IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 January 2024, accepted 19 January 2024, date of publication 23 January 2024, date of current version 2 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3357490

RESEARCH ARTICLE

Real-Time Tracking and Authentication Protocol for Anonymous Operating Vehicles in Vehicle-Infrastructure Collaborative Systems

JIASHENG YUAN[1], BIN LI[1], XINMING MEI[2], AND YANFANG ZHOU[1]
[1]Research Institute of Highway, Ministry of Transport, Beijing 100088, China
[2]Beijing GOTEC ITS Technology Company Ltd., Beijing 100088, China

Corresponding author: Jiasheng Yuan (js.yuan@rioh.cn)

This work was supported by the Country with Strong Transportation Network Pilot Project under Grant QG2021-2-9-1.

ABSTRACT Vehicle-Infrastructure Cooperative Systems (VICS) are widely used in the safe driving and management of operating vehicles (OV). To preserve privacy and resist harmful attacks, digital certificates and signatures are used during vehicle communication. Nonetheless, the existing secure protocol cannot enable the road control center (RCC) to track the anonymous OV in real-time. To implement this additional functionality, this paper proposes a real-time tracking protocol for anonymous OV based on pseudonym certificates and Optimal Asymmetric Encryption padding (OAEP). In this protocol, pseudonym certificates ensure the security of the OV; the OV's real identity padding by OAEP is encrypted as a ciphertext, which is transmitted to RCC in communication, and RCC decrypts it to achieve real-time tracking. According to the security reduction proofs under the Elliptic Curve Discrete Logarithm Problem (ECDLP) given in the random oracle model (RO), the protocol can satisfy the security requirements. Additionally, the performance analysis based on MIRACL shows the protocol is slightly weaker than others, and we analyze the cost of real-time tracking for the reason. Finally, the RSU service rate of the protocol is analyzed according to the performance and velocity-density model, which proves the protocol is stable in this system.

INDEX TERMS Vehicle-infrastructure cooperative systems, anonymous authentication, conditional privacy, elliptic curve, real-time tracking.

I. INTRODUCTION

The Vehicle-Infrastructure Cooperative Systems (VICS) is a new technical application for intelligent transportation systems, which encompasses the areas of 5G, artificial intelligence, data analytics, edge computing, etc. VICS facilitates real-time communication between vehicle-to-vehicle (V2V), vehicle-to-roadside units (V2R), and vehicle-to-cloud (V2C) through Cellular Vehicle-to-Everything (C-V2X) with the aim to enhance driving efficiency and safety as shown in [1] and [2]. Figure 1 shows the VICS model. The VICS can be well applied in Operating Vehicle management to improve operation efficiency and safety.

Operating vehicles (OV) refer to vehicles engaged in social transport and collect freight, such as large buses, trucks, and dangerous goods transport vehicles. OV has traits including long driving distance and times and large passenger and cargo volume, which is more likely to have a major traffic accident. The accidents of OV will have an important influence on both the economy and society, a significant OV-related catastrophe that happened in 2020 left 20 people killed and more than 170 others wounded [3]. According to the latest revised Dynamic Supervision and Management Measures for Operating Vehicles by the Ministry of Transport of China in 2022, OV needs to share operating status data with the management platform during operation, while managers can manage and guide vehicles according to vehicle status. According to IEEE Std 802.11, OV periodically broadcasts operating data

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

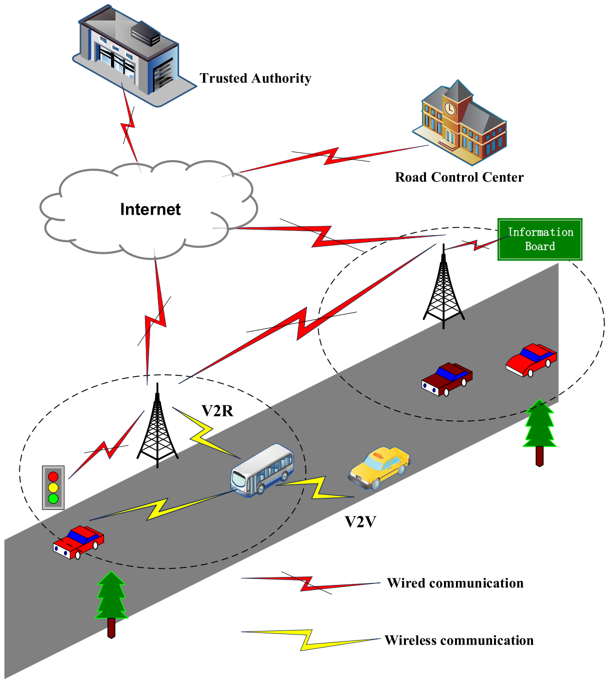

FIGURE 1. The Vehicle-Infrastructure Cooperative System model, including the communication of V2V, and V2R. The vehicle can use the roadside units to communicate with the cloud control platform.

(velocity, position, etc.) every 100-300 *ms* through roadside units (RSU) to the road control center (RCC), which reduces accidents and improves efficiency [4].

One major challenge is the communication between OV and system entities in an open environment, malicious vehicles can eavesdrop and steal communication information or cause traffic accidents by sending false information to OV, particularly for large buses, trucks, and dangerous commodities transport vehicles. Cryptography is widely used in the protection of vehicular communications. Many researchers have established different cryptographic frames, such as PKI-based (Public Key Infrastructure) [5], ID-based [6], and certificateless-based [7], to realize encryption and authentication by digital certificates and signatures [8].

In addition, privacy is another critical problem, OV broadcasts messages with their identity information (including public key, true identity, signature, etc.) to others, and the adversary can easily trace the OV's running route by the outright information [9]. The researchers put forward pseudonymous certificates [10], group signatures [11], mix-zone [12], etc. to achieve anonymity during the OV communication. One major issue however is that malicious vehicles may also have legitimate anonymous identities that could be used to spread false information. Therefore, conditional privacy should be applied in the OV privacy protection, which means the Trusted Authority (TA) can trace the real identity from the anonymized signed message [13].

The Existing conditional privacy is not entirely suitable for OV real-time tracking. When an accident occurs, the RCC can only track the anonymous OV through the TA, which will delay the accident rescue time. On the other hand, the RCC cannot manage and lead OV in real time under the current privacy protection protocols. Another factor that must be considered is effectiveness. Due to the high-speed OV movement, frequent node switches, and restricted RSU computation, the network's stability and communication efficiency would be impacted [14]. Many authentication protocols are built with the bilinear pairing, which will take up a large computational performance [15].

This paper proposes an authentication protocol for anonymous real-time tracking of OV. The protocol uses pre-installed pseudonym certificates to realize the anonymity of OV, which can simplify management and reduce communication overhead at the cost of adding additional storage for OBUs, a small cost that seems insignificant in today's smart vehicles.

We use Optimal Asymmetric Encryption padding (OAEP) and preset public key of the RCC to achieve real-time tracking. The real identity padding with OAEP is encrypted by RCC's public key. The OAEP can ensure that the ciphertext has certain indistinct security. The ciphertext is transmitted along with the message, and RCC can track the real identity of the vehicle after decrypting the message.

To minimize computational consumption, we opt for Elliptic Curve Cryptography (ECC) encryption over bilinear pairing. Although bilinear pairing offers enhanced security compared to ECC, it incurs a significantly higher computational cost, as demonstrated by the experimental results presented in the paper [9].

In addition, we use the Random Oracle model (RO) to prove the protocol's security. Then we use the cryptography library MIRACL to analyze the computational and communication performance of the protocol. In the RSU service rate evaluation model proposed in [16], speed and density are irrelevant. However, vehicle density will affect speed in traffic engineering, so we introduce the Greenshields model [17] to optimize its evaluation.

The primary contributions in this work are summarized as follows:

1) Given the conditional privacy and real-time management requirements, we propose an innovative authentication protocol for anonymous real-time tracking of OV, which uses the pseudonym certificate and OAEP.
2) The protocol is constructed on ECC instead of bilinear pairing operations, which reduces computational consumption. In addition, the pseudonym certificate is generated by the TA and vehicle, that is, even when the part-private key is leaked, the malicious vehicle cannot forge a valid authentication message.
3) We analyze the security by reduction based on the Random Oracle model (RO). The proposed protocol satisfies VICS security requirements for message verifiability and integrity, conditional privacy, non-repudiation, traceability, and defense against common attacks.

4) We use the cryptography library MIRACL to obtain the computational and communication of the protocol. Then, we analyze the RSU service rate based on the Greenshields model (velocity-density model), which proves the protocol is stable in the system.

The rest of the paper is organized as follows. Section II introduces the related work. Section III provides background information relevant to this paper. Section IV describes the proposed protocol for anonymous OV real-time tracking. Section V analyzes the security of the proposed protocol. Section VI analyzes the performance and system stability. Section VII concludes this paper.

II. RELATED WORK

Since the communication of VICS is in an open environment, which has many threats to vehicle privacy and security. To protect the security and privacy of vehicles in VICS, encryption, digital signature, and authentication techniques are applied. There are roughly three different cryptographic frames, that is PKI-based, ID-based, and certificateless-based.

In the PKI system, a third-party Trust Authority (TA), generates public key certificates for users that can verify their identities by the reliability of the certificate chain [14]. In 2007, Raya and Hubaux [18] proposed an anonymous certificate authentication protocol based on the PKI system, which preloaded a large number of anonymous certificates. This method would consume computational and storage costs, and it is difficult to manage, including upgrading and revocation of certificates. Sun et al. [19] proposed a new revocation method for managing certificates, but it still has trouble in certificate management. Based on the pseudonym certificates, some scholars also propose the strategy of pseudonym replacement, which is triggered when the vehicle reaches a certain threshold. Literature [20], [21], and [22] respectively proposed pseudonym replacement schemes based on vehicle density, static and dynamic mixed zones. Wen et al proposed a Ring-signature authentication protocol [23], which solves the problem that TA cannot revoke the vehicles' identity in a group. This protocol constructs a Lattice-based revocable tag on the ciphertext instead of the public key, in this way the privacy of the vehicle in the ring is anonymous, but TA can get the identity. The PKI system has the drawbacks of high calculation overhead and challenging certificate management. An ID-based method has been presented as a solution to the certificate management problem.

Shamir first proposed ID-based cryptography (IBC) in 1984 [24], which eliminates the need for a CA to handle the maintenance of the user's digital certificate by using a string associated with the subject as the public key, through which the private key is generated by the Private Key Generator (PKG). Some researchers proposed the methods of bilinear pairing for signatures, which are generally highly secure [6], [15]. Although the proposed scheme can be batch-verified to improve efficiency, its performance will be slightly lower than the scheme using elliptic curves. Lo and Tsai [25] proposed a conditional privacy-preserving authentication scheme without pairings, which had a higher performance. Genc et al. proposed a novel identity-based protocol [26], the lightweight protocol is based on ECC and can also perform batch message verification; the security analysis shows the protocol can achieve vehicle anonymity.

IBC also has certain problems, PKG keeps both the master key and synthesizes the user's private key, so it is necessary to consider the user key escrow problem [27]. To solve the problem of certificate management and key escrow, the certificateless-based signature technique is proposed. Horng et al. [28] proposed a certificateless aggregated signature scheme that can save a lot of computation, each message in the communication can be mapped to a pseudo-ID, and at the same time can realize conditional privacy protection. To improve the efficiency, Han et al. [7] proposed a certificateless aggregated signature without bilinear pairing, which aggregates individual signatures in messages transmitted by different vehicles into a short signature, and signature checking can meet the security requirements. Samra and Fouzi [29] introduced a certificateless aggregation scheme for traceable ring signatures, aimed at reducing computational overhead. This approach notably diminishes the computational burden associated with signature verification, while simultaneously ensuring conditional privacy protection.

Another privacy problem is the attacker can link the sender by their public key or identity, Liang et al. proposed a protocol based on the Chinese Remainder Theorem (CRT) to solve this problem, this protocol will update its public key before signature, but in this way the update of the key will produce a lot of consumption [30]. Liu et al. proposed a privacy protection protocol based on the elliptic curve Diffie-Hellman problem (ECDH), this protocol uses a hierarchical pseudonym mechanism, which divides pseudonyms into systematic and communication pseudonyms, to protect the vehicles' identities and tracks [31].

III. BACKGROUND

In this section, we introduce the system model, threat model, and referred methods.

A. SYSTEM MODEL

As shown in Figure 2, the protocol of this paper mainly consists of the following four entities: Operating Vehicle (OV), On-Board Unit (OBU), Road Side Unit (RSU), Road Control Center (RCC), and Trust Authority (TA) [6].

1) Trust Authority (TA) is a trusted third-party certification authority that carries out the issuance of trusted credentials to other entities in the VICS to serve as a trust anchor during communication. The TA processes register requests and sends certificates to the RCC and RSU through a wired network.
2) Road Control Center (RCC) is the local road control center, which mainly monitors and schedules the road operation status, as well as monitors the operation

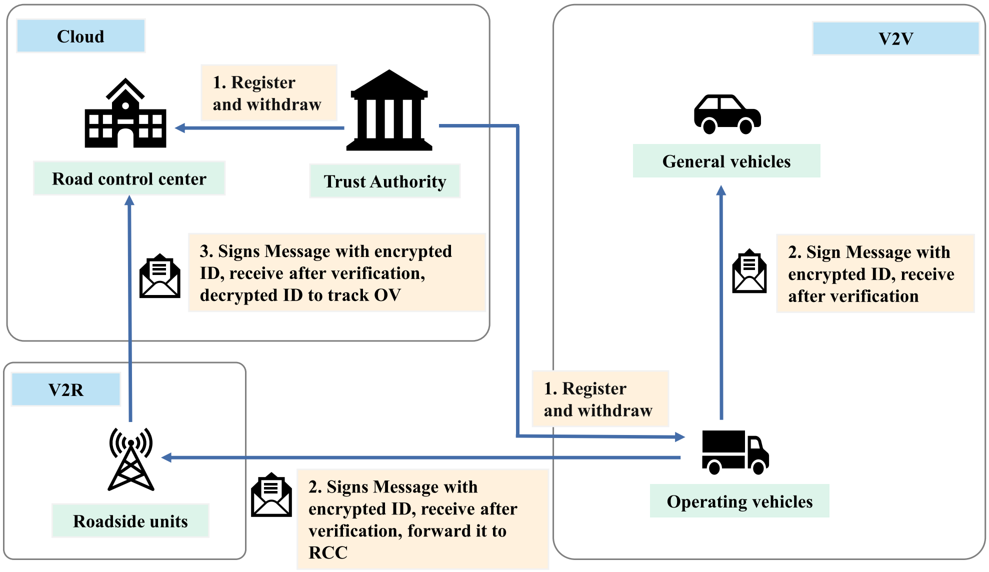
Cloud
1. Register and withdraw
Road control center
Trust Authority
3. Signs Message with encrypted ID, receive after verification, decrypted ID to track OV
V2V
General vehicles
2. Sign Message with encrypted ID, receive after verification
V2R
1. Register and withdraw
Roadside units
2. Signs Message with encrypted ID, receive after verification, forward it to RCC
Operating vehicles

FIGURE 2. System model.

status of the OV belonging to it. The RCC is trusted in the assumptions of this paper.

3) Operating Vehicle's On-Board Unit (OBU), which periodically broadcasts the operating status of OV, including speed, acceleration, load, and position information, to other vehicles and roadside units (RSU) after signature. In order to avoid the disclosure of private keys, the vehicle is equipped with tamper-proof devices (TPD), and it also has a Hardware Security Module (HSM), which can be used for encryption, signing, verification, etc.
4) Roadside Units (RSU), which collect the information after verifying the vehicle signature, perform traffic control and management according to the message content and forward the information to the RCC owning the OV.

B. THREAT MODEL

In this protocol, both OBU and RSU are untrusted entities, the attackers may hijack to launch internal attacks. We define the attackers who launch internal attacks as Type I adversary, who can obtain all the public ones generated by TA System parameters. For example, Type I adversary broadcast false information to suit their interests, affecting the normal operation of other vehicles and RSU. On the other hand, because the communication is in an open environment, the attacker can also launch external attacks. We define the attacker launching external attacks as a type II adversary. The type II adversary can pretend to be a legal identity and launch attacks such as modifying, forging, replaying in the open communication environment, or tracing the intercepted information in the real world by analyzing the true identity of the OV.

Therefore, combined with the adversaries' attack and the need for real-time monitoring of the operating state of the OV, the protocol in this paper needs to satisfy the following requirements:

1) Message authentication and integrity: Ensure that messages periodically sent by OV are verifiable, thus ensuring that the messages have not been tampered with and forged.
2) Conditional privacy protection: On the one hand, the OV must conceal its real identity during the authentication process so that unreliable parties cannot acquire the real identity and related information; on the other hand, when a dispute occurs, only the Trusted Center (TA) and the Road Control Platform (RCC) have access to the real identity of the OV, and the Trusted Center (TA) can revoke the pseudonym certificate of the OV [13].
3) Unlinkability: Attackers cannot extract crucial information from different messages sent by the same users since there is no correlation between messages sent by the same OV.
4) Non-repudiation: OV signed with a pseudonym certificate issued by a Trust Center (TA) and cannot deny the signature.
5) Real-time monitoring: To ensure the safety and management needs of OV, the real-time operating status of OV can be obtained by the RCC owning the OV.

The protocol uses OAEP to achieve indistinguishable security. Optimal Asymmetric Encryption padding (OAEP), which builds a Feistel network containing two Hash functions, the plaintext m filled with random number r and a redundant string of "0" is output, so that the ciphertext encrypted by OAEP has certain indistinct security [32], [33]. Its structure is shown in Figure 3.

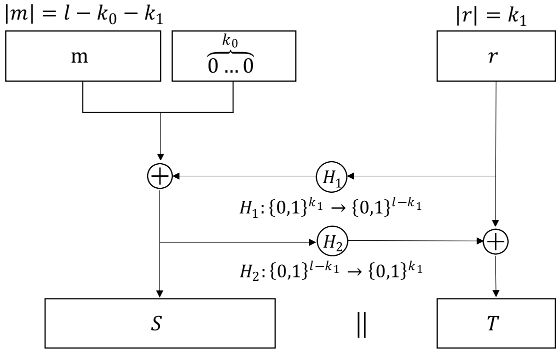
$|m| = l - k_0 - k_1$
m
k_0
0 … 0
$|r| = k_1$
r
H_1
H_1: $\{0,1\}^{k_1} \to \{0,1\}^{l-k_1}$
H_2
H_2: $\{0,1\}^{l-k_1} \to \{0,1\}^{k_1}$
S
||
T

FIGURE 3. The process of OAEP.

The padding process is $OAEP\,(m, r) = (S \parallel T)$, where $S = (m \parallel 0^k) \oplus H_1(r)$, $T = H_2(S) \oplus r$, m is the unencrypted message, r is the random numbers, H_1, H_2 is the hash function.

The protocol in this paper mainly relies on the mathematical hard problems, that is Elliptic Curve Discrete Logarithm Problem (ECDLP).

Definition 1: The Elliptic Curve Discrete Logarithm Problem (ECDLP): Given two random points on a group of elliptic curves in a finite field $P, Q \in G$, which P is the generated element of G, $Q = sP$, $s \in Z_q^*$, $Z_q^* = \{0, 1, \ldots, q-1\}$. Given P, Q, it is difficult to find the value of s with a non-negligible advantage ε in the Probabilistic Polynomial Time (PPT).

The security of the protocol is transformed to solve the mathematical hard problems through security reduction. If the adversary $\mathcal{A}$ can win the game with challenger $\mathcal{C}$ in polynomial time by a non-negligible advantage ε, then the ECDLP problem must be solved in polynomial time. In fact, it is difficult to solve the ECDLP problem, and there is a contradiction, which proves the security of the protocol in this paper.

IV. PROTOCOL DESCRIPTION

In this section, the process of the protocol will be introduced, the protocol in this paper refers to the method proposed by Xiong et al. [34]. There are seven phases in this protocol: setup, registration, pseudonym generation, message signing, verification, batch verification, and tracking. The overall process is shown in Figure 4.

1) OV initiates a registration request to RCC before operation and sends the real ID to RCC.
2) RCC sends OV and RCC's registration requests and information to TA through a secure channel.
3) After verification, TA generates part of the pseudonym certificate according to the information and a traceability list of OV and RCC according to the information. TA returns part of the pseudonym certificate to RCC.
4) RCC verifies the message, injects its preset public key and returns part of the pseudonymous certificate to OV through the security channel.
5) OV verifies the message and generates the complete certificate according to the part of the pseudonym certificate. OV uses OAEP to pad its real ID, randomly selects a pseudonym for signature, and broadcasts messages to other vehicles and RSU.
6) RSU verifies the messages, responds to the message content and forwards the message to the corresponding RCC.
7) After the verification, RCC uses its private key to decrypt the OV's real ID padding with the OAEP and record the operating data of the OV in real-time.

The communication process of this protocol is shown in Figure 5. The protocol symbols and parameters are defined in Table 1.

TABLE 1. Symbol parameter definition.

Notations	Meaning
G	A cyclic group with order q
P	The generator of the cyclic group
p, q	Two large prime numbers
$H_i(\cdot)$	A one-way hash function
PK, s	The master public and private keys of the system
RCC_k	The kth Road Control Center
RID_i	The real identity of ith OV
$PID_{i,j}$	The jth pseudo-identity of ith OV
$SRID_i$	The encrypted real identity of ith OV
$Info_{i,k}$	Correlated data of RCC_k and ith OV
$PKRCC_k, x_k$	The public and private key of RCC_k
$PKA_{i,j}$, $PSa_{i,j}$	The jth partial pseudo-public and private key of ith OV generated by TA
$PKV_{i,j}$, $v_{i,j}$	The jth partial pseudo-public and private key of ith OV generated by itself
T_s , $T_{i,j}$	Timestamp and certificate validity

A. SETUP

In this phase, TA generates the public parameter $para = \{p, q, P, PK, H_1, H_2, H_3, H_4, H_5\}$ to the RCC, RSU, and OV, as follows:

TA chooses a non-singular elliptic curve E and two large prime numbers p, q, E:$y^2 = x^3 + ax + bmod\ p$, $a, b \in Z_p^*$.

A cyclic group G of order q is constructed from points on the elliptic curve E and points at infinity O, TA selected a generator P with order q of group G.

TA randomly selects $s \in Z_q^*$ and computes $PK = s{\cdot}P$, where PK, s are the public and private keys of the system. TA randomly selects the hash function H_1: $\{0, 1\}^{k_1} \to \{0, 1\}^{l-k_1}$, H_2: $\{0, 1\}^{l-k_1} \to \{0, 1\}^{k_1}$, H_3:$G \to \{0, 1\}^n$, H_4: $\{0, 1\}^n \times \{0, 1\}^* \times \{0, 1\}^* \to Z_q^*$, H_5: $\{0, 1\}^n \times \{0, 1\}^* \times \{0, 1\}^* \times \{0, 1\}^* \times \{0, 1\}^* \times \{0, 1\}^* \times \{0, 1\}^* \to Z_q^*$, where n is the length of $RID_{i,j}$, k_0 is the length of the padding random number r, k_1 is the length of the padding "0".

TA publish system parameter $para = \{p, q, P, PK, H_1, H_2, H_3, H_4, H_5\}$.

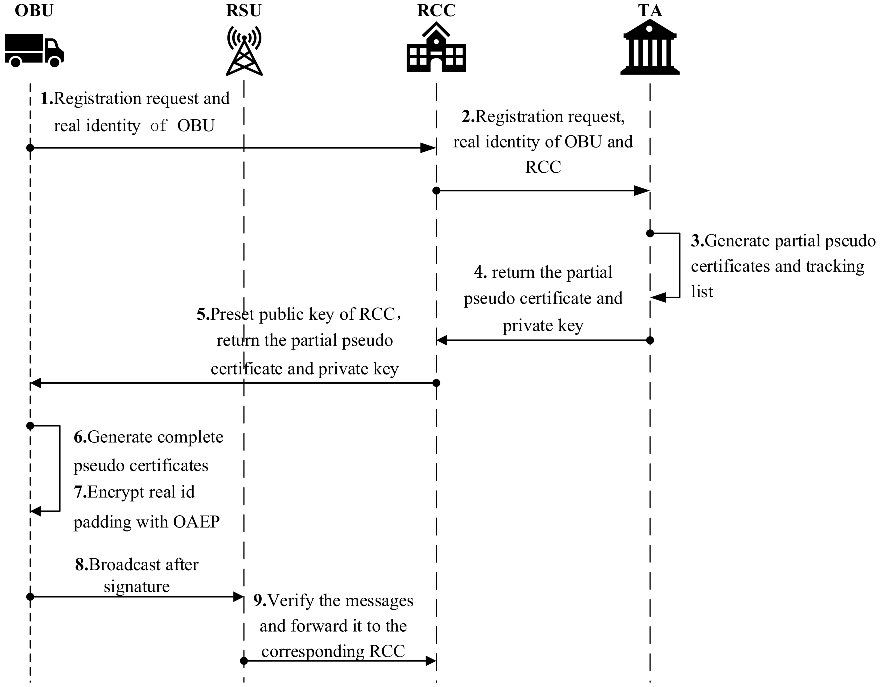
OBU
RSU
RCC
TA
1.Registration request and real identity of OBU
2.Registration request, real identity of OBU and RCC
3.Generate partial pseudo certificates and tracking list
4. return the partial pseudo certificate and private key
5.Preset public key of RCC, return the partial pseudo certificate and private key
6.Generate complete pseudo certificates
7.Encrypt real id padding with OAEP
8.Broadcast after signature
9.Verify the messages and forward it to the corresponding RCC

FIGURE 4. The overview of the protocol process.

B. REGISTRATION

In this phase, OV applies for the pseudonymous certificate from TA through RCC. TA sends $\{PKA_{i,j}, PSa_{i,j}, PID_{i,j}, T_{i,j}, Info_{i,k}\}$ to RCC and generates a traceable list $\{number, time, RCC_k, RID_i, Info_{i,k}\}$. This paper has assumed that RCC and TA are not the communication and that the transmission channel is secure. The process is as follows.

OV sends RID_i to the belonging RCC, and RCC generates $Info_{i,k}$ which only contains the public address of RCC, not involving private information. RCC randomly selects $x_k \in Z_q^*$, $PKRCC_k = x_k \cdot P$, where $PKRCC_k$ and x_k is the public and private key of RCC_k.RCC sends $\{RID_i, RCC_k, Info_{i,k}\}$ and registration request of OV to TA. After verification, TA generates a partial pseudonymous certificate. TA randomly selects $a_{i,j} \in Z_q^*$, and compute:

$$PKA_{i,j} = a_{i,j} \cdot P \tag{1}$$

$$PID_{i,j} = RID_i \oplus H_3\left(a_{i,j} \cdot PK\right) \tag{2}$$

$$w_{i,j} = H_4(PID_{i,j} \parallel T_{i,j} \parallel Info_{i,k}) \tag{3}$$

$$PSa_{i,j} = a_{i,j} + w_{i,j} \cdot s \ mod \ q \tag{4}$$

where $T_{i,j}$ is the certificate validity, $PSa_{i,j}$ is the partial private key generated by TA for OV.

TA sends $\left\{PKA_{i,j}, PSa_{i,j}, PID_{i,j}, T_{i,j}, Info_{i,k}\right\}$ to RCC by a secure channel, then generates a traceable list $\{number, time, RCC_k, RID_i, Info_{i,k}\}$, which include register information of OV and RCC.

RCC presets its public key $PKRCC_k$, which will be used to encrypt RID_i padding with OAEP, RCC sends $\{RCC_k, PKRCC_k, PKA_{i,j}, PSa_{i,j}, PID_{i,j}, T_{i,j}, Info_{i,k}\}$ to OV.

C. PSEUDONYM GENERATION

In this phase, OV generates the other partial of the pseudo key, and OV uses the private key to sign messages.

OV verifies the integrity of $\{RCC_k, PKRCC_k, PKA_{i,j}, PSa_{i,j}, PID_{i,j}, T_{i,j}, Info_{i,k}\}$ and computes if the following formula is valid:

$$PSa_{i,j} \cdot P = PKA_{i,j} + w_{i,j} \cdot PK \tag{5}$$

where $w_{i,j} = H_4(PID_{i,j} \| T_{i,j} \| Info_{i,k})$, generator P is the generator of group G. If the equation is satisfied, OV receives the message; otherwise, reject this message.

OV randomly selects $v_{i,j} \in Z_q^*$, computes $PKV_{i,j} = v_{i,j} \cdot P$, where $PKV_{i,j}$ is the other partial of the pseudo-public key.

D. MESSAGE SIGNING

In this phase, OV uses $PKRCC_k$ to encrypt RID_i padding with OAEP and selects a certificate from $\{PID_{i,j}, PKA_{i,j}, PSa_{i,j}, PKV_{i,j}, v_{i,j}, T_{i,j}\}$. The process is as follows:

OV compute:

$$\begin{aligned} OAEP\,(RID_i, r) &= (S \parallel T) \\ &= ((RID_i \parallel 0^{k_0}) \oplus H_1\,(r) \parallel r \oplus H_2(S)) \end{aligned} \tag{6}$$

$$SRID_i = E_{PKRCC_j}\,(OAEP\,(RID_i, r)) \tag{7}$$

where $S = (RID_i \parallel 0^{k_0}) \oplus H_1\,(r)$, $T = r \oplus H_2(S)$, r is the random number of long k_1, 0^{k_0} is the padding of long 0^{k_0}, $E_{PKRCC_j}(\cdot)$ is using $PKRCC_j$ to encrypt.

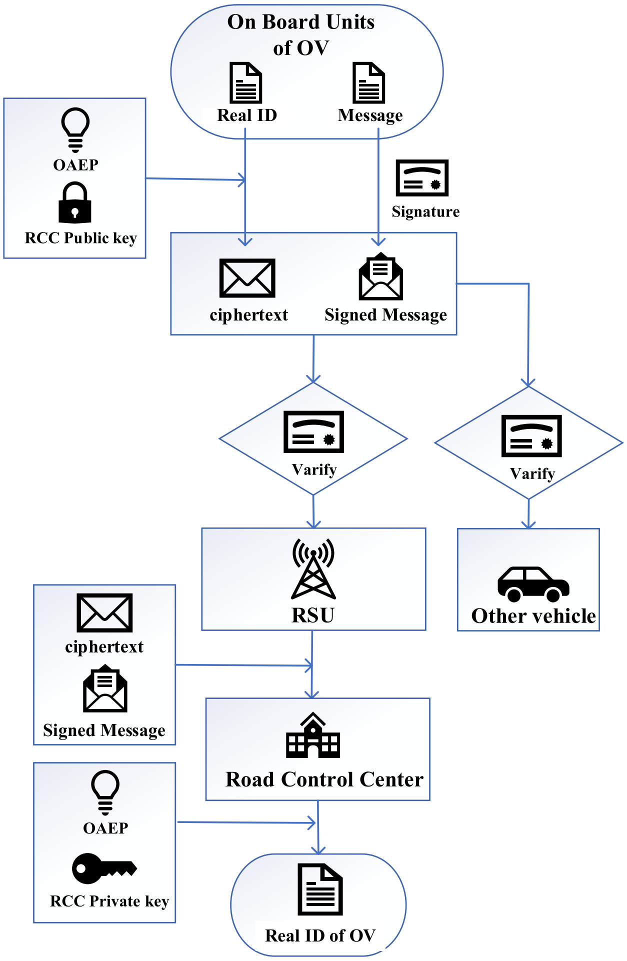

FIGURE 5. Communication process.

OV selects a pseudonymous certificate from $\{PID_{i,j}, PKA_{i,j}, PSa_{i,j}, PKV_{i,j}, v_{i,j}, T_{i,j}\}$ and compute:

$$f_{i,j} = H_5\left(PID_{i,j} \parallel M \parallel PKA_{i,j} \parallel PKV_{i,j} \parallel T_s \parallel SRID_i\right) \tag{8}$$

$$\sigma_{i,j} = PSa_{i,j} + f_{i,j} \cdot v_{i,j} \ mod\ q \tag{9}$$

where M is the plaintext information, $T_{i,j}$ is the pseudonymous certificate validity and T_s is the time stamp.

OV broadcast the signing message $\{SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}\}$.

E. VERIFICATION

In this phase, other entities, such as common vehicles and RSU, can respond to the verified message.

RSU and vehicles receive the message with signing, compute if the following formula is valid:

$$|T_{cur} - T_s| < \delta \tag{10}$$

$$T_{cur} \in T_{i,j} \tag{11}$$

where T_{cur} is the current time. This procedure checks the pseudonym certificate's validity and the signature's freshness. Continue to the next step if the condition is satisfied; otherwise, reject the message.

RSU and vehicles compute if the following formula is valid:

$$w^*_{i,j} = H_4(PID^*_{i,j} \parallel T^*_{i,j} \parallel info^*_{i,k}) = w_{i,j} \tag{12}$$

$$\begin{aligned} f^*_{i,j} &= H_5\left(PID^*_{i,j} \parallel M^* \parallel PKA^*_{i,j} \parallel PKV^*_{i,j} \parallel T^*_s \parallel SRID^*_i\right) \\ &= f_{i,j} \end{aligned} \tag{13}$$

where "$*$" means the parameter is getting from the message. Continue to the next step if the formula is correct; otherwise, reject the message.

RSU and vehicles compute if the following formula is valid:

$$\sigma_{i,j} \cdot P = PKA_{i,j} + w_{i,j} \cdot PK + f_{i,j} \cdot PKV_{i,j} \tag{14}$$

where $w_{i,j} = H_4(PID_{i,j} \| T_{i,j} \| Info_{i,k})$, which is used to prove the legitimacy of the pseudonym certificate. $f_{i,j} = H_5\left(PID_{i,j} \parallel M \| PKA_{i,j} \| PKV_{i,j} \parallel T_s \| SRID_i\right)$, which is used to prove the validity of the signing.

The proof is as follows:

$$\begin{aligned} \sigma_{i,j} \cdot P &= \left(PSa_{i,j} + f_{i,j} \cdot v_{i,j}\right) \cdot P \\ &= \left(a_{i,j} + w_{i,j} \cdot s + f_{i,j} \cdot v_{i,j}\right) \cdot P \\ &= PKA_{i,j} + w_{i,j} \cdot PK + f_{i,j} \cdot PKV_{i,j} \end{aligned} \tag{15}$$

Continue to the next step if the formula is correct; otherwise, reject the message.

F. BATCH VERIFICATION

The RSU checks the certificate validity $T_{i,j}$, and time stamp T_s, then randomly selects $\mathbf{c} = \{c_1, c_2, c_3, \ldots, c_n\}$ and computes:

$$\begin{aligned} \sum_{i=1}^{n} \left(c_i \cdot \sigma_{i,j}\right) \cdot P = \sum_{i=1}^{n} \left(c_i \cdot PKA_{i,j}\right) + \sum_{i=1}^{n} \left(c_i \cdot w_{i,j}\right) \cdot PK \\ + \sum_{i=1}^{n} \left(\left(c_i \cdot f_{i,j}\right) \cdot PKV_{i,j}\right) \end{aligned} \tag{16}$$

if there are invalid messages, pick out and reject them.

The proof is as follows:

$$\begin{aligned} &\sum_{i=1}^{n} \left(c_i \cdot \sigma_{i,j}\right) \cdot P \\ &= \sum_{i=1}^{n} \left(c_i \cdot PSa_{i,j}\right) \cdot P + \sum_{i=1}^{n} \left(c_i \cdot f_{i,j} \cdot v_{i,j}\right) \cdot P \\ &= \sum_{i=1}^{n} \left(c_i \cdot a_{i,j}\right) \cdot P + \sum_{i=1}^{n} \left(c_i \cdot w_{i,j} \cdot s\right) \cdot P + \sum_{i=1}^{n} \left(c_i \cdot f_{i,j} \cdot v_{i,j}\right) \cdot P \\ &= \sum_{i=1}^{n} \left(c_i \cdot PKA_{i,j}\right) + \sum_{i=1}^{n} \left(c_i \cdot w_{i,j}\right) \cdot PK + \sum_{i=1}^{n} \left(\left(c_i \cdot f_{i,j}\right) \cdot PKV_{i,j}\right) \end{aligned} \tag{17}$$

G. TRACKING

This phase includes the real-time tracking of OV status by RCC and tracking the real identity of OV belonging to RCC by TA after a conflict. The specific steps are as follows:

1) REAL-TIME TRACKING BY RCC

After RSU transmits the message to the RCC according to the $Info_{i,k}$, RCC decrypts the real identity of OV. The

verification step of RCC is the same as the RSU and vehicles, then RCC computes:

$$\begin{aligned} D_{x_k}(SRID_i) &= OAEP(RID_i, r) = (S \parallel T) \\ &= \left(\left(RID_i \parallel 0^{k_0}\right) \oplus H_1(r) \parallel r \oplus H_2(S)\right) \end{aligned} \tag{18}$$

$$r = T \oplus H_2(S) \tag{19}$$

$$Z = (RID_i \| 0^{k_0}) = H_1(r) \oplus S \tag{20}$$

where $D_{x_k}(\cdot)$ denotes using the private key of RCC to decrypt the padding real identity by OAEP, r is the random number of lengths k_1, $Z[n, n+1, \ldots, n+k_0-1]$ is the "0" filled with k_0. The real identity $RID_i = Z[0, 1, \ldots, n-1]$.

2) TRACKING BY TA

After a conflict, TA can track the real identity of OV belonging to RCC. TA gets the OV's $PID_{i,j}$ from the conflict message and computes:

$$\begin{aligned} RID_i &= PID_{i,j} \oplus H_3\left(a_{i,j} \cdot P \cdot s\right) \\ &= PID_{i,j} \oplus H_3\left(PKA_{i,j} \cdot s\right) \end{aligned} \tag{21}$$

where s is the system private key, $PKA_{i,j}$ is the jth partial pseudo-public key of ith OV. Then, TA can query $\{number, RCC_k, RID_i, Info_{i,k}\}$, output the OV's RID_i, its road control center RCC_k, and related registration information $Info_{i,k}$.

The above is the complete protocol process, as shown in Figure 6.

V. SECURITY OF THE PROTOCOL

This section mainly analyzes the security of the protocol by security reduction, which is based on the proof of contradiction in mathematics. The security of the cryptographic algorithm is transformed to solve the mathematical hard problems, such as the Discrete Logarithm Problem (DLP) and the Elliptic Curve Discrete Logarithm Problem (ECDLP), through security reduction [35]. Cracking the cryptographic algorithm would mean that mathematical hard problems can be solved, which is currently impossible. Security reduction is achieved through a game between challenger and adversary in a certain model, such as the Standard Model and Random Oracle model (RO). The Random Oracle model (RO) is used to prove the security of the protocol based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The RO is a black box model with a polynomial number of inputs and random and uniformly distributed outputs [36]. The demonstration method of the security proof refers to three papers [9], [34], and [37] and further analyzes the functions realized by the protocol.

A. SECURITY PROOF

Game: The security of the protocol is proved by the Game between challenger $\mathcal{C}$ and adversary $\mathcal{A}$. Based on the network model and the capability of the adversary, the security model of the scheme in this paper is set up, and the Game interaction is as follows:

Definition 2: Based on the assumption of ECDLP, under the Random Oracle model (RO), the protocol can achieve unforgeability under an adaptive chosen message attack.

Assuming challenger $\mathcal{C}$ can solve the ECDLP problem, then adversary $\mathcal{A}$ can be used as a subroutine to solve the ECDLP problem, given the ECDLP problem instance. $(P, Q) \in G$, $Q = sP$, $s \in Z_q^*$, $Z_q^* = \{0, 1, \ldots, q-1\}$, the goal of challenger $\mathcal{C}$ is to compute s.

Setup: Challenger $\mathcal{C}$ sets $Q = sP$, randomly selects $s \in Z_q^*$, calculates public key $PK = Q$, and sends system public parameter $para = \{p, q, P, PK, H_1, H_2, H_3, H_4, H_5\}$ to adversary $\mathcal{A}$. Challenger $\mathcal{C}$ builds the empty list L_{H_i}, $i = 3, 4, 5$.

Queries:

1) H_3 oracle query: adversary $\mathcal{A}$ makes H_3 query, and challenger $\mathcal{C}$ checks if the tuple $< \Gamma, \tau >$ exists in the list L_{H_3}. If it does, challenger $\mathcal{C}$ returns τ to adversary $\mathcal{A}$. Otherwise, challenger $\mathcal{C}$ randomly selects $\tau \in \{0, 1\}^n$ to store tuple $< \Gamma, \tau >$ in list L_{H_3} and returns τ to adversary $\mathcal{A}$.
2) H_4 oracle query: adversary $\mathcal{A}$ makes an H_4 query with the anonymous name $PID_{i,j}$, Challenger $\mathcal{C}$ checks whether the tuples $< PID_{i,j}, T_{i,j}, Info_{i,k}, \tau >$ exist in list L_{H_4}. If it does, challenger $\mathcal{C}$ returns τ to adversary $\mathcal{A}$. Otherwise, challenger $\mathcal{C}$ randomly selects $\tau \in \{0, 1\}^n$ to store the tuple $< \Gamma, \tau >$ into list L_{H_4} and returns τ to adversary $\mathcal{A}$.
3) H_5 query: adversary $\mathcal{A}$ makes H_5 query with anonymous messages and challenger $\mathcal{C}$ checks whether the tuples $< SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}, \tau >$ exists in list L_{H_5}. If it does, challenger $\mathcal{C}$ returns τ to adversary $\mathcal{A}$. Otherwise, challenger $\mathcal{C}$ randomly selects $\tau \in \{0, 1\}^n$ to store tuples $< SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}, \tau >$ into list L_{H_5} and returns τ to adversary $\mathcal{A}$.
4) Signature query: adversary $\mathcal{A}$ inputs M, challenger $\mathcal{C}$ randomly selects $\alpha_i, \beta_i \in Z_q^*$, $PKV_{i,j}$, $SRID_i \in \{0, 1\}^n$, then compute:

$$PKA_{i,j} = \sigma_{i,j} \cdot P - \alpha_i \cdot PK - \beta_i \cdot PKV_{i,j} \tag{22}$$

$$PID_{i,j} = RID_{i,j} \oplus H_3\left(PKA_{i,j} \cdot s\right) \tag{23}$$

Challenger $\mathcal{C}$ adds to $< PID_{i,j}, T_{i,j}, Info_{i,k}, \tau >$ to L_{H_4}, adds $< SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}, \tau >$ to L_{H_5}, and returns the signature message $\{SRID_i, PID_{i,j},$

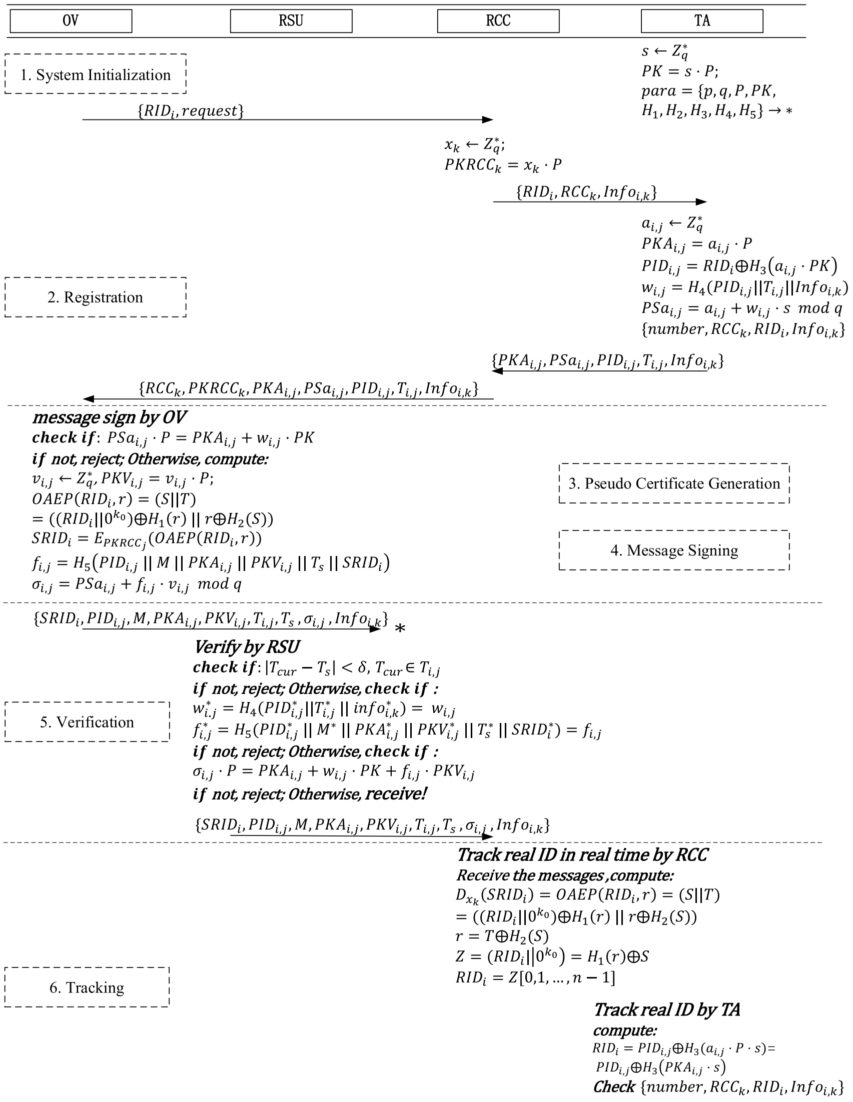
OV
RSU
RCC
TA
1. System Initialization
$s \leftarrow Z_q^*$
$PK = s \cdot P;$
$para = \{p, q, P, PK,$
$H_1, H_2, H_3, H_4, H_5\} \rightarrow *$
$\{RID_i, request\}$
$x_k \leftarrow Z_q^*;$
$PKRCC_k = x_k \cdot P$
$\{RID_i, RCC_k, Info_{i,k}\}$
$a_{i,j} \leftarrow Z_q^*$
$PKA_{i,j} = a_{i,j} \cdot P$
$PID_{i,j} = RID_i \oplus H_3(a_{i,j} \cdot PK)$
$w_{i,j} = H_4(PID_{i,j} || T_{i,j} || Info_{i,k})$
$PSa_{i,j} = a_{i,j} + w_{i,j} \cdot s \ mod\ q$
$\{number, RCC_k, RID_i, Info_{i,k}\}$
2. Registration
$\{PKA_{i,j}, PSa_{i,j}, PID_{i,j}, T_{i,j}, Info_{i,k}\}$
$\{RCC_k, PKRCC_k, PKA_{i,j}, PSa_{i,j}, PID_{i,j}, T_{i,j}, Info_{i,k}\}$
message sign by OV
check if: $PSa_{i,j} \cdot P = PKA_{i,j} + w_{i,j} \cdot PK$
if not, reject; Otherwise, compute:
$v_{i,j} \leftarrow Z_q^*, PKV_{i,j} = v_{i,j} \cdot P;$
$OAEP(RID_i, r) = (S||T)$
$= ((RID_i||0^{k_0}) \oplus H_1(r) \,||\, r \oplus H_2(S))$
$SRID_i = E_{PKRCC_j}(OAEP(RID_i, r))$
$f_{i,j} = H_5(PID_{i,j} \,||\, M \,||\, PKA_{i,j} \,||\, PKV_{i,j} \,||\, T_s \,||\, SRID_i)$
$\sigma_{i,j} = PSa_{i,j} + f_{i,j} \cdot v_{i,j} \ mod\ q$
3. Pseudo Certificate Generation
4. Message Signing
$\{SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}\}$ *
Verify by RSU
check if: $|T_{cur} - T_s| < \delta, T_{cur} \in T_{i,j}$
if not, reject; Otherwise, check if :
$w_{i.j}^* = H_4(PID_{i,j}^* || T_{i,j}^* \,||\, info_{i,k}^*) = w_{i,j}$
$f_{i,j}^* = H_5(PID_{i,j}^* \,||\, M^* \,||\, PKA_{i,j}^* \,||\, PKV_{i,j}^* \,||\, T_s^* \,||\, SRID_i^*) = f_{i,j}$
if not, reject; Otherwise, check if :
$\sigma_{i,j} \cdot P = PKA_{i,j} + w_{i,j} \cdot PK + f_{i,j} \cdot PKV_{i,j}$
if not, reject; Otherwise, receive!
5. Verification
$\{SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}\}$
Track real ID in real time by RCC
Receive the messages ,compute:
$D_{x_k}(SRID_i) = OAEP(RID_i, r) = (S||T)$
$= ((RID_i||0^{k_0}) \oplus H_1(r) \,||\, r \oplus H_2(S))$
$r = T \oplus H_2(S)$
$Z = (RID_i||0^{k_0}) = H_1(r) \oplus S$
$RID_i = Z[0,1, \ldots, n-1]$
6. Tracking
Track real ID by TA
compute:
$RID_i = PID_{i,j} \oplus H_3(a_{i,j} \cdot P \cdot s) =$
$PID_{i,j} \oplus H_3(PKA_{i,j} \cdot s)$
Check $\{number, RCC_k, RID_i, Info_{i,k}\}$

FIGURE 6. Specific protocol process.

$M, PKA_{i,j}, PKV_{i,j}, T_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}\}$ to the adversary $\mathcal{A}$. Then, the equation below should be satisfied.

$$\begin{aligned}\sigma_{i,j} \cdot P &= PKA_{i,j} + \alpha_i \cdot PK + \beta_i \cdot PKV_{i,j} \\ &= \sigma_{i,j} \cdot P - \alpha_i \cdot PK - \beta_i \cdot PKV_{i,j} + \alpha_i \cdot PK + \beta_i \cdot PKV_{i,j} \\ &= \sigma_{i,j} \cdot P \end{aligned} \tag{24}$$

Output: Adversary $\mathcal{A}$ inputs the forged message M' and outputs the forged message signature:

$$\{SRID_i', PID_{i,j}', M', PKA_{i,j}', PKV_{i,j}', T_{i,j}', T_s', \sigma_{i,j}', info_{i,j}'\}$$

challenger $\mathcal{C}$ can verify:

$$\sigma_{i,j}' \cdot P = PKA_{i,j}' + \alpha_i' \cdot PK + \beta_i' \cdot PKV_{i,j}' \tag{25}$$

According to the forgery lemma [38], adversary $\mathcal{A}$ can output another signature message within a probabilistic polynomial-time:

$$\{SRID_i', PID_{i,j}', M'', PKA_{i,j}', PKV_{i,j}', T_{i,j}'', T_s'', \sigma_{i,j}'', info_{i,j}'\}$$

Then, the adversary can get the equation (26).

$$\sigma_{i,j}'' \cdot P = PKA_{i,j}' + \alpha_i'' \cdot PK + \beta_i'' \cdot PKV_{i,j}' \tag{26}$$

Equation (27) can be obtained by equation (26) - (25).

$$\begin{aligned}\left(\sigma_{i,j}'' - \sigma_{i,j}'\right) \cdot P &= PKA_{i,j}' + \alpha_i'' \cdot PK + \beta_i'' \cdot PKV_{i,j}' \\ &\quad - \left(PKA_{i,j}' + \alpha_i' \cdot PK + \beta_i' \cdot PKV_{i,j}'\right) \\ &= \left(\alpha_i'' - \alpha_i'\right) \cdot PK + \left(\beta_i'' - \beta_i'\right) \cdot PKV_{i,j}' \\ &= \left(\alpha_i'' - \alpha_i'\right) \cdot s \cdot P + \left(\beta_i'' - \beta_i'\right) \cdot v_{i,j}' \cdot P \end{aligned} \tag{27}$$

Then

$$s = \frac{\left(\sigma_{i,j}{}'' - \sigma'_{i,j}\right) - \left(\beta_i{}'' - \beta'_i\right) \cdot v'_{i,j}}{\left(\alpha_i{}'' - \alpha'_i\right)} \tag{28}$$

where adversary $\mathcal{A}$ can obtain all the parameters in equation (28), challenger $\mathcal{C}$ can output the solution s of the ECDLP problem with a non-negligible advantage ε', but it contradicts the premise that the ECDLP problem is difficult.

As a result, the protocol's signature method in this paper is secure under the RO model.

B. SECURITY ANALYSIS

This section analyzes the security features of the protocol and compares them with other existing protocols.

1) MESSAGE AUTHENTICATION AND INTEGRITY

According to the proof of Definition 2, under the premise of ECDLP, an adversary cannot forge a valid signature in probabilistic polynomial time. The receiver can compute $\sigma_{i,j}{\cdot}P = PKA_{i,j}+w_{i,j}{\cdot}PK+f_{i,j}{\cdot}PKV_{i,j}$ to verify the authentication and integrity of the message.

2) CONDITIONAL PRIVACY PROTECTION

This includes vehicle privacy protection and vehicle traceability [13].

- *Vehicle privacy protection:* In the process of communication, TA generates $PID_{i,j} = RID_i \oplus H_3(a_{i,j} \cdot PK)$ based on OV's real identity. The adversary cannot get the $a_{i,j}$ generated by TA, and it is hard to solve the ECDLP to obtain $a_{i,j}$ from $PKA_{i,j}$, Thus, the adversary cannot find out the OV's real identity.
- *Vehicle traceability:* If a conflict occurs on the OV's message during the communication, TA can obtain the real identity of the OV from the pseudonymous identity $PID_{i,j}$ that gets from signature message $\{SRID_i, PID_{i,j}, M, PKA_{i,j}, PKV_{i,j}, T_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}\}$, and use the system private key s to find out the real identity of the OV by $RID_i = PID_{i,j} \oplus H_3(PKA_{i,j} \cdot s)$. TA can also trace the RCC associated with the OV according to $\{number, RCC_k, RID_i, Info_{i,k}\}$.

3) UNLINKABILITY

This mainly prevents the adversary from associating any signature message with the same OV. The OV randomly selects a pseudonym to sign during the communication, and the adversary cannot solve the ECDLP problem to obtain the private key s of the system. The specific identity cannot be determined by $PID_{i,j}$. The OV's real identity padding with OAEP has IND-CPA (indistinguishable security under chosen plaintext attack) level security and ensures each $SRID_i$ is different due to the random number r in the $SRID_i = E_{PKRCC_j}(OAEP\,(RID_i, r))$.

4) RESISTANT ATTACKS

This part will analyze the security of the protocol under common attacks [39].

- *Impersonation attack:*To cheat other vehicles and RSU, The adversary needs to generate a fake message $\{SRID'_i, PID'_{i,j}, M', PKA'_{i,j}, PKV'_{i,j}, T'_{i,j}, T'_s, \sigma'_{i,j}, info'_{i,j}\}$ which satisfy $\sigma'_{i,j}{\cdot}P = PKA'_{i,j}+\alpha'_i{\cdot}PK+\beta'_i{\cdot}PKV'_{i,j}$, but according to the security proof, the adversary cannot generate this message. So, this protocol can withstand the impersonation attack.
- *Replay attack:*The adversary cheats the vehicles by sending a valid but used message. To deal with this problem, the $\{T_{i,j}, T_s\}$, that is the certificate validity and time stamp, are included in the message's signature that was sent by the OV. The receiver receives the message only when the receiving time is $|T_{cur} - T_s| < \delta$.
- *Tampering attack:*According to Definition 2, it is difficult to tamper with an authenticable signature message under the ECDLP problem. The vehicles and RSU can verify the integrity of the message by $\sigma_{i,j}{\cdot}P = PKA_{i,j}+w_{i,j} \cdot PK + f_{i,j} \cdot PKV_{i,j}$.
- *Man-in-the-middle attack:*In the message authentication phase, the protocol can provide identity verification for all communication entities in the system to prevent man-in-the-middle attacks.

5) REAL-TIME TRACKING

The OV presets the cryptography public key of the RCC and encrypts RID_i padding with OAEP, the process is $SRID_i = E_{PKRCC_j}(OAEP\,(RID_i, r))$. After the RSU transmits the message to the RCC owning the OV, the RCC can decrypt $SRID_i$ by the private key to obtain the RID_i of the OV to realize real-time tracking of the OV.

The protocol proposed in this paper is compared with the function achieved by the other protocol. The results are shown in Table 2. S1 represents authentication and integrity, S2 represents conditional privacy protection, S3 represents unlinkability, S4 represents the resistance to various attacks, including impersonation attacks, replay attacks, tampering attacks and man-in-the-middle attacks, S5 represents real-time tracking. Most of the protocols can realize the basic security and privacy requirements, but cannot realize the real-time traceability of the OV.

VI. PERFORMANCE ANALYSIS

In this section, the performance of this protocol is evaluated with existing protocols [6], [8], [13], [15], [40] about computing and communication overhead, and the service rate of RSU is analyzed. The protocols to be compared are based on ID [6], [13], PKI [15], [40], and certificateless signature [8] protocols, and the protocols using methods are based on bilinear pairing encryption [6], [15] and elliptic curve encryption [8], [13], [40]. This paper uses the MIRACL

TABLE 2. **Protocol function comparison.**

Protocol	S1	S2	S3	S4	S5
Horng *et al.*[15]	√	√	√	√	×
Tzeng *et al.* [6]	√	√	√	√	×
He *et al.* [13]	√	√	√	√	×
Gowri *et al.* [8]	√	√	√	√	×
Cui *et al.* [40]	√	√	√	√	×
The proposed	√	√	√	√	√

library to achieve the simulation of this paper and the control protocol.

The compared protocol mainly uses elliptic curve encryption and bilinear pairing encryption. Construct a bilinear pair encryption algorithm $e' : G_1 \times G_1 \rightarrow G_T$ with a security level of 80 bit, where G_1 is an addition group on a singular elliptic curve $E' : y^2 = x^3 + x \, mod \, p'$. Construct an elliptic curve encryption algorithm with a security level of 80bit, where G is an addition group on q order non-singular elliptic curve $E : y^2 = x^3 + ax + b \, mod \, p$, p, q is a large prime number with the length of 160 bit and $a, b \in Z_p^*$.

A. COMPUTATION COST

We analyze the basic operation cost of our protocol and compared protocols by the cryptography library MIRACL. The encryption and decryption operation used the SM2 algorithm published in China, which is based on ECC. The basic operation was referred to [13], as shown in Table 3.

TABLE 3. **Operational definition and AVG.COST.**

Notation	Descriptions	Avg. cost (ms)
T_{par}	A bilinear paring (BP)operation, $e'(S', T'), S', T' \in G_1$	4.211
T_{bp-m}	A scale multiplication operation $x' \cdot P'$ related to BP, $x' \in Z_{q'}^*, P' \in G_1$	1.7090
T_{bp-a}	A point addition operation $S' + T'$ related to BP	0.0071
T_{ecc-m}	A scale multiplication operation $x \cdot P$ related to ECC, $x \in Z_q^*, P \in G$	0.4420
T_{ecc-sm}	A small-scale multiplication operation $v_i \cdot P$ related to ECC, $v_i \in [1, 2^t]$, t is the small integer	0.0138
T_{ecc-a}	A point addition operation $S + T$ related to ECC, $S, T \in G$	0.0018
T_{mtp}	A Map-to-Point hash operation related to BP	4.406
T_h	A general hash function operation	0.0001
$T_{E_{ecc}}$	The execution time of SM2 encrypt related to ECC	3.536
$T_{D_{ecc}}$	The execution time of SM2 decrypt related to ECC	1.725

In this protocol, executing one signature requires two elliptic curve scale multiplications, four general hash operations, one elliptic curve encryption, and the signature computation cost is about $2T_{ecc-m} + 4T_h + T_{E_{ecc}} \approx 4.4204 \, ms$. Executing one verification requires two elliptic curve scale multiplication, one elliptic curve point addition, two general hash operations and the verification cost is $2T_{ecc-m} + T_{ecc-a} + 2T_h \approx 0.886ms$. In the batch message verification, it is assumed that there are n different messages, and the cost of the verification is $(2+n) \, T_{ecc-m} + (n) \, T_{ecc-a} + (2n) \, T_h \approx 0.444n + 0.884 \, ms$. In addition, the RCC needs to obtain the OV reality identity to realize real-time tracking of the communication data of the OV. The RCC's verification needs to add an elliptic curve decryption operation and two hash operations based on the RSU's verification, and the cost is about $2T_{ecc-m} + T_{ecc-a} + 4T_h + T_{D_{ecc}} \approx 2.6112 \, ms$. Similarly, the cost of other protocols in signature, single, and batch message verification can be obtained, as shown in Table 4. The result is shown in Figure 7. Compared to other protocols, the signature consumption of the protocol is not the most efficient, our protocol's signature computation performance is better than Horng et al. [15] which is based on bilinear pairing and PKI and Tzeng et al. [6] which is based on bilinear pairing and IBC. But the signature efficiency is worse than other protocols that used ECC, that is, He et al. [13] based on IBC, Thumbur et al. [8] based on certificateless signature, and Cui et al. [40] based on PKI.

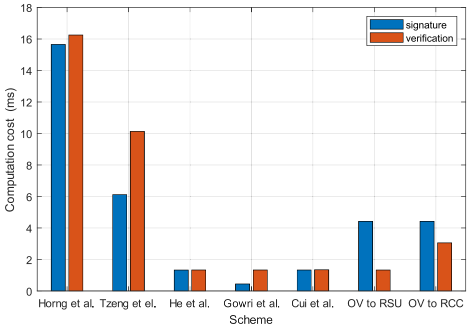

FIGURE 7. **Comparison of the message signature and verification cost.**

The reason is that the protocol in this paper encrypts the OV's real identity padding with OAEP by SM2, which causes higher signature consumption than other protocols using ECC. By using this method, OV's each message will not leak the real identity, and the ciphertext including real identity in each message is different.

In addition, Figure 8 shows the number of messages verified by all protocols in 300ms. As shown in the figure, in our protocol, the number of messages verified by RSU in 300ms is about 673, which is the largest among the compared protocols. So, the verification of OV to RSU has the highest efficiency compared with the other protocols. However, the verification of OV to RCC has a lower efficiency. That is because the RCC has an additional decrypt process, RCC decrypts the OV's real identity padding with OAEP by

TABLE 4. **Comparison of computational efficiency.**

Protocols		Signature (ms)	Single verification (ms)	Batch verification (ms)
Horng *et al.* [15]		$4T_{bp-m} + T_{bp-a} + 2T_{mtp} + T_h \approx 15.6552$	$2T_{par} + 2T_{bp-m} + T_{bp-a} + T_{mtp} + T_h \approx 16.2532$	$2T_{par} + 2nT_{bp-m} + nT_{bp-a} + nT_{mtp} + nT_h \approx 8.422 + 7.8312n$
Tzeng *et al.* [6]		$T_{bp-m} + T_{mtp} \approx 6.115$	$2T_{par} + T_{bp-m} + 2T_h \approx 10.1312$	$2T_{par} + (2n+1)T_{bp-m} + (2n)T_h \approx 10.131 + 3.4182n$
He *et al.* [13]		$3T_{ecc-m} + 3T_h \approx 1.3263$	$3T_{ecc-m} + 2T_{ecc-a} + 2T_h \approx 1.3298$	$(n+2)T_{ecc-m} + (2n)T_{ecc-sm} + (3n-1)T_{ecc-a} + 2nT_h \approx 0.8822 + 0.4752n$
Gowri *et al.* [8]		$T_{ecc-m} + 2T_h \approx 0.4422$	$3T_{ecc-m} + 2T_{ecc-a} + 2T_h \approx 1.3298$	$(2n+1)T_{ecc-m} + (3n-1)T_{ecc-a} + (2n)T_h \approx 0.4402 + 0.8896n$
Cui *et al.* [37]		$3T_{ecc-m} + 3T_h + T_{ecc-a} \approx 1.3281$	$3T_{ecc-m} + T_{ecc-sm} + 2T_{ecc-a} + 2T_h \approx 1.3436$	$(n+2)T_{ecc-m} + (n)T_{ecc-sm} + (2n)T_{ecc-a} + (2n)T_h \approx 0.884 + 0.4596n$
The proposed	OV to RSU	$2T_{ecc-m} + 4T_h + T_{E_{ecc}} \approx 4.4204$	$3T_{ecc-m} + T_{ecc-a} + 2T_h \approx 1.328$	$(2+n)T_{ecc-m} + (n)T_{ecc-a} + (2n)T_h \approx 0.884 + 0.444n$
	OV to RCC	$2T_{ecc-m} + 4T_h + T_{E_{ecc}} \approx 4.4204$	$3T_{ecc-m} + T_{ecc-a} + 4T_h + T_{D_{ecc}} \approx 3.0532$	$(2+n)T_{ecc-m} + (n)T_{ecc-a} + (4n)T_h + (n)T_{D_{ecc}} \approx 0.884 + 2.1812n$

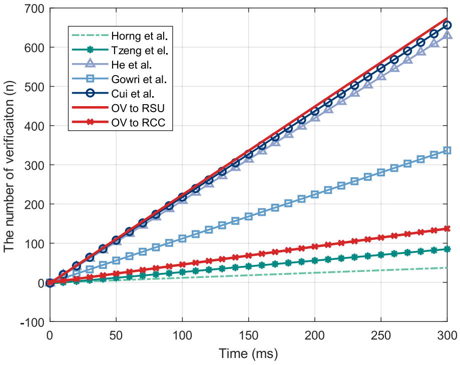

FIGURE 8. **The number of verifications in 300 *ms*.**

SM2 to track the OV's status in real-time, but RSU does not need to.

B. COMMUNICATION COST

This section compared the communication cost of the proposed protocol with others. To ensure a security level of 80 bits, the protocol selects p' (64 bytes, 512 bits) and p (20 bytes, 160 bits) for bilinear pairing and elliptic curve. The element size in G_1 and G is 128 bytes (1024 bits) and 40 bytes (320 bits), the general hash function and time stamp are 20 bytes (160 bits) and 4 bytes (32 bits), and the real identity size of the OV is 20 bytes (160 bits) [13]. According to the standard of SM3 hash algorithm and SM2 elliptic curve encryption, the ID is 64 bytes (512 bits) after padding with OAEP, and 64 +96 = 160 bytes (1280 bits) after SM2 encryption.

The signature message structure of the proposed protocol sent by the OV is $\{SRID_i, PID_{i,j}, PKA_{i,j}, PKV_{i,j}, T_{i,j}, T_s, \sigma_{i,j}, Info_{i,k}\}$, where $PID_{i,j}, \sigma_{i,j} \in Z_q^*, PKA_{i,j}, PKV_{i,j} \in G, T_{i,j}, T_s$ is the time stamp, $Info_{i,k}$ is the Correlated data of RCC_k and i th OV which size is 20 bytes. Then, the communication consumption of a message sent by the OV is $160 + 40 \times 2 + 20 \times 2 + 4 \times 2 + 20 = 308 bytes$. The communication messages of other protocols can be obtained, as shown in Table 5.

TABLE 5. **Comparison of transmission cost.**

Protocol	Single message communication (bytes)	Batch messages communication (bytes)
Horng *et al.* [15]	384	384n
Tzeng *et al.* [6]	388	388n
He *et al.* [13]	144	144n
Gowri *et al.* [8]	184	184n
Cui *et al.* [40]	144	144n
The proposed	308	308n

Table 5 shows the cost of different protocols during the message communication. From Table 5, It is clear that the communication consumption of each message is 308 bytes, which is lighter than that of Horng et al. 384 bytes [15] and Tzeng et al. 388 bytes [6], which is based on bilinear pairing. But our protocol has more consumption than others which is based on ECC. The reason is the additional data $SRID_i$, which is 160 bytes, has to been transmit during the communication process, and this will help RCC to track the anonymous OV in real time at the cost of 160 bytes.

C. RSU SERVING CAPABILITY

When the OV enters the communication range of RSU, it conducts identity authentication with RSU. After successful authentication, the OV can obtain the location information and RCC guidance information (such as the accident information, traffic flow information) within the range of RSU. OV broadcasts its status information to RSU every 100-300 *ms* [41]. The service rate of RSU describes the number of services that can be completed by a single service channel in the system and reflects the ability of RSU to process messages.

In the proposed protocol, the signature time of OV is $T_{sign} = 2T_{ecc-m} + 4T_h + T_{E_{ecc}} \approx 4.4204\ ms$, the verification time of RSU is $(2+n)\,T_{ecc-m} + (n)\,T_{ecc-a} + (2n)\,T_h \approx 0.884 + 0.444 n ms$. A Single message verification time is $3T_{ecc-m} + T_{ecc-a} + 2T_h \approx 1.328\ ms$.

According to queuing theory, $T_{sign} > T_{ver}$, which means the server rate is less than the server time, then the queue system is stable [42]. According to the [16], the server rate of RSU can be defined as:

$$R_{ser} = \frac{P^* \cdot T_{ver} \cdot r}{v \cdot k} \tag{29}$$

where v is the vehicle velocity, r is the range of RSU, k is the density of the vehicle, and P^* is the possibility of the vehicle successfully receiving the message.

According to the Greenshields model [17], which is a microscopic model of general traffic flow, the relationship between velocity and density is:

$$v = v_m \left(1 - \frac{k}{k_j}\right) \tag{30}$$

$$k = \left(1 - \frac{v}{v_m}\right) k_j \tag{31}$$

where v_m is the free-flow velocity, which means the traffic flow is small and the velocity is independent of upstream and downstream conditions, k_j is the jammed-flow density, which is the density of occurring traffic jam, the speed is nearly to 0, r is the range of RSU, N is the number of vehicles.

According to equations (29), (31), the relationship between the N, P^*, and R_{ser} can be obtained:

$$R_{ser} = \frac{P^* \cdot T_{ver} \cdot r}{k_j \left(1 - \frac{v}{v_m}\right) \cdot v} \tag{32}$$

We assume the OV's operating speed ranges from 10 m/s to 20 m/s (36 km/h to 72 km/h), the range of speed limit is 64-87 km/h (40-55 mi/h) [43]. The range of RSU r is 1000 m, and the jammed-flow density of a single lane is 0.118 veh/m/ln (190 veh/mi/ln) [44]. Assume the road has two lanes, $k_j = 0.236$ veh/m, then the maximum number of vehicles in this section is 236 vehicles. The relationship of N, P^* and R_{ser} is:

$$R_{ser} = 1.328 \times \frac{P^*}{0.236 \cdot v \cdot \left(1 - \frac{v}{24}\right)} \tag{33}$$

Figure 9 shows the relationship under the parameters above.

As we can see from Figure 9, when the probability P^* is at a fixed value, the RSU service rate is at a peak when the velocity is about 12 m/s. With the velocity increased the RSU service rate is down. The reason is when the density of vehicles is down, the vehicles' velocity will increase, which allows the vehicle to spend less time within the RSU range.

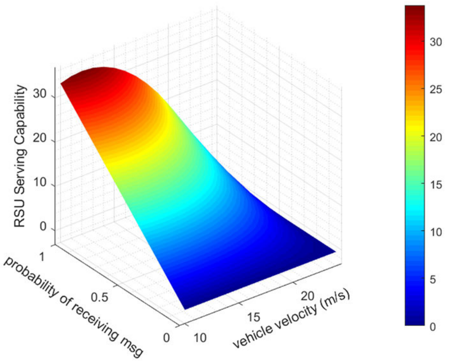

FIGURE 9. Service rate of RSU.

According to our result in Figure 8, the RSU can verify n signatures in $0.884 + 0.444 n ms$, which can verify 673 messages in 300 ms, an OV can sign a message in 4.4204 ms, which can sign 67 messages in 300 ms and the verification time is less than the signature, which means the OV's message will be processed by RSU timely. In addition, the RSU serving rate is at a peak when the velocity reaches 12 m/s. At this time, the density is 0.0944 veh/m, so there are 94 vehicles in the range of RSU. The last point is when the velocity is 0 m/s, the jammed-flow density is 0.236 veh/m and there are 236 vehicles in the range of RSU. According to our result, RSU can verify 673 vehicles in 300 ms, which can satisfy the situation above.

As a result, we conclude that the proposed protocol can satisfy the system requirement. The above analysis is based on the assumption that the vehicle will successfully receive the message 100% of the time. Therefore, we will have a good service rate when the vehicles have a higher possibility of successfully receiving the message.

VII. CONCLUSION

In this paper, we proposed a real-time traceable authentication protocol with indistinguishable security for anonymous operating vehicles (OV) in Vehicle-Infrastructure Systems (VICS). The protocol uses pseudonym certificates to protect vehicle privacy, and uses Optimal Asymmetric Encryption padding (OAEP) and preset public key to implement road control center (RCC) to track anonymous identity in real-time. The protocol uses partial pseudonym certificates and the private key of vehicle to enhance security, and uses Elliptic Curve Cryptography (ECC) to reduce computational consumption.

To analyze the security of the protocol, we use security reduction under the Elliptic Curve Discrete Logarithm Problem (ECDLP) given in the Random Oracle model (RO), which demonstrates our protocol can satisfy the security requirements and defense common attacks. The performance analysis demonstrated our protocol is slightly weaker than others, and we analyze the cost of real-time tracking for the reason. In addition, we analyze the RSU service rate of the protocol in a certain scenario by combining the traffic flow model, and prove that our protocol is stable in this scenario.

REFERENCES

[1] A. Ogawa, S. Kuroda, K. Ushida, R. Kudo, K. Tateishi, H. Yamashita, and T. Kantou, ''Field experiments on sensor data transmission for 5G-based vehicle-infrastructure cooperation,'' in *Proc.88th Vehicular Technol. Conf.*, Chicago, IL, USA, 2018, pp. 1–5, doi: 10.1109/VTCFall.2018.8690934.

[2] D. A. Vignon, Y. Yin, S. Bahrami, and K. Laberteaux, ''Economic analysis of vehicle infrastructure cooperation for driving automation,'' *Transp. Res. C, Emerg. Technol.*, vol. 142, Sep. 2022, Art. no. 103757, doi: 10.1016/j.trc.2022.103757.

[3] M. Yan, W. Chen, J. Wang, M. Zhang, and L. Zhao, ''Characteristics and causes of particularly major road traffic accidents involving commercial vehicles in China,'' *Int. J. Environ. Res. Public Health*, vol. 18, no. 8, p. 3878, Apr. 2021, doi: 10.3390/ijerph18083878.

[4] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, IEEE Standard 802.11p (Amendment to IEEE Standard 802.11-2007 as amended by IEEE Standard 802.11k-2008, IEEE Standard 802.11r-2008, IEEE Standard 802.11y-2008, IEEE Standard 802.11n-2009, and IEEE Standard 802.11w-2009), Jul. 2010, doi: 10.1109/IEEESTD.2010.5514475.

[5] M. Asghar, R. R. M. Doss, and L. Pan, ''A scalable and efficient PKI based authentication protocol for VANETs,'' in *Proc. 28th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Sydney, NSW, Australia, Nov. 2018, pp. 1–3.

[6] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, ''Enhancing security and privacy for identity-based batch verification scheme in VANETs,'' *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017, doi: 10.1109/TVT.2015.2406877.

[7] Y. Han, W. Song, Z. Zhou, H. Wang, and B. Yuan, ''ECLAS: An efficient pairing-free certificateless aggregate signature for secure VANET communication,'' *IEEE Syst. J.*, vol. 16, no. 1, pp. 1637–1648, Mar. 2022, doi: 10.1109/JSYST.2021.3116029.

[8] G. Thumbur, G. S. Rao, P. V. Reddy, N. B. Gayathri, D. V. R. K. Reddy, and M. Padmavathamma, ''Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks,'' *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1908–1920, Feb. 2021, doi: 10.1109/JIOT.2020.3019304.

[9] 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 Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar. 2021, doi: 10.1109/TDSC.2019.2904274.

[10] D. Förster, F. Kargl, and H. Löhr, ''PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks,'' *Ad Hoc Netw.*, vol. 37, pp. 122–132, Feb. 2016, doi: 10.1016/j.adhoc.2015.09.011.

[11] Y.-H. Kung and H.-C. Hsiao, ''GroupIt: Lightweight group key management for dynamic IoT environments,'' *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5155–5165, Dec. 2018, doi: 10.1109/JIOT.2018.2840321.

[12] N. Guo, L. Ma, and T. Gao, ''Independent mix zone for location privacy in vehicular networks,'' *IEEE Access*, vol. 6, pp. 16842–16850, 2018, doi: 10.1109/ACCESS.2018.2800907.

[13] D. He, S. Zeadally, B. Xu, and X. Huang, ''An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,'' *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015, doi: 10.1109/TIFS.2015.2473820.

[14] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, ''VANet security challenges and solutions: A survey,'' *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017, doi: 10.1016/j.vehcom.2017.01.002.

[15] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, ''B-SPECS+: Batch verification for secure pseudonymous authentication in VANET,'' *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013, doi: 10.1109/TIFS.2013.2277471.

[16] M. Azees, P. Vijayakumar, and L. J. Deboarh, ''EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017, doi: 10.1109/TITS.2016.2634623.

[17] F. Kessels, ''The fundamental diagram,'' in *Traffic Flow Modelling: Introduction to Traffic Flow Theory Through a Genealogy of Models*. Cham, Switzerland: Springer, 2019, ch. 2, sec. 2, p. 23, doi: 10.1007/978-3-319-78695-7.

[18] M. Raya and J.-P. Hubaux, ''Securing vehicular ad hoc networks,'' *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, 2007.

[19] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, ''An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,'' *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603, Sep. 2010, doi: 10.1109/TVT.2010.2051468.

[20] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, ''Wireless location privacy protection in vehicular ad-hoc networks,'' *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 160–171, Feb. 2010, doi: 10.1007/s11036-009-0167-4.

[21] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, ''Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,'' *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012, doi: 10.1109/TVT.2011.2162864.

[22] B. Ying, D. Makrakis, and H. T. Mouftah, ''Dynamic mix-zone for location privacy in vehicular networks,'' *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1524–1527, Aug. 2013, doi: 10.1109/LCOMM.2013.070113.122816.

[23] J. Wen, L. Bai, Z. Yang, H. Zhang, H. Wang, and D. He, ''LaRRS: Lattice-based revocable ring signature and its application for VANETs,'' *IEEE Trans. Veh. Technol.*, vol. 73, no. 1, pp. 739–753, Jan. 2024, doi: 10.1109/tvt.2023.3305037.

[24] A. Shamir, ''Identity-based cryptosystems and signature schemes,'' in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 196, G. R. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, pp. 47–53, doi: 10.1007/3-540-39568-7_5.

[25] N.-W. Lo and J.-L. Tsai, ''An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016, doi: 10.1109/TITS.2015.2502322.

[26] Y. Genc, C. Korkuc, N. Aytas, E. Afacan, M. H. Sazli, and E. Yazgan, ''A novel identity-based privacy-preserving anonymous authentication scheme for vehicle-to-vehicle communication,'' *Elektronika IR Elektrotechnika*, vol. 29, no. 2, pp. 69–77, Apr. 2023, doi: 10.5755/j02.eie.30990.

[27] A. Boualouache, S.-M. Senouci, and S. Moussaoui, ''A survey on pseudonym changing strategies for vehicular ad-hoc networks,'' *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018, doi: 10.1109/COMST.2017.2771522.

[28] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, ''An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks,'' *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015, doi: 10.1016/j.ins.2015.04.033.

[29] B. Samra and S. Fouzi, ''New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET,'' *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100414, doi: 10.1016/j.vehcom.2021.100414.

[30] Y. Liang, H. Yan, and Y. Liu, ''Unlinkable signcryption scheme for multi-receiver in VANETs,'' *IEEE Trans. Intell. Transport. Syst.*, vol. 24, no. 9, pp. 10138–10154, Sep. 2023, doi: 10.1109/TITS.2023.3271110.

[31] J. Liu, C. Peng, R. Sun, L. Liu, N. Zhang, S. Dustdar, and V. C. M. Leung, ''CPAHP: Conditional privacy-preserving authentication scheme with hierarchical pseudonym for 5G-enabled IoV,'' *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 8929–8940, Jul. 2023, doi: 10.1109/TVT.2023.3246466.

[32] E. Ebrahimi, ''Post-quantum security of plain OAEP transform,'' in *Public-Key Cryptography—PKC* (Lecture Notes in Computer Science), vol. 13177, G. Hanaoka, J. Shikata, and Y. Watanabe, Eds. Cham, Switzerland: Springer, 2022, pp. 34–51, doi: 10.1007/978-3-030-97121-2_2.

[33] S. More, R. Gupta, R. Verma, S. Agarwal, S. K. Nayak, and B. R. Senapati, ''Decentralized fingerprinting for secure peer-to-peer data exchange of aadhaar via public key infrastructure,'' in *Proc. Int. Conf. Adv. Power, Signal, Inf. Technol. (APSIT)*, Bhubaneswar, India, Jun. 2023, pp. 318–323, doi: 10.1109/apsit58554.2023.10201789.

[34] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, ''CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs,'' *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3456–3468, Apr. 2021, doi: 10.1109/TVT.2021.3064337.

[35] F. Guo, W. Susilo, and Y. Mu, ''Foundations of security reduction,'' in *Introduction to Security Reduction*. Cham, Switzerland: Springer, 2018, ch. 4, sec. 3, p. 47, doi: 10.1007/978-3-319-93049-7_4.

[36] F. Guo, W. Susilo, and Y. Mu, "Foundations of security reduction," in *Introduction to Security Reduction*. Cham, Switzerland: Springer, 2018, ch. 4, sec. 8, p. 85, doi: 10.1007/978-3-319-93049-7_4.

[37] J. Cui, W. Xu, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Privacy-preserving authentication using a double pseudonym for Internet of Vehicles," *Sensors*, vol. 18, no. 5, p. 1453, May 2018, doi: 10.3390/s18051453.

[38] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, Jun. 2000, doi: 10.1007/s001450010003.

[39] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017, doi: 10.1016/j.vehcom.2017.02.001.

[40] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2972–2986, Mar. 2019, doi: 10.1109/TVT.2019.2896018.

[41] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang, and F. Xu, "A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transport. Syst.*, vol. 24, no. 10, pp. 10456–10466, Oct. 2023, doi: 10.1109/TITS.2023.3275077.

[42] S. A. Afolalu, O. M. Ikumapayi, A. Abdulkareem, M. E. Emetere, and O. Adejumo, "A short review on queuing theory as a deterministic tool in sustainable telecommunication system," *Mater. Today, Proc.*, vol. 44, pp. 2884–2888, Jan. 2021, doi: 10.1016/j.matpr.2021.01.092.

[43] H. C. Manual, *Highway Capacity Manual*, 5th ed. Washington, DC, USA: Transportation Research Board of the National Academies, 2010, ch. 10. [Online]. Available: http://www.trb.org/Main/Blurbs/164718.aspx

[44] H. C. Manual, *Highway Capacity Manual*, 5th ed. Washington, DC, USA: Transportation Research Board of the National Academies, 2010, ch. 14. [Online]. Available: http://www.trb.org/Main/Blurbs/164718.aspx

JIASHENG YUAN is currently pursuing the M.S. degree with the Research Institute of Highway, Ministry of Transport, Beijing, China. His current research interests include cryptography of intelligent transport systems and information security.

BIN LI received the Ph.D. degree from Jilin University, China. He is currently the Vice President and the Chief Engineer of the Research Institute of Highway, Ministry of Transport, and the Director of the National Intelligent Transport Systems Center of Engineering and Technology. His current interests include cybersecurity, cryptography of intelligent transport systems, electric toll collection, and vehicle-infrastructure cooperative systems.

XINMING MEI received the M.S. degree from Jilin University (JLU), China, in 2001. He is currently a Professor with Beijing GOTEC ITS Technology Company, China. His research interests include the cybersecurity and cryptography of intelligent transport systems and electric toll collection.

YANFANG ZHOU received the Ph.D. degree in transportation planning and management from Beijing Jiaotong University (BJU), in 2012. Since July 2012, she has been with the Research Institute of Highway, Ministry of Transport, where she is currently an Associate Researcher. She has drafted multiple cybersecurity policies for the transportation industry. Her main research interest includes transportation industry network security.