CPAHP: Conditional Privacy-Preserving Authentication Scheme With Hierarchical Pseudonym for 5G-Enabled IoV

Jingwei Liu, *Member, IEEE*, Chuntian Peng, Rong Sun, *Member, IEEE*, Lei Liu, *Member, IEEE*, Ning Zhang, *Senior Member, IEEE*, Schahram Dustdar, *Fellow, IEEE*, and Victor C. M. Leung, *Life Fellow, IEEE*

***Abstract*—As a representative application scenario of the Internet of Things (IoT), the Internet of Vehicles (IoV) plays an important function in the area of intelligent transportation. However, data traffic exchanged in IoV is usually correlated with plenty of sensitive information, thus leading to privacy leakage. Nevertheless, if all personal data about vehicles are completely protected, it will be hard to trace the real identities of malicious vehicles, which also raises other security issues in IoV. In addition, existing schemes are not fully suitable for 5G-enabled IoV due to their complex structure and high computation requirements. In order to realize more efficient communication and anonymous authentication of vehicles with superior security, we propose a conditional privacy-preserving authentication scheme with hierarchical pseudonyms (CPAHP) in 5G-enabled IoV, which is based on the elliptic curve Diffie-Hellman (ECDH) problem. Through the hierarchical pseudonym mechanism, CPAHP can protect the real identities and movement tracks of vehicles. Whereas, if vehicles have malicious behaviors, their real identities can be recovered through the corresponding pseudonyms. Furthermore, by taking advantage of a batch verification method, receivers can easily cope with a huge influx of messages in a short space of time. Moreover, by introducing blockchain technology, traffic information can be shared smoothly among all vehicles. Through the security analysis and performance evaluation, it is demonstrated that CPAHP can not only meet the security requirements but also provide higher computational efficiency.**

***Index Terms*—IoV, Conditional Privacy-Preservation, Anonymous Authentication, 5G, Blockchain.**

Manuscript received 28 June 2022; revised 4 October 2022 and 20 December 2022; accepted 8 February 2023. Date of publication 20 February 2023; date of current version 18 July 2023. This work was supported in part by the Key Research and Development Program of Shaanxi Province under Grants 2023-ZDLGY-34, 2020ZDLGY05-04, and 2021ZDLGY05-03, and in part by Collaborative Innovation Center of Information Sensing and Understanding at Xidian University. The review of this article was coordinated by Dr. Ying He. *(Corresponding author: Jingwei Liu.)*

Jingwei Liu and Chuntian Peng are with the Shaanxi Key Laboratory of Blockchain and Secure Computing, Xidian University, Xi'an 710071, China (e-mail: jwliu@mail.xidian.edu.cn; chuntianp@126.com).

Rong Sun is with the State Key Lab of ISN, Xidian University, Xi'an 710071, China (e-mail: rsun@mail.xidian.edu.cn).

Lei Liu is with the Xidian Guangzhou Institute of Technology, Guangzhou 510555, China (e-mail: leiliu@xidian.edu.cn).

Ning Zhang is with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON N9B 3P4, Canada (e-mail: ning.zhang@uwindsor.ca).

Schahram Dustdar is with the Distributed Systems Group, Technische Universität Wien, 1040 Vienna, Austria (e-mail: dustdar@dsg.tuwien.ac.at).

Victor C. M. Leung is with the College of Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China, and also with the Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: vleung@ieee.org).

Digital Object Identifier 10.1109/TVT.2023.3246466

I. Introduction

IOV plays a crucial role in the development of intelligent control of vehicles [1], intelligent management of traffic, and decision of traffic information services, to improve road safety and efficiency [2]. However, due to the high mobility, network dynamics, and massive data in IoV, it poses a great challenge to the capacity of networks [3], [4]. Compared with the 4G network, 5G is characterized by ultra-high bandwidth, ultra-low latency, and high-density connectivity, which is expected to greatly boost the development of IoV. The combination of 5G and IoV constitutes a three-layer complex network, including the vehicle layer, network layer, and application layer. The 5G-enabled IoV can not only provide infotainment services but also improve the velocity of information exchange in Vehicle-to-Everything (V2X) to maximize the value of transportation infrastructure. It can help reduce the risk of traffic accidents, balance the traffic load, optimize the resource allocation, and provide a safe driving experience for users [5], [6], [7], [8], [9].

In spite of the above benefits, IoV is subject to various cybersecurity attacks, including the impersonation attack, Man-in-the-Middle (MITM) attack, and modification attack, due to its mobility, uncertainty, and scalability [10], [11]. For instance, Nissan Leaf and Tesla were found to have system security vulnerabilities [12], [13] that allow hackers to access historical driving records, fake malicious messages, remotely control vehicles, and so on. Therefore, without an appropriate authentication mechanism, the security of IoV is easily compromised. In addition, vehicular sensors can capture important personal information such as the vehicular identity and location during driving. In the absence of privacy protection technology, personal information can easily be leaked through messages sent by vehicles during communications. However, if the sensitive data of vehicles are adequately protected, it can be difficult to trace the real identities of malicious vehicles, which will incur additional security problems to IoV.

For the above reasons, many authentication schemes have been put forward [14], [15]. However, these schemes are not suitable for 5G-enabled IoV due to security loopholes, complex structure, and high computational overhead. To address the aforementioned problems, we design a new conditional privacy-preserving authentication scheme for 5G-enabled IoV, which is based on the ECDH protocol. The contributions of this paper can be summarized as follows:

- We devise a hierarchical pseudonym mechanism that divides vehicular pseudonyms into a systematic pseudonym and a communication pseudonym. Among them, the systematic pseudonym ensures that only the vehicle and the Trusted Authority (TA) know the real identity of the vehicle itself during the whole communication process. The communication pseudonym of each vehicle changes as it is linked to different 5G Micro Base Stations (MBSs), which is better to prevent the leakage of vehicular movement routes. Moreover, TA can easily calculate the real identity of a malicious vehicle from its two pseudonyms.
- We provide a batch verification method to shorten the latency of the message process. This capability allows recipients to verify multiple messages at once, significantly reducing the complexity of the message validation process, which enables vehicles to effectively adapt to rapidly changing traffic environments with high mobile data flows.
- We propose a blockchain framework for 5G-enabled IoV to store messages (e.g the traffic information, pseudonyms of malicious vehicles, ID and signature of MBS who uploaded the record to the blockchain, and so on), which enables traffic information to be smoothly shared among all vehicles.

The remainder of this paper is organized as follows. Related work is reviewed in Section II. We provide the preliminaries in Section III. Section IV introduces the workflow of the proposed scheme in detail. The correctness and security of the proposed scheme are analyzed in Section V. In Section VI, we analyze and compare the performance of the proposed scheme with some benchmarks. Section VII summarizes the paper.

II. Related Work

In order to protect the personal data of vehicles, many anonymous authentication schemes have been proposed. In 2007, Raya et al. [16] first proposed an anonymous authentication scheme, in which every vehicle has a Tamper-Proof Device (TPD) to hide the system private key. In addition, the Certification Authority (CA) in the scheme maintains a Certification Revocation List (CRL) which grows rapidly in size as the number of revoked vehicles increases. To reduce the storage pressure of CA, Alazzawi et al. [17] devised an identity anonymous scheme that uses the registration list instead of the revocation list. Wei et al. [18] and Zhang et al. [19] devised respectively authentication schemes to resist the side channel attack (SCA) from obtaining the system private key in TPD to forge legal identities. Rajput et al. [20] designed an authentication scheme using hierarchical pseudonyms that fully ensures the security of vehicles' real identities and movement tracks. Shim et al. [21] designed a conditional privacy-preserving authentication scheme that uses bilinear pairing to deal with privacy issues in IoV. To reduce the complexity of certificate management in IoV, Yang et al. [22] proposed an anonymous certificateless aggregation signcryption scheme. Meanwhile, some researchers focused on using vehicular attributes to hide real identities instead of pseudonyms [23], [24], [25]. However, due to the complex computation introduced in the process, these schemes are not suitable for IoV with ultra-low latency where the validation time of messages should be short.

Moreover, to enhance the efficiency of message authentication, many batch verification schemes have been proposed. Jiang et al. [26] devised an anonymous authentication scheme based on hash functions to quickly validate messages in batches. Zhang et al. [27] designed a scalable and effective anonymous batch verification scheme that can not only shorten the time of verification but also resist SCA. Xiong et al. [28] designed a batch verification scheme with double-insurance, in which the signature is generated from the system private key and the vehicle's private key. However, as the number of incorrect signatures increases, the efficiency of batch verification decreases significantly. Therefore, different batch verification schemes were devised by Liu et al. [29] and Ferng et al. [30] respectively, in which RSAs can dynamically regulate the batch size according to the number of failed validations.

With the emergence and development of the 5G technology, researchers have tried to apply 5G into IoV, in which the security issues loomed largely. For this reason, researchers have proposed many different solutions. Wang et al. [31] designed a privacy-preserving technology for 5G-enabled IoV, which adopts a new group signature algorithm to achieve mutual identification in Vehicle-to-Vehicle (V2V) communication. Ouaissa et al. [32] provided a lightweight authentication scheme for 5G-enabled IoV with huge data-flows. Cao et al. [33] designed a new architecture for 5G-enabled IoV based on fog-cloud computing and software-defined networking (SDN), for reducing service delay and energy consumption.

III. Preliminaries

In this section, we present the system model and security requirements.

A. System Model

As shown in Fig. 1, the system model of CPAHP mainly includes five parts, namely, TA, City Traffic Management Center (CTMC), MBSs, Consortium Blockchain, and vehicles. The specific information for each part is as follows:

- *Trust Authority (TA):* TA, regulated by the government, is a fully trusted server that has powerful computing and storage resources. It is principally responsible for initializing the system parameters, generating the system public and private keys, and providing registration services for vehicles and MBSs. If a vehicle is detected to be malicious, TA can reveal its real identity on the basis of the message it sent and revoke its real identity from the system.
- *City Traffic Management Center (CTMC):* CTMC is a reliable government department responsible for managing urban traffic. It can forecast the road condition and balance the traffic load by analyzing the real-time traffic

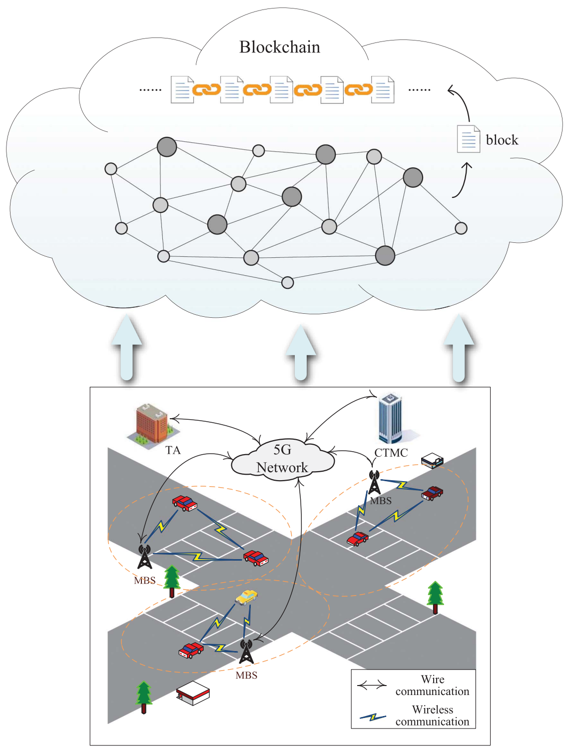


Fig. 1. System Model.

information maintained on the blockchain, to realize the maximum utilization of road resources. It can also directly issue instructions to TA to revoke the identities of malicious vehicles.

- *5G Micro Base Stations (MBSs):* MBSs are semi-trusted and are widely distributed along the roadsides. They interact with TA and vehicles via the wired and wireless networks respectively. MBSs are primarily accountable for information dissemination, generating group verification keys and communication pseudonyms for vehicles in their coverage regions, and uploading traffic information sent by these vehicles to the blockchain.
- *Consortium Blockchain:* The blockchain stores traffic information and the pseudonyms of vehicles that have been revoked.
- *Vehicles:* Every vehicle is equipped with a 5G-enabled On-Board Unit (OBU) which assists the vehicle to communicate with others. Each vehicle has a real identity and a series of pseudonyms, which are used to register and send messages, respectively.

B. Security Requirements

The proposed scheme needs to meet the following security requirements in 5G-enabled IoV.

1) *Message authentication:* To ensure the security of transmission, the receivers (i.e. vehicles and MBSs) should be able to verify the integrity of received messages and the legality of senders.
2) *Identity privacy-preservation:* The proposed scheme should guarantee that no third party knows the real identities of vehicles other than TA, to prevent the real info of vehicles from being leaked during the transmission.
3) *Movement Track Protection:* Movement tracks should be protected because adversaries can deduce private information of the vehicle owner from them, such as the home address, consumption preference, and even interpersonal relationships, etc.
4) *Traceability:* Messages broadcast by vehicles should be associated with vehicles' pseudonyms. If a vehicle has misbehaviors, TA should be able to recover the real identity of the vehicle on the basis of the vicious messages it dispatched and prevent it from continuing to communicate in the system.
5) *Resisting replay attack:* Adversaries deceive vehicles and MBS by repeatedly transmitting a message that has been sent previously. Secure 5G-enabled IoV systems should resist this kind of attack.
6) *Resisting Man-in-the-Middle (MITM) attack:* Receivers should be able to defend against MITM attack in which adversaries can intercept and falsify the message transmitted between vehicles and other participants.
7) *Resisting modification attack:* Vehicles and MBSs should protect against the modification attack in which adversaries tamper with any message.
8) *Resisting impersonation attack:* Receivers should be able to resist the impersonation attack in which adversaries can broadcast malicious messages disguised as legitimate vehicles.

IV. The Proposed Scheme

In this section, a conditional privacy-preserving authentication scheme with hierarchical pseudonyms is elucidated clearly. The main notations used in CPAHP and their descriptions are given in Table I.

The scheme is composed of four stages: system initialization, registration, message delivery, and tracking of malicious vehicles. In system initialization and registration phases, TA generates the public parameters, system public and private key pairs, and then registers the identities of vehicles and MBSs. The message delivery phase is mainly divided into three parts. First, an MBS authenticates the identities of vehicles in its coverage area with the help of TA and generates the communication pseudonym and group verification key for each vehicle. Subsequently, these vehicles can broadcast messages within the range of the MBS with their communication pseudonyms and group verification keys. After that, the MBS and the vehicles can verify the received messages, and the MBS uploads the verified messages to the blockchain. In the tracking of malicious vehicle phase, TA can easily recover the real identity of a malicious vehicle based on the message sent by it and remove it from the registration list L.

Fig. 2 demonstrates the flow diagram of CPAHP. The specific steps of CPAHP are as follows:

TABLE I
SYMBOLS AND DESCRIPTIONS

Notations	Descriptions	Notations	Descriptions
k	The security parameter	SK_{V_i}	The private key of vehicle V_i
G_1	An additive cyclic group with order q	PK_{B_j}	The public key of MBS B_j
G_2	A multiplicative cyclic group with order q	SK_{B_j}	The private key of MBS B_j
P	A generator of G_1	$Cert_{B_j}$	The public key certificate of MBS B_j
s	The system private key	gvk_i	The group verification key of vehicle V_i
P_{pub}	The system public key	$CPID_i$	The communication pseudonym of vehicle V_i
V_i	The ith vehicle	$Sig(\cdot)$	Signature algorithm
B_j	The jth MBS	$Enc(\cdot)$	Symmetric encryption algorithm
RID_{V_i}	The real identity of vehicle V_i	$Dec(\cdot)$	Symmetric decryption algorithm
$SPID_i$	The systemic pseudonym of vehicle V_i	m	A message broadcast by a vehicle
PK_{V_i}	The public key of vehicle V_i	δ_m	The signature of m

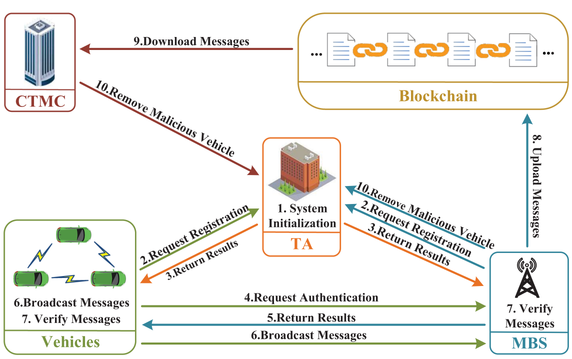


Fig. 2. Flow diagram of CPAHP.

A. System Initialization

1) TA selects a security parameter k, two cyclic groups G_1 and G_2 with order q, where G_1 is an additive group, G_2 is a multiplicative group, and $q(q \geq 2^k)$ is a large prime.
2) TA defines $e : G_1 \times G_1 \rightarrow G_2$, computes $g = e(P, P)$, and selects five hash functions:

$$H_1 : G_1 \times G_1 \rightarrow \{0, 1\}^l$$

$$H_2 : G_1 \times \{0, 1\}^l \times Z_q^* \rightarrow G_1$$

$$H_3 : G_1 \times Z_q^* \rightarrow \{0, 1\}^l$$

$$H_4 : \{0, 1\}^l \times Z_q^* \rightarrow Z_q^*$$

$$H_5 : \{0, 1\}^n \times Z_q^* \times \{0, 1\}^l \times G_1 \rightarrow Z_q^*$$

where P is the generator of G_1, l is the length of a vehicle's identity, and n is the length of a message.
3) TA randomly chooses $s \in Z_q^*$ as the system private key and calculates the system public key $P_{pub} = sP$.
4) TA announces the public parameters $params = \{k, P, g, G_1, G_2, H_1, H_2, H_3, H_4, H_5, P_{pub}\}$, and keeps the system private key s secretly.

B. Registration

1) Vehicle Registration

a) A vehicle V_i first picks $\gamma_i \in Z_q^*$ at random, and calculates its partial systemic pseudonym $SPID_{i,1} = \gamma_i P$. Then, V_i sends its real identity RID_{V_i} (e.g., the engine number of V_i) and $SPID_{i,1}$ to TA through a secure channel.
b) On receiving the message of V_i for registration, TA first checks whether RID_{V_i} has been recorded in the registration list L maintained secret by TA. If yes, V_i is registered and the process terminates.
c) TA calculates the partial systemic pseudonym $SPID_{i,2}$:

$$SPID_{i,2} = RID_{V_i} \oplus H_1(SPID_{i,1} \| sP_{pub}) \quad (1)$$

Then, TA sets the systemic pseudonym of V_i as $SPID_i = (SPID_{i,1}, SPID_{i,2}, T_{SPID_i})$, where T_{SPID_i} is the validation time of this pseudonym.
d) TA calculates the public key $PK_{V_i} = Q_i = H_2(SPID_i)$ and the private key $SK_{V_i} = sQ_i$ of V_i.
e) Finally, TA sends $\{SPID_i, PK_{V_i}, SK_{V_i}, \sigma_{TA,i}\}$ to V_i via a secure channel, where $\sigma_{TA,i} = Sig(SPID_i, PK_{V_i}, SK_{V_i})_s$. Meanwhile, it stores RID_{V_i} and $SPID_i$ in the registration list L.

The procedure of the vehicle registration is shown in Algorithm 1.

2) MBS Registration

MBS B_j picks out a random value $\theta_j \in Z_q^*$ as its private key SK_{B_j}, and calculates its public key $PK_{B_j} = \theta_j P$. Then, B_j submits $\{PK_{B_j}, ID_{B_j}, \sigma_{B_j}\}$ to TA through a secure channel, where ID_{B_j} is its identity and $\sigma_{B_j} = Sig(PK_{B_j}, ID_{B_j})_{SK_{B_j}}$. Upon receiving the message from B_j, TA first checks the signature σ_{B_j} by the public key PK_{B_j}. Then, TA generates the public key certificate $Cert_{B_j} = (PK_{B_j}, T_{B_j}, \sigma_{TA,j})$ of B_j, where T_{B_j} is the validation time of the public key certificate, and $\sigma_{TA,j} = Sig(PK_{B_j}, T_{B_j})_s$. Finally, TA sends $Cert_{B_j}$ to B_j.

The registration process of CTMC is similar to that of MBS. And the procedure of the MBS registration is shown in Algorithm 2.

Algorithm 1: Vehicle Registration Algorithm.

V_i picks a random number $\gamma_i \in Z_q^*$, then calculates its partial pseudonym $SPID_{i,1} = \gamma_i P$
V_i sends $\{RID_{V_i}, SPID_{i,1}\}$ to TA through a secure channel
if RID_{V_i} has been recorded in the registration list L **then**
  TA terminates the process
else
  TA calculates:
  $SPID_{i,2} = RID_{V_i} \oplus H_1(SPID_{i,1} \| sP_{pub})$
  TA sets the systemic pseudonym of V_i as $SPID_i = (SPID_{i,1}, SPID_{i,2}, T_{SPID_i})$
  TA generates V_i's public key $PK_{V_i} = Q_i = H_2(SPID_i)$
  TA calculates V_i's private key $SK_{V_i} = sQ_i$
  TA sends $\{SPID_i, PK_{V_i}, SK_{V_i}, \sigma_{TA,i}\}$ to V_i via a secure channel
  TA stores RID_{V_i} and $SPID_i$ in L
end if

C. Message Delivery

1) MBS-Assisted Group Verification Key Generation

a) Request Generation

- B_j regularly broadcasts a hello message $Mes : \{hello, Cert_{B_j}, \sigma_{B_j,m}, T_{Mes}\}$ within its coverage, where $\sigma_{B_j,m} = Sig(hello, T_{Mes})_{SK_{B_j}}$, and T_{Mes} is the timestamp of the message Mes.
- V_i can receive the message Mes when enters the coverage of B_j. Provided that V_i has no message to broadcast, it ignores the message Mes. Otherwise, it performs the following steps.
- V_i extracts the public key certificate $Cert_{B_j} = (PK_{B_j}, T_{B_j}, \sigma_{TA,j})$ in Mes, and verifies if $Cert_{B_j}$, T_{B_j} and T_{Mes} are correct. If not, V_i terminates the process.
- V_i selects a random constant $a \in Z_q^*$ and calculates $K = aP$. Then, it encrypts the request $req = (SPID_i, K, T_q, \sigma_{V_i})$ under PK_{B_j} to get the ciphertext C_{V_i} and sends C_{V_i} to B_j, where T_q is the timestamp of the request req and $\sigma_{V_i} = Sig(SPID_i, K, T_q)_{SK_{V_i}}$.

The procedure of the request generation is shown in Algorithm 3.

b) Authentication

- When B_j receives the ciphertext C_{V_i} of the request req from V_i, it decrypts C_{V_i} with its own private key SK_{B_j} to obtain $req = (SPID_i, K, T_q, \sigma_{V_i})$. Then, B_j verifies whether the timestamp of the request satisfies $T - T_q \leq \triangle T$, where T is the current time, and $\triangle T$ is the maximum delay time for B_j receiving V_i's request req. If the verification fails, B_j terminates the process.
- B_j uses $SPID_i$ to compute the vehicle's public key $PK_{V_i} = Q_i = H_2(SPID_i)$, and then verifies whether the signature σ_{V_i} is correct through PK_{V_i}. If incorrect, B_j rejects req from V_i. Otherwise, B_j sends $SPID_i$ to TA via a secure channel.
- Once receiving $SPID_i$, TA uses it to check whether V_i has been recorded in the registration list L. If V_i's identity is legal, TA returns $respond = TRUE$ to B_j, otherwise, it returns $respond = FALSE$.
- On receiving the message $\{respond = TRUE/FALSE\}$ from TA, B_j first checks that the content of the message is $respond = TRUE$. If not, it denies the request req. Otherwise, B_j calculates the communication pseudonym $CPID_i$ and the group verification key gvk_i that V_i uses to broadcast messages in B_j's range:

$$CPID_i = SPID_{i,2} \oplus H_3\left(\theta_j Q_i \| T_{gvk_i}\right)$$
$$gvk_i = \frac{1}{\theta_j} H_4\left(CPID_i \| T_{gvk_i}\right) Q_i \tag{2}$$

Here, T_{gvk_i} represents the validation time of the group verification key gvk_i. Then, B_j encrypts the tuple $\{CPID_i, gvk_i, T_{gvk_i}\}$ under key and sends $C_{B_j} = Enc(CPID_i, gvk_i, T_{gvk_i})_{key}$ to V_i, where $key = SK_{B_j} K$. Finally, B_j saves and broadcasts $\{T_{gvk_i}, CPID_i\}$.
- After V_i receives C_{B_j}, it computes $key' = aPK_{B_j}$ and decrypts C_{B_j} through the symmetric decryption algorithm $Dec(\cdot)_{key'}$ to obtain $\{CPID_i, gvk_i, T_{gvk_i}\}$. Then, V_i can use gvk_i to sign messages and $CPID_i$ to hide its systemic pseudonym $SPID_i$ when broadcast messages within B_j's coverage area.

The procedure of the group verification key generation is shown in Algorithm 4.

2) Message Signing

a) V_i randomly elects $\mu_i \in Z_q^*$, and calculates $U_i = \mu_i Q_i$.

b) V_i generates the signature δ_{m_i}:

$$\delta_{m_i} = \mu_i H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right) gvk_i \tag{3}$$

where T_{δ_i} is the timestamp of m_i.

c) V_i broadcasts a tuple $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}$. Then, B_j and vehicles within the range of B_j can receive the tuple.

Algorithm 2: MBS Registration Algorithm.

B_j randomly chooses $\theta_j \in Z_q^*$ as its private key SK_{B_j}, and calculates its public key $PK_{B_j} = \theta_j P$
B_j submits $\{PK_{B_j}, ID_{B_j}, \sigma_{B_j}\}$ to TA through a secure channel
if σ_{B_j} is valid **then**
  TA generates the public key certificate $Cert_{B_j} = (PK_{B_j}, T_{B_j}, \sigma_{TA,j})$ of B_j
  TA sends $Cert_{B_j}$ to B_j
else
  TA terminates the process
end if

Algorithm 3: Request Generation Algorithm.

Input: The message Mes from B_j

V_i obtains the public key PK_{B_j}, the public key certificate $Cert_{B_j}$, signature $\sigma_{B_j,m}$ of B_j, and the timestamp T_{Mes} of the message
if $\sigma_{B_j,m}$, $Cert_{B_j}$ and T_{Mes} are valid **then**
  V_i chooses a random constant $a \in Z_q^*$, and calculates $K = aP$
  V_i generates the request $req = (SPID_i, K, T_q, \sigma_{V_i})$ for authentication
  V_i encrypts req under the public key PK_{B_j} of B_j to get C_{V_i} and sends C_{V_i} to B_j
else
  V_i terminates the process
end if

3) Verification

a) Single Message Verification: When vehicles in B_j's coverage region and B_j receive $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}$, they execute the following steps to verify the legality of m_i.

- First, they verify whether the timestamp T_{δ_i} satisfies $T - T_{\delta_i} \leq \triangle T_m$, where $\triangle T_m$ is the max validation time interval of messages. Then they check if the group verification key gvk_i is expired by the validation time T_{gvk_i}. If T_{δ_i} fails to meet the condition or gvk_i is expired, they abort the process.
- Then, vehicles and B_j verify that the signature δ_{m_i} of message m_i satisfies the following equation:

$$\begin{aligned} & e(PK_{B_j}, \delta_{m_i}) \\ & = e(P, H_4(CPID_i \| T_{gvk_i}) \\ & H_5(m_i \| T_{\delta_i} \| CPID_i \| U_i) U_i) \\ & = G_s \end{aligned} \tag{4}$$

If the above equation holds, the signature δ_{m_i} is valid and m_i is accepted. Otherwise, the signature is invalid and m_i is discarded.

b) *Batch Verification:* If a receiver connects and communicates with n vehicles at the same time, the verification burden of the received messages increases greatly. In this case, the receiver performs the batch verification algorithm to reduce computational stress.

Suppose a vehicle within B_j's range or B_j receives multiple tuples $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}_{i=1}^n$ from the vehicles $\{V_1, V_2, \ldots, V_n\}$, it can verify the messages $\{m_i\}_{i=1}^n$ in batches with the following formula:

$$\begin{aligned} & e\left(PK_{B_j}, \sum_{i=1}^{n} \delta_{m_i}\right) \\ & = e\left(P, \sum_{i=1}^{n} H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right)\right. \\ & H_4\left(CPID_i \| T_{gvk_i}\right) U_i) \\ & = G_b \end{aligned} \tag{5}$$

Algorithm 4: Group Verification Key Generation Algorithm.

Input: The request req from V_i

if $T - T_q \leq \triangle T$ and σ_{V_i} is valid **then**
  B_j sends $SPID_i$ to TA via a secure channel
  TA checks whether V_i's identity is legal according to L
  if $SPID_i = Valid$ **then**
    TA returns $respond = TRUE$ to B_j
  else
    TA returns $respond = FALSE$ to B_j
  end if
  if $respond = TRUE$ **then**
    B_j calculates:
    $CPID_i = SPID_{i,2} \oplus H_3(\theta_j Q_i \| T_{gvk_i})$,
    $gvk_i = \frac{1}{\theta_j} H_4(CPID_i \| T_{gvk_i}) Q_i$
    B_j encrypts $\{CPID_i, gvk_i, T_{gvk_i}\}$ under $key = SK_{B_j} K$, and sends $C_{B_j} = Enc(CPID_i, gvk_i, T_{gvk_i})_{key}$ to V_i
    V_i decrypts C_{B_j} under $key' = aPK_{B_j}$ to obtain $\{CPID_i, gvk_i, T_{gvk_i}\}$
  else
    B_j terminates the process
  end if
else
  B_j terminates the process
end if

If the above equation does not hold, it means that there are malicious data in these messages. These illegal messages can be located through dichotomy.

4) Data Storage

After verifying the vehicles' messages, B_j first filters the authenticated messages, and then uploads $\{m_i, CPID_i, ID_{B_j}, \sigma_{i,j}\}_{i=1}^n$ to the blockchain, where $\sigma_{i,j} = Sig(m_i, CPID_i, ID_{B_j})_{SK_{B_j}}$. Hence, vehicles within the range of other MBSs can also search for the records on the blockchain to learn about the latest road traffic information here.

D. Tracking of Malicious Vehicle

1) *Situation 1.* CTMC finds that a record m_i on the blockchain is illegal.

a) CTMC sends $Rem_c = (m_i, CPID_i, ID_{B_j}, \sigma_{i,j}, illegal, \sigma_{c,j})$ to B_j who uploaded the record m_i previously, where $\sigma_{c,j} = Sig(m_i, CPID_i, ID_{B_j}, \sigma_{i,j}, illegal)_{SK_{CTMC}}$.

b) Upon receiving Rem_c, B_j calculates $SPID_{i,2} = CPID_i \oplus H_3(\theta_j Q_i \| T_{gvk_i})$ and sends $\{SPID_{i,2}, Revoke\}$ to TA. Next, it sets T_{gvk_i} to 0, which means the group verification key gvk_i is expired. Then, B_j broadcasts the hello message Mes with parameters $\{CPID_i, T_{gvk_i}\}$, and uploads the parameters to the blockchain as a transaction.

c) On receiving $\{SPID_{i,2}, Revoke\}$, TA finds out the corresponding real identity RID_{V_i} in the registration list L according to the pseudonym $SPID_{i,2}$. Then, TA revokes the real identity RID_{V_i} of the malicious vehicle V_i from L.

2) *Situation 2.* Vehicles find the message m_i is illegal.

a) A vehicle V_k that is within the range of any MBS finds the record m_i on the blockchain to be illegal and tries to remove the real identity of the vehicle V_i who sent m_i previously.

- V_k sends $Rem_{V_k} = (m_i, CPID_i, ID_{B_j}, \sigma_{i,j}, illegal, \sigma_{V_{i,k}})$ to the MBS B_h that V_k interacts with, where $\sigma_{V_{i,k}} = Sig(m_i, CPID_i, ID_{B_j}, \sigma_{i,j}, illegal)_{SK_{V_k}}$.
- B_h transmits Rem_{V_k} to B_j that uploaded the message m_i previously.
- B_j arbitrates the message m_i. If B_j confirms that the message m_i is correct and legal, it, B_h, and TA execute steps b) and c) in the *Situation 1* to revoke V_k's real identity. Conversely, the identity of V_i that broadcast m_i is revoked.

b) V_k directly discovers the message m_i sent by V_i is illegal when interacting with V_i.

- V_k sends $Rem'_{V_k} = (CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}, illegal, \sigma'_{V_{i,k}})$ to B_j, where $\sigma'_{V_{i,k}} = Sig(CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}, illegal)_{SK_{V_k}}$.
- B_j arbitrates the message m_i as described in step a).

V. Correctness and Security Analysis

In this section, we prove the correctness and analyze the security of CPAHP.

A. Correctness Analysis

We prove the correctness of the single message verification and batch verification. The lemmas are as follows.

Lemma 1: Any receiver in the coverage of B_j can check the equation $e(PK_{B_j}, \delta_{m_i}) = G_s$ to verify if the signature δ_{m_i} is valid, where $G_s = e(P, H_4(CPID_i \| T_{gvk_i}) H_5(m_i \| T_{\delta_i} \| CPID_i \| U_i) U_i)$.

Proof: B_j publishes $\{PK_{B_j}, T_{gvk_i}, CPID_i\}$ in the group verification key generation process, and V_i needs to broadcast the message m_i with a tuple $\{CPID_i, T_{gvk_i}, U_i, \delta_{m_i}, T_{\delta_i}\}$ after signing m_i. Any receiver can calculate and compare $e(PK_{B_j}, \delta_{m_i})$ with G_s to verify whether the signature δ_{m_i} is legal, where $PK_{B_j} = \theta_j P$, $\delta_{m_i} = \mu_i H_5(m_i \| T_{\delta_i} \| CPID_i \| U_i) gvk_i$, $gvk_i = \frac{1}{\theta_j} H_4(CPID_i \| T_{gvk_i}) Q_i$, and $U_i = \mu_i Q_i$.

$$
\begin{aligned}
& e\left(PK_{B_j}, \delta_{m_i}\right) \\
&= e\left(PK_{B_j}, \mu_i H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right) gvk_i\right) \\
&= e\left(\theta_j P, \left(\frac{1}{\theta_j}\right) H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right)\right. \\
&\quad \left. H_4\left(CPID_i \| T_{gvk_i}\right) \mu_i Q_i\right) \\
&= e\left(P, H_4\left(CPID_i \| T_{gvk_i}\right)\right. \\
&\quad \left. H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right) U_i\right) \\
&= G_s
\end{aligned} \tag{6}
$$

Lemma 2: Any receiver with in the range of B_j can check the equation $e(PK_{B_j}, \sum_{i=1}^{n} \delta_{m_i}) = G_b$ to verify if the signatures $\{\delta_{m_i}\}_{i=1}^{n}$ are valid, where $G_b = e(P, \sum_{i=1}^{n} H_5(m_i \| T_{\delta_i} \| CPID_i \| U_i) H_4(CPID_i \| T_{gvk_i}) U_i)$.

Proof: B_j publishes $\{PK_{B_j}, T_{gvk_i}, CPID_i\}_{i=1}^{n}$ in the group verification key generation process, and $\{V_i\}_{i=1}^{n}$ need to broadcast the messages $\{m_i\}_{i=1}^{n}$ with tuples $\{CPID_i, T_{gvk_i}, U_i, \delta_{m_i}, T_{\delta_i}\}_{i=1}^{n}$ after signing $\{m_i\}_{i=1}^{n}$. Any receiver can calculate and compare $e(PK_{B_j}, \sum_{i=1}^{n} \delta_{m_i})$ with G_s to verify whether the signatures $\{\delta_{m_i}\}_{i=1}^{n}$ are legal, where $PK_{B_j} = \theta_j P$, $\{\delta_{m_i} = \mu_i H_5(m_i \| T_{\delta_i} \| CPID_i \| U_i) gvk_i\}_{i=1}^{n}$, $\{gvk_i = \frac{1}{\theta_j} H_4(CPID_i \| T_{gvk_i}) Q_i\}_{i=1}^{n}$, and $\{U_i = \mu_i Q_i\}_{i=1}^{n}$.

$$
\begin{aligned}
& e\left(PK_{B_j}, \sum_{i=1}^{n} \delta_{m_i}\right) \\
&= e\left(PK_{B_j}, \sum_{i=1}^{n} \mu_i H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right) gvk_i\right) \\
&= e\left(\theta_j P, \sum_{i=1}^{n} \frac{1}{\theta_j} \mu_i H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right)\right. \\
&\quad \left. H_4\left(CPID_i \| T_{gvk_i}\right) Q_i\right) \\
&= e\left(P, \sum_{i=1}^{n} H_5\left(m_i \| T_{\delta_i} \| CPID_i \| U_i\right)\right. \\
&\quad \left. H_4\left(CPID_i \| T_{gvk_i}\right) U_i\right) \\
&= G_b
\end{aligned} \tag{7}
$$

B. Security Analysis

We analyze the security of CPAHP in the aspect of message authentication, identity privacy-protection, movement track protection, traceability, the resistance of replay attack, modification attack, impersonation attack, and MITM attack.

1) *Message Authentication:* In Mes broadcast by MBS B_j, $\sigma_{B_j,m}$ is the signature of the message $\{hello, T_{Mes}\}$ generated by B_j's private key SK_{B_j}. Similarly, the signature of request $req = (SPID_i, K, PK_{V_i}, T_q, \sigma_{V_i})$ is generated by SK_{V_i}. Meanwhile, before broadcasting a message, V_i signs the message using a randomly selected number μ_i and the group verification key gvk_i which is generated by B_j's private key SK_{B_j}. If the ECDLP assumption holds, adversaries cannot forge the signatures $\sigma_{B_j,m}, \sigma_{V_i}$, and δ_{m_i}, because they do not have SK_{B_j}, SK_{V_i}, and μ_i. Therefore, CPAHP realizes secure message authentication.

2) *Identity Privacy-Preservation:* The real identities of vehicles are hidden through the hierarchical pseudonym mechanism. The first layer of pseudonyms is the systemic pseudonym $SPID_i = (SPID_{i,1}, SPID_{i,2}, T_{SPID_i})$ generated by TA for V_i during the vehicle registration, where $SPID_{i,1} = \gamma_i P$, $SPID_{i,2} = RID_{V_i} \oplus H_1(SPID_{i,1} \| sP_{pub})$, and s is the system private

key. The second layer is the communication pseudonym $CPID_i = SPID_{i,2} \oplus H_3(\theta_j Q_i \| T_{gvk_i})$ generated by B_j after V_i passes its identity authentication, where θ_j is the private key of B_j. If the ECDLP assumption holds, no adversary can gain the real identity RID_{V_i} of the vehicle based on $SPID_i$ and $CPID_i$, because it does not have the system private key s and the private key of B_j. Therefore, CPAHP can guarantee the security of the vehicle's identity privacy.

3) *Movement Track Protection:* In the authentication phase, MBS B_j uses its private key θ_j and the validation time T_{gvk_i} to generate V_i's communication pseudonym $CPID_i = SPID_{i,2} \oplus H_3(\theta_j Q_i \| T_{gvk_i})$. Because θ_j is only known to and correlated with B_j, and T_{gvk_i} is disposable, no adversary can associate any two communication pseudonyms with a particular vehicle. Thus, CPAHP successfully protects the vehicle's trajectory.

4) *Traceability:* If a vehicle V_i sends a malicious message, MBS B_j can calculate the partial systemic pseudonym of the vehicle V_i by executing $SPID_{i,2} = CPID_i \oplus H_3(\theta_j Q_i \| T_{gvk_i})$. Then, TA can query the registration list L to obtain the vehicle's real identity RID_{V_i} according to $SPID_{i,2}$. In other words, on the premise of ensuring the security of the legal vehicles' real identities, TA can find out all malicious vehicles through the malicious vehicles' communication pseudonyms with the assistance of MBSs. Hence, CPAHP satisfies traceability.

5) *Resistance of Replay Attack:* The tuple $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}$ broadcast by V_i contains the current timestamp T_{δ_i} and the signature δ_{m_i} generated by V_i. The freshness of the message m_i is confirmed by checking whether the formula $T - T_{\delta_i} \leq \triangle T_m$ holds. If the message is not fresh, it will be thrown out. In addition, a hash function $H_5(\cdot)$ is used to generate the signature $\delta_{m_i} = \mu_i H_5(m_i \| T_{\delta_i} \| CPID_i \| U_i) gvk_i$ to ensure the integrity of T_{δ_i}. So even if adversaries change the timestamp of m_i, the message can still be discarded because the signature cannot pass the verification. Therefore, the replay attack is ineffective in CPAHP.

6) *Resistance of Modification Attack:* The message broadcast by V_i is $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}$, where the integrity of the tuple $\{CPID_i, T_{gvk_i}, U_i, m_i, T_{\delta_i}\}$ is guaranteed by signature δ_{m_i}. And any modification of the tuple can be recognized by checking if the equation $e(\delta_{m_i}, PK_{B_j}) = G_s$ holds. Therefore, CPAHP can resist the modification attack.

7) *Resistance of Impersonation Attack:* The group verification key $gvk_i = (\frac{1}{\theta_j}) H_4(CPID_i \| T_{gvk_i}) Q_i$ of V_i is specifically generated using the private key θ_j of B_j. Meanwhile, V_i simultaneously uses gvk_i and a random number μ_i to generate the signature δ_{m_i}. It is impossible for adversaries to forge the signature δ_{m_i} without θ_j and μ_i due to the Elliptic Curve Discrete Logarithm Problem. So, if a adversary broadcasts a new message $\{CPID_i, T'_{gvk_i}, U'_i, m'_i, \delta'_{m_i}, T'_{\delta_i}\}$ where $CPID_i$ is lifted from $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}$, the message can not pass the verification. Therefore, CPAHP can resist the impersonation attack.

8) *Resistance of MITM Attack:* All messages transmitted in the proposed scheme need to check the legality and validity, so it is impossible for any adversary to successfully falsify a message. For example, if a malicious vehicle intercepts and changes a message $\{CPID_i, T_{gvk_i}, U_i, m_i, \delta_{m_i}, T_{\delta_i}\}$ from V_i, the proof $e(\delta_{m_i}, PK_{B_j}) = G_s$ can not be fulfilled and m_i will be discarded. Therefore, the MITM attack is ineffective in CPAHP.

TABLE II
CRYPTOGRAPHY OPERATION TIME

Operation	Notation	Time(ms)
Bilinear pairing	P	2.74
Scalar multiplication in G_1	M	1.40
Exponentiation in G_2	E	1.35
Point addition in G_1	A	0.0079

VI. Performance Analysis

In this section, we compare the computational overhead and processing rate (i.e. the maximum number of messages that can be processed per second) of CPAHP with several existing authentication schemes. First, we use the cryptography PBC-0.5.14 library under Linux Ubuntu 16.04 environment to compute the execution time of basic cryptographic operations, as shown in Table II. Then, we consider the time cost of the message signing phase (MS), single message verification phase (SMV), and batch verification phase (BV), and compare them with four existing schemes MDBV [34], CL-CPPA [35], CASA [36], IBAS [37] in Table III.

Here, we make a detailed analysis of CL-CPPA [35]. In CL-CPPA [35], the message signing needs two scalar multiplication operations and three exponential operations. Thus, the entire computational overhead of MS is $2M + 3E \approx 6.85$ ms. In single message verification, a receiver requires three scalar multiplication operations and three exponential operations. Thus, the computational complexity of single message verification is $3M + 3E \approx 8.25$ ms. The batch verification involves $(3n + 2)$ scalar multiplication operations and $(3n)$ exponential operations. So, the entire computational overhead of batch verification is $(3n + 2)M + 3nE \approx (8.25n + 2.81)ms$.

In CPAHP, the message signing needs two scalar multiplication operations. So, the computational cost of MS is $2M \approx$ 2.80 ms. To verify a message, each receiver needs two bilinear pairing operations and one scalar multiplication operation. So, the entire time cost of single message verification is $2P + M \approx 6.88$ ms. BV includes the following operations: two bilinear pairing operations, n scalar multiplication operations, and $2(n - 1)$ point addition operations. Thus, the computational overhead of batch verification is $2P + nM + 2(n - 1)A \approx (1.41n + 5.46)$ms. We also calculated the computational overhead of MDBV [34], CASA [36], and IBAS [37] similarly, as shown in Table III.

TABLE III
COMPUTATIONAL OVERHEAD IN THE MESSAGE SIGNING PHASE AND VERIFICATION PHASE OF EACH SCHEME

Scheme	MS	SMV	BV
MDBV [34]	$3M \approx 4.20ms$	$3P + 2M + A \approx 11.03ms$	$3P + 2nM + (2n-1)A \approx (2.82n + 8.21)ms$
CL-CPPA [35]	$2M + 3E \approx 6.85ms$	$3M + 3E \approx 8.25ms$	$(3n+2)M + 3nE \approx (8.25n + 2.81)ms$
CASA [36]	$4M \approx 5.60ms$	$3P + 3M \approx 12.42ms$	$3P + 3nM + (2n-1)A \approx (4.22n + 8.21)ms$
IBAS [37]	$3M + A \approx 4.21ms$	$2P + M + A \approx 6.89ms$	$(n+1)P + nM + nA \approx (4.15n + 2.74)ms$
Ours CPAHP	$2M \approx 2.80ms$	$2P + M \approx 6.88ms$	$2P + nM + 2(n-1)A \approx (1.41n + 5.46)ms$

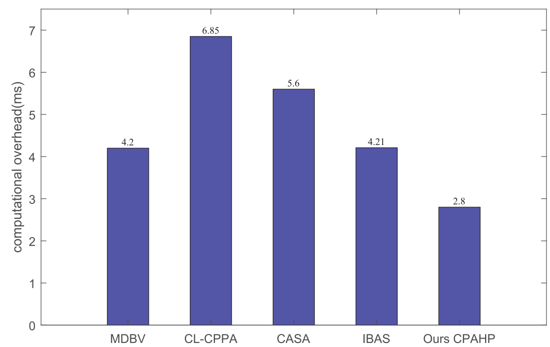


Fig. 3. Comparison of computational overhead in MS.

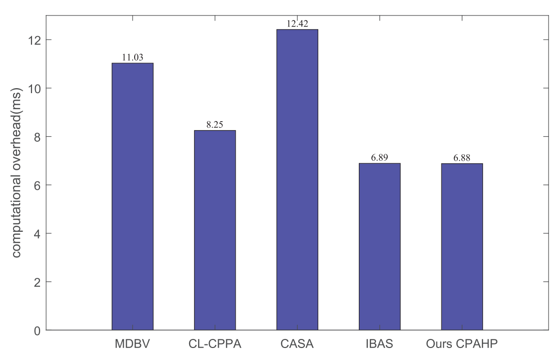


Fig. 4. Comparison of computational overhead in SMV.

The comparison of the computational overhead of each scheme in MS and SMV is shown in Fig. 3 and Fig. 4. Specifically, it is clear that the time overhead of MDBV [34], CL-CPPA [35], CASA [36], IBAS [37], and CPAHP in MS are 4.20 ms, 6.85 ms, 5.60 ms, 4.21 ms, and 2.80 ms, respectively. Hence, the schemes [34], [35], [36], and [37] are consuming $4.20/2.80 \approx 150.00\%$, $6.85/2.80 \approx 244.64\%$, $5.60/2.80 \approx 200.00\%$, and $4.21/2.80 \approx 150.34\%$ of CPAHP in message signing. Similarly, the time consumed in SMV for the schemes [34], [35], [36], and [37] are 160.32%, 119.91%, 180.52%, and 100.15% of CPAHP, respectively. This is because the expensive operations in these schemes are mainly the bilinear pairing and scalar multiplication. And in MS and SMV, CPAHP requires the least number of these two expensive operations. Therefore, the proposed scheme CPAHP has the lowest computational cost in MS and SMV compared to schemes [34], [35], [36], and [37].

Then, we compare the time consumption of CPAHP in single message verification and batch verification phases. From Fig. 5, as the number of messages n increases, the time cost of CPAHP in SMV increases significantly, while that of BV increases much more slowly. This shows that BV of CPAHP has a significant advantage over SMV when the number of messages received is large. We also compare the time consumption of these schemes in the batch verification phase. As shown in Fig. 6, no matter how the number of messages n increases, the computational cost of CPAHP is always the lowest. For example, as shown in Table IV, when $n = 50$, the computational cost of MDBV [34], CL-CPPA [35], CASA [36], and IBAS [37] in BV are 322.14%, 545.21%, 287.20%, and 275.57% of CPAHP respectively. This

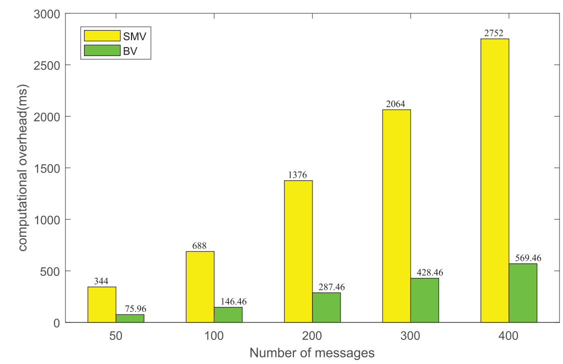


Fig. 5. Comparison of computational overhead between SMV and BV of CPAHP.

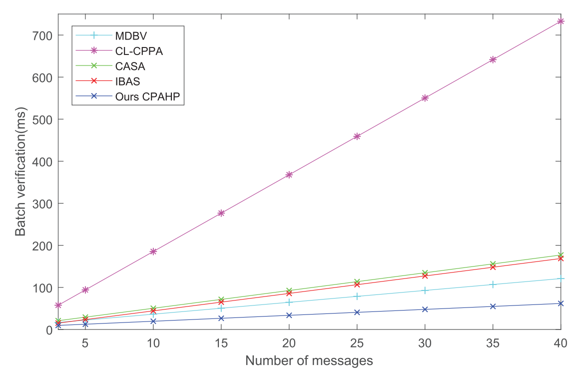


Fig. 6. Comparison of computational overhead in BV.

TABLE IV
THE COMPUTATIONAL OVERHEAD COMPARISON

Scheme	MS	SMV	BV(50 messages)
MDBV [34]	150.00%	160.32%	322.14%
CL-CPPA [35]	244.64%	119.91%	545.21%
CASA [36]	200.00%	180.52%	287.20%
IBAS [37]	150.34%	100.15%	275.57%

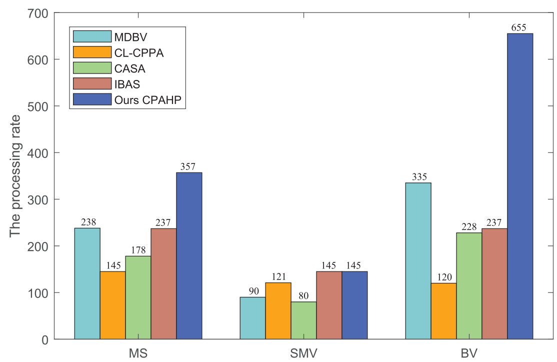


Fig. 7. Comparison of processing rate in MS, MSV and BV.

is because our batch verification only has two expensive operations, i.e. the bilinear pairing and scalar multiplication, and only the number of scalar multiplication increases with n. In addition, the increased coefficient of scalar multiplication in BV of CPAHP is the smallest compared with schemes [34] and [36].

We also compare the processing rate of MDBV [34], CL-CPPA [35], CASA [36], IBAS [37], and CPAHP in phases MS, MSV, and BV, as shown in Fig. 7. It can be seen that the rate of CPAHP is the fastest in MS. It allows vehicles to feed back faster and more details about themselves and the road conditions. Although the processing rate of CPAHP in MSV is the same as IBAS [37], the rate of CPAHP has a great advantage over the other schemes in BV. So, it can better handle plenty of messages pouring in at the same time. Consequently, CPAHP is more propitious to 5G-enabled IoV with high-density connectivity.

VII. Conclusion

In this paper, we proposed a conditional privacy-preserving authentication scheme with hierarchical pseudonyms (CPAHP) for 5G-enabled IoV. Through the designed hierarchical pseudonym mechanism, vehicles broadcast messages without revealing their real identities and movement tracks, and the malicious vehicles can be located by TA. Further, by introducing blockchain technology, traffic information can be shared among vehicles within the range of different MBSs. Moreover, with the help of lightweight message signing and batch verification methods, the delay in processing messages is greatly reduced. The performance analysis demonstrates that CPAHP is more efficient than the benchmark schemes due to the lower computation overhead. These results show that CPAHP is more suitable for 5G-enabled IoV with high-density connectivity and ultra-low latency.

References

[1] H. Zhang and Q. Sun, "Optimal control and safe operation of energy interconnection systems," Beijing: Science Press, (in Chinese), Jul. 2022.

[2] L. Liu, M. Zhao, M. Yu, M. A. Jan, D. Lan, and A. Taherkordi, "Mobility-aware multi-hop task offloading for autonomous driving in vehicular edge computing and networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2169–2182, Feb. 2023.

[3] X. Ge, Z. Li, and S. Li, "5G software defined vehicular networks," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 87–93, Jul. 2017.

[4] Y. He, N. Zhao, and H. Yin, "Integrated networking, caching, and computing for connected vehicles: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 44–55, Jan. 2018.

[5] H. Zhou, W. Xu, Y. Bi, J. Chen, Q. Yu, and X. S. Shen, "Toward 5G spectrum sharing for immersive-experience-driven vehicular communications," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 30–37, Jan. 2018.

[6] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 33, no. 11, pp. 2687–2700, Nov. 2022.

[7] N. Cheng, N. Lu, N. Zhang, X. Shen, and J. W. Mark, "Vehicular wifi offloading: Challenges and solutions," *Veh. Commun.*, vol. 1, no. 1, pp. 13–21, Jan. 2014.

[8] J. Feng, W. Zhang, Q. Pei, J. Wu, and X. Lin, "Heterogeneous computation and resource allocation for wireless powered federated edge learning systems," *IEEE Trans. Commun.*, vol. 70, no. 5, pp. 3220–3233, May 2022.

[9] Y. He, Y. Wang, Q. Lin, and J. Li, "Meta-hierarchical reinforcement learning (MHRL)-based dynamic resource allocation for dynamic vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 4395–3506, Apr. 2022.

[10] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[11] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions," *Veh. Commun.*, vol. 20, 2019, Art. no. 100182.

[12] T. Hunt, "Controlling vehicle features of Nissan leafs across the globe via vulnerable APIs," 2016, [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

[13] K. S. L.of Tencent, "Keen security lab of tencent car hacking research remote attack to tesla cars," 2016. [Online]. Available: https://keenlab.tencent.com/zh/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars

[14] P. Vijayakumar, M. Azees, S. A. Kozlov, and J. J. P. C. Rodrigues, "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 2, pp. 1630–1638, Feb. 2022.

[15] H. Xiong, J. Chen, Q. Mei, and Y. Zhao, "Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 3, pp. 2089–2104, May-Jun. 2022.

[16] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[17] M. A. Alazzawi, H. Lu, A. A. Yassin, and K. Chen, "Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 71424–71435, 2019.

[18] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 1681–1695, 2021.

[19] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar.-Apr. 2021.

[20] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[21] K.-A. Shim, "$\mathcal{CPAS}$: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

[22] Y. Yang, L. Zhang, Y. Zhao, K.-K. R. Choo, and Y. Zhang, "Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 317–331, 2022.

[23] H. Cui, R. H. Deng, and G. Wang, "An attribute-based framework for secure communications in vehicular ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 721–733, Apr. 2019.

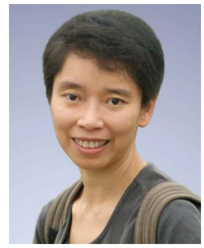
[24] H. Hou, J. Ning, Y. Zhao, and R. H. Deng, "A traitor-resistant and dynamic anonymous commun. serv. for cloud-based VANETs," *IEEE Trans. Serv. Comput.*, vol. 15, no. 5, pp. 2551–2564, Sep.-Oct. 2022.

[25] X. Liu, W. Chen, and Y. Xia, "Security-aware information dissemination with fine-grained access control in cooperative multi-RSU of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2170–2179, Mar. 2022.

[26] 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.
[27] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "An extensible and effective anonymous batch authentication scheme for smart vehicular networks," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3462–3473, Apr. 2020.
[28] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, "CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3456–3468, Apr. 2021.
[29] Z. Liu, M. Yuan, Y. Ding, and B. Wang, "Efficient small-batch verification and identification scheme with invalid signatures in VANETs," *IEEE Trans. Veh. Technol.*, vol. 70, no. 12, pp. 12836–12846, Dec. 2021.
[30] H.-W. Ferng, J.-Y. Chen, M. Lotfolahi, Y.-T. Tseng, and S.-Y. Zhang, "Messages classification and dynamic batch verification scheme for VANETs," *IEEE Trans. Mobile Comput.*, vol. 20, no. 3, pp. 1156–1172, Mar. 2021.
[31] P. Wang et al., "HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5071–5080, Aug. 2021.
[32] M. Ouaissa, M. Houmer, and M. Ouaissa, "An enhanced authentication protocol based group for vehicular communications over 5G networks," in *Proc. IEEE 3rd Int. Conf. Adv. Commun. Technol. Netw.*, 2020, pp. 1–8.
[33] B. Cao, Z. Sun, J. Zhang, and Y. Gu, "Resource allocation in 5G IoV architecture based on SDN and fog-cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3832–3840, Jun. 2021.
[34] J. Liu, Q. Li, H. Cao, R. Sun, X. Du, and M. Guizani, "MDBV: Monitoring data batch verification for survivability of internet of vehicles," *IEEE Access*, vol. 6, pp. 50974–50983, 2018.
[35] J. Li, Y. Ji, K.-K. R. Choo, and D. Hogrefe, "CL-CPPA: Certificate-less conditional privacy-preserving authentication protocol for the internet of vehicles," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10332–10343, Dec. 2019.
[36] D. Wang and J. Teng, "Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc network," *J. Electron. Inf. Technol.*, vol. 40, no. 1, pp. 11–17, 2018.
[37] X. Yang, R. Liu, M. Wang, and G. Chen, "Identity-based aggregate signature scheme in vehicle ad-hoc network," in *Proc. IEEE 4th Int. Conf. Mech., Control Comput. Eng.*, 2019, pp. 1046–10463.

Jingwei Liu (Member, IEEE) received the B.S. degree majoring in applied mathematics, and the M.S. and Ph.D. degrees majoring in communication and information systems from Xidian University, Xi'an, China, in 2001, 2004, and 2007, respectively. He is currently with the School of Telecommunications Engineering, Xidian University. He has authored or coauthored more than 70 papers in journals and conference proceedings and authored or coauthored two books. His research interests include Big Data security and privacy preservation, cloud and edge computing, and cryptography. He is a Member of the Chinese Association for Cryptologic Research.

Chuntian Peng is currently working toward the M.S. degree in information and communication engineering with Xidian University, Xi'an, China. Her research interests include vehicular network security, secure authentication protocols and privacy preservation.



Rong Sun (Member, IEEE) received the B.E. degree in telecommunications engineering, the M.E. degree in communications and information systems, and the Ph.D. degree in communications and information systems from Xidian University, Xi'an, China in 1998, 2001, and 2008, respectively. She is a member of IEICE. She is currently with the School of Telecommunications Engineering, Xidian University. Her research interests include wireless communications, channel coding design, and information theory.

Lei Liu (Member, IEEE) received the B.Eng. degree in communication engineering from Zhengzhou University, Zhengzhou, China, in 2010, and the M.Sc. and Ph.D. degrees in communication engineering from Xidian University, Xi'an, China, in 2013 and 2019, respectively. From 2013 to 2015, he was employed a subsidiary of China Electronics Corporation, Beijing, China. From 2018 to 2019, he was supported by the China Scholarship Council to be a Visiting Ph.D. Student with the University of Oslo, Oslo, Norway. He is currently with the Research Center of Trusted Digital Economy, Xidian Guangzhou Institute of Technology, Xi'an. His research interests include vehicular ad hoc networks, intelligent transportation, mobile-edge computing, and Internet of Things.

Ning Zhang (Senior Member, IEEE) received the B.S. degree from Beijing Jiaotong University, Beijing, China, in 2007, the M.S. degree from the Beijing University of Posts and Telecommunications, Beijing, in 2010, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2015. He was a Postdoctoral Research Fellow with the University of Waterloo and the University of Toronto, Toronto, ON. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Windsor, Windsor, ON. His research interests include connected vehicles, mobile edge computing, wireless networking, and machine learning. He is a Highly Cited Researcher (Web of Science). He was the recipient of the NSERC PDF Award in 2015, Six best paper awards from IEEE Globecom in 2014, IEEE WCSP in 2015, IEEE ICC in 2019, IEEE ICCC in 2019, IEEE Technical Committee on Transmission Access and Optical Systems in 2019, and *Journal of Communications and Information Networks* in 2018. He is also an Associate Editor for the IEEE INTERNET OF THINGS JOURNAL, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, IEEE ACCESS, and IEEE SYSTEMS JOURNAL, an Area Editor of *Encyclopedia of Wireless Networks* (Springer) and Cambridge Scholars, and the Guest Editor of several international journals, such as IEEE WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING. He is/was also the TPC Chair for the IEEE SAGC 2020, the Track Chair of several international conferences including IEEE VTC 2020, IEEE ICC 2022, AICON 2020 and CollaborateCom 2020, and the Co-Chair of numerous international workshops.

Schahram Dustdar (Fellow, IEEE) received the M.Sc. and Ph.D. degrees from the University of Linz, Linz, Austria, in 1989 and 1992, respectively. He is Full Professor of computer science heading the Research Division of Distributed Systems with the Vienna University of Technology, Vienna, Austria. He is the Co-Founder of an EdTech company in the U.S. (edorer.com) and SinoAus.net based in Nanjing, China, an R&D Lab focusing on AI and Edge Intelligence. He is the Founding Co-Editor-in-Chief of the *ACM Transactions on Internet of Things* and the Editor-in-Chief of *Computing* (Springer). He is an Associate Editor of the IEEE TRANSACTIONS ON SERVICES COMPUTING, IEEE TRANSACTIONS ON CLOUD COMPUTING, *ACM Computing Surveys*, *ACM Transactions on the Web*, and *ACM Transactions on Internet Technology*, and on the Editorial Board of IEEE INTERNET COMPUTING and IEEE Computer. Dustdar was the recipient of multiple awards: IEEE TCSVC Outstanding Leadership Award (2018), IEEE TCSC Award for Excellence in Scalable Computing (2019), TCI Distinguished Service Award 2021 by the IEEE Technical Committee on the Internet (TCI) (2021), ACM Distinguished Scientist (2009), ACM Distinguished Speaker (2021), IBM Faculty Award (2012). He is an Elected Member of the Academia Europaea: The Academy oz Europe, where he is chairman of the Informatics Section, and an IEEE Fellow (2016) and an Asia-Pacific Artificial Intelligence Association Fellow and president (2021) and Member of the Academy of the United Nations Science and Technology Organization (2021).

Victor C. M. Leung (Life Fellow, IEEE) received the B.A.Sc. (Hons.) and Ph.D. degrees in electrical engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 1977 and 1982, respectively. He is a Distinguished Professor of Computer Science and Software Engineering with Shenzhen University, Shenzhen, China. He is also an Emeritus Professor of Electrical and Computer Engineering and the Director of the Laboratory for Wireless Networks and Mobile Systems, UBC. His research interests include wireless networks and mobile systems, and he has published widely in these areas. Dr. Leung was the recipient of the 1977 APEBC Gold Medal, 1977C1981 NSERC Postgraduate Scholarships, IEEE Vancouver Section Centennial Award, 2011 UBC Killam Research Prize, 2017 Canadian Award for Telecommunications Research, the 2018 IEEE TCGCC Distinguished Technical Achievement Recognition Award, and the 2018 ACM MSWiM Reginald Fessenden Award. His coauthored papers were the recipient of the 2017 IEEE ComSoc Fred W. Ellersick Prize, the 2017 IEEE Systems Journal Best Paper Award, the 2018 IEEE CSIM Best Journal Paper Award, and the 2019 IEEE TCGCC Best Journal Paper Award. He is serving on the Editorial Board of the IEEE TRANSACTIONS ON GREEN COMMUNICATIONS AND NETWORKING, IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE ACCESS, IEEE NETWORK, and several other journals. He is a Fellow of the Royal Society of Canada (Academy of Science), Canadian Academy of Engineering, and Engineering Institute of Canada. He is named in the current Clarivate Analytics list of Highly Cited Researchers.