2025 IEEE International Conference on High Performance Computing and Communications (HPCC) | 979-8-3315-6874-0/25/$31.00 ©2025 IEEE | DOI: 10.1109/HPCC67675.2025.00093

Edge Computing-Based Anonymous Cross-Domain Authentication Scheme for VANETs

Bei Li[1], Hong Zhong[1*], Chengdong Gu[1], Jing Zhang[1], Qingyang Zhang[1], Jiaxin Li[1, 2], Jie Cui[1*]
[1]*School of Computer Science and Technology, Anhui University, Hefei, China*
[2]*Security Research Institute, New H3C Group, Hefei, 230088, China*
*Corresponding Authors: Hong Zhong (zhongh@ahu.edu.cn) and Jie Cui (cuijie@mail.ustc.edu.cn)

***Abstract*—In the vehicular ad-hoc networks (VANETs), cross-domain communication among vehicles significantly improves traffic efficiency and road safety. However, due to the vulnerabilities of vehicle communication, it faces numerous security challenges when performing cross-domain communication. Existing schemes rely on trusted third parties for cross-domain authentication, resulting in issues such as low computational efficiency and weak privacy protection for vehicles, which cannot meet the demands of large-scale vehicle cross-domain communication. To address these problems, we propose an efficient and anonymous cross-domain authentication scheme based on edge computing. By using edge gateways to manage vehicle groups and handle cross-domain event requests, we solve the performance bottleneck issues caused by centralized authentication. Additionally, the use of a batch authentication mechanism further improves computational efficiency during large-scale authentications and reduces authentication latency. Security and performance analyses show that the proposed scheme can meet the security and performance requirements for cross-domain vehicle communication.**

***Index Terms*—VANETs, cross-domain communication, edge computing, authentication**

I. Introduction

Vehicular ad-hoc networks (VANETs) connects vehicles and other infrastructure to form a dynamic and cooperative network. It enables environmental sensing and information exchange for applications like driving assistance and traffic management, thereby improving traffic efficiency and safety [1]. Due to the mobility of vehicles, they frequently move across different regions, often requiring data communication across distinct administrative domains [2]. For example, when a vehicle in Region A detects a traffic accident ahead, it needs to broadcast a warning message to vehicles in the adjacent Region B that are about to enter, in order to prevent congestion caused by a sudden influx of vehicles. However, this process faces numerous security threats. Adversaries may launch impersonation or tampering attacks to disrupt the system or obtain vehicle privacy. Therefore, a secure cross-domain authentication protocol is necessary to ensure the authenticity and integrity of communication messages between vehicles.

To ensure the security of vehicle authentication, many schemes have been proposed. Most existing solutions rely on a centralized Public Key Infrastructure (PKI), requiring a trusted authority to issue certificates for identity verification [3], [4]. Vehicles in one domain (domain A) first have to be centrally authenticated by a third-party authentication server before the authentication request can be sent to another domain (domain B), and the request returned in domain B needs to go through the authentication server again.

For cross-domain authentication, Brecht *et al.* [5] proposed a secure communication system based on a trust list, but the scheme suffers from limited flexibility and high computational overhead [6]. Feng *et al.* [7] proposed an identity-based cross-domain authentication protocol, but it relies on bilinear pairings, resulting in significant computational cost. There are a large number of vehicles in each domain in VANETs, and when the number of authentication in a domain surges at the same moment, it can cause a large delay if the domain servers do not process the messages in a timely manner. Consequently, existing schemes fall short in meeting the efficiency requirements of large-scale cross-domain authentication for vehicles. This calls for the design of an efficient and anonymous cross-domain authentication protocol.

The distributed nature of edge computing can help alleviate the computational bottleneck and authentication latency issues caused by the centralized authentication of third-party servers [8]. By leveraging edge gateways to perform vehicle authentication, edge computing can be effectively integrated into cross-domain authentication in VANETs, thereby reducing transmission delays and enhancing overall system efficiency.

A. Contributions

In this paper, we propose an efficient anonymous cross-domain message authentication scheme for VANETs, with the following main contributions:

- The proposed scheme introduces an edge gateway to manage the local group within a cross-domain cooperative scenario. Specifically, the gateway is responsible for authenticating vehicles and distributing local temporary private keys to those joining the event. This design mitigates the drawbacks of centralized authentication and significantly reduces authentication latency.
- The proposed scheme supports dynamic domain scalability by enabling the trusted authority (TA) to register the public-private key pairs of domain private key generators using the Schnorr signature scheme. Furthermore, batch authentication in the vehicle-to-vehicle communication phase reduces the computational overhead associated with message authentication, thereby improving efficiency.

979-8-3315-6874-0/25/$31.00 ©2025 IEEE
DOI 10.1109/HPCC67675.2025.00093

- Formal security analysis demonstrates that the proposed scheme satisfies the security and privacy requirements of cross-domain vehicular communications. Furthermore, a thorough performance evaluation and comparative analysis with existing state-of-the-art schemes demonstrate the advantages of the proposed scheme.

B. Related Works

To protect vehicle's privacy, Jo *et al.* [9] proposed a cooperative authentication scheme based on pseudonyms. Haider *et al.* [10] introduced a pseudonym generation mechanism to reduce memory overhead and enhance the confidentiality of vehicle location privacy. However, such pseudonym-based approaches often result in significant certificate management overhead. Therefore, some works adopt identity-based signatures to achieve privacy preservation [11], but most of these schemes rely on bilinear pairings, leading to high computational costs. To address this, several pairing-free authentication schemes have been proposed [12]–[14], which reduce computation while ensuring anonymity. Nevertheless, these schemes do not consider the cross-domain authentication requirements of vehicles, thus failing to support secure cross-domain communication.

To enable secure cross-domain authentication, Ma *et al.* [15] proposed a model based on multiple intermediate entities, where users' private keys are distributedly stored to enhance system efficiency. Shen *et al.* [16] presented a blockchain-based cross-domain authentication scheme that integrates identity-based cryptography, but the collaborative interactions required during authentication introduce high computational overhead. Cheng *et al.* proposed a privacy preserving authentication scheme for multiple domains. Mahmood *et al.* [17] also designed a blockchain-based cross-domain authentication scheme, but its reliance on third-party servers during the authentication process can lead to increased communication latency. Liu *et al.* [18] proposed a certificateless anonymous cross-domain authentication scheme to achieve efficient cross-domain communication. Zhu *et al.* [19] developed a lightweight cross-domain authentication protocol, which significantly improves efficiency by precomputing communication credentials within the local domain. Zhong *et al.* [20] proposed a blockchain-based efficient cross-domain authentication scheme that employs batch authentication to improve performance. Seifelnasr *et al.* [21] designed a conditional message authentication protocol for VANETs cross-domain communication, allowing vehicles to interact with authorities from different domains without requiring prior registration. Liu *et al.* [22] proposed a mobile edge computing based cross-domain authentication scheme, which supports anonymous and batch verification.

II. Preliminaries and Background

A. Mathematical Assumption

Computational Diffie-Hellman problem (CDH): Given two unknowns $a, b \in Z_q^*$, the CDH problem is defined as follows: given points $P, aP, bP \in G$, compute $abP \in G$.

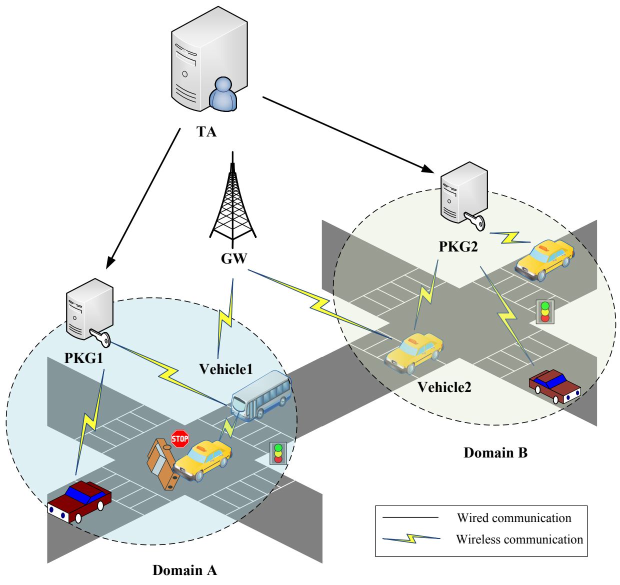

Fig. 1. System Model

B. System Model

As shown in Fig. 1, there are four entities in the system model, which are trust authority (TA), domain private key generator (PKG), edge gateway (GW), and vehicles.

- *TA*: TA is fully trusted and is responsible for coordinating the generation of system parameters and providing registration services for domain private key generators and edge gateways. It does not participate in the cross-domain vehicle authentication process.
- *PKG*: PKG manages vehicles within its domain, handling vehicle registeration and tracing the identities of compromised vehicles. It does not participate in the cross-domain vehicle authentication process.
- *GW*: The gateway is responsible for managing the local group involved in a specific cross-domain cooperative communication, Specifically, it handles vehicle-to-gateway authentication and distributes temporary local group keys when a vehicle joins the group communication.
- *Vehicle*: A vehicle typically has limited computational resources and storage capacity. However, these resources are generally adequate for performing public-key cryptographic operations and store pseudonyms, which is reasonable given the capabilities of modern onboard units.

C. Threat Model

Since vehicles are connected through insecure public channels, they are vulnerable to various attacks defined in the Dolev-Yao threat model. In the case of passive attacks, attackers may eavesdrop on wireless transmissions to extract sensitive information or sender's identity. Active adversaries can intercept and modify transmitted messages or inject forged data to mislead other vehicles.

D. Security Requirements

For the above threat model, we mainly focus on the following security requirements.

1) *Message Integrity and Authentication*: The receiver can verify the legitimacy of the message and ensure that it has not been modified or forged by employing message authentication techniques.
2) *Identity Privacy Preservation*: Only the PKG of the domain to which the vehicle belongs can extract its private information from intercepted messages. No other entity can do so, ensuring the privacy of the vehicle's identity.
3) *Traceability and Identity Revocation*: If a compromised vehicle disseminates false information that threatens traffic safety or disrupts vehicular communication, the PKG of its domain can retrieve its real identity and revoke its credentials to mitigate further risk.
4) *Unlinkability*: No gateway or malicious vehicle can associate two messages sent by the same vehicle if the time interval between them exceeds Δt.
5) *Replay Attack*: An attacker attempts to interfere with vehicular communication by replaying previously captured messages.
6) *Impersonation Attack*: In this attack, an adversary pretends to be a legitimate vehicle to obtain an identity token from gateways or to inject malicious messages into the vehicular network.
7) *Modification Attack*: An attacker alters intercepted legitimate messages to mislead vehicles or disrupt traffic coordination.
8) *Man-in-the-Middle Attack*: During communication between two vehicles or between a vehicle and a gateway, an attacker cannot tamper with transmitted information by acting as an intermediary and impersonating both communicating parties.

III. Proposed Scheme

In this section, we describe our scheme through the following stages: *System Initialization*, *Domain PKG Registration*, *Gateway Registration Phase*, *Vehicle Registration Phase*, *Authentication*.

A. System Initialization

In this phase, the trust authority (TA) generates the system master key and the system parameters by executing the following processes.

1) The TA selects two random numbers p, q, an elliptic curve $E(F_p)$ defined on F_p, and an addition group G of order q with generator P. TA also chooses four secure hash functions $h_i : \{0,1\}^* \rightarrow Z_q^*(i = 1,2,3,4,5)$.
2) The TA chooses a random number $s \in Z_q^*$ as the private key, and computes the corresponding public key $P_{pub} = sP$;
3) The TA publishes $\{p, q, E(F_p), P, P_{pub}\}$ and saves s secretly.

B. Domain PKG Registration Phase

When PKG_i of Domain D_i intends to join the system, it must first register with TA. The following steps will be executed by PKG_i and TA.

1) TA randomly picks an element k_i and computes $P_{pkg_i} = k_i P$, and $sk_{pkg_i} = s + k_i h_1(D_i, P_{pkg_i}) \bmod q$. Finally, TA sends $\{sk_{pkg_i}, P_{pkg_i}\}$ to PKG_i through a secure channel.
2) PKG_i stores $\{sk_{pkg_i}, P_{pkg_i}\}$ securely.

C. Gateway Registration Phase

For GW_l responsible for a cross-domain event E_l, TA generates its certificate $Cert_{GW_l}$ as following steps:

1) TA randomly chooses $\upsilon_l \in Z_q^*$ as GW_l's private key and computes $P_{GW_l} = \upsilon_l P$ as its public key.
2) TA computes the signature S_{GW_l} on P_{GW_l}, where $S_{GW_l} = Sign(s, P_{GW_l} || E_l)$ and $||$ is connect operation.
3) TA sends υ_l, P_{GW_l}, and $Cert_{GW_l}$ to GW_l over a secure channel, where $Cert_{GW_l} = (P_{GW_l}, E_l, S_{P_{GW_l}})$.

Additionally, within a specified time interval (e.g., one day), the TA generates temporary local group parameters (G_l, P_l, q_l) for the gateway GW_l, where P_l is the generator of the local cyclic group G_l. The TA then securely sends these temporary parameters (G_l, P_l, q_l) along with the signature $Sig_k(G_l, P_l, q_l, TS_l)$ to GW_l to GW_l, where TS_l denotes the current timestamp.

D. Vehicle Registration Phase

When a vehicle V_i of domain D_j that will participate in the cross-domain event E_l wishes to join the system, V_i will register with PKG_j. The following steps will be executed by PKG_j and V_i.

1) V_i sends its identity ID_{V_i} and E_l to PKG_j.
2) PKG_j randomly picks an element ϵ_i and computes V_i's pseudo identity $pid_{V_i} = Enc_{k_j}(ID_i + \epsilon_i, \epsilon_i)$. PKG_j randomly picks an element r_{V_i} and computes $R_{V_i} = r_{V_i} \cdot P$, and $sk_{V_i} = sk_{pkg_j} + h_2(pid_{V_i}, D_i, E_l, P_{pkg_j}, R_{V_i}) \cdot r_{V_i} \bmod q$. Finally, PKG_j sends $\{pid_{V_i}, sk_{V_i}, R_{V_i}, D_j, P_{pkg_j}, E_l\}$ to V_i through a secure channel.
3) V_i stores $\{pid_{V_i}, sk_{V_i}, R_{V_i}, D_j, P_{pkg_j}, E_l\}$.

E. Authentication

The authentication process in the proposed scheme consists of two phases: V2G authentication phase and V2V authentication phase. When a vehicle seeks to participate in a collaborative communication within a cross-domain event managed by a gateway, it initiates a request to the gateway, triggering the V2G authentication phase. Upon successful authentication, the gateway generates a local group signature private key pair and transmits it to the vehicle. The vehicle then utilizes this key pair to establish communication with other vehicles involved in the collaborative communication. Subsequently, the V2V authentication phase starts.

1) V2G Authentication: In this phase, the vehicle V_i from domain D_j sends a request to GW_l, which then authenticates the vehicle and generates a locally signed private key pair for V_i. V_i chooses a random r_i, and computes $R_i = r_i P$, $Z_i = sk_{V_i} + r_i \cdot h_3(m_i, pid_{V_i}, R_{V_i}, TS_i)$, where TS_i is the current timestamp. Then V_i sends $(m_i, pid_{V_i}, R_{V_i}, D_j, P_{pkg_j}, TS_i, R_i, Z_i)$ to GW_l. When GW_l receives the request information, it performs the following steps.

1) GW_l checks whether pid_{V_i} is in the certificate revocation list (CRL). If it is found in the CRL, the request is rejected.
2) GW_l computes $c_{i,1} = h_3(m_i, pid_{V_i}, R_{V_i}, TS_i)$, $c_{i,2} = h_2(pid_{V_i}, D_j, E_l, P_{pkg_j}, R_{V_i})$ and then verifies the legitimacy of V_i by checking equation (1). If the verification fails, V_i is rejected.

$$Z_i \cdot P = P_{pub} + h_1(D_j, P_{pkg_j}) \cdot P_{pkg_j} + c_{i,2} R_{V_i} + c_{i,1} R_i \tag{1}$$

3) GW_l randomly chooses ξ_i, and creates a local group signature private key pair $lsk_i = (\alpha_i, \omega_i)$, where $\alpha_i = \xi_i P_l$, and $\omega_i = \xi_i + h_4(\alpha_i) \cdot \upsilon_l$. It then records the mapping between lsk_i and pid_{V_i} in the vehicle's identity mapping (VIM) table.
4) GW_l computes session key $sk_{i,l} = h_4(\upsilon_i R_i)$, $pk'_{GW_l} = k_l P_l$, sets $msg_i = ENC_{sk_{i,l}}(lsk_i)$ $||(G_l, P_l, q_l, TS_l, pk'_{GW_l})||Sig_k(G_l, P_l, q_l, TS_l)$, $mac_i = MAC_{sk_i}(msg_i)$, and sends $\{msg_i, mac_i\}$ to V_i.

Once receiving the message from GW_l, V_i carries out the following process:

1) V_i first verifies mac_i by using the pair-wise key $sk_{i,l} = h_4(r_i PK_{GW_l})$.
2) V_i checks TS_l and uses TA's public key P_{pub} to validates the signature $Sig_k(G_l, P_l, q_l, TS_l)$. It then obtains lsk_i to check whether $\omega_i P_l = \alpha_i + h_4(\alpha_i) \cdot pk'_{GW_l}$ holds. And V2V authentication uses lsk_i as temporary local group signature private key for cross-domain cooperative event E_l.

2) V2V Authentication: If the vehicle successfully obtains lsk_i from the gateway and wishes to establish communication with other vehicles, it starts the V2V authentication.

When a vehicle V_i needs to send a message m_i, It needs to choose $b_i \in Z_q^*$, computes $Q_i = b_i P_l$. It computes $f_i = h_5(m_i, \alpha_i, Q_i, TS_i)$, $\beta_i = \omega_i + f_i \cdot b_i$, where TS_i is the current timestamp. Then V_i sends $(m_i, TS_i, \alpha_i, Q_i, \beta_i)$ to the receiver.

Upon receiving the message $(m_i, TS_i, \alpha_i, Q_i, \beta_i)$ from V_i, the receiver first checks the validity of TS_i. Refuse to receive if it is invalid. Then it computes $f_i = h_5(m_i, \alpha_i, Q_i, TS_i)$ and verify the message by checking equation (2).

$$\beta_i \cdot P_l = \alpha_i + h_4(\alpha_i) \cdot pk'_{GW_l} + f_i \cdot Q_i \tag{2}$$

If the vehicle has n messages $(m_i, TS_i, \alpha_i, Q_i, \beta_i)$ $(i \in [1, n])$ to be authenticated, then it can use the batch authentication technique to reduce the computation overhead and reduce the authentication delay. The vehicle randomly selects $\varpi = (\varpi_1, \varpi_2, ..., \varpi_n)$ $(\varpi_i \in [1, 2^n]$, and subsequently checks equation (3) to check the authenticity of this batch of messages.

$$\begin{aligned}(\sum_{i=1}^{n} \varpi_i \cdot \beta_i) \cdot P_l = \sum_{i=1}^{n} \varpi_i \cdot \alpha_i + (\sum_{i=1}^{n} \varpi_i \cdot h_4(\alpha_i)) \cdot pk'_{GW_l} \\ + \sum_{i=1}^{n} \varpi_i \cdot f_i \cdot Q_i\end{aligned} \tag{3}$$

Here we give the correctness derivation for batch authentication. Due to $Q_i = b_i \cdot P_l$, $\alpha_i = \xi_i P_l$, $\omega_i = \xi_i + h_4(\alpha_i) \cdot \nu_l$, $f_i = h_5(m_i, \alpha_i, Q_i, TS_i)$, $\beta_i = \omega_i + f_i \cdot b_i$, $pk'_{GW_l} = \nu_l P_l$, we obtain

$$\begin{aligned}(\sum_{i=1}^{n} \varpi_i \cdot \beta_i) \cdot P_l &= (\sum_{i=1}^{n} \varpi_i \cdot (\omega_i + f_i \cdot b_i)) \cdot P_l \\ &= (\sum_{i=1}^{n} \varpi_i \cdot (\xi_i + h_4(\alpha_i) \cdot \nu_i + f_i \cdot b_i)) \cdot P_l \\ &= \sum_{i=1}^{n} \varpi_i \cdot (\xi_i \cdot P_l) + (\sum_{i=1}^{n} \varpi_i \cdot h_4(\alpha_i)) \\ &\quad \cdot (\nu_i \cdot P_l) + (\sum_{i=1}^{n} \varpi_i \cdot f_i) \cdot (b_i \cdot P_l) \\ &= \sum_{i=1}^{n} \varpi_i \cdot \alpha_i + (\sum_{i=1}^{n} \varpi_i \cdot h_4(\alpha_i)) \cdot pk'_{GW_l} \\ &\quad + \sum_{i=1}^{n} \varpi_i \cdot f_i \cdot Q_i.\end{aligned} \tag{4}$$

IV. Security Proof and Analysis

In this section, we analyze the security of the proposed scheme and demonstrate that it fulfills the security requirements outlined in Section II.

A. Security Proof

Theorem 1: For the proposed scheme, no PPT adversary can forge a legitimate request message to negotiate a secret key with the gateway and get a temporary local group private key, i.e., the advantage of winning the above game $Adv_{\mathcal{P}}^{\mathcal{A}}$ is negligible.

$$\begin{aligned}Adv_{\mathcal{P}}^{\mathcal{A}} \leq & \frac{(q_s + q_e)^2}{q} + \frac{\sum_{i=1}^{4} q_{h_i}^2}{q} + \frac{2q_s}{q} \\ & + 2\sum_{i=0}^{3} q_{h_i} \cdot q_s \cdot Adv_{CDH}^{\mathcal{A}}\end{aligned} \tag{5}$$

where q_{h_i}, q_s, q_e denote the number of hash queries, Send queries, and Execute queries that $\mathcal{A}$ can perform in polynomial time t. $Adv_{CDH}^{\mathcal{A}}$ denotes the advantage of winning the CDH problem. The theorem is proved by five games between $\mathcal{A}$ and $\mathcal{C}$. The event E_i represents the win of $\mathcal{A}$ in the game G_i.

Game G_0: In this game, $\mathcal{A}$ can initiate a predicator query to $\mathcal{C}$, and $\mathcal{C}$ needs to return a corresponding response to

$\mathcal{A}$. $\mathcal{C}$ first initialize some system parameters $param = \{q, E, G, P, P_{pub}, h_i(\cdot)\}$ $(i \in [1, 4])$.

Extract Query: It can be divided into two sub-queries according to the specific query type as follows:

- $ExtractPKG(D_j)$: Receiving $ExtractPKG(D_j)$, $\mathcal{C}$ checks if the tuple $(D_j, P_{pkg_i}, sk_{pkg_i})$ is recorded in $list_{PKG}$. If exists, return P_{pkg_i} to $\mathcal{A}$. Otherwise, $\mathcal{C}$ randomly selects an element k_i and computes $k_{pkg_i} = s + k_i - h_1(D_i, P_{pkg_i})$ and $P_{pkg_i} = k_i - P$. Finally, $\mathcal{C}$ records $(D_i, P_{pkg_i}, h_1(D_i, P_{pkg_i}))$ in $list_{h_1}$, records $(D_j, P_{pkg_i}, sk_{pkg_i})$ in $list_{PKG}$ and send P_{pkg_i} to $\mathcal{A}$.
- $ExtractV(D_j, ID_{V_i})$: After receiving the query for vehicle identity ID_{V_i}, $\mathcal{C}$ checks whether the tuple $(ID_{V_i}, pid_{V_i}, R_{V_i}, sk_{V_i})$ is recorded in $list_V$. If exist, $\mathcal{C}$ returns pid_{V_i} to $\mathcal{A}$. Otherwise, $\mathcal{C}$ randomly selects k_i and calculates $sk_{pkg_i} = s + k_i - h_1(D_i, P_{pkg_i})$ and $P_{pkg_i} = k_i - P$. $\mathcal{C}$ records $(D_i, P_{pkg_i}, h_1(D_i, P_{pkg_i}))$ in $list_{h_1}$ and $(D_j, P_{pkg_i}, sk_{pkg_i})$ in $list_{PKG}$. Then, $\mathcal{C}$ randomly selects the event E_l as well as pid_{V_i}, $r_{V_i} \in Z_q^*$ and calculates $R_{V_i} = r_{V_i} \cdot P$ as well as $sk_{V_i} = sk_{pkg_j} + h_2(pid_{V_i}, D_i, E_l, P_{pkg_j}, R_{V_i}) \cdot r_{V_i}$. Finally, $\mathcal{C}$ records the tuple $(pid_{V_i}, D_i, E_l, P_{pkg_j}, R_{V_i}, \eta_{h_2})$ in the list $list_{h_2}$ and $(ID_{V_i}, pid_{V_i}, sk_{V_i}, R_{V_i})$ in the list $list_V$, and send pid_{V_i} to $\mathcal{A}$.

Send Query: It can be divided into three sub-queries according to the specific query type as follows:

- $Send(V_i, start)$: When this query is received, $\mathcal{C}$ randomly selects $r_i \in Z_q^*$ and computes $R_i = r_i P$ as well as $Z_i = sk_{V_i} + r_i \cdot h_3(pid_{V_i}, R_{V_i}, TS_i)$. Finally, $\mathcal{C}$ returns the result of this query $M_{V2G} = (pid_{V_i}, R_{V_i}, D_j, P_{pkg_j}, TS_i, R_i, Z_i)$.
- $Send(GW_j, M_{V2G})$: When this query is received, $\mathcal{C}$ checks the correctness of Z_i, then randomly selects msg_i and computes $pk'_{GW_l} = \nu_l P_l$, $sk_{il} = h_4(\nu_i R_i)$, $mac_i = MAC_{sk_{il}}(msg_i)$, and finally returns $M_{G2V} = (msg_i, mac_i)$. If the check is wrong, reject the query and return $\perp$. Otherwise, add $(M_{V_{i1}}, M_{G2V})$ to $list_M$.
- $Send(V_i, M_{G2V})$: Receiving this query, $\mathcal{C}$ computes $sk^*_{il} = h_4(r_i P_{GW_l})$ and checks if mac_i is equal to $MAC_{sk^*_{il}}(msg_i)$. If not equal, terminate the game.

Execute Query: When the query $Execute(V_i, GW_j)$ is received, $\mathcal{C}$ looks up (M_{V2G}, M_{G2V}) from $list_M$ and sends it to $\mathcal{A}$.

Reveal Query: When $\mathcal{C}$ receives the $Reveal(\Pi^k_\Lambda)$ query, determine whether Π^k_Λ is accepted or not. If accepted, return the session secret key sk_{il} for it; otherwise, output $\perp$.

Corrupt Query: It can be divided into two sub-queries according to the specific query type as follows:

- $CorruptPKG(D_j)$: When receiving this query, $\mathcal{C}$ checks the data (P_{pkg_i}, sk_{pkg_i}) in $list_{PKG}$ and returns it to $\mathcal{A}$.
- $CorruptV(ID_j)$: When receiving this query, $\mathcal{C}$ checks the data (R_{V_i}, sk_{V_i}) in $list_V$ and returns it to $\mathcal{A}$.

Test Query: At the end of the game, $\mathcal{A}$ initiates this query and $\mathcal{C}$ randomly selects a $b \in \{0, 1\}$. If $b = 0$, $\mathcal{C}$ randomly selects a value whose length is equal to the session secret key and returns it to $\mathcal{A}$. If $b = 1$, $\mathcal{C}$ replies the sk_{il} obtained by $Reveal(\Pi^k_\Lambda)$ to $\mathcal{A}$. This game simulates a real attack and all queries are executed according to the scheme. Therefore, the probability that adversary $\mathcal{A}$ wins in G_0 is

$$Adv^{\mathcal{A}}_{\mathcal{P}} = 2|Pr[E_0] - \frac{1}{2}| \tag{6}$$

Game G_1: This game differs from G_0 in that it simulates a hash prediction machine, and $\mathcal{C}$ builds four lists $list_{h_i}$ $(i \in [1, 4])$ to store the corresponding hash information. When $\mathcal{A}$ initiates a hash query, $\mathcal{C}$ checks whether m_i is recorded in $list_{h_i}$, and if so, $\mathcal{C}$ sends $list_{h_i}(m_i)$ to A. Otherwise, $\mathcal{C}$ randomly selects $\alpha_i \in Z_q$, records α_i in the response list and sends it to $\mathcal{A}$. In G_1, A wins with the same probability as G_0. Therefore

$$Pr[E_1] = Pr[E_0] \tag{7}$$

Game G_2: The game differs from G_1 in that there are no collisions. There are two types of collisions in G_1: hash collisions and random number collisions. Among them, the probability of a collision between hash predictors is maximized as $\frac{\sum_{i=1}^{4} q^2_{h_i}}{2q}$, and the probability of a collision between random numbers r_i and v_l is maximized as $\frac{(q_s+q_e)^2}{2q}$. Therefore,

$$|Pr[E_2] - Pr[E_1]| \leq \frac{(q_s + q_e)^2}{2q} + \frac{\sum_{i=1}^{4} q^2_{h_i}}{2q} \tag{8}$$

Game G_3: The game simulates all queries in G_2. If $\mathcal{A}$ is lucky enough to guess the correct validator value without asking for a random prediction, G_2 will be aborted. Since it is impossible to distinguish the difference, it is possible to obtain

$$|Pr[E_3] - Pr[E_2]| \leq \frac{q_s}{2q} \tag{9}$$

Game G_4: In the final game, the simulation is executed using the CDH problem. Given a CDH instance $R_i = r_i P$, $P_{GW_l} = \nu_l P$, it is obtained that

$$|Pr[E_4] - Pr[E_3]| \leq \sum_{i=1}^{4} q_{h_i} \cdot q_s \cdot Adv^{\mathcal{A}}_{CDH} \tag{10}$$

When adversary $\mathcal{A}$ has completed all queries, it can win the game by sending one bit b' to challenger $\mathcal{C}$. So

$$|Pr[E_4]| = \frac{1}{2} \tag{11}$$

There, by the above equation, it is obtained that

$$
\begin{aligned}
Adv_{\mathcal{P}}^{\mathcal{A}} &= 2|Pr[E_0] - 1/2| \\
&= 2|Pr[E_1] - Pr[E_2] + Pr[E_2] - Pr[E_3] \\
&\quad + Pr[E_3] - Pr[E_4] + Pr[E_4] - 1/2| \\
&= 2(|Pr[E_2] - Pr[E_1]| + |Pr[E_3] - Pr[E_2]| \\
&\quad + |Pr[E_4] - Pr[E_3]| + |Pr[E_4] - 1/2|) \\
&\leq \frac{(q_s + q_e)^2}{q} + \frac{\sum_{i=1}^{4} q_{h_i}^2}{q} + \frac{2q_s}{q} \\
&\quad + 2\sum_{i=0}^{3} q_{h_i} \cdot q_s \cdot Adv_{CDH}^{\mathcal{A}}
\end{aligned} \tag{12}
$$

B. Security Analysis

1) Message Integrity and Authentication: According to Theorem 1, the proposed scheme is secure against existential forgery under adaptive selective message attack. Therefore, no probabilistic polynomial time adversary can forge a valid message m_i and signature $(m_i, TS_i, \alpha_i, Q_i, \beta_i)$ which can make the equation $\beta_i \cdot P_l = \alpha_i + h_4(\alpha_i) \cdot pk'_{GW_l} + f_i \cdot Q_i$ holds. Therefore, the scheme can ensures both message integrity and authentication.

2) Identity Privacy Preserving: The real identity ID_i of vehicle V_i is hidden in $pid_{V_i} = Enc_{k_j}(ID_i + \varsigma_i, \varsigma_i)$, and the attacker can only decrypt pid_{V_i} to get the real identity ID_i of V_i by the secret key k_j of the private key generator of its domain. According to the security of symmetric encryption algorithm, the attacker cannot compute the true identity of the vehicle without k_ϵ. Therefore, the attacker cannot obtain the privacy about the identity of the vehicle from the messages sent by the vehicle.

3) Traceability and Identity Revocation: The PKG of each domain can recover the true identity ID_i of a malicious vehicle under its domain from the vehicle's pseudonym pid_{V_i}. Firstly, the gateway gets the vehicle's pseudonym pid_{V_i} from the VIM table via α_i in the message. pid_{V_i} is encrypted by the vehicle identity ID_i and random number ς_i to get $pid_{V_i} = Enc_{k_j}(ID_i + \varsigma_i, \varsigma_i)$, domain PKG_j can get ID_i by decrypting pid_{V_i} with domain private key k_j.

4) Replay Attack: The gateway and the vehicle can determine whether the messages $(m_i, pid_{V_i}, R_{V_i}, D_j, P_{pkg_j}, TS_i, R_i, Z_i)$ and $(m_i, TS_i, \alpha_i, Q_i, \beta_i)$ are expired by checking the timestamp TS_i of the received message, respectively. If the adversary modifies the timestamp TS_i to TS'_i which has not yet expired, the new message cannot pass the receiver verification because the adversary cannot recalculate the legitimate signature Z_i or β_i. Therefore, the attacker cannot replay the expired message.

5) Impersonation Attack: According to Theorem 1, the adversary cannot obtain the local group private key by sending a legitimate request to the gateway. To pretend to be a legitimate vehicle to send a valid message that passes the equality check $\beta_i \cdot P_l = \alpha_i + h_4(\alpha_i) \cdot pk'_{GW_l} + f_i \cdot Q_i$, they must possess a legitimate local group private key. But the adversary cannot send a legitimate request to get the local group private key through gateway authentication. Therefore, our scheme is resilient impersonation attacks.

6) Man-in-the-middle Attack: In the V2G phase, mutual authentication is performed between the vehicle and the gateway, ensuring that an adversary cannot successfully execute a man-in-the-middle attack. In the V2V phase, the receiver is required to authenticate each message. According to Theorem 1, an adversary is unable to modify or forge a legitimate message from an intercepted one. Therefore, the proposed scheme is resilient man-in-the-middle attacks.

TABLE I
BENCHMARK OF CRYPTOGRAPHIC OPERATIONS

Notations	Definitions	Cost
$\widetilde{sm}$	Scalar multiplication on G_1	1.651
$\widetilde{ep}$	Exponential on G_T	0.109
$\widetilde{bp}$	Pairing	0.699
$\widetilde{pa}$	Addition on G_1	0.007
$\widetilde{mtp}$	Map to G_1	3.141
sm	Scalar multiplication on G	0.248
sm'	Small scalar multiplication on G	0.011
pa	Point addition on G	0.001
h_q	Hash to Z_q	0.001

V. PERFORMANCE ANALYSIS

This section presents the experimental setup and related parameters, followed by an evaluation of the computational and communication overhead. The proposed scheme is compared with three representative schemes [19], [20], [22]. All experiments were conducted on a machine equipped with an Intel Core i7-7500 processor, 16 GB of RAM and running Ubuntu 18.04. Cryptographic operations were implemented in Python using the Charm-Crypto library (version 0.5). For scheme [22], the bilinear pairing $G_1 \times G_1 \rightarrow G_T$ was instantiated over a Type-I pairing-friendly elliptic curve with an embedding degree of 2 and a base field size of 512 bits. The proposed scheme and [19], [20] employ a prime-order elliptic curve $E : y^2 = x^3 + ax + b$ with a base field of 192 bits and achieves 80-bit security level with the underlying group having a 160 bits prime order. The benchmark time of cryptographic operations involved in these schemes was recorded over 100 independent trials and can be found in Table I.

A. Computation Cost

In the V2G authentication phase, the vehicle signs the message and verifies the information returned by the gateway to obtain the local group private key, which will perform 4 scalar multiplications, 1 point addition and 3 hash operations, i.e., $4sm + pa + 3h_q \approx 0.996$(ms), the gateway verifies the message signature and generates the local group private key for it to perform 6 scalar multiplications, 3 point additions and 5 hash operations, i.e., $6sm+3pa+5h_q \approx 1.496$(ms). Since V2G authentication is executed only once within a given period, and multiple message signatures can be executed afterward using the obtained temporary private key, the computational overhead of the V2V phase mainly lies in message authentication.

TABLE II
COMPUTATIONAL COMPARISON

Schemes	Signing	Verification	Batch Verification
Zhu *et al.* [19]	$2sm + 2h_q$	$7sm + 7pa + 6h_q$	-
Zhong *et al.* [20]	$4sm + 2h_q$	$3sm + 2pa + h_q$	$(n + 2)sm + 3npa + 2h_q$
Liu *et al.* [22]	$\widetilde{sm}$	$2\widetilde{bp} + \widetilde{mtp}$	$n\widetilde{pa} + n\widetilde{mtp} + n\widetilde{bp}$
Ours	$sm + h_q$	$3sm + 2pa + 2h_q$	$(n + 2) \cdot sm + n \cdot sm' + 2n \cdot pa + 2n \cdot h_q$

Therefore, the performance comparison primarily focuses on the message authentication phase.

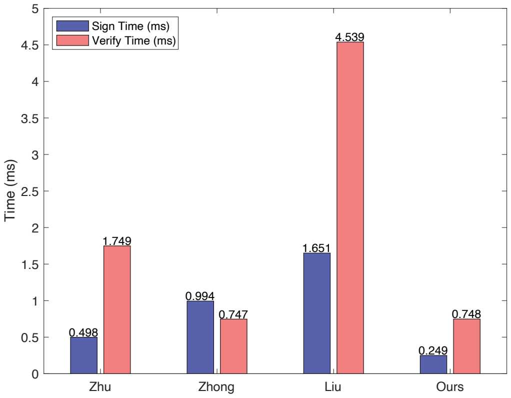

Fig. 2. Sign and verify time

Table II presents the main computational costs for the proposed scheme and the three comparison schemes during the the message authentication phase. In Zhu *et al.* [19], message signing consumes $2sm + 2h_q \approx 0.498$(ms), while verification requires $7sm + 7pa + 6h_q \approx 1.749$(ms). In Zhong *et al.* [20], signing requires $4sm + 2h_q \approx 0.994$(ms), and verification consumes $3sm + 2pa + h_q \approx 0.747$(ms). For batch verification of n messages, the cost is $(n + 2)sm + 3npa + 2h_q \approx 0.251n$(ms). In Liu *et al.* [22], the signature process consumes $\widetilde{sm} \approx 1.651$(ms), and verification consumes $2\widetilde{bp} + \widetilde{mtp} \approx 4.539$(ms). The batch verification cost for n messages is $n\widetilde{pa} + n\widetilde{mtp} + n\widetilde{bp} \approx 3.847n$(ms). The message signature in the proposed scheme requires $sm + h_q \approx 0.249$(ms), and verification takes $3sm + 2pa + 2h_q \approx 0.748$(ms). For batch verification of n messages, the cost is $(n+2) \cdot sm + n \cdot sm' + 2n \cdot pa + 2n \cdot h_q \approx 0.263n$(ms). As shown in Figure 2, the proposed scheme achieves the lowest computational overhead among all compared schemes.

B. Communication Cost

This section discusses the overhead during communication. Based on the two curves and their parameters introduced earlier, the element sizes in the relevant groups are as follows: elements in group G_1 and G_T are 64 bytes and 128 bytes respectively, elements in group G is 24 bytes, and elements in the large integer group Z_q^* are 20 bytes. Both the identity ID and pseudonym are represented by one element of Z_q^*, which is 20 bytes. And the size of the timestamp TS is 4 bytes.

During the V2G authentication phase, the vehicle sends a request message $(m_i, pid_{V_i}, R_{V_i}, D_j, P_{pkg_j}, TS_i, R_i, Z_i)$ to the gateway, which incurs a communication overhead of approximately $3|G| + 2|Z_q^*| + |TS| = 116$bytes. After successful authentication, the gateway replies with a local temporary private key information (msg, mac), which is about $|G| + 2|Z_q^*| = 64$ bytes. Since this phase is executed only once within a certain period, the communication overhead of the V2V message authentication phase is mainly compared. Table III shows the communication overhead of the proposed scheme and the other three schemes during the message authentication phase.

TABLE III
COMMUNICATION COST

Scheme	Cost
Zhu *et al.* [19]	$3|G| + 5|Z_q^*| + |TS|$
Zhong *et al.* [20]	$4|G| + |Z_q^*| + |TS|$
Liu *et al.* [22]	$2|G_1| + |TS|$
Ours	$2|G| + |Z_q^*| + |TS|$

In Zhu *et al.* [19], the size of the information exchanged between vehicles is approximately $3|G| + 5|Z_q^*| + |TS| = 176$ bytes. In Zhong *et al.* [20], the communication overhead is about $4|G| + |Z_q^*| + |TS| = 120$ bytes. For Liu *et al.* [22], the exchanged information is approximately $2|G_1| + |TS| = 132$ bytes. In contrast, the proposed scheme requires only $2|G| + |Z_q^*| + |TS| = 72$ bytes. From the comparison, it is evident that the V2V authentication communication overhead of the proposed scheme is significantly lower than the other schemes.

VI. CONCLUSION

In this paper, we proposed an efficient and anonymous cross-domain authentication scheme to meet the needs of data cross-domain transmission in the VANETs. By introducing edge gateways to manage local vehicle user groups and handle cross-domain event authentication and local group key distribution, we avoid the involvement of third-party trusted authorities, reducing authentication latency. To further reduce computational overhead, we design a batch authentication mechanism that significantly reduces authentication delay during large-scale authentication requests. Experimental analysis shows that the proposed scheme has significant advantages in the signing and verification phases compared to other schemes, making it suitable for practical cross-domain communication in VANETs. In the future, we plan to integrate blockchain technologies to design decentralized and tamper-resistant authentication protocols, and apply lightweight privacy-preserving techniques to enhance anonymity. Additionally, we aim to evaluate the proposed scheme under realistic vehicular mobility and network conditions through large-scale simulations or real-world applications.

VII. Acknowledgment

The work was supported in part by the National Natural Science Foundation of China under Grant U23A20308, Grant 62472003, Grant 62202008 and Grant 62302008, in part by the Natural Science Foundation of Anhui Province, China under Grant 2408085JX010 and in part by the University Synergy Innovation Program of Anhui Province under Grant GXXT-2022-049. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

References

[1] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong, "Dbcpa: Dual blockchain-assisted conditional privacy-preserving authentication framework and protocol for vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 23, no. 2, pp. 1127–1141, 2022.

[2] R. Li, J. Cui, J. Zhang, L. Wei, H. Zhong, and D. He, "Blockchain-assisted revocable cross-domain authentication for vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, 2025.

[3] Y. Lin, X. Wang, Q. Gan, and M. Yao, "A secure cross-domain authentication scheme with perfect forward security and complete anonymity in fog computing," *Journal of Information Security and Applications*, vol. 63, p. 103022, 2021.

[4] J. Sun, G. Xu, T. Zhang, X. Cheng, X. Han, and M. Tang, "Secure data sharing with flexible cross-domain authorization in autonomous vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7527–7540, 2022.

[5] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[6] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A blockchain-based multidomain authentication scheme for conditional privacy preserving in vehicular ad-hoc network," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8078–8090, 2021.

[7] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K.-K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5g-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, 2021.

[8] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in vanets-an efficient and privacy-preserving cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[9] H. J. Jo, I. S. Kim, and D. H. Lee, "Reliable cooperative authentication for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 4, pp. 1065–1079, 2017.

[10] S. Haider, D. Gao, R. Ali, A. Hussain, and M. T. Ikram, "A privacy conserves pseudonym acquisition scheme in vehicular communication systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 15 536–15 545, 2022.

[11] Y. Yang, L. Zhang, Y. Zhao, K.-K. R. Choo, and Y. Zhang, "Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based vanet," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 317–331, 2022.

[12] X. Li, Y. Liu, and X. Yin, "An anonymous conditional privacy-preserving authentication scheme for vanets," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 2019, pp. 1763–1770.

[13] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2019.

[14] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in vanets," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1681–1695, 2020.

[15] M. Ma, S. Wang, and Y. Li, "A model based on multiple intermediate entity for cross-domain authentication in public key infrastructure and blockchain system," in *2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT)*. IEEE, 2022, pp. 446–453.

[16] 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 Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[17] K. Mahmood, S. Shamshad, M. A. Saleem, R. Kharel, A. K. Das, S. Shetty, and J. J. Rodrigues, "Blockchain and puf-based secure key establishment protocol for cross-domain digital twins in industrial internet of things architecture," *Journal of Advanced Research*, vol. 62, pp. 155–163, 2024.

[18] X. Liu, L. Wang, L. Li, X. Zhang, and S. Niu, "A certificateless anonymous cross-domain authentication scheme assisted by blockchain for internet of vehicles," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 3488977, 2022.

[19] Y. Zhu, Y. Zhou, J. Wang, B. Yang, and M. Zhang, "A lightweight cross-domain direct identity authentication protocol for vanets," *IEEE Internet of Things Journal*, 2024.

[20] Q. Zhong, X. Zhao, Y. Xia, and X. Liu, "Cd-basa: An efficient cross-domain batch authentication scheme based on blockchain with accumulator for vanets," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[21] M. Seifelnasr, R. AlTawy, and A. Youssef, "A conditional privacy-preserving protocol for cross-domain communications in vanet," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[22] G. Liu, H. Lu, W. Wang, Z. Liu, and H. Huang, "A cross-domain authentication scheme for vehicular networks based on mobile edge computing," *IEEE Internet of Things Journal*, 2025.