IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 27, 2019, accepted July 24, 2019, date of publication August 2, 2019, date of current version August 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2933137

A New Message Authentication Scheme for Multiple Devices in Intelligent Connected Vehicles Based on Edge Computing

HONG ZHONG[1,2,3], LEI PAN[1,2], QINGYANG ZHANG[1,2], AND JIE CUI[1,2,3]

[1]School of Computer Science and Technology, Anhui University, Hefei 230039, China
[2]Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China
[3]Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China

Corresponding author: Jie Cui (cuijie@mail.ustc.edu.cn)

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 Open Fund of Key Laboratory of Embedded System and Service Computing, Ministry of Education, Tongji University, under Grant ESSCKF2018-03, in part by the Open Fund for Discipline Construction, Institute of Physical Science and Information Technology, Anhui University, and in part by the Excellent Talent Project of Anhui University.

ABSTRACT Intelligent connected vehicles are autonomous vehicles. With the increasing degree of automation of autonomous vehicles and the development of open applications in the future, the computing tasks of autonomous vehicles are becoming more and more complex. In practice, the computing resources of vehicles are limited and the processing of data is not always guaranteed to be completed in time. However, the timely processing and integrity of the data are very important for vehicles because it affects the path selection of the traveling vehicle and the passenger experience. Therefore, it is necessary to reduce latency in processing data and verify the integrity of data for vehicles. In this paper, a novel message authentication scheme for multiple mobile devices in intelligent connected vehicles based on edge computing is proposed. The task of processing data in the vehicle is migrated to mobile devices, and tasks are executed utilizing the computing resources of multiple mobile devices in the edge computing model. The vehicle use certificateless ring signature technology to ensure the integrity of data processed by mobile devices. A security analyses show that our proposed schemes are secure in the random oracle model and can resist two types of adversaries under certificateless public key encryption. One type of adversary may be able to replace the mobile device's public key and the other type of adversary has access to the system master key. The results of performance analysis indicate the proposed scheme has high efficiency and applicability in practical intelligent connected vehicles system.

INDEX TERMS Edge computing, intelligent connected vehicles, message authentication, security.

I. INTRODUCTION

With the development of technology in communication, sensing, machine learning, and artificial intelligence, the connected and autonomous vehicle (CAV) is being implemented [1]–[3]. This vehicle leverages various sensors (*e.g.,* cameras, Lidar.) and computing units to sense and analyze the surrounding environment. Once the driver-less SAE Level-5 CAV is realized, riders in a CAV will have more time to enjoy their trip on the road. To improve the experience for users, open applications such as video players and communication software will be loaded into CAVs. Moreover, because of the camera equipment and the mobility of CAVs, some video analysis applications [4] can be installed on CAVs to improve public safety, including applications such as A3 [5], a kidnapper searching application, which recognizes license plate numbers in videos. To support the various open applications, CAVs require high volume computing resources, however, they are limited by the requirement to process data in real time [6], especially for time-intensive applications, such as autonomous driving-related applications.

Cloud computing [7] processes data in a centralized manner. This was first proposed in 2005 and widely adopted

The associate editor coordinating the review of this manuscript and approving it for publication was Lu Liu.

by companies such as Amazon, Google, Facebook, Baidu and so on, to enrich people's daily lives. However, cloud computing requires data to be uploaded to a remote cloud, resulting in potentially large data transmission delays and network bandwidth overload. To address these issues, there is an increasing focus on edge computing. Edge computing is an open platform which integrates network, computing, storage, and application core capabilities on the edge of the network near the source. With respect to the need for increased open applications on autonomous vehicles and the increased computing requirements in the future, we introduced mobile devices such as mobile phones under the model of edge computing in a previous work [3] to enhance the computing power of CAVs, as shown in FIGURE 1., where mobile devices connected with a CAV via WiFi, and CAVs are able to communicate with roadside units or a remote cloud using wireless technologies, *e.g.,* 4G and dedicated short range communications (DSRC). It is important to introduce mobile devices as edge nodes to enhance the computing power of a CAV. The data response latency will be significantly reduced, especially on a bus, which usually has a large number of passengers with mobile phones. In such a model, the CAV assigns different tasks to mobile devices.

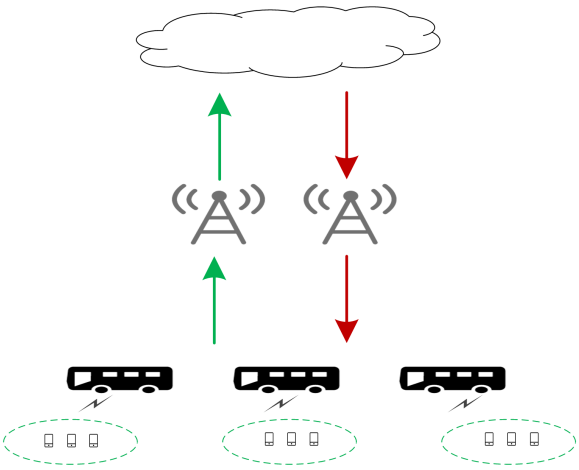


FIGURE 1. An architecture based on edge computing.

Although the collaboration from mobile devices enhances a CAV's computing capability, it also brings about potential security issues with malicious mobile devices attempting to tamper or just randomly counterfeit the results of offloaded tasks. It is dangerous because an inaccurate path might be traced from an incorrect result of roadblock recognition. In this case, mobile devices need to sign messages, including task results, to maintain integrity, thus, CAVs need to execute authentication of messages. However, the signature of the message may enable a CAV to trace a mobile device's action. This means that the risk of privacy leakage of mobile devices exists, resulting in a low degree of mobile device participation. Thus, we also consider the privacy of mobile devices. In a previous study, the message was signed with a group signature, however, this conditional privacy protects the identity of the signer as the group manager can be traced back to the specific signer [8]. In the proposed model, the mobile device will send the message to the vehicle through ring signature technology to protecting the identity privacy of the mobile device and if the mobile device is malicious and the message is incomplete, the trusted authority (TA) can trace it by the mobile device's pseudonym.

In this paper, we propose a novel message authentication scheme for multiple mobile devices in intelligent connected vehicles based on edge computing (MA-DVEC) and we also propose an improved message authentication scheme, which is supporting batch authentication. The main contributions of our proposed schemes are summarized as follows:

- Firstly, we propose the MA-DVEC scheme and introduce the concept of edge computing. To facilitate edge computing well, we focus on adding mobile devices as edge devices to the intelligent connected vehicles system to obtain real-time message for vehicles. Therefore, a message authentication scheme based on edge computing is proposed.
- Secondly, we use certificateless ring signature to improve efficiency and security in the MA-DVEC scheme. The proposed message authentication based on certificateless public key cryptosystem avoids the overhead of managing certificates. Our scheme adopts a technology of ring signature, which is self-organizing and neither ring members nor the vehicle track specific signers to guaranteeing the privacy preserving of mobile devices.
- Finally, we present a security analysis of the proposed scheme, which shows that it is provably secure under the random oracle model. Meanwhile, we implement performance analysis to compare our schemes with previous message authentication schemes.

The rest of the paper is organized as follows: In order to facilitate understanding, we introduce related works in Section II and propose some preliminary knowledge in Section III. We propose the MA-DVEC scheme in Section IV and introduce an improved scheme in Section V. Section VI introduces the security analysis of the proposed scheme and we present performance analysis in Section VII. Finally, we make a conclusion of this paper in Section VIII.

II. RELATE WORKS

The IEEE 802.11 standards committee established in 1991 adopted the term "Ad hoc network" to describe the particular peer-to-peer wireless mobile network. Ad hoc is a P2P connection and cannot communicate with other networks. All nodes in the network have equal status, and no need to set any central control nodes to automatically form an independent network, which is mainly used in sensor networks and vehicular networks such as [9], [10]. In [9], He *et al.* proposed a public auditing scheme for wireless body area networks based on Ad hoc networks, which could improve medical care and the monitoring of patients. In [10], Dietzel *et al.* proposed the aggregation of the vehicle networks based on Ad hoc networks, which could improve communication efficiency by summarizing information that is exchanged

between vehicles. One of the characteristics of the Ad Hoc networks is that it is less secure and vulnerable to eavesdropping and attacks. Therefore, it is necessary to study the security architecture and technology applicable to the vehicle networks based on Ad Hoc networks.

The vehicular ad hoc networks (VANETs) consist of an on-board unit, a roadside unit (RSU), a trusted authority and an application server, in order to improve safety communication, vehicles to vehicles and vehicles to RSU should to achieve message authentication. He *et al.* propose [11], which is a public key cryptography (PKC)-based authentication scheme. The PKC-based authentication scheme will bring problems in certificate management. Therefore, the previous proposed authentication scheme unsuitable for message authentication.

To address the certificate management problem which has been brought by the PKC-based authentication scheme. In 1985, Shamir has been proposed the concept of identity-based cryptosystems [12]. In the identity-based cryptosystems, the mobile device's identity information (e.g., identification number, cell phone number and email.) can be as the mobile device's public key. Therefore, it avoid the drawbacks of the management of a large number of mobile devices' certificates in the traditional public key cryptosystems. Whereafter, many identity-based encryption schemes have been proposed [13]–[15]. To address the problem that certificate management with message authentication in PKC mechanism, some identity-based message authentication scheme have been proposed [16]–[18]. Tiwari *et al.* [16] proposed scheme more suitable for high traffic area and provides cost effective, highly privacy preserving of user, efficient message authentication and verification than existing system for VANETs. Wang and Yao [17] also proposed the scheme of message authentication is based on identity and in the identity-based schemes, every vehicle holds too many valid identities in order to protect privacy. Later, Biswas *et al.* [18] proposed an identity-based authentication scheme for safety messages in WAVE-enabled VANETs and has been proved that the scheme is resilient to all major security threats in the paper. However, the identity-based message authentication scheme also bring the problem of key escrow.

To solve the prolem of key escrow, in 2013, Al-Riyami and Paterson [19] first proposed the concept of certificateless public key encryption. The user's private key consists of two parts: one is the information by the user and the other is generated by the key generate center. Later, the certificateless-based encryption scheme has been address the certificate management issue which is based on the PKC encryption scheme and solves the key escrow problem caused by the identity-based encryption scheme. Therefore, many certificateless-based encryption schemes are proposed [20]–[22], [31].

Because the vehicle has limited resources, an edge computing model [23] has appeared. Whereafter, a message authentication scheme based on edge computing is proposed [24], where edge nodes assists the RSU in message authentication. The specific process is the trusted authority selects part of vehicles as the edge nodes and sends the result of message authentication to the RSU, then the RSU verifies the correctness of the result and finally broadcasts the result to vehicles. As open applications increase, edge nodes not only assist message authentication, mobile devices join around the autonomous driving vehicle as edge devices and participate in the execution of computing tasks of the vehicle. The vehicle do not needs send data to the vehicle computing unit and performs centralized processing, therefore, it is easier to meet the real-time nature of autonomous driving under the edge computing model.

III. PRELIMINARIES

To improve the understanding of our schemes, in this section, we will introduce preliminaries of knowledge as mathematical background, system model and security requirements of the proposed scheme.

A. BILINEAR PAIRING

A q is a large prime number, we assume G_1, G_2, G_T are three cyclic multiplicative groups with the same order q and set a and b are random numbers of Z_q^*. If a map $e : G_1 \times G_2 \rightarrow G_T$ satisfies the following three conditions, we called it's a bilinear pairing.

1) Bilinear: For all $Q \in G_1$, $P \in G_2$ and $a, b \in Z_q^*$ are satisfy $e(a \cdot P, b \cdot Q) = e(a \cdot b \cdot P, Q) = e(P, a \cdot b \cdot Q) = e(P, Q)^{ab}$;

2) Non-degeneracy: Existing $Q \in G_1$, $P \in G_2$, and there satisfy the inequation $e(P, Q) \neq 1$;

3) Computability: For all $Q \in G_1$, $P \in G_2$, there exists an effective algorithm to compute $e(P, Q)$.

It is hard to find an algorithm to solve the following problems in polynomial time:

- *Discrete logarithm problem*: For two random elements $P \in G_2$, $Q \in G_1$, it is hard to find an integer $n \in Z_q^*$ satisfies equation $Q = nP$.
- *Computational Diffe Hellman Problem(co-CDHP)*: For three random points $P, aP \in G_2$ and $Q \in G_1$, it's hard to compute aQ in polynomial time, where $a \in Z_q^*$.

B. SYSTEM MODEL

In our proposed scheme, the system model consists of three entities, including TA, vehicle and mobile devices, which can be formed into three layers. As shown in FIGURE 2., the top layer is the TA, which is a fully trusted entity and usually hosted into a remote cloud. The second layer is the vehicle, the vehicle has limited storage resources and computing capability. However, mobile devices may be malicious and tamped messages cause the false result. The bottom layer includes many mobile devices, where we set mobile devices as edge devices, they have enough storage and computing capabilities and can execute different tasks which are come from vehicles. Therefore, the aim of our proposed scheme is checked message integrity, which has been stored or computed by different mobile devices.

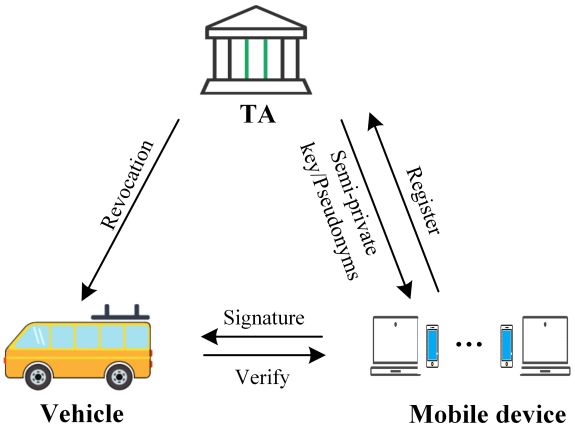


FIGURE 2. System model.

1) TA

The TA is a trusted entity, which used to generate system public parameters, semi-private keys and pseudonyms for mobile devices according to the mobile devices' requirement and their real identity. The TA maintains a revocation list and initiates the list is empty, which the list includes malicious mobile devices' real identity and a series pseudonym. According to the list of the mobile devices' revocation, the TA could trace malicious mobile devices.

2) VEHICLE

The vehicle is a limited storage resources and computing capability entity and equivalent to the user whose messages are stored in the mobile device. Because mobile devices have enough storage and computing capabilities, the vehicle could separate tasks to mobile devices and obtain messages, which has been processed. However, before receiving the message, the vehicle should check the integrity of messages stored on mobile devices.

3) MOBILE DEVICE

A mobile device is a user who has themselves electronic equipment (*e.g.,* mobile phone, laptop, iPads.) and could support enough storage and computing resources as the edge devices in edge computing model. It's a malicious entity. Every mobile device has a trusted execution environment and before access, it must input the right password. In order to secure communication with the vehicle, mobile devices should use pseudonyms which have generated by the TA.

C. SECURITY REQUIREMENTS

The security requirements of our proposed scheme are to satisfy the certificateless signature fundamental privacy preserving and tracking malicious mobile devices. The proposed MA-DVEC scheme consists of three entities TA, mobile device and vehicle, where the TA is an absolutely trusted entity, the mobile device is a malicious entity and the vehicle needs handle a lot of messages. Therefore, the concrete describes security requirements as follows:

1) Message authentication and integrity: To ensure that the vehicle could get complete data. It is necessary to provide a message authentication scheme between the vehicle and multiple mobile devices for a intelligent connected vehicles system.

2) Conditional privacy preserving: Any vehicle unknown the real identity of the signer complete achieve protect mobile devices privacy during the process of check the integrity of the stored message. However, when there are some malicious mobile devices, the TA can extract the real identity from the pseudo identity of the mobile device.

3) Identity privacy preserving: The real identity of mobile devices are not in any transmitted message. All other mobile devices and any third party except the TA cannot obtain the real identity of the mobile device from the transmitted message.

4) Unforgeability: Mobile devices signature a message and cannot be forged by a third party adversary, satisfy this requirement is easier to achieve retrospect the malicious mobile device.

5) Revocation: After the vehicle found a malicious mobile device, the TA could retrospect malicious mobile device's real identity. That is, TA could revoke malicious mobile device and prevent tampering other valid messages.

6) Unlinkability: An adversary cannot link various relative information to achieve the purpose of tracking mobile device, satisfy this requirement aim to protect mobile device's privacy.

IV. SCHEME

In this section, we aim to propose a novel message authentication scheme for multiple mobile devices in intelligent connected vehicles based on edge computing. The scheme supports the vehicle and multiple mobile devices communication, and it consists of five phases: Setup, Register, Ring signature, Verify, Revocation.

A. SETUP

The TA executes this algorithm to generate system public parameters and the master key and sends system parameters to the vehicle and mobile devices by the secure channel, which are specified describe as follows:

1) Input a security parameter l, then the TA chooses a large prime number $q > 2^l$, and three cyclic multiplicative groups $< G_1, \cdot >, < G_2, \cdot >, < G_T, \cdot >$ respectively.

2) The TA chooses a bilinear pairing $e : G_1 \times G_2 \to G_T$, and Q, P are generators of G_1, G_2 respectively.

3) The TA determines two one way hash functions h and H. $h : \{0,1\}^* \to Z_q^*, H : \left\{G_1, \{0,1\}^*, \{0,1\}^*, G_1^n\right\} \to Z_q^*$.

4) The TA selects a random number $k \in Z_q^*$ as the master key, and generate $PK_{TA} = k \cdot P$ as the public key. Then the TA returns system parameters $(q, P, Q, G_1, G_2, h, H, PK_{TA})$.

B. REGISTER

Mobile devices interact with the TA to execute this algorithm. The TA generates mobile device's pseudonyms and

semi-private key. The algorithm includes four phases: mobile device secret value, mobile device public value, generate pseudonyms and semi-private key extract.

1) MOBILE DEVICE SECRET VALUE

The mobile device i have a trusted execution environment, where pw is the login password, RID_i is the mobile device's real identity. In the trusted execution environment, the mobile device chooses a random number $u \in Z_q^*$ as the mobile device's secret value, where the mobile device sets $SK_{i,1} = u$.

2) MOBILE DEVICE PUBLIC VALUE

The mobile device i computes $PK_i = u \cdot Q$ and sets it as the mobile device's public key.

3) GENERATE PSEUDONYMS

The mobile device i obtains pseudonyms by sent $(RID_i, h(pw \oplus a), PK_i)$ to the TA, where $a \in Z_q^*$ is a large random number was chosen by the mobile device. Then the TA computes:

$$ID_{i,j} = k \times h(Enc_{PK_{TA}}(RID_i) \oplus h(pw \oplus a) \parallel PK_i) + r_j \quad (1)$$

where r_j is a random number $r_j \in Z_q^*$, then the TA computes $R_j = r_j \cdot P \cdot Q$, $j = 1 \ldots p$ it indicates that a mobile device i has p pseudonyms. In order to convenient, we set $\overline{h_i} = Enc_{PK_{TA}}(RID_i) \oplus h(pw \oplus a)$.

Then the TA sends $(ID_{i,j}, \overline{h_i}, R_j)$ to the mobile device simultaneously and the mobile device stores this information in a trusted execution environment, meanwhile the TA stores the $(ID_{i,j}, Enc_{PK_{TA}}(RID_i), h(pw \oplus a)_i, \overline{h_i}, R_j)$ in its remember. When the mobile device received $(ID_{i,j}, \overline{h_i}, R_j)$, the mobile device checks $ID_{i,j}$ firstly, then checks it whether are legitimate:

$$ID_{i,j} \cdot P \cdot Q \stackrel{?}{=} PK_{TA} \cdot Q \cdot h(\overline{h_i} \parallel PK_i) + R_j \quad (2)$$

If the equation is true, the mobile device computes:

$$ID_i = ID_{i,j} + u \cdot P \quad (3)$$

Then the mobile device stores p pseudonyms in a trusted execution environment. In the subsequent sections, it will be as real pseudonyms.

4) SEMI-PRIVATE KEY EXTRACT

The mobile device requests semi-private key extract by the mobile device selects an ID_i and sends (ID_i, PK_i) to the TA, when the TA received the request, firstly, to check the following equation whether is legitimate:

$$ID_i \cdot P \cdot Q \stackrel{?}{=} PK_{TA} \cdot Q \cdot h(\overline{h_i} \parallel PK_i) + R_j + PK_i \cdot P \cdot P \quad (4)$$

If the equation is true, the TA computes:

$$SK_{i,2} = h(ID_i) \cdot k \cdot Q \quad (5)$$

Then send $(ID_i, SK_{i,2})$ to the mobile device. When the mobile device received it and checks:

$$SK_{i,2} \cdot P \stackrel{?}{=} h(ID_i) \cdot PK_{TA} \cdot Q \quad (6)$$

If the equation is true, the mobile device stores $SK_{i,2}$ and sets $SK_i = (SK_{i,1}, SK_{i,2})$ as the mobile device's private key and stores it in a trusted execution environment.

C. RING SIGNATURE

The mobile device executes this algorithm to generate the message signature. The message m is a result of a mobile device to storage or computing task and send it to the vehicle.

1) Input $(m, PK_1, PK_2, \ldots, PK_n, (SK_{s,1}, SK_{s,2}), ID_s)$, for $i \in [1, n]$, $i \neq s$, mobile devices chooses n random numbers, $S_1, S_2, \ldots, S_{s-1}, S_{s+1}, \ldots, S_n \in G_1$.

2) For $i \in [1, n]$, mobile devices compute $h_i = H(S_i, m, ID_s, PK_1, PK_2, \ldots, PK_n)$.

3) The mobile device chooses two random numbers x, $y \in Z_q^*$, and computes $S_s = y \cdot Q + x \cdot SK_{s,2} - \sum_{i \neq s}^{n} (h_i PK_i + S_i)$, $N = (y + h_s \cdot SK_{s,1}) \cdot P$, $L = x \cdot h(ID_s)$. Then return the signature $(S_1, S_2, \ldots, S_n, N, L)$.

D. VERIFY

The vehicle executes this algorithm to check the integrity of the message.

1) Query the revocation list: When the vehicle obtains the pseudonym ID_s corresponding to the signature of the message m, the vehicle makes the query and the vehicle looks up the revocation list. If the pseudonym ID_s exist in the list, the vehicle stops execute this algorithm, else the vehicle does as follows:

2) Input $(S_1, S_2, \ldots, S_n, N, L, m, PK_1, PK_2, \ldots, PK_n, ID_s)$, for $i \in [1, n]$, the vehicle computes $h_i = H(S_i, m, ID_s, PK_1, PK_2, \ldots, PK_n)$.

3) The vehicle checks the equation whether is legitimate:

$$e(Q, N + L \cdot PK_{TA}) \stackrel{?}{=} e(\sum_{i=1}^{n} (h_i PK_i + S_i), P) \quad (7)$$

If the above equation is legitimate, it means that the message m was corrected storage or the calculation task has been finished without tampered and return "true", else return "false".

The verification process as follows:

$$\begin{aligned} e(Q, N + L \cdot PK_{TA}) &= e(Q, (y + h_s \cdot SK_{s,1}) \cdot P + x \cdot h(ID_s) \cdot k \cdot P) \\ &= e(Q \cdot (y + h_s \cdot SK_{s,1} + x \cdot h(ID_s) \cdot k), P) \\ &= e(y \cdot Q + x \cdot SK_{s,2} + h_s \cdot PK_s, P) \\ &= e(\sum_{i \neq s}^{n} (h_i PK_i + S_i) + S_s + h_s \cdot PK_s, P) \\ &= e(\sum_{i=1}^{n} (h_i PK_i + S_i), P) \end{aligned} \quad (8)$$

E. REVOCATION

When the equation (7) returns "true", it means that the message is legal. If the equation (7) returns "false", it means that the message is illegal. The TA is the only authorized entity can execute this algorithm to retrospect the illegal mobile

device and updates the revocation list. After the vehicle sends (m, ID_s) to the TA and the TA computes: $ID_s \cdot P \cdot Q = PK_{TA} \cdot h(\overline{h_i} \parallel PK_s) + R_s + PK_s \cdot P$. If exists a $\overline{h_i}$ satisfies the equation, then the TA can extract the mobile device's real identity by $\overline{h_i} = Enc_{PK_{TA}}(RID_i) \oplus h(pw \oplus c)$. Add the tuple $(RID_i, \{ID_{i,1}, ID_{i,2}, \ldots, ID_{i,p}\})$ into the list, where p represents the TA generates p pseudonym identities for the mobile device i. Next, the TA updates the revocation list and sends it to the vehicle.

There is a problem of inefficiency in this scheme. In the next section, we present an improved scheme. In order to improve the efficiency of detection, when the vehicle receives multiple messages and needs to be detected, batch verify is used and as long as the detection once time, which greatly improves the efficiency.

V. IMPROVED SCHEME

If the vehicle needs to couple many information and separate different tasks to different mobile devices and mobile devices couple these tasks simultaneously, in order to improve verify results with efficiency, we propose the second scheme, which is an improved scheme and batch detection message has been implemented. It consists of five phases: Setup, Register, Ring signature, Verify, Revocation. (The improved scheme and the previous scheme are the same in the Setup, Register and Ring signature phases, so no longer write in the following.)

A. IMPROVED VERIFY

The vehicle executes this algorithm to checks the integrity of the aggregated message M. The message M is aggregated from the relevant parameters of the chosen c messages. Therefore, the vehicle only executes the verification phase once time. Improved the efficiency of the verification phase.

1) Aggregate: The vehicle chooses c messages to aggregate a message M and other relative parameters: $S_1 = \sum_{i=1}^{c} r_i \cdot S_{i,1}$, $S_2 = \sum_{i=1}^{c} r_i \cdot S_{i,2}$, $\cdots$, $S_n = \sum_{i=1}^{c} r_i \cdot S_{i,n}$, $N = \sum_{i=1}^{c} r_i \cdot N_i$, $L = \sum_{i=1}^{c} r_i \cdot L_i$, $M = \sum_{i=1}^{c} r_i \cdot m_i$, $ID_s = \sum_{i=1}^{c} r_i \cdot ID_{s_i}$ and return the signature $(S_1, S_2, \ldots, S_n, N, L)$.

2) Query the revocation list: When the vehicle obtains the aggregated pseudonym ID_s corresponding to the signature of the message M, the vehicle makes the query and the vehicle looks up the revocation list. If the pseudonym ID_s exist in the list, the vehicle stops execute this algorithm, else the vehicle does as follows:

3) Input $(M, PK_1, PK_2, \ldots, PK_n, ID_s, S_i)$, the vehicle computes $h_i = H(S_i, M, ID_s, PK_1, PK_2, \ldots, PK_n)$.

4) The vehicle checks the equation whether is legitimate:

$$e(Q, N + L \cdot PK_{TA}) \stackrel{?}{=} e(\sum_{i=1}^{n} (h_i PK_i + S_i), P) \tag{9}$$

If the above equation is legitimate, it means that the aggregated message M was corrected storage or the calculation task has been finished without tampered and return "true", else return "false".

The verification process as follows:

$$\begin{aligned} & e(Q, N + L \cdot PK_{TA}) \\ &= e(Q, \sum_{i=1}^{c} r_i \cdot (y + h_{i,s} \cdot SK_{s_i,1} + x \cdot h(ID_{s_i}) \cdot k \cdot P)) \\ &= e(\sum_{i=1}^{c} r_i \cdot (y \cdot Q + x \cdot SK_{s_i,2} + h_{i,s} \cdot PK_{s_i}), P) \\ &= e(\sum_{i=1}^{c} r_i \cdot (\sum_{j \neq s}^{n} (h_{i,j} \cdot PK_j + S_{i,j}) + S_{i,s} + h_{i,s} \cdot PK_{s_i}), P) \\ &= e(\sum_{i=1}^{n} (h_i PK_i + S_i), P) \end{aligned} \tag{10}$$

When the equation (9) returns "true", it means that the aggregated message is legal. If the equation (9) return "false", it means that the aggregated message M is illegal. That is existing malicious mobile devices in all mobile devices. We can retrospect the illegal mobile devices by the binary search $(ID_s, (ID_{s_1}, ID_{s_2}, \ldots, ID_{s_c}))$ (It indicates the identity of the mobile device corresponding to the i messages and $i \in [1, c]$, c represents the message M is aggregated from c messages.) to identify the specific mobile device who cause the aggregated message M is illegal. Then the vehicle return (M, PK_{s_i}, ID_{s_i}) to the TA, where ID_{s_i} is the malicious mobile device's a pseudonym identity.

B. IMPROVED REVOCATION

The TA is the only authorized entity can execute this algorithm to retrospect the illegal mobile device and updates the revocation list. When the TA received the tuple (M, PK_{s_i}, ID_{s_i}) and computes: $ID_{s_i} \cdot P \cdot Q = PK_{TA} \cdot h(\overline{h_{s_i}} \parallel PK_{s_i}) + R_{s_i} + PK_{s_i} \cdot P$. If exists a $\overline{h_{s_i}}$ satisfy the equation, then the TA can extract the mobile device's real identity by $\overline{h_{s_i}} = Enc_{PK_{TA}}(RID_{s_i}) \oplus h(pw \oplus c)$. Add the tuple $(RID_i, ID_s, \{ID_{i,1}, ID_{i,2}, \ldots, ID_{i,p}\})$ into the list, where p is represents the TA generates p pseudonym identities for the mobile device i. Next, the TA updates the revocation list and sends it to the vehicle.

VI. SECURITY ANALYSIS

In this section, we analyze the security of the proposed two schemes.

A. SECURITY MODEL

A certificateless cryptography scheme exists two type adversaries. Type I adversary A_1 does not know the system master key but can replace the mobile device's public key. Type II adversary A_2 knows the system master key, but cannot replace the target mobile device's public key. According to the ability of the adversary can be divided into a normal adversary, a strong adversary, and a super adversary. Our scheme resists super adversaries, which are defined the game between the two types adversaries and the challenger C. C executes the

Setup algorithm to generate system parameters and the master key. Then, if the inquirer is a type I adversary, C returns the system parameters; else, returns the system parameters and the master key. An adversary could access the following random oracles:

1) *Mobile device secret value oracle*: Upon receiving a query with the real identity RID_i of the adversary A, the challenger C returns secret key $SK_{i,1}$ to A.

2) *Mobile device public key replacement oracle*: When A makes the query of the public key with the real identity RID_i and PK_i, then C returns the replaced public key PK_i^* to A.

3) *Generate pseudonyms oracle*: A makes the query of the pseudonym with the real identity RID_i, C returns ID_i to A.

4) *Semi-private key extract oracle*: Upon receiving a query of the adversary A with pseudonym ID_i, C returns semi-private key $SK_{i,2}$ to A.

5) *Signature oracle*: Upon receiving a request with pseudonym ID_i and message m_i to execute the signature, then C returns $(ID_i, m_i, (S_1, S_2, \ldots, S_n, N, L)$ to A.

Finally, the adversary A outputs $(m_i{}^*, (S_1{}^*, S_2{}^*, \cdots S_n{}^*, N^*, L^*))$. The adversary wins the game if the following conditions are met:

1) Verify $(ID_i{}^*, m_i{}^*, PK_i{}^*, (S_1{}^*, S_2{}^*, \cdots S_n{}^*, N^*, L^*)$ is true;

2) For the type I adversary, $ID_i{}^*$ has never been sent to the semi-private key oracle, otherwise, $ID_i{}^*$ has never been sent to the secret value oracle.

B. SECURITY PROOF

This section aims to proof our schemes are secure under two type adversaries in the random oracle environment. In the process, there are two parties to participate: the adversary A and the challenger C.

Lemma 1: Our proposed scheme is secure against type I adversary if solve the co-CDHP is difficult.

Proof: Assume the adversary A could successfully forge a signature of the message and the challenger C can call the adversary A's attack algorithm to output the solution of the co-CDH problem. In this process, the adversary A could execute the following queries:

H query: The challenger C maintains a list L_H, it consists of a tuple $(S_i, m, ID_s, PK_1, PK_2, \ldots, PK_n, H_i)$ and initializes it to empty. When receiving a query $(S_i, m, ID_s, PK_1, PK_2, \ldots, PK_n)$, C checks whether exist the tuple $(S_i, m, ID_s, PK_1, PK_2, \ldots, PK_n, H_i)$ in the list L_H. If so, C return the H_i to A, else C generates a random number $H_i \in Z_q^*$ and returns it to A.

h query: C maintains a list L_h, it consists of a tuple (ID_i, h_i) and initializes it to empty. When receiving a query ID_i, C checks whether exist the tuple (ID_i, h_i) in the list L_h. If so, C returns the h_i to A, else C generates a random number $h_i \in Z_q^*$ and returns it to A.

Register query: 1) *Mobile device secret value*: C maintains a list $L_K(ID_i, SK_{i,1}, SK_{i,2}, PK_i)$, and initializes it to empty. When A makes the query, C checks the tuple $(ID_i, SK_{i,1}, SK_{i,2}, PK_i)$ in the list L_K and returns $SK_{i,1}$ to A.

2) *Mobile device public key replacement*: When A makes the query of the public key, C checks the tuple $(ID_i, SK_{i,1}, SK_{i,2}, PK_i)$ in the list L_K and return the replaced PK_i^* to A.

3) *Generate pseudonyms*: A makes the query of the pseudonym, C checks the tuple $(ID_i, SK_{i,1}, SK_{i,2}, PK_i)$ in the list L_K, if existing, returns ID_i to A, otherwise, C aborts the game.

4) *Semi-private key extract*: C checks the tuple $(ID_i, SK_{i,1}, SK_{i,2}, PK_i)$ in the list L_K firstly, if existing, return $SK_{i,2}$ to A, otherwise, C aborts the game.

Signature query: Upon receiving a message m request to execute the signature algorithm, the adversary A calls the forge algorithm to generate the signature.

1) For $i \in [1, n]$, $i \neq s$, A chooses n-1 random numbers, $S_1, S_2, \ldots, S_{s-1}, S_{s+1}, \ldots, S_n \in G_1$.

2) The mobile device chooses two random numbers x, $y \in Z_q^*$, executes h query and H query respectively. Then computes $S_s = y \cdot Q + x \cdot SK_{s,2} - \sum_{i \neq s}^{n} (h_i PK_i + S_i)$, $N = (y + h_s \cdot SK_{s,1}) \cdot P$, $L = x \cdot h(ID_s)$, and returns the signature $(S_1^*, S_2^*, \ldots, S_n^*, N^*, L^*)$.

Input the forge signature $(S_1^*, S_2^*, \ldots, S_n^*, N^*, L^*)$ into the verify equation. The challenger C can get the following equation:

$$\begin{aligned} & e(Q, N^* + L \cdot PK_{TA}) \\ &= e(Q, (y + h_s^* \cdot SK_{s,1}) \cdot P + x \cdot h(ID_s) \cdot k \cdot P) \\ &= e(Q \cdot (y + h_s^* \cdot SK_{s,1} + x \cdot h(ID_s) \cdot k), P) \\ &= e(y \cdot Q + x \cdot SK_{s,2} + h_s^* \cdot PK_s, P) \\ &= e(\sum_{i \neq s}^{n} (h_i PK_i + S_i) + S_s + h_s^* \cdot PK_s, P) \end{aligned} \tag{11}$$

Finally: the challenger C could obtain two signatures of the message m, for $i \in [1, n]$, $i = s$, $h_i \neq h_i^*$, according to the equations (8), (11) and computes (8)/(11) as follows:

$$\begin{aligned} e(N - N^*, Q) &= e((h_s - h_s^*) \cdot PK_s, P) \\ &= e((h_s - h_s^*) \cdot u \cdot Q), P) \\ &= e((h_s - h_s^*) \cdot u \cdot P, Q) \end{aligned} \tag{12}$$

According to the equation (12) we can obtains:

$$\begin{aligned} N - N^* &= (h_s - h_s^*) \cdot u \cdot P \\ u \cdot P &= (N - N^*)/(h_s - h_s^*) \end{aligned}$$

The challenger C could outputs $u \cdot P$ indicates that C could solve the co-CDHP. We assume to solve the co-CDHP is hard, so our proposed scheme is secure in the random oracle.

Lemma 1:* Our proposed the improved scheme is secure against type I adversary if solve the co-CDHP is difficult.

Proof: As it does the previous lemma 1, A and C are the parties to do the game, besides the previous queries A also calls the following query:

Improved Signature query: Upon receiving multiple messages m_i requests to execute the signature algorithm,

where $i \in [1, c]$, the adversary A calls the forge algorithm to generate the signature.

1) For $i \in [1, n], i \neq s$, A chooses n-1 random numbers, $S_{i,1}, S_{i,2}, \ldots, S_{i,s-1}, \ldots, S_{i,s+1}, \ldots, S_{i,n} \in G_1$.

2) The mobile device chooses two random numbers x, $y \in Z_q^*$, executes h query and H query respectively. Then computes $S_{i,s} = y \cdot Q + x \cdot SK_{s_i,2} - \sum_{j \neq s}^{n} (h_{i,j} PK_j + S_{i,j})$, $N_i = (y + h_{i,s} \cdot SK_{s_i,1}) \cdot P$, $L_i = x \cdot h(ID_{s_i})$.

For c messages, the vehicle aggregates a message M and other relative parameters: $S_1 = \sum_{i=1}^{c} r_i \cdot S_{i,1}$, $S_2 = \sum_{i=1}^{c} r_i \cdot S_{i,2}$, $\cdots$, $S_n = \sum_{i=1}^{c} r_i \cdot S_{i,n}$, $N = \sum_{i=1}^{c} r_i \cdot N_i$, $L = \sum_{i=1}^{c} r_i \cdot L_i$, $M = \sum_{i=1}^{c} r_i \cdot m_i$, then return the signature $(S_1^*, S_2^*, \ldots, S_n^*, N^*, L^*)$.

Input the forge signature $(S_1^*, S_2^*, \ldots, S_n^*, N^*, L^*)$ into the verify equation. The challenger C can get the following equation:

$$\begin{aligned} & e(Q, N^* + L \cdot PK_{TA}) \\ &= e(Q, \sum_{i=1}^{c} r_i \cdot (y + h_{i,s}^* \cdot SK_{s_i,1} + x \cdot h(ID_{s_i}) \cdot k \cdot P)) \\ &= e(\sum_{i=1}^{c} r_i \cdot (y \cdot Q + x \cdot SK_{s_i,2} + h_{i,s}^* \cdot PK_{s_i}), P) \\ &= e(\sum_{i=1}^{c} r_i \cdot (\sum_{j \neq s}^{n} (h_{i,j} \cdot PK_j + S_{i,j}) + S_{i,s} + h_{i,s}^* \cdot PK_{s_i}), P) \end{aligned} \quad (13)$$

Finally: the challenger C could obtain two signatures of the message M, for $i \in [1, n]$, $i = s$, $h_{i,s} \neq h_{i,s}^*$, according to the equations (10), (13) and computes (10)/(13) as follows:

$$\begin{aligned} e(N - N^*, Q) &= e((h_{i,s} - h_{i,s}^*) \cdot PK_s, P) \\ &= e((h_{i,s} - h_{i,s}^*) \cdot u \cdot Q), P) \\ &= e((h_{i,s} - h_{i,s}^*) \cdot u \cdot P, Q) \end{aligned} \quad (14)$$

According to the equation (14) we can obtains:

$$\begin{aligned} N - N^* &= (h_{i,s} - h_{i,s}^*) \cdot u \cdot P \\ u \cdot P &= (N - N^*)/(h_{i,s} - h_{i,s}^*) \end{aligned}$$

The challenger C could outputs $u \cdot P$ indicates that C could solve the co-CDH problem. We assume to solve the co-CDHP is hard, so our proposed the improved scheme is secure against type *I* adversary in the random oracle.

Lemma 2: Our proposed scheme is secure against type *II* adversary if solve the co-CDHP is hard.

Proof: The adversary A is an insider attacker from the TA in the register. We aim to proof our scheme is secure against the second adversary, so assume A could access the system master key, but cannot replace the target mobile device's public key. Set the challenger C's identity is RID^* and maintains three tables $L_h(RID_i, H_i, Z_i, PK_i, b)$, $L_k(RID_i, SK_{i,1}, SK_{i,2}, PK_i)$, $L_{TA}(RID_i, k)$, where initialize it to empty.

h query: When A make the query of (RID_i, H_i, PK_i), then C checks the list L_h whether exist the tuple, if so, return Z_i, else, C generates a random number $b \in \{0, 1\}$, if $b = 0$ indicates the challenger C's identity and RID_i are the same and chooses a random number $R \leftarrow Z_i$ and return it to the A.

Master key query: When A make the query, C checks the list L_h, if $b = 1$, C chooses a random number $K_{i,1} \leftarrow u$ and computes $PK_i = u \cdot Q$, then C return $(RID_i, SK_{i,1}, \perp, PK_i)$, (RID_i, kt) to L_k and L_{TA} respectively, and return s to the TA. If $b = 0$, C return $(RID_i, \perp, \perp, PK_i)$, (RID_i, s) to L_k and L_{TA} respectively, and return s to the TA.

Semi-private key query: Upon receiving the query, C checks the list L_h, if $b = 0$, aborts the game, otherwise, C checks the list L_K, if the tuple is existing and return it to the A, else C makes a Master key query, then return $SK_{i,1}$ to the A.

Pseudonym identity query: When A makes the query of the identity, C checks the list L_h, if $b = 0$, aborts the game, otherwise, C chooses three random number $u, d_i, ID_i \in Z_q^*$, and computes $PK_i = u \cdot Q$, $h_i \leftarrow d_i$, $R_i = ID_i \cdot P \cdot Q - h_i \cdot Q - PK_i \cdot P \cdot P$, then return the tuple (ID_i, h_i, R_i, PK_i) to A.

Finally, According to [25], A can forge a pseudonym identity with the different coefficient t of PK_i:

$$ID_i \cdot P \cdot Q = h_i \cdot Q + R_i + PK_i \cdot P \cdot P \quad (15)$$

$$ID_i^* \cdot P \cdot Q = h_i \cdot Q + R_i + m \cdot PK_i \cdot P \cdot P \quad (16)$$

According to the equations (15) and (16), we can obtain:

$$\begin{aligned} (ID_i - ID_i^*) \cdot Q &= (1 - m) \cdot u \cdot P \cdot Q \\ u \cdot P &= (ID_i - ID_i^*)/(1 - m) \end{aligned}$$

The challenger C could output $u \cdot P$ indicates that C could solve the co-CDH problem. We assume to solve the co-CDHP is hard, so our proposed scheme is secure against type *II* adversary in the random oracle. The improved scheme and the previous scheme proof process are same and not write it here.

C. OTHER DISCUSSIONS

1) MESSAGE AUTHENTICATION AND INTEGRITY

The proposed scheme is a message authentication scheme based on certificateless ring signature. The vehicle verifies the message signed by multiple mobile devices before receiving the message. Therefore, the integrity of the message received by the vehicle is guaranteed.

2) CONDITIONAL PRIVACY PRESERVING

In our proposed scheme, the pseudonym of each mobile device includes the TA's master key k and the mobile device's own semi-private key u. The master key and the semi-private key are known only to the TA and the mobile device, respectively. Therefore, it is impossible for any adversary to calculate the pseudonym. When a malicious mobile device appears, the TA can obtain the real identity of the mobile device by calculating: $\overline{h_i} = Enc_{PK_{TA}}(RID_i) \oplus h(pw \oplus a)$.

3) IDENTITY PRIVACY PRESERVING

Each mobile device in the proposed scheme communicates with the vehicle under a pseudonym, where $ID_{i,j} = k \times h(Enc_{PK_{TA}}(RID_i) \oplus h(pw \oplus a) \parallel PK_i) + r_j$, $ID_i = ID_{i,j} + u \cdot P$. The message transmitted by the communication does not contain the true identity of the mobile device, which cannot be obtained by other mobile devices or any third party from the pseudonym.

4) UNFORGEABILITY

Through the proof of Lemma 1 and Lemma 1*, we can obtain a conclusion that the proposed scheme is unforgeability.

5) REVOCATION

when the vehicle founds a malicious mobile device, by executing the revocation algorithm, then could extract its real identity of the TA, so, the proposed scheme is satisfied revocation.

6) UNLINKABILITY

The pseudonym identity generated by the equation $ID_{i,j} = k \times h(Enc_{PK_{TA}}(RID_i) \oplus h(pw \oplus a) \parallel PK_i) + r_j, ID_i = ID_{i,j} + u \cdot P$, where r_j is a random number, any adversary cannot link various relative information to achieve the purpose of tracking mobile devices, so, the proposed scheme is to satisfy unlinkability.

VII. PERFORMANCE ANALYSIS

In this section, we specific analysis of the performance of the proposed MA-DVEC scheme and the improved scheme. In order to have better credibility, we compare the performance of the proposed two schemes with [14] and [26], [27]. To demonstrate the efficiency of our message authentication scheme, we use the simulation parameters in [28]. In one area of the network, a service provider manages 5 small edge areas, each of which has 8 GHz/ea computing resources through multiple mobile devices. Generally, the computer runs in 4G memory to simulate the computing resources of a vehicle. In 5 edge regions, the computational task scheduling of vehicles is similar to the computational task migration in [29].

A. COMPUTATION COST ANALYSIS

We use a bilinear pairing: $\overline{e} : G_2 \times G_2 \rightarrow G_T$, which can reach 80 bits security levels for identity-based schemes. G_2 is a cyclic multiplication group generated by the generator P with the order is q, where P and q are two prime number, 512 bits, and 160 bits respectively. For our proposed schemes based on bilinear pairing, we use a bilinear pairing: $e : G_1 \times G_2 \rightarrow G_T$, where G_1 is a cyclic multiplication group generated by the generator Q with the order is q, where Q is a prime number of 128 bits. As shown in TABLE 1, which the platform of 3.4GHZ i7-4770 [30], we can obtain basic cryptographic operations execution time by using MIRACL library [32].

TABLE 1. Cryptographic operation time.

Cryptographic operation	Symbol	Time(ms)
A bilinear pairing operation	T_{bp}	4.211
A bilinear pairing scale multiplication operation	T_{bp-m}	1.709
The small scale multiplication operation of a bilinear pairing	T_{bp-sm}	0.054
The point addition operation of a bilinear pairing	T_{bp-a}	0.007
A bilinear pairing hash-point operation	T_H	4.406
A generic hash function operation	T_h	0.0001

According to the cryptographic operation type and processing efficiency in each algorithm, compare the time cost for five schemes in the signature phase, verify a single message and batch verification messages, as shown in TABLE 2. In order to more intuitively show the effect of the number of messages on the delay and we made three figures, where FIGURE 3. is compared execution time in the signature phase, FIGURE 4. is compared execution time in the verification phase and FIGURE 5. is compared execution time for the batch authentication.

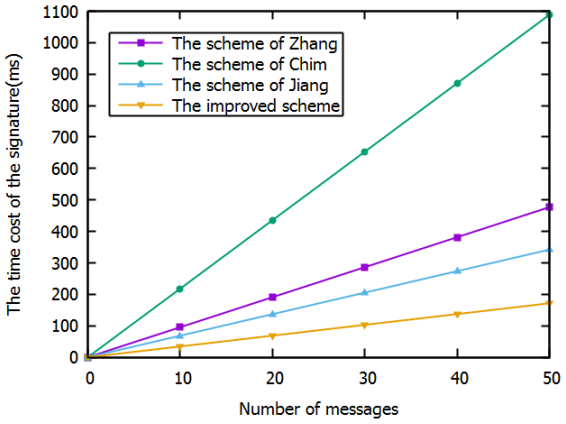


FIGURE 3. Comparison of execution time in the signature phase.

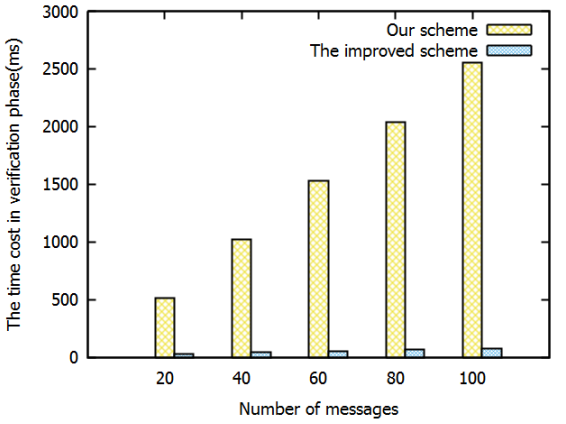


FIGURE 4. Comparison of execution time in the verification phase.

TABLE 2. comparisons the performance time for five schemes.

Scheme	Signature(ms)	Verify a single message(ms)	Verify c messages(ms)
Scheme [26]	$T = m(5T_{bp-m} + 3T_H + T_{bp-a}) \approx 21.77m$	$T = 2T_{bp} + 2T_{bp-m} + T_H \approx 16.246$	$T = 2T_{bp} + 2cT_{bp-m} + cT_H \approx 7.824c + 8.422$
Scheme [27]	$T = m(4T_{bp-m} + T_{bp-a} + T_h) \approx 6.843m$	$T = 3T_{bp} + 2T_{bp-m} + T_{bp-a} + 2T_h \approx 16.052$	$T = 3T_{bp} + (c+1)T_{bp-m} + (3c-2)T_{bp-a} + 2cT_h \approx 1.7302c + 12.633$
Scheme [14]	$T = m(2T_{bp-m} + T_{bp-a} + T_H) \approx 7.831m$	$T = 2T_{bp} + T_{bp-a} + T_H \approx 14.544$	$T = 2T_{bp} + (3c+1)T_{bp-sm} + cT_H \approx 4.568c + 8.429$
Our first scheme	$T = m((n+5)T_{bp-m} + (n+1)2T_{bp-a} + (n+1)T_h)) \approx 1.716mn$	$T = 2T_{bp} + (n+1)T_{bp-m} + nT_h \approx 1.7091n + 8.422$	$T = c(2T_{bp} + (n+1)T_{bp-m} + nT_h) \approx c(1.7091n + 8.422)$
Our second scheme	$T = m((n+5)T_{bp-m} + (n+1)2T_{bp-a} + (n+1)T_h)) \approx 1.716mn$	$T = 2T_{bp} + (n+1)T_{bp-m} + nT_h \approx 1.7091n + 8.422$	$T = (n+4)c(T_{bp-sm} + T_{bp-a}) + 2T_{bp} + (n+1)T_{bp-m} + nT_h \approx (0.061c + 1.716)n$

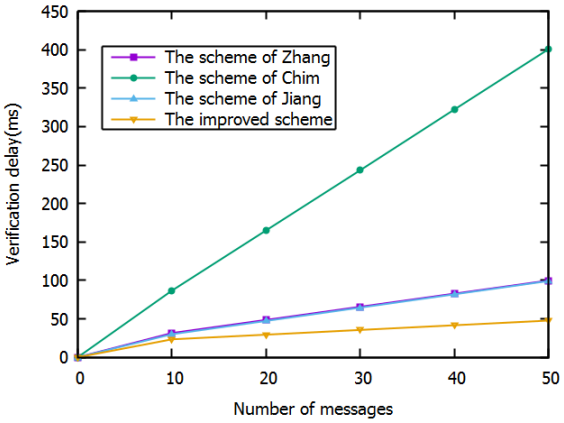


FIGURE 5. Comparison of execution time for the batch verification.

In the signature phase, since the computational costs of the two schemes proposed in the paper are the same, only one of them is represented in the figure. Therefore, we will compare the proposed improvement scheme with [14], [26], [27]. The comparison results of the four schemes are shown in FIGURE 3., we can see that the Jiang *et al.*'s [27] execution time is less than the Horng *et al.*'s [14] and the Chim *et al.*'s [26] in the signature phase and our proposed schemes performance time are a little better than [14], [26], [27]. The computational efficiency of our second scheme in this phase has been improved 84.24% than [26], higher 49.85% than [27] and higher 56.17% than [14].

In FIGURE 4., we compared the previous scheme of this paper cannot implement batch authentication and the improved scheme of achieving batch authentication. It is explained that the efficiency of the scheme implements batch authentication is far higher than the general message authentication scheme.

For the schemes of Chim *et al.* [26], Jiang *et al.* [27], Horng *et al.* [14] and our propose the improved scheme are achieved batch authentication. We set c to denote the number of signatures aggregated by the vehicle. In order to improve the efficiency of message authentication, let the number of aggregated signatures is equal to the total number of messages, where m represents the number of messages. Because the previous scheme in this paper did not implement batch authentication, therefore, comparison of execution time for the batch verification of four schemes is shown in FIGURE 5. We can see from the figure, the Jiang *et al.*'s [27] execution time is more than the Chim *et al.*'s [26] and the Horng *et al.*'s [14] in the batch authentication phase, our proposed schemes performance time are better than [14], [26] and [27]. The computational efficiency of our second scheme in this phase has been improved 82.19% than [26], superior 37.85% than [27] and higher 70.58% than [14].

TABLE 3. comparisons of communication overhead for five schemes.

Scheme	Message	The length of the message(bytes)
Scheme [26]	$\{ID_i, M_i, \sigma_i\}$	384
Scheme [27]	$\{M, tt, ID, Y\}$	408
Scheme [14]	$\{ID_i, M_i, \sigma_i, T_i\}$	388
Our first scheme	$\{ID_i, M, (S_1, S_2, \cdots, S_n, N, L), (PK_1, PK_2, \cdots, PK_n)\}$	128+64n
Our second scheme	$\{ID_i, M, (S_1, S_2, \cdots, S_n, N, L), (PK_1, PK_2, \cdots, PK_n)\}$	128+64n

B. COMMUNICATION COST ANALYSIS

In this subsection, we analyze the communication cost for five schemes. Since the length of P,Q are 512 bits, 128 bits respectively, so the length of elements of G_1, G_2 corresponding to 32 bytes, 128 bytes. We set timestamp is 4 bytes, a generic hash function output value is 20 bytes. TABLE 3 shows communication overhead of five schemes.

For the scheme of the proposed of the Chim *et al.*'s [26], the verifier received the pseudonym identity, message, and signature $\{ID_i, M_i, \sigma_i\}$ from the vehicle, where $ID_i = \{ID_i^1, ID_i^2\}$, and $ID_i^1, ID_i^2, \sigma_i \in G_2$. Therefore, the communication cost is $128 \times 3 = 384$ *bytes*. For the scheme of the proposed of the Jiang *et al.*'s [27], the verifier received

message, timestamp, the pseudonym identity, and signature $\{M, tt, ID, Y\}$ from the vehicle, where the pseudonym identity is $ID = H_3(S_{1,j} \oplus S_{2,C-j+1})$ equals to 20 bytes, $Y = (T, U, W)$ is signature and $T, U, W \in G_2$, and tt is 4 bytes and denotes timestamp. Therefore, the communication cost is $128 \times 3 + 20 + 4 = 408$ *bytes*. For the scheme of the proposed of the Horng *et al.*'s [14], the verifier received the pseudonym identity, message, signature and timestamp $\{ID_i, M_i, \sigma_i, T_i\}$ from the vehicle, where $ID_i = \{ID_i^1, ID_i^2\}$, and $ID_i^1, ID_i^2, \sigma_i \in G_2$, T_i is 4 bytes and denotes timestamp. Therefore, the communication cost is $128 \times 3 + 4 = 388$ *bytes*. For the proposed two schemes in this paper, the vehicle received the pseudonym identity, message, signature, and public key $\{ID_i, M, (S_1, S_2, \ldots, S_n, N, L), (PK_1, PK_2, \ldots, PK_n)\}$, where $S_i, PK_i \in G_1$, $ID_i \in G_2$. Therefore, the communication cost is $128 + 64n$ *bytes*.

The communication overhead of the two schemes proposed in this paper is the same and compared with [14], [26], [27] are reduced corresponding to 50%, 52.94%, 50.52%, where these percentage results are in the case of n = 1, as the number of n increases, the communication cost of our proposed schemes will also increase. Compared with [14], [26], [27], our second scheme is to provide high security in a high-bandwidth environment with a small communication cost and our schemes are guaranteed the privacy of mobile devices.

VIII. CONCLUSION

It is very important to improve the efficiency of message authentication in intelligent connected vehicles. In this paper, we propose the MA-DVEC scheme. By introducing edge computing, vehicles can send messages to mobile devices for processing data instead of sending them to the cloud for centralized processing. The secure communication between vehicle and multiple mobile devices is realized by certificateless ring signature technology. The security analysis shows that we can prove that our proposed two schemes are secure under the random oracle model and can resist two types of adversaries under certificateless public key encryption. The performance analysis supports that the improved scheme is better than traditional schemes and improves the efficiency of message authentication. Therefore, the improved scheme is more suitable for deployment in intelligent connected vehicles.

ACKNOWLEDGMENT

The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

REFERENCES

[1] S. Brechtel, T. Gindele, and R. Dillmann, "Probabilistic decision-making under uncertainty for autonomous driving using continuous POMDPs," in *Proc. 17th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2014, pp. 392–399.

[2] E. Galceran, A. G. Cunningham, R. M. Eustice, and E. Olson, "Multipolicy decision-making for autonomous driving via changepoint-based behavior prediction: Theory and experiment," in *Robot., Sci. Syst.*, vol. 41, no. 6, pp. 1367–1382, 2015.

[3] Q. Zhang, Y. Wang, X. Zhang, L. Liu, X. Wu, W. Shi, and H. Zhong, "OpenVDAP: An open vehicular data analytics platform for CAVs," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. 1310–1320.

[4] Q. Zhang, Z. Yu, W. Shi, and H. Zhong, "Demo abstract: Evaps: Edge video analysis for public safety," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Oct. 2016, pp. 121–122.

[5] Q. Zhang, Q. Zhang, W. Shi, and H. Zhong, "Distributed collaborative execution on the edges and its application to AMBER Alerts," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3580–3593, Oct. 2018.

[6] Y. Kuwata, J. Teo, G. Fiore, S. Karaman, E. Frazzoli, and J. P. How, "Real-time motion planning with applications to autonomous urban driving," *IEEE Trans. Control Syst. Technol.*, vol. 17, no. 5, pp. 1105–1118, Sep. 2009.

[7] M. Armbrust, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[8] Y.-C. Wei, Y.-M. Chen, and H.-L. Shan, "Rssi-based user centric anonymization for location privacy in vehicular networks," in *Proc. Int. Workshop Secur. Emerg. Wireless Commun. Netw. Syst.*, vol. 42, 2009, pp. 39–51.

[9] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," *IEEE Syst. J.*, vol. 12, no. 1, pp. 64–73, Mar. 2018.

[10] S. Dietzel, J. Petit, F. Kargl, and B. Scheuermann, "In-network aggregation for vehicular ad hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1909–1932, 4th Quart., 2014.

[11] D. He, S. Zeadally, N. Kumar, and W. Wu, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2052–2064, Sep. 2016.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, 1984, pp. 47–53.

[13] M. C. Gorantla, R. Gangishetti, and A. Saxena, "A survey on ID-based cryptographic primitives," *IACR Cryptol. ePrint Arch.*, vol. 2005, p. 94, 2005.

[14] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "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] C. Meshram, "An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem," *Inf. Process. Lett.*, vol. 115, no. 2, pp. 351–358, Feb. 2015.

[16] D. Tiwari, M. Bhushan, A. Yadav, and S. Jain, "A novel secure authentication scheme for VANETs," in *Proc. 2nd Int. Conf. Comput. Intell. Commun. Technol. (CICT)*, Feb. 2016, pp. 287–297.

[17] S. Wang and N. Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs," *Comput. Commun.*, vol. 112, pp. 154–164, Nov. 2017.

[18] S. Biswas, J. Mišić, and V. Mišić, "An identity-based authentication scheme for safety messages in WAVE-enabled VANETs," *Int. J. Parallel Emergent Distrib. Syst.*, vol. 27, no. 6, pp. 541–562, 2012.

[19] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2003, pp. 452–473.

[20] A. W. Dent, "A survey of certificateless encryption schemes and security models," *Int. J. Inf. Secur.*, vol. 7, no. 5, pp. 349–377, 2008.

[21] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signatures secure against realistic adversaries," *J. Supercomput.*, vol. 55, no. 2, pp. 173–191, Feb. 2011.

[22] C. Li, X. Zhang, H. Wang, and D. Li, "An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks," *Sensors*, vol. 18, no. 1, p. 194, 2018.

[23] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.

[24] 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.*, vol. 20, no. 5, pp. 1621–1632, May 2018.

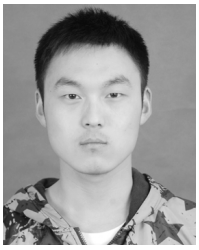
[25] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000.

[26] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "SPECS: Secure and privacy enhancing communications schemes for VANETs," *Ad Hoc Netw.*, vol. 9, no. 2, pp. 189–203, 2011.

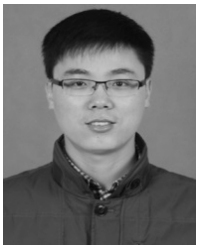
[27] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.
[28] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.
[29] Z. Wang, Z. Zhao, G. Min, X. Huang, Q. Ni, and R. Wang, "User mobility aware task assignment for mobile edge computing," *Future Gener. Comput. Syst.*, vol. 85, pp. 1–8, Aug. 2018.
[30] 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.
[31] 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.
[32] Shamus Software Ltd. *MIRACL Library*. Accessed: May 19, 2014. [Online]. Available: http://www.shamus.ie/index.php?page=home

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, in 2005. She is currently a Professor and a Ph.D. Supervisor with the School of Computer Science and Technology, Anhui University. Her research interests include applied cryptography, the IoT security, vehicular ad hoc networks, cloud computing security, and software-defined networking (SDN). She has more than 120 scientific publications in reputable journals (e.g., the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 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 and, the IEEE INTERNET OF THINGS JOURNAL), academic books, and international conferences.

LEI PAN is currently a Research Student with the School of Computer Science and Technology, Anhui University. Her research interest includes vehicle ad hoc networks.



QINGYANG ZHANG is currently pursuing the Ph.D. degree with the School of Computer Science and Technology, Anhui University, Hefei, China. His research interests include edge computing and security protocol for wireless networks.



JIE CUI was born in Henan, China, in 1980. He received the Ph.D. degree from the University of Science and Technology of China, in 2012. He is currently an Associate Professor and a Ph.D. Supervisor with the School of Computer Science and Technology, Anhui University. His current research interests include applied cryptography, the IoT security, vehicular ad hoc networks, cloud computing security, and software-defined networking (SDN). He has more than 80 scientific publications in reputable journals (e.g., the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 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, and the IEEE INTERNET OF THINGS JOURNAL), academic books, and international conferences.