Experimental Research on Certificate less Fault-Tolerant Aggregate Signature Scheme in Internet of Vehicles

Jiashuo Cheng, Bingxu Han, Shutong Li, Mengyao Li

***Abstract*- As a key component of intelligent transportation systems, Vehicular Ad Hoc Network (VANET) has been widely used to improve traffic congestion, optimize driving paths, improve driving safety, and provide diverse entertainment services. However, due to its open communication architecture, the Internet of Vehicles faces many security challenges in message transmission and user identity protection. First, when vehicles communicate with other vehicles (Vehicle-to-Vehicle, V2V) or infrastructure (Vehicle-to-Infrastructure, V2I), information is vulnerable to security threats such as forgery, eavesdropping, message replay, and denial of service attacks. This may lead to driver misjudgment and safety accidents. Secondly, the Internet of Vehicles also faces problems in user privacy protection, such as location privacy leaks and identity information abuse. Compared with existing PKI and identity-based schemes, the certificateless architecture proposed in this paper has significant advantages and benefits in the following aspects: efficiency, fault tolerance, privacy protection, scalability, and security. Through security analysis and performance evaluation, the results show that this solution is superior to existing methods in terms of computing efficiency, storage requirements, communication overhead, etc., and on the basis of ensuring privacy protection and data integrity, it achieves high-dynamic environment Secure authentication and efficient communication.**

***Index Terms*—Internet of Vehicles authentication; no certificate; digital signature; fault-tolerant aggregatesignature; elliptic curve**

I. INTRODUCTION

vehicular ad hoc networks (VANETs) refer to technologies that connect and interact vehicles with the Internet, other vehicles and road infrastructure. It integrates various technologies such as sensors, communication, artificial intelligence, and big data, bringing numerous advantages to modern transportation systems. For example, vehicle networking technology can monitor vehicle status, road condition information, and other vehicle dynamics in real time. Through functions such as fault warning, danger warning, and autonomous driving assistance, it effectively avoids or reduces the occurrence of vehicle failures and accidents. Through real-time sharing and processing of traffic information, the Internet of Vehicles can provide drivers with navigation optimization, route planning, and traffic management suggestions, helping to avoid congested road sections and improve road traffic efficiency. And provide personalized navigation, entertainment, and information services based on the needs and preferences of drivers.

The Internet of Vehicles utilizes technologies such as sensor data collection, wireless radio frequency identification (RFID), and short-range communication to achieve mutual communication and information exchange between vehicles (V2V) and between vehicles and roadside infrastructure (V2I). This type of communication and information exchange makes the control of vehicles and roads more precise and comprehensive. In the connected car system, the working principle of OBU is to integrate and utilize various technologies such as Global Positioning System (GPS), microsensors, and embedded systems with the help of a dedicated short-range communication system. This enables the vehicle to efficiently and accurately communicate with other vehicles or roadside units (RSUs) in the surrounding area. RSUs communicate information with Trusted Centers (TAs) or OBU through wired and wireless channels. RSUs can receive information from OBU and transmit it to TA, as well as receive information sent by TA and transmit it to OBU. The bidirectional transmission of this information enables the vehicle networking system to achieve more extensive and in-depth information sharing and interaction.

With the continuous development of the Internet of Vehicles, communication between vehicles has become increasingly common. However, due to the open communication nature of the Internet of Vehicles, the information transmitted by vehicles is vulnerable to security attacks and privacy violations. Secure authentication of transmitted content and privacy protection of vehicle identity are two key points.

II. RELATED RESEARCH

The research solutions for privacy protection and data authentication in the context of connected vehicles can be roughly divided into three categories: the first category is certificate based solutions, the second category is identity signature based solutions, and the third category is certificate free solutions.

A. Certificate based solutions

In 2007, Raya and Hubaux [1] proposed the first CPPA (Conditional Privacy Preserving Authentication) scheme for the Internet of Vehicles based on a modified PKI (Public Key Infrastructure) framework. This scheme uses anonymous certificates to protect user identity privacy and provide message authentication. In this scheme, a large number of keys and related anonymous certificates are preloaded into the onboard units of the vehicle, and the anonymous certificates are frequently replaced during communication to send messages under different pseudonyms, ensuring the

Manuscript received April 08, 2025

Jiashuo Cheng，School of Software,Tiangong University, Tianjin , 300380, China.

Bingxu Han，School of Software,Tiangong University, Tianjin ,300380, China.

Shutong Li，School of Computer Science and Technology,Tiangong University, Tianjin , 300380, China

Mengyao Li，School of Software,Tiangong University, Tianjin ,300380, China

[1]Funding Support : This work was supported by the Tianjin Polytechnic University 2024 Undergraduate Innovation and Entrepreneurship Training Program Funding Project (No.202410058087)

unlinkability of the data. This scheme requires a certificate issuing authority to manage a large number of certificates, and frequent exchange of anonymous certificates between vehicles and roadside facilities, resulting in high storage and communication costs.

In order to address the aforementioned issues, Lu et al. [2] proposed a new anonymous authentication scheme based on group signatures and temporary anonymous certificates in 2008. In this scheme, vehicles obtain temporary anonymous certificates from nearby roadside facilities for anonymous communication to ensure identity privacy. However, this scheme is affected by roadside facilities, and the data sharing process requires roadside facilities to remain online.

Although there have been advances in traditional public key certificate based schemes in recent years [3-5], the efficiency of this scheme is relatively low, and there are insurmountable problems in certificate management and storage. In such schemes, not only do certificate authorities need to issue and revoke a large number of anonymous certificates, but vehicles also need to frequently store and forward anonymous certificates during communication, resulting in high storage and communication costs for the vehicles.

B. Identity based solutions

In 1984, Shamir proposed identity based cryptography, which solved the problem of certificate management. Identity based cryptographic systems do not use any certificates and do not require certificate issuing authorities as in traditional public key cryptographic systems. In this cryptographic system, the user's public key is any string or identifiable information selected by the user, and the user's private key is generated by a trusted institution. In the process of generating a private key, the user first needs to prove their identity to a trusted institution, and then the trusted institution uses their master key to generate a secret key for the user. The system master key is only held by trusted institutions, and only users who successfully prove their identity can obtain the private key. Users sign the information they send, and the sender's identification code can be used as a public key to verify the information signature. Compared with traditional PKI based cryptographic systems, identity based cryptographic systems do not require the distribution of certificates through CA institutions, nor do they require the use of certificates for authentication through public key verification, reducing the complexity and overhead of certificate management.

Lu et al. [7] proposed an identity based authentication mechanism that protects the privacy of users in the Internet of Vehicles by using adaptively generated pseudonyms, suitable for adaptive identity privacy protection in vehicular ad hoc networks. Although in identity signature based authentication schemes, trusted institutions can generate private keys corresponding to any identity in the system, reducing reliance on third-party institutions that issue certificates, attacks on trusted institutions may result in the leakage of private keys for all users. Zhang et al. [8] proposed an efficient identity based anonymous authentication scheme using identity based public key cryptography. In this scheme, vehicles and roadside facilities do not need to store any certificates and provide batch verification, enabling the simultaneous verification of multiple messages and improving the efficiency of the authentication scheme. However, this scheme cannot provide non repudiation functionality, is susceptible to relay attacks and impersonation attacks, and has key custody issues.

Existing identity based schemes suffer from key custody issues due to the use of a key centralized structure [9-10]. Once the trusted infrastructure is breached, the private keys of all vehicles will be leaked, posing a serious security threat to the vehicle networking system.

C. Certificate free Solution

In order to solve the huge certificate and CRL overhead in basic public key infrastructure and the hosting problem in identity signature schemes, Al Riyami and Paterson [11] proposed the first certificate free signature scheme in 2003. The key generation center in its scheme is mainly responsible for providing users with local private keys. The use of a local private key and a secret value chosen by the user to form the user's complete private key ensures that a valid signature cannot be forged without only obtaining a partial private key of the user.

In 2003, Boneh et al. [12] proposed the concept of aggregate signatures at the European Cryptography Conference. Aggregation signature technology can compress the signature messages of multiple users into a single signature message for processing, thereby improving the authentication efficiency of messages and reducing communication overhead, making it very suitable for vehicular communication environments.

Based on uncertified digital signatures, not only can the problem of key custody be solved, but it can also be well combined with cryptographic techniques to improve computational efficiency, such as using aggregate verification and combining with elliptic curve cryptography. Certificate free digital signatures are of great significance for the deployment of vehicle networking authentication schemes.

In 2012, Shim et al. [13] proposed a conditional privacy protection authentication scheme based on pseudo identity signatures for communication. The use of bilinear pairing to enhance security or improve authentication performance in the connected vehicle environment has a major drawback of high computational overhead during information processing. Therefore, bilinear pairing methods may not be suitable for dynamic authentication in connected vehicles. In 2012, He et al. [14] proposed the first certificate free digital signature scheme without bilinear pairs, which was proven to be secure in a random oracle model. Later, it was found that the scheme was vulnerable to attacks from a second type of strong adversary.

Horng et al. [15] proposed a method for communication between vehicles and roadside units, which strengthens the privacy protection of signature schemes. This scheme supports multi platform aggregation signature verification, but the cost is relatively high, which can have a negative impact on normal vehicle communication and is vulnerable to malicious key generation center attacks. In 2018, Cui et al. [16] designed a new uncertified CPPA scheme that significantly reduces computational overhead, requiring only operations on elliptic curves and a universal one-way hash function, without any bilinear pairing operations. However, this scheme cannot resist passive attacks. Kamil et al. [17] proposed an improved scheme based on Cui et al.'s design, but this scheme cannot resist signature forgery attacks.

In 2021, Chattaraj et al. combined blockchain technology with certificate free solutions to ensure the security of connected vehicle transmission and created a voting function that can revoke the legitimate identity of vehicles with poor reputation. In 2023, XIA [19] designed a certificate free scheme by combining attribute encryption technology based on ciphertext strategy with blockchain technology.

In 2023, XIONG et al. proposed a certificate free batch authentication scheme, which achieved batch authentication in both V2V and V2I communication modes, improved the efficiency of the scheme, and provided traceability function

for malicious entities.

In response to the shortcomings of uncertified schemes in terms of computational complexity and security, reference [21] proposes to combine fault-tolerant aggregate signature mechanisms with uncertified schemes and apply them to the Internet of Vehicles environment to improve system efficiency and security. However, this scheme has not yet been experimentally validated for its effectiveness in actual vehicle networking scenarios. This article uses computer simulation technology to construct a virtual environment, simulate various scenarios and conditions, quickly evaluate the performance and reliability of the vehicle networking system, further verify the practical superiority of the proposed solution in reference [21], and provide important reference for related research.

III. PREPARATORY KNOWLEDGE

A. Assumptions for Difficult Problems

Definition 1. The content of the elliptic curve discrete logarithm problem (ECDLP) is: G is a finite cyclic group with a large prime q on the elliptic curve, P is the generator of group G, and for a given P, Q ∈ G, ECDLP is to find x ∈ Z such that Q=xP. If there is no algorithm ξ that can solve the ECDLP problem on group G with a non negligible probability within the computation time t, then the ECDLP problem is said to be difficult in group G.

Definition 2: The content of the Computational Diffie Hellman Problem (CDHP) is: Let G be an additive cyclic group composed of points on an elliptic curve, and its generator is P. Given aP ∈ G and bP ∈ G, but the specific values of a ∈ Z and b ∈ Z are unknown. In this case, the goal of calculating CDHP is to find abP. If there is no algorithm ξ that can successfully calculate abP with non negligible probability within time t, then the CDHP problem is considered computationally difficult in group G.

B. Hash Algorithm

Hash function is an irreversible one-way mapping that maps any length message to a fixed length value without the need for a key. Its characteristics include arbitrary input length, fixed output length, unidirectionality, resistance to weak collisions, and resistance to strong collisions. These features make it widely used in encryption and digital signatures for verifying message integrity and ensuring data security.

C. Elliptic Curve Cryptography (ECC)

ECC is a public key cryptographic system based on the mathematical properties of elliptic curves. On a finite field F, an elliptic curve E is usually defined by the equation y2=x3+ax+b, where a, b∈F, and 4a3+27b2≠0 must be satisfied to ensure that the curve has no singular points. The points on the curve, including the point O at infinity, form an additive cyclic group. Point addition and scalar multiplication are defined on this basis.

For point addition: given two points P and Q on a curve, the sum R=P+Q is calculated as follows:

Different points P≠Q: The straightline connecting P and Q intersects the curve at the third point R', then R is the symmetric point of R' about the x-axis.

Same point P=Q: The tangent at point P intersects the curve at point R', then R is the symmetric point of R' about the x-axis.

Points that are opposite to each other P=−Q: At this time, P+Q=O, that is, the point at infinity.

For scalar multiplication: add point P to itself m times, that is, mP=P+P+⋯+P (a total of m times).

The security of ECC is based on the computational difficulty of the elliptic curve discrete logarithm problem (ECDLP). Compared with traditional public key cryptography systems (such as RSA), ECC can use a shorter key length while providing the same level of security, resulting in higher computational efficiency and lower resource consumption. This makes it particularly suitable for resource-constrained environments such as mobile devices and smart cards.

D. Uniform (k, n)-sets of finite sets

Assume two sets $D=\{\sigma_1,\sigma_2,...,\sigma_m\}, B=\{B_1,B_2,...B_n\}$, $B_j \in D$, and $1\le j\le m$, B is a uniform (k, n)-set of D if and only if the following conditions are met, $((^n_{k-1})\le m)$:

1) $|B_1|=|B_2|=...=|B_n|$

2) For any k subsets $B_{i_1},...,B_{i_k}\in\{B_1,...,B_n\}$, $\bigcup_{k}^{j=1} B_{i_j}=B$

3) For any k−1 subsets $B_{i_1},...,B_{i_k}\in\{B_1,...,B_n\}$, $\bigcup_{k-1}^{j=1} B_{i_j}=B\setminus\{\sigma_i\}$

As for how to construct a uniform (k, n)-set, we only consider the case of $((^n_{k-1})=m)$, the details are as follows: Assume the set $D=\{\sigma_1,\sigma_2,...,\sigma_m\}$, the uniform (k, n)-set of D is $B=\{B_1,B_2,...B_n\}$ where $((^n_{k-1})=m)$. Then split it into *m* groups $W_1,W_2,..W_m$, and each group consists of *K-1* elements in B.

The formal definition is as follows:

$$W_1=B_{l_1}\cup B_{l_2}...\cup B_{l_{k-1}}$$
$$W_2=B_{2_1}\cup B_{2_2}...\cup B_{2_{k-1}}$$
$$...$$
$$W_m=B_{m_1}\cup B_{m_2}...\cup B_{m_{k-1}}$$

$B_{i_j}\in B, i=1,2,...,m, j=1,2,...,k-1$. Where for set B, $|B_1|=|B_2|=...=|B_n|$ and $B_1\cap B_2\cap...B_n=\ell_0$ for $1\le i\ne j\le m$, $W_I\ne W_j$. For $1\le\alpha\le m$, there is $\partial_a W_\alpha$ and $\partial_a\in W_\alpha$ where $1\le b\le m, b\ne a$ Finally, the output uniform (k, n)-set of D is $B=\{B_1,B_2,...B_n\}$.

System Model

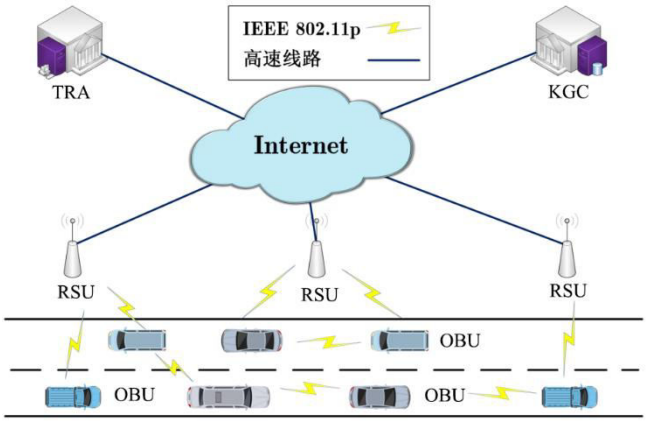

Fig.1 System model diagram

As shown in Figure 1, our system model includes the following four entities: Trust Registration Authority (TRA), Key Generation Centre (KGC), Roadside Unit (RSU), and Onboard Unit (OBU)

1) Trusted Registry Center (TRC)

The trusted registration center is responsible for system initialization, including generating system public parameters and initializing other entities. TRC is the root of trust for the entire system, managing the trust relationships of the entire network and providing basic trust support for other components. When a vehicle joins the network, TRC verifies its identity and issues basic authentication information.

2) Key Generation Center (KGC)

The key generation center is responsible for generating key pairs for vehicles and roadside units. In the uncertified encryption scheme, the key generation center generates a partial private key for each vehicle, while the vehicle itself generates the remaining private key parts, thus forming a complete private key pair. This key generation method not only ensures the security of the private key, but also avoids the key custody problem in traditional identity based schemes.

3) Roadside Units (RSUs)

Roadside units are relay nodes in the Internet of Vehicles, distributed on both sides of the road, responsible for receiving and forwarding information from vehicles. The main responsibilities of RSU include broadcasting and transmitting auxiliary information, verifying vehicle signatures, and sharing some system information with vehicles. RSU can collaborate with the key generation center to update system parameters for newly added vehicles. In addition, RSUs can also cache public information to reduce communication latency and improve overall system efficiency.

4) On board Unit (OBU)

The onboard unit is installed on the vehicle and is the main body of vehicle communication. Each vehicle's OBU is responsible for information exchange with other vehicles and RSUs. OBU generates temporary pseudonyms for communication to protect user privacy. During the signature verification process, OBU needs to combine partial keys withits own generated keys for signature calculation, and broadcast the signature message to other vehicles and RSUs.

IV. FAULT TOLERANT AGGREGATION AUTHENTICATION SCHEME WITHOUT CERTIFICATE

A. *Overview of the Proposed Scheme*

The symbols and meanings involved in this plan are shown in Table 1.

Symbol	indicates meaning
TRA	Trust Registration Authority
KGC	Key Generation Center
OBU	On board Unit
RSU	Public and private keys of TRA
(T_{pub},b)	Public and private keys of the KGC
(T_{pub},s)	The true identity of the vehicle
ID_i	The pseudonym of the vehicle
PID_i	The vehicle's private key pair
$VSK_{PIDi}=(x_i,d_i)$	Public key pair of the vehicle
$VPK_{PIDi}=(X_i,R_i)$	Key Generation Center

In order to meet the efficient and secure authentication requirements in the Internet of Vehicles, this paper proposes an unlicensed fault-tolerant aggregation authentication scheme based on elliptic curves. This scheme combines elliptic curve cryptography and batch verification mechanism, which not only ensures the confidentiality and integrity of information, but also significantly outperforms traditional schemes in terms of communication overhead and computational efficiency. By utilizing distributed key generation and certificate free mechanisms, the issue of key custody has been effectively eliminated. The entire process is shown in Figure 2, which illustrates the complete steps from initial vehicle authentication to key generation and information transmission.

B. *Algorithm steps*

Next, the eight steps of the certificateless signature aggregation fault tolerance scheme will be explained in detail.

- **System settings:** Select two large prime numbers p and q and generate an elliptic curve $E: y^2 = x^3 + ax + b \bmod p, a, b \in Z_p^*, (4a^3 + 27b^2) \bmod p \neq 0$ .Select a group G with order q and generator p from E.KGC randomly generates $s \in Z_q^*$ as its master private key and calculates $T_{pub} = bP$ as its master public key.TRA randomly generates $b \in Z_q^*$ as its master private key and calculates $T_{pub} = bp$ as its master public key.
- **Pseudonym generation:** The vehicle randomly selects $t \in Z_q^*$ to calculate $PID_{t1} = t_i P$, $K_i = t_i T_{pub} \oplus ID_i$ and sends PID_i , K_i to TRA. TRA calculates $ID_i = K_i \oplus bPID_{i1}$ to verify the legitimacy of the vehicle's identity. If verified, $PID_{i2} = ID_i \oplus H_1(bPID_{i1})$ is calculated and thevehicle's pseudonym information $PID_i = \{PID_{i1}, PID_{i2}\}$ is sent to KGC.
- **Partial key generation:** KGC receives the message sent by the vehicle and generates a partial key for the vehicle. KGC randomly selects $r_i \in Z_q^*$ and calculates $R_i = r_i P$. Generates the vehicle's partial key $d_i = (r_i + h_{1i}) \bmod q$, where $h_{1i} = (PID_i, R_i, P_{pub})$. KGC sends $\{d_i, R_i, PID_i, \Delta T_i\}$ to the vehicle and stores it in its OBU. The vehicle uses $d_i P = R_i + h_{1i} P_{pub}$ to verify the legitimacy of the partial private key.
- **Vehicle key generation:** The vehicle randomly selects $x_i \in Z_q^*, X_i = x_i P$ and calculates $h_{2i} = H_2(PID_i, X_i)$. Sets public key $VPK_{PID_i} = (X_i, R_i)$ and private key $VSK_{PID_i} = (x_i, d_i)$.
- **Signature process:** The vehicle randomly selects $U_i = u_i P$ and calculates $U_i = u_i P$, $h_{2i} = H_2(PID_i, X_i)$, $h_{3i} = H_3(PID_i, m_i, VPK_{PID_i}, U_i, T_i, h_{2i})$ .The signature value of message m is $S_i = u_i^{-1}(h_{2i} x_i + h_{3i} d_i)$, and finally the message signature is sent to RSU.
- **Signature verification process:** After receiving the message signature, the RSU first calculates $h_{1i} = (PID_i, R_i, P_{pub})$, $h_{2i} = H_2(PID_i, X_i)$ and $h_{3i} = H_3(PID_i, m_i, VPK_{PID_i}, U_i, T_i, h_{2i})$, for each vehicle and determines whether the following equation is true $S_i U_i = h_{2i} X_i + h_{3i}(R_i + h_{1i} P_{pub})$.
- **Aggregate signature verification process:** If the RSU receives messages from different vehicles $V_i, i \in \{1,2,\ldots,m\}$, it calculates $\alpha = \sum_{i=1}^{\omega} S_i U_i - \sum_{i=1}^{\omega} h_{2i} X_i - \sum_{i=1}^{\omega} h_{3i}(R_i + h_{1i} P_{pub})$. If $\alpha = 0$, the aggregate signature verification is successful, otherwise it enters the fault-tolerant aggregate signature phase.

C. *Fault-tolerant aggregate signature verification process*

When the RSU receives and processes m signature information from vehicles, if these signatures fail to pass the conventional aggregate signature verification process, the system will automatically enter the fault-tolerant verification phase. In this phase, the RSU will construct a unified (k, n) set according to a certain algorithm.

However, in actual operation, it is not easy to determine the appropriate k and n values. Considering the differences in road traffic in different time periods and locations, it first

divides the received signatures into multiple batches. The number of signatures in each batch will vary according to the actual situation to ensure that a unified (k, n) set can be easily constructed later. The RSU closely monitors and analyzes the changes in traffic flow, and selects a suitable value h based on the real-time traffic flow in the area to ensure that there are suitable n and k, so that C(n, k-1) = h. In this way, the required (k, n) set can be smoothly constructed in the subsequent steps.

For the m signatures received, the RSU finds an h value that is greater than m and as close to m as possible, which can ensure that there is no excessive additional computational burden when generating virtual signatures. After finding a suitable h value, the RSU will generate (h-m) virtual signatures. These virtual signatures, together with the original m signatures, are used to construct a (k, n) set B, where B contains n elements, that is, B = {B1, B2, ..., Bn}.

After constructing the set B, the RSU will delete the virtual signatures in the set and only keep the real signature information. Then, it will use this processed (k, n) set to generate n groups of aggregated signatures. These aggregated signatures will undergo further verification to ensure their authenticity and validity.

Through such a fault-tolerant verification process, the RSU can still maintain the normal operation and security of the system when encountering a signature verification failure. At the same time, this flexible strategy also ensures that the system can efficiently and accurately process the signature information from vehicles under different traffic flow conditions.

D. Algorithm Correctness

Theorem 1: (Correctness) If the signature uploaded by the signer $V_i(i \in 1,2.....n)$ is correct, it can be verified by RSU_j.

Proof: Correctness of single signature verification:

$$S_iU_i = \left(u_i^{-1}\left(h_{2i}x_i + h_{3i}d_i\right)\right)U_i$$
$$S_iU_i = \left(u_i^{-1}\left(h_{2i}x_i + h_{3i}d_i\right)\right)u_iP$$
$$S_iU_i = u_i^{-1}u_i\left(h_{2i}x_i + h_{3i}d_i\right)P$$
$$S_iU_i = h_{2i}x_iP + h_{3i}d_iP$$
$$S_iU_i = h_{2i}X_i + h_{3i}\left(R_i + h_{1i}P_{hub}\right)$$

Correctness of aggregate signature verification:

$$\alpha = \sum_i^n S_iU_i - \sum_i^n \left(u_i^{-1}\left(h_{2i}x_i + h_{3i}d_i\right)\right)U_i$$
$$\alpha = \sum_i^n S_iU_i - \sum_i^n \left(u_i^{-1}\left(h_{2i}x_i + h_{3i}d_i\right)\right)u_iP$$
$$\alpha = \sum_i^n S_iU_i - \sum_i^n u_iu_i^{-1}\left(h_{2i}x_i + h_{3i}d_i\right)P$$
$$\alpha = \sum_i^n S_iU_i - \sum_i^n h_{2i}x_iP + h_{3i}d_iP$$
$$\alpha = \sum_i^n S_iU_i - \sum_i^n h_{2i}X_i + h_{3i}\left(R_i + h_{1i}P_{pub}\right)$$

Reference [21] analyzes the security of this scheme from seven aspects: unforgeability, anonymity, traceability, resistance to man-in-the-middle attacks, anti-collusion attacks, forward security and backward security, and anti-replay attacks. For details, see reference [21], which will not be repeated here.

V. EXPERIMENTS AND ANALYSIS

A. Experimental Environment

This simulation study utilizes the Veins simulation software, which is composed of three main components: SUMO, OMNet++, and Veins. SUMO handles the modeling of the traffic system and can construct road networks; however, it lacks capabilities for vehicular network information exchange and communication protocol implementation. OMNet++ is a C++-based simulation framework that enables the modular simulation of various network structures. Veins acts as a bridge between the two.

TABLE 2
SOFTWARE AND HARDWARE ENVIRONMENT

Name	Model and Version
CPU	Intel® Core™ i5-10210U CPU @
Mem	1.60GHz × 2
Veins	4GB
SUMO	5.1-i2
OMNet++	5.6.2

The software and hardware environment used for the simulations are presented in Table II. The simulation was executed on a virtual machine environment running the Debian GNU/Linux 10 operating system with the official virtual machine provided by Veins.

The functions of the entities in the simulation process are shown in Table 3. The specific code logic and algorithm flow will be elaborated in the pseudo-code section that follows.

TABLE 3
ENTITY FUNCTION

Entity	Function	Description
OBU	CarSendID(PID1, K)	The vehicle sends the identity information
	CarVerifyPartPrivateKey(d, R, PID)	The vehicle verifies part of the private key
	CarGenerateKey();	The vehicle generates the full public key private key
	CarSignature(Message, VPK, U, S);	The vehicle signs the message
TRA	TRAGenerateAlias(PID1, K, PID)	TRA generates vehicle pseudonyms
KGC	KGCGeneratePartPrivateKey(PID, d, R)	The KGC generates a partial private key of the vehicle
RSU	RSUVerifySignature(PID, Message, VPK, U, S)	The RSU verifies the signature of the vehicle

B. Algorithm Pseudocode

1) OBU Entity

The CarSendID function generates partial pseudonyms to protect vehicle privacy. A random number is generated as a private key, and a corresponding elliptic curve point is calculated as a temporary identity marker. Another random number is used to encrypt the real identity, and the encrypted identity and partial pseudonym are sent to the TRA. The detailed workflow is presented in Algorithm 1.

The CarVerifyPartPrivateKey function ensures the integrity and authenticity of pseudonyms and partial private keys received from the KGC. Through hash computations

and elliptic curve equations, it prevents data tampering and stores valid partial keys for future communication. Algorithm 2 provides detailed steps.

The CarGenerateKey() function combines a vehicle's private key with the partial private key from the KGC to generate a complete key pair. This key pair ensures secure communication through authentication, encryption, and signing. Algorithm 3 provides detailed steps.

The CarSignature() function signs messages using the vehicle's private key. A random number is generated and multiplied with a base point to calculate a new point. The pseudonym, public key, and message are hashed, and the hash result is multiplied with the private key and divided by the random number to produce the signature. Algorithm 4 provides detailed steps.

2) TRA Entity

The TRAGenerateAlias() function receives partial pseudonyms and encrypted identities from vehicles, decrypts them to obtain full vehicle IDs, and generates new pseudonyms. These are combined with original pseudonyms to create complete pseudonyms, ensuring privacy and data integrity. Algorithm 5 provides detailed steps.

3) KGC Entity

The KGCGeneratePartPrivateKey() function generates a vehicle's partial private key. A random number is generated and multiplied by the elliptic curve base point to create a new point. The pseudonym, point, and KGC's public key are hashed to ensure data integrity. The partial private key is computed by combining the random number, KGC's private key, and the hash result. Algorithm 6 provides detailed steps.

4) RSU Entity

The RSUVerifySignature(PID, Message, VPK, U, S) function aggregates messages and signatures from multiple vehicles for batch verification. If the batch verification fails, the faulty signatures are identified using a fault-tolerant algorithm, and the erroneous vehicles are reported. Algorithm 7 provides detailed steps.

C. *Experiment Results*

A traffic scenario simulating an intersection was set up in this experiment. In total, 62 vehicles crossed the simulated intersection within 10 seconds after the experiment started. According to the preset algorithm process, each vehicle first sends its identity information to the TRA. Upon receiving this information, TRA will quickly generate a unique pseudonym for each vehicle to protect the privacy of the vehicle and prevent its true identity from being revealed. Subsequently, TRA sends the generated pseudonyms to KGC.

After receiving the pseudonyms of the vehicles, KGC generates a partial key for each vehicle, which ensures that only the vehicle holding the corresponding private key can decrypt and verify it. Then, KGC sends back the generated partial key and the pseudonym of the vehicle to the corresponding vehicle. After receiving part of the key and pseudonym from the KGC, the vehicle generates the remaining part of the key itself. In this way, each vehicle obtains its own complete key and has the ability to communicate securely.

Next, the vehicle signs its own message with its full key. These signatures ensure the integrity of the message and the reliability of the source, so that the receiver can verify the authenticity of the message and the message has not been tampered with. The vehicle sends the signed message to the RSU.

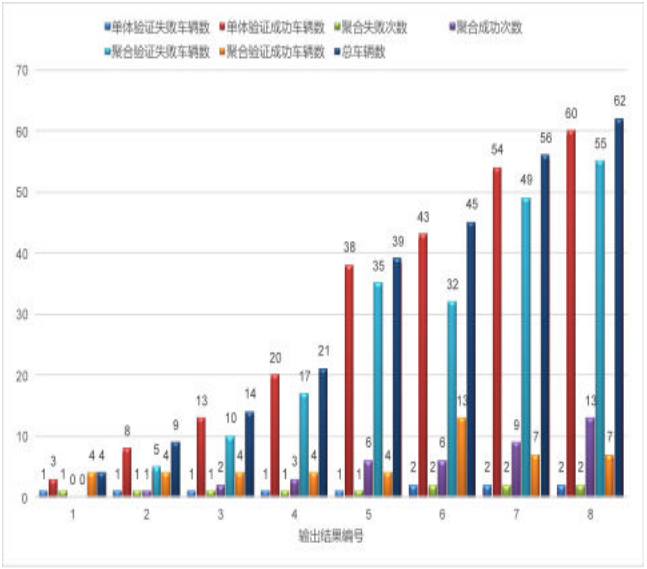

FIG. 3. Output of signature and verification in a simulation.

FIG. 3 shows the output of monolithic signature and aggregate signature and their verification in the simulation experiment in detail. For example, in the output result 8, 60 vehicles were verified successfully and only 2 vehicles failed. The success rate of single vehicle verification was very high, nearly 97%, indicating that the performance or test conditions of the vehicle were effective at the single level. The success rate of aggregation verification is also relatively high, about 88.7%. The cooperative work performance of vehicles is also quite good.

D. *Performance analysis of fault-tolerant aggregation*

The fault-tolerant aggregate signature is used in this scheme. When an aggregate signature contains one or more wrong signatures, the whole set of signatures will be certified as invalid, resulting in the need to recalculation one by one. This significantly increases the computational consumption.

The fault-tolerant technique based on uniform (k, n) -set reorganizes the original mixed signatures into several different sets by a specific algorithm. Signatures within each set will be individually aggregated and verified instead of the entire set at once as in the traditional approach. When there is an error in a signature set, it can quickly locate and isolate the set without recalculating the whole signature set. This not only improves the accuracy of verification, but also significantly reduces the consumption of computational resources.

In order to verify the practical effect of this technique, we conducted a series of simulation experiments. In the simulation, we simulate different road scenarios, setting up scenarios where 20, 40, 60, 80 and 100 vehicles pass the intersection in a fixed time period. These vehicles individually generate signatures and try to perform aggregate verification to simulate the verification under different traffic densities and traffic flows. Through this simulation, we can evaluate the performance performance of the introduction of the fault tolerance mechanism under different conditions.

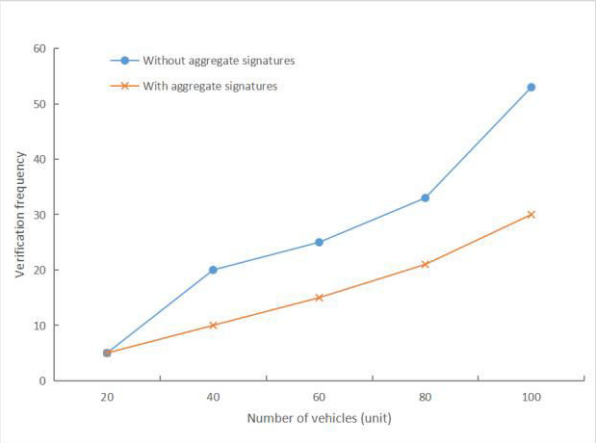

FIG. 4. Verification under different traffic

Figure 4 illustrates the scenarios without and with fault-tolerant aggregation verification times in a scenario with different numbers of vehicles passing through an intersection. It can be found that the vehicles are sparse at the beginning, and there is no wrong signature in the verification process. Both schemes verify the signatures of 20 vehicles with the same small number of aggregated verification. With the increase of traffic density, there are some signature errors in the scene, such as signal collision. At this time, the scheme without fault tolerance needs to spend more times on reverification, but the intervention of fault tolerance greatly reduces this overhead. When the traffic density is very high, the cost of the two schemes is obviously different because of the increase of the number of wrong signatures.

In summary, using fault-tolerant aggregation outperforms the approach without using fault-tolerant aggregation in a variety of distribution situations. It also further verifies the superiority of the scheme.

VI. Summary and Prospect

At the beginning of this paper, the research background of Internet of vehicles communication authentication is comprehensively sorted out, and the academic value and practical significance of this research direction are deeply analyzed, which lays a foundation for subsequent discussion. Then, the basic concepts of IoV are expounded in detail, and the principle and application of elliptic curve cryptosystem, a key technology in the field of cryptography, are deeply interpreted, which further enrich the theoretical basis.

Focusing on the scheme proposed in reference [21], this paper focuses on the detailed analysis and introduction of multiple key entities involved, such as vehicles, authentication servers, etc., and deeply explores the interaction logic and complex algorithm details between them. The scheme in literature [21] innovatively adopts elliptic curve encryption technology. Compared with the traditional bilinear pairings encryption method, it successfully reduces the calculation delay and effectively meets the strict requirements of low delay and high throughput in the Internet of vehicles scenario. At the same time, the application of aggregate signature technology realizes the rapid batch verification of multi-vehicle signatures, which significantly improves the overall verification efficiency. In addition, the introduction of fault-tolerant technology enables the roadside unit to quickly and accurately locate the problem when it encounters an erroneous signature, which effectively ensures the efficiency and stability of the authentication process and greatly improves the speed of authentication.

In terms of research methods, the scheme proposed in literature [21] is reproduced through simulation experiments. Specifically, the IoV environment is constructed and simulated with the help of three professional tools: SUMO, OMNet++ and Veins, and the pseudo-code in the implementation process is shown in detail. Through the comparative analysis of a variety of different scenarios, the significant role of various technologies in the scheme to reduce overhead is clearly presented.

In summary, this paper systematically expounds the design idea and implementation process of the certificateless fault-tolerant aggregation authentication scheme based on elliptic curve proposed in reference [21]. Combined with the experimental results, this paper proposes the following potential improvement directions for the scheme:

Firstly, the encryption and decryption algorithm process of the scheme in reference [21] is relatively fixed. Although the current communication overhead is in an acceptable range, in order to further optimize the communication overhead and transmission delay, more fine adjustment and optimization in the design of signature format and data packet format can be considered in the future to explore greater space for performance improvement.

Secondly, there are certain idealization factors in the simulation scenario designed by literature [21]. Subsequent research can try to introduce the actual scene parameters of the real world, conduct a comprehensive and in-depth performance test of the scheme in the real Internet of vehicles environment with high traffic, and make targeted improvements and consummations according to the test results. So as to enhance the feasibility and adaptability of the scheme in practical applications, and promote the development and progress of the communication authentication technology of the Internet of vehicles.

References

[1] Raya M, Hubaux J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1):39–68.

[2] Lu R, Lin X, Zhu H, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications[C]. IEEE International Conference on Computer Communications, Phoenix, USA, 2008:1229-1237.

[3] Cincilla P, Hicham O, Charles B. Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios[C].2016 IEEE Vehicular Networking Conference, Columbus, USA,2006:1-8.

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

[5] Khodaei M, Papadimitratos P. Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in VANETs[C].ACM Conference on Security & Privacy in Wireless and Mobile Networks, New York, USA,2018:172-183.

[6] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. CRYPTO, 1984, pp. 47–53.

[7] Lu H , Li J , Guizani M .A novel ID-based authentication framework with adaptive privacy preservation for VANETs[C]//2012 Computing, Communications and Applications Conference.IEEE, 2012.DOI:10.1109/ComComAp.2012.6154869.

[8] Zhang C X, Lu R X, Lin X D, et al. An efficient identity-based batch verification scheme for vehicular sensor networks[C].Proceedings of the 27th Conference on Computer Communications. IEEE,2008:246–250.

[9] Liu J K , Yuen T H , Au M H ,et al.Improvements on an authentication scheme for vehicular sensor networks[J].Expert Systems with Applications, 2014.DOI:10.1016/j.eswa.2013.10.003.

[10] Shim K A. CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J].IEEE Transactions on Vehicular Technology,2012,61(4):1874-1883.

[11] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]. 9th International Conference on the Theory and Application of Cryptology. 2003.

[12] Boneh D, Gentr Y C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps [C] .International conference on the theory and applications of crypto graphic techniques. Berlin: Springer, 2003:416 - 432 .
[13] Shim K A. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular technology,2012,61(4):1874-1883.
[14] D. He, J. Chen, R. Zhang, An efficient and provably-secure certificateless signature scheme without bilinear pairings, Int. J. Commun. Syst. 25 (11) (2012) 1432–1442.
[15] Horng S J, Tzeng S F, Huang P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences,2015,317:48-66.
[16] Cui J, Zhang J, Zhong H, et al. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. Information Sciences,2018,451:1-15.
[17] Kamil I A , Ogundoyin S O .An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks[J].Journal of Information Security and Applications, 2018, 44(FEB.):184-200.DOI:10.1016/j.jisa.2018.12.004.
[18] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz and Y. Park, "Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation," in IEEE Transactions on Vehicular Technology, vol. 70, no. 8, pp. 8092-8107, Aug. 2021, doi: 10.1109/TVT.2021.3091163.
[19] Xiong Wanjun, Wang Ruomei, Wang Yujue, Zhou Fan, Luo Xiaonan. Conditional Privacy Protection Batch Authentication Scheme based on Certificateless aggregate Signature in Internet of Vehicles [J]. Chinese Journal of Cryptography, 2016,10(3): 462-475.
[20] Xia Ying, Qin Juan, Zhao Jing et al. Anonymous identity authentication algorithm for vehicle networking based on CP-ABE and blockchain [J]. Journal of Qiqihar University (Natural Science Edition),2023,39(06):34-41.
[21] Liu Q. Research on Privacy protection and security authentication Technology in Vehicle networking [D]. Nanjing university of posts and telecommunications, 2022. DOI: 10.27251 /, dc nki. GNJDC. 2022.001372.