change the nonce and then calculate the hash values of the block including the nonce. The one getting the hash value lower than a threshold is elected as the miner and is able to publish its block. All nodes have the same threshold, which makes nodes with more powerful computation capacity easier to get the right nonce and win the election. Based on PoW, the proof-of-stake is proposed which makes different nodes have different hash thresholds, and thus different generation speeds of blocks.

In this system, a *joint PoW and proof-of-stake* miner election method is designed, which takes the *sum of absolute offsets* as stakes and the difficulty to complete the PoW depends on the stake. RSUs with more stakes can find the nonce and win the election easier (i.e., more quickly to publish their blocks), which ensures the timely update of data stored in the blockchain. The proposed miner election method is

$$\text{Hash}(\text{ID}_{\text{RSU}},\ \text{time},\ \text{PreHash},\ \text{nonce}) \leqslant S_i \tag{5}$$

where S_i is the hash threshold of RSU i. All RSUs continuously change the nonce and calculate the hash values according to (5). The one getting the nonce satisfying the above condition is elected as the miner. S_i is positively correlated with F_i, which is defined as the sum of absolute values of trust value offsets

$$F_i = \min\left(\sum_{o_k^j \in O_i} \left|o_k^j\right|, F_{\max}\right) \tag{6}$$

where O_i is the current offset set of RSU i. Therefore, the RSU with larger F_i is more likely to win the election and then publish its block. In this way, large variation of trust values can be timely updated in the blockchain. $F_{\max}$ is the upper bound of F_i, which is used to avoid the situation that the RSU with too large F_i continuously wins the election. Therefore, the relative fairness is achieved among RSUs. Once the RSU successfully adds the offset block into the blockchain, it will clear the elements in O_i.

Construction of S_i: S_i is series of binary bits which stars from several continuous zeros. S_i can greatly influence the generation speed of offset blocks for each RSU. In the proposed system, the relationship between S_i and F_i is defined as follows:

$$\begin{aligned} N_z &= \text{int}\left(e^{-(\eta \cdot F_i + \mu)}\right) \\ S_i &= 2^{N_m - N_z} - 1 \end{aligned} \tag{7}$$

where int(.) returns the integral part of the value; N_z is the number of continuous zeros at the top of S_i; and N_m is the bits of the hash value depending on the hash algorithm (e.g., 160 for SHA-1, 256 for SHA-256, etc.), as illustrated in Fig. 4.

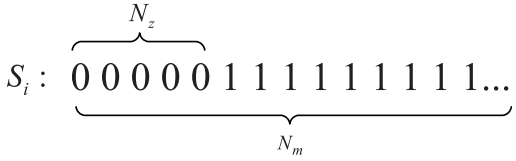


Fig. 4. Relationships among N_z, N_m, and S_i.

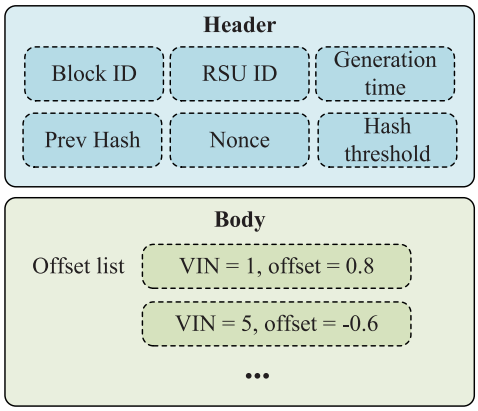


Fig. 5. Format of offset block.

The format of an offset block is shown in Fig. 5, which contains two parts, i.e., the header and body. The header stores: 1) the basic information about the block, such as block ID, RSU ID, and generation time; 2) the hash of the previous rating block, which is used to chain this block to the existing blockchain; and 3) information to prove the validity of this block, i.e., the nonce and hash threshold. The body mainly contains the list of trust value offsets.

Step 4 (Distributed Consensus): Once receiving a block from the miner, the RSU needs to check the validity of the nonce and then add it to its blockchain. Sometimes the RSU may receive more than one blocks at the same time. Under this circumstances, the blockchain starts to fork. A distributed consensus scheme is used to cope with this issue. Each RSU chooses one fork and continues to add new blocks after it. As time goes by, 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 the other forks are discarded. In addition, each RSU needs to collect blocks generated by themselves in the discarded forks and try to add them to the blockchain in the future. In this way, all RSUs store the same version of blockchain, which ensures the consistency of the network.

B. Application Interface

1) Trust Value Query: Once a vehicle wants to know the trust value of another, it needs to send a query request ($QueryReq$, VIN_i, VIN_j) to the RSU nearby. VIN_i and VIN_j are the vehicle identity numbers of the request sender and the target vehicle, respectively. After receiving the query request, the RSU first checks the identity of the request sender. Then, based on the offsets stored in the blockchain, the RSU can accumulate all the offsets together and obtain the current trust value of vehicle j. Finally, the RSU sends response $(VIN_j, En(Tr_j)_{pk_i})$ to the requester. Tr_j is the trust value of the target vehicle, which is encrypted using the public key of the requester.

2) Warning and Revocation: For the vehicles whose trust values are relatively low, RSUs are able to take certain actions, e.g., warning and revocation. Two thresholds, i.e., R_{warn} and $R_{\min}$, are defined to punish these vehicles, where $R_{\text{warn}} > R_{\min}$. Vehicles with trust values lower than R_{warn} will be added into the warning list, which is broadcasted by RSUs. The warned vehicles need to sense the environments and broadcast credible messages actively, in order to improve their trust values in time. More seriously, vehicles with trust values lower than $R_{\min}$ will be added into the revocation list. Once being revoked, vehicles cannot receive any services from the vehicular network.

VI. Security Analysis

A. Defense Against Malicious Vehicle

1) Message Spoofing Attack: A malicious vehicle may broadcast fake messages to neighbors, which can cause severe traffic accidents or congestions. In the proposed system, a Bayesian inference-based rating generation scheme is used to thwart this attack. The message receiver can comprehensively analyze messages broadcasted by different reference vehicles about this event and decide which message is trustworthy. As the number of attackers is limited, vehicles are usually able to know the credibilities of received messages. Moreover, with the help of the API, vehicles can easily query the trust value of a specific neighbor, which is also an important factor for message credibility assessment.

2) Bad Mouthing and Ballot Stuffing Attack: Malicious vehicles may generate unfair ratings and upload them into the RSU. However, in the proposed system, messages are broadcasted to all neighbors and each receiver can only generate one binary rating for a specific event. Due to the limited number of attackers, the unfair ratings can hardly change the aggregated trust values of vehicles.

B. Defense Against Compromised RSU

In the proposed system, it is assumed that a small portion of RSUs may be compromised during a short time period. Data stored in the RSU may be added, deleted, or tampered by attackers. However, based on blockchain techniques, all RSUs store the same version of the blockchain and continuously add new blocks on the current chain. Once getting rid of the control from attackers, the compromised RSUs can easily detect their differences from others. This is because any changes to the locally stored data will inevitably change the hash value of the last block, which is different from the previous hash stored in the new coming block generated by benign RSUs.

Moreover, the compromised RSUs may also generate and broadcast fake blocks. However, they still need to compete with others for adding blocks into the blockchain. Due to the limited number of attackers and the short compromising time periods, the number of fake blocks generated by the compromised RSUs remains small. In addition, the upper bound of the stakes in each block [i.e., $F_{\max}$ in (6)] prevents attackers

TABLE I
KEY PARAMETERS

Parameters	Values
Vehicle number	50
Distance between vehicles	Uniform distribution between 5 and 100 meters
β	0.5
γ	0.014
Thr	0.5
Vehicle number in reference set	Uniform distribution between 0 and 10
Hash algarithm	SHA-256
η	0.01
μ	-3
Packet size	Message: 800 bytes; Rating block: 8000 bytes

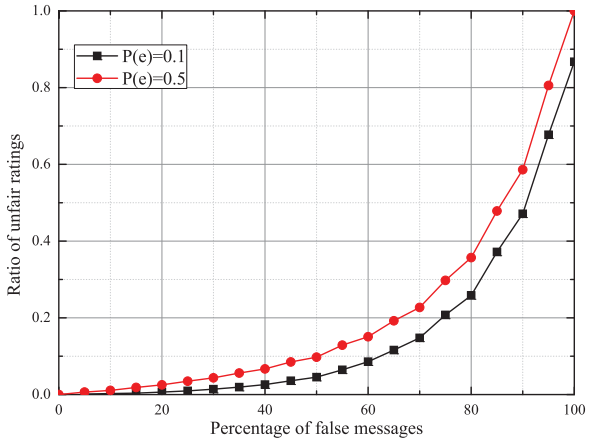


Fig. 6. Percentage of unfair ratings versus false messages.

from generating fake blocks with too large stakes, which can also reduce the impacts of compromised RSUs.

VII. PERFORMANCE EVALUATION

In order to validate the effectiveness and feasibility of the proposed system, performance evaluations are conducted using vehicular and blockchain simulation platform based on MATLAB. The configurations of key parameters are listed in Table I. This section is divided into three parts. The first part studies the calculation of ratings and trust value offsets. The generation time intervals of blocks with the variation of absolute offsets are provided in the second part. Finally, the third part analyzes the communication overheads of this system.

A. Calculation of Trust Value Offsets

This part mainly shows the procedures from messages to ratings, and from ratings to trust value offsets. Fig. 6 plots the relationship between unfair ratings and false messages. In this test, attackers deliberately send fake messages to the receivers. Once being puzzled by the attackers, benign vehicles may generate unfair ratings on the received messages. It is evident that the percentage of unfair ratings is very low when

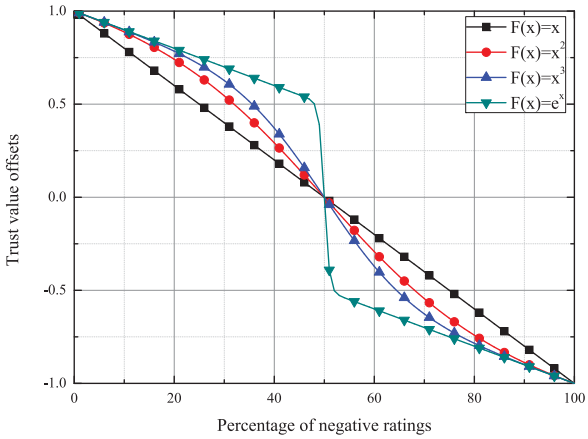


Fig. 7. Trust value offset versus percentage of negative ratings.

there are small numbers of false messages. This is because the Bayesian-based model is able to find the truth using the reports from the benign majority. However, the percentage of unfair ratings grows gradually with the increase of false messages and finally reaches a high value near 1. This is because the false messages gradually become the majority and severely mislead the model. In addition, the line with more prior knowledge about the event probability (i.e., $P(e) = 0.1$) outperforms the one with neutral prior probability (i.e., $P(e) = 0.5$), due to the effect of prior knowledge on decision making.

The relationship between trust value offsets and the percentage of negative ratings is shown in Fig. 7. Four functions are tested for the calculation of the offsets based on (3) and (4). The offsets decrease gradually with the increase of negative ratings, whose lower and upper bounds are -1 and $+1$, respectively. In addition, different $F(x)$ may have different effects on offsets. For example, the blue line is above the black line when the negative ratings are less than 50%, which means that the offset with $F(x) = x^3$ is less vulnerable to unfair ratings when a small proportion of negative ratings generated by the attackers are included in the rating set.

B. Block Generation

After obtaining the trust value offsets of vehicles, RSUs try to become the miner and publish their blocks. The block generation time T of each RSU is mainly influenced by two parameters, i.e., the sum of absolute offsets F_i and the hash rate M. As shown in Fig. 8, T drops gradually with the increase of F_i. This is because a larger F_i indicates a larger hash threshold S_i, which makes it easier to get the right nonce. Moreover, T also drops with the increase of M. M represents the number of hash operations that an RSU is able to conduct per second, which is related to the computation capacity of this RSU. A larger M enables RSUs to try more nonces within specific time period, and thus obtain the right nonce faster.

In comparison, the block generation time based on the PoW scheme is also evaluated. In this scheme, all nodes have the same hash threshold and the block generation time only depends on the hash rate of each node. However, as RSUs

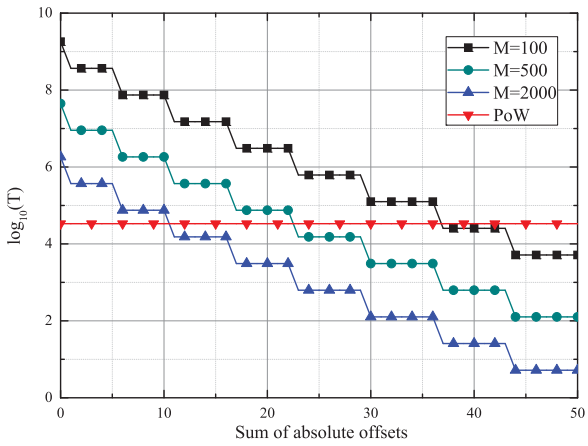


Fig. 8. Generation time of offset blocks.

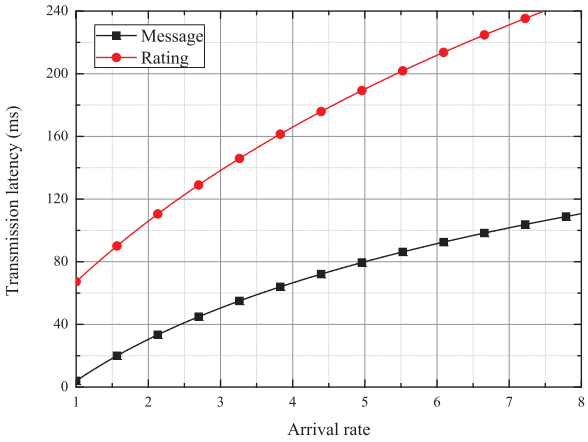


Fig. 9. Transmission latency of messages and ratings.

usually have similar hash rate, the opportunities of block generation among all RSUs are relatively equal. Therefore, in this evaluation, it is assumed that $N_z = 24$ and $M = 500$ for all RSUs. From Fig. 8, it can be clearly seen that the block generation time of PoW does not change with the stake, i.e., the F_i. Compared with the PoW, the proposed scheme is able to reflect the differences between high stake RSUs and low stake RSUs, and thus faster to update the trust values with larger variations.

C. Communications Overhead

Two kinds of data are transmitted using the wireless channels in vehicular networks, i.e., messages and ratings. Messages are triggered by certain road-related events and broadcasted by vehicles. The packet size of message is set to be 800 bytes, which corresponds with the event-triggered data defined in [23]. Ratings are nonsafety data which are generated by message receivers. A vehicle can accumulate several ratings within a certain time period, pack them together into a data packet, and upload them to the nearby RSU. Therefore, the size of rating packet is usually larger than that of message. As shown in Fig. 9, it is evident that with the increase of data arrival rate, the transmission latency of both messages and ratings are increased. Moreover, the latency of rating packet is larger than that of the message, due to the larger packet size.

VIII. Discussion

A. Trust-Based Data Credibility Assessment

In the proposed system, the Bayesian Inference is utilized to generate message ratings. During the rating generation, the distance between message sender and event location is considered as the indicator of message credibility. Apart from this factor, the current trust value of the message sender is also very important for the assessment of message credibility. Through querying the trust values from the RSU, the message receiver is able to aggregate this information with the distance factor and obtain a more reliable result, as illustrated in the following equation:

$$c_k^j = \alpha_1 \cdot e^{-\gamma \cdot d_k^j} + \alpha_2 \cdot \left(\frac{R_k}{\max_{m \in \mathrm{Ref}}(R_m)} \right) \tag{8}$$

where R_k is the trust value of the message sender; Ref is the reference set of the receiver; and α_1 and α_2 are two parameters to control the weight of each part.

B. Privacy Issues

Privacy is usually regarded as one of the most significant issues in vehicular networks [25]. In the proposed system, the vehicle identity number is used as the identifier of each vehicle, which has the potential of privacy leak. For example, using the vehicle identity number, attackers may find out the real identity of the vehicle owner. A possible solution for this problem is using the public key as the identifier of each vehicle, which is just a meaningless string. Furthermore, vehicles can periodically change the public keys through interacting with the RSUs. However, these tasks inevitably increase the communication and computation overheads of the network. Therefore, how to jointly assure the privacy preservation and efficient trust management is still an interesting but challenging problem in vehicular networks.

IX. Conclusion

In this paper, we proposed a blockchain-based decentralized trust management system in vehicular networks. With the aid of this system, vehicles are able to query the trust values of neighbors and then assess the credibilities of received messages. Trust values are aggregated in the RSU based on ratings generated by messages receivers. Using blockchain techniques, all RSUs work together to maintain a reliable and consistent database. A number of simulations are carried out in order to evaluate the performance of the entire system. Simulation results demonstrate that the proposed system is effective and feasible for decentralized trust management. Further studies are still needed in the future. For example, how to jointly assure the trust management and privacy preservation is an open problem which needs to be studied in detail. It is believed that a reliable decentralized trust management system can

greatly help vehicles evaluate the credibilities of neighbors and establish a safe and efficient intelligent transportation network.

REFERENCES

[1] H. Zhou *et al.*, "ChainCluster: Engineering a cooperative content distribution framework for highway vehicular communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 6, pp. 2644–2657, Dec. 2014.

[2] S. He, D.-H. Shin, J. Zhang, J. Chen, and Y. Sun, "Full-view area coverage in camera sensor networks: Dimension reduction and near-optimal solutions," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7448–7461, Sep. 2016.

[3] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[4] A. Wasef, R. Lu, X. Lin, and X. Shen, "Complementing public key infrastructure to secure vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 22–28, Oct. 2010.

[5] K. Zheng, F. Liu, L. Lei, C. Lin, and Y. Jiang, "Stochastic performance analysis of a wireless finite-state Markov channel," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 782–793, Feb. 2013.

[6] K. Zhang *et al.*, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[7] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 4095–4108, Nov. 2012.

[8] T. Roosta, M. Meingast, and S. Sastry, "Distributed reputation system for tracking applications in sensor networks," in *Proc. 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.*, San Jose, CA, USA, Jul. 2006, pp. 1–8.

[9] S. Li and X. Wang, "Quickest attack detection in multi-agent reputation systems," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 4, pp. 653–666, Aug. 2014.

[10] M. E. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3947–3962, Oct. 2011.

[11] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.

[12] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 1238–1246.

[13] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *Proc. Int. Conf. Netw. Syst. Security*, Madrid, Spain, Jun. 2013, pp. 94–108.

[14] Z. Li and C. T. Chigan, "On joint privacy and reputation assurance for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 10, pp. 2334–2344, Oct. 2014.

[15] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.

[16] J. Oluoch, "A distributed reputation scheme for situation awareness in vehicular ad hoc networks (VANETs)," in *Proc. IEEE CogSIMA*, San Diego, CA, USA, Mar. 2016, pp. 63–67.

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

[18] A. Lei *et al.*, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[19] C. Cai, X. Yuan, and C. Wang, "Towards trustworthy and private keyword search in encrypted decentralized storage," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–7.

[20] C. Cai, X. Yuan, and C. Wang, "Hardening distributed and encrypted keyword search via blockchain," in *Proc. IEEE Symp. Privacy Aware Comput. (PAC)*, Washington, DC, USA, Aug. 2017, pp. 119–128.

[21] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[22] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[23] "Study on LTE-based V2X services, V1.0.0," TSG RAN, 3GPP, Sophia Antipolis, France, Rep. TR 36.885, 2016.

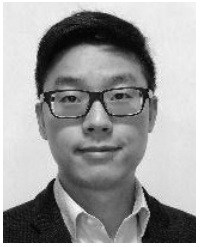
[24] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, "A blockchain-based reputation system for data credibility assessment in vehicular networks," in *Proc. IEEE Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[25] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, 1st Quart., 2015.

[26] N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, Sep. 2017.

Zhe Yang received the B.S. degree from Shandong University, Jinan, China, in 2014. He is currently pursuing the Ph.D. degree at the Intelligent Computing and Communication Laboratory, Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing, China.

His current research interests include data mining and security issues in heterogeneous wireless networks, cloud computing, and Internet of Things.



Kan Yang (M'14) received the B.Eng. degree in information security from the University of Science and Technology of China, Hefei, China, in 2008, and the Ph.D. degree in computer science from the City University of Hong Kong, Hong Kong, China, in 2013.

He is currently a tenure-track Assistant Professor with the Department of Computer Science, University of Memphis, Memphis, TN, USA. His current research interests include security and privacy issues in cloud computing, big data, crowdsourcing, Internet of Things, applied cryptography, wireless communication and networks, and distributed systems.

Lei Lei (M'13–SM'16) received the B.S. and Ph.D. degrees in telecommunications engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 2001 and 2006, respectively.

She is currently with the School of Science and Engineering, James Cook University, Cairns, QLD, Australia. Her current research interests include Internet of Things and mobile cloud computing.

Kan Zheng (S'02–M'06–SM'09) received the B.S., M.S., and Ph.D. degrees from the Beijing University of Posts and Telecommunications, Beijing, China, in 1996, 2000, and 2005, respectively.

He is currently a Professor with the Beijing University of Posts and Telecommunications. He has rich experiences on the research and standardization of the new emerging technologies. He has authored over 200 journal and conference papers in the fields of wireless networks, Internet of Things, vehicular communication, etc.

Dr. Zheng holds Editorial Board positions for several journals and has organized several special issues in IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, *IEEE Communication Magazine*, and the IEEE SYSTEM JOURNAL.

Victor C. M. Leung (S'75–M'89–SM'97–F'03) received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 1977, and the Ph.D. degree in electrical engineering from the Graduate School, UBC, in 1982.

From 1981 to 1987, he was a Technical Staff Senior Member and a Satellite System Specialist with MPR Teltech Ltd., Burnaby, BC, Canada. In 1988, he was a Lecturer with the Department of Electronics, Chinese University of Hong Kong, Hong Kong. He returned to UBC, as a faculty member, in 1989, and currently holds the positions of Professor and TELUS Mobility Research Chair of Advanced Telecommunications Engineering with the Department of Electrical and Computer Engineering. He has co-authored over 1100 journal/conference papers, 40 book chapters, and co-edited 14 book titles. His current research interests include wireless networks and mobile systems.

Dr. Leung was a recipient of the APEBC Gold Medal as the Head of the Graduating Class of the Faculty of Applied Science, the IEEE Vancouver Section Centennial Award, the 2011 UBC Killam Research Prize, the 2017 Canadian Award for Telecommunications Research, the 2017 IEEE ComSoc Fred W. Ellersick Prize, the 2017 IEEE SYSTEMS JOURNAL Best Paper Award, and the Canadian Natural Sciences and Engineering Research Council Postgraduate Scholarship, and was nominated for Best Paper Awards. He was a Distinguished Lecturer of the IEEE Communications Society. He is serving on the Editorial Board of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, the IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE ACCESS, *Computer Communications*, and several other journals, and has previously served on the Editorial Board of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS—Wireless Communications Series and Series on Green Communications and Networking, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON COMPUTERS, IEEE WIRELESS COMMUNICATIONS LETTERS, and the *Journal of Communications and Networks*. He has guest edited several journal special issues and provided leadership to the Organizing Committees and Technical Program Committees of numerous conferences and workshops. He is a registered Professional Engineer in the Province of British Columbia, Canada. He is a Fellow of the Royal Society of Canada, the Engineering Institute of Canada, and the Canadian Academy of Engineering.