A Privacy-Preserving Authentication Scheme Based on an Improved Blockchain for VANET

Xian Guo, Bangcai Zhong, Yongbo Jiang, Jing Wang,
Junli Fang and Ye Lu

July 19, 2023

A Privacy-Preserving Authentication Scheme Based on an Improved Blockchain for VANET

Xian Guo
School of computer and communication
Lanzhou University of Technology
Lanzhou,China
iamxg@163.com

Bangcai Zhong
School of computer and communication
Lanzhou University of Technology
Lanzhou,China
1746343186@qq.com

Yongbo Jiang
School of computer and communication
Lanzhou University of Technology
Lanzhou,China
jiangyb@lut.edu.cn

Jing Wang
School of computer and communication
Lanzhou University of Technology
Lanzhou,China
wangjing@lut.edu.cn

Junli Fang
School of computer and communication
Lanzhou University of Technology
Lanzhou,China
fangji@lut.edu.cn

Ye Lu
School of computer and communication
Lanzhou University of Technology
Lanzhou,China
luye528@126.com

Abstract*—In Vehicle Ad Hoc Networks (VANETs), the protection of the vehicle's identity privacy as well as identity authentication is crucial. However, existing authentication schemes to protect privacy are compromised by the opacity of trusted third-party activities to individual tuples in VANETs, the insecurity of key pairs for each tuple, the high workload of revoking certificates, and the high computational overhead of identity and message authentication. In this paper, an improved blockchain-based privacy protection and authentication method for VANETs is proposed. In the scheme proposed in this paper, the private key of the tuple is generated by a trusted third party in half with itself, thus making the key secure. To address the issues of large proof sizes and high bandwidth costs when verifying element existence in Merkle Trees and Merkle Patricia Trees, a proposed improvement is the Verkle Tree-based blockchain solution. A distributed identity verification method is adopted to effectively identify vehicle identity information for identity verification. To tackle security and privacy protection problems in blockchain-based VANETs, a conditional privacy-protecting distributed identity authentication scheme without revocation lists is proposed based on cryptographic security mechanisms. This paper implements the improved blockchain-based VANETs privacy protection authentication scheme on the Ethereum consortium chain platform. Simulation experiments are conducted to analyze the proposed scheme and compare it with existing solutions. The experimental results demonstrate that the proposed approach is feasible and effective.

Keywords—VANET, Verkle Tree, Improved Blockchain, Conditions Privacy Protection, Distributed Authentication

I. Introduction

In recent years, the speed of economic and scientific development is increasing, the scale of vehicle use is also increasing year by year, and people's reliance on vehicles is gradually increasing, but this also increases the risk of traffic injuries. Vehicles are able to exchange information with each other in V2V and communicate directly with other components located in V2I through dedicated short-range communication (DSRC)[1]. In order to prevent potential attacks due to the open nature of VANETs, it is necessary to implement an authentication scheme that preserves privacy[2]. In the absence of authentication, a malicious vehicle may forge messages and release false information to the vehicle in question, which would allow an attacker to track the target vehicle and pose a serious threat to the driver. Therefore, the frequent occurrence of network security incidents in VANETs has attracted people's attention[3].

In the traditional public key infrastructure (PKI)-based scheme[4], Certificates are typically used for authentication by issuing a unique number to the vehicle and a certificate provided by a Certification Authority (CA). The scheme is centralized due to the centralized authentication node, which makes the central node task heavy, unproxy and easy to compromise. This problem can cause data leakage of sensitive user information and cannot effectively protect user identity privacy. In the identity-based signature (IBS) scheme[5], the Private Key Generator (PKG) serves as a Trusted Authority (TA) that generates and assigns private keys to vehicles, and uses its own private key to sign messages. However, IBS encounters the issue of private key escrow where the PKG has knowledge of all vehicles and their corresponding private keys. A scheme based on certificateless signature (CLS) is proposed[6], the solution is to simplify certificate management, prevent public key replacement attacks and key escrow issues, but increases computational costs and overhead.

The privacy protection authentication scheme based on group signature mainly realizes group key management by generating group public key and group private key by the group manager[7]. The group public key is public to all group members and is used for group members to sign the received messages, and the group private key is used to generate certificates for group members and verify the signatures. When a member needs to join a group, the group administrator issues a group certificate to the member using the group private key and agrees to the member joining the group, and the member uses his or her private key and certificate to perform a group signature on the accepted message after joining the group, and uses the group public key to verify the legitimacy of the group signature, but cannot verify the member who signed the message.

To solve these problems, this paper proposes a privacy-preserving authentication scheme for VANETs based on improved blockchain.

II. Privacy Protection and Authentication Scheme for VANET Based on Improved Blockchain

A. Improved blockchain

As shown in Fig. 1, the improved blockchain is a data structure composed of Verkle Tree(VT)and the original state tree Merkle Patricia Tree(MPT)used together, replacing the traditional Merkle Tree(MT). The reason for replacing the traditional MT is that in MT, the hash value of a value is the complete set of all sibling nodes, and a path is formed from the root node to the target node. All nodes that share a parent node with nodes on this path must be included, which inadvertently increases bandwidth and adds to the cost. In contrast, for VT, proof of a value does not require providing sibling nodes, only proof along the path from the leaf node to the root node is required. Compared to MT, VT effectively reduces bandwidth and decreases cost, making it superior to MT.

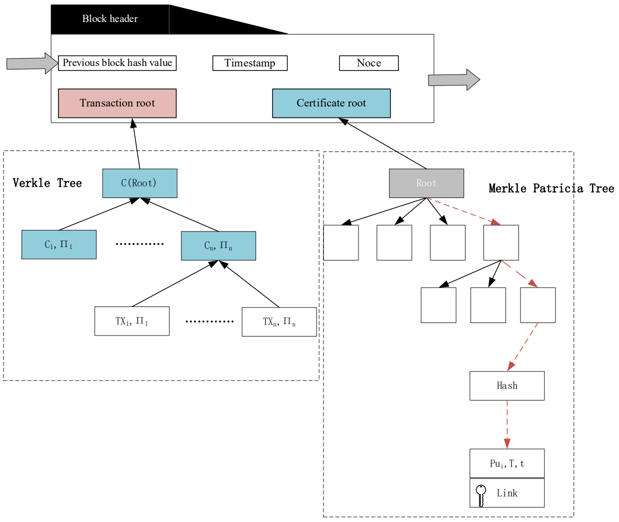

Fig. 1. A blockchain framework improved based on VT and MPT.

Based on the proposed approach in this paper, the benefits of using the improved blockchain with VT can be summarized in three aspects. Firstly, it provides a simplified verification method for distributed identity authentication. Regardless of whether a specific certificate is in MPT, as long as the certificate root and the tuple of nodes along the path are given, the receiver can calculate the hash using the tuple. If the hash value of the received certificate is equal to the hash value of the certificate root stored in the blockchain, then the certificate is proven to exist in MPT, and during the proof process, the size and bandwidth cost of the proof can be reduced. Secondly, it makes CA and LEA activities transparent, and the process of issuing or revoking certificates can be verified by components in the V2X network through the given transaction root and tuple. Finally, according to the properties of VT and MPT themselves, any modification in the system will cause a change in the value of the root node, thereby changing the hash value of the block. This can effectively prevent data stored in the blockchain from being tampered with, demonstrating that the improved blockchain serves as a secure data framework for the proposed approach in this paper.

B. System model

A vehicular ad hoc network (VANET) refers to a group of mobile or stationary vehicles connected via wireless networks. Initially aimed at providing security for vehicle-to-vehicle communication, VANET is now viewed as the infrastructure for intelligent transportation systems. VANET supports any system connected to the internet and makes on-board computers minimal in terms of internet infrastructure support, acting as a computing resource on the move. Content produced and consumed by vehicles is only related to time, space, and agents (producers and consumers), generating locally relevant information with limited spatial and temporal scope. For example, it is only relevant to a specific stretch of road at a specific time and applicable only to vehicles in close proximity. In the proposed scheme of this paper, the main components of the VANET system architecture include law enforcement agencies (LEA), certificate authorities (CA), roadside units (RSU), blockchain, and vehicles. Fig. 2 illustrates the system model of this scheme using the example of how blockchain operates and introduces each component and the processing flow of the scheme.

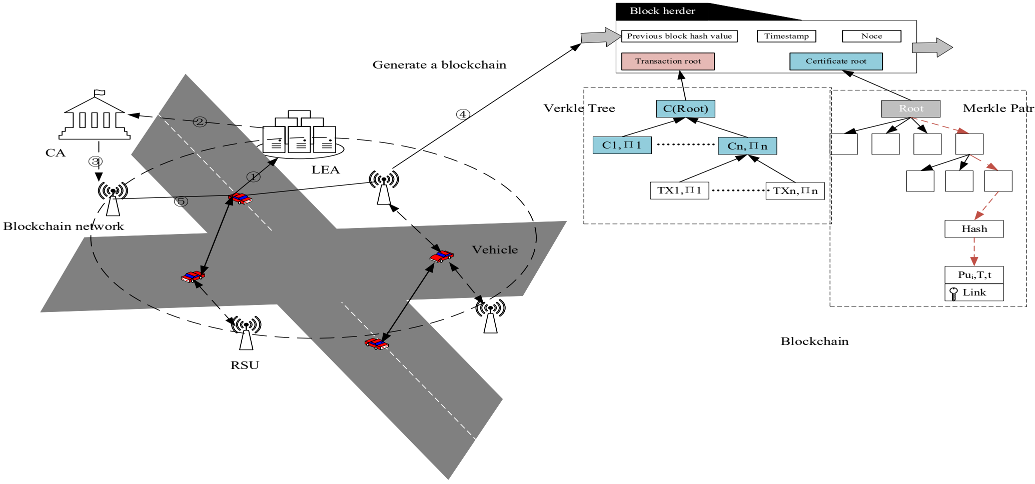

Fig. 2. System architecture model of the solution.

The numbered arrows in Fig. 2 illustrate the processing flow of the proposed scheme in this paper, which is described below:

1.Vehicles send certificate requests to LEA.

2.LEA authorizes CA to issue or revoke certificates.

3.CA generates transactions and updates the distributed ledger.

4.RSUs act as miners, verifying CA-generated transactions and generating new blocks stored in the blockchain for global consensus.

5.Vehicles receive the latest version of the blockchain and data for distributed identity verification from RSUs via V2I communication, enabling them to monitor the activities of

LEA and CA.

C. Design objective

The security issues in VANETs have been receiving increasing attention. To address the existing security problems, the design objectives of this paper are based on the following four aspects. The specific contents are shown as follows:

1.Verify identity security: In order to resist replay attacks, man-in-the-middle attacks, and forgery attacks, the proposed scheme needs to be used to ensure corresponding security, including identity authentication, integrity, and non-repudiation. When receiving messages, the receiver needs to verify whether the sender's certificate has been issued, and whether the message has been forged or replayed.

2.Conditional privacy protection: On one hand, the aim is to safeguard the privacy of vehicles by preventing adversaries from obtaining the true identity of target vehicles through analysis of broadcast messages and distributed ledgers. On the other hand, if the legitimacy or authenticity of a vehicle's identity is in question, LEA can reveal the actual identity of the relevant vehicle.

3.Certificate issuance and revocation transparency: Each component within VANETs relies on the authorization of trusted authorities, as they play a critical role in vehicle registration and dispute arbitration. This emphasizes the vital need for trustworthy authorities in VANETs. The proposed scheme in this paper aims to make the activities of these trusted third parties transparent, so that each component can check when certificates are issued or revoked by verifying transactions from the CA.

D. Scheme description

1) System initialization

LEA sets up an elliptic curve E for the system, in the form of $y^2 = x^3 + ax^2 + b$, where $a, b \in Z_q^*$ and p is a large prime number. The system selects the elliptic point group $E_q(a, b)$, where q is the order and G is the generator. LEA and CA respectively choose their private keys PR_{LEA} and PR_{CA}, compute their public keys $PU_{LEA} = PR_{LEA} \times G$ and $PU_{CA} = PR_{CA} \times G$. SHA is selected as the hash function ($H: \{0,1\}^* \rightarrow Z_q^*$), AES as the symmetric encryption algorithm (E_{key} and D_{key}), ECC as the asymmetric encryption algorithm (AE_{PU} and AD_{PR}), and ECDSA as the digital signature algorithm (Sig_{PR}). Finally, LEA publishes the system parameters as $param = G, PU_{LEA}, PU_{CA}, H, E_{key}, D_{key}, AE_{PU}, AD_{PR}, Sig_{PR}$

2) Vehicle registration

In order to ensure the legitimacy of a vehicle's identity in VANETs, all of vehicles must be registered to LEA. The vehicle registration process is described as follows.

Step 1: Firstly, a vehicle V_i submits its real identity RID_iobtained from the motor vehicle manufacturer (MVM) to the LEA through a secure channel, and then the LEA randomly selects an integer $r_i \in Z_q^*$ to share with V_i and RSU_i.

Step 2: The LEA computes the partial private key of the vehicle.

$$R_i = r_i G, u_{1i} = H_1(R_i, PU_{LEA}),$$
$$PPR_i = (r_i + su_{1i}) \mod p \qquad (1)$$

Step 3: The LEA sends $\{PPR_i, R_i\}$ to vehicle V_i through a secure channel, and then the vehicle saves it in its OBU.

Step4: The vehicle randomly selects a secret value , and calculate

$$X_i = x_i G, u_{2i} = H_2(X_i, R_i),$$
$$D_i = R_i + X_i + u_{2i} \qquad (2)$$

to generate the public key $PU_i = (D_i, R_i)$ and private key $PR_i = (PPR_i, x_i)$ of the vehicle. In a similar way, LEA registers RSU and generates its public key PU_r and private key PR_i .

3) Certificate issuance

When a vehicle enters the VANETs system, for security and privacy reasons, when the vehicle needs a certificate, vehicle V_i sends a certificate request to LEA, and the certificate issuance requires the following four steps.

Step 1: V_i sends to LEA a certificate issuance request encrypted with LEA public key req_{iss} Among them, PU_i is the public key of V_i , t is the timestamp, and Sig_{PR_i} is the digital signature of the message by the vehicle with its own private key.

$$req_{iss} = AE_{PU_{LEA}}(PU_i, t, Sig_{PR_i}) \qquad (3)$$

Step 2: First, LEA verifies the timeliness of the certificate issuance request through the timestamp, and secondly verifies the authenticity of the message through the signature in req_{iss} . Then LEA encrypts the encrypted link $Link_i = E_{LEA}(ID_i||r_{LEA})$between the vehicle and its real identity with its own public key. Finally, LEA sends authorization authority to CA to issue a new certificate to V_i.

$$auth_{iss} = (PU_i, T, t, E_{LEA}(ID_i||r_{LEA}), Sig_{PR_{LEA}}) \qquad (4)$$

Where PU_i is the public key of V_i, T is the expiration time of PU_i , t is the timestamp, r_{LEA} is the random number chosen by LEA, $E_{LEA}(ID_i||r_{LEA})$ is the encrypted link between V_i and its real identity, $Sig_{PR_{LEA}}$ is the authorization of LEA with its own private key the message is signed.

Step 3: The CA verifies the authenticity of the authorization through the signature of the LEA in $auth_{iss}$ and then issues the certificate issuance transaction TX_{iss} and certificate C_i containing the authorization of the LEA.

$$TX_{iss}(PU_i, T, t, E_{LEA}(ID_i||r_{LEA}), Sig_{PR_{LEA}}, Sig_{PR_{CA}}) \qquad (5)$$
$$C_i = (PU_i, T, t, E_{LEA}(ID_i||r_{LEA}), Sig_{PR_{CA}}) \qquad (6)$$

Step 4: The CA sends the certificate issuance transaction TX_{iss} and the new certificate C_i to the RSU, and the RSU verifies the correctness of the transaction and the certificate through the signature of the CA in the transaction TX_{iss} and the certificate C_i, and writes the transaction TX_{iss} and the certificate C_i as the new leaf node respectively Verkle Tree and MPT.

After the certificate is issued, RSU is verified by the digital signature $Sig_{PR_{CA}}$ in C_i. After the verification, RSU will spawn a new block and store it in the blockchain, and store the public key in MPT. The verification process for RSU is as follows.

Step 1: RSU verifies the signature with the CA's public key, and obtains the vehicle's public key from it.

$$\mathrm{AD}_{\mathrm{PU}_{\mathrm{CA}}}(\mathrm{C_i}=(\mathrm{PU_i},\mathrm{T},\mathrm{t},\mathrm{E}_{\mathrm{LEA}}(\mathrm{ID_i}||\mathrm{r}_{\mathrm{LEA}}),\mathrm{Sig}_{\mathrm{PR}_{\mathrm{CA}}})) \quad (7)$$

Step 2: RSU uses the public key expiration time to determine whether the public key has expired. If $\mathrm{T}_{\mathrm{PU_i}}-\mathrm{T}<\Delta\mathrm{T}$, then $\mathrm{PU_i}$ is valid.

Step 3: RSU will pass the verification, generate a new block and store it in the blockchain, and the stored content is$\mathrm{H}_3(\mathrm{PU_i},\mathrm{T},\mathrm{t},\mathrm{E}_{\mathrm{LEA}}(\mathrm{ID_i}||\mathrm{r}_{\mathrm{LEA}}))$.

4) Certificate update

After the vehicle obtains the certificate, the vehicle needs to send a certificate update request to LEA to update the vehicle's certificate when encountering the following situations. The first is that the current certificate is about to expire, the second is that the security of the vehicle's private key is threatened, and the last is that the vehicle wants to replace its public key. The certificate renewal process is as follows.

Step 1: Vehicle $\mathrm{V_i}$ combines with LEA to jointly generate a new pair of public key and private key $\{\mathrm{PU}_{\mathrm{i+1}},\mathrm{PR}_{\mathrm{i+1}}\}$.

Step 2: Vehicle $\mathrm{V_i}$ sends a certificate renewal request to the LEA encrypted with the LEA public key. It includes the public key $\mathrm{PU_i}$ of the current vehicle, the public key $\mathrm{PU}_{\mathrm{i+1}}$ to be updated, the signature $\mathrm{Sig_i}$ and the timestamp t of the current private key $\mathrm{PR_i}$ of the vehicle.

$$\mathrm{E}_{\mathrm{LEA}}\mathrm{req}=(\mathrm{PU_i},\mathrm{PU}_{\mathrm{i+1}},\mathrm{Sig}_{\mathrm{i}_{\mathrm{PR}}},\mathrm{t}) \quad (8)$$

Step 3: LEA receives the request from the vehicle, decrypts it with its own private key, and then verifies the timeliness of the message with the timestamp. If it is valid, LEA sends a signed authorization letter to CA.

$$\mathrm{auth}_{\mathrm{iss}}=(\mathrm{PU_i},\mathrm{PU}_{\mathrm{i+1}},\mathrm{T},\mathrm{t},\mathrm{Sig}_{\mathrm{PR}_{\mathrm{LEA}}}) \quad (9)$$

Where T is the certificate expiration time, $\mathrm{PU_i}$ is the current public key, $\mathrm{PU}_{\mathrm{i+1}}$ is the public key to be updated, and t is the timestamp.

Step 4: The CA will verify the signature in the authorization letter, and then generate a new certificate $\mathrm{C}_{\mathrm{i+1}}$ and issue the authorization transaction $\mathrm{TX}_{\mathrm{iss}}$ of the LEA.

$$\mathrm{C}_{\mathrm{i+1}}=(\mathrm{PU}_{\mathrm{i+1}},\mathrm{T},\mathrm{t},\mathrm{Sig}_{\mathrm{PR}_{\mathrm{CA}}}) \quad (10)$$

$$\mathrm{TX}_{\mathrm{iss}}=(\mathrm{PU_i},\mathrm{PU}_{\mathrm{i+1}},\mathrm{T},\mathrm{t},\mathrm{Sig}_{\mathrm{PR}_{\mathrm{LEA}}},\mathrm{Sig}_{\mathrm{PR}_{\mathrm{CA}}}) \quad (11)$$

Step 5: CA sends the issued certificate and transaction to RSU for verification.

Step 6: After the RSU verifies the correctness of the signature in each transaction, a new block is recorded in the blockchain, the transaction is stored in the verkle tree, and the certificate is inserted into the MPT as a new single node. RSU publishes the updated blockchain and sends the data that requires distributed authentication of the vehicle to the vehicle.

5) Certificate revocation

If it is found throughout the system that the vehicle public key is about to expire, the certificate will be revoked before the vehicle public key expires. The specific process of certificate revocation steps is as follows.

Step 1: LEA first looks up $\mathrm{PU_i}$ in MPT to get $\mathrm{Link_i}$, then LEA decrypts $\mathrm{Link_i}$ and displays $\mathrm{ID_i}$.

Step 2: LEA sends authorization $\mathrm{auth}_{\mathrm{rev}}$ to CA to revoke public key $\mathrm{PU_i}$.

$$\mathrm{auth}_{\mathrm{rev}}=(\mathrm{PU_i},\mathrm{t},\mathrm{Sig}_{\mathrm{PR}_{\mathrm{LEA}}}) \quad (12)$$

Step 3: CA issues a revocation transaction $\mathrm{TX}_{\mathrm{rev}}$ that includes LEA authorization.

$$\mathrm{TX}_{\mathrm{rev}}=(\mathrm{PU_i},\mathrm{t},\mathrm{auth}_{\mathrm{rev}},\mathrm{Sig}_{\mathrm{PR}_{\mathrm{CA}}}) \quad (13)$$

Step 4: RSU deletes the leaf node associated with $\mathrm{PU_i}$, and then publishes the revocation transaction.

6) Distributed verification process

The scheme proposed in this paper allows the receiver to verify the legitimacy of the vehicle identity by means of distributed authentication. The distributed authentication process has the following three steps.

Step 1: The vehicle sends an authentication message to the receiver, including the vehicle certificate, certificate expiration time and time stamp. The receiver checks the timeliness of the message through the timestamp, and then the receiver checks whether the certificate $\mathrm{C_i}$ of the vehicle is expired. If $\mathrm{T}_{\mathrm{rec}}-\mathrm{T}<\Delta\mathrm{T}$, it means that the certificate has not been revoked and the certificate has not expired.

Step 2: The receiver checks whether they are associated with $\mathrm{V_i}$ public key $\mathrm{PU_i}$ by extracting the prefixes of the same path as the current node from the tuples (leaf nodes, branch nodes, extension nodes) containing associated nodes in the MPT. Then the recipient calculates the hash value from the node where the received certificate is located to the root node and compares it with the hash value of the certificate root stored in the latest block.

Step 3: The recipient validation the signature $\mathrm{Sig}_{\mathrm{PR_i}}$ in the Tuple through the public key of the vehicle to ensure the correctness of the vehicle.

III. Safety analysis and Performance evaluation

A. Safety analysis

In this section, based on the design objectives proposed in this paper, an informal analysis is conducted on the security of the scheme concerning identity verification, conditional privacy protection, and transparency in the certificate issuance and revocation process.

Proposition 1: The scheme is secure for vehicles where the authentication in the scheme is resistant to attacker attacks.

Proof: During the distributed authentication process, the sender provides tuple $\mathrm{Tuple}=(\mathrm{C_i},\mathrm{tuple_M},\mathrm{Sig}_{\mathrm{PR_i}})$ .The receiver uses certificate $\mathrm{C_i}$ and tuple $\mathrm{tuple_M}$ to compute the root hash. If the calculated root hash value is equal to the hash value of the certificate root stored in the latest block in the blockchain, it proves that the certificate of $\mathrm{V_i}$ exists in the MPT, which means that the certificate of the vehicle has been issued and not revoked by the CA. If an attacker forges a certificate, it will make the leaf node in MPT change, which in turn will make the root node change, because the SHA used is conflict resistant, so it is impossible for an attacker to forge a certificate. The characteristics of ECDSA ensure that signature forgery is not possible without knowledge of the vehicle's private key.

Proposition 2: In the whole system, except LEA, It is impossible for any component to know the true identity of the vehicle from the distributed ledger and the messages sent.

Proof: Throughout the system, the true identity of the vehicle during the communication between V2V and V2I is known only to the LEA. By encrypting the link between the vehicle and its true identity, the adversary can be prevented from tracking the target vehicle. The certificate $C_i = (PU_i, T, t, E_{LEA}(ID_i||r_{LEA}))$ of the vehicle is recorded in the MPT as a leaf node. Without LEA's private key PR_{LEA} , it is impossible for an attacker to decipher $Link_i = E_{LEA}(ID_i||r_{LEA})$ to reveal the vehicle's true identity, because the encrypted link is encrypted by LEA's private key. In addition, the random number r_{LEA} makes the link in $V_i's$ certificate completely different, which makes it impossible for the attacker to obtain the linking ability between V_i and its real identity. When the identity of the vehicle is in dispute, LEA decrypts the encrypted link $Link_i$ by itself and reveals the real identity ID_i of the target vehicle V_i .

Proposition 3: Components in the VANETs can verify the activities of trusted third parties.

Proof: All transactions issued by the CA and certificates issued by the CA are publicly and immutably recorded in the blockchain, as the Verkle Tree is built from proofs and vector promises, while the MPT is built from SHA, which effectively prevents the blockchain data from being tampered with by attackers. All issued transactions contain the signatures of the CA and the LEA, and the authorization sent by the LEA to the CA to issue or revoke the certificate is undeniable. Since certificate issuance and revocation are equivalent to node insertion and deletion operations, this changes the root of the MPT and the corresponding transactions, and the issued transactions are stored in the Verkle Tree. The receiver can determine whether this transaction is correct by calculating the vector commitment of the transaction resulting from each step of the certificate issuance process and the hash value of the certificate deposited as a leaf node into the root node in the MPT.

B. Experiment settings

In order to verify the correctness and feasibility of the proposed privacy protection and authentication scheme for the Internet of Vehicles based on improved blockchain, simulation experiments will be conducted on the Ethereum platform. The device information used in the experiment is shown in Table Ⅰ.

TABLE I. DEVICE AND INFORMATION

Name	Details
DELL	Windows 10，16GB
CPU	Intel Core i5-1035G1,1.00GHz
Lenovo	Ubuntu，8GB
CPU	Intel Core i3-4160T, 3.10GHz
Smart contract programming language	Solidity
Blockchain platform	Ethereum
Smart contract compilation platform	Remix IDE
Smart contract deployment platform	Ropsten
Ethereum test network connection tool	MetaMask

C. Experimental Results and Analysis

1) Certificate issuance and revocation

In the experimental process of verifying the security of certificate issuance and revocation transactions, this paper sets the number of certificates N to 100,500,1000, 1500,2000,2500,3000, and verifies the certificate issuance and revocation transactions. Fig. 3 respectively indicate the time consumed for issuance and revocation of different numbers of certificates in blockchain systems based on VT and MPT combination improvements, and original blockchain systems based on MT and MPT combination.

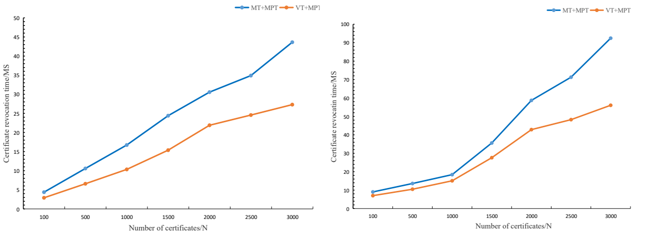

Fig.3. Certificate issuance transaction and revocation transaction time.

The experimental results show that in the blockchain system based on VT and MPT combination improvements, the time consumed for verifying certificate issuance transactions in a VANET with 3000 certificates are 27.79ms, and the time consumed for verifying certificate revocation transactions is 56.05ms. Under the same number of certificates, the certificate issuance and revocation processes are conducted in the original blockchain system based on MT and MPT combination.

This paper evaluates the impact of block size on certificate issuance and revocation transaction throughput and transaction latency. In this paper, the block size is set from 1MB to 3MB for the same number of certificates, and conduct experiments to compare the differences between the two types of blockchains. The transaction throughput of certificate issuance and revocation processes is shown in Fig. 4.

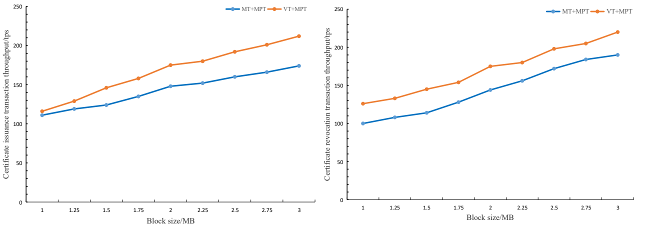

Fig. 4. Certificate issuance transaction throughput and revocation throughput.

The results from the figures indicate that as the block size increases, the throughput of certificate issuance and revocation transactions in both types of blockchains also increases. The latency of certificate issuance and revocation transactions with the same block size is shown in Fig. 5 respectively.

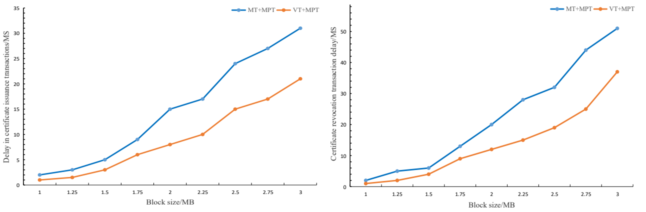

Fig. 5. Certificate issuance and revocation transaction delays.

In Ethereum's consortium blockchain, the amount of Gas consumed by smart contract deployment is also a performance evaluation criterion. As shown in Fig. 6, it shows the Gas costs consumed for certificate issuance and revocation on the blockchain based on two types of blockchains for different numbers of certificates.

As shown in the figure, as the number of certificates increases, the gas costs for certificate issuance and revocation both increase. Since these operations require frequent state updates and hash calculations, significant gas costs are incurred. However, for a blockchain based on the combination of VT and MPT improvements, it is possible to optimize the gas costs associated with certificate issuance and revocation.

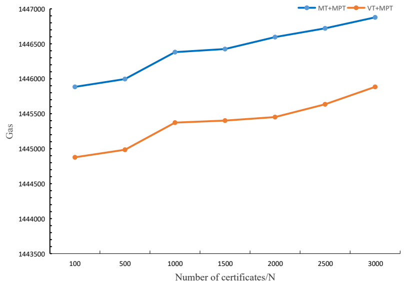

Fig. 6. Distributed identity authentication Gas cost.

2) Distributed identity verification

When vehicles interact with each other, the receiving party needs to verify the legitimacy of the sender's identity. In the distributed identity authentication experiment, this paper sets the number of certificates N to100, 500, 1,000, 1500,2000,2500 and 3000, and then performs the distributed identity authentication process. The time consumption, communication overhead, and Gas costs during the distributed identity verification process are shown below.

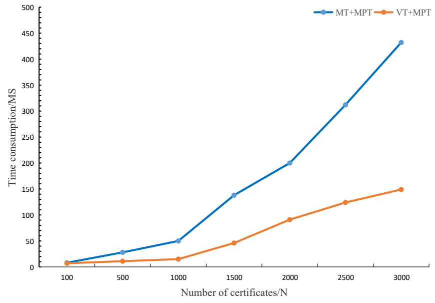

Fig. 7. Time consumption during distributed identity authentication.

Fig. 7 shows the time consumption during the distributed identity authentication process. From the experimental results, it can be seen that the improved blockchain performance based on VT and MPT is superior to traditional blockchains.

Fig. 8 shows the communication overhead consumed during the distributed identity authentication process. From the experimental results, it can be seen that the improved blockchain performance based on VT and MPT is superior to traditional blockchains.

Fig. 9 shows the Gas cost incurred in deploying smart contracts during the distributed identity authentication process. From the experimental results, it can be observed that in a blockchain using MT and MPT, Gas cost increases linearly with the increase in the number of certificates .

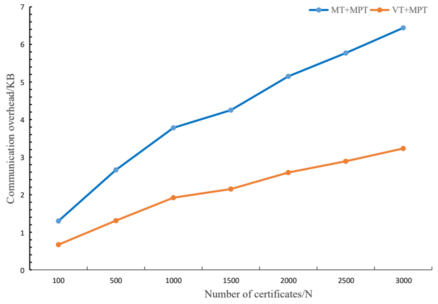

Fig. 8. Distributed identity authentication communication overhead.

Overall, when performing distributed identity authentication in a blockchain improved by combining VT and MPT, it exhibits less time consumption, smaller communication overhead, and lower Gas cost compared to a blockchain using MT and MPT, especially when the number of certificates is large.

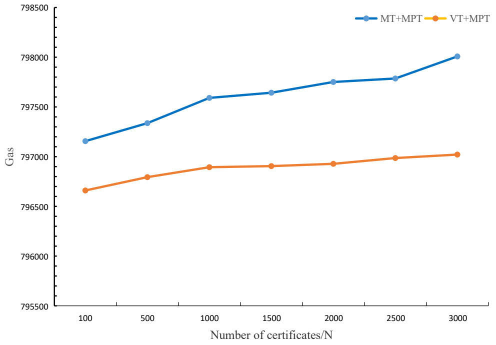

Fig. 9. Distributed identity authentication Gas cost.

Based on the above analysis, this paper compares the Privacy Protection and Authentication Scheme for Vehicular Ad Hoc Networks based on an improved blockchain （PPASIB）with existing state-of-the-art privacy protection and authentication schemes. These include the Efficient Anonymous Authentication with Conditional Privacy Protection (EAAP)[8],A Blockchain-Based Anonymous Authentication Scheme for Internet of Vehicles（ABBAA）[9],Privacy-preserving blockchain-based authentication and trust management in VANETs (PPBBA)[10], and Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems (BECBA)[11]. By providing the average execution time of different cryptographic operations, the time consumption for certificate verification is analyzed under different numbers of certificates.

The Python Charm encryption library is utilized to carry out cryptographic operations in these schemes[12]. In this paper, the average execution time of different cryptographic operations is provided, as shown below:

1.T_{pb} is the execution time used for performing bilinear pairing operations. $T_{pb} \approx 4.421$ms.

2. T_{ep1} is the execution time used for performing exponential operations in G_1 during bilinear pairing. $T_{ep1} \approx 1.171$ms.

3. T_{ep2} is the execution time used for performing exponential operations in G_2 during bilinear pairing. $T_{ep2} \approx 0.928$ms.

4.T_{pm} is the execution time to perform elliptic curve point multiplication. $T_{pm} \approx 0.273$ms.

5.$T_{pa}$is the execution time to perform the addition of elliptic curve points. $T_{pa} \approx 0.019$ms.

6. $T_h$is the execution time to execute the hash function. $T_h \approx 0.001$ms.

As shown in Fig. 10, the PPASIB only needs 26ms to authenticate 80 certificates, while the time consumption for verifying 80 certificates in other schemes is much higher than that of the proposed scheme. This means that the proposed scheme in this paper can operate normally in situations of severe traffic congestion. The efficiency of VT is higher than that of MT when verifying the existence of elements, so the proposed PPASIB scheme in this paper consumes much less time for certificate verification than the compared schemes in the distributed identity authentication process.

From the above analysis, it can be seen that the proposed solution in this paper has lower costs in certificate issuance, revocation, and distributed identity verification compared to most existing solutions, showing significant advantages and better meeting the performance requirements for privacy protection in vehicular networks. Therefore, the proposed PPASIB in this paper is effective, feasible, and superior to existing blockchain-based solutions for privacy protection in vehicular networks.

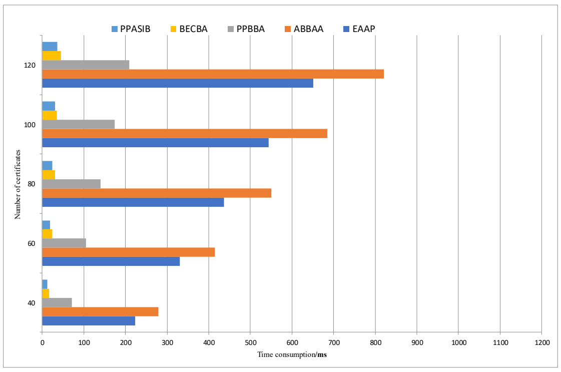

Fig. 10. The time consumed for certificate verification.

Conclusion

In this paper, Verkle Tree and MPT are used to improve the blockchain and thus a new blockchain-based authentication scheme for privacy protection in VANETs is proposed. First, the transactions issued by CAs and LEAs are recorded in Verkle Tree and the certificates are recorded in MPT, which makes the whole transactions stored in the Verkle Tree, thus each component in VANETs can be verified by viewing the activities of trusted third parties. Secondly, the LEA and the vehicle share half of the private key as the private key of the vehicle, which ensures the security of the vehicle key. Finally, he true identity of the vehicle is encrypted with a law enforcement agency (LEA) key, thus preventing the leakage of the vehicle's true identity. Finally, we simulate and analyze the scheme on the Ethernet federation chain. The experimental results show that the PPASIB scheme proposed in this paper provides an effective solution to the problem of privacy-preserving authentication of vehicles in VANETs.

References

[1] Lu Z, Qu G, Liu Z. A survey on recent advances in vehicular network security, trust, and privacy[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 20(2): 760–776.

[2] Azees M, Vijayakumar P, Jegatha Deborah L. Comprehensive survey on security services in vehicular ad-hoc networks[J]. IET Intelligent Transport Systems, 2016, 10(6): 379–388.

[3] Abdulkadhim F G, Yi Z, Tang C, et al. Design and development of a hybrid (SDN+ SOM) approach for enhancing security in VANET[J]. Applied Nanoscience, 2023, 13(1): 799–810.

[4] Canetti R, Shahaf D, Vald M. Universally composable authentication and key-exchange with global PKI[C]//Public-Key Cryptography--PKC 2016. Springer: 265–296.

[5] Jiang W, Li H, Xu G, et al. PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI[J]. Future Generation Computer Systems, 2019, 96: 185–195.

[6] Kumar P, Kumari S, Sharma V, et al. Secure CLS and CL-AS schemes designed for VANETs[J]. the journal of supercomputing, 2019, 75: 3076–3098.

[7] Jiang Y, Ge S, Shen X. AAAS: An anonymous authentication scheme based on group signature in VANETs[J]. IEEE Access, 2020, 8: 98986–98998.

[8] Azees M, Vijayakumar P, Deboarh L J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467–2476.

[9] Hy A, Yl A. A Blockchain-Based Anonymous Authentication Scheme for Internet of Vehicles[J]. Procedia Computer Science, 2022, 201: 413–420.

[10] Ahmed W, Di W, Mukathe D. Privacy-preserving blockchain-based authentication and trust management in VANETs[J]. IET Networks, 2022, 11(3–4): 89–111.

[11] Vangala A, Bera B, Saha S, et al. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems[J]. IEEE Sensors Journal, 2020, 21(14): 15824–15838.

[12] Akinyele J A, Garman C, Miers I, et al. Charm: a framework for rapidly prototyping cryptosystems[J]. Journal of Cryptographic Engineering, 2013, 3(2): 111–128.