Hindawi
Security and Communication Networks
Volume 2021, Article ID 6638453, 14 pages
https://doi.org/10.1155/2021/6638453

Research Article

Efficient Anonymous Data Authentication for Vehicular Ad Hoc Networks

Ping Yu,[1,2] **Wei Ni**,[3] **Guangsheng Yu**,[2] **Hua Zhang**,[1] **Ren Ping Liu**,[2] **and Qiaoyan Wen**[1]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*Global Big Data Technologies Centre, University of Technology Sydney, Sydney 2007, NSW, Australia*
[3]*CSIRO, Sydney 2122, NSW, Australia*

Correspondence should be addressed to Hua Zhang; zhanghua_288@bupt.edu.cn and Qiaoyan Wen; wqy@bupt.edu.cn

Received 15 October 2020; Revised 16 January 2021; Accepted 31 January 2021; Published 23 February 2021

Academic Editor: Leandros Maglaras

Vehicular ad hoc network (VANET) encounters a critical challenge of efficiently and securely authenticating massive on-road data while preserving the anonymity and traceability of vehicles. This paper designs a new anonymous authentication approach by using an attribute-based signature. Each vehicle is defined by using a set of attributes, and each message is signed with multiple attributes, enabling the anonymity of vehicles. First, a batch verification algorithm is developed to accelerate the verification processes of a massive volume of messages in large-scale VANETs. Second, replicate messages captured by different vehicles and signed under different sets of attributes can be dereplicated with the traceability of all the signers preserved. Third, the malicious vehicles forging data can be traced from their signatures and revoked from attribute groups. The security aspects of the proposed approach are also analyzed by proving the anonymity of vehicles and the unforgeability of signatures. The efficiency of the proposed approach is numerically verified, as compared to the state of the art.

1. Introduction

Vehicular ad hoc network (VANET), also known as the Internet of Vehicles (IoV), enables vehicles to broadcast road incidents and supports critical road safety and traffic management applications, such as emergency warning, collision avoidance, road condition broadcast, and lane-changing assistance [1]. Each vehicle is expected to be equipped with an on-board unit (OBU) to collect traffic information and transmit captured data to the network to support various applications [2]. Road side units (RSUs) are infrastructures that connect vehicles to the internet and collect data captured by vehicles [3]. They can communicate with vehicles by using communication protocols, such as IEEE 802.11p protocol [4]. Based on the aggregated data, some timely actions can be taken, and hence, traffic safety and efficiency can be improved.

As a large-scale open network, VANET faces a critical issue in message authentication [5]. One of the key challenges is how to protect the anonymity of vehicles that capture, authenticate, and upload data against potential adversaries, while preserving the traceability of any malicious vehicles which forge data and infrastructure which conclude with those vehicles. Another challenge is efficiency in terms of computation and storage [6]. There can be large amounts of data captured and certified by different vehicles at every moment in a large-scale VANET. Computational efficiency is critical to the authentication process. There can also be many replicas of the same data in the network. Multiple vehicles can make the same observation, separately authenticate, and upload replicas [7]. The replicas would incur substantial storage overhead, e.g., at cloud service provider (CSP).

1.1. Aim, Background, and Motivation. Typical solutions for anonymous message authentication are pseudonym-based techniques, group signature, ring signature, and attribute-based signature (ABS). In pseudonym-based schemes [8–10], each vehicle is equipped with multiple credentials or

public keys to break the linkage between its messages. Such schemes define a time period τ and require each vehicle to change its pseudonym every τ time. Besides the anonymity of vehicles, the signature techniques, such as group signature [11–13], ring signature [14, 15], and ABS [16, 17], can be applied to achieve data integrity. Specifically, a message can be embedded into its signature by using a public hash function and then attached to the signature [17]. If the attached message is incomplete or tampered with, the hash value would be different from the embedded, and then the verification fails. In group signature schemes [11–13], a group manager integrates the identities of individuals in a group as the public information of the group, and each vehicle signs its messages on the behalf of the group [18]. In these schemes [11–13], each vehicle maintains a list of revoked vehicles. This method makes the verification time (or delay) of the signatures to grow linearly with the number of revoked vehicles. Ring signature [14, 15, 19] is considered to be a simplified group signature that only consists of vehicles, not managers. Each signer collects the public keys of vehicles in the ring and signs its messages on the behalf of the ring for anonymity. However, the revocation of compromised signers is challenging in many practical scenarios [20].

Attribute-based cryptography defines each vehicle by referring to a set of attributes, all of which are owned by multiple vehicles [21]. It protects the identities of the signers from being obtained by the public network and thus provides the anonymity of the signers. A trusted authority (TA) validates the attributes of each vehicle and generates the corresponding secret keys to ensure that data is only uploaded by vehicles with legitimate attributes. Most of the ABS techniques, such as [16, 17], only allow the signatures to be verified one by one, resulting in linear growth of the delay required to verify signatures with an increasing number of messages. The attribute-based techniques are generally unsuitable to large-scale systems where the volume of data is large, such as VANETs [22].

1.2. Contribution. This paper presents a new and effective ABS approach for data authentication in VANETs, which protects the anonymity of vehicles against adversaries and the integrity and unforgeability of data, preserves the traceability of malicious vehicles, and facilitates revocations of malicious vehicles. The approach is also efficient in the sense that multiple signatures by different vehicles for different data can be computationally and efficiently verified together. Moreover, replicas signed by different vehicles can be aggregated and dereplicated with improved storage efficiency. The key contributions of the paper are summarized as follows:

(1) We propose a new ABS scheme enabling the identification of malicious vehicles and infrastructures and the revocation of the attribute memberships of the vehicles. The malicious vehicles forging data can be revoked from their attribute groups.

(2) Multiple messages generated and authenticated by different vehicles can be verified together via batch operations. New algorithms are developed to verify the signatures, based on the attributes involved, and are independent of the number of messages, hence substantially cutting off the authentication delay.

(3) The same data signed by different vehicles can be dereplicated while the traceability of each of the vehicles remains, hence significantly saving the storage overhead of the data.

The proposed anonymous authentication approach is numerically verified by comparing it with the state of the art. As shown by the simulations, the batch verification algorithm and the data dereplication approaches can significantly reduce the computational cost in verifying multiple signatures and the storage overhead of replicas at the CSP, respectively.

1.3. Organization and Notation. The rest of this paper is organized as follows. In Section 2, related studies are reviewed, followed by the system architecture in Section 3. In Sections 4 and 5, we propose the new authentication approach and two new efficient algorithms to accelerate signature verification. We define the security model and prove the security of the proposed approach in Section 6. In Section 7, the efficiency of the proposed approach is validated numerically in comparison with existing techniques, followed by concluding remarks in Section 8. Table 1 lists the notations used in the paper.

2. Related Work

In pseudonym-based schemes, each vehicle is issued a short-term pseudonym and corresponding private key. With the pseudonym and private key, a vehicle can anonymously generate identity-based aggregate signatures by choosing a one-time string. In [9], the authors adopted a hash message authentication code to achieve efficient authentication. However, frequent changes of pseudonyms could not be avoided. In [22], a pseudonym-based anonymous authentication in VANET was proposed. Multiple vehicles shared the same secret value to support batch verification. This would be inconvenient for highly dynamic networks, such as VANET, where vehicles move all the time and the messages to be batch-verified may be from the vehicles not sharing the same secret value.

In group signature schemes [11–13], a group manager integrates the identities of individuals in a group as the public information of the group, and each vehicle signs its messages on the behalf of the group [18]. In these schemes [11–13], each vehicle maintains a list of revoked vehicles. This method makes the verification time (or delay) of the signatures to grow linearly with the number of revoked vehicles. The authors of [23] proposed an anonymous authentication system by using a time-dependent group signature technique supportive of signer revocation. The authors assumed the existence of a time-dependent token. Each signer with a unique identity can generate a signature on a message by using its secret keys and the time token. Multiple messages of the same signer are linkable if they are signed within a given period. The authors of [12] proposed a

Table 1: Notation and definition.

Notation	Definition
N	The number of attributes in the system
S_N	The set of attributes in the system
λ	Security parameter of the system
$\mathscr{V}_i$, $\mathscr{A}_k$	i-th vehicle and the k-th RSU
K_P	System-wide public key
K_M	System master secret key
K_j	System attribute public key
$K_{S,\mathscr{V}_i}$	Vehicle secret key of the i-th vehicle $\mathscr{V}_i$
$K_{S,\mathscr{V}_i,j}$	Vehicle attribute secret key of $\mathscr{V}_i$
u_i	Identity of the i-th vehicle
S_i	Attribute set of vehicle $\mathscr{V}_i$
$\mathscr{M}, \Delta$	A message and its signature
S_{A_j}	The set of vehicles equipped with attribute j
v_j	The membership version of attribute j
$\mathbb{VL}_j$	The list of public keys of vehicles with attribute j

threshold group signature scheme, where receivers only accept messages confirmed by more than a prespecified number of vehicles.

Ring signature [14, 15, 19] is considered to be a simplified group signature that only consists of vehicles, not managers. Each signer collects the public keys of vehicles in the ring and signs its messages on the behalf of the ring for anonymity. Au [14] proposed a scheme with constant signature size and proved its security under the Diffie–Hellman inversion assumption. In [19], a secure and unrestricted identity-based ring signature scheme was developed. The authors proved that their scheme can achieve signer anonymity in the standard model. However, the revocation of compromised signers is challenging in many practical scenarios [20].

ABS was first proposed in [21] as a primitive to protect the privacy of message signers. Each message is signed by a predicate of attributes. In [16], the ABS technique was employed to achieve outsourced cloud data integrity auditing. A data owner could specify designated auditors with particular attributes to confirm the integrity of the data. In [17], the anonymity of vehicles was ensured by a (t, n) threshold predicate. In addition, the authors designed that the identity of a malicious vehicle could be traced from its signature and revoked from the attribute groups. In [20], all data were signed under a threshold predicate. Specifically, a signature was generated under a threshold gate predicate. The verification of the signature could only confirm that the signatures were generated by t attributes out of n.

Batch verification has been widely employed in anonymous vehicular scenarios to accelerate signature verification [9, 22, 24–30]. Multiple signatures can be verified together, thus shortening latency. An identity-based aggregate signature was proposed in [26]. The individual identity-based signatures generated by different vehicles can be aggregated and verified together. The messages signed under the same one-time string can be aggregated and verified by the nearby RSUs. Zhang et al. [30] proposed a one-time identity-based aggregate signature. The system proposed in [30] includes a trusted authority (TA) and multiple lower-level TAs. The signature is only valid under the user's identity and public information of the lower-level TAs. Multiple signatures can be verified together, and the signatures can be compressed into one to reduce storage requirement.

3. System Architecture

Figure 1 shows the proposed system which consists of a TA, a large number of vehicles, multiple RSUs, and a CSP.

The TA is the only fully trusted entity in the system. It produces public parameters of the system, initializes RSUs by publishing public keys, and registers vehicles by issuing secret keys for their legitimate attributes. The TA is also responsible for identifying malicious vehicles that forge messages and revoking the vehicles and/or their attributes. Each vehicle registers at the TA and requests the secret keys corresponding to its attributes. The TA issues a dedicated random value (as the identity of the vehicle) and embeds the value into all of the attribute-related secret keys of the vehicle. This ensures the traceability of the signatures of the vehicle by the TA.

Each vehicle can sign messages by using a subset of its attribute secret keys and send the signed messages to its nearest RSU. The use of attributes ensures the anonymity of vehicles. Any adversaries can only infer that the message is generated by a qualified vehicle with legitimate attributes and cannot identify the vehicle.

The RSUs are fixed infrastructures at the roadside and act as a bridge between vehicles and CSP. They are responsible for collecting messages sent by vehicles, transferring the messages to the CSP, and providing services to nearby vehicles.

In our scheme, the CSP is connected to all the RSUs. It has the ability to verify all the signatures from the network and make decisions based on these data. The CSP can verify multiple signatures at once by using the proposed batch verification algorithm and suppress replicas signed by different vehicles to improve its storage efficiency.

The proposed efficient attribute-based anonymous authentication system constitutes the following suite of new algorithms:

(i) Initialization: $\lambda \longrightarrow \left\{K_P, K_P', K_M, \left\{K_j\right\}_{\forall j \in S_N}\right\}$. The TA takes a security parameter λ as the input and outputs the system public keys (PKs) K_P and K_P', the system master secret key (MSK) K_M, and system attribute public keys K_j for each legitimate attribute $j \in S_N$ of the system.

(ii) Vehicle registration: $\left\{\mathscr{V}_i, S_i, K_M, \left\{K_j\right\}_{\forall j \in S_i}\right\} \longrightarrow \left\{K_{S,\mathscr{V}_i}, \left\{K_{S,\mathscr{V}_i,j}\right\}_{\forall j \in S_i}\right\}$. By taking K_M and $\left\{K_j\right\}_{\forall j \in S_i}$ as the input, the TA generates the vehicle secret key $K_{S,\mathscr{V}_i}$ for the vehicle and vehicle attribute secret keys $K_{S,\mathscr{V}_i,j}$ for each attribute $j \in S_i$ of the vehicle $\mathscr{V}_i$.

(iii) Signature generation: $\left\{K_P, K_P', \left\{K_j\right\}_{\forall j \in S_i}, K_{S,\mathscr{V}_i}, \left\{K_{S,\mathscr{V}_i,j}\right\}_{\forall j \in S_i}, \mathscr{M}\right\} \longrightarrow \Delta$. With the input of the public parameters, i.e., K_P, K_P', and $\left\{K_j\right\}_{\forall j \in S_i}$, the vehicle $\mathscr{V}_i$ signs the data $\mathscr{M}$ by using a subset of its

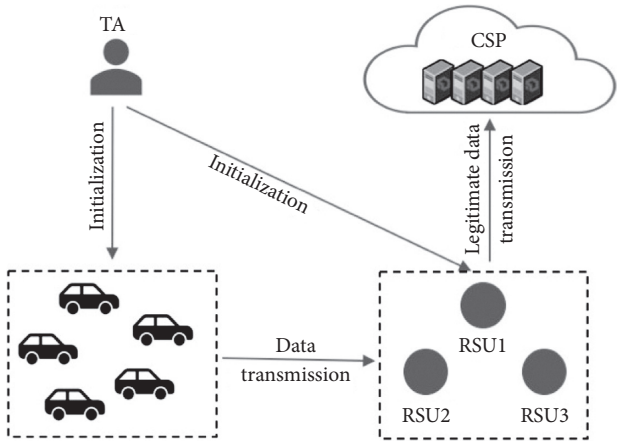

Figure 1: Architecture of the proposed system.

attribute set, denoted by $S_i' \subset S_i$. The vehicle $\mathscr{V}_i$ outputs the signature Δ with the data $\mathscr{M}$.

(iv) Signature verification: $\left\{K_P, K_P', \left\{K_j\right\}_{\forall j \in S_i'}, \Delta\right\} \longrightarrow$ "0" or "1". The CSP takes the system public parameters and the signature Δ as the input, verifies the signature, and outputs "0" or "1" to indicate that the signature is verified unsuccessfully or successfully, respectively.

(v) Trace: $\{K_M, \Delta\} \longrightarrow \mathscr{V}_i$. Given the MSK and Δ, the TA retrieves the identity of the vehicle by running this algorithm.

(vi) Attribute revocation: $\left\{K_M, K_j, \mathscr{V}_i\right\} \longrightarrow \left\{K_j', K_{S,\mathscr{V}_i,j}'\right\}$. The TA can revoke any attribute j of any vehicle i by taking the system attribute public key of attribute j as the input and then generates a new system attribute public key and vehicle attribute secret keys.

As part of the suite of algorithms, two new algorithms are explicitly designed to accelerate the verification process of the proposed attribute-based anonymous authentication system in VANETs.

(i) Batch verification: $\left\{K_P, K_P', \left\{K_j\right\}_{\forall j \in S_N}, \left\{\Delta_k\right\}_{\forall k \in [1,L]}\right\} \longrightarrow$ "0" or "1". The CSP is designed to verify multiple messages signed by different vehicles together using batch operations. Given the signatures $\Delta_1, \ldots, \Delta_L$, the CSP outputs "1" to indicate that all the L signatures are legitimate. Otherwise, the CSP outputs "0."

(ii) Dereplication: $\left\{K_P, K_P', \left\{K_j\right\}_{\forall j \in S_N}, \left\{\Delta_k\right\}_{\forall k \in [1,K]}\right\} \longrightarrow \Delta$. Given K signatures of the same message, the CSP generates a new signature Δ, which records that the message has been signed by K vehicles and preserves the traceability of the vehicles.

4. Anonymous Authentication Algorithm

4.1. System Parameter Initialization. The TA initializes the system by generating the system public key, MSK, and the system attribute public keys. Suppose that there are N attributes in the system. The set S_N collects all the N attributes. The TA first generates two groups $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$. Let g and $e(g, g)$ be the generators of groups $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$, respectively. e is a bilinear mapping (given two multiplicative groups $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ with prime order p, the bilinear mapping e maps two elements in $\mathbb{G}$ to another element in $\mathbb{G}_{\mathbb{T}}$, i.e., e: $\mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_{\mathbb{T}}$. This mapping has two properties: (1) bilinearity: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$, $a, b \in \mathbb{Z}_P$, where $\mathbb{Z}_P$ is an additive cyclic group [31]. (2) Nondegeneracy: $e(g, g) \neq 1$. Here, the number of bits in an element of the multiplicative group depends on a security parameter λ) which maps any two elements in $\mathbb{G}$ to an element in $\mathbb{G}_{\mathbb{T}}$. $H(\cdot)$ is a hash function which maps a binary sequence to an element in $\mathbb{G}$, i.e., $\{0, 1\}^* \longrightarrow \mathbb{G}$. By using $H(\cdot)$, any message can be mapped to a group element in $\mathbb{G}$ and embedded into a signature.

The TA selects two random values $\alpha, \beta \in \mathbb{Z}_p$ as the system master secret key (MSK), $K_M = \{\alpha, \beta\}$, and publishes the system public keys $K_P = g^{\alpha\beta}$ and $K_P' = g^{\beta}$. The MSK is only known to the TA to trace misbehaved or malicious vehicles. For each attribute j, the TA selects random values v_j and $s_j \in \mathbb{Z}_p$, sets $h_j = g^{s_j}$, and generates the system attribute public keys for attribute j, denoted by K_j, as given by

$$K_j = h_j^{\beta v_j}, \tag{1}$$

where v_j indicates the current version of the membership of attribute group j. v_j is important to revoke the attributes of vehicles (as will be described in Section 4.5). The system public key and system attribute public keys are given by

$$PP = \left\{K_P, K_P', \left\{\forall j \in S_N \colon K_j\right\}\right\}. \tag{2}$$

For each attribute j, the TA maintains the vehicle public keys of all the vehicles equipped with the attribute, denoted by $\mathbb{VL}_j$:

$$\mathbb{VL}_j = \left\{\forall i \in S_{A_j} \colon e(g, g)^{u_i}\right\}, \tag{3}$$

where S_{A_j} is the current set of vehicles with attribute j. The TA publishes $\mathbb{VL}_j$. If the membership of attribute j changes, the TA updates the value v_j and the system attribute public key K_j and cancels $e(g, g)^{u_i}$ of any revoked vehicle $\mathscr{V}_i$ from $\mathbb{VL}_j$, i.e., $\mathbb{VL}_j' = \mathbb{VL}_j / e(g, g)^{u_i}$.

4.2. Registration of the Vehicle. For each vehicle, the TA assigns a unique random value u_i and generates $e(g, g)^{u_i}$ as the vehicle public key of the vehicle. The TA also computes the vehicle secret key $K_{S,\mathscr{V}_i}$ for the vehicle. $K_{S,\mathscr{V}_i} = g^{u_i}$. Suppose that each vehicle $\mathscr{V}_i$ has the set of attributes S_i. The vehicle can sign messages by using a subset of its attributes. For each attribute of the vehicle $j \in S_i$, the TA generates the vehicle attribute secret key as follows:

$$K_{S,\mathscr{V}_i,j} = h_j^{u_i v_j} \cdot g^{\alpha} a. \tag{4}$$

The secret key of vehicle $\mathscr{V}_i$ is given by

$$SK = \left\{K_{S,\mathscr{V}_i}, \left\{K_{S,\mathscr{V}_i,j}, \forall j \in S_i\right\}\right\}. \tag{5}$$

Note that the random value u_i which is specific to the i-th vehicle is embedded into the vehicle attribute secret key $K_{S,\mathscr{V}_i,j}$ to retain the traceability of the vehicle. The vehicle may broadcast faked messages. The unique value of the vehicle, u_i, can be recovered by the TA from any signature of the vehicle, as will be described in Section 4.5, and thus ensures the traceability of the vehicle. Moreover, no attacker can forge the signatures of the vehicle without the secret value u_i.

4.3. Signature Generation. Any vehicle $\mathscr{V}_i$ can sign a message $\mathscr{M}$ by using a subset of its attributes $S_i' \subset S_i$. The vehicle selects a random value $x \in \mathbb{Z}_p$ and maps $\mathscr{M}$ to an element in $\mathbb{G}$ by using a hash function $H(\cdot)$. The resultant signature of the vehicle $\mathscr{V}_i$ consists of the following:

$$\begin{aligned}\sigma_1 &= \prod_{j\in S_i'} K_{S,\mathscr{V}_i,j}^{x} \cdot H(\mathscr{M})^x \\ &= \prod_{j\in S_i'} h_j^{u_i v_j x} \cdot \prod_{j\in S_i'} g^{\alpha x} \cdot H(\mathscr{M})^x \\ &= \prod_{j\in S_i'} h_j^{u_i v_j x} \cdot g^{\alpha x |S_i'|} \cdot H(\mathscr{M})^x,\end{aligned} \tag{6}$$

$$\sigma_2 = K_{S,\mathscr{V}_i}^{x} = g^{u_i x}, \tag{7}$$

$$\sigma_3 = K_{P'}^{x} = g^{\beta x}, \tag{8}$$

$$\sigma_4 = g^{x}. \tag{9}$$

The message $\mathscr{M}$ is sent to the CSP, together with the attribute set S_i' and the signature, as given by

$$\Delta = \{\mathscr{M}, S_i', \sigma_1, \sigma_2, \sigma_3, \sigma_4\}. \tag{10}$$

4.4. Signature Verification. Given the system public parameters in (2) and the signature Δ in (10), any data users can verify the signature with no need for the identity of the vehicle producing the signature. The data users can confirm that the data is signed by a legitimate vehicle with the up-to-date secret keys of all the attributes in S_i' if and only if

$$e(\sigma_1, K_{P'}) = e\left(\sigma_2, \prod_{j\in S_{i'}} K_j\right) \cdot e(\sigma_3, H(\mathscr{M})) \cdot e(\sigma_4, K_P)^{|S_{i'}|}. \tag{11}$$

Proof. Suppose that the version of the attributes embedded in the signature is $\{v_j, \forall j \in S_i'\}$, and the latest membership version of the j-th attribute is $\{v_j', j \in S_i'\}$. The left-hand side (LHS) of (11) can be written as

$$\begin{aligned}&e\left(\prod_{j\in S_i'} h_j^{u_i v_j x} \cdot g^{\alpha x |S_i'|} \cdot H(\mathscr{M})^x, g^{\beta}\right) \\ &= \prod_{j\in S_i'} e\left(h_j^{u_i v_j x}, g^{\beta}\right) \cdot e\left(g^{\alpha x |S_i'|}, g^{\beta}\right) \cdot e\left(H(\mathscr{M})^x, g^{\beta}\right) \\ &= \prod_{j\in S_i'} e\left(h_j, g\right)^{\beta u_i v_j x} \cdot e(g,g)^{\beta\alpha x |S_i'|} \cdot e(H(\mathscr{M}), g)^{\beta x},\end{aligned} \tag{12}$$

where the equalities are taken based on the bilinearity of the bilinear mapping e. Similarly, we can rewrite the right-hand side (RHS) of (11), as given by

$$\begin{aligned}&e\left(g^{u_i x}, \prod_{j\in S_i'} h_j^{\beta v_{j'}}\right) \cdot e\left(g^{\beta x}, H(\mathscr{M})\right) \cdot e\left(g^{x}, g^{\alpha\beta}\right)^{|S_i'|} \\ &= \prod_{j\in S_i'} e\left(g^{u_i x}, h_j^{\beta v_{j'}}\right) \cdot e(g, H(\mathscr{M}))^{\beta x} \cdot e(g,g)^{x\alpha\beta |S_i'|} \\ &= \prod_{j\in S_i'} e\left(h_j, g\right)^{\beta u_i v_{j'} x} \cdot e(g,g)^{x\alpha\beta |S_i'|} \cdot e(H(\mathscr{M}), g)^{\beta x}.\end{aligned} \tag{13}$$

By comparing (12) and (13), we can see that the LHS and RHS of (11) are equal if and only if $v_j = v_j'$. In other words, it is confirmed that the signature is signed by a legitimate vehicle with the up-to-date vehicle secret keys for the attributes if and only if (11) holds. □

4.5. Traceability of Vehicles and Attribute Revocation

4.5.1. Traceability of Malicious Vehicles. An important aspect of the proposed approach is its traceability of malicious vehicles through anonymous signatures. As described in Section 4.1, u_i is a unique random value for vehicle i, and the TA can use it to identify the vehicle at the TA. The TA stores all the values $\{u_i, \forall i\}$. Then, the TA can take each u_i as the input and test whether the following equation holds:

$$\sigma_2 = \sigma_4^{u_i}. \tag{14}$$

If (14) holds, the TA identifies u_i as the identity of the malicious vehicle. Otherwise, the TA iterates other values until (14) holds.

4.5.2. Attribute Revocation. When a malicious vehicle is found, as described in Section 4.5.1, the TA first detects the attributes of the vehicle and generates new public keys for the attributes. After that, the TA updates the attribute-related secret keys of the other legitimate vehicles equipped with the attributes. In this case, the attribute-related secret keys of the malicious vehicle are no longer up to date and cannot be used to generate legitimate signatures. In other words, the malicious vehicle is revoked from the system.

The TA is able to revoke any attribute, e.g., attribute j, of any vehicle in two steps. The TA chooses a new membership version of the attribute, denoted by v_j', and updates the system public key of this attribute, as given by

$$K_j' = h_j^{\beta v_j'}. \tag{15}$$

The TA also generates an update key for each vehicle $\mathscr{V}_i$ equipped with attribute j since the membership of attribute j has changed. The update key can be given by

$$\mathrm{UK}_{u_i} = h_j^{u_i\left(v_j' - v_j\right)}. \tag{16}$$

After receiving UK_{u_i}, $\mathscr{V}_i$ updates its secret key of attribute j as follows:

$$\begin{aligned} K_{S,\mathscr{V}_i,j'} &= K_{S,\mathscr{V}_i,j} \cdot \mathrm{UK}_{u_i} \\ &= h_j^{u_i v_j} \cdot g^{\alpha} \cdot h_j^{u_i\left(v_{j'} - v_j\right)} \\ &= h_j^{u_i v_{j'}} \cdot g^{\alpha}. \end{aligned} \tag{17}$$

5. Batch Verification and Dereplication

5.1. Batch Verification. The proposed approach allows multiple signatures to be verified at one go, referred to as "batch verification." This is important to reduce the computational complexity and delay of signature verification, especially in the presence of a large number of devices and a high volume of data. Without loss of generality, we consider that L messages, $\mathscr{M}_1, \cdots, \mathscr{M}_L$, are signed by L different vehicles, $\mathscr{V}_1, \ldots, \mathscr{V}_L$, by using the attribute sets $S_1', \ldots, S_L'$, respectively. From (10), for each of the vehicles, i.e., vehicle i, the signatures are given by

$$\Delta_i = \left\{\mathscr{M}_i, S_{i'}, \sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4}\right\}, \quad i = 1, \ldots, L, \tag{18}$$

where, based on (6)–(9), we have

$$\begin{aligned} \sigma_{i,1} &= \prod_{j \in S_{i'}} h_j^{u_i v_j x_i} \cdot g^{\alpha x_i \left|S_{i'}\right|} \cdot H\left(\mathscr{M}_i\right)^{x_i}, \\ \sigma_{i,2} &= g^{u_i x_i}, \\ \sigma_{i,3} &= g^{\beta x_i}, \\ \sigma_{i,4} &= g^{x_i}. \end{aligned} \tag{19}$$

Let $S = S_1' \cup \cdots \cup S_L'$. The set S_{A_j} collects vehicles that have signed one of the L messages by using attribute j. $\mathbf{A}_S$ is the set of RSUs included in the L signatures. It is confirmed that the signatures $\Delta_1, \ldots, \Delta_L$ are signed by the legitimate vehicles with the update-to-date secret keys if and only if

$$\begin{aligned} e\left(\prod_{i \in [1,L]} \sigma_{i,1}, K_{P'}\right) &= \prod_{j \in S} e\left(\prod_{i \in S_{A_j}} \sigma_{i,2}, K_j\right) \\ &\cdot \prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right), \sigma_{i,3}\right) \cdot e\left(\prod_{i \in [1,L]} \sigma_{i,4}, K_P^{\left|S_{i'}\right|}\right). \end{aligned} \tag{20}$$

Proof. The correctness of (20) is proved as follows. Referring to the proof of (11), we assume that the membership version embedded into the signatures is v_j, and the current membership version of attribute j is v_j'. We rewrite the LHS of (20) as

$$\prod_{i \in [1,L]} e\left(\prod_{j \in S_{i'}} h_j^{u_i v_j x_i} \cdot g^{\alpha x_i \left|S_{i'}\right|} \cdot H\left(\mathscr{M}_i\right)^{x_i}, g^{\beta}\right), \tag{21}$$

$$\begin{aligned} &= \prod_{j \in S} e\left(h_j^{v_j \sum_{i \in S_{A_j}} u_i x_i}, g^{\beta}\right) \cdot \prod_{i \in [1,L]} e\left(g^{\alpha x_i \left|S_{i'}\right|}, g^{\beta}\right) \\ &\cdot \prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right)^{x_i}, g^{\beta}\right), \end{aligned} \tag{22}$$

$$\begin{aligned} &= \prod_{j \in S} e\left(h_j, g\right)^{\beta v_j \sum_{i \in S_{A_j}} u_i x_i} \cdot \prod_{i \in [1,L]} e\left(g, g\right)^{\alpha x_i \beta \left|S_{i'}\right|} \\ &\cdot \prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right), g\right)^{\beta x_i}, \end{aligned} \tag{23}$$

where the two equalities are due to the bilinearity of bilinear mapping. In specific, (21) can be written as the product of three bilinear mappings: (a) $\prod_{i \in [1,L]} e\left(\prod_{j \in S_i'} h_j^{u_i v_j x_i}, g^{\beta}\right)$, (b) $\prod_{i \in [1,L]} e\left(\prod_{j \in S_i'} g^{\alpha x_i \left|S_i'\right|}, g^{\beta}\right)$, and (c) $\prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right)^{x_i}, g^{\beta}\right)$. Both (a) and (b) can be rearranged according to the attribute set S which is the union of S_i', $\forall i \in [1, L]$. The collection of vehicles signing messages by using attribute j is S_{A_j}. (22) is rewritten as (23) based on the bilinearity of e. Specifically, the exponents of h_j and g inside the bilinear mappings (a), (b), and (c) are moved out of the mappings.

We also rewrite the RHS of (20), as given by

$$\begin{aligned} &\prod_{j \in S} e\left(\prod_{i \in S_{A_j}} g^{u_i x_i}, h_j^{\beta v_{j'}}\right) \cdot \prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right), g^{\beta x_i}\right) \\ &\cdot e\left(\prod_{i \in [1,L]} g^{x_i}, g^{\alpha\beta \left|S_{i'}\right|}\right), \end{aligned} \tag{24}$$

$$\begin{aligned} &= \prod_{j \in S} e\left(g^{\sum_{i \in S_{A_j}} u_i x_i}, h_j^{\beta v_{j'}}\right) \cdot \prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right), g^{\beta x_i}\right) \\ &\cdot \prod_{i \in [1,L]} e\left(g^{x_i}, g^{\alpha\beta \left|S_{i'}\right|}\right), \end{aligned} \tag{25}$$

$$\begin{aligned} &= \prod_{j \in S} e\left(h_j, g\right)^{\beta v_{j'} \sum_{i \in S_{A_j}} u_i x_i} \cdot \prod_{i \in [1,L]} e\left(H\left(\mathscr{M}_i\right), g\right)^{\beta x_i} \\ &\cdot \prod_{i \in [1,L]} e\left(g, g\right)^{\alpha\beta x_i \left|S_{i'}\right|}, \end{aligned} \tag{26}$$

where the bilinearity of the mapping e ensures the correctness of the equalities.

By comparing (23) and (26), we conclude that the LHS and RHS of (20) are equal if and only if $v_j = v_j'$. In other words, if (20) holds, all the L signatures are generated with up-to-date vehicle attribute secret keys. The L signatures are all legitimate. □

5.2. Data Dereplication. The second feature of the proposed approach is its dereplication of signatures describing the same message while preserving the traceability of the vehicles certifying the message. Suppose that message $\mathscr{M}$ is signed by K vehicles, denoted by $\mathscr{V}_1, \ldots, \mathscr{V}_K$, by using the K attribute sets $S_1', \ldots, S_K'$, respectively. Let $S' = S_1' \cup \cdots \cup S_K'$. The set S_{A_j} collects the vehicles equipped with attribute j. With reference to (10), the signatures are given by

$$\Delta_i = \left\{\mathscr{M}, S_i, \sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}, \sigma_{i,4}\right\}, \quad i = 1, \ldots, K, \tag{27}$$

where, based on (6)–(9), we have

$$\begin{aligned}
\sigma_{i,1} &= \prod_{j \in S_i'} h_j^{u_i v_j x_i} \cdot g^{\alpha x_i \left|S_i'\right|} \cdot H(\mathscr{M}_i)^{x_i}, \\
\sigma_{i,2} &= g^{u_i x_i}, \\
\sigma_{i,3} &= g^{\beta x_i}, \\
\sigma_{i,4} &= g^{x_i}.
\end{aligned} \tag{28}$$

Here, $x_1, \ldots, x_K$ stand for the random values selected by the vehicles $\mathscr{V}_1, \ldots, \mathscr{V}_K$, respectively.

Let a matrix $\Gamma_{K,|S'|}$ specify the attributes used to sign the message $\mathscr{M}$:

$$\Gamma_{K,|S'|} = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,|S'|} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,|S'|} \\ \vdots & \vdots & & \vdots \\ b_{K,1} & b_{K,2} & \cdots & b_{K,|S'|} \end{bmatrix}, \tag{29}$$

where $|S'|$ is the size of S' and $b_{i,j} \in \{0, 1\}$. $b_{i,j} = 1$ indicates that vehicle $\mathscr{V}_i$ signs $\mathscr{M}$ by using attribute j. $b_{i,j} = 0$ indicates otherwise.

The CSP defines the aggregated signature, as given by

$$\Delta = \left\{\mathscr{M}, \Gamma, A_1, \left\{A_{2,j}\right\}_{\forall j \in S'}, A_3, A_4, \left\{\sigma_{i,2}, \sigma_{i,4}\right\}_{i \in [1,K]}\right\}, \tag{30}$$

where

$$\begin{aligned}
A_1 &= \prod_{i \in [1,K]} \sigma_{i,1} = \prod_{j \in S'} h_j^{v_j \sum_{i \in S_{A_j}} u_i x_i} \\
&\quad \cdot \prod_{i \in [1,K]} g^{\alpha x_i \left|S_i'\right|} \cdot H(\mathscr{M})^{\sum_{i \in [1,K]} x_i}, \\
A_{2,j} &= \prod_{i \in S_{A_j}} \sigma_{i,2} = \prod_{i \in S_{A_j}} g^{u_i x_i} = g^{\sum_{i \in S_{A_j}} u_i x_i}, \\
A_3 &= \prod_{i \in [1,K]} \sigma_{i,3} = \prod_{i \in [1,K]} g^{\beta x_i} = g^{\beta \sum_{i \in [1,K]} x_i}, \\
A_4 &= \prod_{i \in [1,K]} \sigma_{i,4} = g^{\sum_{i \in [1,K]} x_i}.
\end{aligned} \tag{31}$$

Any data user has the ability to verify the aggregated signature, i.e., Δ, if and only if

$$e(A_1, K_{P'}) = \prod_{j \in S'} e\left(A_{2,j}, K_j\right) \cdot e\left(A_3, H(\mathscr{M})\right) \cdot e\left(A_4^{\left|S_i'\right|}, K_P\right). \tag{32}$$

Proof. As defined in the proof of (11), the membership version of attribute j embedded into the signatures is v_j, and the membership version in the system attribute public key, i.e., K_j, is v_j'. We rewrite the LHS of (32) as

$$e\left(\prod_{j \in S'} h_j^{v_j \sum_{i \in S_{A_j}} u_i x_i} \cdot \prod_{j \in [1,K]} g^{\alpha x_i \left|S_i'\right|} \cdot H(\mathscr{M})^{\sum_{i \in [1,K]} x_i}, g^{\beta}\right), \tag{33}$$

$$\begin{aligned}
&= e\left(\prod_{j \in S'} h_j^{v_j \sum_{i \in S_{A_j}} u_i x_i}, g^{\beta}\right) \cdot \prod_{j \in [1,K]} e\left(g^{\alpha x_i \left|S_i'\right|}, g^{\beta}\right) \\
&\quad \cdot e\left(H(\mathscr{M})^{\sum_{i \in [1,K]} x_i}, g^{\beta}\right),
\end{aligned} \tag{34}$$

$$\begin{aligned}
&= \prod_{j \in S'} e\left(h_j, g\right)^{\beta v_j \sum_{i \in S_{A_j}} u_i x_i} \cdot \prod_{j \in [1,K]} e(g, g)^{\alpha \beta x_i \left|S_i'\right|} \\
&\quad \cdot e(H(\mathscr{M}), g)^{\beta \sum_{i \in [1,K]} x_i},
\end{aligned} \tag{35}$$

where the two equalities are due to the bilinearity of bilinear mapping. (33) can be rewritten as the product of three mappings in (34). The exponents of the group elements of $\mathbb{G}$ are moved outside the mapping e in (35).

We also rewrite the RHS of (32) as

$$\begin{aligned}
&\prod_{j \in S'} e\left(g^{\sum_{i \in S_{A_j}} u_i x_i}, h_j^{\beta v_{j'}}\right) \cdot e\left(g^{\beta \sum_{i \in [1,K]} x_i}, H(\mathscr{M})\right) \\
&\quad \cdot \prod_{j \in [1,K]} e\left(g^{x_i \left|S_i'\right|}, g^{\alpha \beta}\right),
\end{aligned} \tag{36}$$

$$\begin{aligned}
&= \prod_{j \in S'} e\left(h_j, g\right)^{\beta v_{j'} \sum_{i \in S_{A_j}} u_i x_i} \cdot e(H(\mathscr{M}), g)^{\beta \sum_{i \in [1,K]} x_i} \\
&\quad \cdot \prod_{j \in [1,K]} e(g, g)^{\alpha \beta x_i \left|S_i'\right|}.
\end{aligned} \tag{37}$$

By comparing (35) and (37), we show that the LHS and RHS of (32) are equal if and only if $v_j = v_j'$. Then, we conclude that message $\mathscr{M}$ is signed by K vehicles with legitimate secret keys. □

6. Security Analysis

We consider two security properties of the system, namely, the unforgeability of signatures and the anonymity of vehicles. The unforgeability of signatures ensures that the attackers, such as malicious vehicles or RSUs, cannot forge a signature of other vehicles. The anonymity of vehicles indicates that signatures can only certify that a message is signed by a qualified vehicle with up-to-date related

attributes and cannot reveal the identity of the vehicle. This ensures that any adversary cannot retrieve the identity of the signer from a signature. We first define the decisional Diffie–Hellman (DDH) assumption [32] as follows.

Definition 1 (decisional Diffie–Hellman (DDH) assumption). Given two elements in group $\mathbb{G}$, denoted by $X = g^a$ and $Y = g^b$. It is hard to decide $Z = g^{ab}$ or Z is a random element in $\mathbb{G}$, denoted by $Z = g^z$. Here, z is a random value in $\mathbb{Z}_p$.

6.1. Security Model

6.1.1. Unforgeability of the Signature. With reference to [21, 33, 34], we prove the unforgeability of the proposed system by constructing a game between a challenger and a forger. In this section, we define the game between a challenger and a forger as follows:

(i) Init: the forger first chooses a vehicle $\mathscr{V}^*$ with attribute set S^* as the target vehicle and attempts to forge a signature of this vehicle.

(ii) Setup: the challenger initializes the system, generates the public parameters, and sends them to the forger.

(iii) Phase 1: the forger can request the secret keys of any vehicle $\mathscr{V}_i$ other than $\mathscr{V}^*$. The forger can revoke any attribute of a vehicle $\mathscr{V}_i$ whose secret keys have been queried and obtain the updated attribute-related public keys.

(iv) Forgery: with the results of the queries in phase 1, the forger generates a forged signature σ^* of a message $\mathscr{M}^*$ under the targeted attribute set S^*.

(v) Guess: the challenger checks whether σ^* is a valid signature. If yes, the challenger outputs '1' to indicate that $Z = g^{ab}$.

We say that the proposed approach ensures the unforgeability of the signature if the forger cannot generate a valid signature σ^* with the unique value of $\mathscr{V}^*$ embedded.

6.1.2. Anonymity of the Signer. We adopt the selective indistinguishability of signatures to prove the anonymity of the vehicles with reference to [35]. We define the interaction between a challenger and an adversary as follows:

(i) Init: the adversary chooses a vehicle $\mathscr{V}^*$ as its target.

(ii) Setup: the challenger sets up the system and sends the public parameters with the parameters of DDH assumption embedded into the adversary.

(iii) Phase 1: the adversary can query for the secret keys of any vehicle $\mathscr{V}_i$ with the restriction that $\mathscr{V}_i \neq \mathscr{V}^*$.

(iv) Challenge: the adversary submits a message $\mathscr{M}$ and an attribute set S^* to the challenger. The challenger signs $\mathscr{M}$ under the attribute set S^* by using the secret keys of $\mathscr{V}^*$.

(v) Phase 2: the adversary continues to query for the secret keys of other vehicles different from $\mathscr{V}^*$.

(vi) Guess: the adversary outputs a guess $\delta \in \{0, 1\}$ and sends it to the challenger. Here, "1" and "0" represent Δ^* is a valid and invalid signature of $\mathscr{V}^*$.

We say that the proposed approach achieves the anonymity of the signer if the adversary cannot output a guess $r' = r$ with a nonnegligible probability.

6.2. Security Proof

6.2.1. Unforgeability of the Signature. With reference to [34], we verify the unforgeability of the proposed authentication technique by constructing a game between a challenger and a forger, where the forger can be an adversarial vehicle or RSU which attempts to forge the signature of a predefined attribute set S^*. The challenger interacts with the forger by initializing the system and responding to queries. The details are given as follows:

(i) Setup: the challenger selects two random values $\widehat{\alpha}, \widehat{\beta} \in \mathbb{Z}_p$ and sets $\alpha = a + \widehat{\alpha}$ and $\beta = b + \widehat{\beta}$, respectively. This is achieved by generating the system public keys K_P^* and $K_P^{'*}$ as follows:

$$K_P^* = g^{\alpha\beta} = g^{(a+\widehat{\alpha})(b+\widehat{\beta})} = Z \cdot Y^{\widehat{\alpha}} \cdot X^{\widehat{\beta}} \cdot g^{\widehat{\alpha}\widehat{\beta}}, \tag{38}$$

$$K_{P'}^* = g^{\beta} = g^{b+\widehat{\beta}} = Y \cdot g^{\widehat{\beta}}. \tag{39}$$

For each attribute j, the challenger initializes an empty vehicle list $\mathbb{VL}_j$, chooses random values $s_j \in \mathbb{Z}_p$, and sets $h_j^* = g^{s_j}$. The challenger also selects a random value v_j and generates the attribute-related public key K_j as follows:

$$K_j^* = h_j^{*\beta v_j} = g^{s_j(b+\widehat{\beta})v_j} = Y^{s_j v_j} \cdot g^{s_j \widehat{\beta} v_j}. \tag{40}$$

(ii) Phase 1: the forger can process three types of queries, namely, "$H(\cdot)$ query," "secret key query," and "attribute revocation query," as follows:

$H(\cdot)$ query: the challenger models $H(\cdot)$ as a random oracle and maintains a list of history recordings, denoted by HL. When the forger requests the hash value of a message $\mathscr{M}$, the challenger first checks if $\mathscr{M}$ has been recorded in the list HL. If $\mathscr{M}$ has been recorded, the challenger returns the corresponding value $H(\mathscr{M})$ to the forger. Otherwise, the challenger selects a random value $m \in \mathbb{Z}_p$, generates $H(\mathscr{M}) = g^m$, and sets $\text{HL} = \text{HL} \cup \{\mathscr{M}, m, H(\mathscr{M})\}$.

Secret key query: the forger is able to request the secret keys of a vehicle whose attribute set S_i satisfies the requirement that $S_i \neq S^*$. Specifically, the forger submits a query, denoted by $Q_{\mathscr{V}} = \{\mathscr{V}_i, S_i\}$, to the challenger. Q_V represents that vehicle $\mathscr{V}_i$ is equipped with an attribute set S_i. The challenger selects a random value $u_i \in \mathbb{Z}_p$ and

computes $K^*_{S,\mathscr{V}_i} = g^{u_i}$. For each attribute j, the challenger maintains a vehicle list by setting $\mathbb{VL}_j = \mathbb{VL}_j \cup e(g,g)^{u_i}$. Then, the challenger generates $K^*_{S,\mathscr{V}_i,j}$ as given by

$$K^*_{S,\mathscr{V}_i,j} = h_j^{u_i v_j} \cdot g^{a+\widehat{\alpha}} = g^{s_j u_i v_j} \cdot X \cdot g^{\widehat{\alpha}}. \tag{41}$$

Then, the challenger sends $\left\{K^*_{S,\mathscr{V}_i}, \left\{K^*_{S,\mathscr{V}_i,j}\right\}_{\forall j \in S_i}\right\}$ to the forger.

Attribute revocation query: the forger is able to revoke any vehicle in the vehicle list $\mathbb{VL}_j$. It first transmits $e(g,g)^{u_i}$ to the challenger. The challenger checks whether $e(g,g)^{u_i} \in \mathbb{VL}_j$. If $u_i \notin \mathbb{VL}_j$, the challenger rejects this query. Otherwise, it chooses a new value $v'_j \in \mathbb{Z}_p$ and updates the attribute-related public key K_j as follows:

$$K_j^{*'} = h_j^{\beta v_{j'}} = g^{s_j (b+\widehat{\beta}) v_{j'}} = Y^{s_j v_{j'}} \cdot g^{s_j \widehat{\beta} v_{j'}}. \tag{42}$$

(iii) Forgery: the forger first queries the $H(\cdot)$ oracle and obtains $H(\mathscr{M}^*) = g^{m^*}$. Then, the forger selects a random value $x \in \mathbb{Z}_p$ and outputs a forged signature $\Delta^* = \{\mathscr{M}^*, S^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*\}$ on message $\mathscr{M}^*$ by using the queried public keys and secret keys under the predefined attribute set S^*.

$$\begin{aligned}
\sigma_1^* &= \prod_{j \in S^*} K^x_{S,\mathscr{V}_i,j} \cdot H(\mathscr{M}^*)^x \\
&= \prod_{j \in S^*} \left(g^{s_j u_i v_j} \cdot X \cdot g^{\widehat{\alpha}}\right)^x \cdot g^{m^* x} \\
&= g^{u_i x \sum_{j \in S^*} s_j v_j} \cdot X^{x|S^*|} \cdot g^{x\widehat{\alpha}|S^*|} \cdot g^{m^* x}, \\
\sigma_2^* &= g^{u_i x}, \\
\sigma_3^* &= g^{\beta x} = g^{(b+\widehat{\beta})x} = Y^x \cdot g^{\widehat{\beta} x}, \\
\sigma_4^* &= g^x.
\end{aligned} \tag{43}$$

(iv) Guess: the challenger checks whether Δ^* is a valid signature and outputs a guess of Z in the DDH assumption. If Δ^* is a valid signature, the challenger outputs "1" to indicate that $Z = g^{ab}$.

We say that the forger can violate the unforgeability of the proposed algorithm if and only if Δ^* is a valid signature. According to (11), Δ^* can be successfully verified if and only if the parameter Z in (38) is g^{ab}, instead of g^z. This contradicts the DDH assumption, where the uncertainty of g^{ab} is proved to be hard against any polynomial adversaries [32]. Therefore, the unforgeability of the proposed approach is ensured.

6.2.2. Anonymity of the Signer. We proceed to prove the anonymity of the vehicles based on the signature indistinguishability. Given a vehicle $\mathscr{V}^*$ with a set of attributes S^* and a signature Δ generated by using a subset of S^*, we prove in the following that it is hard to distinguish whether $\mathscr{V}^*$ has signed the data or not. We define interactions between a challenger and an adversary as follows:

(i) Init: the adversary chooses a vehicle $\mathscr{V}^*$ whose attribute set is S^* as its target vehicle.

(ii) Setup: the challenger selects a random value $\overline{u} \in \mathbb{Z}_p$ and sets $u^* = b + \overline{u}$ as the secret value for $\mathscr{V}^*$. The challenger publishes the public key of $\mathscr{V}^*$ as follows:

$$K_{S,\mathscr{V}^*} = g^{u^*} = g^{b+\overline{u}} = Y \cdot g^{\overline{u}}. \tag{44}$$

As described in Section 6.2.1, the challenger chooses random values $\alpha', \beta', \{s'_j, \overline{v}_j\}_{\forall j} \in \mathbb{Z}_p$ and generates $K_P^* = g^{\alpha'\beta'}$, $K_P^{*'} = g^{\beta'}$, and $\left\{h_j^* = g^{s_{j'}}\right\}_{\forall j}$. The challenger also sets $v_j^* = a + \overline{v}_j$ for each attribute $j \in S^*$ by generating

$$K_j^* = h_j^{*\beta' v_j^*} = g^{s_{j'}\beta'\left(a+\overline{v}_j\right)} = X^{\beta' s_{j'}} \cdot g^{\beta' s_j \overline{v}_j}. \tag{45}$$

It is noteworthy that the attribute-related public key K_j^* still preserves the randomness and uniqueness of K_j because of the random values s_j and $\widehat{v}_j$. Then, the challenger sends the public parameters, i.e., K_P^*, $K_P^{*'}$, and $\left\{K_j^*\right\}$, to the adversary.

(iii) Secret key query: the adversary can query the secret keys of vehicle $\mathscr{V}_i$ whose attribute set is S_i, and $\mathscr{V}_i \neq \mathscr{V}^*$. The challenger chooses a random value $u'_i \in \mathbb{Z}_p$ and generates $K^*_{S,\mathscr{V}_i} = g^{u_{i'}}$. Let $Q_{\mathscr{V}} = \{\mathscr{V}_i, S_i\}$ represent the secret key query of $\mathscr{V}_i$. For each attribute $j \in S_i$, the challenger computes the attribute-related secret keys, as given by

$$\begin{aligned}
K^*_{S,\mathscr{V}_i,j} &= h_j^{*u_{i'} v_j^*} \cdot g^{\alpha'} = g^{u_{i'} s_{j'}\left(a+\overline{v}_j\right)} \cdot g^{\alpha'} \\
&= X^{u_{i'} s_{j'}} \cdot g^{u_{i'} s_{j'} \overline{v}_j} \cdot g^{\alpha'}.
\end{aligned} \tag{46}$$

Then, the challenger transmits the secret key of the vehicle $\mathscr{V}_i$, i.e., $\left\{K^*_{S,\mathscr{V}_i}, \left\{K^*_{S,\mathscr{V}_i,j}\right\}_{\forall j \in S_i}\right\}$, to the adversary.

(iv) Challenge: in this phase, the adversary chooses a message $\mathscr{M}^*$ and sends it to the challenger. As done in Section 6.2.1, we model $H(\cdot)$ as $H(\mathscr{M}^*) = g^{m^*}$. The challenger signs $\mathscr{M}^*$ by using the secret keys of vehicle $\mathscr{V}^*$. It also selects a random value $x' \in \mathbb{Z}_p$. The details are given as follows:

$$\begin{aligned}\sigma_1^* &= \prod_{j\in S^*} h_j^{u^* v_j^* x'} \cdot g^{\alpha' x' |S^*|} \cdot H(\mathscr{M}^*)^{x'} \\ &= \prod_{j\in S^*} g^{s_{j'} x' (b+\overline{u})\left(a+\overline{v}_j\right)} \cdot g^{\alpha' x' |S^*|} \cdot g^{m^* x'} \\ &= \prod_{j\in S^*} Z^{s_{j'} x'} \cdot \prod_{j\in S^*} X^{s_{j'} x' \overline{u}} \cdot \prod_{j\in S^*} Y^{s_{j'} x' \overline{v_j}} \\ &\quad \cdot \prod_{j\in S^*} g^{s_{j'} x' \overline{u} \overline{v}_j} \cdot g^{\alpha' x' |S^*|} \cdot g^{m^* x'}, \\ \sigma_2^* &= g^{u^* x'} = g^{(b+\overline{u})x} = Y^{x'} \cdot g^{\overline{u} x'}, \\ \sigma_3^* &= g^{\beta' x'}, \\ \sigma_4^* &= g^{x'}.\end{aligned} \tag{47}$$

Then, the challenger transmits $\Delta^* = \{\mathscr{M}^*, S^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*\}$ to the adversary.

(v) Phase 2: $\mathscr{A}$ can repeatedly query for the secret keys of vehicles $\mathscr{V}_i \neq \mathscr{V}^*$.

(vi) Guess: the adversary can output a guess $\delta \in \{0, 1\}$ and send δ to the challenger. Here, "1" and "0" indicate that Δ^* is a legitimate signature of $\mathscr{V}^*$ or not, respectively.

If $\delta = 1$, the adversary can break the anonymity of the proposed signature algorithm, but in this case, the challenger can confirm that $Z = g^{ab}$, which indicates that the challenger could breach the DDH assumption. Since the security of DDH has been proved in [32], we can assert that the anonymity of the proposed system is ensured.

7. Numerical and Experimental Study

In this section, we implement the proposed attribute-based anonymous authentication approach and conduct a comparison study of efficiency between the proposed scheme and three state-of-the-art ABS techniques, namely, Yu et al.'s algorithm [16], Cui et al.'s algorithm [17], and Xiong et al.'s algorithm [36]. These techniques are based on ABS techniques and can be applied to VANETs to support anonymous authentication. We first compare the schemes from the functionalities and security aspects. The details are provided in Table 2.

Our experimental testbed runs Charm-Crypto in a Mac laptop to provide the framework of our cryptosystem. Charm-Crypto supports a range of cryptographic settings, including pairing, exponential, and multiplicative operations in bilinear elliptic curve groups. We choose "SS512" as the target elliptic curve to simulate the state-of-the-art algorithms [16, 17, 36] and the proposed approach. The Mac laptop runs 10.14.5 operating system and has an Intel Core i5 with an operating frequency of 2.3 GHz and a memory of 8G bytes.

7.1. Efficiency of Batch Verification. We start by comparing the proposed approach with the state-of-the-art techniques in terms of computational overhead at the signature verification phase. We assume that there are K signatures to be verified and use the verification time (or delay) to represent the computational cost of the schemes. $|S|$ denotes the number of attributes included in the K signatures. Three variations of the proposed approach, referred to as "proposed algorithm without batch," "proposed batch verification when $|S| = 10$," and "proposed batch verification when $|S| = 20$," are plotted in Figure 2. We set $|S_I| = 5$; in other words, each message is signed under five attributes. Every result is the average of 100 independent experimental tests in the figure.

In Figure 2, we can see that the verification time of all the schemes increases with the number of messages, and the proposed approaches take shorter verification time than the existing techniques. We also see that "proposed algorithm without batch" intersects "proposed batch verification $|S| = 10$" and "proposed batch verification $|S = 20|$" when the number of signatures is 10 and 20, respectively. With the increase of K, the two variations of the proposed batch verification algorithm can outperform the algorithm without batch verification when the number of data is greater than the number of attributes. Moreover, the batch verification algorithms can perform better when the number of attributes is 10, i.e., $|S| = 10$, than they do when $|S| = 20$.

7.2. Efficiency of Data Dereplication. We compare the communication overhead of the proposed dereplication with that of the existing works in Figure 3(a). We use the length of signatures to represent the communication cost. Assume that there are K signature/replicas describing the same message $\mathscr{M}$. We evaluate the communication overhead of the K signatures by using the bit-length of signatures. Table 3 shows the comparison of the proposed approach and the existing algorithms, i.e., Yu et al.'s scheme [16], Cui et al.'s scheme [17], and Xiong et al.'s scheme [36]. $L_{\mathbb{G}}$ is the length of an element in the group $\mathbb{G}$. $L_{\mathscr{M}}$ denotes the length of a message $\mathscr{M}$. $L_{|S_\Lambda|}$ is the size of an access structure Λ (an attribute set or matrix). $|S_\Lambda|$ is the average size of attributes included in an ABS signature scheme. As shown in Figure 3(a), the proposed dereplication algorithms can show their advantage when the number of replicas is larger than the number of attributes included in the K signatures. Specifically, "proposed dereplication $|S| = 10$" and "proposed dereplication $|S| = 20$" can outperform the "proposed without dereplication" when the number of signatures is around and above 10 and 20, respectively. The proposed approach requires substantially lower communication cost than Yu et al.'s scheme [16] and Cui et al.'s scheme [17].

Besides the communication overhead, we also compare the storage overhead of vehicles in different schemes. We assume that there are up to 50 replicas to be stored. The schemes without dereplication, i.e., Yu et al.'s scheme [16], Cui et al.'s scheme [17], and Xiong et al.'s scheme [36], are expected to store the replicas separately to record the responsible vehicle. The proposed scheme can aggregate the

Table 2: Functional and computational comparisons of the proposed approach with existing ABS techniques, i.e., Yu et al.'s algorithm [16], Cui et al.'s algorithm [17], and Xiong et al.'s algorithm [36].

Scheme	Policy	Traceability	Revocability	Computational cost
Yu et al.'s algorithm [16]	(t, n)	No	No	$((\lvert S_\Lambda\rvert + 2)P_{\mathbb{G}} + 3\lvert S_\Lambda\rvert E_{\mathbb{G}} + 2\lvert S_\Lambda\rvert E_{\mathbb{G}_T})K$
Cui et al.'s algorithm [17]	(t, n)	Yes	Yes	$(4P_{\mathbb{G}} + \lvert S_\Lambda\rvert E_{\mathbb{G}} + 5M_{\mathbb{G}})K$
Xiong et al.'s algorithm [36]	LSSS	No	Yes	$(3P_{\mathbb{G}} + \lvert S_\Lambda\rvert E_{\mathbb{G}} + E_{\mathbb{G}_T})K$
Proposed without batch	(n, n)	Yes	Yes	$(3P_{\mathbb{G}} + (2\lvert S_\Lambda\rvert + 2)M_{\mathbb{G}} + M_{\mathbb{G}_T})K$
Proposed batch verification				$(\lvert S\rvert + K + 1)P_{\mathbb{G}} + (\lvert S_A\rvert + 2K - 3)M_{\mathbb{G}} + (\lvert S\rvert + \lvert K\rvert - 1)M_{\mathbb{G}_T}$

[1]In this example, we use the number of operations to represent the encryption overhead of IoT devices. $P_{\mathbb{G}}$ denotes the bilinear mapping operation e. $E_{\mathbb{G}}$ and $E_{\mathbb{G}_T}$ represent the exponential operation in group $E_{\mathbb{G}}$ and $E_{\mathbb{G}_T}$, respectively, and $M_{\mathbb{G}}$ and $M_{\mathbb{G}_T}$ stand for the multiplicative operation in $E_{\mathbb{G}}$ and $E_{\mathbb{G}_T}$. [2]$|S|$ denotes the size of the whole set of attributes in the system. $|S_\Lambda|$ is the number of attributes involved in an access structure Λ (an access tree or matrix), and n_u stands for the number of users in the ABE systems. $|S_A|$ denotes the average number of vehicles equipped with an attribute.

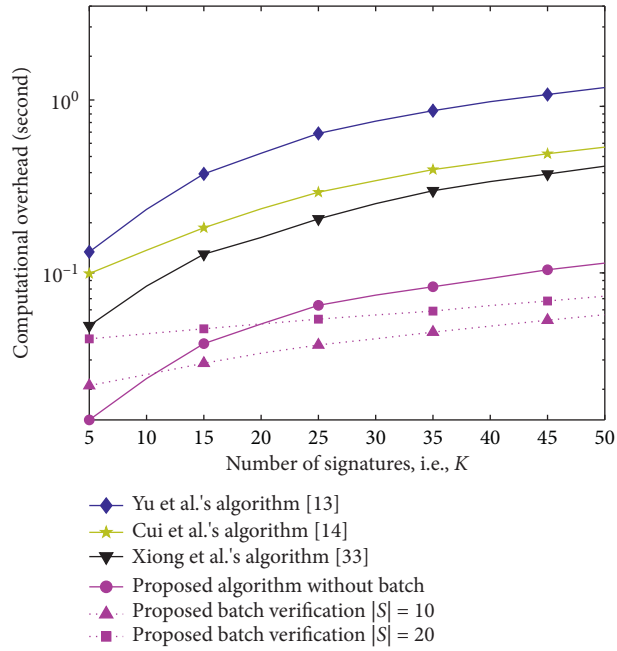

Figure 2: Computational overhead comparison.

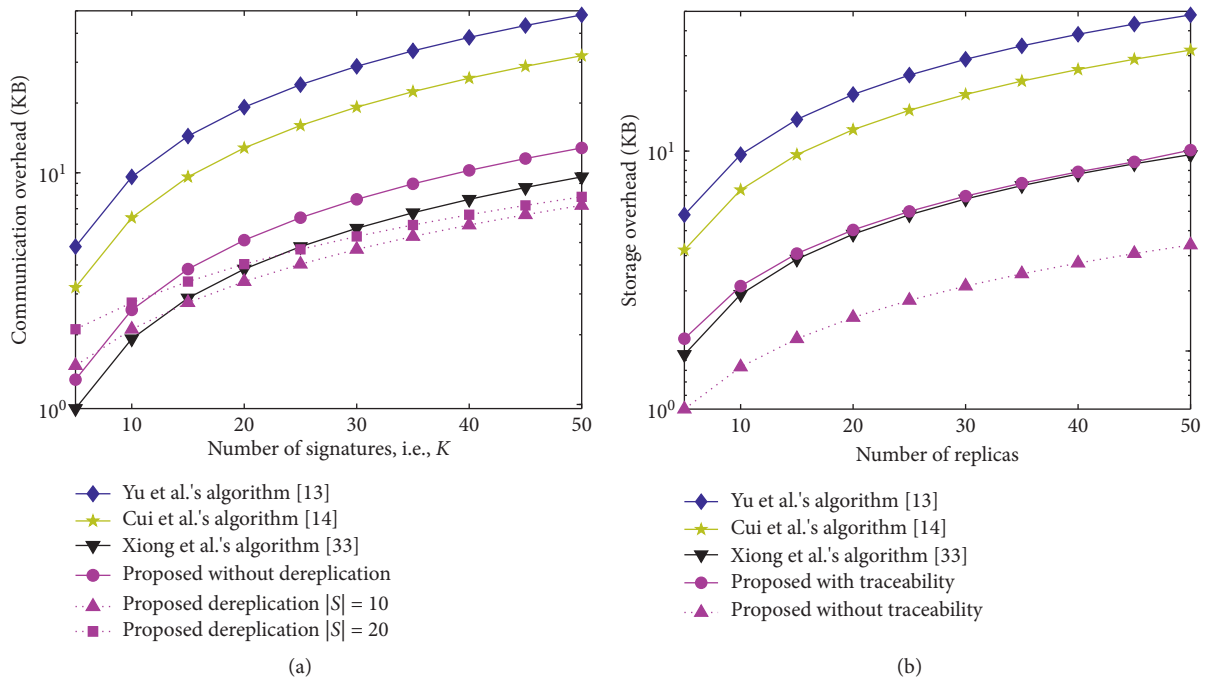

Figure 3: Performance comparison between the proposed approach and the state-of-the-art Yu et al.'s algorithm [16], Cui et al.'s algorithm [17], and Xiong et al.'s algorithm [36]. (a) Communication overhead comparison. (b) Storage overhead comparison.

Table 3: Communication comparison of the proposed dereplication approach and the state-of-the-art techniques, i.e., Yu et al.'s algorithm [16], Cui et al.'s algorithm [17], and Xiong et al.'s algorithm [36].

Schemes	Communication cost
Yu et al.'s scheme [16]	$(L_{\mathscr{M}} + L_{\lvert S_A\rvert} + 3\lvert S_I\rvert L_{\mathbb{G}})K$
Cui et al.'s scheme [17]	$(L_{\mathscr{M}} + L_{\lvert S_A\rvert} + 4L_{\mathbb{G}} + 3L_{\mathbb{G}_T})K$
Xiong et al.'s scheme [36]	$(L_{\mathscr{M}} + L_{\lvert S_A\rvert} + 3L_{\mathbb{G}})K$
Proposed without dereplication	$(L_{\mathscr{M}} + L_{\lvert S_A\rvert} + 4L_{\mathbb{G}})K$
Proposed data dereplication	$L_{\mathscr{M}} + L_{\lvert S_A\rvert} + (\lvert S\rvert + 2K + 3)L_{\mathbb{G}}$

replicas and preserve the traceability of the signers. The aggregated signature is given by $\Delta = \left\{\mathscr{M}, \Gamma, A_1, \left\{A_{2,j}\right\}_{\forall j \in S'}, A_3, A_4, \left\{\sigma_{i,2}, \sigma_{i,4}\right\}_{i \in [1,K]}\right\}$; see (30). In our design, $\left\{\sigma_{i,2}, \sigma_{i,4}\right\}_{i \in [1,K]}$ is preserved in Δ to trace the signers of the replicas and can be stored at a central server only. In this case, the vehicles can store $\Delta' = \left\{\mathscr{M}, \Gamma, A_1, \left\{A_{2,j}\right\}_{\forall j \in S'}, A_3, A_4\right\}$ to reduce storage overhead. We also evaluate the storage overhead of Δ', called "proposed without traceability," as shown in Figure 3(b). In the figure, we show that the proposed scheme can compress the storage space of replicas and largely reduce the storage overhead of vehicles.

7.3. Experiment Analysis. We evaluate the network performance of the proposed scheme by using SUMO and NS3 [4]. OpenStreetMap can help us get traffic data in a certain area and import the data to SUMO, which is a tool for building network simulators. As a C++ library, SUMO can load the road conditions from OpenStreetMap and simulate traffic flows. NS3 is a network simulator and can be combined with SUMO to simulate various communication protocols in different scenarios. We adopt IEEE 802.11p as the transmission protocol.

We generate a realistic map near the University of Technology Sydney (UTS) to simulate the performance of the proposed scheme. Figures 4 and 5 show the map of UTS in the real scenario and in SUMO, respectively. We consider average message transmission delay (ATD) to evaluate the performance of our scheme in VANET. The ATD can be defined as the average time cost to transmit messages from a sender to a receiver, denoted by

$$\text{ATD} = \frac{1}{N}\sum_{i=1}^{N}\left\{\frac{1}{N_i}\sum_{j=1}^{N_i}\left(T_{r,j} - T_{s,j}\right)\right\}. \tag{48}$$

Here, N is the total number of vehicles in the experiment. N_i denotes the number of messages received by the i-th vehicle V_i. $T_{r,j}$ and $T_{s,j}$ represent the receiving time and the sending time of the j-th message of V_i, respectively.

Figure 6 illustrates the relationship between the average transmission delay and the number of vehicles in the considered area. We can observe that the ATD grows linearly with the number of vehicles in the map. We also analyze how the size of packet influences the transmission

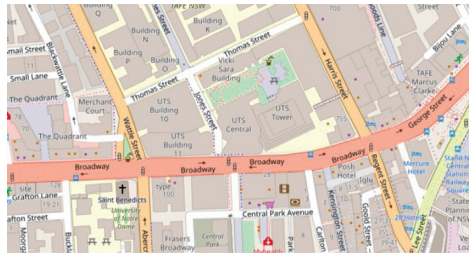

Figure 4: The map of the University of Technology Sydney.

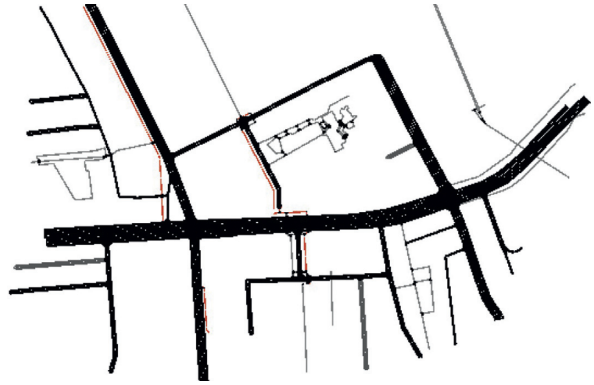

Figure 5: The map of the University of Technology Sydney in SUMO.

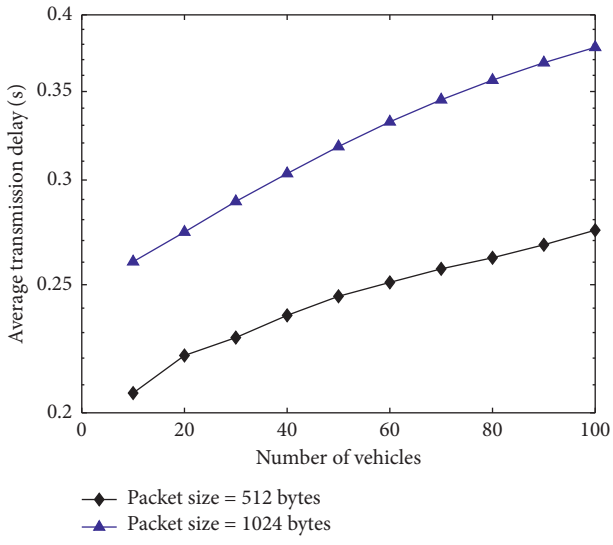

Figure 6: The relationship between the transmission delay and the number of vehicles.

delay. We take "packet size = 512 bytes" and "packet size = 1024 bytes" into consideration. From Figure 6, we can conclude that the ATD increases with the size of packet.

8. Conclusion

This paper presents a new approach for secure, efficient, and anonymous data authentication in VANET. The approach defines each vehicle by using a set of attributes and enables

the vehicle to sign messages under part of its attributes. The malicious vehicles forging data can be identified and revoked. The verification of multiple messages can be conducted together in a batch, hence reducing the delay of verifying massive data in large-scale VANETs. The replicas of the same data can be dereplicated to reduce the storage requirement for data, e.g., at the CSP. The approach is experimentally verified to outperform existing techniques in terms of verification delay and storage requirement.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] F. Qu, Z. Wu, F. Wang, W. Cho, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[2] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 7, pp. 1779–1790, 2018.

[3] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, 2019.

[4] 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.

[5] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[6] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[7] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. S. Shen, "Providing task allocation and secure deduplication for mobile crowdsensing via fog computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 2018, 2018.

[8] J. Li, H. Lu, and M. Guizani, "ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 938–948, 2015.

[9] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 8, pp. 2193–2204, 2016.

[10] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: a secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283–10295, 2017.

[11] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for VANETs," 2013.

[12] 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.

[13] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972–2986, 2019.

[14] M. H. Au, "ID-based ring signature scheme secure in the standard model," 2006.

[15] K. Amit, "ID-based ring signature and proxy ring signature schemes from bilinear pairings," 2005.

[16] Y. Yu, Y. Li, B. Yang, W. Susilo, G. Yang, and J. Bai, "Attribute-based cloud data integrity auditing for secure outsourced storage," *IEEE Transactions on Emerging Topics in Computing*, vol. 2017, 2017.

[17] H. Cui, R. H. Deng, and G. Wang, "An attribute-based framework for secure communications in vehicular ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 2019, 2019.

[18] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," 2007.

[19] M. H. Au, W. Susilo, and J. Zhou, "Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, p. 1909, 2013.

[20] J. Sun, Y. Su, J. Qin, J. Hu, and J. Ma, "Outsourced decentralized multi-authority attribute based signature and its application in IoT," *IEEE Transactions on Cloud Computing*, vol. 2019, 2019.

[21] M. Prabhakaran and M. Rosulek, "Attribute-based signatures," 2011.

[22] S.-J. Horng, S.-F. Tzeng, Y. Pan et al., "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.

[23] K. Emura and T. Hayashi, "Road-to-vehicle communications with time-dependent anonymity: a lightweight construction and its experimental results," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 2, pp. 1582–1597, 2017.

[24] D. He, N. Kumar, and W. Wu, "Efficient hierarchical identity-based signature with batch verification for automatic dependent surveillance-broadcast system," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 454–464, 2016.

[25] K.-A. Shim, "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.

[26] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.

[27] N. Lewis, C. H. Liu, and J. S. Song, "Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles," *Future Generation Computer Systems*, vol. 95, pp. 488–499, 2019.

[28] 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*

Transactions on Vehicular Technology, vol. 66, no. 4, pp. 3235–3248, 2017.

[29] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[30] 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.

[31] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," 2001.

[32] D. Boneh, "The decision diffie-hellman problem," 1998.

[33] D. Boneh, E. Shen, and B. Waters, "Strongly unforgeable signatures based on computational Diffie-Hellman," 2006.

[34] J. Herranz, F. Laguillaumie, B. Libert, and C. Ràfols, "Short attribute-based signatures for threshold predicates," 2012.

[35] D. Khader, "Attribute based group signature with revocation," *IACR Cryptology ePrint Archive*, vol. 241, 2007.

[36] X. Hu, Y. Bao, and X. Nie, "Server-aided attribute-based signature supporting expressive access structures for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 2019, 2019.