Journal of Computer Science and Electrical Engineering
ISSN: 2663-1946
DOI: https://doi.org/10.61784/jcsee3040

AN EFFICIENT CROSS-DOMAIN AUTHENTICATION SCHEME FOR INTERNET OF VEHICLES (IOV) BASED ON REPUTATION

YuChen Shan
Guangzhou University, Cyberspace Institute Advanced Technology, Guangzhou 510006, Guangdong, China.
Corresponding Author: YuChen Shan, Email: shanyuchen0707@163.com

Abstract: With the rapid development of intelligent transportation technologies, the Internet of Vehicles (IoV) has become an essential component of modern transportation systems. However, as the scale of IoV continues to expand, achieving efficient and trustworthy cross-domain authentication has emerged as a critical technical challenge. To address this issue, this paper proposes a blockchain-based reputation framework for IoV, focusing on cross-domain authentication. Specifically, we propose an efficient cross-domain authentication scheme based on short signatures to address the efficiency and security issues in cross-domain authentication. Traditional cross-domain authentication schemes often incur high computational overhead and network bandwidth consumption, especially when there are significant differences in reputation values across different regions, making identity authentication inefficient. To this end, we design a cross-domain authentication algorithm based on reputation value coupling, which dynamically adjusts the reputation values of vehicle nodes according to the reputation weights of different regions. By integrating smart contract technology, the transparency and traceability of the authentication process are ensured. The dual-authentication mechanism based on reputation values further enhances the security and trustworthiness of nodes. Experimental results demonstrate that the proposed authentication scheme not only significantly improves authentication efficiency but also enhances the security and reliability of the IoV system.
Keywords: Blockchain; Reputation; Cross-domain; IoV

1 INTRODUCTION

With the rapid development of information technology, the IoV has become a core technology of the next-generation intelligent transportation system and is being widely applied globally. IoV enables information sharing and collaborative decision-making among vehicles through Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside (V2R), Vehicle -to-Pedestrian (V2P), and Vehicle-to-Internet (V2I) communications[1]. This enhances traffic efficiency, reduces traffic accidents, and improves the driving experience. However, the rapid growth of IoV also brings significant security and privacy challenges, especially in cross-domain authentication and trust management[2].

In traditional IoV architectures, vehicle authentication and information exchange often rely on centralized Certificate Authorities (CAs). While this approach provides a certain level of security, it also suffers from several critical issues, such as single-point failure, low efficiency in cross-domain collaboration, and the formation of trust silos. In cross-domain scenarios, vehicle communication between different regions or service providers requires complex cross-domain authentication processes, which increase system overhead and authentication latency, thereby affecting the real-time requirements of IoV. Moreover, the lack of a vehicle behavior credibility assessment mechanism makes IoV systems vulnerable to Sybil attacks (identity forgery) and man-in-the-middle attacks, threatening the overall network security[3].

To address these challenges, blockchain technology has emerged as a promising solution for IoV security due to its decentralized, tamper-proof, and transparent characteristics[4]. Blockchain can effectively overcome the limitations of traditional centralized authentication mechanisms by recording vehicle identities and behavior information in a distributed ledger, thereby establishing a trustworthy cross-domain authentication system. However, the application of blockchain in IoV also faces new challenges, such as high storage overhead, low throughput, and communication efficiency issues caused by long signatures. Therefore, designing an efficient cross-domain authentication scheme that ensures security while maintaining high efficiency and scalability is a crucial research topic in the IoV field[5].

Short signature technology, as an efficient cryptographic tool, can significantly reduce signature length and computational overhead while ensuring security. Integrating short signature technology with blockchain can further optimize the efficiency of cross-domain authentication, enhancing the real-time and scalable nature of IoV[6]. Based on this, this paper proposes an efficient cross-domain authentication scheme for IoV based on blockchain and short signatures, aiming to address the efficiency and security issues in cross-domain authentication and build a trustworthy, efficient, and scalable IoV ecosystem[7].

In IoV systems, cross-domain authentication is a key link for vehicle information sharing and collaborative decision-making. However, existing cross-domain authentication schemes have several significant shortcomings:

(1) Single-point failure in centralized authentication: Traditional IoV authentication relies heavily on centralized CAs. If a CA is attacked or fails, the entire authentication system may collapse, threatening the security and reliability of IoV.

(2) Low efficiency in cross-domain collaboration: Communication between vehicles in different domains requires complex cross-domain authentication processes, leading to increased authentication latency and difficulty in meeting the real-time requirements of IoV.

(3) Trust silo problem: There is a lack of unified trust assessment mechanisms between domains, making it difficult to quantify vehicle behavior credibility and leaving the system vulnerable to malicious node attacks.

(4) Trade-off between signature efficiency and security: Traditional digital signature algorithms (e.g., RSA, ECDSA) are secure but have long signature lengths and high computational overhead, making them unsuitable for high-concurrency, low-latency IoV scenarios.

To address the aforementioned challenges, blockchain technology offers a decentralized solution for cross-domain authentication in IoV. However, blockchain itself faces several limitations, such as high storage overhead, low throughput, and communication inefficiencies caused by long signatures. Therefore, integrating blockchain with short signature technology to design an efficient and secure cross-domain authentication scheme has become an urgent issue.

In this paper, we propose an efficient cross-domain authentication scheme for IoV based on blockchain and short signatures, leveraging the decentralized nature of blockchain, the efficiency of short signatures, and the trustworthiness of reputation mechanisms to build a reliable, efficient, and scalable cross-domain authentication framework for IoV. Specifically, the main contributions of this paper are as follows:

(1) Partitioned Blockchain Architecture: We divide the IoV into different regions and propose a partitioned blockchain architecture to efficiently manage the complex IoV network. By recording vehicle identities and behavior information in a distributed ledger, we eliminate the single-point failure issue associated with traditional centralized authentication.

(2) Short Signature Algorithm: We employ an efficient short signature algorithm to significantly reduce the signature length and computational overhead while ensuring security. This enhances the efficiency of cross-domain authentication and enables rapid authentication in high-concurrency scenarios, meeting the real-time requirements of IoV. Additionally, we introduce a reputation-based dual-authentication mechanism to ensure the security of cross-domain nodes.

(3) Smart Contract Automation: We incorporate smart contract technology to automate the management of interactions between vehicle nodes, such as message passing and information updates. Suitable API interfaces are embedded in the onboard units to quickly update information to the blockchain system.

The remainder of this paper is organized as follows. Section 2 reviews the related work. Section 3 introduces the preliminaries. Section 4 details the design of the cross-domain authentication scheme. Section 5 presents the simulation experiments. Section 6 concludes the paper.

2 RELATED WORK

In the field of cross-domain authentication for the Internet of Vehicles (IoV), researchers have proposed a variety of solutions tailored to different application scenarios. For example, Zhang et al.[8] proposed a distributed and scalable cross-domain vehicle authentication framework that optimizes the authentication process to reduce system overhead. Experimental data showed that this solution reduced computational resource consumption and communication latency. Wang et al.[9] designed a decentralized authentication architecture from the perspective of edge computing, innovatively incorporating a dynamic management mechanism for centralized certificate revocation tables. Simulation results indicated that compared to traditional solutions, their approach significantly reduced verification latency, making it particularly suitable for high-density vehicle environments.

In the context of cloud-based traffic monitoring, Wang et al.[10] studied a scenario where cloud servers and authoritative institutions should be able to verify the source of reports, i.e., checking whether traffic conditions are reported by legitimate vehicles. They theoretically analyzed the efficiency of their approach and experimentally demonstrated its practicality.

Regarding privacy protection, Zhang et al.[11] constructed a conditional privacy-preserving authentication model based on the Chinese Remainder Theorem, mathematically verifying the scheme's advantages in resisting replay and impersonation attacks. He et al.[12] innovatively used non-bilinear pairing encryption algorithms, proposing an authentication protocol that significantly shortened signature generation time while ensuring data integrity, making it suitable for security-related applications in IoV. Cui et al.[13] developed a one-time registration authentication system that uses pre-configured trusted institution certificate chains to ensure that vehicle cross-domain authentication response times meet the real-time requirements of IoV.

To address complex network threats, Xu et al.[14] proposed a cross-domain group authentication scheme that effectively resolves security issues. Sun et al.[15] designed a dual-layer authentication system capable of defending against DoS attacks, increasing authentication throughput while ensuring privacy by differentiating between intra-domain and cross-domain authentication processes. Meng et al.[16] integrated blockchain technology to build an authentication framework that automatically negotiates keys through smart contracts, demonstrating superior lightweight characteristics and efficiency. Zhang et al.[17] proposed a dual-blockchain-assisted conditional privacy-preserving authentication framework and protocol for IoV. Zhu et al. [18] introduced a certificateless signature scheme that pre-generates cross-domain communication credentials, significantly improving cross-domain authentication efficiency between vehicles, with simulation experiments verifying the protocol's security. Zhong et al.[19] developed a batch authentication mechanism that uses pre-computation techniques to reduce the cost of concurrent multi-vehicle authentication. Tan et al. [20] proposed a dynamic authentication protocol that leverages RSU cluster collaboration to achieve high authentication efficiency even at high vehicle speeds.

These studies collectively demonstrate the ongoing efforts to enhance the security, efficiency, and scalability of cross-domain authentication in IoV. However, challenges such as high computational overhead, communication inefficiencies, and privacy concerns still need to be addressed.

3 PREPARATIONS

3.1 Short Signature Technology

The Boneh-Lynn-Shacham (BLS) short signature scheme is a cryptographic signature mechanism based on elliptic curve cryptography and bilinear pairings. It is characterized by its short signature length, high computational efficiency, and strong security. In the context of low-bandwidth communication in IoV, BLS can significantly reduce the authentication overhead. During cross-domain authentication, vehicle nodes can perform concurrent authentication and aggregate signatures from multiple vehicles, thereby reducing the communication overhead associated with cross-domain interactions.

From a security perspective, BLS signatures are based on the mathematical hardness of bilinear pairings, ensuring the anonymity of vehicle requests. External attackers cannot infer the true identity of vehicles from the signatures. The main construction of BLS is as follows:

$$BB = \left(q, G_1, G_2, G_T, e, P_1, P_2, H(\cdot)\right) \tag{1}$$

In the IoV, the security level of the system is determined by the order q of the elliptic curve. The cyclic groups G_1, G_2 and G_T on the elliptic curve serve as the foundation for implementing bilinear pairings and signature verification. Specifically: G_1 is used for generating public keys, creating signatures, and verifying signatures. It forms the fundamental space for vehicle authentication. G_2 is used for hashing messages and generating/verifying cross-domain credentials. It serves as the basis for message authentication and cross-domain authentication. G_T is the target group of the bilinear pairing. The bilinear pairing function e: $G_1 \times G_2 \rightarrow G_T$ is employed to validate the authenticity of BLS signatures. $P_1 \in G_1$ and $P_2 \in G_2$ are base points on the elliptic curve, used for generating public keys and signatures. The hash function H: $\{0,1\}^* \rightarrow G_2$ maps messages to points in the elliptic curve group G_2, enabling the signing and verification processes.

3.2 Smart Contracts

Smart contract is a self-executing program that operates autonomously once deployed on a blockchain. It enforces predefined rules and executes operations without the need for human intervention. This automation significantly reduces the potential for manual errors and enhances the efficiency and reliability of the system.

Smart contracts are particularly well-suited for applications requiring high levels of transparency and immutability. The inherent properties of blockchain technology ensure that once a smart contract is deployed, its rules and executed operations cannot be altered or tampered with. This immutability guarantees data integrity and transparency, making every transaction publicly verifiable and auditable. The execution of smart contracts is typically governed by conditional logic encoded in the blockchain, often represented as "if...then..." statements. Upon fulfilling specified conditions, the blockchain updates accordingly, reflecting the executed operations.

In the context of cross-domain authentication within the IoV, the integration of smart contracts offers several key advantages. First, it streamlines the authentication process by automating tasks such as vehicle public key registration, reputation value adjustment, and cross-domain credential verification. This automation eliminates the need for intermediaries, thereby reducing operational costs and minimizing delays. Second, the complex logic required for cross-domain authentication can be efficiently implemented and enforced through smart contracts, enhancing both the efficiency and flexibility of the system. By leveraging these capabilities, smart contracts provide a robust and transparent solution for secure and efficient cross-domain authentication in IoV applications.

3.3 System Model

As shown in Figure 1, the IoV based on blockchain technology involves multiple domains, each comprising five main entities: Trust Authority (TA), Vehicle Nodes, Roadside Units (RSUs), Upper-layer Blockchain, and Lower-layer Blockchain. The communication process primarily includes intra-domain authentication and cross-domain authentication. Intra-domain authentication ensures the integrity and trustworthiness of messages within the same domain, while cross-domain authentication guarantees the security and trustworthiness of messages exchanged between different domains. The main functions of each entity are as follows:

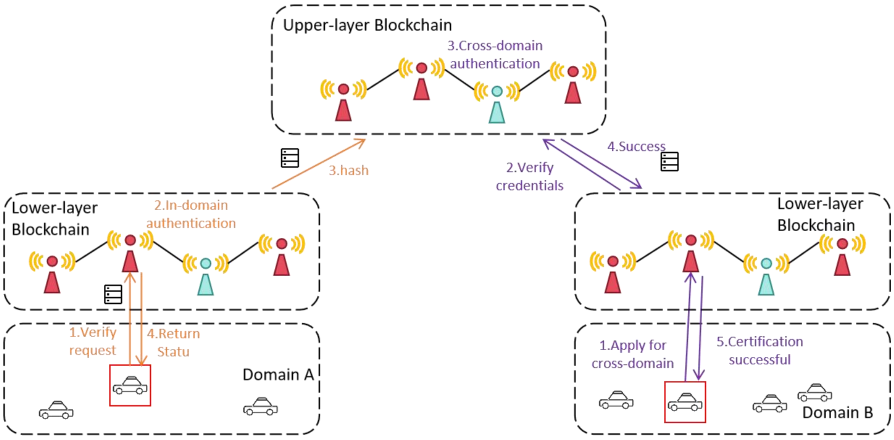

Figure 1 Cross-Domain Authentication Framework Diagram of the Internet of Vehicles

TA: Each domain is managed by a TA, which is considered a trusted institution by default. The primary responsibilities of the TA include managing members within its domain, such as registering nodes, generating public-private key pairs, and tracking member behavior. Additionally, TAs from different domains collectively maintain an upper-layer blockchain, which records their activities and forms a distributed ledger to ensure the overall security of the IoV.

Vehicle Nodes: Vehicle nodes are the fundamental communication units in the IoV, capable of communicating with other vehicle nodes, RSUs, and TAs. During V2V and V2R communications, messages sent by vehicles need to be authenticated by RSUs or TAs to ensure their integrity and trustworthiness. Specifically, if both the sender and receiver belong to the same domain, the message is verified by the local RSU and TA. Otherwise, cross-domain authentication is performed by the source TA and the target TA. The reputation of vehicle nodes is derived from the records of their behaviors, which will be detailed in the following section.

RSUs: RSUs are roadside infrastructure units responsible for collecting local IoV information. Given the vastness of the IoV, multiple RSUs may exist within a single domain to reduce communication latency. RSUs act as intermediaries between different participants, facilitating tasks such as signature verification, message forwarding, invoking smart contract APIs, and contacting TAs. As semi-trusted entities, RSUs do not deviate from predefined protocols but may attempt to access private information such as identities. Their temporary reputation is derived from the average reputation of all nodes within the domain in the previous consensus phase.

Upper-layer Blockchain: The upper-layer blockchain is a distributed database collectively maintained by TAs from different domains. It stores all relevant information of the IoV, including cross-domain authentication records, vehicle public-private key pairs, and other essential data.

Lower-layer Blockchain: The lower-layer blockchain is a distributed database maintained by all RSUs within the same domain. It records vehicle behavior information and serves as an intermediary node between vehicle nodes and the upper-layer blockchain, facilitating communication and data synchronization.

4 DETAILED DESIGN OF CROSS-DOMAIN AUTHENTICATION

This section provides a detailed introduction to the cross-domain authentication scheme based on reputation. The scheme consists of five main steps: Initialization, Registration, Intra-Domain Authentication, Cross-Domain Authentication, and Identity Traceability.

4.1 Initialization Phase

The initialization phase is the foundational setup of the system, involving the generation of system parameters, configuration of regional reputation weights, and deployment of smart contracts. The pseudocode is shown in Table 1.

Table 1 Initialization Algorithm

```
Algorithm 1: Initialization
Input: BB
Output: System Initialized
Get BB
e: $G_1 \times G_2 \rightarrow G_T$
H: $\{0,1\}^* \rightarrow G_2$
for each domains do
    Initialize TA(domain) according to(1)
    for each RSU in domain do
        Initialize RSU(domain) according to(2)
end for
```

```
Get RRW according to(3)
Initialize downblockchain()
end for
Initialize upblockchain()
return "System Initialized"
```

4.1.1 System initialization

Firstly, the IoV generates the basic domain parameters and values based on the bilinear pairing e and the elliptic curve BB. The vehicle authentication space G_1 and the message authentication space G_2 satisfy the bilinear pairing e, and the hash function H: $\{0,1\}^* \rightarrow G_2$ maps relevant authentication messages to G_2. Subsequently, the TA is initialized as the manager of the upper-layer blockchain. Using Equation (1), the TA generates its own public key PK_{TA}. The TA then initializes the RSUs in each region, generating their respective public keys PK_{RSU} using (2). Finally, the upper-layer blockchain deploys its own TA node, while the lower-layer blockchain is maintained by the RSU nodes in each designated region.

$GTA()$: Generates the public key PK_{TA} and private key SK_{TA} for the TA. The private key SK_{TA} is a random large prime number, and the corresponding public key PK_{TA} is derived from the generator g_2 in group G_2:

$$PK_{TA} = SK_{TA} \cdot g_2 \tag{1}$$

$GRSU()$: Generates the public key PK_{RSU} and private key SK_{RSU} for each RSU. The private key SK_{RSU} is a random large prime number, and the corresponding public key PK_{RSU} is derived from the generator g_2 in group G_2:

$$PK_{RSU} = SK_{RSU} \cdot g_2 \tag{2}$$

4.1.2 Regional reputation weight configuration

The Regional Reputation Weight (RRW) is a trust metric at the regional level. It measures the degree of trust a region has in vehicles (or other participants) during the authentication process, thereby determining whether the region is willing to accept a vehicle's authentication request and the extent to which the vehicle's reputation value is adjusted during authentication. The RRW facilitates trust propagation in cross-domain authentication systems. For example, when a vehicle moves from Region A (source region) to Region B (target region), the reputation value of the source region is adjusted in the target region based on the RRW. The RRW of the target region directly affects the vehicle's entry authentication in that region. During cross-domain authentication, a vehicle's reputation value is dynamically adjusted according to the RRW. This ensures fairness and rationality in trust propagation between regions. For instance, if a vehicle has a high reputation in the source region but enters a target region with a low RRW, its reputation value may decrease. Conversely, if the target region has a high RRW, the vehicle's reputation value may increase. These adjustments ensure that trust is fairly and reasonably propagated across regions.

The RRW is calculated based on a combination of multiple factors, including: The average reputation value within the region $\overline{R_{RSU}}$; Historical authentication data HH; The level of IoV activity within the region AA. The formula for calculating the RRW is defined as follows:

$$RRW = \omega_1 \cdot \overline{R_{RSU}} + \omega_2 \cdot HH + \omega_3 \cdot AA + \omega_4 \cdot \sigma \tag{3}$$

Where,

$$HH = \frac{H1}{H2} \tag{4}$$

$$AA = log_2 n \tag{5}$$

$$\omega_1 + \omega_2 + \omega_3 + \omega_4 = 1 \tag{6}$$

$\overline{R_{RSU}}$ is the average reputation value of all RSUs within the region during a consensus phase. HH is the proportion of successful authentications in the region, representing the region's historical trust in vehicles. $H1$ is the number of successful authentications and $H2$ is the total number of authentication attempts. AA represents the level of IoV activity within the region, including communication frequency between vehicles and RSUs. A higher level of activity enhances the efficiency and accuracy of the authentication process. n denotes the number of active vehicles within the region. σ is a noise factor introduced to add randomness and enhance security. $\omega_1, \omega_2, \omega_3, \omega_4$ are weight coefficients for each factor, determining their respective impact on the RRW.

Regarding the visibility analysis of RRW, vehicles can only be aware of the weight of the current area, in order to prevent potential manipulation of the weight of the target area. The source area and the target area TA can know their respective RRW through application(Table 2). Below is a summary of the visibility of RRW.

Table 2 RRW Visibility Table

Participants	Source RRW	Target RRW
Source Vehicle	Visible	Invisible
Source RSU	Visible	Invisible
Source TA	Visible	Visible (Application)
Target TA	Visible (Application)	Visible
External Attacker	Invisible	Invisible

4.1.3 Smart contract deployment

In the initialization phase, vehicle public-private key pairs must be registered on the blockchain to facilitate subsequent signature verification. Smart contracts are deployed to automate and verify this process, which includes the following steps:

(1) Key Pair Generation and Registration

Key Pair Generation: Each vehicle generates a public-private key pair. The private key is used for signing messages, while the public key is used for verification.

Public Key Registration: Vehicles submit their public keys along with other identity information (e.g., vehicle ID) to the smart contract.

Public Key Storage: The smart contract verifies and stores the vehicle's public key on the blockchain, ensuring that it can be validated by other participants during future authentication processes.

(2) Management of Regional Reputation Weights

Regional Reputation Weights (RRWs) are crucial factors influencing vehicle reputation values in cross-domain authentication. The smart contract manages RRWs through the following functionalities:

Storage of Regional Reputation Weights: The smart contract stores the RRWs of each region.

Dynamic Update of Regional Weights: The smart contract updates RRWs dynamically based on predefined criteria and historical data.

Calculation of Vehicle Reputation Values: The smart contract calculates the vehicle's reputation value based on the RRWs of the source and target regions.

(3) Cross-Domain Authentication Process

During the cross-domain authentication phase, vehicles initiate authentication requests through the source region's Trust Authority (TA). The smart contract plays a vital role in this process:

Receiving Authentication Requests: Vehicles submit authentication requests to the smart contract via the source region's TA. The request includes the vehicle ID, source region's reputation value, target region ID, and a timestamp.

Signature Verification: The smart contract verifies the legitimacy of the signature using the vehicle's public key, ensuring the authenticity of the vehicle's identity.

Reputation Value Adjustment: Based on the RRWs of the source and target regions, the smart contract calculates the adjusted reputation value of the vehicle in the target region.

Storing Authentication Results: The authentication result (pass/fail) and the adjusted reputation value are stored on the blockchain via the smart contract.

All authentication processes, verification steps, and authentication results are recorded on the blockchain through the smart contract. This ensures transparency, traceability, and auditability of the entire authentication process. The smart contract automates key management, reputation weight adjustments, and authentication decisions, thereby enhancing the efficiency and security of cross-domain authentication in the Internet of Vehicles (IoV).

4.2 Registration Phase

In the registration phase, vehicles register their identities within the IoV and obtain their public-private key pairs. The pseudocode is shown in Table 3. The Data Flow Diagram is roughly illustrated in Figure 2. The detailed process is as follows:

4.2.1 Vehicle registration request

The vehicle node generates a registration request using its unique identity identifier ID_V and sends the request *GSetup()* to the local RSU. Upon receiving the request, the RSU forwards it to the upper-layer for registration.

4.2.2 Identity verification and key generation

The TA verifies the legitimacy of the vehicle's identity identifier *IDv*. If the verification is successful, the TA generates the vehicle's private key SK_V using Equation (7):

$$SK_V = H(ID_V) \cdot SK_{TA} \tag{7}$$

where *H()* is a cryptographic hash function, ID_V is the vehicle's unique identity identifier, and SK_{TA} is the private key of the TA.

The TA then generates the vehicle's public key PK_V using Equation (8):

$$PK_V = SK_V \cdot g_2 \tag{8}$$

where g_2 is the generator of the group G_2.

4.2.3 Recording and feedback

The TA records the vehicle's public keyPK_V and other relevant information on the upper-layer blockchain. Then, the TA then sends the registration status back to the RSU, which forwards it to the vehicle node.

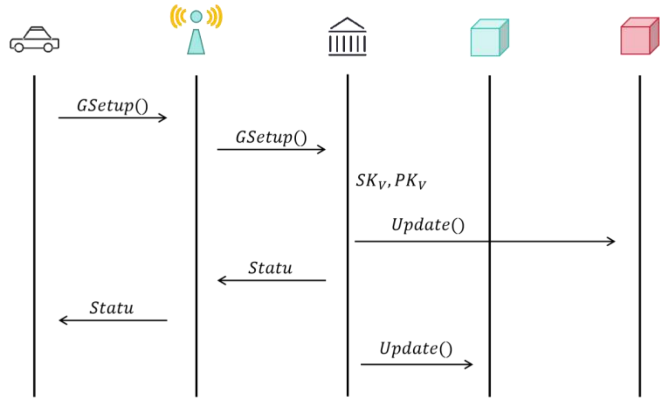

Figure 2 Data Flow Diagram for Registration Phase

Table 3 Registration Phase Algorithm

```
Algorithm 2: Registration algorithm
Input: Vehicles, RSU, TA, blockchain
Output: Registration Statu
for each vehicles do
    Get Vehicle $ID_V$
    Send $GSetup()$ to RSU and TA
    TA get $SK_V$ according to(7)
    TA gat $PK_V$ according to(8)
    Update $upblockchain()$
    Send statu to RSU and Vehicle
    Update $downblockchain()$
    return Registration Statu
end for
```

4.3 Intra-Domain Authentication Phase

The intra-domain authentication phase is a critical step where vehicles must be authenticated within their source region to ensure the legitimacy of their identity, the integrity of the information, and the validity of the authentication request. The pseudocode is shown in Table 4. The Data Flow Diagram is roughly illustrated in Figure 3. The detailed process is as follows:

4.3.1 Authentication request initiation

The vehicle node generates an authentication request and signs the request message before sending it to the local RSU. The authentication message format is:

$$m_V = \{ID_V, R_A, T, H(m_V), starttarget, endtarget\} \tag{9}$$

Where ID_V is the vehicle's unique identifier. R_A is the vehicle's reputation value. T is the timestamp. $H(m_V)$ is the hash of the message. starttarget and endtarget are the sender and receiver targets, respectively.

The vehicle uses its private key SK_V to generate the signature σ_V:

$$\sigma_V = SK_V \cdot H(m_V) \tag{10}$$

4.3.2 Signature verification by RSU

Upon receiving the authentication request, the RSU retrieves the vehicle's public key $PK_V$from the blockchain and verifies the signature using the following bilinear pairing equation:

$$e(\sigma_V, g_2) = ?\, e(H(m_V), PK_V) \tag{11}$$

If the signature verification fails, the RSU rejects the request and notifies the vehicle. If the signature verification succeeds, the RSU forwards the request to the TA.

4.3.3 Further verification by TA

The TA queries the vehicle's information stored on the blockchain to further verify the vehicle's identity, reputation value, and the validity of the authentication request. If the request passes all verifications, the TA returns an authentication success result to the vehicle.

4.3.4 Recording authentication results

All authentication requests and verification results are stored on the blockchain via a smart contract, ensuring the traceability and auditability of the authentication process.

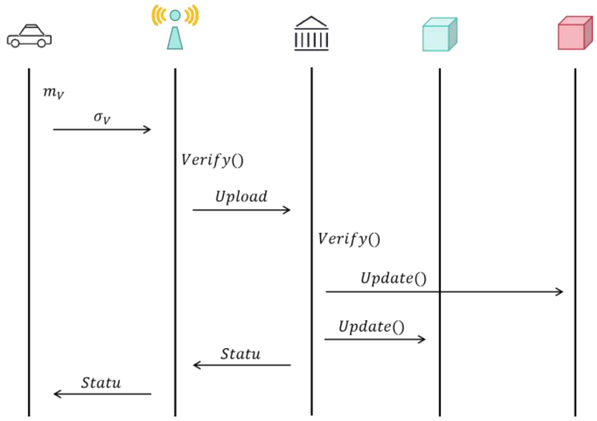

Figure 3 Data Flow Diagram for Intra-Domain Phase

Table 4 In-Domain Authentication Phase Algorithm

```
Algorithm 3: In-domain authentication algorithm
Input: Vehicles, RSU, TA, blockchain
Output: In-domain Statu
for each vehicle do
    Generate $m_V$
    Get $\sigma_V$ according to(10)
    Send to RSU
    if $verify(RSU)$ accoording to(11)
        upload TA
        if $verify(TA)$
            Update $upblockchain()$
        end if
        Update $downblockchain()$
    end if
    Send Statu to vehicle
    return In-domain Statu
end for
```

4.4 Cross-Domain Authentication Phase

The cross-domain authentication phase is initiated when a vehicle moves from one region to another and requests to join the vehicular network of the target region. This phase ensures that the vehicle is authenticated and its reputation is properly adjusted based on the regional reputation weights. The pseudocode is shown in Table 5. The Data Flow Diagram is roughly illustrated in Figure 4. The detailed process is as follows:

4.4.1 Authentication request initiation

The vehicle node in the source region (managed by Source TA) sends an authentication request to the Target TA. The request message format is:

$$m_{TA} = \{ID_V, R_A, RRW_A, T, H(m_{TA}), starttarget, endtarget, \sigma_V\} \tag{12}$$

Where ID_V is the vehicle's unique identifier. R_A is the vehicle's current reputation value. RRW_A is the Regional Reputation Weight of the source region. T is the timestamp. $H(m_{TA})$ is the hash of the message. starttarget and endtarget are the sender and receiver targets, respectively. σ_V is the signature generated by the vehicle.

The vehicle generates the signature σ_{TA} using its private key SK_V:

$$\sigma_{TA} = SK_V \cdot H(m_{TA}) \tag{13}$$

4.4.2 Signature verification by target TA

The Target TA retrieves the vehicle's public key PK_V from the blockchain and verifies the signature σ_{TA} using the bilinear pairing equation:

$$e(\sigma_{TA}, g_2) = ?\, e(H(m_{TA}), PK_V) \tag{14}$$

If the signature verification fails, the request is rejected, and the vehicle is notified.

4.4.3 Reputation adjustment

The Source TA's Regional Reputation Weight RRW_A and the Target TA's Regional Reputation Weight RRW_B are used to calculate the adjusted reputation value R_B for the vehicle in the target region:

$$R_B = R_A \times \frac{RRW_B}{RRW_A} \tag{15}$$

4.4.4 Automated reputation calculation by vehicle

As the vehicle moves through different regions, it automatically calculates its adjusted reputation value R_B' based on the known Regional Reputation Weights RRW_A' and RRW_B:

$$R_B' = R_A \times \frac{RRW_B'}{RRW_A'} \tag{16}$$

4.4.5 Malicious behavior check

The system verifies whether the vehicle's calculated reputation value R_B' matches the adjusted reputation value R_B computed by the TAs:

$$R_B = ?\, R_B' \tag{17}$$

If $R_B \neq R_B'$, the vehicle may be flagged for potential tampering or malicious behavior.

4.4.6 Recording authentication results

All information related to the authentication request (e.g., vehicle ID, source region reputation, target region reputation, signature) is stored on the blockchain via a smart contract. This ensures the transparency and traceability of the authentication process.

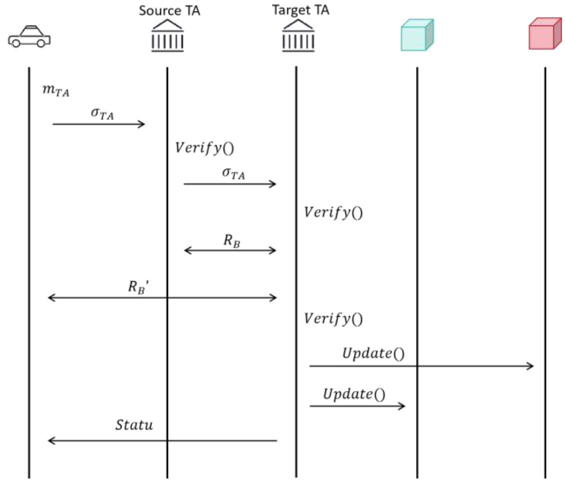

Figure 4 Data Flow Diagram for Cross-Domain Authentication Phase

Table 5 Cross-Domain Authentication Phase Algorithm

```
Algorithm 4: Cross-domain authentication algorithm
Input: Vehicles, Source TA, Target TA, blockchain
Output: Cross-domain Statu
for each vehicle do
    Generate $m_{TA}$
    Get $\sigma_{TA}$ according to(13)
    Send to SourceTA and TargetTA
    if $verify(TargetTA)$ according to(1114)
        TA get $R_B$ according to(15)
        vehilce get $R_B'$ according to(16)
        if $verify(Reputation)$ according to(17)
            Update $upblockchain()$
        end if
    end if
    Update $downblockchain()$
    return Cross-domain Statu
end for
```

4.5 Identity Traceability Phase

The primary objective of the identity traceability phase is to track the historical authentication records of vehicles during the cross-domain authentication process. This ensures the traceability and transparency of the authentication process. Detailed information from each authentication request, such as vehicle ID, reputation value, source region, target region, signature, and authentication status, is stored on the blockchain. This ensures the transparency of the authentication process. Additionally, multi-signature verification is employed to ensure that each step in the authentication decision-making process (e.g., source region TA, target region TA) is trustworthy. The signature records from each step are stored on the blockchain via a smart contract, allowing for the complete traceability of each authentication process. The pseudocode is shown in Table 6.

Table 6 Identity Traceability Algorithm

```
Algorithm 5: Identity traceability algorithm
Input: Vehicles, blockchain
Output: Identity history
for each blockchain do
Get $tranceID$
 if $Decrypt(SK_{TA}, EncrytedID)$== $tranceID$:
```

```
Add to $history()$
end if
if $history$
return $history()$
else
return "No Certification History Found"
end for
```

4.6 Security Analysis

4.6.1Signature Security

In the cross-domain authentication mechanism, the security of signatures is of paramount importance. We employ the BLS short signature algorithm, which is based on the computational difficulty of the discrete logarithm problem. This algorithm effectively prevents forgery attacks. Given the complexity of the discrete logarithm problem in large number fields, it is virtually impossible for attackers to forge a valid signature. Each vehicle's authentication request is encrypted using a BLS short signature, and only the private key held by a legitimate vehicle can generate a valid signature. Therefore, even if an attacker intercepts an authentication request, they cannot forge a valid signature for authentication, ensuring the reliability of identities and the accuracy of verification in cross-regional communications.

4.6.2 Reputation Value Security

The use of blockchain technology ensures the immutability of vehicle reputation records and authentication data. The authentication history and reputation values of vehicles in different regions are stored on the blockchain, and once written, these data cannot be modified or deleted. The distributed ledger of the blockchain not only enhances data transparency but also strengthens the system's defense against tampering attacks. For trust verification of various nodes in the Internet of Vehicles (IoV) (such as vehicles and roadside units), blockchain provides a reliable mechanism, ensuring that all vehicle behavior history and reputation calculations are traceable, public, and trustworthy.

Moreover, vehicles in different regions may face varying trust requirements and authentication standards. To ensure fair reputation adjustments during cross-domain authentication, the reputation values are adjusted based on the source region's reputation value and the target region's reputation weight. The source region's reputation value represents the trustworthiness of vehicles within that region, while the target region's reputation weight reflects the region's trust mechanism and its acceptance of incoming vehicles. Through this adjustment formula, the reputation values of vehicles are dynamically adjusted according to the trust requirements of different regions, ensuring fairness and rationality in the cross-domain authentication process.

4.6.3 Replay Attack Prevention

In the IoV environment, preventing replay attacks is crucial to protect the authentication mechanism from misuse. To this end, we introduce timestamps and unique authentication IDs for each authentication request. Timestamps ensure that each authentication request is accepted within a valid time window, and requests that exceed the time limit are rejected, effectively preventing attackers from replaying delayed requests. Additionally, unique authentication IDs ensure the uniqueness of each authentication request. Even if an attacker captures a legitimate request, they cannot reuse it to forge authentication. Through this mechanism, we not only prevent replay attacks but also ensure that each authentication request is unique and timely, which is particularly important for the high-frequency vehicle identity authentication in IoV.

5 EXPERIMENTAL EVALUATION

This chapter aims to demonstrate the practical usability of our protocol. We conducted simulation experiments using Veins (v 5.0), Omnet++ (v5.4.1), and urban traffic simulation (Sumo v1.11.0). The relevant map data is sourced from OpenStreetMap, and smart contracts were deployed using Solidity (v0.8.0). In the simulation experiments, we tested the write and query latency, message authentication latency, accuracy of introducing reputation authentication, and the message loss rate in the vehicular network. Next, we compared our protocol with FEDAS[9] and RCoM[10] through simulation experiments, with each simulation result being the average of 1000 trials. The map data comes from the streets around the school, and after integrating the road dataset using the Sumo tool, it is specifically shown in Figure 5.

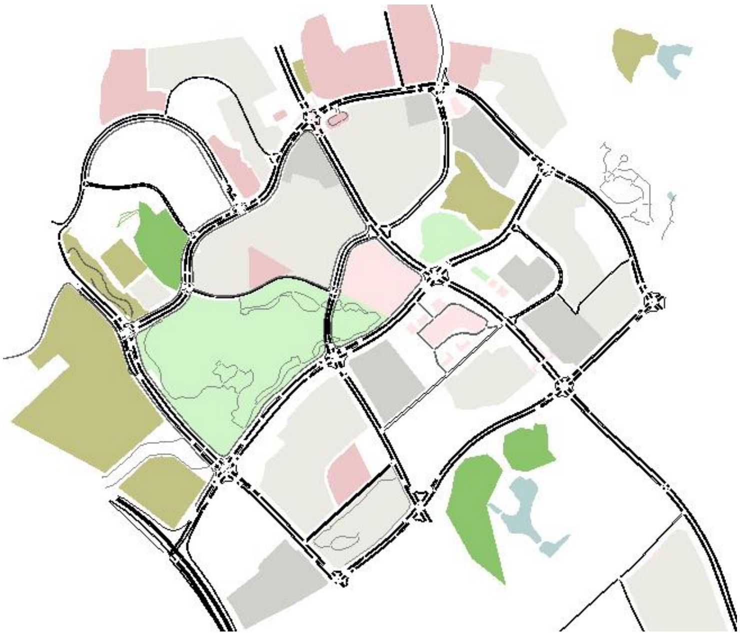

Figure 5 Simulates the Map

5.1 Write and Query Delays

In this protocol, given the introduction of blockchain technology, write delays and query delays have become important indicators for measuring system performance. Write delay refers to the time taken from when a vehicle node sends data until it is successfully written to the blockchain, while query delay refers to the time taken from when the requester sends a query request until the blockchain node returns a response. In this study, we primarily examined the impact of the number of regions (specifically 2, 4, 6, and 8) and vehicle density (ranging from 50 to 400 vehicles per square kilometer) on delays. The experimental results, as shown in Figure 6, indicate that as vehicle density increases, the write and query delays for vehicles within each region gradually increase. This is due to the fact that a higher vehicle density leads to an increase in the number of authentication requests, which in turn increases the load on the network and blockchain nodes, thereby increasing delays. As illustrated in Figure 7, an increase in the number of regions also leads to an increase in write and query delays. The primary reason for this phenomenon is that when vehicles perform cross-domain authentication between different regions, it results in more blockchain interactions, consequently leading to increased write and query delays.

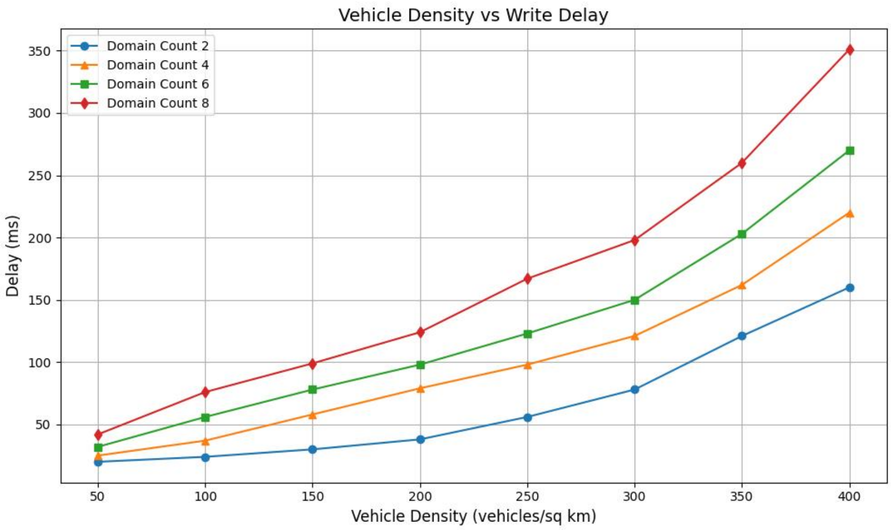

Figure 6 Changes in Vehicle Density and Write Latency

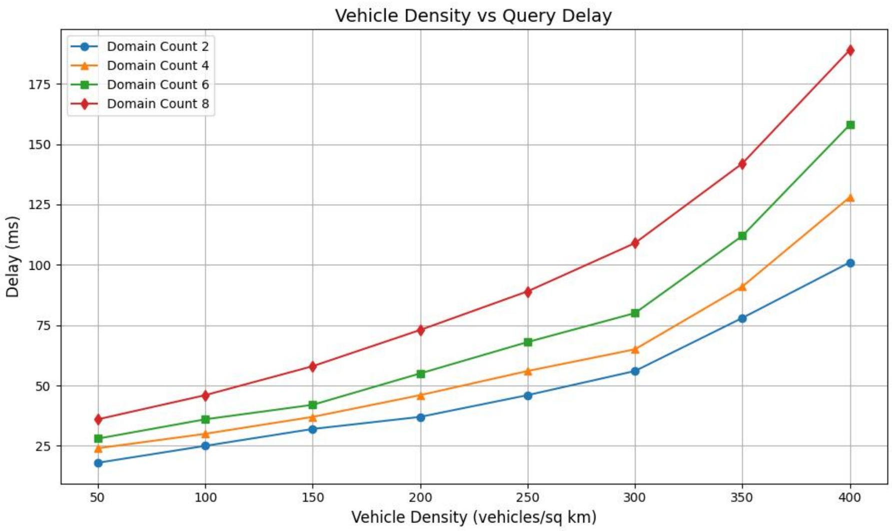

Figure 7 Changes in Vehicle Density and Query Latency

5.2 Delay in Message Authentication

In the Internet of Vehicles, message latency is one of the key indicators to measure system performance and user experience. Specifically, message latency refers to the total time that elapses between when the vehicle sends the certification request and when it receives the certification result. In order to evaluate the efficiency of different authentication protocols, we selected FEDAS[9] and RCoM[10] as the comparison experimental objects, mainly by analyzing the impact of the number of certified vehicles per unit time on the message authentication delay. As shown in Figure 8, the certification delay of the FEDAS and RCoM protocols slowly increases as the number of certified vehicles per unit time increases, until about 40 vehicles begin to increase significantly. This phenomenon may be due to the limited computing resources of centralized authentication, and when the number of authentication requests exceeds the processing capacity, the authentication efficiency of the system decreases rapidly. In contrast, the authentication latency of our solution is always between 200ms and 220ms. This is because we use short signature technology, which has the function of aggregate computation and can process multiple signature verifications in parallel, so as to ensure that the delay of the authentication process remains within a relatively stable range.

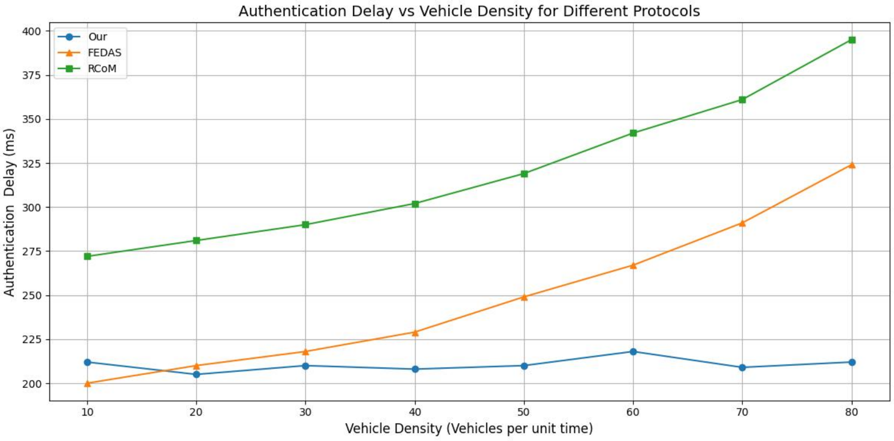

Figure 8 Changes in the Number of Vehicles Per Unit Time and the Certification Delay

5.3 The Introduction of Accuracy in Reputation-Based Authentication

In our cross-domain authentication scheme, reputation-based authentication rules have been introduced. To this end, we conducted comparative experiments between the scheme with a reputation authentication mechanism and the scheme that relies solely on short signatures, evaluating their performance in terms of true positive rate (TPR) and false positive rate (FPR). In the experiments, we assumed that there are 20% malicious vehicles in the network, which include attacks such as external intrusions and identity spoofing. Here, TPR represents the proportion of malicious vehicles correctly identified, while FPR indicates the proportion of normal vehicles misclassified as malicious. Specifically, it is expressed as:

$$\mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP+FN}} \tag{18}$$

$$\mathrm{FPR} = \frac{\mathrm{FP}}{\mathrm{FP+TN}} \tag{19}$$

Here, TP represents the number of vehicles correctly identified as malicious, FNrepresents the vehicles that are truly malicious but are incorrectly classified as normal by the system. FP refers to the vehicles that are truly normal but are incorrectly classified as malicious by the system. TN is the number of vehicles correctly classified as normal. The experimental results are shown in Figure 4-9, indicating that the authentication scheme using the reputation mechanism significantly outperforms the cross-domain authentication scheme that only uses short signatures in terms of TPR, while exhibiting a lower FPR. This is because, in the vehicular network environment, malicious vehicles, when performing cross-domain authentication, cannot access the reputation weight information of the source area for malicious vehicles in the target area, leading to errors in the reputation authentication module in certain cases. This error results in a higher TPR and a lower FPR, thereby enhancing the security of cross-domain authentication.

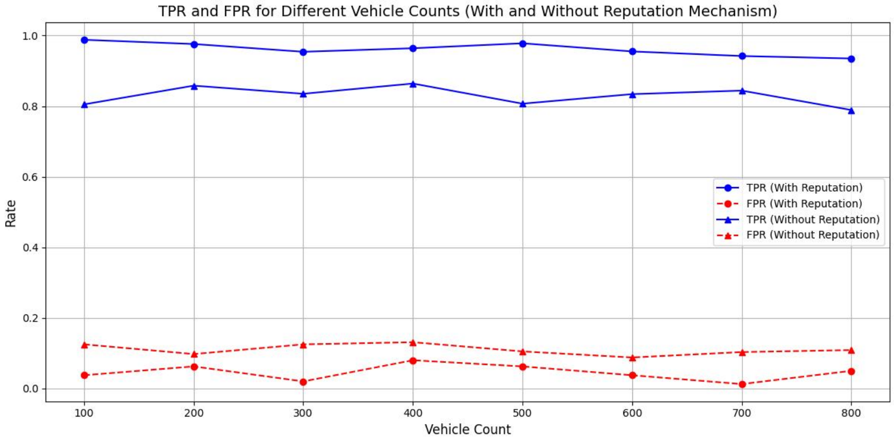

Figure 9 Changes between TPR and FPR

5.4 Packet Loss Rate

To evaluate the packet loss rate during the message transfer phase, we set the simulation experiment time to one hour. FEDAS[9] and RCoM[10] were used as comparison experiments to analyze the packet loss rate of the number of certifications per unit time. The simulation results are shown in 4-10, and we can observe that the influence of vehicle density on the packet loss rate is not significant. The packet loss rate of each protocol is stable within a fixed range, but our protocol has the lowest packet loss rate. The main reason is that each protocol has a fixed signature size, and the short signature technology has the smallest signature size.

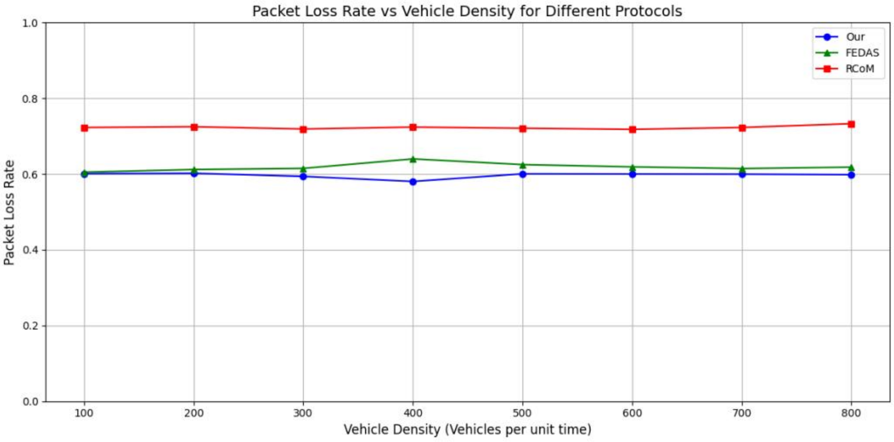

Figure 10 Comparison of Packet Loss Rates

6 CONCLUSION

This chapter discusses the efficiency and security issues faced by cross-domain authentication schemes in the Internet of Vehicles. Firstly, in view of the differences in the reputation evaluation system of different regions in the Internet of Vehicles, a reputation coupling scheme is proposed to ensure the fairness and effectiveness of the Internet of Vehicles. Then, combined with the practical application environment of the Internet of Vehicles, an efficient short signature technology is designed, and it is combined with the reputation mechanism to carry out double authentication, so as to improve the security of the vehicle node. In addition, through the introduction of blockchain and smart contract technology, the automatic execution of cross-domain authentication protocols is ensured, and the transparency and traceability of the authentication process are guaranteed. Finally, the effectiveness of the proposed scheme is verified by simulation experiments, and the experimental results show that the cross-domain authentication scheme of the Internet of Vehicles based on the short signature technology of reputation has improved the security and performance.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCE

[1] Hussain Q, Noor ASM, Qureshi MM. Reinforcement learning based route optimization model to enhance energy efficiency in internet of vehicles. Scientific Reports, 2025, 15: 3113.

[2] Yang Y, Chen Y, Liu Z, et al. Verifiable and redactable blockchain for internet of vehicles data sharing. IEEE Internet of Things Journal, 2025, 12(4): 4249-4261.

[3] Jiang Wenxian, Lv Xianglong, Tao Jun. A secure authentication framework for IoV based on blockchain and ensemble learning. Vehicular Communications, 2024, 50.

[4] Shen X, Ma R. A Blockchain Solution for the Internet of Vehicles with Better Filtering and Adaptive Capabilities. Sensors, 2025, 25(4): 1030.

[5] Ma Z, Jiang J, Wei H, et al. A Blockchain-Based Secure Distributed Authentication Scheme for Internet of Vehicles. IEEE Access, 2024, 12: 81471-81482.

[6] Liu Shuanggen, Zhou Xiayi, Wang Xu An, et al. A hash-based post-quantum ring signature scheme for the Internet of Vehicles. Journal of Systems Architecture, 2025, 160: 103345.

[7] Zhang X, Yang X, Zheng Y, et al. EACAS: An Efficient Anonymous Cross-domain Authentication Scheme in Internet of Vehicles. IEEE Internet of Things Journal, 2025, 160.

[8] Zhang J, Zhong H, Cui J, et al. CVAR: Distributed and Extensible Cross-Region Vehicle Authentication with Reputation for VANETs. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(1): 74-89.

[9] Wang Q, Gao D, Foh C H, et al. An Edge Computing-Enabled Decentralized Authentication Scheme for Vehicular Networks. ICC 2020 - 2020 IEEE International Conference on Communications (ICC). Dublin, Ireland: IEEE, 2020: 1-7.

[10] Wang Y, Ding Y, Wu Q, et al. Privacy-Preserving Cloud-Based Road Condition Monitoring with Source Authentication in VANETs. IEEE Transactions on Information Forensics and Security, 2019, 14(7): 1779-1790.

[11] Zhang J, Cui J, Zhong H, et al. PA-CRT: Chinese Remainder Theorem-Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 722-735.

[12] He D, Zeadally S, Xu B, et al. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[13] Cui J, Zhang X, Zhong H, et al. Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment. IEEE Transactions on Information Forensics and Security, 2020, 15: 1654-1667.

[14] Xu C, Ma M, Huang X, et al. A cross-domain group authentication scheme for LTE-A based vehicular network. In: 2017 IEEE 9th International Conference on Communication Software and Networks (ICCSN). Guangzhou, China: IEEE, 2017: 595-599.

[15] Sun C, Liu J, Xu X, et al. A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETs. IEEE Access, 2017, 5: 24012-24022.

[16] Meng X, Xu J, Liang W, et al. A lightweight anonymous cross-regional mutual authentication scheme using blockchain technology for internet of vehicles. Computers and Electrical Engineering, 2021, 95: 107431.

[17] Zhang J, Jiang Y, Cui J, et al. DBCPA: Dual Blockchain-Assisted Conditional Privacy-Preserving Authentication Framework and Protocol for Vehicular Ad Hoc Networks. IEEE Transactions on Mobile Computing, 2024, 23(2): 1127-1141.

[18] Zhu Y, Zhou Y, Wang J, et al.A Lightweight Cross-Domain Direct Identity Authentication Protocol for VANETs. IEEE Internet of Things Journal, 2024, 11(23): 37741-37757.

[19] Zhong Q, Zhao X, Xia Y, et al. CD-BASA: An Efficient Cross-Domain Batch Authentication Scheme Based on Blockchain With Accumulator for VANETs. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(10): 14560-14571.

[20] Tan H, Xuan S, Chung I. HCDA: Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs. Symmetry, 2020, 12(6): 1003.