Journal of Network Intelligence
Taiwan Ubiquitous Information
 ISSN 2414-8105 (Online)
Volume **9**, Number **2**, May **2024**

Blockchain-based IVPPA Scheme for Pseudonym Privacy Protection in Internet of Vehicles

Hui Wang

School of Software
Henan Polytechnic University, Jiaozuo 454000, China
wanghui_jsj@foxmail.com

Fangyu Zhang, Zihao Shen*

School of Computer Science and Technology
Henan Polytechnic University, Jiaozuo 454000, China
zhangfangyu0425@163.comm, hpuxxfzyjs@qq.com

Peiqian Liu, Kun Liu

School of Software
Henan Polytechnic University, Jiaozuo 454000, China
liupeiqian@hpu.edu.cn

*Corresponding author: Zihao Shen

Received May 22, 2023, revised August 12, 2023, accepted March 26, 2024.

Abstract. *Existing Vehicular Ad-hoc Networks (VANETs), while enabling vehicles to communicate with each other, share data, and connect to external networks, also face a large number of data security challenges, such as data leakage and hijacking, cyber-attacks, and malware. For the security and privacy of vehicle user data in Internet of Vehicles (IoV), this paper proposes a blockchain-based IVPPA scheme for pseudonym privacy protection in IoV using a blockchain to assist the security of VANETs authentication and key certificate protocols. Firstly, Elliptic Curve Cryptography (ECC) and secure hash functions are introduced in the message signing and authentication scheme technique. Second, the hash operation is performed on the vehicle certificate and the certificate hash value and the certificate are stored on the blockchain, and the mutual authentication between the vehicle and the roadside unit (RSU) is realized by querying the hash value on the blockchain, which improves the effectiveness of the mutual authentication between the entities. Finally, the improved Merkle Patricia Trie (MMPT) is used to store and manage the pseudonyms assigned to the vehicle efficiently, thus avoiding the tracking of the vehicle path and the leakage of the vehicle information. Simulation experiments show that this scheme has significantly lower average latency in computing overhead and byte size in communication overhead than the comparison scheme, in which the communication overhead is only 232 bytes, which is about 50% of the highest overhead of the compared schemes, and has better authentication performance and stronger feasibility in the context of vehicle networking.*
Keywords: Internet of vehicles, Identity authentication, Message authentication, Change of pseudonym, Blockchain

1. **Introduction.** In 2022, the number of global IoT devices is expected to grow by 18% and will reach 14.4 billion. Global IoT device shipments have been on a growth trend as supply demand accelerates further [1], with the automotive network is a major factor in its rapid development. The emerging paradigm of Internet of Vehicles (IoV) has been

proposed to support the development of intelligent transportation systems [2, 3, 4], which integrates technologies such as vehicle self-organizing networks and the Internet of Things to enhance its capabilities, playing an important role in helping to avoid traffic accidents, alleviate traffic congestion, and provide diverse services. Generally speaking, IoV consists of a TA network authentication model, including On Board Units (OBUs), Road Side Units (RSUs) and Trusted Authority (TA) [5, 6]. IoV refers to a new generation of information and communication technology to achieve a comprehensive network connection of vehicle-to-pedestrians (V2P), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-network (V2N), to improve vehicle intelligence and autonomous driving capability, to reduce the accident rate, to improve traffic efficiency, and to provide users with intelligent, comfortable, safe, energy-saving and efficient integrated services [7].

Despite many potential benefits of IoV, it still faces some potential privacy issues [8, 9]. As the wireless communication characteristics of IoV, it is vulnerable to malicious attacks while driving on the road. In the absence of an efficient authentication architecture, attackers can easily damage drivers on IoV. For example, malicious vehicles with false content spread on the road may lead to traffic jams or traffic accidents and a series of hazards. Attackers trick or tamper with RSUs to gain access to sensitive information about other vehicles.

To address and protect the issue of vehicle security and privacy, a blockchain-based IoV pseudonym privacy authentication (IVPPA) schema is proposed. If a vehicle uses its true identity to communicate with other entities in IoV, it may be vulnerable to malicious attackers tracking vehicle routes and disclosing vehicle information. Therefore, in the authentication of this scheme, the vehicle uses a set of pseudonym IDs assigned by the TA for the vehicle during all communications and sets up an expiration time for pseudonym replacement, which effectively prevents the attacker from stealing the real identity of the vehicle. The main contributions of this paper are as follows:

(1) In order to ensure the privacy of vehicle user data, entities need to authenticate each other and reach key agreements to enhance security. Introducing the inherent characteristics of blockchain such as tamper-evident, an authentication scheme using digitally signed certificates [10] is proposed to effectively authenticate the vehicle. After that, the hash of the vehicle certificate is calculated and a certificate transaction is created to generate a new block to be attached to the blockchain to maintain information about the vehicle.

(2) By assigning a set of pseudonyms to each vehicle to ensure better pseudonym finding and updating operations, the Modified Merkle Patricia Tree (MMPT) [11] is used to efficiently store the pseudonyms of vehicles and the status of the pseudonyms to achieve vehicle anonymity.

(3) Each RSU assists vehicles in their respective regions in changing their pseudonyms based on the expiration time specified by their pseudonym to avoid tracking vehicle paths and leaking vehicle information. After the expiration of the validity period, each vehicle will communicate with the RSU and reactivate a new pseudonym from the group pseudonym.

The rest of the paper is presented as follows: Section 2 briefly reviews some related work. Section 3 presents the knowledge and preliminary data required for this paper. Section 4 provides a secure and effective authentication framework for vehicles using blockchain assistance. Section 5 analyzes the security and privacy of the scheme. Performance evaluation of the proposed scheme is discussed in Section 6. Finally, we conclude using concluding remarks.

2. **Related work.** Authentication between entities plays a critical role in secure message propagation. PKI-based anonymous authentication protocol was first proposed by Raya

et al. [12] in 2007, Certificate Authority (CA) based on the scheme protocol, all legitimate vehicle nodes in the system are equipped with unique public-private key pairs,and issue corresponding certificates for these public keys, the vehicles randomly select a set of stored keys and certificates when communicating signing the message. However, in this protocol, the vehicle not only needs to pre-load and periodically update a large number of public-private key pairs and certificates, but also needs to maintain a larger Certificate Revocation List (CRL, Certificate Revocation List), so the vehicle needs to store a large number of certificates, and in the process of authentication, the RSU has a huge amount of communication.Authentication between entities plays a critical role in secure message propagation. Kondareddy et al. [13] proposed a scalable CRL distribution method to quickly distribute CRLs to all OBU nodes with as little communication overhead as possible, but the method does not prevent a revoked vehicle from continuing to post messages within the system until all of its pseudonyms have expired. Azees et al. [14] proposed an efficient anonymous authentication scheme based on bilinear mapping, in which a method is designed for vehicles and RSUs to self-generate anonymous certificates through the pre-existing assigned parameters without the need for storage by a trusted authority TA, thus improving computational efficiency. In addition, TA can trace the real identity of malicious vehicles and revoke it, and the revoked vehicle information is placed in the Identity Revocation List (IRL, Identity Revocation List) maintained by TA, which is a process that satisfies the conditional privacy preservation but is computationally efficient.

Compared with PKI-based schemes, in group signature-based schemes, legitimate group member vehicles have private keys and group keys, and can sign messages with their own private keys on behalf of the whole group without disclosing private information. Liu. [15] et al. proposed two verification modes,single and batch verification, in order to reduce the computational pressure on the vehicle unit (OBU). The scheme first establishes a list of ring members, and then generates a group signature secret of ring members through bilinear mapping, which ensures the legitimacy of the system's vehicle identity by adding an accountability authority. However, the scheme does not completel-y solve the problem of auditing malicious vehicles, which can lead to the failure of the verification session. Zhang et al. [16] utilizes the identity of the vehicle, i.e., the vehicle does not need to be preloaded with a key pair and corresponding certificate, eliminating the need for large storage and thus reducing the overall processing overhead. In addition, it alleviates the need to manage certificates and CRLs,However, the scheme does not satisfy traceability requirements and these schemes are also vulnerable to emulation and replay attacks. Xie et al. [17] proposed an authentication scheme based on conditional privacy preservation that utilizes id-based signatures to ensure the reliability and integrity of messages in VANETs. Authentication between entities plays a critical role in secure message propagation.

In a blockchain-based privacy-preserving approach, Kang et al. [18] realized data sharing and information security in the IoV by using mobile edge computing and blockchain, but the authentication scheme does not support two-way authentication, so the security is lower than the two-way authentication scheme. Wang et al. [19] proposed a blockchain-based scheme for computing vehicle trustworthiness and implementing cross-domain authentication. This method can reduce the amount of computing and communication loss in the subsequent authentication process, but the amount of computing in the initial authentication process is still relatively large. Yao et al. [20] proposed a distributed blockchain-assisted lightweight anonymous authentication mechanism that achieves anonymity and grants vehicle users the responsibility to protect their privacy. However, all entities in the scheme are assumed to be trusted, which is difficult to implement in real life. Wang et al. [21] proposed an efficient, blockchain-based decentralized

authentication mechanism for IoV, which can well solve the centralization problem in traditional centralized authentication,but does not protect the privacy information of the vehicle and does not provide a complete security analysis of it,and the vehicle is very vulnerable to security attacks such as identity transfer.

3. **Problem Description.** This section will introduce the system model, prerequisite knowledge, and security objectives required for this paper. Table 1 below shows the symbols and descriptions used in this paper.

Table 1. System Symbols and Descriptions

Notation	Description
V_i	The ith vehicle
RSU_i	The ith RSU
RID_{r_i}	The true identity of the RSU_i
RID_{V_i}	The true identity of the V_i
AID_{V_i}	Initial anonymous identity of V_i
pk_{TA}, sk_{TA}	Public and Private Keys of the TA
pk_{RSU_i}, sk_{RSU_i}	Public and Private Keys of RSU_i
pk_{V_i}, sk_{V_i}	Public and Private Keys of vehicle V_i
pk_{PCA_i}, sk_{PCA_i}	Public and Private Keys of vehicle PCA_i
σ_{TA,RSU_i}	Signature signed by TA secret key for RSU_i
Cre_{RSU_i}	Certificate of RSU_i generated by TA
σ_{TA,V_i}	Certificate of V_i generated by TA
$\|\|$	Message concatenation
T_R	A timestamp of RSU
H	A one-way hash function
$PID_{V_{initial}}$	Initial pseudonym assigned to Vehicle V
$PID_{V_{curr}}$	Pseudonym currently used by Vehicle V
$PID_{V_{new}}$	New Pseudonym activated for Vehicle V
t_{exp}	Initial Pseudonym Expiration Time of V
t_{new}	Current Pseudonym Expiration Time of V
t'_{new}	Newly Activated Pseudonym Expiration Time of V
t_s	Message generation timestamp
K_s	Session key between vehicle V and RSU

3.1. **System model.** The required system model architecture, entity types, and the main functions and related technologies of each entity in this paper are shown in Figure 1.

(1) TA: Each region is managed by a TA, which will issue public parameters and define the code of conduct in the system initialization and is a trusted entity in this paper. It is also responsible for issuing certificate tasks for registered nodes, managing the blockchain network and maintaining block generation.

(2) Pseudonym Certificate Authority (PCA): Pseudonym service is provided for legal vehicles in the system, and vehicles can apply for pseudonyms to PCA only after obtaining certificates.

(3) RSU: Data management node with storage, computing, communication, and other functions, installed by official agencies on traffic sections. Each RSU maintains an MMPT that is responsible for storing and verifying the pseudonyms of vehicles.

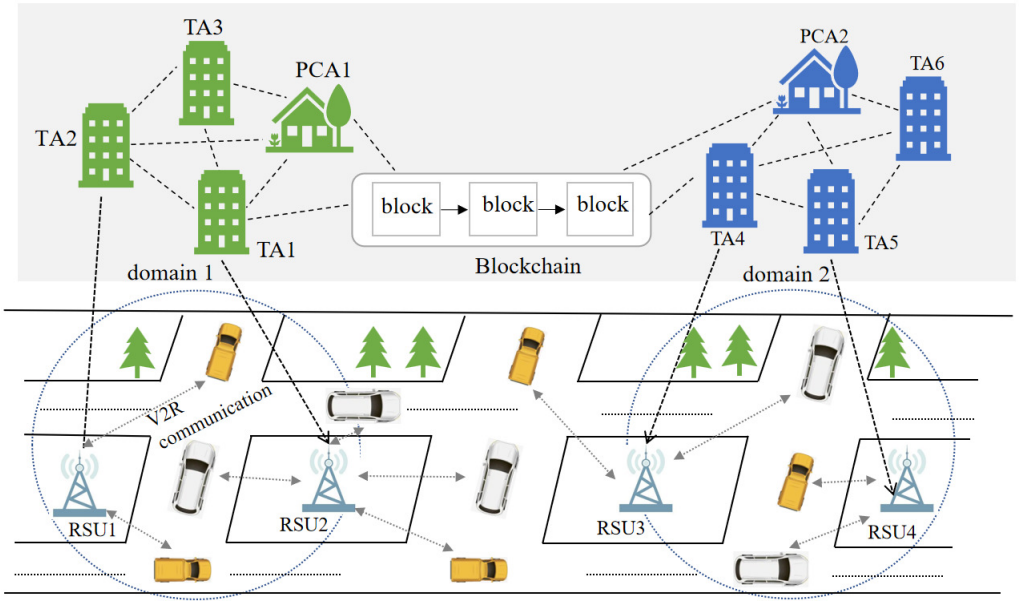

FIGURE 1. Vehicle Internet System Model

(4) OBU: The on-board unit is embedded in the vehicle and broadcasts traffic-related information, location identifiers and driving status, etc. The vehicle is also equipped with multiple sensors, TPD, and communication modules.

3.2. **Blockchain technology.** A blockchain is a chain composed of one block after another, as shown in Figure 2. Certain information is stored in each block, and the block contains two parts: the block header and the block body [22, 23]. Blockchain as a tamper-evident distributed ledger [24], its unique temporality, invariance, unforgeability, transparency, and audibility can automatically record time-stamped vehicle information and interconnect through block hashes, potentially avoiding data tampering and enabling traceability of transactions under the distributed ledger, which helps in accurate auditing. Moreover, blockchain relies on modern cryptography technology, which can provide better security and privacy for IoV. In blockchain-based IoV, each user can manage his key, and each block node only needs to store the encrypted slice of user data. At the same time, all peer nodes are synchronized and replicated with each other, so that even if one or more nodes are damaged, the service can run smoothly, making IoV more resistant to destruction.

3.3. **Safety objectives.** The solution in this paper should meet the following security and privacy protection requirements.

(1) Correctness and integrity of certification. For correctness attributes, it is always possible to verify that the authorized vehicle is indeed a legal entity. For integrity attributes, to ensure the security of the communication, both the vehicle and the RSU need to be able to recognize if there is a change in the received message and to verify the correctness of the received message.

(2) Anonymity and conditional privacy of the vehicle. The IoV has openness, so vehicles must interact with other entities anonymously during communication, and no entity within the network (excluding TA) can obtain the true identity of a network participant, that is, the true identity of the participant is confidential to any entity outside of TA.

(3) Unlinkability. No entity can link two or more received messages to the same vehicle.

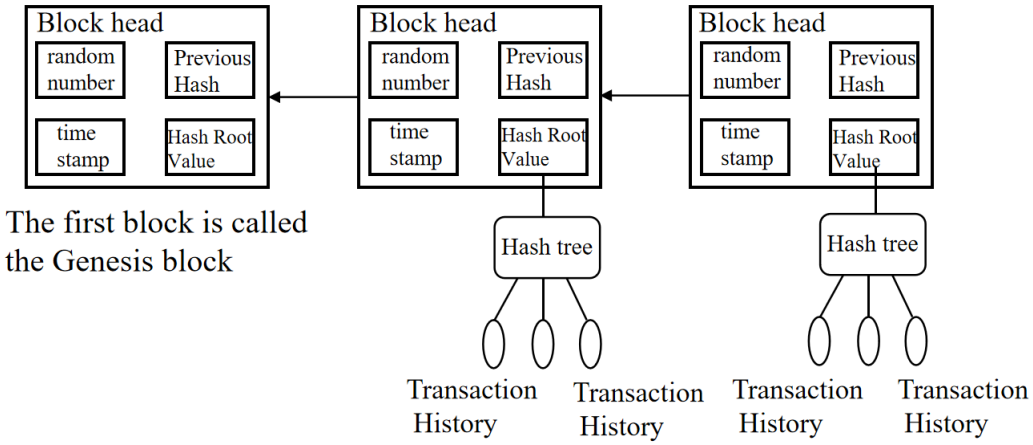

FIGURE 2. Blockchain Structure

(4) Non-repudiation. When transmitting data, the information carried by the vehicle must have its own characteristics and cannot be replicated by others to avoid being denied after the transaction occurs.

(5) Resistance to Sybil attacks. By assigning a certain number of pseudonyms and expiration times to vehicles, attackers can be prevented from using multiple pseudonyms in parallel to simulate witch attacks on multiple vehicles.

(6) Resistance to message injection attack. Using certificates and calculating the hash value of certificates, the blockchain maintains the security of messages.

4. **Blockchain-based pseudonym IVPPA scheme.**

4.1. **Scheme Overview.**

In this paper, the identity trust relationship of the vehicle is established using TA network model. An authentication scheme using digital signature certificates is proposed to effectively authenticate vehicles, and the vehicle certificate and the hash value of the certificate are used as blockchain nodes to maintain the relevant information about the vehicles; at the same time, vehicle pseudonyms are allocated and inserted into the MMPT maintained by RSU to achieve the storage and status of pseudonyms. Figure 3 shows the basic process of vehicle identity management and authentication, with each stage described in detail below.

4.2. **System initialization.**

4.2.1. *System parameter generation.*

(1) TA selects an additive group G of order q, which consists of the point $E : y^2 = x^3 + ax + b(\text{mod p})$ on the elliptic curve and the points at infinity O, where $a, b \in F_p$, p and q are two large prime numbers, and P is its generator. Then TA selects four secure one-way hash functions: $H_0 : G \times \{0,1\}^* \to Z_q^*, H_1 : \{0,1\}^* \to Z_q^*, H_2 : G \times G \to Z_q^*, H_3 : \{0,1\}^* \times \{0,1\}^* \times G \times G \times \{0,1\}^* \to Z_q^*$.

(2) TA randomly selects an integer $sk_{TA} \in Z_p^*$ as the private key and then calculates its public key $pk_{TA} = sk_{TA} \times P$. Publish public parameters $(G, p, q, a, b, pk_{TA}, H_0, H_1, H_2, H_3)$ to all entities and record them on the blockchain, preserving their keys. In addition, PCA generates its key pair $\{pk_{PCAi}, sk_{PCAi}\}$, where the public key is published on the blockchain.

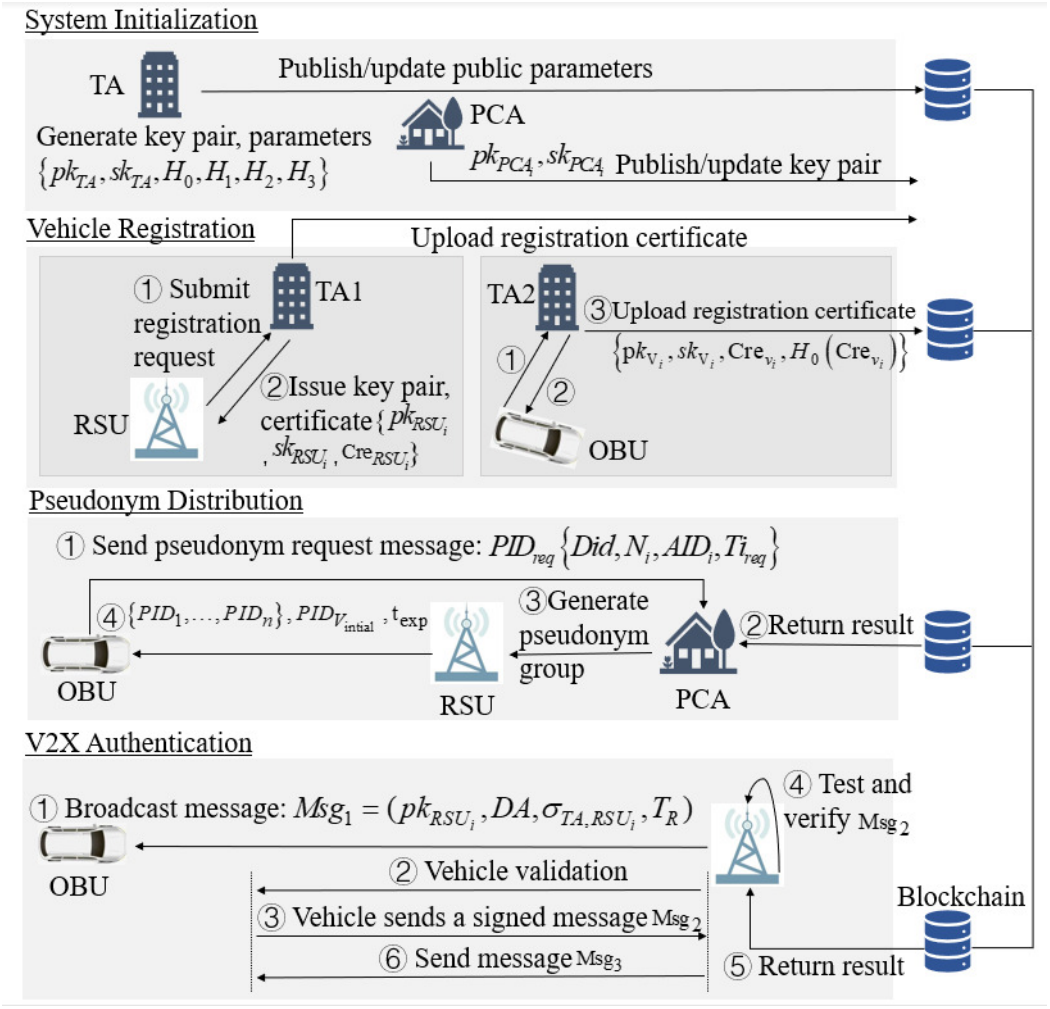

FIGURE 3. Vehicle Identity Management and Authentication

4.2.2. *RSU registration.*

(1) Suppose the real identity of RSU_i is RID_{r_i} , and RSU_i sends RID_{r_i} to TA through a secure channel; After receiving the registration request from RSU_i , TA first detects in its own database whether RID_{r_i} is registered or has been cancelled. If so, TA ignores this message; Otherwise, TA will proceed to the next step.

(2) After the check is successful, the TA selects a random number $sk_{RSU_i} \in Z_p^*$ as the private key of the RSU_i, and then calculates the public key $pk_{RSU_i} = sk_{RSU_i} \times P$. That is the public and private key pair $\{pk_{RSU_i}, sk_{RSU_i}\}$ of the RSU_i .

(3) TA signs RSU_i with its private key, $\sigma_{TA,RSU_i} = \mathrm{Sig}\,(pk_{RSU_i} \| DA, sk_{TA})$, and generate a certificate $\mathrm{Cre}_{RSU_i}\,(ID_{RSU_i}, \sigma_{TA,RSU_i}, C_{R_i})$, C_{R_i} is the valid period of the certificate, and ID_{RSU_i} is the true identity of the RSU_i .

(4) TA provides $\{pk_{RSU_i}, sk_{RSU_i}\}$ and its certificate Cre_{RSU_i} to RSU_i through a secure channel.

4.2.3. *Vehicle registration.*

(1) Suppose the real identity of the vehicle is RID_{V_i}, and V_i sends $< RID_{V_i} >$ to the TA through a secure channel; After receiving the registration request from V_i , TA first detects in its own database whether RID_{V_i} is registered or has been cancelled. If so, TA ignores this message; Otherwise, TA will proceed to the next step.

(2) For vehicle users with real identity RID_{V_i} , TA randomly selects a $a_i \in Z_p^*$ and generates an anonymous identityAID_{V_i} for them through Equation (1) to protect identity privacy.

$$AID_{V_i} = RID_{V_i} \oplus H_1(a_i) \tag{1}$$

TA secretly saves the registration information table registry $= \{a_i, RID_{V_i}, AID_{V_i}\}$ as the identity information of the vehicle.

(3) TA selects a random number $sk_{V_i} \in Z_p^*$ as the private key of V_i and calculates the public key $pk_{V_i} = sk_{V_i} \times P$, which is the public private key pair (pk_{V_i}, sk_{V_i}) of V_i. TA signs V_i with its private key, $\sigma_{TA,V_i} = \mathrm{Sig}(pk_{V_i}\ sk_{TA})$, and generate a blockchain certificate $\mathrm{Cre}_{Vi}(AID_{V_i}, \sigma_{TA,V_i}, C_{Vi})$, Where C_{V_i} is the valid period of vehicle V_i certificate, which is hashed to obtain $H_0(Cre_{V_i})$. The TA sends pk_{V_i}, sk_{V_i}, and $H_0(Cre_{V_i})$ to the V_i for storage in the OBU.

(4) TA will then initiate a transaction offer with the vehicle certificate Cre_{V_i} and the $H_0(Cre_{V_i})$ corresponding to the certificate, create the correct transaction block and attach it to the identity chain, after which the identity chain verifies the legitimacy of the certificate. After the legitimacy verification is completed, if the certificate is legitimate, the node will generate a new block with the legitimate certificate not currently included in the block as a transaction in the blockchain and broadcast it to the entire network. Then the identity chain returns the message of successful authentication to the user, at which point the user has successfully registered. If the certificate is not legal, the user's registration fails and the vehicle cannot access the car network.

4.3. **Process description of vehicle pseudonyms.**

4.3.1. *pseudonyms Generation.* To protect the privacy of the vehicles, the vehicles will not use its true identity during communication. There are multiple ways to generate pseudonyms for vehicles, however, this issue is not discussed in this paper.

Any vehicle with a valid registration certificate can request a new pseudonym from the PCA nearest to its location. When a vehicle V_i needs pseudonym service after registering with a TA, send a pseudonym request and the vehicle certificate hash $H_0(Cre_{V_i})$ to the local PCA:

$$PID_{req}\{Did, N_i, AID_i, Ti_{req}\} \tag{2}$$

Where Did represents the domain identifier, N_i represents the number of pseudonym, Ti represents the current timestamp and the anonymous identity AID_{Vi} given to the vehicle by the TA. After receiving the request, PCA performs verification and pseudonym assignment. PCA based on the vehicle certificate hash value received from the blockchain, PCA verifies that the vehicle is legitimate if the obtained hash value $H_0(Cre_{V_i})$ is equal to the hash value sent by the vehicle. The PCA then generates a set of pseudonyms $\{PID_1, \ldots, PID_n\}$ for each vehicle based on the vehicle's anonymous identity AID_{Vi} stored in the vehicle's OBU and sends $\{PID_1, \ldots, PID_n\}$, $PID_{V_{intial}}$, and t_{exp} to all RSUs in the region, where $PID_{V_{intial}} \in \{PID_1, \ldots, PID_n\}$, t_{exp} is the expiration time of the $PID_{V_{intial}}$.The OBU stores its own public and private key pairs, hash values of vehicle certificates, a set of pseudonyms and $PID_{V_{intial}}$.

Each RSU maintains an MMPT, which is used to store and update the pseudonyms of vehicles. When vehicle V_i uses $PID_{V_{intial}}$ to communicate with the first encountered RSU_i, PCA sends $\{PID_1, \ldots, PID_n\}$, $PID_{V_{intial}}$ and pk_{V_i} to all RSUs in its region. After receiving this message, RSU_i connects pk_{V_i} with the pseudonym and inserts the pseudonym into the MMPT along with the state of the pseudonym. The initialization

$PID_{V_{intial}}$ status is set to 1, and the status of other the remaining pseudonyms is set to 0.

4.3.2. *Pseudonym-based lookup and insertion operations in MMPT.* MMPT is a data structure that improves the combination of two tree structures, Merkle Tree and Patricia Tree. The scheme uses an MMPT to store pseudonyms, where each node is represented by a key-value pair.

(1) Empty node: used to represent the empty string.

(2) Branch nodes: denoted by the prefix 1. There can be up to 16 child nodes, one corresponding to each hexadecimal number from 0 to f.

(3) Leaf nodes: leaf nodes have no children and are denoted by the prefix 2. Each leaf node contains each pseudonym assigned to a vehicle (remaining pseudonym segment, status); the status of that pseudonym (1 or 0) indicates whether the vehicle is currently using that pseudonym.

(4) Extended node: The extended node has a prefix of 0. Its key field contains a partial path (shared nibble) that allow pointing to the next node.

Figure 4 shows the MMPT storing these four pseudonyms and their states, and Table 2 represents an example list of the four pseudonyms contained in the vehicle and their current states. In the MMPT, the root node is an extended node containing the "shaerd nibble" and "next node" fields. The "shaerd nibble" is the public key of the vehicle connected to the pseudonym, and the "next node" field points to the branch node after it.

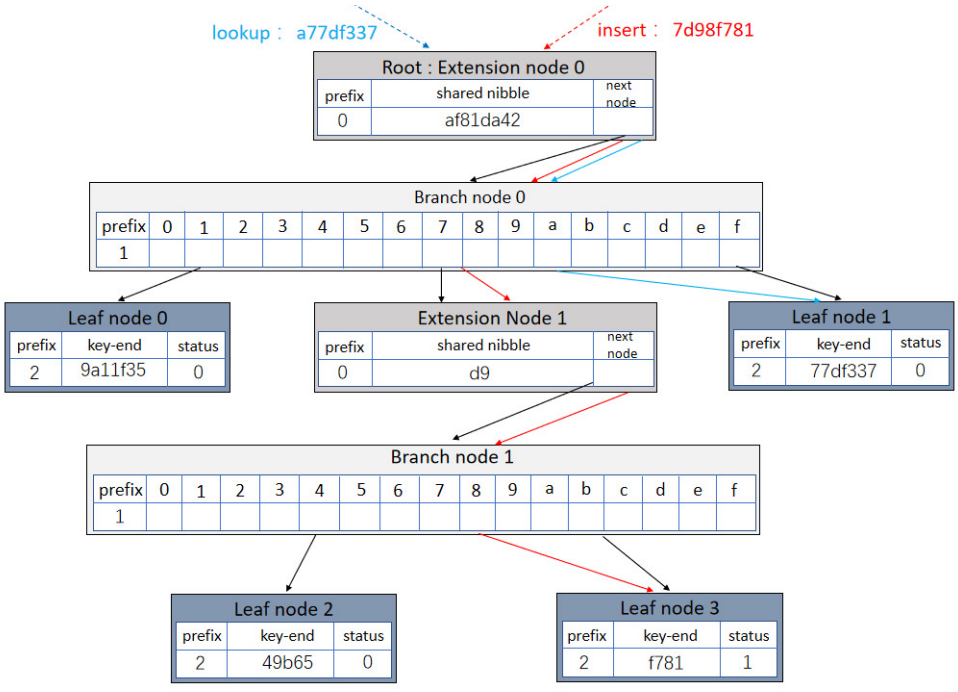

FIGURE 4. MMPT for storing pseudonyms

The lookup operation is based on vehicle pseudonyms traversing down the lookup from the root node of MMPT in order. The second pseudonym in Table 3 "a77df337", can be found after "af81da42" to continue to the next level, which is the leaf node 1 shown in Figure 4, which is used to store the remaining pseudonyms and their current status. So, if you want to find an MMPT pseudonym, you have to start from the root node and then go

Table 2. Pseudonyms and current status

Pseudonym	Status
19a11f35	0
a77df337	0
7d949b65	0
7d98f781	1

to the next node according to "shared nibble" and the remaining pseudonym segments. Eventually, when you reach the leaf node, you will find the pseudonym and its state.

To insert the vehicle's pseudonym into MMPT for maintenance, it should first be inserted from the root node, followed by determining the prefix value and nibbles of the current node. if the slot after the node is NULL, a new leaf node or an extended node is generated and the remaining fields of the pseudonym are written into the node; if the slot is not NULL, it will be traversed to the next given node to continue the lookup. For example, in Figure 4, first, insert the pseudonym "7d98f781" from the root node, then connect it to the public key "af81da42" of the vehicle, and check that the current root node has a prefix of 0, which is an extended node. Next iterate branch node 0, because the slot corresponding to the next prefix 7 in branch node 0 is not NULL, and the number of remaining fields in this pseudonym is greater than 1, therefore, iterate to extension node 1. the Next Node of current extension node 1 point to branch node 1, and the slot corresponding to prefix 8 in branch node 1 is NULL. finally, the slot corresponding to the next prefix 8 in branch node 1 Finally, a new leaf node 3 is generated under the slot corresponding to the next prefix 8 in branch node 1, and the status is set to 1, indicating that this is the pseudonym used by the current vehicle.

4.3.3. *Mutual authentication of vehicle and RSU.*

(1) The RSU broadcasts messages regularly, for an RSU_i in a domain DA, the message is

$$Msg_1 = (pk_{RSU_i}, DA, \sigma_{TA,RSU_i}, T_R) \tag{3}$$

After the vehicle receives the Msg1, it first checks if it is a new domain. If it is, the vehicle validates RSUi according to Equation (4).

$$verify\left(pk_{TA}, \sigma_{TA,RSU_i}, pk_{RSU_i}\right) \stackrel{?}{=} 1 \tag{4}$$

(2) If RSU_i is valid, all messages sent by vehicles must be signed and confirmed before being received by RSUs or other vehicles to ensure the integrity of the message.

a) The vehicle randomly selects a $r_i \in Z_p^*$ and calculates R_i , H_i , and Sig_i as in Equations (5), (6), (7)

$$R_i = r_i \times P \tag{5}$$

$$H_i = H_3\left(PID_{V_{inital}}, pk_{V_i}, R_i, t_s\right) \in Z_p^* \tag{6}$$

$$Sig_i = \left(H_2\left(R_i\right) + sk_{V_i} \cdot H_i\right) \cdot r_i \tag{7}$$

where t_s is the current timestamp of the message signature.

b) Then, the vehicle sends the signature message Msg_2 to the RSU_i.

$$Msg_2 = \left\{H_0\left(Cre_{v_i}\right), PID_{V_{intial}}, pk_{V_i}, R_i, t_s, Sig_i\right\} \tag{8}$$

c) After receiving a signed message from a vehicle, check the freshness of the timestamp t_s and delete this message if it is not fresh.

d) If t_s is valid, calculate H_i.

$$H_i = H_3\left(PID_{V_{inital}}, pk_{V_i}, R_i, t_s\right) \in Z_p^* \tag{9}$$

and verify whether Equation (10) holds.

$$R_i \cdot \mathrm{sig}_i \cdot pk_{V_i} \cdot H_1\left(PID_{V_{initial)}}\right) \cdot H_i = P \times H_2\left(R_i\right) \tag{10}$$

When the Equation (10) is satisfied, the receiver accepts the message Msg_2 , and vice versa, the receiver rejects the message.

(3) After receiving the message, RSU_i queries the blockchain for the hash value $H_0(Cre_{V_i})$.

a) If there is no query result, the RSU_i fails to authenticate the V_i .

b) If the query result obtained is revoke, the V_i certificate is in the revocation state and the authentication fails.

c) If the hash value found is equal to the hash value sent by the V_i , the RSU_i response authentication is successful.

d) After successful authentication, RSU_i will generate a session key K_s, encrypt the random number K_1 with K_s , encrypt K_s and pk_{V_i} with V_i public key pk_{RSU_i}, and send the message Msg_3 to V_i.

$$Msg_3 = \left(E_{pk_{V_i}}\left(K_s, pk_{RSU_i}\right), E_{K_s}\left(K_1\right), K_1\right) \tag{11}$$

(4) After the vehicle receives the message, the vehicle uses its own private key sk_{V_i} to decrypt to obtain K_s and pk_{V_i} and check the validity of K_1, thus completing the mutual authentication of V2R. After the initial authentication, the vehicle and RSU_i will get the session key K_s between them, and the session key can be updated once in a certain time interval by setting the valid time duration of K_s.

(5) After authentication, RSU_i connects the public key pk_{V_i} of the vehicle to the $PID_{V_{intial}}$ and sets the status of the $PID_{V_{intial}}$ to 1 in MMPT. Also, RSU sets a new expiration time t_{new} for the $PID_{V_{intial}}$ and signs it.

4.4. **Update pseudonym status.** Helps vehicles in its area to change their pseudonyms by setting the expiration time of the vehicle pseudonyms. If the expiration time of a pseudonym expires, the vehicle needs to send a pseudonym change request to the RSU in its region in order to reactivate a new pseudonym from the set of pseudonyms received by the PCA. Algorithm 1 gives the update on the pseudonym status through the RSU.

4.5. **Vehicle withdrawal.** When a vehicle performs a malicious act, performing identity revocation ensures effective identity management of the vehicle, including the ability for the RSU to revoke all pseudonyms of a misbehaving vehicle based on revocation before the pseudonym expiration time, while notifying the TA of the revocation of the vehicle's certificate.

If the vehicle is in the process of communication, RSU detects the malicious vehicle, then all the pseudonyms and vehicle certificates of the vehicle should be revoked. First, find the pseudonym $PID_{V_{curr}}$ currently used by the vehicle, find the prefix node with the longest identical path in the MMPT according to the lookup operation, and record it as "node".

(1) If node is an extended node

If the prefix node and the node match exactly, the corresponding node is deleted directly. If the prefix node and node do not match exactly, the that is, delete the extended node and do a recursive call to delete its prefix.

(2) If node is a branch node

The node with the corresponding subscript flag in the child list is deleted, and after the deletion, the branch node is replaced as a leaf node or extension node. Then RSU

Algorithm 1: Pseudonym state update algorithm

Input: $(E(PID_{V_{curr}}, PID_{V_{new}}, pk_{V_i}, t_s), K_s), PID_{V_{curr}}, t_{new}$
Output: $PID_{V_{intial}}$, t_{new}

```
RUS decrypts messages with K_s;
Checks the freshness of the received message using t_s;
if t_s is valid then then
    Looks up into MMPT for PID_{V_curr} and PID_{V_new};
    if PD_{V_curr}, PD_{V_new} ∈ MMPT then
        Sets the status of these pseudonyms to 0 and 1 respectively;
        Sets expiration time t'_new for PID_{V_new};
        Sends (E(E(PID_{V_new}||t'_new), pk_{RSU_i}), t_s), K_s) to V_i;
    else
        Does not update and ignores the message;
    end
else
    Drops the received message;
end
```

sends the request message Msg_r for revoking the vehicle certificate, which is signed by pk_{TA} and sent to TA.

$$Msg_r = \sigma msg, pk_{TA}\{revoke, H(pk_{V_i} \| \sigma TA, V_i)\} \tag{12}$$

After receiving the request to decrypt the message using its private key and verifying the legitimacy of the RSU, the TA looks up the vehicle certificate and certificate hash corresponding to that vehicle from the blockchain to perform the deletion operation and broadcasts the vehicle revocation message to all entities.

5. **Security and privacy analysis.** Next, we analyze the security features of the IVPPA protocol and prove that our designed protocol is anonymous and private, non-repudiation and unlinkable, and resistant to replay attacks, man-in-the-middle attacks, tampering attacks, and Sybil attacks.

(1) Simulation attack: Enemies may disguise themselves as participants in the entire communication, such as a vehicle, RSU, etc.

Challenge 1 (Simulation attack on a vehicle): When Enemy E1 disguises himself as a legitimate vehicle, he can forge a vehicle certificate Cre_{V_i} to make the system subject believe that he is legitimate.

Resistance: Enemy E1 attempts to forge the authorized vehicle. When communicating with each other in the RSU, authentication is performed through the RSU. To calculate the hash value of the certificate $H_0(Cre_{E1})$, enemy E1 needs to guess the real identity of the legal vehicle $RIDv_i$, the signature signed by the TA private key, and the timestamp of the certificate. Since the true identity of the vehicle is known only to the TA, and the anonymized identity AID_{E1} is calculated from Equation (1) $AID_{E1} = RID_{E1} \oplus H_1(a_i)$. If the enemy E1 executes a one-way hash function to calculate the hash value of the certificate and sends it to RSU without knowing these identity parameters, RSU believes that the received hash value does not match the hash value saved by the blockchain, resulting in authentication failure. Similarly, no enemy can forge a vehicle corresponding to $H_0(Cre_{E1})$. Therefore, this scheme can be a good defense against vehicle simulation attacks.

Challenge 2 (Simulation Attack on RSU): When enemy E2 disguises himself as an authorized RSU, he can forge a certificate Cre_{RSU_i} to convince the vehicle that it is legitimate.

Resistance: RSU broadcasts messages regularly, and when the vehicle receives the broadcast message $Msg_1 = (pk_{E2}, DA, \sigma_{TA,E2}, T_{E2})$ sent by E2, the vehicle verifies the credentials of E2 by running Equation (4) $verify\,(pk_{TA}, \sigma_{TA,E2}, pk_{E2}) \stackrel{?}{=} 1$. Since E2 is not authorized by the TA, the verification process fails and the legitimate vehicle does not send any message to the enemy E2. When the vehicle verifies the RSU, the RSU sends the vehicle the certificate issued by the TA signature, and the session key K_s. the vehicle first verifies whether the certificate is issued by the TA registration and since no one can forge the TA signature, the authentication fails; At the same time to forge K_s, enemy E2 needs to guess the random number K_1, which will cause the authentication to fail, because the value of K_1 is wrong,the vehicle then ignores the message.

(2) Privacy Analysis

a) Anonymity and privacy of the vehicle: Firstly, the real identity of the vehicle is never used in the communication process, only the trusted institution TA knows it. Secondly, the vehicle uses a pseudonym for communication, and the hash value of the anonymous identity of the vehicle is stored in the blockchain, which ensures that the real identity of the vehicle is not obtained. Finally, the pseudonym is changed frequently by setting the expiration time of the vehicle pseudonym to ensure the privacy of the message sent by the vehicle.

b) Non-repudiation: The vehicle uses pseudonyms to send messages during communication, including pseudonym expiration times signed by the RSU. Since the vehicle uses the pseudonyms in its stored pseudonym group to communicate with the RSU, the vehicle cannot reject the messages it sends

c) Unlinkability: Vehicles change frequently during communication by means of pseudonym expiration times, and since vehicles change their pseudonyms simultaneously, it reduces the chance of linking messages sent by the same vehicle using two different pseudonyms.

d) Resisting Replay Attacks: When an entity receives a message during communication, each message uses a timestamp to ensure the validity of the message, and by adding a timestamp t_s, the entity can detect whether the message is fresh or not.

e) Resisting man-in-the-middle attacks: Entities authenticate each other during a session to prevent man-in-the-middle attacks. For example, the RSU and PCA authenticate the vehicle through the hash of the vehicle certificate; the vehicle is authenticated through the RSU's certificate and session key.

f) Resistance to tampering attacks: firstly, the hash of the vehicle certificate is calculated by multiple parameters, and it is difficult for an adversary to guess the parameters and calculate the correct hash value; Secondly, the hash value of the vehicle certificate is stored in the blockchain, and the tamper-proof nature of the blockchain can effectively protect the value from malicious acts; Finally, for digital signatures used in vehicles, only a valid signature can be generated with a legitimate and valid pseudonym and key, This ensures that tampering attacks are difficult to achieve during the communication of the system.

g) Resistance to Sybil attacks: In the scheme of this paper, each vehicle stores a set of pseudonyms and the current expiration time of the pseudonyms. When the vehicle's pseudonym expiration time expires, the RSU in the area where the vehicle is located communicates with the vehicle to change the pseudonym and reset a new expiration time. Thus, only one vehicle's pseudonym is valid at a time to resist witch attacks.

6. **Performance evaluation.** For comparison, the experiments are deployed on a desktop based on Python 3.7 using an Intel I7-8700 processor with a 3.20GHz clock frequency and 8GB of RAM. For ECC-based vehicle authentication, the order of the additive group G and the prime number p is set to 256 bits, resulting in a length of 512 bits for the elements in group G. In addition, SHA-256 is chosen as the hash function. The performance in terms of computation and communication overhead will be analyzed and compared with existing similar schemes, including Anil's [25], BASA [26], and EPA-CPPA [27]. In the computational overhead, the type and number of computations that need to be performed for message signing and message verification in these scenarios are analyzed. In the communication overhead, the number of message bytes that need to be added for vehicle-generated broadcast messages in these scenarios is analyzed.

6.1. **Computational Overhead Analysis.** In the mutual authentication phase of the vehicle and RSU, the main operations in authentication are elliptic curve point multiplication, elliptic curve point addition, and hash function. In the operation of the bilinear pair cipher, let T_{bp} denote the time required to perform the bilinear pair operation. Let T_{bp}^{m} and T_{bp}^{a} denote the operation times required for scalar multiplication and addition in the bilinear mapping, respectively. In the operation of elliptic curve cipher, let T_{ecc}^{m} and T_{ecc}^{a} denote the operation time required to perform scalar multiplication and point addition on ecc in the additive group G, respectively; T_{ep} indicates the execution time of exponentiation operation and let T_h denote the time required to perform the cryptographic hash function operation.

BASA scheme is based on bilinear pair cipher, in the message authentication process, The vehicle performs 1 bilinear pair operation, 1 bilinear pair multiplication operation, 1 exponentiation operation and 1 one-way hash function operation on the message signature is $1T_{bp} + 1T_{bp}^{m} + 1T_{ep} + 1T_h$; Message validation requires the execution of 2 linear pair operations, 2 bilinear scalar multiplication operations, 1 bilinear pair addition operation, 1 exponentiation operation operation and 2 one-way hash function operations, and the total computational overhead for message validation is $2T_{bp} + 2T_{bp}^{m} + 1T_{bp}^{a} + 1T_{ep} + 2T_h$.

The message authentication scheme proposed in this paper is based on elliptic curve cipher, in the message authentication process, the vehicle performs 1 elliptic curve scalar multiplication operation and 2 one-way hash function operations on the message signature, and the computational overhead of the message signature is $1T_{ecc}^{m} + 2T_h$; the message authentication needs to perform 3 elliptic curve scalar multiplication operations, 1 elliptic curve point addition operation and 2 one-way hash function operations, and the computational overhead of the message authentication is $3T_{ecc}^{m} + 1T_{ecc}^{a} + 2T_h$. Similarly, the computational overheads in other schemes can be calculated, and the computational overheads of this paper's scheme and the comparison scheme are listed in Table 3.

Table 3. Comparison of computational overhead

programs	Message signature	Message Authentication
Anil's	$1T_{ecc}^{m} + 1T_h$	$3T_{ecc}^{m} + 2T_{ecc}^{a} + 2T_h$
BASA	$1T_{bp} + 1T_{bp}^{m} + 1T_{ep} + 1T_h$	$2T_{bp} + 2T_{bp}^{m} + 1T_{bp}^{a} + 1T_{ep} + 2T_h$
EPA-CPPA	$1T_{ecc}^{m} + 2T_h$	$4T_{ecc}^{m} + 1T_{ecc}^{a} + 2T_h$
IVPPA	$1T_{ecc}^{m} + 2T_h$	$3T_{ecc}^{m} + 1T_{ecc}^{a} + 2T_h$

As can be seen from Figure 5, the computational overhead increases linearly with the number of vehicles, and the BASA scheme has the largest computational overhead. The average delay of the scheme in this paper is smaller, and vehicles with limited computational power can handle these overheads even under heavy traffic conditions.

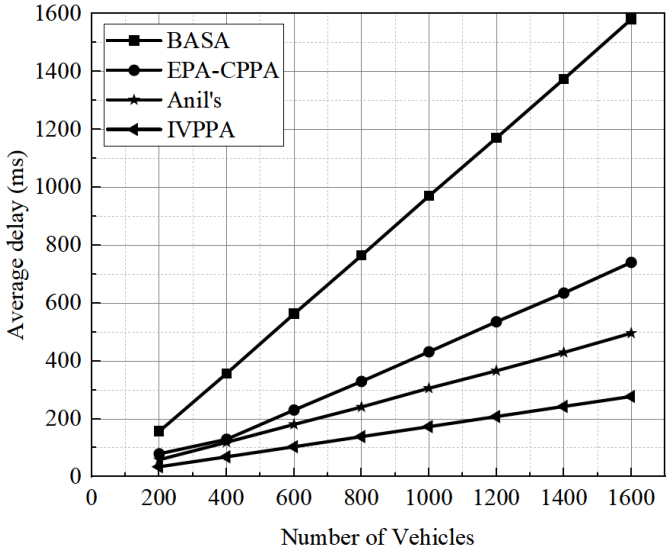

FIGURE 5. Comparison of computational overhead

6.2. **Communication overhead analysis.** In calculating the communication overhead, only the size of the message signature is considered. Assume that the size occupied by the elements in group G is 64 bytes, let the element timestamp in Z_p^* occupy a byte size of 4 bytes, and the one-way hash function occupies a byte size of 32 bytes.

In the EPA-CPPA scheme, the structure of the signature message generated by message M_i is $\{M_i, PID_i,$
$PK_{i,l}, R_i, T_i, Sig_i\}$, where T_i is timestamp, PID_i is Vehicle pseudonym, $PK_{i,l}$ is public key, R_i is parameters and Sig_i is Signature. so the communication overhead of the EPA-CPPA scheme is $64 \times 5 + 32 = 324$bytes.

In this scheme, the vehicle generates the message signature structure as $\{H_0(Cre_{v_i}),$ $PID_{V_{inital}}, pk_{Vi}, R_i,$
$t_s, Sig_i\}$, where t_s is the timestamp, vehicle pseudonym $PID_{V_{inital}} \in Z_p^*$; R_i, Sig_i, $pk_{Vi} \in G$, and $\{H_0(Cre_{v_i})$ is the hash operation, so the communication overhead of the message signature is 64×3+4×2+32
=232bytes. Similarly, the computational overhead in other schemes can be calculated, and the computational overhead of this paper scheme and the comparison scheme are listed in Table 4. The analysis shows that the message structure of this scheme is better and has lower additional communication overhead.

TABLE 4. Communication Overhead Comparison

programs	Message signature	Message Authentication
Anil's	$\{b^{-1}, vpk_{1j}, vpk_{3_i}, M_i, R_i, T_i, PID_i, k_i^{-1}\}$	456bytes
BASA	$\{M, w, N, r, h, sk_e\}$	292bytes
EPP-CPPA	$\{M_i, PID_i, PK_{i,l}, R_i, T_i, Sig_i\}$	324bytes
IVPPA	$\{H_0(Cre)_{v_i}, PID_{V_{inital}}, pk_{Vi}, R_i, t_s, Sig_i\}$	232bytes

6.3. **Additional overhead for cross-domain information synchronization.** In this paper, we use blockchain technology to achieve cross-regional information sharing and solve the problems of vehicle registration and cross-regional information update caused by the inability to synchronize data among multiple nodes. The consensus process assists

each node to achieve the synchronization of ledger data, which contains information about each management area, public keys, auxiliary parameters, and false distribution records. Although this data is not used directly in the V2V authentication system, it has an impact on the registration process of the authentication system and the sharing of information across domains. Figure 6 evaluates the additional latency using chain code deployment analysis, the results show that when the sending rate increases, the check time of the peer nodes and the sequencing time of the sequential nodes increase, which leads to an increase in the average delay as well. In addition, when the number of domains increases, the number of peer nodes also increases, which means that the average latency of peer nodes is greater than the number of other domains in the case of 8 domains. Also, in Figure 7 the maximum throughput of write data is shown, it decreases gradually as the number of domains increases, due to the increase in the number of communication rounds in the consensus.

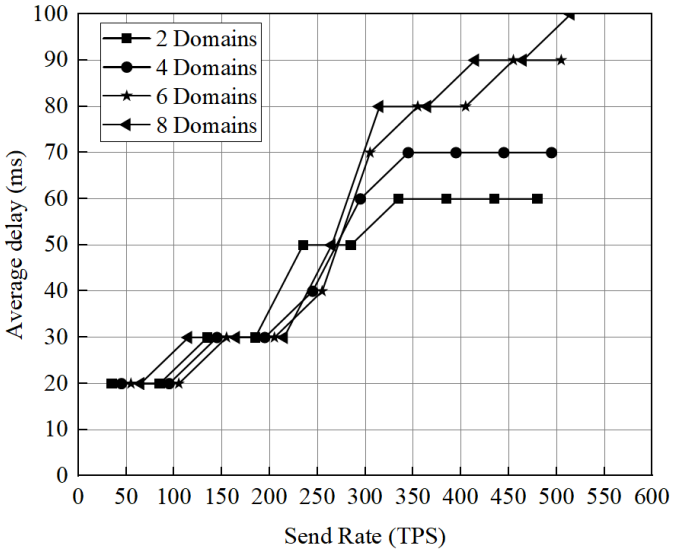

FIGURE 6. Average latency of write data

7. **Conclusion.** The scheme in this paper utilizes blockchain technology to establish a trust relationship with vehicles through the TA network authentication model to achieve efficient and privacy-preserving authentication in a virtual network. It is demonstrated that the proposed authentication is resistant to entity simulation attacks and achieves security features such as anonymity, privacy, non-repudiation, and unlinkability. In addition, the computational overhead, communication overhead, and additional overhead of cross-domain analysis with the introduction of blockchain are performed and compared with other authentication schemes. The simulation results show that the scheme is a promising and efficient authentication scheme with better feasibility in the Internet of Vehicles. Future work will focus on how to further improve the efficiency of certification and achieve mass certification of vehicles by RSU.

Acknowledgment. This work was supported in part by the Key scientific research projects of colleges and universities in Henan Province under Grant 23A520033, the Doctoral Scientific Fund of Henan Polytechnic University under Grant B2022-16 and B2010-32, and the Youth Fund of Henan Polytechnic University(Q2014-05).

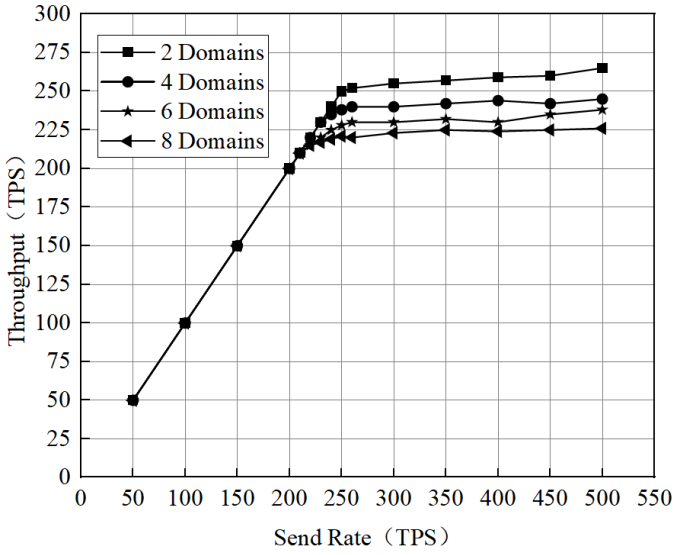

FIGURE 7. Throughput of write data

REFERENCES

[1] S.-S Moni, and D. Manivannan, "CREASE: Certificateless and REused-pseudonym based Authentication Scheme for Enabling security and privacy in VANETs," *Internet of Things*, vol. 20, 100605 ,2022.

[2] Z. Zheng, Y. Zhou, Y. Sun, Z. Wang, B. Liu, and K. Li, "Applications of federated learning in smart cities: recent advances, taxonomy, and open challenges," *Connection Science*, vol. 34, no. 1, pp. 1-28, 2022.

[3] T.-Y. Wu, X. Guo, Y.-C Chen, S. Kumari, and C.-M. Chen, "SGXAP: SGX-Based Authentication Protocol in IoV-Enabled Fog Computing," *Symmetry*, vol. 14, no. 7, pp. 1393, 2022.

[4] T.-Y. Wu, X. Guo, L. Yang, Q. Meng, and C.-M. Chen, "A lightweight authenticated key agreement protocol using fog nodes in Social Internet of vehicles," *Mobile Information Systems*, vol. 2021, 3277113, 2021.

[5] Y. Genc, N. Aytas, A. Akkoc, E. Afacan, and E. Yazgan, "ELCPAS: A new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV," *Vehicular Communications*, vol. 39, 100549, 2023.

[6] T.-Y. Wu, Z. Lee, L.Yang, and C.-M. Chen, "A Provably Secure Authentication and Key Exchange Protocol in Vehicular Ad Hoc Networks," *Security and Communication Networks*, Vol. 2021, 9944460, 2021.

[7] J. Wang, J.Liu, and N.Kato, "Networking and Communications in Autonomous Driving: A Survey," *IEEE Communications Surveys Tutorials*, vol. 21, no. 2, pp. 1243–1274, 2018.

[8] K.-N. Qureshi, A. Alhudhaif, S.-W. Haidar, S. Majeed, and G. Jeon, "Secure data communication for wireless mobile nodes in intelligent transportation systems," *Microprocessors and Microsystems*, vol. 90, 104501, 2022.

[9] C.-M. Chen, Z. Li, S. Kumari, G.Srivastava, K.Lakshmanna, and T.-R. Gadekallu, "A provably secure key transfer protocol for the fog-enabled Social Internet of Vehicles based on a confidential computing environment," *Vehicular Communications*, vol. 39, 100567, 2023.

[10] S. PU, and J.-S.-L. Lam, "The benefits of blockchain for digital certificates: A multiple case study analysis," *Technology in Society*, vol. 72, 102176, 2023.

[11] R.-C. Merkle, "Protocols for Public Key Cryptosystems," *Proceedings of the 1980 IEEE Symposium on Security and Privacy*, vol. 1980.

[12] M. Raya, and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007.

[13] Y. Kondareddy, G.-D. Crescenzo, and P. Agrawal, "Analysis of certificate revocation list distribution protocols for vehicular networks," *in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE, 2010, pp. 1-5.

[14] M. Azees, P.Vijayakumar, and L.-J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no 9, pp. 2467-2476, 2017.

[15] F. Liu, and Q. Wang, "IBRS: An Efficient Identity-based Batch Verification Scheme for VANETs Based on Ring Signature," *in 2019 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2019, pp. 1-8.

[16] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," *in IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, IEEE, 2008, pp. 246-250.

[17] Y. Xie, L. Wu, J. Shen, and A. Alelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs," *Telecommunication Systems*, vol. 65, no. 2, pp. 229-240, 2017.

[18] J. Kang, R. Yu, X. Huang, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for Secure and Efficient Data Sharing in VehicularEdge Computing and Networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660-4670, 2018.

[19] C. Wang, J. Shen, J.-F. Lai, and J. Liu, "B-TSCA: Blockchain Assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1386-1396, 2020.

[20] Y. Yao, X. Chang, J. Misic, V.-B. Misic, and L. Li, "BLA: Blockchain-Assisted Lightweight Anonymous Authentication for Distributed Vehicular Fog Services," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3775-3784, 2019.

[21] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology," *IEEE Access*, vol. 7, pp. 45061-45072, 2019.

[22] Y. Lu, "The blockchain: State-of-the-art and research challenges," *Journal of Industrial Information Integration*, vol. 15, pp. 80-90, 2019.

[23] J. Chen, H. Xiao, M. Hu, and C.-M. Chen "A blockchain-based signature exchange protocol for metaverse," *Future Generation Computer Systems*, vol. 142, pp. 237-247, 2023.

[24] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-Based Lightweight and Secured V2V Communication in the Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 3997-4004, 2022.

[25] A.-K. Sutrala, P. Bagga, A.-K. Das, N. Kumar, J. Rodrigues, and P. Lorenz, "On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment," *IEEE Trans. Veh. Technol*, vol. 65, no. 5, pp. 5535–5548, 2020.

[26] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun*, vol. 38, no. 5, pp. 942–954, 2020.

[27] J. Li, K.-K.-R. Choo, and W. Zhang, "EPA-CPPA: An efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *Vehicular Communications*, vol. 13, pp. 104-113, 2018.