An Adaptive Authentication Protocol for Internet of Vehicles Based on Vehicle Density

Hao Peng[1], Zisang Xu[1(✉)], Ruirui Zhang[1], and Jianbo Xu[2]

[1] School of Computer and Communication Engineer, Changsha University of Science and Technology, Changsha, China
shirleyfe911@163.com, xzsszx111@csust.edu.cn, zrr@stu.csust.edu.cn
[2] School of Computer science and Engineering, Hunan University of Science and Technology, Xiangtan, China
jbxu@hnust.edu.cn

Abstract. With the influx of a large number of vehicles into the coverage area of the Roadside Unit (RSU), the increase in vehicle density makes it difficult for single vehicle authentication protocol to complete vehicle authentication quickly, resulting in authentication delays. In a low-density vehicle environment, batch authentication is usually inefficient and poses certain security risks. Aiming at the balance between security and efficiency, an adaptive authentication protocol for Internet of Vehicles based on vehicle density is proposed. According to the change of vehicle density near RSUs, batch authentication protocol or single vehicle authentication protocol is adaptively selected to improve authentication efficiency. The results of security and performance analysis show that compared to existing protocols, the proposed protocol either meets more security attributes such as conditional anonymity and resist tampering attacks, or has better performance in terms of computation and communication costs.

Keywords: Batch authentication · Internet of Vehicles · Security · ECC · Small exponent test

1 Introduction

The Internet of Vehicles (IoV) is a self-organizing and self-configuring network formed by vehicles utilizing wireless communication technology to communicate with other vehicles and RSUs through On-Board-Unit (OBU) [11]. Vehicles use Dedicated Short Range Communication (DSRC) or cellular communication technology to communicate with surrounding vehicles (V2V) and roadside traffic infrastructure (V2I) [14].

J. Xu—This work is supported in part by the National Natural Science Foundation of China under Grants 61872138.

H. Duan et al. (Eds.): SecureComm 2023, LNICST 567, pp. 187–204, 2025.
https://doi.org/10.1007/978-3-031-64948-6_10

The emergence of the IoV enables drivers to obtain real-time traffic information, reduces traffic accidents, and ensures travel safety. Due to the wireless communication method in the IoV, attackers can obtain the driver's identity information by monitoring and forging communication data, posing a huge threat to the safety of users' lives and property [2]. Anonymous identity authentication technology is an access control technology for both network communication parties to authenticate real identities. Designing an authentication protocol based on this technology ensures the security of communication in the IoV [9].

Although researchers have proposed various types of identity authentication protocols to address security issues in the IoV, most existing authentication protocols still have the following shortcomings. First, there is an authentication efficiency problem in single vehicle authentication protocol. While single vehicle authentication protocol is usually more efficient in a low-density vehicle environment, as vehicle density increases, the computational or communication bottlenecks that occur at the RSU will significantly reduce the authentication efficiency of these protocols. Second, there are security risks in batch authentication protocol. Most batch authentication protocols are implemented using verification equivalence or bilinear pairing, but these two methods are vulnerable to tampering attacks during the authentication process [1]. In a word, many protocols do not comprehensively consider the advantages and disadvantages of batch authentication and single vehicle authentication in different vehicle density environments, and cannot adaptively select single vehicle authentication or batch authentication to improve authentication efficiency.

Therefore, this paper designs an adaptive authentication protocol for the IoV based on vehicle density to solve the above problems. Especially, the main contributions of this paper can be summarized as follows:

- We proposed an adaptive authentication protocol. According to the density of vehicle, RSU can adaptively select single vehicle authentication protocol or batch authentication protocol to improve the authentication efficiency.
- We use small exponent testing technology to design a batch authentication protocol, which reduces the probability of the protocol being tampered with to 2^{-L} and greatly reduces the security risk of the authentication process.
- Finally, the proposed protocol does not require real-time involvement of the Trusted Authority (TA), reducing the possibility of computational bottlenecks for the TA. Additionally, batch authentication protocol does not require the selection of proxy vehicles to integrate messages.

The remaining part of this paper is outlined as follows. Section 2 discusses the related works. Section 3 introduces the related preliminaries. Section 4 defines the system model. Section 5 introduces the details of the proposed protocol. Section 6 is the security analysis of the protocol. Section 7 evaluates the performance of the protocol and determines the vehicle density threshold, followed by the conclusions made in Sect. 8.

2 Related Works

To ensure data privacy and security in vehicular networks, various message authentication protocols have been proposed. Wazid et al. [18] proposed a key agreement protocol for vehicular networks where vehicles communicate with other vehicles and RSUs through cluster heads. This protocol provides traceability, anonymity, and privacy preservation. However, it is vulnerable to impersonation attacks on vehicles, fog servers and RSUs. Cui et al. [5] proposed a message authentication scheme for Vehicular Ad-hoc Networks (VANETs) that combines edge computing. Although this scheme addresses the issues of redundant authentication and failure to identify invalid messages, the adopted collaborative authentication approach easily leads to significant delays. Ma et al. [12] proposed a secure and efficient authentication protocol for fog-based VANETs. However, they use cloud servers instead of fog nodes for vehicle authentication, resulting in unavoidable latency between edge nodes and servers. Zhang et al. [23] proposed a novel 5G-based vehicular networks authentication protocol. This protocol no longer requires RSU involvement and instead establishes a secure communication channel between ordinary vehicles and edge computing vehicles (ECVs). However, the dynamic addition of vehicles imposes a significant burden on the TA. Although the above protocols effectively address security issues in the IoV, the computational bottleneck caused by the large volume of message authentication in high-density vehicle environments leads to low authentication efficiency in the RSU.

In order to address these issues, batch authentication protocols and proxy vehicle-based authentication protocols have emerged. Liu et al. [10] proposed a hybrid proxy-based authentication scheme (HPBS) that reduces the computational burden on RSUs by introducing proxy vehicles. However, this scheme involves a significant number of certificates and signatures, leading to high communication and computation costs. Thumbur et al. [15] proposed a new certificateless aggregate signature based authentication protocol for VANETs. This protocol aggregates a variety of personal signatures from different vehicles as a signature, thereby reducing the authentication time, storage space, and computational cost of the RSU. Ferng et al. [7] proposed a dynamic batch authentication scheme, in which the number of messages waiting for authentication can be dynamically adjusted based on the results of the previous authentication to improve the authentication efficiency of the RSU. Vijayakumar et al. [16] proposed a batch authentication protocol for 6G-enabled VANETs. While their protocol reduces the computational burden on RSUs in congested areas, the authentication efficiency remains relatively low. Yang and Zhang [20,25] proposed a protocol to implement V2I secure communication using bilinear pairing. These protocols improve the efficiency of authentication by adopting batch authentication of messages, but the bilinear pairing operations impose a significant computational overhead on RSUs. Zhang et al. [26] proposed a new batch anonymous authentication scheme that utilizes ECC algorithm and distributed digital signatures to relieve the burden of the trusted center. Zhang and Yang [21,22] proposed conditional privacy-preserving batch authentication schemes.

These schemes achieve a more efficient authentication process by not involving bilinear pairing operations and map-to-point hash operations. Furthermore, these schemes are capable of effectively tracking illegal vehicles.

3 Preliminaries

3.1 Small Exponent Test

In 1998, Mihir [4] was the first to propose and prove the small exponent test. Generally, there are two verification methods for verifying multiple equations $a_i = b_i P$, where $i = 1, 2, \ldots, n$:

- Verify one by one.
- Equivalence verification of polynomials $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i P$.

However, the equivalence verification has the following situation: assuming (a_1, b_1) and (a_2, b_2) are two sets of data that can be verified one by one, it is easy to construct another two sets of data $(a_1 + f, b_1)$ and $(a_2 - f, b_2)$, which can pass the equivalence verification but cannot be verified one by one. The small exponent test is an effective approach to reduce the occurrence probability of this situation.

Small exponent test [27]: By selecting a number ω_i with a length of l bits and incorporating it into the equivalence verification of polynomials, such as $\sum_{i=1}^{n} \omega_i a_i = \sum_{i=1}^{n} \omega_i b_i P$, then the probability of the above situation will be as low as 2^{-l}.

3.2 Elliptic Curve Cryptosystem

Let p, q be large prime numbers. An elliptic curve $E_p(a, b)$ is defined by the equation $y^2 = x^3 + ax + b \pmod{p}$, where $a, b \in F_p$ and $\triangle = 4a^3 + 27b^2 \pmod{p} \neq 0$. Given the point $P \in E_p(a, b)$. Scalar multiplication is defined as $n \cdot P = P + P + \cdots + P$ (n times), where $n \in F_p$.

- Elliptic curve discrete logarithm problem (ECDLP) [8]: Given two points $P, Q \in E_p(a, b)$, where $Q = s \cdot P$, it is difficult to compute s in polynomial time.
- Elliptic curve computational Diffie-Hellman problem (ECCDHP): Given three points $Q, a \cdot Q$ and $b \cdot Q \in E_p(a, b)$, it is difficult to compute $ab \cdot Q$ in polynomial time.

3.3 Bilinear Pairing

Suppose G_1 is an additive cyclic group whose order is a prime number q, G_2 is a multiplicative cyclic group whose order is a prime number q, and the bilinear pair $e : G_1 \times G_1 \rightarrow G_2$ satisfies the following properties.

- Bilinearity: For all $P, Q \in G_1$, it is satisfied that $e(aP, bQ) = e(P, Q)^{ab}$, where $a, b \in Z_q^*$.
- Non-degeneracy: $e(P, Q) \neq 1$.
- Computability: The map e can be computed efficiently.

4 System Model

4.1 Network Model

As shown in Fig. 1, the network model defined in our protocol consists of the following three main entities:

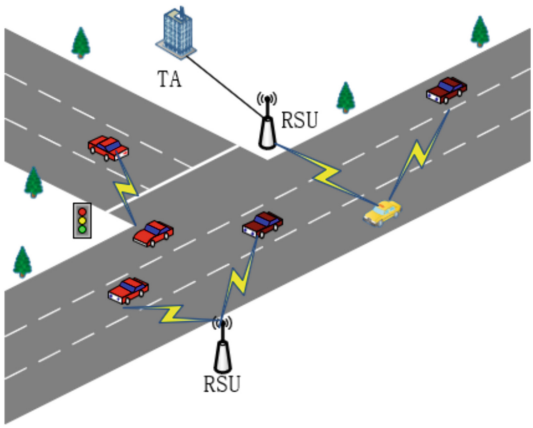

Fig. 1. The network model used in our protocol

- TA: As a fully trusted entity in the system, TA is responsible for the registration of vehicles and RSUs, and it can also track the real identity of vehicles.
- RSU: As an infrastructure installed on either sides of the road, RSU is equipped with a built-in Tamper-Resistant Device (TPD), whose main task is to ensure the integrity of vehicle messages and verify the authenticity of vehicle identities.
- Vehicles: In the IoV, each vehicle can communicate with the RSU or other vehicles through the equipped device OBU to obtain the corresponding service.

4.2 Threat Model

The threat model used in this article is based on the widely used Dolev-Yao (DY) model [6], which is defined as follows:

- The attacker can eavesdrop on the messages transmitted by each entity over the wireless channel, modify or replay the eavesdropped messages, or deliver false messages to the communicating entities [19].
- The attacker can obtain the information stored in the vehicle's memory by capturing the vehicle.
- All authentication data in RSU is stored in TPD, which means that even if an attacker captures RSU, he cannot get any information from it.

Table 1. Notations and definitions used

Notation	Definition
ID_i	Identity of V_i
PID_i	Pseudo identity of V_i
k_{TA}, x_i, y_j	Private key of TA, V_i and RSU_j
P_{pub}, X_i, Y_j	Public key of TA, V_i and RSU_j
t_1, t_2	Timestamps
K_s	Session key
a, b	Auxiliary parameters of V_i
n_1, n_2, n_3	Random numbers
ξ_i	The signature issued by V_i
M_i	The message sent by V_i
$H(\cdot)$	One-way hash function
$\oplus$	Exclusive or operation
$\|\|$	Concatenation operation

5 The Proposed Protocol

In this section, the details of an adaptive authentication protocol based on vehicle density are presented, including system initialization, registration phase, single vehicle authentication phase, batch authentication phase. The level of vehicle density is defined by the density threshold τ. The notations used in the proposed protocol are defined in Table 1.

5.1 System Initialization

TA performs the following steps to initialize system parameters:

Step I1. Given an elliptic curve E of order q, P is the generator of E, and q is a large prime number. TA chooses an additive cyclic group G_1 whose order is q, Q is a generator of G_1. Get a bilinear pairing $e : G_1 \times G_1 \rightarrow G_T$.

Step I2. TA chooses a random number $k_{TA} \in Z_q^*$, and then computes $P_{pub} = k_{TA} \cdot P$, where P_{pub} and k_{TA} represent the public key and private key of the system, respectively.

Step I3. TA selects a secure hash function $H{:}\{0,1\}^* \rightarrow Z_q^*$, and publishes system parameters $\{E, q, Z_q^*, P, Q, H, P_{pub}\}$.

5.2 Registration Phase

Vehicle Registration

Step V1. TA generates a unique permanent identity ID_i for the vehicle, then generates three unique random numbers x_i, a, b, and computes $A = a \cdot P$, $B = b \cdot P$, $X_i = x_i \cdot P$, where $\{a, b\}$ and $\{x_i, X_i\}$ respectively represent the auxiliary authentication parameters and the public-private key pair of the vehicle.

Step V2. TA sends parameters $\{ID_i, a, b, x_i\}$ to the vehicle, the vehicle stores the parameters $\{ID_i, a, b, x_i\}$ in the vehicle OBU and publishes parameters $\{A, B, X_i\}$.

RSU Registration

Step R1. TA generates a unique random numbers y_j, and computes $Y_j = y_j \cdot P$, $\{y_j, Y_j\}$ as RSU public and private keys.

Step R2. TA exposes the parameter $\{Y_j\}$ and sends the parameter $\{y_j\}$ to the RSU, which is stored in the TPD by the RSU.

5.3 Single Vehicle Authentication Phase

The vehicle and the RSU perform the following operations separately to achieve mutual authentication and ultimately negotiate the session secret key. Figure 2 provides a detailed view of the entire interaction process.

Step S1. V_i generates random numbers n_1, n_2. Let t_1 denote the timestamp. V_i computes $PID_i = H(x_i \cdot P_{pub}||n_1) \oplus ID_i$, $W_1 = H(PID_i||n_1||n_2||t_1||X_i)$, $Ver_1 = a \cdot W_1 + H(A||n_2||PID_i) \cdot b$, $W_2 = x_i \cdot Y_j \oplus (A||n_2||Ver_1)$, and sends $\{n_1, W_2, PID_i, t_1\}$ to RSU.

Step S2. RSU first checks t_1, then computes $A||n_2^*||Ver_1 = y_j \cdot X_i \oplus W_2$, $W_1^* = H(PID_i||n_1||n_2^*||t_1||X_i)$, and checks $Ver_1 \cdot P \stackrel{?}{=} A \cdot W_1 + H(A||n_2^*||PID_i) \cdot B$. If the equation is incorrect, RSU terminates the session. Otherwise, RSU generates random numbers n_3, c and timestamp t_2, then computes $C = c \cdot P$, $W_3 = H(A||n_2^*||t_2||C||n_3)$, $Ver_2 = c \cdot W_3 + y_j$, $W_4 = n_2^* \oplus (C||n_3||Ver_2)$ and sends $\{W_4, t_2\}$ to V_i.

Step S3. V_i checks the freshness of t_2, then computes $C||n_3||Ver_2 = W_4 \oplus n_2$, $W_3^* = H(A||n_2||t_2||C||n_3)$, and checks whether $Ver_2 \cdot P \stackrel{?}{=} C \cdot W_3 + Y_j$. If the equation is incorrect, V_i terminates the session. Otherwise, this session ends, the vehicle and RSU generate the same session key $K_s = H(n_2||n_3)$.

V_i		RSU_j
$< x_i, X_i, a, b >$		$< y_j, Y_j >$
Generates random numbers n_1,n_2.		
Generates timestamp t_1.		
Computes PID_i=$H(x_i \cdot P_{pub}\|\|n_1) \oplus ID_i$		
W_1=$H(PID_i\|\|n_1\|\|n_2\|\|t_1\|\|X_i)$		
Ver_1=$a \cdot W_1 + H(A\|\|n_2\|\|PID_i) \cdot b$		
W_2=$x_i \cdot Y_j \oplus (A\|\|n_2\|\|Ver_1)$		
	$\xrightarrow{(n_1, W_2, PID_i, t_1)}$	
		Checks validity of t_1.
		Computes $A\|\|n_2^*\|\|Ver_1 = y_j \cdot X_i \oplus W_2$
		$W_1^* = H(PID_i\|\|n_1\|\|n_2^*\|\|t_1\|\|X_i)$
		$Ver_1 \cdot P \stackrel{?}{=} A \cdot W_1 + H(A\|\|n_2^*\|\|PID_i) \cdot B$
		Generates random numbers n_3, c.
		Generates timestamp t_2.
		Computes $C = c \cdot P$
		$W_3 = H(A\|\|n_2^*\|\|t_2\|\|C\|\|n_3)$
		$Ver_2 = c \cdot W_3 + y_j$
		$W_4 = n_2^* \oplus (C\|\|n_3\|\|Ver_2)$
	$\xleftarrow{(W_4, t_2)}$	
Checks validity of t_2.		
Computes $C\|\|n_3\|\|Ver_2 = W_4 \oplus n_2$		
$W_3^* = H(A\|\|n_2\|\|t_2\|\|C\|\|n_3)$		
Check $Ver_2 \cdot P \stackrel{?}{=} C \cdot W_3^* + Y_j$		

Fig. 2. Single vehicle authentication

5.4 Batch Authentication Phase

If the RSU detects that the number of vehicles around it exceeds the threshold of vehicle density τ, it will automatically switch to batch authentication and broadcast a notification for vehicles to enter the batch authentication phase. Vehicles will perform the following actions to authenticate with RSU:

Step B1. The vehicle generates a random number n_i and computes $PID_i = ID_i \oplus H(x_i \cdot P_{pub}||n_i)$.

Step B2. The vehicle computes $K_i = (a \cdot H(PID_i||t_i||P_{pub}||M_i) + x_i) \cdot Q$, $S_i = K_i + b$, where t_i is a timestamp.

Step B3. The vehicle takes $\xi_i = (S_i, M_i)$ as a signature to message M_i and sends (ξ_i, n_i, PID_i, t_i) to the RSU.

After receiving message (ξ_i, n_i, PID_i, t_i), the RSU will first checks the freshness of t_i. If the timestamp of a message exceeds the valid time, it will be

discarded. After receiving the number of qualified messages exceeding n, RSU completes the authentication by performing the following operations:

Step B4. The RSU receives the message $\{A_i, B_i, X_i\}$ broadcast by n signed vehicles, and then computes $h_1^i = H(PID_i||t_i||P_{pub}||M_i)$, and selects n vectors $\{V_1, V_2, \cdots, V_n\}$ for n batches of signed messages to be verified, where $V_i \in [1, 2^t]$, t is a small integer.

Step B5. RSU verifies whether the equation

$$e(\sum_{i=1}^{n} V_i(X_i + A_i h_1^i), Q)e(\sum_{i=1}^{n} V_i B_i, 1) \stackrel{?}{=} e(\sum_{i=1}^{n} V_i S_i, P) \tag{1}$$

is true, and if so, accepts the signature.

The following is the correctness verification of Eq. (1):

$$\begin{aligned}
H &= e(\sum_{i=1}^{n} V_i(X_i + A_i h_1^i), Q)e(\sum_{i=1}^{n} V_i B_i, 1) \\
&= e(\sum_{i=1}^{n} V_i(x_i + a_i h_1^i)P, Q)e(\sum_{i=1}^{n} V_i b_i P, 1) \\
&= e(\sum_{i=1}^{n} V_i(x_i + a_i h_1^i)P, Q)^{Q\frac{1}{Q}} e(\sum_{i=1}^{n} V_i b_i P, 1) \\
&= e(\sum_{i=1}^{n} V_i(x_i + a_i h_1^i)PQ, 1)e(\sum_{i=1}^{n} V_i b_i P, 1) \\
&= e(\sum_{i=1}^{n} V_i(K_i + b_i)P, 1) \\
&= e(\sum_{i=1}^{n} V_i S_i P, 1) \\
&= e(\sum_{i=1}^{n} V_i S_i, P)
\end{aligned} \tag{2}$$

6 Security Analysis

6.1 Formal Security Analysis

In this part, we will analyze the security of the session key generated by single vehicle authentication protocol using the Real-or-Random (ROR) model, which is widely used to prove the security of session keys for various protocols. The single vehicle authentication protocol defines three participants: V, RSU, TA, and their entities can all be collectively represented as I^t. Here, we use V_i, R_j, TA_k to refer to instances i, j, and k of V, RSU, and TA, respectively. For the adversary $\mathcal{A}$, it can perform the following operations for querying:

- $Execute(V_i, R_j, TA_k)$: This operation simulates an eavesdropping attack, through which the adversary can obtain all the information exchanged during the entire protocol execution.
- $Reveal(I^t)$: $\mathcal{A}$ can query the session secret key of the current session through this operation.
- $Send(V_i, R_j, m)$: Through this operation, $\mathcal{A}$ can send a message m to R_j to make an inquiry. Based on the correctness of message m, R_j will provide feedback or abort the request.
- $Test(I^t)$: If $\mathcal{A}$ asks the query, I^t will randomly select a random number $d \in \{0, 1\}$. If $d \neq 1$, instance I^t will return a random number with the same length as the session key, otherwise return the real session key to $\mathcal{A}$.

Theorem 1. *Let's assume that $\mathcal{A}$ is an adversary in the ROR model with a polynomial running time of t. The advantage $Adv(\mathcal{A})$ of adversary $\mathcal{A}$ obtaining the session key and breaking the semantic security of the protocol is negligible.*

$$Adv(\mathcal{A}) \leq \frac{q_h^2}{2^{l_s+1}} + \frac{(q_s + q_e)^2}{2(q-1)} + \frac{(3q_h + q_s)}{2^{l_s}}$$

Among them, l_s, q_s, q_e, and q_h respectively represent the length of the hash function output value, the number of times to execute the Send request, the number of times to execute the Execute request, and the number of times to execute the hash query. $q > 2^k$, k is a security parameter.

Proof. This chapter defines four games, namely $G_i (i = 0, 1, 2, 3)$. Suppose Suc_i represents the event in game G_i where A successfully guesses bit d. The following are the specific descriptions of each game:

- G_0: In G_0, $\mathcal{A}$ launches an attack by utilizing a random oracle and outputs the value of d. Therefore, we derive the result.

$$Adv(\mathcal{A}) = |2Pr[suc_0] - 1| \tag{3}$$

- G_1: In G_1, $\mathcal{A}$ implements an eavesdropping attack by initiating the hash query and the Execute query, and finally verifies whether the returned Test request result is a real session key or a random number. Due to the fact that the session key is calculated using random numbers generated between RSU and the vehicle, $\mathcal{A}$ cannot calculate the session key through these queries. Therefore, we derive the following result.

$$Pr[suc_1] = Pr[suc_0] \tag{4}$$

- G_2: This game simulates all random number collisions and hash collisions in the authentication phase. According to the birthday paradox, hash collisions probability is $\frac{q_h^2}{2^{l_s+1}}$, and random number collisions probability in this protocol is $\frac{(q_s+q_e)^2}{2(q-1)}$. So we derive the result.

$$|Pr[suc_2] - Pr[suc_1]| \leq \frac{q_h^2}{2^{l_s+1}} + \frac{(q_s + q_e)^2}{2(q-1)} \tag{5}$$

- G_3: This game simulates the probability of $\mathcal{A}$ successfully forging the communication message between V and RSU without a random oracle. $L_{\mathcal{A}}$ is a record list that stores $\mathcal{A}$'s hash query, and L_P stores a list of messages transmitted between V and RSU during the authentication phase. In this protocol, the simulator needs to verify $(*\cdot P_{pub}||*)$, $(PID_i||*||*||t_1||X_i, W_1)$, $(A||*||PID_i, Ver_1)$, $(A||*||t_2||C||*, W_3) \in L_{\mathcal{A}}$ and all messages that belong to L_P. If any of the above verifications fail, the entire request will be terminated. In this protocol, the probability of successfully forging $(*\cdot P_{pub}||*)$, $(PID_i||*||*||t_1||X_i, W_1)$, $(A||*||t_2||C||*, W_3)$ is $\frac{q_h}{2^{l_s}}$, the probability of successfully forging $(A||*||PID_i, Ver_1)$ is $\frac{q_s}{2^{l_s}}$. So we derive the following result.

$$|Pr[suc_3] - Pr[suc_2]| \leq \frac{(3q_h + q_s)}{2^{l_s}} \tag{6}$$

The attacker performs the Test query to guess bit d. The result we obtained is as follows.

$$Pr[suc_3] = \frac{1}{2} \tag{7}$$

According to (3), (4) and (7), the following result can be obtained.

$$\begin{aligned} \frac{1}{2}Adv(\mathcal{A}) &= |Pr[suc_0] - \frac{1}{2}| \\ &= |Pr[suc_1] - \frac{1}{2}| \\ &= |Pr[suc_1] - Pr[suc_3]| \end{aligned} \tag{8}$$

According to (5), (6) and (8), the following result can be obtained.

$$\begin{aligned} Adv(\mathcal{A}) &= 2|Pr[suc_1] - Pr[suc_3]| \\ &\leq 2|Pr[suc_1] - Pr[suc_2]| + 2|Pr[suc_2] - Pr[suc_3]| \\ &\leq \frac{q_h^2}{2^{l_s+1}} + \frac{(q_s + q_e)^2}{2(q-1)} + \frac{(3q_h + q_s)}{2^{l_s}} \end{aligned} \tag{9}$$

6.2 Informal Security Analysis

We will informally analyze the proposed authentication protocol in this subsection and compare the protocol features of our proposed protocol with existing protocols [3,13,16,17,27]. Table 2 clearly show that our protocol has lower security risks.

Eavesdropping Attack
The attacker can capture all communication information between the vehicle and RSU on the public channel, which means the attacker can obtain (W_4, t_2) and (n_1, W_2, PID_i, t_1). The vehicle's real identity ID_i is hidden within the pseudonymous identity PID_i, and the attacker cannot obtain it through the eavesdropped message. Due to the ECCDLP, the attacker cannot obtain the vehicle's real identity ID_i through the pseudonymous identity PID_i, nor can they obtain the

random number n_2 and n_3 through W_2 and W_4, so the session secret key is safe. Therefore, our protocol can resist eavesdropping attack.

Vehicle Impersonation Attack
In single authentication protocol, the attacker executes an impersonation attack by creating a valid tuple (n_1, W_2, PID_i, t_1), where $W_2 = x_i \cdot Y_j \oplus (A||n_2||Ver_1)$. W_2 is composed of the vehicle's private key, and due to the ECCDLP, the attacker cannot obtain the parameters A, n_2, and Ver_1 included in W_2. Even if the vehicle's key x_i is compromised, the attacker cannot obtain the values a and b generated by TA during the initialization stage, so the attacker cannot forge a valid Ver_1 to pass the subsequent RSU authentication. Therefore, our protocol can resist vehicle impersonation attack.

Conditional Anonymity
In our protocol, the vehicle's real identity is not transmitted over the public channel and is hidden in pseudonymous identity that changes every round. The vehicle use the generated PID_i to request services for each communication, where $PID_i = H(x_i \cdot P_{pub}||n_1) \oplus ID_i$. Furthermore, only TA has the capability to trace vehicles by calculating $ID_i = H(X_i \cdot k_{TA}||n_1) \oplus PID_i$, where k_{TA} represents the system's master private key.

Replay Attack
The protocol we designed uses the timestamp mechanism to resist replay attacks. When the vehicle sends an authentication message, the RSU will first verify the timestamp. If the timestamp is outdated, the authentication message will be discarded directly to ensure the security and stability of the system.

Man-in-the-Middle Attack
Through the previous analysis of vehicle impersonation attack, it has been demonstrated that attackers are unable to impersonate the vehicle to communicate with the RSU. When the attacker wants to generate a valid (W_4, t_2) to impersonate the RSU, since the random number n_2 generated by the vehicle cannot be obtained, it is difficult to pass the vehicle's authentication by forging a valid W_4. Therefore, it is clear that our protocol can resist the man-in-the-middle attack.

Vehicle Capture Attack
Even if the attacker captures the vehicle, he cannot get TA's private key k_{TA}. Due to the session key being composed of different random numbers each round, attackers cannot decipher the previous session. In addition, due to the different private keys of different vehicles, even if a vehicle is captured, it will not affect other vehicles. Therefore, our protocol can resist vehicle capture attack.

Tampering Attack
To ensure the tamper resistance of batch authentication signatures, we have adopt the small exponent test technique to quickly detect any modifications to a batch of signatures. Even if attackers obtain a large number of legitimate signatures through eavesdropping, they still cannot construct two sets of

(ξ_i, n_i, PID_i, t_i) values to pass batch authentication. Therefore, our protocol can resist tampering attack.

7 Performance Analysis and Determination of Vehicle Density Threshold

7.1 Computation Cost Analysis

To ensure a fair comparison, we use the same execution time as in [24], which is obtained by performing simulation experiments using MIRACL library on a machine equipped with an Intel I7-4770 processor and 4.00 GB RAM. The cryptographic operations in the single vehicle authentication protocol are mainly based on ECC, including $(7n)T_h$, $(10n)T_{e.m}$, and $(3n)T_{e.a}$. Thus, the total computation cost is $(10n)T_{e.m} + (3n)T_{e.a} + (7n)T_h \approx 4.4261n$ ms. The cryptographic operations in batch authentication are mainly based on bilinear pairing, including $3T_{bp}$, $(n)T_{bp.m}$, $(3n)T_{bp.sm}$, $(n)T_{bp.a}$. Thus, the total computation cost is $3T_{bp} + (n)T_{bp.m} + (3n)T_{bp.sm} + (n)T_{bp.a} \approx 1.8766n + 12.633$ ms. Table 3 lists the execution times of the cryptographic operations used in this protocol. Table 4

Table 2. Protocol features comparison

Protocol features	[17]	[3]	[13]	[16]	[27]	Our
Resist eavesdropping attack	✓	✓	✓	✓	✓	✓
Resist vehicle impersonation attack	✓	✓	✓	✓	✓	✓
Conditional anonymity	✓	×	✓	×	×	✓
Resist replay attack	✓	✓	✓	✓	✓	✓
Resist man-in-the-middle attack	✓	✓	✓	✓	✓	✓
Resist vehicle capture attack	✓	×	×	✓	✓	✓
Resist tampering attack	×	×	×	×	✓	✓
No need TA real-time participation	×	✓	×	✓	×	✓

"✓" indicates the protocol meets the protocol features while "×" indicates the opposite.

Table 3. Execution time of cryptographic operations

Notation	Description	Time (milliseconds)
T_{bp}	Bilinear pairing.	4.2110
$T_{bp.m}$	Scale multiplication on bilinear pairing	1.7090
$T_{bp.sm}$	Small scale multiplication on bilinear pairing.	0.0535
$T_{bp.a}$	Point addition on bilinear pairing.	0.0071
$T_{e.m}$	Scale multiplication on ECC.	0.4420
$T_{e.sm}$	Small scale multiplication on ECC.	0.0138
$T_{e.a}$	Point addition on ECC.	0.0018
T_h	Hash function.	0.0001

shows the computation cost of our designed protocol with existing protocols [3,13,16,17,27] in terms of batch authentication. Figure 3 will present a more intuitive comparison of the computation cost. Table 2 and Table 4 demonstrate that the proposed protocol either meets more protocol features or has lower computation costs. It is worth mentioning that, since the protocol [27] assumes the existence of a secure channel between RSU and TA, it eliminates the need for additional cryptographic tools to ensure vehicle anonymity and confidentiality of some secret parameters. Otherwise, their protocol would require higher computational and communication costs.

Table 4. Comparison on computation cost of various protocols

Protocol	Verify one message	Verify n messages (n $> \tau$)
Wang et al. [17]	$T_{bp} + 2T_{bp.m}$ $\approx$7.629 ms	$(n)T_{bp} + (2n)T_{bp.m}$ $\approx 7.629n$ ms
Bagga et al. [3]	$3T_{bp} + 5T_{bp.m} + 4T_{bp.a}$ $+3T_h \approx 21.2067$ ms	$3T_{bp} + (5n)T_{bp.m} + (3n+1)T_{bp.a}$ $+(2n+1)T_h \approx 8.5665n + 12.6402$ ms
Mei et al. [13]	$4T_{bp} + 2T_{bp.m}$ $\approx$20.262 ms	$4T_{bp} + (2n)T_{bp.m}$ $\approx 3.418n + 16.844$ ms
Vijayakumar et al. [16]	$T_{bp} + T_{bp.m}$ $\approx$5.920 ms	$(n)T_{bp} + (n)T_{bp.m}$ $\approx 5.920n$ ms
Zhang et al. [27]	$5T_{e.m} + 1T_{e.a} + 8T_h$ $\approx$2.210 ms	$(3n)T_{e.sm} + (n+4)T_{e.m} + (2n+6)T_h$ $\approx 0.4834n + 1.7681$ ms
Our protocol	$6T_{e.m} + 2T_{e.a} + 3T_h$ $\approx$2.6559 ms	$3T_{bp} + (n)T_{bp.m} + (n)T_{bp.a}$ $+(3n)T_{bp.sm} \approx 1.8766n + 12.633$ ms

7.2 Communication Cost Analysis

In this subsection, we compare the communication cost of four existing protocols [3,13,16,17,27] for the IoV. We assume the sizes of p and $\bar{p}$ to be 20 and 64 bytes respectively, with the timestamp size of 4 bytes, random number size of 20 bytes, and hash function output size of 20 bytes. Therefore, the sizes of these elements in G and G_1 are 40 and 128 bytes respectively.

We will calculate the communication costs required for the authentication process in the proposed protocol for both single vehicle authentication and batch authentication. In single vehicle authentication protocol, the vehicle broadcasts the message $\{n_1, W_2, PID_i, t_1\}$, the RSU broadcasts the message $\{W_4, t_2\}$, where $W_2 = x_i \cdot Y_j \oplus (A||n_2||Ver_1)$, $W_4 = n_2^* \oplus (C||n_3||Ver_2)$, $\{Ver_1, A, C, Ver_2\} \in G$, PID_i is the hash function's output, n_1 is a random number and $\{t_1, t_2\}$ is a timestamp. So the total communication cost is $40 \times 4 + 20 \times 2 + 4 \times 2 = 208$ bytes. In batch authentication protocol, the vehicle broadcasts the message $\{\xi_i, n_i, PID_i, t_i\}$, where $\xi_i = (S_i, M_i) \in G_1$, PID_i is the hash function's output, n_i is a random number and t_i is a timestamp. So the total communication cost

is $128 + 20 \times 2 + 4 = 172$ bytes. Table 5 shows the communication cost of our protocol and existing protocols for batch authentication. Figure 4 will present a more intuitive comparison of the communication cost.

Table 5. Comparison on communication cost of various protocols

Protocol	Sending one message	Sending n messages (n > τ)
Wang et al. [17]	424 bytes	424n bytes
Bagga et al. [3]	324 bytes	324n bytes
Mei et al. [13]	648 bytes	648n bytes
Vijayakumar et al. [16]	276 bytes	276n bytes
Zhang et al. [27]	436 bytes	124n+312 bytes
Our protocol	208 bytes	172n bytes

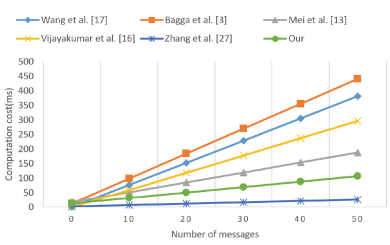

Fig. 3. Comparison of computation cost

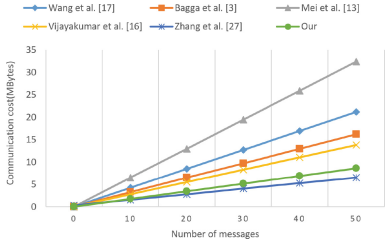

Fig. 4. Comparison of communication cost

7.3 Determination of Vehicle Density Threshold

The vehicle density threshold τ will change in different experimental environments, and τ is obtained by calculating the intersection point of RSU computation costs between single vehicle authentication and batch authentication. According to the experimental environment defined in [24], the cryptographic operations for RSU to verify n messages in single vehicle authentication includes $(3n)T_h$, $(6n)T_{e.m}$, and $(2n)T_{e.a}$. Thus, the total computation cost is $2.6559n$ ms. Additionally, through the previous analysis, it is determined that the computation cost for RSU to verify n messages in batch authentication is $1.8766n+12.633$ ms. By comparing these two computation costs for different vehicle densities, we can determine τ. The analysis results show that $\tau \approx 16$, that is, when the density of the vehicle is lower than τ, the RSU selects single vehicle authentication, and batch authentication is selected when the density of the vehicle is higher than τ. The details will be shown in Fig. 5.

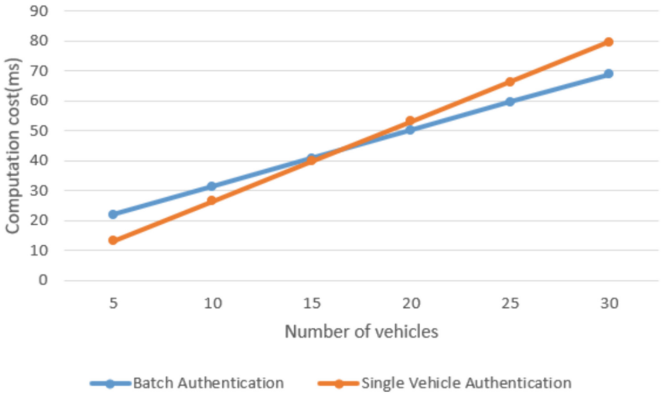

Fig. 5. Vehicle density threshold analysis

8 Conclusion

We propose an adaptive authentication protocol for the IoV based on vehicle density, which uses single vehicle authentication in low-density vehicle environments and batch authentication in high-density vehicle environments. Not only can meet privacy and security requirements, effectively resist malicious attacks, but also reduce computation and communication overhead to a certain extent. Furthermore, the proposed protocol has better performance than current anonymous authentication protocols.

References

1. Baee, M.A.R., Simpson, L.R., Boyen, X., Foo, E., Pieprzyk, J.: On the efficiency of pairing-based authentication for connected vehicles: time is not on our side! IEEE Trans. Inf. Forensics Secur. **16**, 3678–3693 (2021)
2. Bagga, P., Das, A.K., Wazid, M., Rodrigues, J.J., Park, Y.: Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges. IEEE Access **8**, 54314–54344 (2020)
3. Bagga, P., Sutrala, A.K., Das, A.K., Vijayakumar, P.: Blockchain-based batch authentication protocol for internet of vehicles. J. Syst. Archit. **113**, 101877 (2021)
4. Bellare, M., Garay, J.A., Rabin, T.: Fast batch verification for modular exponentiation and digital signatures. IACR Cryptology ePrint Archive (1998)
5. Cui, J., Wei, L., Zhang, J., Xu, Y., Zhong, H.: An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks. IEEE Trans. Intell. Transp. Syst. **20**, 1621–1632 (2019)
6. Dolev, D., Yao, A.: On the security of public key protocols. IEEE Trans. Inf. Theory **29**(2), 198–208 (1983)
7. Ferng, H.W., Chen, J.Y., Lotfolahi, M., Tseng, Y.T., Zhang, S.: Messages classification and dynamic batch verification scheme for VANETs. IEEE Trans. Mob. Comput. **20**, 1156–1172 (2021)

8. Galbraith, S.D., Gaudry, P.: Recent progress on the elliptic curve discrete logarithm problem. Des. Codes Crypt. **78**, 51–72 (2016)
9. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: VANET security challenges and solutions: a survey. Veh. Commun. **7**, 7–20 (2017)
10. Liu, H., Wang, H., Gu, H.: HPBS: a hybrid proxy based authentication scheme in VANETs. IEEE Access **8**, 161655–161667 (2020)
11. Lu, H., Liu, Q., Tian, D., Li, Y., Kim, H., Serikawa, S.: The cognitive internet of vehicles for autonomous driving. IEEE Netw. **33**, 65–73 (2019)
12. Ma, M., He, D., Wang, H., Kumar, N., Choo, K.K.R.: An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks. IEEE Internet Things J. **6**, 8065–8075 (2019)
13. Mei, Q., Xiong, H., Chen, J., Yang, M., Kumari, S., Khan, M.K.: Efficient certificateless aggregate signature with conditional privacy preservation in IoV. IEEE Syst. J. **15**(1), 245–256 (2021)
14. Naik, G., Choudhury, B., Park, J.M.J.: IEEE 80211bd & 5G NR V2X: evolution of radio access technologies for V2X communications. IEEE Access **7**, 70169–70184 (2019)
15. Thumbur, G., Rao, G.S., Reddy, P.V., Gayathri, N.B., Reddy, D.V.R.K., Padmavathamma, M.: Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. IEEE Internet Things J. **8**, 1908–1920 (2021)
16. Vijayakumar, P., Azees, M., Kozlov, S.A., Rodrigues, J.J.P.C.: An anonymous batch authentication and key exchange protocols for 6G enabled VANETs. IEEE Trans. Intell. Transp. Syst. **23**, 1630–1638 (2022)
17. Wang, P., Liu, Y.: SEMA: secure and efficient message authentication protocol for VANETs. IEEE Syst. J. **15**, 846–855 (2021)
18. Wazid, M., et al.: Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks. IEEE Access **5**, 14966–14980 (2017)
19. Xu, Z., Liang, W., Li, K.C., Xu, J., Jin, H.: A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. J. Parallel Distrib. Comput. **149**, 29–39 (2021)
20. Yang, A., Weng, J., Yang, K., Huang, C., Shen, X.: Delegating authentication to edge: a decentralized authentication architecture for vehicular networks. IEEE Trans. Intell. Transp. Syst. **23**, 1284–1298 (2022)
21. Yang, Y., Huang, X., Hu, J.: A batch authentication design to protect conditional privacy in internet of vehicles. Secur. Commun. Netw. (2021)
22. Zhang, J., Cui, J., Zhong, H., Chen, Z., Liu, L.: PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. IEEE Trans. Dependable Secure Comput. **18**(2), 722–735 (2021)
23. Zhang, J., Zhong, H., Cui, J., Tian, M., Xu, Y., Liu, L.: Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Trans. Veh. Technol. **69**, 7940–7954 (2020)
24. Zhang, J., Zhong, H., Cui, J., Xu, Y., Liu, L.: An extensible and effective anonymous batch authentication scheme for smart vehicular networks. IEEE Internet Things J. **7**, 3462–3473 (2020)
25. Zhang, M., Zhu, B., Li, Y., Wang, Y.: TPM-based conditional privacy-preserving authentication protocol in VANETs. Symmetry **14**, 1123 (2022)

26. Zhang, M., Zhou, J., Zhang, G., Zou, M., Chen, M.: EC-baas: elliptic curve-based batch anonymous authentication scheme for internet of vehicles. J. Syst. Archit. **117**, 102161 (2021)
27. Zhang, R., Xu, Z., Xu, J.: A batch authentication protocol based on small exponent test for internet of vehicles. In: 2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta), pp. 580–587 (2022)