RSMA: Reputation System-Based Lightweight Message Authentication Framework and Protocol for 5G-Enabled Vehicular Networks

Jie Cui, Xiaoyu Zhang, Hong Zhong, Zuobin Ying, and Lu Liu

***Abstract*—Traditional public key infrastructure-based authentication schemes provide vehicular networks with identity authentication and conditional privacy protection, which are not sufficient for assessing the credibility of messages. Additionally, although the new generation of cellular networks (5G) can dramatically improve the transmission efficiency of the messages, many existing authentication schemes are based on complex bilinear pairing operations, and the calculation time is too long to be suitable for delay-sensitive 5G-enabled vehicular networks. To address these issues, we propose a reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks. The trusted authority (TA) is in charge of reputation management. A vehicle with a reputation score below the given threshold cannot obtain a credit reference from the TA for participating in the communication; therefore, the number of untrusted messages in vehicular networks is reduced from the source. Security analysis shows that our scheme is secure against an adaptively chosen-message attack, and also satisfies a series of requirements of vehicular networks. The scheme is based on the elliptic curve cryptosystem and supports batch authentication; therefore, it shows better performance in terms of time consumption when compared with related schemes.**

***Index Terms*—Authentication, elliptic curve, reputation system, vehicular networks.**

I. Introduction

PRESENTLY, governments in various nations are racing to invest in the development and application of 5G [2], [17], [34]. As a new technology, 5G is characterized by high speed, low delay, wide coverage, and support for device-to-device communications. This technology creates a huge opportunity for the mobile ad-hoc network, especially in vehicular networks [6], [10]. The so-called vehicular networks are a type of distributed self-organizing network in which many different types of vehicles communicate with neighboring vehicles using an installed on-board unit (OBU), in a wireless network environment. Through information sharing between vehicles, two main types of applications can be realized: 1) safety-related applications and 2) infotainment applications [13]. The former mainly indicates that drivers can give an early response, using the instant information obtained from other vehicles for avoiding traffic congestion, improving traffic efficiency, and reducing traffic accidents. The latter aims to enhance people's driving experience and enjoyment during travel; it includes peer-to-peer gaming, video streaming downloads, Internet content sharing, etc.

Despite such numerous advantages of launching vehicular networks, there are some difficulties and challenges need to be solved [7], [45], [47]. Messages are transmitted in an open wireless environment; therefore, a strong security protection system must be provided. An adversary could intercept, modify, and replay the transmitted messages by controlling communication channels, the normal communication under the vehicular networks could be destroyed. Meanwhile, users' requirements for fast authentication and privacy protection must be guaranteed [45]. In general, the implementation scheme of the vehicular networks should be able to ensure the privacy, integrity, and credibility of messages while achieving rapid and efficient authentication, as well as resisting ordinary security attacks.

A number of authentication schemes have been proposed. Unfortunately, owing to the inherently expensive overhead of bilinear pairing operations and MapToPoint functions, these schemes cannot efficiently handle the authentication process [9]. Additionally, some of them require roadside units (RSUs) to participate in the authentication process [44]. However, RSUs are expensive and vulnerable to physical attacks in the open areas. More importantly, traditional public key infrastructure (PKI) can only build defense for identity authentication, but it cannot distinguish untrusted vehicles from all the authorized vehicles; consequently, the credibility of the message can hardly be guaranteed [6]. In fact, once the content of a message is not credible, efforts for both identity authentication and data integrity verification may be in vain [42].

In this paper, besides using elliptic curve encryption algorithm to achieve secure message authentication with lower

Manuscript received August 11, 2018; revised November 17, 2018 and December 28, 2018; accepted January 20, 2019. Date of publication January 24, 2019; date of current version July 31, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61872001, Grant 61572001, and Grant 61702005, in part by the Key Program of National Natural Science Foundation of China under Grant U1405255, in part by the Open Fund of Key Laboratory of Embedded System and Service Computing (Tongji University), Ministry of Education under Grant ESSCKF2018-03, and in part by the Open Fund for Discipline Construction, Institute of Physical Science and Information Technology, Anhui University, and the Excellent Talent Project of Anhui University. *(Corresponding author: Hong Zhong.)*

J. Cui, X. Zhang, H. Zhong, and Z. Ying are with the School of Computer Science and Technology, Anhui University, Hefei 230039, China, with the Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China, and also with the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China (e-mail: zhongh@ahu.edu.cn).

L. Liu is with the School of Electronics, Computing, and Mathematics, University of Derby, Derby DE22 1GB, U.K. (e-mail: l.liu@derby.ac.uk).

Digital Object Identifier 10.1109/JIOT.2019.2895136

computation overhead, we also propose a reputation system for reducing the number of untrusted messages. It is worth noting that reputation system has played an increasingly important role in vehicular networks. It has been applied to multiple scenarios in vehicular networks, such as stimulating resource collaborative downloading [20], recommending platoon head vehicles [15], optimizing resources assignment [27], and assessing data credibility [22]. Additionally, we set our novel sights into the 5G technology, as it can integrate multiple radio access technologies into the cellular system architecture. Reusing the available cellular network infrastructure will reduce the cost of deploying vehicular networks. This technology can also provide peak-data-rate up to 20 Gb/s, average data-rate greater than 100 Mb/s, in support of high data-rate services [30]. 5G's up to a 1000-fold increase in capacity makes it possible for more efficient vehicle-to-vehicle (V2V) communications [40], and reliable connections as well as low latency (around 1 ms) also provide enough support for the transmission of messages [41]. More importantly, although 5G can dramatically improve the transmission efficiency of messages, many existing authentication schemes are based on complex bilinear-pairing operations, making the calculation time too large to be suitable for delay-sensitive 5G-enabled vehicular networks. Therefore, in this paper, we focus on innovating a novel and practical 5G-enabled vehicular network framework, and propose the reputation system-based lightweight message authentication (RSMA) framework and protocol using the elliptic curve cryptosystem (ECC).

A. Our Contributions

To the best of our knowledge, this is the first authentication protocol based on the reputation system for 5G-enabled vehicular communications. Specifically, three main contributions of this paper are given as follows.

1) First, a reputation system is proposed for reducing the number of untrusted messages from the source in 5G-enabled vehicular networks. A vehicle with a reputation score below the threshold is unable to participate in the communication because it cannot obtain the credit reference from the TA.
2) Second, a lightweight message authentication framework and protocol is designed for 5G-enabled vehicular networks. The framework does not require RSU participates in the authentication process, as it will increase the computational latency and system security risks. The 5G base-station (5G-BS) in our scheme is only responsible for assisting transmission of messages.
3) Finally, a security proof is conducted and detailed security analysis shows that our scheme could achieve security objectives in vehicular networks. Our scheme adopts elliptic curve cryptography and supports batch verification, therefore, compared with related schemes it shows better performance in time consumption.

B. Organization of This Paper

Section II provides an overview of related work. Section III gives background information and preliminary knowledge related to this paper. Section IV briefly describes our protocol. In Sections V and VI, the specific security analysis and time consumption analysis are presented. Then, in Section VII, preliminary evaluation is given. Finally, We provide some concluding remarks in Section VIII.

II. Related Work

To achieve secured communication in vehicular networks, some authentication schemes have been proposed. Anonymous certificates are used by Raya and Hubaux [31] for the integrity check and authentication of messages. However, the PKI-based scheme has a serious problem of certificate management [13]. For this reason, some researchers proposed an identity-based (ID-based) public key encryption scheme. Through generating private keys for pseudonyms, certificates are no longer needed in Zhang *et al.*'s scheme [45], consequently, the overhead of transmission is significantly reduced. However, the scheme is easily affected by the modification attacks [21], [25]. Later, Lu *et al.* [26] used the dynamic short-term anonymous key issued by the RSUs to prevent the vehicular communication from being traced. The proposed protocol not only capable of achieving the conditional privacy preservation, but also minimize the anonymous keys storage at each OBU. Unfortunately, Huang *et al.* [16] and Vijayakumar *et al.* [38] pointed out that since the pseudonym keys of vehicles in this ECPP scheme are generated by the RSUs, there is a fairly high latency in the key generation process. Besides, ubiquitous presence of RSUs are needed for assisting vehicles to get their pseudonyms and private keys. Additionally, since the vehicles can acquire their pseudonyms from each RSU, the revocation of the malicious vehicle cannot be achieved. Later, using a group signature, Wu *et al.* [39] proposed a conditional privacy preservation protocol (CPPA). Each RSU maintains an on-the-fly generated group so vehicles are able to generate and verify messages anonymously. However, the network topology formed by vehicles changes very quickly so this scheme cannot easily select group members [48]. In 2012, Shim [35] designed a new CPPA which dedicated to vehicle-to-infrastructure communications based on their ID-based signature scheme. However, since the scheme uses complex bilinear pairing operations, there is a high computational and communication delay.

Obviously, although the certificate management problem existed in the PKI-based authentication schemes can be solved by utilizing the ID-based scheme, there are still some challenges. On the one hand, many schemes use complex bilinear pairing operations and require RSUs to participate in authentication, so they are not well suited for time-delay-sensitive vehicular networks [13]. Besides, once the RSU is compromised, some important information stored in the RSU will be leaked, thereby the system security is reduced [38]. On the other hand, the performances of such schemes are not satisfactory, since there are still security vulnerabilities. More importantly, few researchers take into account the credibility issue of messages. In fact, legitimate vehicles that have already been authenticated are still likely to send malicious or meaningless messages, which causes the efforts for both identity authentication and data integrity verification in vain [1].

For the former problem, researchers have used the ECC for designing the efficient authentication scheme. In He *et al.*'s scheme [13], an ID-based authentication scheme was proposed. It does not use bilinear pairing and supports

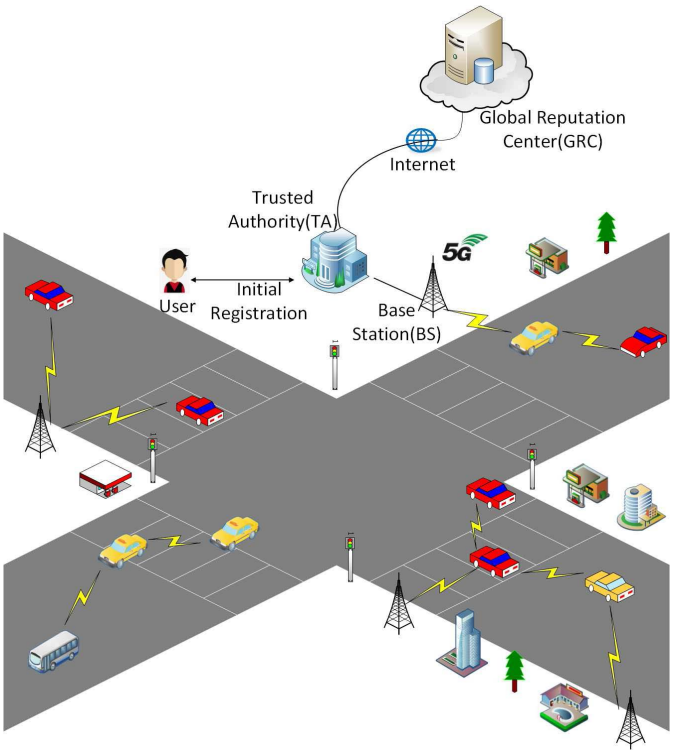


Fig. 1. Model of 5G-enabled vehicular networks.

batch verification; consequently, computational complexity is reduced while achieving lower communication costs. As for the latter problem, in recent years, researchers have proposed reputation systems to ensure the credibility of messages in vehicular networks. Based on a reputation system, a announcement scheme was proposed by Li *et al.* [22]. It allows vehicles to evaluate the credibility of messages. Vehicles can quickly determine whether the information is reliable according to the sender's reputation score. Because it reflects to which extent the vehicle has published credible information before, which also reflects the probability that the vehicle may announce credible information later. In the scheme of Yang *et al.* [42], a reputation system was proposed for evaluating data credibility by means of blockchain technology. Based on the ratings stored in the blockchain, vehicles can assess the credibility of the message by calculating the reputation score of the sender. However, the safety problems of vehicular networks are not considered in these two schemes.

III. Background

In this section, we introduce the 5G-enabled vehicular network model and system assumptions first. There are mainly four types of entities in the network, namely, a global reputation center (GRC), the TA, the fixed roadside 5G-BS, and vehicles equipped with OBUs. Then we describe three modules of the reputation system managed by the TA. Finally, we identify the security objectives.

A. Network Model and Assumptions

Fig. 1 illustrates the model of the 5G-enabled vehicular network considered in our framework. Details of network entities and system assumptions are described below.

1) *TA:* The TA has excellent computing and storage capabilities. In the reputation system-based authentication protocol, TA mainly performs the following two functions.
   a) *Vehicle Registration:* Before joining into the 5G-enabled vehicular network, vehicles need to register in the local TA [8]. The TA records basic information of the vehicle. Then the TA stores the security parameters, a pseudo-ID, and corresponding private key into the OBU. In order to resist malicious attacks, the TA will generate a new pseudo-ID and private key for the legitimate vehicle applying for updating.
   b) *Reputation Management:* Apart from the registration, the TA needs to manage the vehicle's reputation score based on the feedback from other vehicles. Only the vehicle whose reputation score exceeds the threshold can obtain a credit reference (CR) which is only valid for a period of time.
2) *GRC:* It is a global reputation database that stores reputation information of all vehicles sent by the TA. The main function is to facilitate TA in other areas to obtain the reputation scores of newly joined vehicles.
3) *5G-BS:* 5G base stations are located at the intersections or hotspots, and it is responsible for relaying the messages exchanged between V2V and vehicles to TA. We assume that 5G-BS already be able to provide good network coverage, with super-fast information transmission speed [12].
4) *Vehicle:* With the wireless communication capabilities provided by the equipped OBU, vehicles can communicate with the TA and other vehicles. The OBU supports the 5G protocol and is a tamper-proof device which stores the vehicle's private data and provides the cryptographic processing capabilities.

System Assumptions:

1) The TA is fully trustworthy and will never be compromised.
2) No secret data stored in the vehicles can be learned by anyone.
3) The time in all parts of vehicular networks is kept in sync.

If vehicles calculate their reputation scores by themselves, the accuracy and reliability of reputation update cannot be ensured [18], [23]. Therefore, underlying reputation management tasks are executed by the TA [31]. Besides, in view of the fact that the number of vehicles is too large, we propose a scalable solution that redundant TAs are installed according to the size of service areas which have identical functionalities, to avoid becoming a bottleneck or a single fault [3]. Geo-distributed TAs collaborate for vehicular networks. Note that in our protocol, TAs send the same new CR for all legitimate vehicles within a fixed period of time, therefore all TAs need to store the same set of CR at the very beginning.

B. Reputation System

Reputation is defined as the opinion of one user or device about the other, and more specifically, it can be considered as

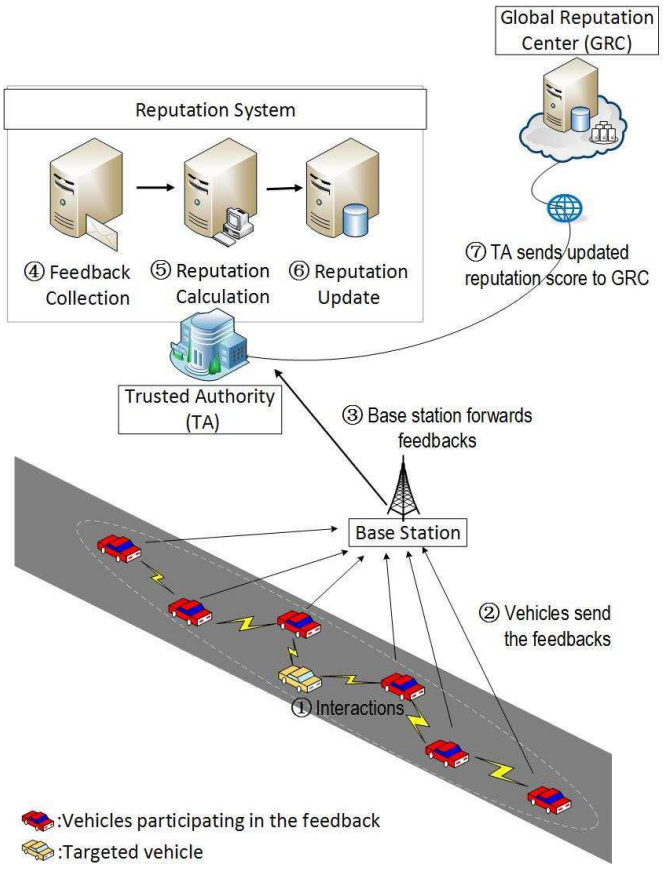


Fig. 2. Framework of the reputation system.

the user's trustworthiness [37]. In our framework, the reputation system managed by the TA consists of three modules: 1) the feedback collection module (FC); 2) the reputation calculation module (RC); and 3) the reputation update module (RU). The reputation of the vehicles are expressed by the numerical scores, which are a quantitative form of vehicles' long-term behavioral performance. Reputation scores are updated but not cleared or reset. Fig. 2 shows the overall framework of our reputation system.

1) *FC:* After the interaction, vehicles participating in the feedback, according to whether the content of the message is useful, put forward individual feedback about the target vehicle V_i to the TA through the 5G base station. The feedback contains the timestamp tt, the message M_v of the target vehicle, and the identity of themselves. The TA collects and filters out all the valid feedbacks [46]. Afterward, TA classifies this feedbacks according to the type of the M_v (kind or malicious) and retrieves the reputation scores of V_{Fi}. In order to ensure the freshness of the feedback messages, a message filtering time window is introduced in this module.
2) *RC:* Ensure the accurate of the reputation score is of critical importance [36]. Existing reputation score calculation methods mainly use weighted sums [4], Bayesian neutron networks [5], reputation heuristic algorithms [32], or Google PageRank algorithm [33]. Inspired by the work of Chen and Wang [6] and Huang *et al.* [18], in this protocol we use a weighted sum method and set user's reputation score as the initial score of the vehicle to solve the cold start problem. Different messages and different reputation scores of participating vehicles leading to reputation segments with diverse qualities. Therefore, we use multiweighted for accurate reputation update in RSMA. Using the results of the feedback collection module, the new reputation score for a given target vehicle V_i can be calculated through the four steps shown in Algorithm 1. Here, we give the corresponding explanation of our reputation calculation algorithm. First, we assume that vehicles V_{Fi} that participating in the feedback constitute the set A, where $A = \{V_{Fi}|i = 1, \ldots, N\}$, and the reputation scores RS_{Fi} of V_{Fi} constitute the set S, where $S = \{RS_{Fi}|i = 1, \ldots, N\}$. In step 1, the total number N of participating vehicles is multiplied by the weight ω_i, which is corresponding to the effect of message M_v (M_v is sent by V_i with a timestamp tt), for obtaining the effect degree score D^t, therefore $D^t = N * \omega_i$. To be clear, we set the effect of the message to three levels: 1) light (ω_1); 2) medium (ω_2); and 3) heavy (ω_3). The deeper the effect of M_v, the larger the value of ω_i, that is, $\omega_1 < \omega_2 < \omega_3$. In step 2, we first classify the participating vehicles into three different levels *low*, *medium*, *high*, based on their reputation scores. *low*,

Algorithm 1 Reputation Calculation Framework

Input:
M_{vi}; the reputation scores of V_i and V_{Fi};
// $A = \{V_{Fi}|i = 1, \ldots, N\}$, $S = \{RS_{Fi}|i = 1, \ldots, N\}$
Output:
the new reputation score $RS_{Vi}^{(t+1)}$ of V_i ($TA \rightarrow V_i$);
// T_c denotes the current time
// Δt denotes the time threshold
while $(T_c - tt < \Delta t)$ **do**
  Step 1: The Effect Degree Score D^t
  Check the effect of M_v
  Calculate $D^t = N * \omega_i$
  // $\omega_1 \leftarrow light$, $\omega_2 \leftarrow medium$, $\omega_3 \leftarrow heavy$
  // $\omega_1, \omega_2, \omega_3 \in [0, 1]$, $\omega_1 + \omega_2 + \omega_3$=1
  Step 2: The Objective Evaluation Score E^t
  for each $RS_{Fi} \in low$
    n_1 = the number of $RS_{Fi} \in low$;
      for each $RS_{Fi} \in medium$
        n_2 = the number of $RS_{Fi} \in medium$;
          for each $RS_{Fi} \in high$
            n_3 = the number of $RS_{Fi} \in high$;
  Calculate $E^t = n_1 * \mu_1 + n_2 * \mu_2 + n_3 * \mu_3$;
  // $\mu_1 \leftarrow low$, $\mu_2 \leftarrow medium$, $\mu_3 \leftarrow high$
  // $\mu_1, \mu_2, \mu_3 \in [0, 1]$, $\mu_1 + \mu_2 + \mu_3 = 1$
  // $n_1 + n_2 + n_3 = N$
  Step 3: Historical Reputation Score H^t
  Get the RS_{Vi}^t of V_i from database;
  Let $H^t = RS_{Vi}^t$;
  Step 4: The Final Reputation Score RS_{Vi}^{t+1}
  Calculate $RS_{Vi}^{(t+1)} = \alpha * H^t \pm (\beta * E^t + \gamma * D^t)$;
  // $(\alpha + \beta + \gamma = 1)$
end while

medium, and *high*, correspond to three different numerical intervals of reputation scores, for example, [60–75], [75–90], and [90–100], respectively. Considering that the higher level of V_{Fi}'s reputation score belongs to, indicates the vehicle V_{Fi} performed better in the past period of time, therefore their feedbacks are more closer to the real situation, so we give the *high* level the maximum weight. Then step 2 calculates the objective evaluation score E^t through multiply the number of vehicles n_1 of different reputation levels by its corresponding weight μ_1; consequently, we get $E^t = n_1 * \mu_1 + n_2 * \mu_2 + n_3 * \mu_3$. Step 3 is to get V_i's historical reputation score RS_{Vi}^t and set $H^t = RS_{Vi}^t$. Finally, in step 4, the new reputation score $RS_{Vi}^{(t+1)} = \alpha * H^t \pm (\beta * E^t + \gamma * D^t)$ is generated based on steps 1–3 which is the weighted average of D^t, E^t, and H^t. α, β, and γ are three predefined weighting factors and satisfy $\alpha + \beta + \gamma = 1$. As time elapses, the reputation score evolves. Good feedback will increase the reputation score of V_i, whereas negative feedback will reduce the reputation score of V_i.

3) *RU:* The TA updates reputation score in its local reputation database. Meanwhile, TA sends this latest score into the GRC via the Internet. Upon the bad feedbacks accumulate to a certain extent, causing the reputation score of the vehicle below the given threshold, TA will add this vehicle to the blacklist and broadcast its real identity.

Note that the reputation calculation is a relatively independent module, so our protocol can easily be combined with other efficient reputation calculation methods.

C. Security Objectives

Our scheme is targeted at achieving the following security objectives.

1) *Message Authentication:* The vehicle can verify that messages are not actually forged or modified by others.
2) *Identity Privacy Preservation:* Any third party cannot obtain vehicle's true identity through the message from a given vehicle.
3) *Credibility:* The message should be a valuable message sent by a legitimate vehicle. It is not malicious or meaningless message that just wastes bandwidth resources and consumes computing power.
4) *Traceability:* Although the true identity of the vehicle is hidden from any other vehicle. However, if necessary, the TA is able to get the real identity of vehicle.
5) *Unlinkability:* No third party can link messages from the same vehicle through the message content.
6) *Resistance to Ordinary Attacks:* The scheme should be able to resist common attacks, for instance, impersonation attack, replay attack, offline password guessing attack, and modification attack that exist in vehicular networks.

IV. Proposed Protocol

In this section, we describe the proposed protocol in detail. At first, TA setups the system. Before a vehicle can join into the vehicular network, it must register with the TA. After successfully passing through the login phase, vehicle sends the encrypted and signed messages, then neighboring vehicles verify these messages and put forward feedbacks to the TA according to the content of messages. Upon receiving the feedbacks, the TA invokes the reputation management system to update the reputation score of the vehicle. Only the vehicle with a reputation score greater than the threshold can obtain the new pseudonym and corresponding private key as well as CR from TA, in the pseudo-ID and private key extraction phase. Moreover, we provide a password change phase for user friendly. Our scheme has the following advantages.

1) Our scheme shows better performance in time consumption since it does not require any MapToPoint operation and is pairing free.
2) To improve performance further, the function of batch verification of multiple messages is included.
3) We propose a reputation system for reducing the number of untrusted messages, and with the CR generated based on one-way hash function, vehicles can more quickly verify whether the message comes from TA or other legitimate vehicles. Fig. 3 shows the framework of our protocol. Notations are listed in Table I.

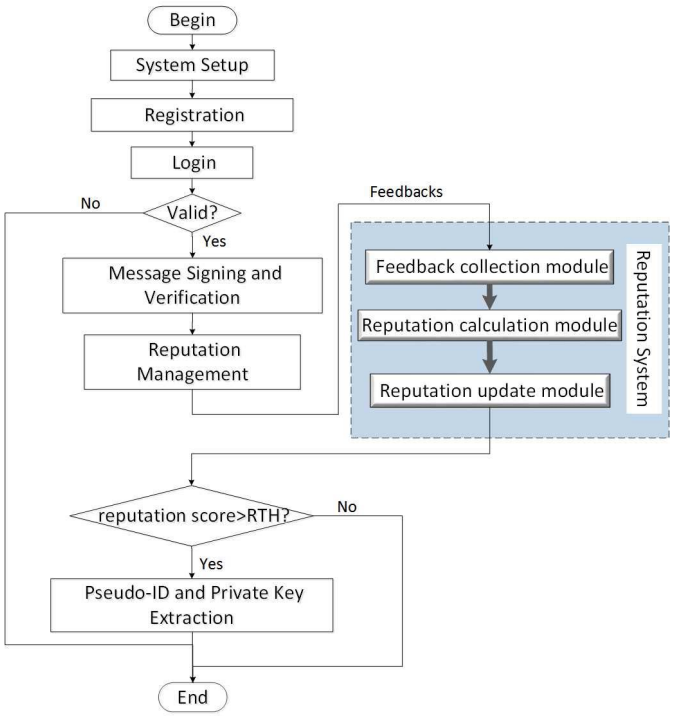


Fig. 3. Framework of the proposed protocol.

A. System Setup

Let F_p be the finite field over p, and p is a prime number denotes the size of finite field. $(a, b) \in F_p$ are the parameters of elliptic curve E, and P is the generator point of E with a prime order of q. O denotes infinity and $P \neq O$.

1) The TA chooses $h : \{0,1\}^* \rightarrow Z_q$, $H_1 : \{0,1\}^* \rightarrow Z_q$, $H_2 : \{0,1\}^* \rightarrow Z_q$ and sets the randomly selected number $s \in Z_q$ as its private key, then computes $P_{\text{pub}} = sP$ as

TABLE I
NOTATIONS

Notations	Definitions
TA	Trusted authority
s	The private key of the TA
P_{pub}	The public key of the TA
UID_i	The real identity of user
V_i	The $i-th$ vehicle
ID_i	The real identity of V_i
AID_i	The pseudo identity of V_i
PW_i	The password of V_i
CR	Credit reference
M_{ku}	A CR_i and AID_i update request message
RTH	Reputation threshold
tt_i	The latest timestamp
h, H_1, H_2	Three collision-free one-way hash functions
$\|$	Concatenation operation
$\oplus$	Exclusive-OR operation

$$CR_n \qquad CR_{n-1} \qquad\qquad CR_2 \qquad CR_1$$
$$h\,(nonce) \rightarrow h^2(nonce) \rightarrow \cdots \rightarrow h^{n-1}(nonce) \rightarrow h^n(nonce)$$

Fig. 4. Credit references set generation scheme.

its corresponding public key. TA keeps s and publishes $\{H_1, H_2, P, P_{\text{pub}}, q\}$ as the system public parameters. Note that h will not be published, it only stored in TA and vehicles for further improvement of the robustness of our scheme.

2) The TA generates the CRs set $\{\text{CR}_i, i = 1, \ldots, N\}$ using the hash-chain method. Moreover, the lifetime of CR_i is short for strong security. Because all TAs will update CRs that used for vehicle communications within a fixed period. Therefore, before the current CR going to end, each vehicle must send M_{ku} to the nearest TA. Fig. 4 shows that new CR cannot be inferred from the old one. Existing authentication schemes for value-added services in 5G-enabled vehicular networks contain the cloud server [11], [28], due to such services require huge computing and storage capabilities [19]. We will add cloud servers in our framework to support value-added vehicular services, such as video streaming download service, and use CR to provide a reference for the cloud server when the vehicle requests video stream information, i.e., the cloud server only provides service to vehicles with CR.

B. Registration

Prior to joining 5G-enabled vehicular networks, vehicles must register in the local TA before leaving the factory.

1) The user sends UID_i, ID_i along with the selected login password PW_i to the local TA.
2) The TA checks the reputation score of the user according to his identity information, and sets this score RS_i as the initial reputation score of the vehicle, at the same time, TA issues a CR for the vehicle. After that, TA computes secret authentication parameters $A_i = h(\text{UID}_i \| \text{ID}_i \| s)$ and $B_i = h(\text{PW}_i) \oplus A_i$. TA generates a pseudo-ID $\text{AID}_i = \text{ID}_i \oplus h(s \| R_i)$ and the corresponding private key $S_{\text{AID}i} = r_i + s \cdot H_1(\text{AID}_i \| R_i) \bmod q$ for V_i, where $r_i \in Z_q$ is a randomly selected number and $R_i = r_i P$ [13]. Note that unlike CR, TA in each region can generate different R_i and just need to guarantee that CR and R_i are updated synchronously.
3) The TA stores $\{\text{UID}_i, \text{ID}_i, \text{PW}_i, \text{CR}, \text{AID}_i, S_{\text{AID}i}, h\}$ and the secret authentication parameters A_i, B_i into the V_i, and locally stores $\{\text{ID}_i, \text{RS}_i\}$. Moreover, the adversary cannot launch a stolen-verified attack successfully, because TA does not save the vehicle's login password.

C. Login

As the first checkpoint, in the login phase, V_i verifies the legitimacy of the user by the following two steps.

1) User inputs $(\text{PW}_i, \text{UID}_i, \text{ID}_i)$ to the V_i.
2) Vehicle V_i verifies whether the PW_i makes the equation $B_i = h(\text{PW}_i) \oplus A_i$ hold. If the user enters wrong PW_i, then this login request will be rejected, otherwise this request will be permitted.

D. Message Signing and Verification

After the login phase, V_i sends messages to neighboring vehicles. Messages are encrypted using CR, so only vehicles with valid CR can decrypt the information sent by V_i. This operation improves the credibility of the messages and reduces the participation of malicious vehicles.

1) Vehicle V_i uses the randomly selected number $d_i \in Z_q$ to calculate $D_i = d_i P$, $M_1 = CR \oplus M_i$, $M_2 = CR \oplus D_i$. Then V_i signs the message M_i by calculating $\sigma_{vi} = S_{\text{AID}i} + d_i \cdot H_2(\text{AID}_i \| R_i \| D_i \| M_1 \| tt_i) \bmod q$, where M_i is a safety-related or infotainment information. Note that D_i can be calculated before signing the message.
2) V_i sends the $\{\text{AID}_i, R_i, M_1, M_2, tt_i, \sigma_{vi}\}$ to the neighboring vehicles.
3) Upon receiving the $\{\text{AID}_i, R_i, M_1, M_2, tt_i, \sigma_{vi}\}$, the verifier first checks the timestamp of the message. The verifier would reject the message if it is invalid.
4) The verifier uses CR to decrypt M_1 and M_2 to obtain M_i and D_i. After that the verifier calculates $h_{(i,1)} = H_1(\text{AID}_i \| R_i)$, $h_{(i,2)} = H_2(\text{AID}_i \| R_i \| D_i \| M_1 \| tt_i)$ to check whether the (1) holds. If so, the verifier accepts the message; otherwise, it will be rejected.

$$\sigma_{vi} P = h_{(i,2)} D_i + R_i + h_{(i,1)} P_{\text{pub}}. \tag{1}$$

1) Batch Verification: This scheme supports batch verification, that is, a vehicle can simultaneously verify n messages sent from other vehicles. To resist the new attacks on ID-based batch signatures [25], for the received message tuples of different vehicles, the verifier randomly chooses a vector $a = \{a_1, a_2, \ldots, a_n\}$, further more, $a_i \in [1, 2^t]$ and t is a small random integer. If the tt_i $(i = 1, 2, \ldots, n)$ is invalid, the verifier rejects the message. Then, the verifier checks if the (2) holds. If so, the verifier accepts the message; otherwise, it will be rejected

$$\left(\Sigma_{i=1}^n a_i \cdot \sigma_{vi}\right) \cdot P = \left(\Sigma_{i=1}^n a_i \cdot h_{(i,2)} \cdot D_i\right) + \Sigma_{i=1}^n a_i \cdot R_i + \left(\Sigma_{i=1}^n a_i \cdot h_{(i,1)}\right) \cdot P_{\text{pub}}. \tag{2}$$

E. Reputation Management

Upon receiving the feedback messages, the TA invokes the reputation system designed by us as described in Section III to update the reputation score and uploads it to the global reputation center. For the vehicle whose reputation score below the threshold, TA will blacklist the vehicle, refuse to send a new private key and a CR for it, and broadcast its true identity. Meanwhile, in order to encourage vehicles to behave well and actively participate in the feedback process, it is necessary to set up an incentive mechanism, such as reducing the insurance of vehicles whose reputation score exceeds the threshold [43].

F. Pseudo-ID and Private Key Extraction

As previously mentioned, the TA will update the credit reference CR in a new time period; consequently, when CR's life is about to end, the vehicle will send the update request message M_{ku} to the TA. At first, TA checks the reputation score of this vehicle. If the reputation score greater than the threshold, TA sends a new credit reference CR_{i+1} to the vehicle in an encrypted way. Note that all vehicles in this time period receive the same new CR.

1) Vehicle V_i uses the randomly selected number $n_i \in Z_q$ to calculate $N_i = n_i P$. Then uses CR_i to encrypt the update request $M_{vi} = \mathrm{CR}_i \oplus M_{ku}$ and signs the message by computing $\sigma_{vi} = S_{\mathrm{AID}i} + d_i \cdot H_2(\mathrm{AID}_i \| R_i \| N_i \| M_{ku} \| tt_i) \bmod q$.
2) Vehicle V_i sends the tuple $\{\mathrm{AID}_i, R_i, N_i, M_{vi}, \sigma_{vi}, tt_i\}$ to the nearest TA. Once the request message is received by the TA, TA first checks the timestamp of the message and obtains the M_{ku} using CR_i. TA computes $h_{(i,1)} = H_1(\mathrm{AID}_i \| R_i)$, $h_{(i,2)} = H_2(\mathrm{AID}_i \| R_i \| N_i \| M_{ku} \| tt_i)$ to verify whether the equation $\sigma_{vi} P = h_{(i,2)} N_i + R_i + h_{(i,1)} P_{\mathrm{pub}}$ holds. If it does hold, the TA calculates $\mathrm{ID}_i = \mathrm{AID}_i \oplus h(s \| R_i)$ to get the true identity of the vehicle.
3) The TA uses the randomly selected number r'_i to compute $R'_i = r'_i P$ (publish R'_i each time) to generate a new pseudo-ID $\mathrm{AID}'_i = \mathrm{ID}_i \oplus h(s \| R'_i)$ and the corresponding private key $S'_{\mathrm{AID}} = r'_i + s \cdot H_1(\mathrm{AID}'_i \| R'_i) \bmod q$. Then TA computes $M_{(T,1)} = h(B_i \| N_i) \oplus \mathrm{CR}_{(i+1)}$, $M_{(T,2)} = h(B_i \| N_i) \oplus \mathrm{AID}'_i$, and $M_{(T,3)} = h(B_i \| N_i) \oplus S'_{\mathrm{AID}i}$. Obviously, only the vehicle with private authentication parameter B_i is able to obtain AID'_i, $S'_{\mathrm{AID}i}$, and $\mathrm{CR}_{(i+1)}$. Finally, TA signs the message by calculating $\sigma_{TA} = H_2(P_{\mathrm{pub}} \| B_i \| N_i \| M_{(T,1)} \| M_{(T,2)} \| M_{(T,3)} \| tt_i) \times r_i + s \bmod q$.
4) The TA sends the reply message $\{M_{(T,1)}, M_{(T,2)}, M_{(T,3)}, \sigma_{TA}\}$ to V_i.
5) Vehicle V_i first checks the timestamp of the message, then checks if CR_i equals $h(\mathrm{CR}_{(i+1)})$ to verify the identity of the sender, because only TA has the set of CRs generated using the hash function. Then V_i computes $h_{(i,2)} = H_2(P_{\mathrm{pub}} \| B_i \| N_i \| M_{(T,1)} \| M_{(T,2)} \| M_{(T,3)} \| tt_i)$ for verifying if the equation $\sigma_{TA} \cdot P = H_{(i,2)} \cdot R_i + P_{\mathrm{pub}}$ holds. If it does hold, the V_i calculates and stores AID'_i and $S'_{(\mathrm{AID}i)}$ for participating in the next communication of vehicular networks.

G. Password Change

This scheme provides users with a convenient password change procedure. Due to there is no need for TA's assistance, through the following steps the passwords can be changed whenever users like.

1) The user keys in PW_i, UID_i, ID_i, and PW'_i.
2) V_i checks whether the information entered by the user makes the equation $B_i = h(\mathrm{PW}_i) \oplus A_i$ hold. Afterward, V_i performs $B'_i = B_i \oplus h(\mathrm{PW}_i) \oplus h(\mathrm{PW}'_i)$ for changing PW_i into PW'_i.

V. Security Analysis and Comparison

A. Security Proof

First, we introduce the elliptic curve discrete logarithm problem (ECDLP).

Definition 1 (ECDLP): $t \in Z_q$ and $T = tP \in G$, where P is the generator of the group G. Given $T = tP$, it is not feasible to learn t.

Next, the security model for the RSMA is defined by a game played between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$. Note that $\mathcal{C}$ maintains hash lists L_{H1} and L_{H2}.

1) *Setup-Oracle:* $\mathcal{C}$ generates the private key and parameters of the system. Then, $\mathcal{C}$ sends the system parameters to $\mathcal{A}$, when $\mathcal{A}$ invokes this query.
2) *H_1-Oracle:* $\mathcal{C}$ returns the selected random number $x \in Z_q$ to $\mathcal{A}$ and inserts the tuple $\langle m, x \rangle$ into L_{H1}, when $\mathcal{A}$ invokes this query.
3) *H_2-Oracle:* $\mathcal{C}$ returns the selected random number $x \in Z_q$ to $\mathcal{A}$ and inserts the tuple $\langle m, x \rangle$ into L_{H2}, when $\mathcal{A}$ invokes this query.
4) *Extract-Oracle:* When $\mathcal{A}$ invokes this query using the AID_i about user's identity, $\mathcal{C}$ generates a message $\langle \mathrm{AID}_i, S_{\mathrm{AID}i} \rangle$ and sends it to $\mathcal{A}$.
5) *Sign-Oracle:* When $\mathcal{A}$ invokes this query using the message M_i about traffic status, $\mathcal{C}$ generates a message $\langle M_i, D_i, \sigma_i \rangle$ and sends it to $\mathcal{A}$.

Within a time bound T and with a probability of ε, $\mathcal{A}$ performs existential forgery under an adaptively chosen message attack against the proposed scheme. If $\mathcal{A}$ could generate a valid login request message, then $\mathcal{A}$ could violate the RSMA. Let $\mathrm{Adv}^{\mathrm{Auth}}(\mathcal{A})$ denote the probability that $\mathcal{A}$ could violate the RSMA.

Theorem 1: Q and R represent times that $\mathcal{A}$ can ask the random oracle and the sign oracle. If $\mathcal{A}$ can break the proposed authentication scheme, then within a time period T, $\mathcal{C}$ that can break ECDLP, which is expected to be less than $120686QT/\varepsilon$, if $\varepsilon \geq 10(R+1)(R+Q)/q$.

Proof: Suppose that an ECDLP sample $(P, S_{\mathrm{AID}i}P)$ is given for $S_{\mathrm{AID}i} \in Z_q$, $\mathcal{C}$ performs our signature scheme. Suppose $\mathcal{A}$ is able to break the proposed scheme. By performing the following queries from adversary $\mathcal{A}$, challenger $\mathcal{C}$ can solve the ECDLP by run $\mathcal{A}$ as a subroutine with a nonignorable probability.

Setup: The setup algorithm takes a security parameter k as input. $\mathcal{C}$ sets the randomly selected number s as its private key, then computes the public key P_{pub}, where $P_{\mathrm{pub}} = sP$. Afterward, $\mathcal{C}$ sends $\{P, P_{\mathrm{pub}}, q, H_1, H_2\}$ to adversary $\mathcal{A}$.

H_1 Hash Query: If $\mathcal{A}$ invokes an H_1 queries using the tuple $\langle \mathrm{AID}_i, R_i \rangle$, $\mathcal{C}$ exams if the tuple $\langle \mathrm{AID}_i, R_i \rangle$ has already existed in L_{H1} under the tuple $\langle \mathrm{AID}_i, R_i, h_1 \rangle$. If so, $\mathcal{C}$ sends the corresponding value h_1 in the tuple to $\mathcal{A}$; otherwise, $\mathcal{C}$ selects a random h_1 and inserts a new tuple $\langle \mathrm{AID}_i, R_i, h_1 \rangle$ into L_{H1}. Afterward, $\mathcal{C}$ returns the value $h_1 = H_1(\mathrm{AID}_i \| R_i)$ to $\mathcal{A}$.

H_2 Hash Query: If $\mathcal{A}$ invokes an H_2 query using the tuple $\langle R_i, D_i, \mathrm{AID}_i, M_i, tt_i \rangle$, $\mathcal{C}$ will check whether the tuple $\langle R_i, D_i, \mathrm{AID}_i, M_i, tt_i \rangle$ has already stored in L_{H2} under the tuple of $\langle R_i, D_i, \mathrm{AID}_i, M_i, tt_i, h_2 \rangle$. If so, $\mathcal{C}$ outputs h_2 to $\mathcal{A}$; otherwise, $\mathcal{C}$ selects a random number h_2 then inserts the new tuple $\langle R_i, D_i, \mathrm{AID}_i, M_i, tt_i, h_2 \rangle$ into the hash list L_{H2}. Afterward, $\mathcal{C}$ returns the value $h_2 = H_2(R_i \| D_i \| \mathrm{AID}_i \| M_i \| tt_i)$ to $\mathcal{A}$.

Extract Query: If $\mathcal{A}$ invokes this query on a user's identity AID_i, $\mathcal{C}$ calculates $R_i \doteq r_i P$, and then checks if the tuple $\langle \mathrm{AID}_i, R_i \rangle$ already stored in L_{H1}, where r_i is a randomly selected number. If a corresponding pair $\langle \mathrm{AID}_i, R_i, h_1 \doteq H_1(\mathrm{AID}_i \| R_i) \rangle$ cannot be found based on $\langle \mathrm{AID}_i, R_i \rangle$, $\mathcal{C}$ sends a failure message to $\mathcal{A}$ and refuses this query. Otherwise, $\mathcal{C}$ computes $S_{\mathrm{AID}i} = r_i + H_1(\mathrm{AID}_i \| R_i) \times s \bmod q$ and returns $\langle \mathrm{AID}_i, S_{\mathrm{AID}i} \rangle$ to $\mathcal{A}$. Note that $\mathcal{A}$ cannot get the S_{AID_k} of the target user with AID_k by making this extract query.

Sign Query: If $\mathcal{A}$ uses the pseudo-ID AID_i to make a sign query on a message M_i, $\mathcal{C}$ first checks the tuple $\langle \mathrm{AID}_i, R_i, h_1 \rangle$ from L_{H1}. $\mathcal{C}$ gets h_1 from the tuple $\langle \mathrm{AID}_i, R_i, h_1 \rangle$. Next, $\mathcal{C}$ randomly selects two numbers d_i and h_2. Besides, $\mathcal{C}$ randomly selects two numbers u_i and v_i and tries again. Otherwise, $\mathcal{C}$ computes $D_i = h_2^{-1} u_i P - Q$ and $\sigma_i = u_i$ and sends $\langle M_i, D_i, \sigma_i \rangle$ to $\mathcal{A}$, where $H_2(R_i \| D_i \| \mathrm{AID}_i \| M_i \| tt_i) = h_2$.

Analysis: By using Forking lemma [29], once $\mathcal{A}$ can generate two valid signatures $(D_i, \sigma_i = h_2 \times d_i + S_{\mathrm{AID}i} \bmod q)$ and $(D'_i, \sigma'_i = h'_2 d_i + S_{\mathrm{AID}i} \bmod q)$, and $h_2 \neq h'_2$, then $\mathcal{C}$ can get $S_{\mathrm{AID}i}$ from these two valid signatures successfully by computing

$$\begin{aligned} &\frac{\left(h'_2 \sigma_{Vi} - h_2 \sigma'_{Vi}\right)}{(h'_2 - h_2)} \bmod q \\ &\quad = \frac{\left(h'_2 h_2 d_i + h'_2 S_{\mathrm{AID}i} - h_2 h'_2 d_i - h_2 S_{\mathrm{AID}i}\right)}{(h'_2 - h_2)} \bmod q \\ &\quad = S_{\mathrm{AID}i}. \end{aligned} \tag{3}$$

Consequently, $\mathcal{C}$ has the ability to solve the ECDLP within an expected time less than $120686QT/\varepsilon$, where $\varepsilon \geq 10(R+1)(R+Q)/q$. This conclusion contradicts with Definition 1, so the proposed scheme is secure against forgery under an adaptive chosen message attack in the random oracle model. ■

B. Security Analysis

1) *Message Authentication:* No adversary can generate a valid message in polynomial time because of the ECDLP. Therefore, the receiver can check the integrity of the message received from other vehicles using $\sigma_{vi} P = h_{(i,2)} D_i + R_i + h_{(i,1)} P_{\mathrm{pub}}$.
2) *Identity Privacy Preservation:* The true identity of the vehicle is hidden in the pseudo-ID. Because the master key of the TA is secret, so others cannot get the true identity of the vehicle.
3) *Credibility:* Only the vehicle with a reputation score greater than the threshold can obtain a credible reference CR issued by the TA for further participating in vehicular communications.
4) *Traceability:* Once the signature message is disputed, the TA can extract vehicle's real identity by computing $\mathrm{ID}_i = \mathrm{AID}_i \oplus h(s \| R_i)$.
5) *Un-Linkability:* Because the vehicle uses the dynamically updated pseudo-ID to sign the message, and the message contains random numbers, so it is impossible for the adversary to connect multiple messages from the same vehicle.
6) *Resistance to Ordinary Attacks:* Our scheme could withstand the following common types of attacks.
   a) *Impersonation Attack:* The adversary cannot impersonate the TA to generate a valid CR and new pseudo-ID, since both of them contain the master key of the TA. On the other hand, due to the CR is generated using the one-way hash function, so if vehicles receive the CR, the correctness of the CR can be verified by computing $\mathrm{CR}_i = h(\mathrm{CR}_{(i+1)})$.
   b) *Replay Attack:* Each message contains the timestamp. By checking the validity of the timestamp, participants could discover the replay of the message.
   c) *Modify Attack:* Once the message has been modified, the equation will no longer hold. Therefore, the scheme can resist modification attacks.
   d) *Offline Password Guessing Attack:* In the initial registration process, the TA uses s to calculate $A_i = h(\mathrm{UID}_i \| \mathrm{ID}_i \| s)$ for the vehicle V_i. Additionally, users can change the password PW_i frequently, therefore, the adversary can not guess both s and the password PW_i correctly in polynomial time.

C. Security Comparison

Let SEC-1, SEC-2, SEC-3, SEC-4, SEC-5, and SEC-6 denote message authentication, identity privacy preservation, unlinkability, replaying resistance, offline password guessing resistance, and the message credibility. The security comparison results listed in Table II shows that our protocol can achieve more merits.

VI. Performance Analysis

In the next two sections, we analyze the time consumption of our protocol and compare it with four recent batch verification supported schemes for vehicular networks.

In the schemes of Azees *et al.*'s [3] and Horng *et al.*'s [14], the crypto-operations are established on bilinear pairings. In the schemes of He *et al.*'s [13] and Li *et al.*'s [24] as well as the proposed protocol, the crypto-operations are established on ECC. Here, we adopt the method of computation evaluation proposed in [14]. The bilinear pairing $\overline{E} : G_1 \times G_1 \rightarrow G_T$ is created for achieving the security level of 80 bits, a point $\overline{P}$ is G_1's generator. The G_1 with the order $\overline{q}$ on the super singular elliptic curve $\overline{E} : y^2 = x^3 + x \bmod \overline{p}$. Besides, $\overline{p}$ is

TABLE II
SECURITY COMPARISON

	SEC-1	SEC-2	SEC-3	SEC-4	SEC-5	SEC-6
Azees's scheme [3]	⋆	⋆	⋆	×	×	×
Tzeng's scheme [14]	⋆	⋆	⋆	⋆	×	×
He's scheme [13]	⋆	⋆	⋆	⋆	×	×
Li's scheme [24]	⋆	⋆	⋆	⋆	×	×
Our scheme	⋆	⋆	⋆	⋆	⋆	⋆

⋆ : The requirement is satisfied.
× : The requirement is not satisfied.

TABLE III
EXECUTION TIME

Cryptographic operation	Time (ms)
T_{bp}	5.086
T_{bm}	0.694
T_{ba}	0.0018
T_{mtp}	0.0992
T_{em}	0.3218
T_{ea}	0.0024
T_h	0.001

made up of a 512 prime number and $\overline{q}$ is made up of a 160-bit Solinas prime number. We use G whose generator is a point P on a nonsingular elliptic curve $E : y^2 = x^3 + ax + b \pmod p$ $(a, b \in Z_p)$ for achieving the security level of 80 bits, where p, q are made up of two 160-bit prime number. Notations about execution time of related operations are defined as follows.

1) T_{bp}: The time for performing a bilinear pairing operation $\overline{e}(\overline{S}, \overline{T})$, where $\overline{S}, \overline{T} \in G_1$.
2) T_{bm}: The time for performing a scale multiplication operation $\overline{x} \cdot \overline{P}$ about the bilinear pairing, where $\overline{P} \in G_1$ and $x \in Z_q$.
3) T_{ba}: The time for performing a point addition operation $\overline{S} + \overline{T}$ about the bilinear pairing, where $\overline{S}, \overline{T} \in G_1$.
4) T_{mtp}: The time for performing a MapToPoint hash operation about the bilinear pairing.
5) T_{em}: The time for performing a scale multiplication operation $x \cdot P$ about the ECC, where $P \in G$ and $x \in Z_q$.
6) T_{ea}: The time for performing a point addition operation $S + T$ about the ECC, where $S, T \in G$.
7) T_h: The time for performing a one-way hash function operation.

The execution time of above cryptographic operations is computed using the MIRACL [31]. The hardware platform contains an Intel I7-6700 processor, 8 gigabytes memory and runs Windows 7 operating system. Table III lists out the execution time.

A. Computation Cost Analysis

We only introduce Azees *et al.*'s scheme [3] and our scheme in detail. The specific analysis of [13], [14], and [24] could be achieved in the same way. The computation cost of each step listed in Table IV.

TABLE IV
COMPARISON OF COMPUTATION COST

	AIGMS	SVM	BVM
Azees's scheme [3]	$1T_{bm} + 1T_h$	$2T_{bp} + 5T_{bm} + 2T_{ba}$	$(n+1)T_{bp} + (5n)T_{bm} + (2n)T_{ba}$
Tzeng's scheme [14]	$3T_{bm} + 2T_h$	$2T_{bp} + 1T_{bm} + 1T_{ba} + 1T_h$	$2T_{bp} + (2n+1)T_{bm} + (2n+1)T_{ba} + (n)T_h$
He's scheme [13]	$3T_{em} + 3T_h$	$3T_{em} + 2T_{ea} + 2T_h$	$(2n+2)T_{em} + (2n+2)T_{ea} + (2n)T_h$
Li's scheme [24]	$1T_{em} + 2T_h$	$4T_{em} + 1T_{ea} + 2T_h$	$(2n+2)T_{em} + (n)T_{ea} + (2n)T_h$
Our scheme	$1T_{em} + 1T_h$	$3T_{em} + 2T_{ea} + 2T_h$	$(n+2)T_{em} + (2n+2)T_{ea} + (2n)T_h$

AIGMS: Sign a single message.
SVM: Verify a single message.
BVM: Batch verification of multiple messages.

The bilinear pairing is adopted in Azees *et al.*'s scheme [3]. For a single message signing step of Azees *et al.*'s scheme [3], the vehicle is required to perform one point addition operation and one hash function operation; consequently, the execution time is $1T_{bm} + 1T_h \approx 0.695$ ms. To verify a single message of Azees *et al.*'s scheme [3], the verifier is required to carry out two bilinear pairing operations, two scalar multiplication operations, and five point addition operations. Accordingly, the execution time is $2T_{bp} + 5T_{bm} + 2T_{ba} \approx 13.6456$ ms. For the batch verification of multiple messages in Azees *et al.*'s scheme [3], the verifier is required to perform $(n + 1)$ bilinear pairing operations, $(5n)$ scalar multiplication operations, and $(2n)$ point addition operations; consequently, the execution time is $(n+1)T_{bp} + (5n)T_{bm} + (2n)T_{ba} \approx 5.086 + 8.5596n$ ms.

The proposed scheme is established on ECC. For the single message signing step, the verifier is required to carry out one scalar multiplication operation and one general hash function operation. Thus, the execution time only needs $1T_{em} + 1T_h \approx 0.3228$ ms. To verify a single message of the proposed scheme, the verifier is required to perform three scalar multiplication operations, two point addition operations and two general hash function operations. Accordingly, the execution time of the phase is $3T_{em} + 2T_{ea} + 2T_h \approx 0.9722$ ms. For batch verifying multiple messages of the proposed scheme, the verifier is required to execute $(n+2)$ scalar multiplication operations, $(2n+2)$ point addition operations and $(2n)$ general hash function operations; consequently, the execution time is $(n+2)T_{em} + (2n+2)T_{ea} + (2n)T_h \approx 0.6484 + 0.3286n$ ms.

Form the results shown in Fig. 5, we can see that, for signing and verifying a single message, the proposed scheme achieves much lower computational delay. In order to demonstrate the major benefit of our scheme in batch verifying of multiple messages, in Fig. 6, we compare the execution time of batch verification in proposed protocol with four related schemes [3], [13], [14], [24]. Obviously, our scheme achieves better performance.

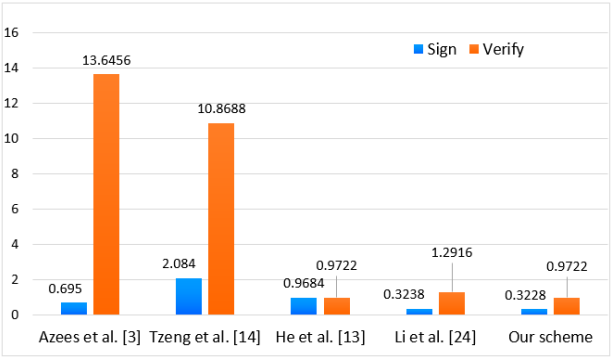


Fig. 5. Computational delay to sign and verify a message.

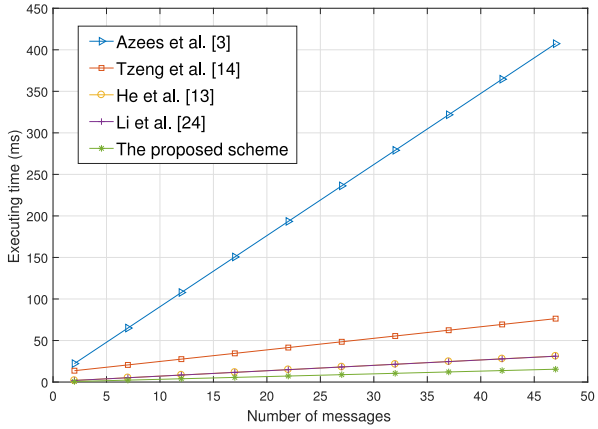


Fig. 6. Delay in the batch verification of multiple messages.

TABLE V
COMMUNICATION COST

	Sending a single message	Sending n messages
Azees's scheme [3]	848 bytes	848n bytes
Tzeng's scheme [14]	388 bytes	388n bytes
He's scheme [13]	144 bytes	144n bytes
Li's scheme [24]	144 bytes	144n bytes
Our scheme	84 bytes	84n bytes

B. Communication Cost Analysis

Because $\overline{p}$ is 64 bytes and p is 20 bytes, the sizes of the elements in G_1 and G are $64 \times 2 = 128$ bytes and $20 \times 2 = 40$ bytes. Let the size of general hash function's output be 20 bytes and timestamp be 4 bytes. Here, we consider the size of signature only. Table V shows the specific computation costs.

In Azees's scheme [3], the vehicle sends its signature messages $\{\text{sig}, Y_k, \text{Cert}_k\}$ to the verifier, where $\text{Cert}_k = (Y_k \| E_i \| \text{DID}_{ui} \| \gamma_u \| \gamma_v \| c \| \lambda \| \sigma_1 \| \sigma_2)$, c is a hash operation result, $\{\text{sig}, E_i, \text{DID}_{ui}, \gamma_u, \gamma_v, Y_k\} \in G_1$, $\{\lambda, \sigma_1, \sigma_2\} \in Z_q$; consequently, the communication cost is $128 \times 6 + 4 \times 20 = 848$ bytes. In Horng *et al.* scheme [14], the vehicle broadcasts the anonymous identity and signature $\{\text{AID}_i, M_i, S_i, T_i\}$, where $\text{AID}_i = (\text{AID}_{(i,1)}, \text{AID}_{(i,2)}) \in G_1$, T_i is the timestamp. Accordingly, the communication cost is $128 \times 3 + 4 = 388$ bytes. In He *et al.* scheme [13], the vehicle broadcasts the anonymous identity and signature $\{M_i, \text{AID}_i, T_i, R_i, \sigma_i\}$, where $\text{AID}_i = (\text{AID}_{(i,1)}, \text{AID}_{(i,2)}) \in G, \sigma_i \in Z_q$, T_i is the timestamp. Accordingly, the communication cost is $40 \times 3 + 20 + 4 = 144$ bytes. In Li *et al.* scheme [24], the vehicle broadcasts the anonymous identity and signature $\{PID_{i,l}, PK_{i,l}, R_i, T_i, \text{sig}_i\}$, where $\{R_i, \text{sig}_i, PK_{i,l}\} \in G$, T_i is the timestamp. Accordingly, the communication cost is $40 \times 3 + 20 + 4 = 144$ bytes.

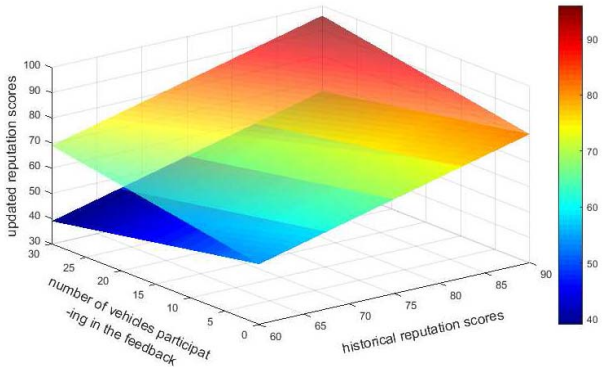


Fig. 7. Influence of different behaviors (good or malicious) on the vehicle's reputation score.

The vehicle in the proposed scheme broadcasts the anonymous identity and signature $\{\text{AID}_i, R_i, M_{Vi}, tt_i, \sigma_{Vi}\}$, where $\text{AID}_i, \sigma_i \in Z_q$ and tt_i is the timestamp. Accordingly, the communication cost is $20 \times 2 + 40 + 4 = 84$ bytes. Therefore, our scheme incurs a much lower communication cost than these four latest schemes [3], [13], [14], [24].

VII. EVALUATION

To prove the validity of our reputation system, we conducted preliminary simulation experiments. Because TA has filtered the messages in the feedback collection module, the feedback messages we used in reputation calculation module are all valid. Here, we set the number of vehicles participating in the feedback from 0 to 30. Targeted vehicles' initial reputation scores are set to 60 to 90, and the reputation threshold is 60. The multiple weighting method is used to calculate vehicles' reputation scores; therefore, in order to get realistically close to real world scenario, we have carefully chosen the values of these parameters after trying different parameters. For a reputation segment, the weights of the effect degree D^t, the objective evaluation score E^t, and the historical reputation score H^t are $\alpha = 0.9, \beta = 0.05$, and $\gamma = 0.05$.

From Fig. 7, we can clearly see that at a certain time different behaviors (good or malicious) of vehicles will lead to different results, good behavior increases the reputation score of a vehicle, whereas malicious behavior can result in a decrease in its reputation score. We use the coordinate values obtained from the 3-D coordinate axis to explain this conclusion. For example, the corresponding meaning of [60, 25, 66.5] is that a vehicle with an initial reputation score of 60 is reported by 25 vehicles because of its good behavior (such as timely inform traffic congestion information to other vehicles). Then, after the TA performs reputation calculation, the vehicle's reputation score rises to 66.5. On the contrary, [60, 25, 41.5] indicates that if the vehicle is reported by 25 vehicles for its malicious behavior (such as send false

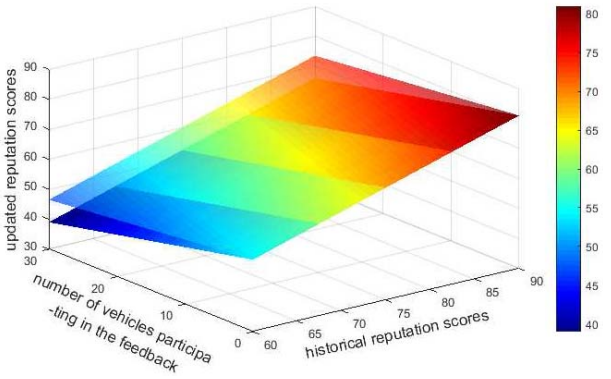


Fig. 8. Influence of different degrees of malicious behavior on the vehicle's reputation score.

information to other vehicles leading to traffic accidents), the reputation score of this vehicle will decrease to 41.5. In the same way, from Fig. 8, we know that different malicious behavior of the target vehicle will lead to the decline of its reputation score at different speeds. The greater the malicious influence caused by the message, the faster the reputation score of the vehicle drops. On the other hand, both Figs. 7 and 8 show that, generally speaking, the more vehicles participate in the feedback, the faster the reputation score of the target vehicle changes.

Since the reputation threshold is set in the system, if the reputation score of the vehicle below the threshold, TA will regard this vehicle as a malicious one, and refuse to send the required information to the vehicle. By removing malicious vehicles in time, the environment of vehicular networks can be improved. Therefore, the proposed reputation system can improve the credibility of messages in vehicular networks to a certain extent. Besides, different weights can be set for the parameters according to actual application.

VIII. Conclusion

In this paper, an RMSA framework and a protocol for 5G-enabled vehicular networks were proposed. The TA is in charge of the reputation management for preventing vehicles with a reputation score below a given threshold from participating in the communication. This reduces the existence of untrusted messages in the vehicular networks. We also proved that the proposed scheme is secure against existential forgery in the random oracle model. Detailed security analysis shows that our protocol not only achieves the security objectives but also resists various common types of security attacks. This scheme is based on the ECC and supports batch authentication, thereby achieving better performance. As future work, we will continue our efforts to conduct further simulation for demonstrating the efficiency of the proposed framework.

Acknowledgment

The authors would like to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] D. Alishev, R. Hussain, W. Nawaz, and J. Y. Lee, "Social-aware bootstrapping and trust establishing mechanism for vehicular social networks," in *Proc. IEEE Veh. Technol. Conf. (VTC-Spring)*, 2017, pp. 1–5.

[2] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[3] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[4] F. Bao, I.-R. Chen, and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems," in *Proc. IEEE 11th Int. Symp. Auton. Decentralized Syst.*, 2013, pp. 1–7.

[5] I.-R. Chen and J. Guo, "Dynamic hierarchical trust management of mobile groups and its application to misbehaving node detection," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, 2014, pp. 49–56.

[6] X. Chen and L. Wang, "A trust evaluation framework using in a vehicular social environment," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM)*, 2017, pp. 1004–1005.

[7] J. Cheng *et al.*, "Routing in Internet of Vehicles: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 5, pp. 2339–2352, Oct. 2015.

[8] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, to be published. doi: 10.1109/TITS.2018.2827460.

[9] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.

[10] P. Dong, T. Zheng, S. Yu, H. Zhang, and X. Yan, "Enhancing vehicular communication using 5G-enabled smart collaborative networking," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 72–79, Dec. 2017.

[11] M. H. Eiza, Q. Ni, and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868–7881, Oct. 2016.

[12] M. Gharba *et al.*, "5G enabled cooperative collision avoidance: System design and field test," in *Proc. IEEE 18th Int. Symp. World Wireless Mobile Multimedia Netw. (WoWMoM)*, 2017, pp. 1–6.

[13] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[14] S.-J. Horng *et al.*, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

[15] H. Hu, R. Lu, Z. Zhang, and J. Shao, "REPLACE: A reliable trust-based platoon service recommendation scheme in VANET," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1786–1797, Feb. 2017.

[16] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 3, pp. 736–746, Sep. 2011.

[17] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, "Exploring mobile edge computing for 5G-enabled software defined vehicular networks," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 55–63, Dec. 2017.

[18] 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.

[19] M. Kazim, L. Liu, and S. Y. Zhu, "A framework for orchestrating secure and dynamic access of IoT services in multi-cloud environments," *IEEE Access*, vol. 6, pp. 58619–58633, 2018.

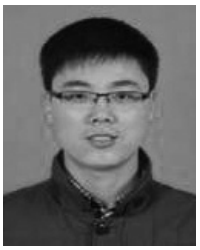
[20] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, Jun. 2017.

[21] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Netw.*, vol. 19, no. 6, pp. 1441–1449, 2013.

[22] 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.

[23] W. Li and H. Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 960–969, Apr. 2016.

[24] J. Li *et al.*, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Veh. Commun.*, vol. 13, pp. 104–113, Jul. 2018.
[25] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Syst. Appl.*, vol. 41, no. 5, pp. 2559–2564, 2014.
[26] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE 27th Conf. Comput. Commun. INFOCOM*, 2008, pp. 1229–1237.
[27] N. Magaia, Z. Sheng, P. R. Pereira, and M. Correia, "REPSYS: A robust and distributed incentive scheme for collaborative caching and dissemination in content-centric cellular-based vehicular delay-tolerant networks," *IEEE Wireless Commun.*, vol. 25, no. 3, pp. 65–71, Jun. 2018.
[28] A. Mohseni-Ejiyeh and M. Ashouri-Talouki, "Sevr+: Secure and privacy-aware cloud-assisted video reporting service for 5G vehicular networks," in *Proc. IEEE Iran. Conf. Elect. Eng. (ICEE)*, 2017, pp. 2159–2164.
[29] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.
[30] K. N. R. S. V. Prasad, E. Hossain, and V. K. Bhargava, "Energy efficiency in massive MIMO-based 5G networks: Opportunities and challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 86–94, Jun. 2017.
[31] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, 2007.
[32] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Commun. ACM*, vol. 43, no. 12, pp. 45–48, 2000.
[33] U. Sehgal, K. Kaur, and P. Kumar, "The anatomy of a large-scale hyper textual Web search engine," in *Proc. 2nd Int. Conf. Comput. Elect. Eng.*, 2009, pp. 491–495.
[34] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.
[35] K.-A. Shim, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.
[36] N. B. Truong and G. M. Lee, "Poster abstract: Trust evaluation for data exchange in vehicular networks," in *Proc. IEEE/ACM 2nd Int. Conf. Internet Things Design Implement.*, 2017, pp. 325–326.
[37] M. Usman, M. R. Asghar, I. S. Ansari, and F. Granelli, "Towards bootstrapping trust in D2D using PGP and reputation mechanism," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2017, pp. 1–6.
[38] P. Vijayakumar, M. Azees, V. Chang, J. Deborah, and B. Balusamy, "Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks," *Clust. Comput.*, vol. 20, no. 3, pp. 2439–2450, 2017.
[39] Q. Wu, J. Domingo-Ferrer, and U. González-Nicolás, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.
[40] Q. Wu, G. Y. Li, W. Chen, D. W. K. Ng, and R. Schober, "An overview of sustainable green 5G networks," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 72–80, Aug. 2017.
[41] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, "5G mmWave positioning for vehicular networks," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 80–86, Dec. 2017.
[42] 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 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2017, pp. 1–5.
[43] B. Ying and D. Makrakis, "Reputation-based pseudonym change for location privacy in vehicular networks," in *Proc. IEEE Int. Conf. Commun.*, 2015, pp. 7041–7046.
[44] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "Raise: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. ICC*, vol. 8, 2008, pp. 1451–1457.
[45] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE 27th Conf. Comput. Commun. INFOCOM*, 2008, pp. 246–250.
[46] L. Zhang, G. Ding, Q. Wu, and F. Song, "Defending against Byzantine attack in cooperative spectrum sensing: Defense reference and performance analysis," *IEEE Access*, vol. 4, pp. 4011–4024, 2016.
[47] L. Zhang *et al.*, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1342–1363, 3rd Quart., 2015.
[48] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, "Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 2241–2250, 2018.



Jie Cui was born in Henan, China, in 1980. He received the Ph.D. degree from the University of Science and Technology of China, Hefei, China, in 2012.

He is currently an Associate Professor and the Ph.D. Supervisor with the School of Computer Science and Technology, Anhui University, Hefei. He has authored or co-authored over 80 scientific publications in reputable journals (e.g., the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, the IEEE INTERNET OF THINGS JOURNAL, *Information Sciences*, and the *Journal of Parallel and Distributed Computing*), academic books and international conferences. His current research interests include applied cryptography, Internet of Things security, vehicular ad hoc network, cloud computing security, and software-defined networking.

Xiaoyu Zhang is currently a Research Student with the School of Computer Science and Technology, Anhui University, Hefei, China. Her current research interest includes vehicle ad hoc networks.

Hong Zhong was born in Anhui, China, in 1965. She received the Ph.D. degree in computer science from the University of Science and Technology of China, Hefei, China, in 2005.

She is currently a Professor and the Ph.D. Supervisor with the School of Computer Science and Technology, Anhui University, Hefei. She has over 120 scientific publications in reputable journals (e.g., the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, the IEEE TRANSACTIONS ON BIG DATA, the IEEE INTERNET OF THINGS JOURNAL, and the *Journal of Parallel and Distributed Computing*), academic books, and international conferences. Her current research interests include applied cryptography, Internet of Things security, vehicular ad hoc networks, cloud computing security, and software-defined networking.

Zuobin Ying was born in Anhui, China, in 1982. He received the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2016.

He is currently a Lecturer with the School of Computer Science and Technology, Anhui University, Hefei, China. His current research interests include cloud security and applied cryptography.

Lu Liu received the Ph.D. degree from the University of Surrey, Guildford, U.K.

He is currently the Head of the School of Electronics, Computing, and Mathematics and the Professor of Distributed Computing with the University of Derby, Derby, U.K., and an Adjunct Professor with Jiangsu University, Zhenjiang, China. He has authored or co-authored over 170 scientific publications in reputable academic books, and international conferences, and has secured many research projects that are supported by U.K. research councils, BIS, Innovate U.K., British Council, and leading U.K., industries.

Dr. Liu is a Fellow of the British Computer Society.