Hindawi
Security and Communication Networks
Volume 2022, Article ID 8758156, 15 pages
https://doi.org/10.1155/2022/8758156

Research Article

Trust-Based Certificateless Privacy-Preserving Authentication in Internet of Vehicles

Chang Yu [1] and Kezhong Lu [2]

[1] *College of Finance and Economics, Anhui Technical College of Industry and Economy, Hefei230000, Anhui, China*
[2] *School of Big Data and Artificial Intelligence, Chizhou University, Chizhou 247100, China*

Correspondence should be addressed to Kezhong Lu; luck@czu.edu.cn

Received 6 March 2022; Revised 16 April 2022; Accepted 21 May 2022; Published 18 August 2022

Academic Editor: Jie Cui

Owing to the security requirements of Internet of vehicles (IOV), it is necessary to design a secure privacy-preserving scheme for communication. Traditional privacy-preserving schemes have two deficiencies. One is the high cost of computation and communication. Another is the inability to prevent the spread of malicious or modified messages. Motivated by those facts, we proposed a trust-based authentication scheme for certificateless privacy-preserving of IOV, based on the advantages of the short key, fast speed, and high security performance of elliptic curve cryptography (ECC). We proposed a method to replace the revocation list by authenticating trust to prevent broadcasting fake and altered massages. Our scheme can encrypt the message sent by the node while adopting a certificateless authentication method to complete the anonymous authentication function, which protects the privacy of the node information and effectively reduces the system storage load. In addition, aggregate signatures can effectively reduce computational and communication overhead. It is proven theoretically that the proposed scheme can satisfy correctness, anonymity, confidentiality of messages, and unforgeability of signatures. Therefore, this scheme is more suitable for the deployment and application of physical IOV.

1. Introduction

Internet of vehicles (IOV) are applications of mobile ad hoc networks (MANETs) and wireless sensor networks in the field of intelligent transportation to implement the communication between intelligent vehicles and increase the safety and efficiency of road traffic. The key features that distinguish IOV from other MANETs are vehicle density, self-organization, multihop, rapid change of network topology, limited network capacity, no power and storage constraints, predictable node mobility patterns owing to fixed roads and lanes, and a large number of nodes in urban traffic [1]. A typical IOV architecture usually includes three components: service center, road side unit (RSU), and a vehicle node that configures the onboard unit (OBU), where the OBU is mounted on the vehicle to provide wireless communication capabilities. The RSU is used to provide a wireless and radio-covered vehicle interface [2]. As networks become more common, there is a growing need for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [3], and the communication between V2V and V2I is realized by dedicated short range communication (DSRC) [4] systems. Most importantly, the IOV is a promising technology for providing effective traffic management solutions, navigation-based services, infotainment, and vehicle safety.

Privacy and security issues in IOV have attracted a significant amount of attention. Since IOV supports emergent real-time applications and processes vital message, relevant schemes should meet security requirements such as privacy, confidentiality, integrity, and nonrepudiation to provide secure communication to attackers and malicious nodes [5]. All Kinds of security attacks such as denial of service (DOS), Sybil attack, illusion attack, and wormhole attack will affect the privacy of the vehicle and possibly lead to traffic congestion, misinformation dissemination, positioning and identity leakage, disguise or forgery of data, and intrusion of private information. Therefore, data security and privacy-preserving issues in the IOV environment have become the focus of attention [2, 6].

A number of asymmetric cryptography-based security authentication schemes have been proposed to prevent such attacks. Anonymous authentication is one of the basic methods used for preserving privacy. The typical anonymous authentication mechanisms in IOV include pseudonyms, random silence, group signatures, ring signatures, blind signatures, and smart cards. In recent years, scholars have proposed a variety of anonymous schemes for IOV security authentication, such as digital signature scheme [7] and group signature scheme [8] based on public key infrastructure (PKI). However, these traditional anonymous authentication schemes have the following disadvantages. (1) The computational and communication costs of message authentication are large. In the case of high traffic density, there will be more delay, and a large number of messages will get lost. (2) Requirement for vehicle to store a large number of certificates and dependence on the revocation list to achieve vehicles revocation. It results in a large storage overhead of the system. Therefore, improving the efficiency of anonymous authentication based on ensuring security is also one of the principal challenges facing IOV [9].

Except for efficiency issues, authentication mechanism also has a major limitation, as it only ensures that the messages are transmitted from a legitimate sender, and does not prevent legitimate senders from maliciously spreading false or modified information to other vehicles. False or altered messages can reduce traffic efficiency and, at worst, threaten people's lives. The question to be considered is how a vehicle decides whether to believe a message sent by a dependable vehicle. In order to prevent the above problems from causing improper behavior of the vehicle, misconduct detection mechanisms [10] and reputation systems [11] have been put forward. Trust vehicles can be distinguished from untrusted vehicles by building trust relationships and detecting malicious behavior in IOV, thereby preventing the vehicle from being misdirected by other malicious vehicles. Therefore, trust is essential to protect IOV. Anonymous authentication trust is becoming a compelling method of preserving privacy in IOV. Nevertheless, there is a lack of research on this topic, especially for the IOV system. Trust management of IOV [12] has been studied and attempted.

In this study, we propose a certificateless anonymous authentication scheme based on the trust of the IOV. In our scheme, the trust value is combined with the traditional encryption scheme for preserving privacy. Only if the vehicle generating the message has a certain trust value, the message is thought to be reliable. The proposed method can not only ensure the effective communication of vehicles in the vehicle network but also make sure the vehicles receive information that is reliable. The basic principle of the scheme is to allow a trusted authority (TA) or authorized parties (AP) to announce the latest aggregate list of integrated node trust (INT) and verify the node trust without certificates. In our proposed scheme, a TA updates the trust value of each vehicle, stores the values in the trust value table using hashing techniques, and then broadcasts the trust value table. Thus, all vehicles can obtain the trust value of the adjacent vehicle by querying the trust value table to strengthen security. Depending upon the location of the trust value in the INT aggregation list, the receiving node can verify the sender's message anonymously and without a certificate, and aggregate signatures can effectively reduce the computational costs and communication overhead. Furthermore, multiple APs may flexibly coordinated to achieve trust authentication while supporting aggregation signature verification. The method can provide fast, anonymous authentication and preserve privacy, and can ensure the reliability of the message of V2V communication.

1.1. Our Contributions. The main contributions of the proposed scheme are summarized:

(i) We propose a scheme to guarantee the security of communication and the reliability of messages in IOV by combining trust with traditional privacy-preserving encryption scheme. We demonstrated that the proposed method was secure, and evaluated the performance by analyzing the proposed scheme.

(ii) We propose a method to replace the revocation list by authenticating trust, and our scheme does not involve PKI certificates, thus reducing the storage burden of the system vehicles. It also does not involve complex bilinear pairing operations, which effectively improves authentication efficiency.

1.2. Organization. The rest of this article is arranged as following: Section 2 describes the related work of the proposed scheme. Section 3 introduces preliminaries and background information. In Section 4, we described the proposed scheme in detail. Section 5 gives a proof of the security in the random oracle model under ECDLP. Security analysis and performance evaluation are described in detail in Section 6. Finally, Section 7 summarizes the future work of this paper.

2. Related Work

In the last several years, scholars have done a lot of research on the preserving privacy and data security of nodes in IOV.

2.1. Anonymous Authentication. Many anonymous authentication schemes have been proposed for IOV, which can be divided into five categories based on the encryption mechanism employed: public key infrastructure (PKI), certificateless signature, symmetric cryptography, identity-based signature, and group signature.

To realize preserving privacy and security in IOV, in 2007, Raya and Hubaux [13] used anonymous certificates to hide the identity of users and a PKI-based scheme is proposed. Raya advises to store huge amounts of public/private keys and corresponding certificates in each vehicle, and the vehicle randomly selects the certificate to sign the message. The privacy of the vehicle is protected by regular replacement of keys and certificates. In 2008, Lu et al. [2] proposed an efficient conditional privacy preservation (ECPP) protocol based on bilinear mapping. The main limitation of ECPP is the large latency of RSU in generating pseudonym. In 2012, Shim proposed an identity-based signature scheme [14], which stores the master key in the vehicle's tamper-proof device. The vehicle can use the system master key to generate pseudo-names and other information. In 2013, Horng et al. proposed a scheme [15] to use RSU to generate different pseudo-names for vehicles to generate a distinctive anonymous authentication scheme, avoiding the use of a great deal of public and private key pairs by using pseudonym communication. However, guaranteeing the security of the RSU is also a problem. Shao et al. [16] through the use of the new group signature scheme proposed new IOV authentication protocol. However, it can cause random tracking, which reduces user privacy. In 2018, Li et al. [17] proposed an anonymous conditional privacy-preserving authentication scheme based on pseudoidentity method. Each OBU should prestore pseudoidentity in order to maintain their identity privacy. Liu et al. [18] designed a distributed MAC layer antiattack pseudonym scheme. In 2019, Liu et al. [19] designed an anonymous authentication scheme based on group signature, where area TA provided anonymous authentication services. Boualouache et al. [20] proposed an effective pseudonym changing and management framework. This approach can keep the message integrity, and the sender's privacy, but it also has some disadvantages. When the vehicle's private key has been revoked, the system needs to be updated regularly for vehicle certificate; it may take time. Key distribution, management, and storage are challenges. To solve these problems, Du et al. [21] designed a certificateless signature scheme combined with certificateless public key cryptography. Zhong et al. [22] presented a full aggregation authentication scheme for VANETs, which achieved conditional privacy protection by using pseudonyms. In 2020, Bayat et al. [23] proposed a new security and privacy protection scheme based on RSU. In this scheme, the TA stored the master key in the temper-proof device of the RSU, and the verifier used the public key of the RSU instead of the system to check whether the signature is valid. Therefore, vehicles cannot check the signatures of other vehicles on the road from other RSUs. However, bilinear pairing and map-to-point operations are used in the scheme, which results in high computational overhead. Verma et al. [24] proposed the pairing-free certificate-based aggregated signature scheme. Xu et al. [25] proposed a certificateless signature scheme based on the CDH assumption. However, the scheme utilized the expensive map-to-point hash function, which also increased computational and communication overhead. To reduce computational and bandwidth costs, Mei et al. [26] proposed a conditional privacy certificateless signature scheme, which achieved full aggregation. But the scheme is also based on bilinear pairing. To further reduce the overhead of the vehicle, Chen et al. [27] designed a certificateless aggregated signature scheme without the expensive map-to-point hash function and bilinear pairing operations. Ali et al. [28] proposed a certificateless short signature-based conditional privacy-preserving authentication scheme based on ECC, which supported the batch signature verification method. Table 1 provides the nature of the above scheme for the sake of clarity.

Table 1: Properties of related IOV schemes.

Scheme	Crypto.primitive	Comp.&comm.cost
Raya and Hubaux [13]	PKI	High
Lu et al. [2]	Group signature	Medium
Shim [14]	ID based	Low
Shao et al. [16]	Group signature	Medium

However, only anonymity is not sufficient to prevent an attacker from illegally tracking, even if the broadcast message remains completely anonymous [29]. In addition, traditional public key infrastructure (PKI) guarantees user identity authentication in IOV; however, PKI cannot distinguish untrustworthy information from authorized users. Therefore, a trust evaluation is necessary to guarantee the trustworthiness of information by distinguishing malicious users from networks.

2.2. Trust. The issue of trust stems from the field of security and social psychology. In the past decade, the concept of trust has been suggested to introduce information and communication technology (ICT). There is little research about trust management of IOV during the preceding years. In 2014, MC Chuang and Lee [30] proposed a lightweight authentication scheme for distributed trust extension, called trust extension authentication mechanism, applicable to the vehicle network, with good anonymity and security. In fact, they are designed to further enhance the performance of the authentication process by using the concept of passing trust relationships. Nevertheless, because of the selfish and malicious nodes, the security of mobile ad hoc networks has been greatly reduced. Then, Sugumar et al. [31] proposed a trust-based authentication protocol for cluster-based IOV in 2016. The vehicles are clustered and the trust level of each node is estimated. Inspired by the estimated trust, the cluster head is selected. Because the CRL check requires time, the group signature-based scheme has a long computing delay. In 2018, Yan et al. [32] proposed a scheme to anonymously verify the trust of pervasive social networking (PSN) nodes in a semi-distributed way. It was emphasized that trust plays an important role in maintaining pervasive social networking. It can be seen that anonymous authentication of trust is emerging as a novel way to ensure privacy. In 2020, Liang et al. [33] proposed a reputation scheme based on implicit generalized mixed transition distribution model, which can evaluate the credibility of neighbor vehicles. Begriche et al. [34] proposed a vehicle-mounted network reputation system node based on Bayesian statistical filter that would establish a profile based on the behavior of its neighbors. However, there are only two categories of vehicle states. In the same year, Awan et al. [35] proposed a centralized trust-based clustering mechanism, using multiple parameters to select reliable cluster head and a backup cluster head, thus improving network security. In addition, the method selects a backup cluster head to achieve stable clusters. However, the scheme relies on the RSU. Alnasser et al. [36] proposed a recommendation-based trust model. The trust of this model comes from two methods: direct trust and indirect trust, but the trust value is calculated in the way of weighted sum, which cannot resist collusion attacks. Chen et al. [37] proposed a decentralized trust management system based on blockchain. The trust model only allows trusted nodes to participate in the verification and consensus process, and a trusted execution environment is applied to protect the trust evaluation process and an incentive model for incentivizing more participation and punishing malicious behavior. Gao [38] proposed a trust management scheme. In the scheme, the trust of nodes includes direct trust and recommendation trust. Direct trust is computed dynamically through history and Bayesian inference. Recommendation trust takes into account the trust and reputation of other nodes and their reputation. Ahmad et al. [39] proposed a hybrid trust management scheme called NOTRINO, which calculates the trust value of nodes at the transport layer and calculates the trust value of data at the application layer.

Unlike all the previous work, this paper combines IOV application scenarios based on the research trust-based [32] and encryption scheme [40], a certificateless anonymous authentication scheme suitable for preserving privacy is proposed for IOV.

3. Preliminaries

In this section, we will briefly cover the mathematical foundations, system model, security and authentication requirements.

3.1. Mathematical Foundations. This subsection describes some of the basics associated with anonymous authentication protocols, namely, elliptic curve cryptography (ECC) and mathematical assumptions.

3.1.1. Elliptic Curve Cryptography (ECC). After elliptic curve cryptography was proposed by Koblitz [41] and Miller [42] in 1986, respectively, ECC began to be commonly used in security-related fields such as encryption and protocols. In the following sections, we briefly introduce elliptic curve cryptography, which is extensively used to design many encryption and security schemes because of its availability in computing and communication costs. In the case that the safety strength provided is the same as that of the discrete logarithm system, the parameters required by ECC are far less than those of the discrete log-based system [43]. The elliptic curve can be characterized by the set of solutions of a two element equation.

If the group $\mathbb{G}$ is a finite cyclic group on the elliptic curve E, its order is p and the generator is P. Let p be a prime number greater than 3, and the elliptic curve $y^2 = x^3 + ax + b$ on Z_p consist of a group of solutions $(x, y) \in Z_p \times Z_p$ based on congruence $y^2 \equiv x^3 + ax + b \mathrm{mod} p$ and an exceptional point o called infinite point, where $a, b \in Z_p$ comprises two constants satisfying $4a^3 + 27b^2 \neq 0 \mathrm{mod} p$. In addition, $\mathbb{G}$ has two rules of operation:

(1) Addition (±): let $P, Q \in \mathbb{G}$, if $P \neq Q$, $R = P + Q$, then R is the point where the line crosses P and Q and E; if $P = Q$, $R = P + Q$, then R is the intersection of the tangent of E and $P(Q)$; if $P = -Q$, there is $P + Q = P - P = \mathcal{O}$.

(2) Scalar multiplication (·): let $P \in \mathbb{G}$, $m \in Z_q^*$, and P have a scalar multiplication of $m \cdot P = P + P + \cdots + P$ (m times in total).

3.1.2. Difficult Problem. Let $\mathbb{G}$ be a finite cyclic group with large prime q on an elliptic curve and P be a generator. To demonstrate the security of our scheme, two difficult problems are defined. The mathematical difficulties of participating in the proposed scheme are shown.

Definition 1. Elliptic curve discrete logarithm problem (ECDLP): random point $P, Q \in \mathbb{G}$ on E are presented, and $Q = xP$, output $x \in Z_q^*$.

Definition 2. Computation of Diffie–Hellman problem (CDHP): given $P, aP, bP \in \mathbb{G}$, where $a, b \in Z_q^*$, calculate abP.

If the algorithm of the ECDLP or the CDHP on the group $\mathbb{G}$ cannot be solved by a nonnegligible probability ε within the time τ, then the ECDLP or the CDHP is difficult in the group $\mathbb{G}$.

3.2. System Model. We describe the system model of the proposed anonymous authentication scheme in Figure 1. The trusted authority (TA) has adequacy functions and is trusted to provide identity management and trust management. What is more, TA or IOV nodes that are more stable and dependable than other vehicle nodes (for example, wi-fi access points and base stations) can act as authorizers (AP). AP uses adequate information about nodes to estimate the trust value of the node. In order to achieve instant communication, the nodes interact with each other. Because message integrity and privacy are important, it is necessary to verify node trust anonymously for reliable communication and preserving privacy. TA is used by vehicle nodes to manage the correspondence among real identity, pseudonym, key and trust in the cloud to save computing and storage costs. When the TA is inaccessible, the IOV node can use some of the IOV nodes as APs to correspond to each other.

(1) Trusted authority (TA): it is based on the assumption that TA is fully trusted and has sufficient computing and storage capacity. Through a secure channel, entities (vehicles and RSU) must register with the TA using some personal credentials that uniquely identify the entity. TA is responsible for the registration of fixed RSU on the roadside and mobile OBU installed on vehicles and can reveal the true OBU identity of secure messages.

(2) Road side units (RSU): suppose the RSUs are widely deployed on the road and can be viewed as the router

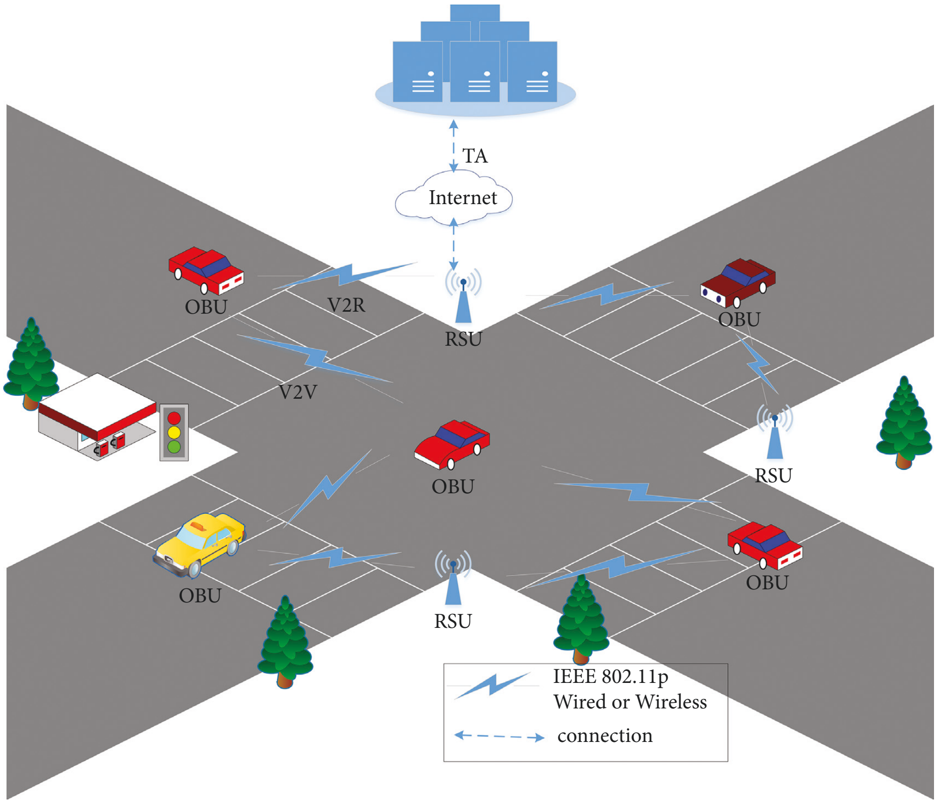

Figure 1: The system model of IOV.

between the TA and vehicle nodes. RSU are not entirely credible, so they have to be supervised by TA.

(3) Vehicles (OBU): each vehicle is equipped with OBU which has a shorter communication range and less computing power than RSU. With the built-in OBU and DSRC protocols, each vehicle can communicate with neighboring vehicles, RSU and TA. The real identity of the vehicle and some secret information about the operation are stored in the OBU.

3.3. Security Requirements. Because messages are transported in an open access environment, security and privacy issues related to IOV must be considered. For anonymous authentication on trust in IOV, the following safety requirements must be met [6]:

3.3.1. Authentication. This requirement consists of vehicle authentication and message integrity. Vehicle authentication allows the receiver to verify the authenticity of the sender, and the message integrity ensures that the message is not changed during the transmission.

3.3.2. Anonymity. The system proposed in this scheme is shown in Figure 1. No entity other than TA can know any information about the real identity of the vehicle, that is, only TA can reveal the real identity of the participating vehicle.

3.3.3. Traceability. This function is used to identify malicious vehicles that may transmit false messages. Vehicles and RSU have no way to know the real sender of the received message, but TA can recover the true identity of the sender in case of an accident, which is called conditional traceability in IOV.

3.3.4. Unlinkability. The user's unlinkability means that the attacker could not judge whether any two messages are from the same vehicle.

3.3.5. Replaying Resistance. Malicious vehicles cannot collect and send messages that have been received by the recipient.

3.4. Authentication Requirements. In order to ensure the safety of IOV communication, the following authentication requirements must be met:

(1) The computational and communication overhead of digital signatures must be low

(2) Authentication should be robust and extensible

(3) The process of reauthentication and revocation should be provided

4. The Proposed Scheme

In this section, we describe a trust-based authentication scheme proposed in this paper, which can authenticate node trust and verify node signature by anonymous method, which is suitable for secure V2V communication in IOV. Specifically, after system settings and node registration, authorized parties (AP) issue aggregated lists of INT values and INT hash (in short, aggregated lists) to each IOV node. On the basis of INT, nodes generate their one-time key pairs to sign their messages. Based on previous research on trust in IOV, we can assume that the trust of a node is a specific value, such as context-aware trust generation [12].

The scheme is divided into seven phases: system initialization, node registration, issue trust value, aggregate list, one-off key pair generation, signature generation, and verification. The symbols used in the proposed scheme are given in Table 2. Detailed procedures for the proposed scheme are as follows:

4.1. System Initialization. In this subsection, TA generates system parameters and loads them to the vehicle node. The system initialization of the scheme is the responsibility of TA, which consists of two parts, namely, key generation center (KGC) and tracing authorization (TRA), assuming that both parties have enough storage space and computing capacity. Since we assume that TA is reliable in this paper, we can conclude that KGC and TRA are also reliable.

(1) Given the safety parameter ℓ, TAs use two large prime numbers p, q and an elliptic curve defined by $y^2 = x^3 + ax + b(\text{mod})p, a, b \in F_p$.

(2) The KGC chooses point P from E and generates group $\mathbb{G}$ through P. KGC selects the random number $\alpha \in Z_q^*$ and calculates

$$P_{pub} = \alpha P, \tag{1}$$

where α is the secret value stored in KGC and is the master key used to extract part of the key.

(3) The TRA picks point P from E and produces the group $\mathbb{G}$ through P. TRA selects the random number $\beta \in Z_q^*$ and calculates

$$T_{pub} = \beta P, \tag{2}$$

where β is the secret value stored in TRA and the master key for traceability.

(4) TAs choose four secure hash functions H_1: $\mathbb{G} \longrightarrow Z_q^*$, H_2: $\{0,1\}^* \longrightarrow \mathbb{G}$, H_3: $\{0,1\}^* \longrightarrow \mathbb{G}$, h_1: $\{0,1\}^* \longrightarrow \{0,1\}^n$, h_2: $\{0,1\}^* \longrightarrow Z_q^*$.

(5) They publish the system parameters *Para*:

$$Para = \left(P, p, q, E, \mathbb{G}, H_1, H_2, H_3, h_1, h_2, P_{pub}, T_{pub}\right). \tag{3}$$

When the system is initialized, these public system parameters, *Para*, are reloaded into the tamper-proof device in the vehicle node.

4.2. Node Registration. In this subsection, when each vehicle node V_i registers with the system (TA), it needs to rely on its unique real identity (RID_i. In addition, the public key can be authenticated using the aggregation list distributed by AP, thus achieving certificateless, trust-based authentication. Therefore, the proposed scheme does not need the public key certificate (Figure2).

Table 2: System notations.

Notations	Description
V_i	The ith vehicle
M	Messages from vehicles
$t_i T_i$	A timestamp
TV_i	The short-lived trust value of V_i
T_TV_i	The validity period of TV_i
AC_TV_i	The authentication code of TV_i
$Cert_i$	The certificate of ID_i issued by TA
P_{pub}, P_{pub}	The public key pair of KGC and TRA
RID_i	The real identity of V_i
(U_i, V_i)	The one-off public/private pair key of TV_i
sign_i	The signature from V_i
$\mathbb{G}$	A cycle additive group
P	A generator of the group $\mathbb{G}$
q	The order of $\mathbb{G}$
$H(\cdot)$	A MapToPoint hash function
$h(\cdot)$	The hash function
TA	Trusted authority
CRL	Certificate revocation list
OBU	On board unit
RSU	Road side unit

(1) The vehicle V_i selects a random number $k_i \in Z_q^*$ and calculates

$$ID_{i,1} = k_i P. \tag{4}$$

TRA receives $(RID_i, ID_{i,1})$ from the vehicle, and the communication channel between the two parties is safe, where the vehicle node V_i can be uniquely identified through RID_i.

(2) When TRA receives RID_i from vehicle V_i, where RID_i is the real identity of V_i, it first checks for RID_i and then calculates

$$ID_{i,2} = RID_i \oplus H_1\left(\beta \cdot ID_{i,1}, T_i, T_{pub}\right), \tag{5}$$

where T_i indicates the validity period of this pseudoidentity. The TAs choose random $u_i \in Z_q$, TAs also provide certificate $Cert_i = u_i P$. The node uses this certificate to request its trust value from TAs. Going down this, KGC can receive pseudoidentity ID_i and $Cert_i$ in a secure manner.

$$ID_i = \left(ID_{i,1}, ID_{i,2}, T_i\right). \tag{6}$$

(3) When KGC obtains the pseudoidentity ID_i, it calculates part of the private key psk_{ID_i} after selecting a random number $d_i \in Z_q^*$ and computing $Q_{ID_i} = d_i P$.

$$psk_{ID_i} = d_i + h_2\left(ID_i, Q_{ID_i}\right) \times \alpha \bmod q. \tag{7}$$

The vehicle receives $(ID_i, psk_{ID_i}, Cert_i, Q_{ID_i})$ from KGC in a secure manner, including the pseudoidentity, partial private key, and certificate.

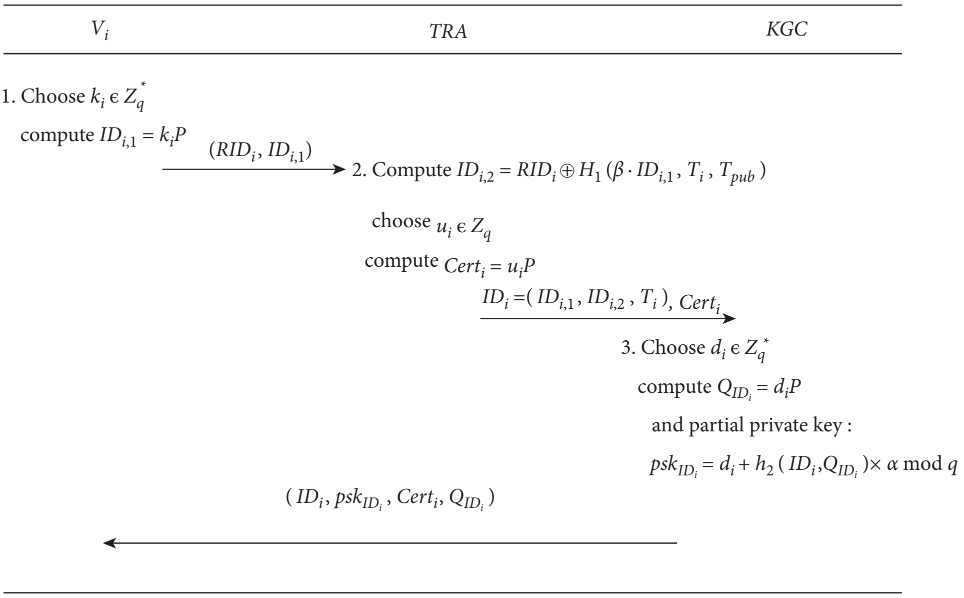
V_i
TRA
KGC
1. Choose $k_i \in Z_q^*$
compute $ID_{i,1} = k_i P$
$(RID_i, ID_{i,1})$
2. Compute $ID_{i,2} = RID_i \oplus H_1(\beta \cdot ID_{i,1}, T_i, T_{pub})$
choose $u_i \in Z_q$
compute $Cert_i = u_i P$
$ID_i = (ID_{i,1}, ID_{i,2}, T_i), Cert_i$
3. Choose $d_i \in Z_q^*$
compute $Q_{ID_i} = d_i P$
and partial private key :
$psk_{ID_i} = d_i + h_2(ID_i, Q_{ID_i}) \times \alpha \bmod q$
$(ID_i, psk_{ID_i}, Cert_i, Q_{ID_i})$

Figure 2: Registration of vehicle node.

4.3. Issue Trust Value and Aggregate List. First of all, each AP (executed by TA or IOV nodes) delivers an original trust value with a valid period and the aggregate list of INT hashes for node V_i in the system; the AP then notifies all vehicle nodes of the newly generated aggregation list. The AP first inspects the validity of the previous trust value before deciding whether to reissue the trust value. In this subsection, one of its essential components is nodes to verify the trust values of other nodes during communication. Nodes request and receive INT in a trustworthy way. In addition, AP will use its signature to distribute the latest INT summary list. Based on its current INT, the trusted processor can produce a one-time public and private key pair.

The trust value of the vehicle can be obtained by analyzing the message records issued by the vehicle collected by AP. At AP, the information collector saves the results in a database after collecting and processing message records from the vehicle nodes. The trust evaluator is used to evaluate the trust value of the vehicle node and detect the malicious vehicle node. The trusted publisher issues an aggregated list of INT hash values for all nodes on the IOV node on a regular or per request basis. When a vehicle node is registered, TAs issue an original trust value on the basis of the behavior of the vehicle node. The TAs collaborate with APs to determine the node's INT and track its true identity without revealing the node's true identity to any other IOV node. The TA database also holds the trust value of each node and its true identity. The AP can communicate with the TA more stably and reliably than a normal node.

After the AP reevaluates the trust, a new trust value is obtained, and it then stores the hash value of the new INT value to the appropriate location of Ha or Ha_AP_j. When the value of trust expires, the trust value is re-requested, and the AP deletes the old value. Its corresponding INT is saved to the appropriate location in the latest aggregation list. The AP then publishes the updated list to all vehicle nodes. All AP simultaneously broadcasts its latest INT summary list. The value of the node's trust can be verified through the presence and location $h_1(Q_i \| h_1(n_i))$ or $h_1(Q_i \| h_1(n_i\_AP_j))$ of the aggregation list (Ha or Ha_AP_j). Because INT values are sorted in the list (for example, in ascending order), the node during the message authentication is easy to compare trust value. The following will be described separately in two cases, as described in detail below.

(1) AP is executed by TAs: in this phase, based on the true identity of the vehicle, the TAs construct an original or new INT value for the vehicle node. When the current period of trust value expires, a new trust value is requested, at which point TA reevaluates the trust value of V_i and publishes it to V_i using the authentication code AC_TV_i. The vehicle node transmits a random number $d1$ and its certificate $Cert_i$ to TAs to request a trust value. The shared session key between TA and V_i is established using the Diffie–Hellman key agreement protocol, and $d2$ is selected by TA. Afterwards TAs transmit parameters: $\{h_1(TV_i \| AC\_TV_i), T\_TV_i, s_i, Q_i = s_i \cdot P\}$, where TV_i is due at T_TV_i. The list Ha of INT hashes is produced periodically by TAs: $Ha = \{h_1(Q_1 \| h_1(n_1)), \cdot, h_1(Q_i \| h_1(n_i)), \cdot\}$, where $n_i = h_1(TV_i \| AC\_TV_i)$. And then all the nodes will receive $\{Ha \| sign_{TS}(Ha)\}$ from TAs.

(2) AP is carried out by the IOV node: AP (AP_j) can be played by node V_j to assess the others' trust value in IOV. In the same way, Diffie–Hellman key agreement protocol is adopted to establish the shared session key between AP and V_i. Afterwards AP_j transmits parameters: $\{h_1(TV_i\_AP_j \| AC\_TV_i\_AP_j), T\_TV_i\_AP_j\}$ to V_i,

where $TV_i\_AP_j$ is due at $T\_TV_i\_AP_j$. In this case, V_j also can be authenticated with by node V_i. If there are multiple APs, Ha_AP_j is produced periodically by AP_j. And publish it to all nodes after signing: $\left\{Ha\_AP_j \middle\| sign_{AP_j}(Ha\_AP_j)\right\}$ with his private key. Of which

$$Ha\_AP_j = \left\{ \begin{array}{c} h_1\left(Q_1 \| h_1\left(n_1\_AP_j\right)\right), \ldots \\ h_1\left(Q_i \| h_1\left(n_i\_AP_j\right)\right), \ldots \end{array} \right\}. \tag{8}$$

4.4. One-Off Key Pair Generation. In this subsection, vehicle nodes can construct its one-off key pair on INT to sign the messages it sends. Receivers can verify received messages individually or aggregately.

Be based on $n_i = h_1(TV_i \| AC\_TV_i)$, one-off anonymous public and private key pairs (Y_i and r_i) can be constructed by V_i. The production of one-off anonymous key pairs is depicted in Algorithm 1. By randomly changing the nonce a, V_i can produce a distinctive key pair for a new one-off public and private key pair. Therefore, if n_i is the same, different key pairs can be generated to achieve advanced privacy.

4.5. Signature Generation. In this subsection, the vehicle must sign the message with the one-off private key before sending the message, in order to authenticate and preserve the integrity of a message. Vehicle V_i first randomly selects pseudo ID_i from memory and selects the latest timestamp t_i. The updated timestamp t_i protects signature messages from replay attacks. Given the signature key (psk_{ID_i}, r_i) and message M_i, the following steps will be performed by vehicle V_i.

(1) The node sends the message M_i by calculating h_i and signing on M_i using the private key Y_i.

$$\begin{aligned} h_i &= H_3(M_i, ID_i, Y_i, t_i) \\ sign_i(M_i) &= h_i \cdot s_i + psk_{ID_i} \bmod q. \end{aligned} \tag{9}$$

(2) After that, V_i outputs the final message and uses the following format to send msg to other nodes

$$msg = (ID_i, Y_i, sign_i, M_i, t_i, Q_i). \tag{10}$$

4.6. Aggregate. If different nodes send many messages to the same node over a period of time, we can calculate multiple signature combinations as $S = \sum_{i=1}^{n} sign_i(M_i)$ for getting a collection of individual certificateless signatures at a receiver.

4.7. Verification. When adjacent vehicles communicate with each other and send messages, the receiving vehicle needs to check the signature of the message to ensure that the corresponding vehicle does not attempt to propagate a false message (Figure3).

(1) Individual verify: when the node receives the message, the receiver first extracted $h_1(n_i)$ from Y_i:

$$h_1(n_i) = Y2_i \oplus H_1(Y1_i), \tag{11}$$

and calculates $h_1(Q_i \| h_1(n_i))$ to verify the trust value of V_i according to the location in the list. Once the authenticity of the sender's trust value is verified, the recipient performs signature verification. The receiver uses system common parameters to validate the sender's signature by computing $h_{i,2} = h_2(ID_i, Q_{ID_i})$ and $h_i = H_3(M_i, ID_i, Y_i, t_i)$, then checks if the following equation is met, $sign_i(M_i) \cdot P = h_i \cdot Q_i + Q_{ID_i} + h_{i,2} \cdot P_{pub}$, and if satisfied, the recipient accepts this certificateless signature. Since $P_{pub} = \alpha P$, $psk_{ID_i} = d_i + h_2(ID_i, Q_{ID_i}) \times \alpha \bmod q$, $Q_{ID_i} = d_i P$, $Q_i = s_i \cdot P$, and $sign_i(M_i) = h_i \cdot s_i + psk_{ID_i} \bmod q$. We obtain

$$\begin{aligned} sign_i(M_i) \cdot P &= \left(h_i \cdot s_i + psk_{ID_i}\right) \cdot P \\ &= h_i \cdot s_i \cdot P + \left(d_i + h_{i,2} \times \alpha\right) \cdot P \\ &= h_i \cdot Q_i + Q_{ID_i} + h_{i,2} \cdot P_{pub}. \end{aligned} \tag{12}$$

(2) Aggregate verify: when the node receives the message, the receiver first calculates:

$$h_1(n_i) = Y2_i \oplus H_1(Y1_i). \tag{13}$$

Extract from Y_i and calculate $h_1(Q_i \| h_1(n_i))$ to verify the trust value of V_i according to the location in the list, in which $i =, 1, 2, \ldots, n$. Once the authenticity of the sender's trust value is verified, the recipient performs signature verification. The receiver uses system common parameters to validate the sender's signature by computing $h_{i,2} = h_2(ID_i, Q_{ID_i})$ and $h_i = H_3(M_i, ID_i, Y_i, t_i)$, which $i =, 1, 2, \ldots, n$, then check that the following equation is met, $sign_i(M_i) \cdot P = \sum_{i=1}^{n}(h_i \cdot Q_i) + \sum_{i=1}^{n}(Q_{ID_i}) + \sum_{i=1}^{n}(h_{i,2}) \cdot P_{pub}$, and if satisfied, the recipient accepts this certificateless signature. Since $P_{pub} = \alpha P$, $Q_{ID_i} = d_i P$, $psk_{ID_i} = d_i + h_2(ID_i, Q_{ID_i}) \times \alpha \mathrm{mod} q$, $Q_i = s_i \cdot P$, and $sign_i(M_i) = h_i \cdot s_i + psk_{ID_i} \mathrm{mod} q$. We can get

$$\begin{aligned} S \cdot P &= \sum_{i=1}^{n} sign_i(M_i) \cdot P \\ &= \sum_{i=1}^{n}\left(h_i \cdot s_i + psk_{ID_i}\right) \cdot P \\ &= \sum_{i=1}^{n} h_i \cdot s_i \cdot P + \sum_{i=1}^{n}\left(d_i + h_{i,2} \times \alpha\right) \cdot P \\ &= \sum_{i=1}^{n} h_i \cdot Q_i + \sum_{i=1}^{n} Q_{ID_i} + \sum_{i=1}^{n} h_{i,2} P_{pub}. \end{aligned} \tag{14}$$

4.8. Identity Tracking. Once a vehicle sends a malicious message, the TRA can track the identity of the vehicle. Through the pseudoidentity $ID_i = (ID_{i,1}, ID_{i,2}, T_i)$, TRA

```
Require:
    $n_i = h_1 (TV_i \| AC\_TV_i)$
Ensure:
    $Y_i (Y1_i$ and $Y2_i)$ and $r_i (r1_i$ and $r2_i)$
    (i) The one-off public key $Y_i$ can be calculated as:
    $Y1_i = n_i \cdot a \cdot Q_i$; $Y2_i = h_1 (n_i) \oplus H_1 (n_i \cdot a \cdot Q_i)$
    Where $\alpha$ is a random number and $\oplus$ represent an XOR operation;
    (ii) The private key $r_i$ can be calculated as
    $r1_i = Y1_i \cdot s_i$; $r2_i = H_2 (Y1_i \| Y2_i) \cdot s_i$
```

Algorithm 1: Generation of one-off anonymous key pairs.

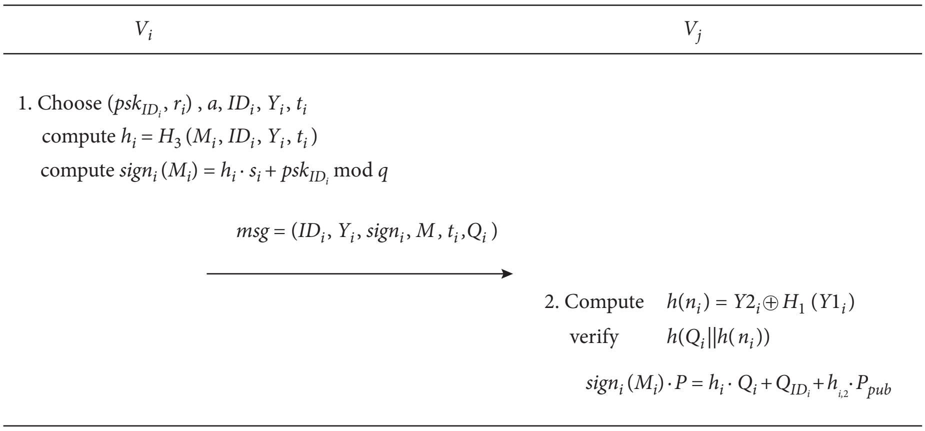
V_i
V_j
1. Choose (psk_{ID_i}, r_i) , a, ID_i, Y_i, t_i
compute $h_i = H_3 (M_i, ID_i, Y_i, t_i)$
compute $sign_i (M_i) = h_i \cdot s_i + psk_{ID_i} \bmod q$
$msg = (ID_i, Y_i, sign_i, M, t_i, Q_i)$
2. Compute $h(n_i) = Y2_i \oplus H_1 (Y1_i)$
verify $h(Q_i \| h(n_i))$
$sign_i (M_i) \cdot P = h_i \cdot Q_i + Q_{ID_i} + h_{i,2} \cdot P_{pub}$

Figure 3: Anonymous authentication process based on trust.

calculates the equation $RID_i = ID_{i,2} \oplus H_1 (\beta \cdot ID_{i,1}, T_i, T_{pub})$ to trace the vehicle's true identity. At the same time, the AP will reevaluate the trust of the vehicle and publish the updated list to all vehicle nodes. In addition, TA will update its database.

5. Security Proof and Analysis

Before we show that the proposed scheme has the security and privacy requirements, existential unforgeability of the signature, $sign_i (M_i)$, is proved in the random oracle model.

5.1. Security Model. The security model of the proposed scheme is to design a game between challenger $\mathscr{C}$ and adversary $\mathscr{A}$, that is, whether adversary $\mathscr{A}$ can win the challenge given by challenger $\mathscr{C}$ in polynomial time with a nonnegligible probability. Adversary $\mathscr{A}$ performs the query described below in the game.

(i) Setup: challenger $\mathscr{C}$ creates the public key and gives it to $\mathscr{A}$.

(ii) $h_2 (\cdot)$ queries: in this query, challenger $\mathscr{C}$ chooses a random $v_i \in Z_q^*$ and then adds (ID_i, Q_{ID_i}, v_i) into the hash list h_2^{list}. Finally, $\mathscr{C}$ sends $v_i = h_2 (ID_i, Q_{ID_i})$ to $\mathscr{A}$.

(iii) $Y (\cdot)$ queries: challenger $\mathscr{C}$ picks random $x_i \in Z_q^*$, inserts tuple $Y1_i$, $Y2_i$, x_i into Y^{list} and responds to $\mathscr{A}$ with $Y1_i$, $Y2_i$ in query i.

(iv) $H_2 (\cdot)$ queries: in this query, challenger $\mathscr{C}$ picks random $y_i \in Z_q^*$, inserts the tuples $Y1_j$, $Y2_i$, y_i, H_{2i} into Y^{list} and responds to $\mathscr{A}$ with H_{2i} in query i.

(v) $H_3 (\cdot)$ queries: in this query, challenger $\mathscr{C}$ picks random $u_i \in Z_q^*$, inserts the tuple u_i, m_i, H_{3i} to H_3^{list} and responds to $\mathscr{A}$ with $H_3 (m_i, ID_i, Y_i, t_i) = H_{3i}$.

(vi) Partial private key queries: in this query, challenger $\mathscr{C}$ calculates psk_{ID_i} and then the value psk_{ID_i} is outputted to $\mathscr{A}$.

(vii) Sign queries: after receiving the message M_i, $\mathscr{C}$ generates the request message $(ID_i, Y_i, sign_i, M_i, t_i, Q_i)$ and sends it to $\mathscr{A}$.

The probability that $\mathscr{A}$ may violate the authentication of proposed scheme Γ is expressed as $A\,dv_\Gamma^{Auth} (\mathscr{A})$.

Definition 3. The proposed scheme Γ for IOV is secure if $A\,dv_\Gamma^{Auth} (\mathscr{A})$ is negligible for any polynomial adversary $\mathscr{A}$.

5.2. Security Proof. In this subsection, to prove unforgeability of the proposed scheme, we need to show that it is unforgeable against adversary $\mathscr{A}$. If and only if CDHP is difficult, our scheme is safe under adaptive selective message attack in the random prediction model.

Theorem 1. *Unforgeability: make the prime order group $\mathbb{G}$ into $(\tau, t', \varepsilon')-$ CDH group, which implies that no challenger*

$\mathscr{C}(t\prime, \varepsilon\prime)$ can destroy CDHP on it. Therefore, the proposal is that the existence of an attack on adaptive selection is $(t, \varepsilon, q_Y, q_{h_2}, q_{H_2}, q_{H_3}, q_{pk}, q_S)$-secure, and $\varepsilon = eq_S\varepsilon\prime$, and $c_{\mathscr{C}}$ and $t = t\prime - c_{\mathscr{C}}(q_Y + q_{h_2} + q_{H_2} + q_{H_3} + q_{pk} + q_S)$ is constant, where e is the basis of the natural logarithm.

Game: adversary $\mathscr{A}$ has the advantage of ε and time t. Suppose $\mathscr{A}$ queries q_Y times for Y queries, q_{h_2} times for h_2 queries, q_{H_2} times for H_2 queries, q_{H_3} times for H_3 queries, q_{pk} times for Partial private key queries, and q_S times for Sign queries. And then, a challenger $\mathscr{C}$ who has the advantage of at least ε/eq_S and runtime:

$$t + c_{\mathscr{C}}\left(q_Y + q_{h_2} + q_{H_2} + q_{H_3} + q_{pk} + q_S\right), \tag{15}$$

to solve CDHP.

Proof. Challenger $\mathscr{C}$ gives parameters q, $\mathbb{G}$, e and random instance of CDHP, which is P, aP, bP, whereas P is a random generator of $\mathbb{G}$ with order q, a and b are random in Z_q^*. Let $D = abP \in \mathbb{G}$ be the solution for CDHP. Challenger $\mathscr{C}$ interacts with $\mathscr{A}$ to find the solution through the following query.

Setup: challenger $\mathscr{C}$ creates $K_{pub} = q, \mathbb{G}, P, h_2, H_2, H_3$ and gives it to $\mathscr{A}$. This is h_2, H_2, and H_3, which is a random oracle controlled by $\mathscr{C}$, as follows:

$h_2(\cdot)$ queries: when $\mathscr{A}$ makes a h_2 query with parameter (ID_i, Q_{ID_i}), $\mathscr{C}$ checks whether tuples already exist in the hash list h_2^{list}. In that case, $\mathscr{C}$ transfers $v_i = h_2(ID_i, Q_{ID_i})$ to $\mathscr{A}$. If not, $\mathscr{C}$ selects a random $v_i \in Z_q^*$ and then adds (ID_i, Q_{ID_i}, v_i) into the hash list h_2^{list}. Finally, $\mathscr{C}$ sends $v_i = h_2(ID_i, Q_{ID_i})$ to $\mathscr{A}$.

$Y(\cdot)$ queries: challenger $\mathscr{C}$ can query the public key Y. In response to queries, challenger $\mathscr{C}$ keeps tuple list $Y1_j$, $Y2_j$, x_j called Y^{list}. At first, it was empty. $\mathscr{C}$ selects random $x_i \in Z_q^*$, $Y2_i \in \{0,1\}^n$ and calculates $Y1_j = x_iP \cdot aP$. It then adds the tuples $Y1_i, Y2_i, x_i$ into Y^{list} and when querying i, it responds to $\mathscr{A}$ with $Y1_i$ and $Y2_i$.

$H_2(\cdot)$ queries: in response to queries, challenger $\mathscr{C}$ maintains list H_2^{list} in tuple $Y1_j$, $Y2_j$, y_j, H_{2j}. $\mathscr{C}$ picks random $y_i \in Z_q^*$ and sets $H_{2i} = H_2(Y1_i \| Y2_i) = y_iP$. Then, it adds the tuples $Y1_j$, $Y2_i$, y_i, H_{2i} into Y^{list} and when querying i, it responds to $\mathscr{A}$ with H_{2i}.

$H_3(\cdot)$ queries: in response to queries, challenger $\mathscr{C}$ keeps tuple list u_j, m_j, H_{3j}, called H_3^{list}. At first, it was empty. To respond to the query m_i, challenger $\mathscr{C}$ will do the following:

(1) If it already exists in the tuple u_i, m_i, H_{3i} in H_3^{list} when m_i is queried, $\mathscr{C}$ responds to $H_3(m_i, ID_i, Y_i, t_i) = H_{3i}$

(2) Otherwise, $\mathscr{C}$ only produces random bit $i_b \in \{0,1\}$, which will be determined later for ξ in $P_r[b_i = 1] = \xi$

(3) $\mathscr{C}$ selects random number $u_i \in Z_q^*$. If $b_i = 0$, it then sets $H_3(m_i, ID_i, Y_i, t_i) = H_{3i} = u_iP$. If $b_i = 1$, it then sets $H_3(m_i, ID_i, Y_i, t_i) = H_{3i} = bP \cdot u_iP$. Afterwards, $\mathscr{C}$ adds the tuple u_i, m_i, H_{3i} to H_3^{list} and responds to $\mathscr{A}$ with $H_3(m_i, ID_i, Y_i, t_i) = H_{3i}$. Note that H_{3i} is homogeneous in $\mathbb{G}$ and independent of $\mathscr{A}$.

Partial private key queries: $\mathscr{A}$ queries partial private key for pseudoidentity ID_i, $\mathscr{C}$ calculates $Q_{ID_i} = d_iP$ and then examines if the tuple (ID_i, Q_{ID_i}, v_i) already exists in the hash list h_2^{list}, where d_i is a random number. When the corresponding tuple $(ID_i, Q_{ID_i}, v_i)\mathscr{C}$ is not found, $\mathscr{C}$ will output a failure and stop because the query cannot be answered coherently. Or else $\mathscr{C}$ evaluates $psk_{ID_i} = d_i + h_2(ID_i, Q_{ID_i}) \times \alpha \mathrm{mod} q$ and outputs psk_{ID_i} to $\mathscr{A}$. It is worth noting that by calling this part of the partial private key query, $\mathscr{A}$ cannot obtain the psk_{ID_j} of the target user through ID_j.

Sign queries: the signature oracle is simulated by maintaining the list of tuples m_j, H_{3j}, σ_j in response to any message m_j signature query. We call this list S^{list}, which was initially empty. When $\mathscr{A}$ uses the message m_i to query oracle $Sign$, $\mathscr{C}$ responds to the query.

(1) If the query m_i already exists in the tuple m_i, H_{3i}, σ_i in S^{list}, challenger $\mathscr{C}$ responds with σ_i.

(2) Besides, $\mathscr{C}$ inspects whether (u_i, m_i, H_{3i}), $(Y1_i, Y2_i, x_i)$, (ID_i, Q_{ID_i}, v_i), and $(Y1_i, Y2_i, y_i, H_{2i})$ exist. Otherwise, $\mathscr{C}$ executes h_2-queries to obtain (ID_i, Q_{ID_i}, v_i), Y-queries to gain $(Y1_i, Y2_i, x_i)$, H_2-queries to obtain $(Y1_i, Y2_i, y_i, H_{2i})$, and H_3-queries to gain (u_i, m_i, H_{3i}). Next, $\mathscr{C}$ picks two random numbers r_i and h_i. If $b_i = 0$, $\sigma_i = h_i \cdot r_i + psk_{ID_i} \mathrm{mod} q$. If $b_i = 1$, it sets $\sigma_i = *$, value of placeholder. Finally, it adds tuple m_i, H_{3i}, σ_i to list S^{list} and replies to σ_i.

Challenge: challenger $\mathscr{C}$ publishes the signature query m_i. Challenger $\mathscr{C}$ obtains $\sigma_i \in \mathbb{G}$ by running the above algorithm in response to Sign queries. Note that $\mathscr{C}$ can use the public key K_{pub} to run $\mathscr{A}$ to obtain P, aP, H_{3i}, σ_i, which can be converted into a valid Diffie–Hellman tuple.

Claim: $\mathscr{A}$ stops, admit defeat, or forged signature $m\prime$, $\sigma\prime$, where $m\prime = m_{i*}$, for some i^* where $\mathscr{A}$ does not query the signature. If $\mathscr{A}$ is successfully forged, it means that CDHP is solved. At this time, $\mathscr{C}$ outputs "success." Otherwise, the $\mathscr{C}$ output "fails." $\mathscr{A}$ performed exactly as expected in the game model. Thus,

$$\begin{aligned} A\ dv_{\mathscr{C}} &= P_r\left[\mathscr{C}^{\mathscr{A}}(P, aP, bP) = \text{success: } a, b \in Z_q^*\right] \\ &= \left[\text{Verify}(Y, m\prime, \sigma\prime) = \text{valid: } \begin{smallmatrix} (Y,r)\leftarrow\text{OneoffKeyGen} \\ (m',\sigma')\leftarrow\mathscr{A}(Y) \end{smallmatrix}\right] \\ &= \varepsilon. \end{aligned} \tag{16}$$

By modifying, if $\mathscr{A}$ cannot create forgery, $\mathscr{C}$ will also fail. But if $\mathscr{A}$ finds m_{i^*}'s forgery successfully, $\mathscr{C}$ claims success only at $b_{i^*} = 1$, and $\mathscr{A}$ use index $i_1, i_2, \ldots, i_{q_S}$ to q_S sign oracle query for messages with $b_i = 0$ (for $b_i = 1$, $\mathscr{A}$ will stop immediately after the failure is declared), then $A\ dv_{\mathscr{C}}' = A\ dv_{\mathscr{C}} \cdot \Pr[b_{i^*} = 1] \cdot \Pr[b_{i_j} = 0, j = 1, 2, \ldots, q_S] = \xi(1-\xi)^{q_S}\varepsilon$.

Therefore, challenger $\mathscr{C}$ uses signature forger $\mathscr{A}$ to solve CDHP, which has the advantage of $\varepsilon\prime$ and time $t\prime$. The maximization of function $\xi(1-\xi)^{q_S}\varepsilon$ is at $\xi = 1/(1+q_S)$, of which it has the following values:

$$\frac{1}{1+q_S}\left(1-\frac{1}{1+q_S}\right)^{q_S}\cdot\varepsilon=\frac{1}{q_S}\left(1-\frac{1}{1+q_S}\right)^{q_S+1}\cdot\varepsilon. \tag{17}$$

For large q_S, $(1-1/(1+q_S))^{q_S+1}\approx 1/e$.

Meanwhile, $\mathscr{C}$'s running time consists of $\mathscr{A}$'s running time and the additional overhead, in which the group multiplication to evaluate each signature and hash request from $\mathscr{C}$ is the main part. Any such multiplication can be done by using up to $c_{\mathscr{C}}$ time units on $\mathbb{G}$. $\mathscr{C}$ may have to answer a request like $q_Y+q_{h_2}+q_{H_2}+q_{H_3}+q_{pk}+q_S$. Therefore, its overall runtime is $t+c_{\mathscr{C}}(q_Y+q_{h_2}+q_{H_2}+q_{H_3}+q_{pk}+q_S)$.

If there is a forgery $\mathscr{C}$ that $(t,\varepsilon,q_Y,q_{h_2},q_{H_2},q_{H_3},q_{pk},q_S)$ breaks our proposed scheme on $\mathbb{G}$, then there is a challenger $\mathscr{C}(t',\varepsilon')$ that can destroy CDHP, where $\varepsilon'=\varepsilon/(eq_S)$ and $t'=t+c_{\mathscr{C}}(q_Y+q_{h_2}+q_{H_2}+q_{H_3}+q_{pk}+q_S)$. On the contrary, if the group $\mathbb{G}$ is a (τ,t',ε')-CDH group, no challenger could break the proposed scheme, where $t=t'-c_{\mathscr{C}}(q_Y+q_{h_2}+q_{H_2}+q_{H_3}+q_{pk}+q_S)$ and $\varepsilon=eq_S\varepsilon'$. □

5.3. Security Analysis. We demonstrate that our proposal complies with all security and privacy requirements described in Section 3.3. As summarized by the comparison results in Table 3, we compared the proposal with other schemes for meeting security requirements, where SR1, SR2, SR3, SR4, and SR5, respectively, represent the authentication, anonymity, traceability, unlinkability, and replaying resistance. The comparison results show that the proposed scheme is superior. The security requirements of the proposed scheme are analyzed next.

Table 3: Comparison of security between related schemes and ours.

Scheme	[15]	[44]	[45]	Proposed
SR1	√	√	√	√
SR2	√	√	√	√
SR3	√	√	√	√
SR4	√		√	√
SR5				√

5.3.1. Authentication. For the following reasons, the proposed scheme provides message integrity and validity of sender identity: signature $sign_i(M_i)\cdot P$ is used to verify the authenticity of the message sent from vehicle to verifier vehicle. And, as shown in Theorem 1, in the random oracle model, signature $sign_i(M_i)\cdot P$ is nonforgery for adaptive selection message and identity attack under the difficulty of CDHP.

5.3.2. Anonymity. The INT value n_i given by AP (node or TAs) produces the one-off public key Y_i used in message authentication, which cannot be linked to the real identity. Moreover, in order to distinguish a one-off key pair for each message, V_i changes the random number each time (Y_i,r_i) is produced. Therefore, for the reason that TA is completely trusted, node privacy can be securely protected. For trust-based anonymous authentication, TA periodically distributes Ha to IOV nodes and uses its private key to sign. Ha's internal position on behalf of the trust value of V_i, however, does not link to the real identity of V_i and the true value of trust. Therefore, the proposed scheme provides anonymous authentication of identity privacy-preserving based on trust.

5.3.3. Traceability. Through the equation $RID_i=ID_{i,2}\oplus H_1(\beta\cdot ID_{i,1},T_i,T_{pub})$, TRA can track the identity of a malicious vehicle. Accordingly, when a vehicle is marked as controversial, TRA can track malicious vehicles to meet traceability requirements. Hence, our proposed scheme provides conditional privacy-preserving authentication.

5.3.4. Unlinkability. In our proposal, the INT values in aggregated lists (Ha or Ha_AP_j) are broken down into different levels. According to the INT value published by AP, each node generates n_i. We can set up an INT value range $n_i=h_1(TV_i\|AC\_TV_i)$ to represent a set of nodes that have the same trust level. Therefore, the trust value of many nodes may belong to the same level of trust. Even if the message receiver validates that the same n_i exists in Ha or Ha_AP_j, if during the period of authentication from the same node sent two or more messages, message receiver is indistinguishable. Specific vehicles cannot be linked to any two signatures, so the proposed scheme supports unlinkability.

5.3.5. Replaying Resistance. The time stamp t_i in the message $(ID_i,Y_i,sign_i,M_i,t_i,Q_i)$ is used to keep the message fresh. Vehicles will check the timestamp t_i freshness, so that they can detect the replay message. Therefore, our proposed scheme for IOV provides resistance against the replay attack.

6. Performance Evaluation

In this section, we will analyze the performance of the proposed scheme and compare it with the existing schemes proposed by Horng et al. [15], Bayat et al. [44], and Zhang et al. [45], respectively. The analysis of computation cost and communication overhead is highlighted below.

6.1. Computation Overhead and Comparison. The computational cost refers to the computational overhead of each entity in the authentication process. Table4provides the main operations of the four schemes in signing messages and authenticating a single signature, respectively.

The crypto-operations of Horng et al.'s scheme [15], Bayat et al.'s scheme [44] and Zhang et al.'s scheme [45] are established on bilinear pairings. Furthermore, the crypto-operations of the proposed scheme are established on ECC. In order to reach the 80-bit security level, we consider various parameters in pairing and ECC-based schemes, as given in Table 5.

Before the analysis of the computation cost, we define the time required for each cryptographic-related operation for signature and verification; a few notes to be used in comparison will be described below. In this paper, we use the experiment in Ref. [40] to learn the execution time of the

Table 4: Comparison of computation cost.

Scheme	Signing	Verification
Horng et al. [15]	$4T_{sm-bp} + 1T_{mtp}$	$2T_{bp} + 2T_{sm-bp} + 1T_{mtp}$
Bayat et al. [44]	$5T_{sm-bp} + 1T_{mtp}$	$3T_{bp} + 1T_{mtp}$
Zhang et al. [45]	$2T_{mtp}$	$2T_{bp} + 2nT_{sm-bp} + 2nT_{mtp}$
Proposed scheme	$1T_{mtp} + 1T_{sm-ecc}$	$3T_{sm-ecc} + 1T_{mtp}$

Table 5: Length of the group in bilinear pairing and ECC.

Type of the system	Type of curve	Cyclic group	$\vert \bar{p} \vert\vert p\vert$	$\vert G\vert$	Length of elements of the group
Bilinear pairing	E: $y^2 = x^3 + x(\mathrm{mod})p, a, b \in F_p$	$G_1(P)$	$\vert \bar{p} \vert = 512$ bits (64 bytes)	$q = 160$ bits	$\vert G_1\vert = 1024$ bits
ECC	E: $y^2 = x^3 + ax + b(\mathrm{mod})p, a, b \in F_p$	$G(P)$	$\vert p\vert = 160$ bits (20 bytes)	$q = 160$ bits	$\vert G\vert = 320$ bits

basic cryptographic operation by using the MIRACL library, running on the platform of 3.4 GHZ i7-4770. The following results are obtained from [40]: T_{sm-ecc} is 0.442 ms, $T_{sm-ecc-s}$ is 0.0276 ms, T_{sm-bp} is 1.709 ms, T_{mtp} is 4.406 ms, and T_{bp} is 4.211 ms. As a result of these, operating mainly determines the speed of signature verification, We're just going to talk about these five operations and ignore others, such as addition and one-way hash function.

(i) T_{sm-ecc}: the execution time of a scale multiplication operation $x \cdot P$ associated with ECC, where $x \in Z_q^*$ and $P \in \mathbb{G}$

(ii) $T_{sm-ecc-s}$: the execution time of a small scale multiplication operation $v_i \cdot p$ used in the small exponential test technique, where $P \in \mathbb{G}$, v_i is a small random integer in $[1, 2^t]$ and t is a small integer

(iii) T_{sm-bp}: the execution time of a scale multiplication operation $x \cdot P$ associated with the bilinear pairing, where $x \in Z_q^*$ and $P \in \mathbb{G}$

(iv) T_{mtp}: the execution time of a hash-to-point operation associated with the bilinear pairing, where the hash function maps a string to a point of $\mathbb{G}$

(v) T_{bp}: the execution time of a bilinear pairing operation $e(S, T)$, where $S, T \in \mathbb{G}$

First, we review the message signature time overhead. For Horng et al.'s b-SPECS + scheme [15], the vehicle needs to perform four scalar multiplication operations and one hash-to-point operation associated with the bilinear pairing. To sum up, the time overhead for this scheme is $4T_{sm-bp} + 1T_{mtp}$. For Bayat et al.'s scheme [44], the vehicle is required to perform five scalar multiplication operations and one hash-to-point operation associated with the bilinear pairing. To sum up, the time overhead for this scheme is $5T_{sm-bp} + 1T_{mtp}$. For Zhang et al.'s scheme [45], the vehicle needs to perform two hash-to-point operations related to the bilinear pairing. To sum up, the time overhead for this scheme is $2T_{mtp}$. For the proposed scheme, the vehicle needs to perform one scalar multiplication operation associated with the ECC and one hash-to-point operation associated with the bilinear pairing. To sum up, the time overhead for this scheme is $1T_{sm-ecc} + 1T_{mtp}$.

We observe the verification time of the signature through the verification equation. For Horng et al.'s scheme [15], the verifier is required to perform two bilinear pairing operations, two scalar multiplication operations, and one hash-to-point operation associated with the bilinear pairing. To sum up, the time overhead for this scheme is $2T_{bp} + 2T_{sm-bp} + 1T_{mtp}$. For Bayat et al.'s scheme [44], the verifier is required to perform three bilinear pairing operations, one scalar multiplication operation, and one hash-to-point operation associated with the bilinear pairing. To sum up, the time overhead for this scheme is $3T_{bp} + 1T_{mtp}$. For Zhang et al.'s scheme [45], the verifier is required to perform two bilinear pairing operations, two hash-to-point operations associated with the bilinear pairing, and two scalar multiplication operations. To sum up, the time overhead for this scheme is $2T_{bp} + 2T_{sm-bp} + 2T_{mtp}$. In our scheme, we evaluate the operation time of two parts of verification: trust authentication and signature verification. Thus, the verifier needs to perform three scalar multiplication operations associated with the ECC and one hash-to-point operation associated with the bilinear pairing. To sum up, the time overhead for this scheme is $3T_{sm-ecc} + 1T_{mtp}$.

The number of signatures during verification is then denoted by n. By batch verification of the equation, we can obtain that the verification time of n different signatures is $2T_{bp} + 2nT_{sm-bp} + nT_{mtp} = 7.824n + 8.422ms$ for Horng et al.'s scheme [15], $3T_{bp} + nT_{mtp} = 4.406n + 12.633ms$ for Bayat et al.'s scheme [44], and $2T_{bp} + 2nT_{sm-bp} + 2nT_{mtp} = 12.23n + 8.422ms$ for Zhang et al.'s scheme [45], respectively. For the authentication phase of n signatures of our proposed scheme, the execution time of the phase is $3nT_{sm-ecc} + nT_{mtp} = (5.732n)ms$.

Figure 4 shows the computational overhead of signing messages in each scheme. The linear relationship between the computation cost and the number of messages of four authentication schemes is given. Our proposed scheme has a slightly better performance time than Refs. [15, 44, 45]. The computational efficiency of our second scheme in this phase has been improved by 56.88% than Horng et al.'s scheme

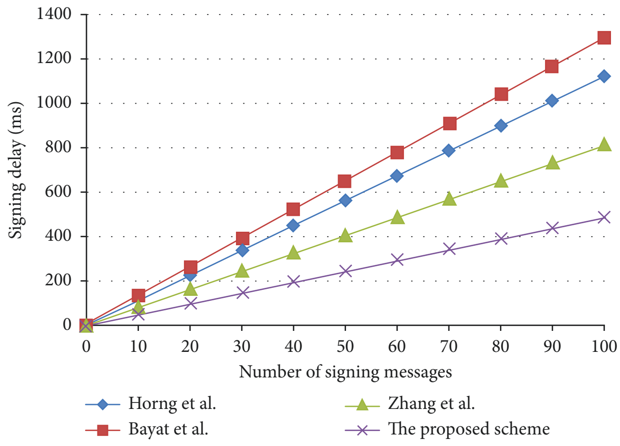

FIGURE 4: Delay in signing messages with respect to the number of messages.

[15], by 62.57% than Bayat et al.'s scheme [44], and by 40.30% than Zhang et al.'s scheme [45].

Figure 5 shows the total execution time for verifying n messages, as the number of vehicles in each scenario is increasing. We can see from the figure that Bayat et al.'s scheme's [44] execution time is less than Horng et al.'s scheme [15], Zhang et al.'s scheme [45], and our scheme in the authentication phase.

6.2. Communication Overhead. In this subsection, we compare the communication overhead of the proposed scheme with other schemes, as given in Table 6.

According to the analysis in Section 6.1, $|\bar{p}|$ and $|p|$ are 64 and 20 bytes, respectively. Consequently, bytes of elements in group $\mathbb{G}_1$ and group $\mathbb{G}$ are 128 bytes and 40 bytes, respectively. Assuming that the number of bytes of message time t_i is 4 bytes, the number of bytes of RID is 20 bytes, and the number of bytes of the general hash function's output is 20 bytes, the communication overhead of a complete verification in the authentication scheme of IOV usually consists of vehicle signatures, pseudoidentities, current time stamps, and public keys, while the message itself is not considered.

Because of identity-based encryption, Horng et al.'s scheme [15] does not require any signing certificate together with the message to send. Instead, send a 42 byte pseudoidentity, i.e., $|ID_i| = |ID_{i_1}| + |ID_{i_2}| = 42$ bytes, and the length of a signature is 21 bytes. Thus, the total transmission overhead is 42 + 21 = 63 bytes. In Bayat et al.'s scheme [44], the verifier receives the broadcast anonymous identity and signature (AID_i, T_i, U_i) from the vehicle, where $AID_i = \{AID_i^1, AID_i^2\}, AID_i^1, AID_i^2, U_i \in G_1$ and T_i is the timestamp. To sum up, the communication cost is $128 \times 3 + 4 = 388$ bytes. In Zhang et al.'s scheme [45], the vehicle signs the message as $(m_i, PPID_{i,t}, \sigma_{i,t})$. The overhead of communication can also be calculated using the method shown above. For our proposed scheme, the vehicle signs the message as $ID_i, Y_i, sign_i, M, t_i, Q_i$ and broadcasts it to the verifier, where $ID_i = (ID_{i,1}, ID_{i,2}, T_i)$, Q_i, $sign_i$ both are elements in $\mathbb{G}$. $Y_i = (Y1_i, Y2_i)$ where $Y1_i$ is an element in $\mathbb{G}$, and $Y2_i$ is an array of 20 bytes. T_i and t_i are the timestamp. Thus, the proposed scheme has a communication overhead of $40 \times 5 + 20 + 4 \times 2 = 228$ bytes.

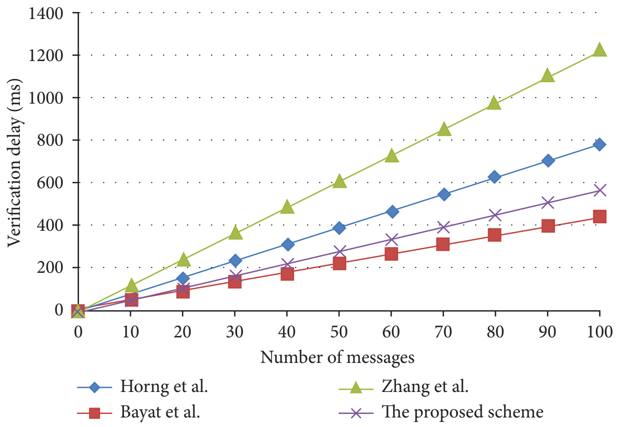

FIGURE 5: Delay in verifying messages with respect to the number of messages.

TABLE 6: Comparison of communication cost.

Scheme	Message	Length (byte)
Horng et al. [15]	$(ID_i, M_i, \sigma i)$	63
Bayat et al. [44]	(AID_i, T_i, U_i)	388
Zhang et al. [45]	$(m_i, PPID_{i,t}, \sigma_{i,t})$	148
Proposed scheme	$(ID_i, Y_i, sign_i, M_i, t_i, Q_i)$	228

7. Conclusion and Future Work

In the proposal, we proposed a scheme to authenticate the trust of vehicle nodes in IOV. First, our scheme not only provided anonymous authentication of trust but also an effective conditional privacy tracking mechanism, which achieved identity authentication and conditional preserving of privacy, and improved the reliability of V2V communication messages. Next, our proposed scheme realized efficient certificateless authentication, which is based on ECC and replaced the trust on revocation list. Furthermore, we also proved that the proposed scheme is secure against existential forgery in the random oracle model under the CDHP. In future work, we will further consider the characteristics of IOV to design a more efficient scheme, such as high dynamics. In addition, testing the efficiency, adaptability, and robustness of the scheme in a real environment is also an issue to be addressed in the future.

Data Availability

The data used to support this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was funded by the Anhui first-class undergraduate talent demonstration and leading base (2019rcsfjd088).

References

[1] S. S. Manvi and S. Tangade, “A survey on authentication schemes in vanets for secured communication,” *Vehicular Communications*, vol. 9, pp. 19–30, 2017.

[2] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, “Ecpp: efficient conditional privacy preservation protocol for secure vehicular communications,” in *Proceedings of the INFOCOM 2008. The Conference on Computer Communications*, pp. 1229–1237, IEEE, Phoenix, AZ, U.S.A, April 2008.

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

[4] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, “Pa-crt: PA-CRT: Chinese remainder Theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2021.

[5] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, “Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in vanets,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 1681–1695, 2021.

[6] S. J. Horng, S. F. Tzeng, T. Li, X. Wang, P. H. Huang, and M. K. Khan, “Enhancing security and privacy for identity-based batch verification scheme in vanet,” *IEEE Transactions on Vehicular Technology*, vol. 66, p. 1, 2017.

[7] 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 Transactions on Vehicular Technology*, vol. 70, no. 4, pp. 3456–3468, 2021.

[8] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, “A scalable robust authentication protocol for secure vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

[9] L. Wei, J. Cui, H. Zhong, I. Bolodurina, and L. Liu, “A lightweight and conditional privacy-preserving authenticated key agreement scheme with multi-ta model for fog-based vanets,” *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2021.

[10] S. Gyawali, Y. Qian, and R. Q. Hu, “A privacy-preserving misbehavior detection system in vehicular communication networks,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, pp. 6147–6158, 2021.

[11] M. Najafi, L. Khoukhi, and M. Lemercier, “A multidimensional trust model for vehicular ad-hoc networks,” in *Proceedings of the 2021 IEEE 46th Conference on Local Computer Networks (LCN)*, pp. 419–422, IEEE, Canada, October 2021.

[12] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung, “A context-aware trust-based information dissemination framework for vehicular networks,” *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 121–132, 2015.

[13] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[14] K. A. Shim, “${\cal CPAS}$: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks,” *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1874–1883, 2012.

[15] S. J. Horng, S. F. Tzeng, Y. Pan et al., “b-specs+: b-SPECS+: batch verification for secure pseudonymous authentication in VANET,” *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1860–1875, 2013.

[16] J. Shao, X. Lin, R. Lu, and C. Zuo, “A threshold anonymous authentication protocol for vanets,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[17] J. Li, K. K. R. Choo, W. Zhang et al., “Epa-cppa: an efficient, provably-secure and anonymous conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *Vehicular Communications*, vol. 13, pp. 104–113, 2018.

[18] Z. Liu, Z. Liu, L. Zhang, and X. Lin, “Marp: a distributed mac layer attack resistant pseudonym scheme for vanet,” *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 4, pp. 869–882, 2020.

[19] X. Liu, Y. Yang, E. Xu, and Z. Jia, “An authentication scheme in vanets based on group signature,” in *Proceedings of the International Conference on Intelligent Computing*, pp. 346–355, Springer, Berlin, Germany, July 2019.

[20] A. Boualouache, S. M. Senouci, and S. Moussaoui, “Privanet: an efficient pseudonym changing and management framework for vehicular ad-hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 8, pp. 3209–3218, 2020.

[21] H. Du, Q. Wen, and S. Zhang, “An efficient certificateless aggregate signature scheme without pairings for healthcare wireless sensor network,” *IEEE Access*, vol. 7, pp. 42683–42693, 2019.

[22] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, “Privacy-preserving authentication scheme with full aggregation in vanet,” *Information Sciences*, vol. 476, pp. 211–221, 2019.

[23] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, “Nera: a new and efficient rsu based authentication scheme for vanets,” *Wireless Networks*, vol. 26, no. 5, pp. 3083–3098, 2020.

[24] G. K. Verma, B. B. Singh, N. Kumar, and V. Chamola, “Cb-cas: certificate-based efficient signature scheme with compact aggregation for industrial internet of things environment,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2563–2572, 2020.

[25] Z. Xu, D. He, N. Kumar, and K. K. R. Choo, “Efficient certificateless aggregate signature scheme for performing secure routing in vanets,” *Security and Communication Networks*, vol. 2020, Article ID 5276813, 12 pages, 2020.

[26] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, “Efficient certificateless aggregate signature with conditional privacy preservation in iov,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 245–256, 2021.

[27] Y. Chen and J. Chen, “Cpp-clas: efficient and conditional privacy-preserving certificateless aggregate signature scheme for vanets,” *IEEE Internet of Things Journal*, vol. 9, 2021.

[28] I. Ali, Y. Chen, N. Ullah, R. Kumar, and W. He, “An efficient and provably secure ecc-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in vanets,” *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1278–1291, 2021.

[29] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, “Privacy in inter-vehicular networks: why simple pseudonym change is not enough,” in *Proceedings of the International Conference on Wireless On-Demand*, pp. 176–183, Network Systems & Services, Slovenia, February 2010.

[30] M.-C. Chuang and J. F. Lee, "Team: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Systems Journal*, vol. 8, no. 3, pp. 749–758, 2014.

[31] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (vanet)," *Wireless Networks*, vol. 24, no. 2, pp. 373–382, 2016.

[32] Z. Yan, P. Wang, and W. Feng, "A novel scheme of anonymous authentication on trust in pervasive social networking," *Information Sciences*, vol. 445, pp. 79–96, 2018.

[33] J. Liang and M. Ma, "Ecf-mrs: an efficient and collaborative framework with markov-based reputation scheme for idss in vehicular networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 278–290, 2021.

[34] Y. Begriche, R. Khatoun, A. Rachini, and L. Khoukhi, "A reputation system using a bayesian statistical filter in vehicular networks," in *Proceedings of the 2020 Sixth International Conference on Mobile and Secure Services (MobiSecServ)*, pp. 1–7, IEEE, Miami Beach, FL, USA, February 2020.

[35] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, and S. Khan, "Stabtrust—a stable and centralized trust-based clustering mechanism for iot enabled vehicular ad-hoc networks," *IEEE Access*, vol. 8, pp. 21159–21177, 2020.

[36] A. Alnasser, H. Sun, and J. Jiang, "Recommendation-based trust model for vehicle-to-everything (v2x)," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440–450, 2020.

[37] X. Chen, J. Ding, and Z. Lu, "A decentralized trust management system for intelligent transportation environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 558–571, 2022.

[38] H. Gao, C. Liu, Y. Yin, Y. Xu, and Y. Li, "A hybrid approach to trust node assessment and management for vanets cooperative data communication: historical interaction perspective," *IEEE Transactions on Intelligent Transportation Systems*, 2021.

[39] F. Ahmad, F. Kurugollu, C. A. Kerrache, S. Sezer, and L. Liu, "Notrino: a novel hybrid trust management scheme for internet-of-vehicles," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 9244–9257, 2021.

[40] J. Cui, L. Wei, J. Zhang, Y. Xu, and H. Zhong, "An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, 2018.

[41] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[42] V. S. Miller, *Use of elliptic curves in cryptography Advances in Cryptology-CRYPTO'85*, Springer, vol. 218pp. 173–1933, 1986.

[43] S. Biswas, J. Mišic, and V. Mišic, "Id-based safety message authentication for security and trust in vehicular networks," in *Proceedings of the International Conference on Distributed Computing Systems Workshops*, pp. 323–331, Minneapolis, MN, U.S.A, June 2011.

[44] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[45] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.