A Trust-Based and Secure Real-Time Traffic Information Sharing Scheme

Yuhao Wang(✉) and Chengzhe Lai

National Engineering Laboratory for Wireless Security, Xian University of Posts and Telecommunications, Xian, China
13720736623@163.com

Abstract. Real-time Traffic information sharing can make the transportation more effective, which requires the vehicles on the road to participate in the road condition report actively. However, in the untrustworthy network environment, malicious traffic information dissemination will result in severe traffic issues, meanwhile, the risk of disclosure of users' privacy information may also be increased. To address these problems, we propose a trust-based and secure real-time traffic information sharing scheme. Particularly, the trust value of the vehicle is calculated by the trusted organization, and the system updates the real road conditions according to the calculated results. Moreover, we utilize the improved pairing-free certificateless aggregate signature technique to provide the security service. As shown in the simulation results, the computing cost can be reduced because of using aggregate signature technique. In addition, the reliability of data is improved through trust management of vehicle users, and the sybil attack can be alleviated.

Keywords: Internet of vehicle · Real-time traffic information sharing · Trust · Anonymity

1 Introduction

According to the statistics, licensed vehicles exceed 1 billion around the world, a number that will double in the next 10 to 20 years. The explosive growth of car ownership has caused many serious social problems, such as road safety, traffic congestion and air pollution [3]. In order to make the vehicle driving environment safe and efficient, vehicles can upload the ultramodern traffic information with the various kinds of communication devices and vehicle-mounted transducer [9,16]. At present, the traffic information sharing schemes based on GPS (Global Positioning System) positioning have been widely studied and applied [4], but they can not reflect the accurate traffic information. In these schemes, the reporting vehicle voluntarily uploads its GPS information to a trusted agency, but these schemes lack privacy and data security protection as well as information authenticity judgment. For these reasons, the development of traffic information

W. Bao et al. (Eds.): ADHOCNETS 2021/TridentCom 2021, LNICST 428, pp. 217–228, 2022.
https://doi.org/10.1007/978-3-030-98005-4_16

sharing system has been seriously affected. When the reporting vehicle reports the traffic information, its reporting information is no longer controlled by itself, but calculated and processed by RSU (Roadside Units) and TA (Trusted Agencies). Therefore, how to ensure the integrity of the reported traffic information and the confidentiality of the reported vehicle has become a new challenge for traffic information sharing [10]. In the meantime, due to the lack of verification measures, the exactitude of the traffic information sharing will be reduced when the malicious vehicles distribute the incorrect road condition information deliberately in the system, thus affecting the efficiency and safety of vehicles on the road. Therefore, academic boffins have been aware of the assurance of the security in IoV (Internet-of-Vehicles). In the ordinary way, cryptography-based solutions [15] and trust-based solutions [5] are the two ways to address the security issues in the IoV.

To solve the above problems, this paper introduces the ideas of certificateless aggregate signature and trust management into the traffic information sharing. The general process of the system can be described as follows. RSU send the massage to the nearby verifying vehicles when the RSU receive the road information from the reporting vehicle, and then verifying vehicles will give their feedbacks. After RSU verifying the legitimacy of the vehicles, it will send all vehicles' massages to the TA (Trusted Institutions) by aggregation signatures. After that, to prevent the spread of malicious messages, TA calculates trust value from vehicles by using trust management. During the whole process, the privacy of the user's vehicle will not be disclosed to any party. Underneath, we have summed up the main contributions in this paper:

- An effective trust evaluation scheme is designed. Vehicles can share the traffic information independently in the scheme, which can avert the malicious vehicles diffusing the incorrect information to the scheme.
- To ensure that only legitimate vehicles are certified, a certificateless encryption and aggregate signature technique [6] is equipped, which can also protect the privacy of the user's vehicle.
- By using aggregate signature technique, the computing cost is reduced. In addition, the reliability of data is improved through credit management of vehicle users, and the sybil attack can be alleviated.

2 Related Work

2.1 Trust Management

Currently, trust has become momentous in the IoV. Trust scheme foresee the uers' future behaviour by calculating the past-reputation. Trust management scheme plays an important role in the security and privacy of user information in the Internet of Vehicles. In the traffic information sharing system, the trust value describes the user's expectation also as known as trust level, and employs the user vehicle's historical interaction experience to reduce various threats and risks by trust management. The author proposes a true-filtering algorithm for

wireless sensor networks. The basic idea is that if the data of the user's vehicle is closer to the preset credit score, it will be assigned a higher weight, and the data provided by the user's vehicle with a higher weight will be more likely to be considered as the true feedback information [11]. In order to deal with the report of false news, Zhang, C. et al. [13] proposes an artificial intelligence trust management system for vehicle-mounted network based on blockchain technology. Malicious vehicles can occur in the scheme for a longtime because the system don't exist the punitive measure to the evil users. The fatal part in the traffic information sharing scheme is zapping the malicious vehicles [12]. A protocol for anonymously aggregating vehicle notifications in a base station controller is proposed. It uses identities-based group signature technology to achieve conditional privacy. If a malicious vehicle sends a false message, the trusted institution can track its identity in an anonymous announcement through the public address of the blockchain [7].

2.2 Certificateless Aggregate Signature

In 2003, Al-Riyami et al. proposed the Certificateless public key cryptography in the Asian Society of Secrets, and the cryptosystem was gradually studied and applied in the V2N system. A new, efficient, certificateless set signature based on elliptic curve cryptosystem is proposed, and its ability to support conditional privacy protection is proved [2]. In order to deal with the problem that encrypted data is difficult to search after encryption, Du, H. et al. [1] proposes a scheme to grant the cloud server the right to perform equality tests on encrypted data. This scheme can retrieve the results without the cloud server knowing any relevant information of the ciphertext [8]. A lightweight certificateless and pairing-free scheme is proposed, which is feasible without infrastructure. The scheme can resist attacks with a small computational cost. Some studies have proposed a privacy-protected certificateless set signature scheme based on hierarchical trust institutions for message authentication. The scheme does not require key escrow, and any entity within the scheme can verify the messages received by vehicles running under different trust institutions. In this paper, we utilize the improved pairing-free certificateless aggregate signature technique [6] to provide the security service in our scheme.

3 System Background

In this section, we describe the background of the system, including the system model and the adversary model.

3.1 System Model

The system model is mainly composed of three parts: vehicle, TA and RSU.

– Vehicles: These nodes are OBUs (On Board Unit) on the vehicle and have some storage capability. The vehicle can actively report the road condition information to the nearby RSU, and also put forward its own opinion on the road condition information sent by the RSU and report the opinion to the RSU. In this scheme, vehicles are divided into reporting vehicles and verification vehicles.

  Reporting vehicle: The reporting vehicle can report its road condition information to the RSU at any time and wait for the system to verify the correctness of the message through calculation.

  Verification vehicles: These vehicles receive traffic information from the RSU and choose whether or not to participate in the validation. When verifying the vehicle validation message, it sends its opinion, agree or disagree with the traffic information reported by the vehicle to the RSU and waits for the system to verify.

– TA (Trusted Authority): This entity is responsible for all participants and maintains a database to store the trust value of the user's vehicle. It has full resource storage and data computing capabilities. The trusted agency can calculate the credibility of each vehicle based on the data submitted by the RSU to determine whether the traffic information is true or not. Based on the results of the calculation, the traffic information is updated and the lying vehicle is punished.

– RSU (Roadside Units): The RSU, known as the roadside unit, is a subsidiary of the trusted authority TA. It has limited resources but higher computing power than the vehicle to ensure that the RSU can verify the legitimacy of the user's vehicle identity and perform the aggregation operation to send to the trusted authority TA.

3.2 Adversary Model

Both reporting vehicles and verifying vehicles will attempt to upload false traffic information to the system to interfere with the normal traffic environment. The main attack in this paper is message spoofing attack, in which the attacker covers up the real information of the road condition by reporting false information to the RSU. For example, a malicious vehicle may send a traffic jam to a nearby RSU when the road is clear for its own purposes.

4 Proposed Scheme

A road condition evaluation scheme based on privacy and trust management is proposed, which includes system overview, vehicle reporting and authentication stage, and information management and verification stage (Fig. 1).

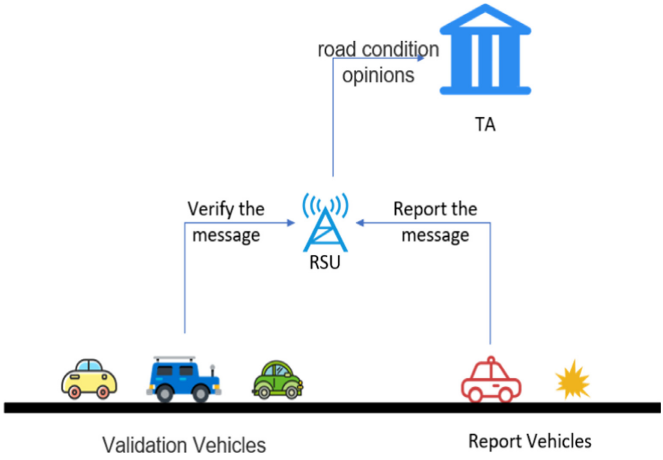

Fig. 1. System architecture

4.1 Overview

The vehicle reports the road condition information to the RSU, which is called the reporting vehicle. The RSU sends the road condition information to other nearby vehicles other than the reporting vehicle, and the other nearby vehicles are called verification vehicles. Verify that the vehicle submits its opinion to the RSU regarding the road condition information, agrees or disagrees. The RSU then verifies the legitimacy of the vehicle through a certificateless encryption scheme. When the verified vehicle passes the verification, the RSU submits the vehicle information and road condition opinions of the verified vehicle to the TA through the aggregate signature. TA calculates and verifies the authenticity of the road condition information submitted by the vehicle with the trust evaluation algorithm based on the historical data of the vehicle. Based on the verification results, TA records the report of the vehicle and verifies the new credit score of the vehicle and updates the latest traffic conditions on the traffic information sharing system according to the results of the trust evaluation algorithm (Table 1).

4.2 System Initialization

Vehicle outputs the following system parameters when it gets the security parameter $k \epsilon Z^+$. Select a group G of prime order q and a generator P of the group G. Compute vehicle's master public $P_{pub} = sP$ which s is master secret key by choosing $s \epsilon Z_q^*$. Pick hash functions $H : G \times G \rightarrow Z_q^*$,$H_1 : \{0,1\}^* \times G \times G \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$, and $H_2 : \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$ for $i = 3, 4$. Publish system parameters as $params = \{q, G, P, P_{pub}, H, H_1, H_2, H_3, H_4\}$ and keep master secret keys secure.

Table 1. Formalized notations involved in traffic information sharing scheme

Notation	Descriptions
k	Security parameter
q	Prime
G	Cyclic group of prime order q
params	System parameter
Z_q	Finite field
Z_q^*	$Z_q/0$
H_1, H_2, H_3, H_4	Cryptographic hash function
(P_{pub}, s)	Public and private key pair of TA
RID_i	Real identity of V
ID_i	Pseudo identity of V
D_i	Partial private key of V
(PK_i, SK_i)	Public and private key pair of V
ROT	Role-oriented trust
isT	Credit scores for individual vehicles
d	Distance score
ξ	Tier-boundary
Trust	Whether the message is trusted

4.3 Vehicle Registration and Verification Stage

With the input of params and s, the real identity of Vehicle RID_i, TA computes the following vehicles partial private key. Choosing $r_i \epsilon Z_q^*$ and computing $R_i = r_i P$. Compute the pseudoidentity $ID_i = RID_i \oplus H(r_i P_{pub}, T_i)$, which T_i is the validity period of the corresponding pseudo identity. Generate $h_{1i} = H_1(ID_i, R_i, P_{pub})$ and $d_i = r_i + sh_{1i} modq$. TA send the (ID_i, R_i, D_i) to the homologous vehicle and install $D_i = (d_i, R_i)$. Vehicle will compute the equation $d_i p = R_i + h_{1i} P_{pub}$. If the equation eligible, vehicle will accept the partial private key D_i for ID_i at T_i. Each vehicle performs the following to generate the public and private key pairs when they accept the $D_i = (d_i, R_i)$. Compute $X_i = x_i P$ where $x_i \epsilon Z_q^*$ as the secret key and set $PK_i = (X_i, R_i)$ sa public key and $SK_i = (x_i, d_i)$ as the secret key. When the public key and the secret key set done, vehicle will signature for a given massage $m_i \epsilon \{0,1\}^*$ with the ID_i,SK_i, params and current timestamp t_i. Choose $y_i \epsilon Z_q^*$ and compute $Y_i = y_{1i} P$. Let $u_i = H_2(m_i, ID_i, Y_{1i}) W_i = (u_i(y_i + h_{3i} x_i) + h_{4i} d_i) P$ where $h_{3i} = H_3(m_i, ID_i, PK_i, t_i)$, $h_{4i} = H_4(m_i, ID_i, PK_i, t_i)$. Output a signature $\sigma_i = (Y_{1i}, W_i)$ on the message $m_i \| t_i$. When the RSU get the given massage from the vehicle, RSU computes $h_{3i} = H_3(m_i, ID_i, PK_i, t_i)$, $h_{4i} = H_4(m_i, ID_i, PK_i, t_i)$ and $u_i = H_2(m_i, ID_i, Y_i)$ to accept the signature when the $W_i - u_i(Y_i + h_{3i} X_i) = h_{4i}(R_i + h_{1i} P_{Pub})$ holds. Plus, RSU will generate aggregate signatures σ which collected by n distinct signatures $(\sigma_i)_i = 1, ..., n$

on different messages $(m_i \| t_i)_{i=1,...,n}$ from different vehicles with corresponding identities $(ID_i)_i = 1, ..., n$. $\sigma = (Y, W)$, where $W = \sum_{i=1}^{n} W_i$,$Y = \sum_{i=1}^{n} u_i Y_{1i}$, $u_i = H_2(m_i, ID_i, Y_{1i})$. RSU send $\sigma = (Y, W)$ to the TA. TA check whether the $W - Y - U = \sum_{i=1}^{n} h_{4i}(R_i + h_{1i} P_{Pub})$ holds, where $h_{1i} = H_1(ID_i, R_i, P_{Pub})$. $h_{3i} = H_3(m_i, ID_i, PK_i, t_i)$, $h_{4i} = H_4(m_i, ID_i, PK_i, t_i)$, $U = \sum_{i=1}^{n} u_i h_{3i} X_i$. If it holds, accepts the aggregated signature σ, else rejects.

4.4 Trust Management

After the Verification vehicle entity is evaluated, the next step is evaluate the data sent by the verification vehicle. The trust score is defined as follows:

$$isT = f(d, ROT) \tag{1}$$

The formula describes the two parameters of isT. Since the occurrence of traffic accidents is highly deterministic, the trust function must consider the trust value of the verified vehicle and the accurate geographical location, that is, the trust value of the vehicle Vtrust is represented by ROT and effective distance of the vehicle is represented by d. Further, the formula can be described as:

$$isT = -\sum_{n=1}^{n} e^{-ROT \cdot d} \tag{2}$$

Firstly, TA compute the trust value ROT. When a vehicle is first registered with TA, TA will assign an initial value to the vehicle. Every vehicle is considered as the part of the trust network, which includes official vehicles, public vehicles and private cars. Our trust management scheme integrates all the vehicles on the road and the initial trust value may vary depending on their identity. This article uses the following method to assign the initial trust value

$$ROT = \begin{cases} 0.8{-}1 \;\; if\ veh \;=\; Authority\ Vehicles \\ 0.6{-}0.8 \;\; if\ veh \;= Public\ Transport\ Vehicles \\ 0.4{-}0.6 \;\; if\ veh \;=\; Traditional\ Vehicles \end{cases} \tag{3}$$

We divide the cars as three types on account of the relationship with the authorities.

Authority Vehicles: Such vehicles include police cars, ambulances, etc., which are authorized by central authorities, so they are highly credible.

Public Transport Vehicles: Such vehicles include buses as well as taxis operated by government companies, which are considered to be moderately reliable because they are authorized by specific government departments.

Traditional Vehicles: These vehicles are social vehicles with no relationship with the authorities like Uber service cars or other private cars. Such vehicles have no connection with the authorities so these vehicles must remain honest in the network so that their information can make an impact in the network.

$$ROT^{l+1} = \eta \times ROT^{l} + (1 - \eta) \times ROT^{l-1} \tag{4}$$

We adopt the improved (EMWA: Exponential weight moving average) technique to calculate the future credit value of the vehicle. Where ROT^{l+1}, ROT^{l} and ROT^{l-1} respectively represent the vehicle's future, current and historical credit values. And we also defines the influence factor η to influence the influence of the credit value in different historical time on the future credit value. A higher weight is given to the first two vehicle (Authority Vehicles, Public Transport Vehicles)

$$\begin{cases} 0.7 \leq \eta < 1.0 & if\ veh\ = V_{av}, V_{ptv} \\ 0.5 \leq \eta < 0.7 & if\ veh\ = V_{tv} \end{cases} \tag{5}$$

Note that some user vehicles may increase their trust value by performing well at first, but intentionally underperform when the trust value is high enough. For this reason, we further designed a trust circuit breaker mechanism, as shown below:

$$ROT^{l+1} = \begin{cases} ROT^{l+1} & if\ ROT^{l+1} > ROT^{threshold} \\ 0 & if\ ROT^{l+1} < ROT^{threshold} \end{cases} \tag{6}$$

Through the formula, we can calculate whether the future credit value is greater than the predetermined value of the system. Through calculation, we conclude that the predetermined value needs to be satisfied at least $ROT^{threshold} \geq 0.2$ otherwise the newly registered traditional vehicle will not be able to update their scores. Further, when $ROT^{l+1} = 0$, the circuit breaker mechanism is triggered, the predicted trust value will be reduced to $ROT^{l+1} = \alpha \cdot ROT^{l}$, where $\alpha\, \epsilon\, (0, 1)$, called the penalty factor. This will allow the attacker to spend more time to improve their reputation to the previous level.

After that, TA calculates the distance between the verification vehicle and reporting vehicle,

$$dis = \sqrt{\left(m_{Sender_x} - m_{in_x}\right)^2 + \left(m_{Sender_y} - m_{in_y}\right)^2} \tag{7}$$

where m_{Sender_x}, m_{Sender_y} represents the coordinates x and y of the reporting vehicle. m_{in_x}, m_{in_y} represents the coordinate x and y of the i-th verification vehicle. In addition, the distance coefficient ξ is defined. As shown in the Fig. 2, the location of the reporting vehicle v_i is divided into three geographical areas, including high confidence area, medium confidence area and low confidence area. In practical application, the shape of this area may change with the actual situation of the road. For the sake of loss of generality, we assume that all three layers are circular,

$$d = \begin{cases} 1 & 0 < dis \leq \xi_1 \\ 0.6 & \xi_1 < dis \leq \xi_2 \\ 0.3 & \xi_2 < dis \leq \xi_3 \end{cases} \tag{8}$$

Once each parameter (d, ROT) has been calculated, TA divides the vehicle into two groups based on the message $m_i = (1 or 0)$ upload by the validation vehicle $(V_1, V_2, V_3, ..., V_n)$ and calculates the isT of each group, where $isT_1 = -\sum_{n=1}^{n} e^{-ROT \cdot d}$ represents the message as $m_i = 1$, $isT_2 = -\sum_{n=1}^{n} e^{-ROT \cdot d}$ represents the message as $m_i = 0$. Plus, TA compute the Trust $= |isT_1| - |isT_2|$, if Trust > 0, $m_i = 1$ is taken as the opinion of the verified vehicle, else, $m_i = 0$

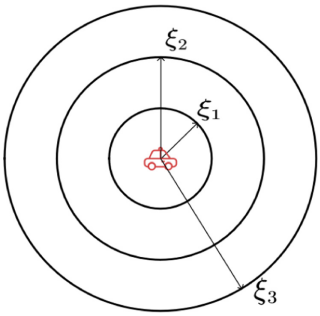

Fig. 2. Threshold approach

is taken as the opinion of the verified vehicle. After TA calculates the truth of the road condition information, TA will increase or decrease the reputation score of the vehicles in the corresponding verification vehicle group and the reporting vehicle according to the result, and carry out the traffic information sharing system update.

5 Scheme Analysis

According to the security objectives of the previous adversary model, the following analysis as follows

5.1 Trust Management

Unregistered vehicles can be effectively excluded from the system through the system initialization phase. When receiving road condition information, TA can score the different opinions on the same traffic accident through the trust management scheme, so as to select the true opinions representing the group. In the calculation of trust value, vehicles with better historical performance and closer to the accident site are given higher weight, so as to ensure that the traffic information provided is true and reliable, and resist the reporting of false news of malicious vehicles.

5.2 Resistance to Sybil Attacks

Because of Sybil attack, the reliability of traffic information and the operation of evaluation mechanism will be greatly damaged [14]. In this scheme, a penalty factor is introduced to make the trust value of the vehicle drop rapidly after the malicious behavior. And since the credit score is related to the historical credit score, it takes more effort for the vehicle to restore its trust score to a higher level after committing a malicious act. Figure 4 shows the status of a vehicle's reputation when it spreads malicious messages. Apparently, the more malicious vehicles spread the false traffic information, the more trust value be deduct.

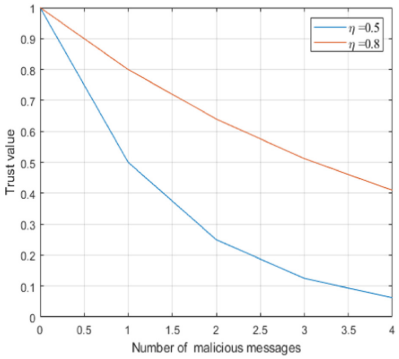

Fig. 3. Trust value changing of malicious messages

5.3 Performance Evaluation

We use a personal computer conduct a test which we put forward in this paper. The computer's core is Intel I5-9300H. RAM is 16.00 GB. The operation system is 64-b windows 10. We accomplish the cryptosystem with Java and the compiler is IDEA. As one shall see from Fig. 3, the time cost of aggregate signature and aggregate signature verification steps increases with the increase of the vehicle number. The total time cost of our scheme is extremely fast. At the same time, compared with single signature verification, aggregate signature verification has the advantages of low computational overhead, so it is more suitable for resource-constrained network environments such as the Internet of vehicles.

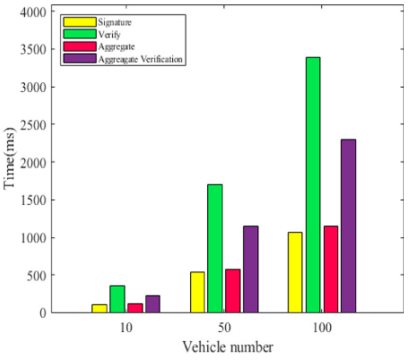

Fig. 4. Total time cost

6 Conclusion

Aiming at the problem of traffic information sharing, this paper proposes a trust-based and secure real-time traffic information sharing scheme. In this paper, the certificateless aggregate signature technique is used to achieve the integrity, identity verifiability and non-repudiation of data. The trust management system is introduced to improve the reliability of data. Using aggregate signature technology, the computing cost is reduced. In order to protect the privacy of users, this paper realizes the anonymity of users by generating pseudonyms for users. Finally, through the simulation, the incentive of the scheme is verified, and the effectiveness of the proposed scheme is proved from the aspect of computational cost.

References

1. Du, H., Wen, Q., Zhang, S.: An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network. IEEE Access **7**, 42683–42693 (2019). https://doi.org/10.1109/ACCESS.2019.2907298
2. Elhabob, R., Zhao, Y., Sella, I., Xiong, H.: Efficient certificateless public key cryptography with equality test for internet of vehicles. IEEE Access **7**, 68957–68969 (2019). https://doi.org/10.1109/ACCESS.2019.2917326
3. Elleuch, W., Wali, A., Alimi, A.M.: Mining road map from big database of GPS data. In: 2014 14th International Conference on Hybrid Intelligent Systems, pp. 193–198 (2014). https://doi.org/10.1109/HIS.2014.7086197
4. Jia, D., Lu, K., Wang, J., Zhang, X., Shen, X.: A survey on platoon-based vehicular cyber-physical systems. IEEE Commun. Surv. Tutor. **18**(1), 263–284 (2016). https://doi.org/10.1109/COMST.2015.2410831
5. Kerrache, C.A., Calafate, C.T., Cano, J.C., Lagraa, N., Manzoni, P.: Trust management for vehicular networks: an adversary-oriented overview. IEEE Access **4**, 9293–9307 (2016). https://doi.org/10.1109/ACCESS.2016.2645452
6. Liu, J., Wang, L., Yu, Y.: Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks. IEEE IoT J. **7**(6), 5256–5266 (2020). https://doi.org/10.1109/JIOT.2020.2979613
7. Liu, X., Huang, H., Xiao, F., Ma, Z.: A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. IEEE IoT J. **7**(5), 4101–4112 (2020). https://doi.org/10.1109/JIOT.2019.2957421
8. Song, J., He, C., Zhang, L., Tang, S., Zhang, H.: Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs. China Commun. **11**(9), 93–103 (2014). https://doi.org/10.1109/CC.2014.6969774
9. Sou, S.I., Lee, Y.: SCB: store-carry-broadcast scheme for message dissemination in sparse VANET. In: 2012 IEEE 75th Vehicular Technology Conference (VTC Spring), pp. 1–5 (2012). https://doi.org/10.1109/VETECS.2012.6240177
10. Wang, X., et al.: Privacy-preserving content dissemination for vehicular social networks: challenges and solutions. IEEE Commun. Surv. Tutor. **21**(2), 1314–1345 (2019). https://doi.org/10.1109/COMST.2018.2882064
11. Willink, T.: Possibility-based trust for mobile wireless networks. IEEE Trans. Mob. Comput. **19**, 1896–1909 (2019)

12. Zhang, C., Li, W., Luo, Y., Hu, Y.: AIT: an AI-enabled trust management system for vehicular networks using blockchain technology. IEEE IoT J. **8**(5), 3157–3169 (2021). https://doi.org/10.1109/JIOT.2020.3044296
13. Zhang, C., et al.: TPPR: a trust-based and privacy-preserving platoon recommendation scheme in VANET. IEEE Trans. Serv. Comput. (2019). https://doi.org/10.1109/TSC.2019.2961992
14. Zhang, K., Liang, X., Lu, R., Shen, X.: Sybil attacks and their defenses in the internet of things. IEEE IoT J. **1**(5), 372–383 (2014). https://doi.org/10.1109/JIOT.2014.2344013
15. Zhong, H., Huang, B., Cui, J., Xu, Y., Liu, L.: Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks. IEEE Access **6**, 2241–2250 (2018). https://doi.org/10.1109/ACCESS.2017.2782672
16. Zhou, H., et al.: Chaincluster: engineering a cooperative content distribution framework for highway vehicular communications. IEEE Trans. Intell. Transp. Syst. **15**(6), 2644–2657 (2014). https://doi.org/10.1109/TITS.2014.2321293