

Article

An Efficient Privacy-Preserving Batch Authentication Scheme in Fog-Enabled VANETs

Cong Zhao ¹, Xuan Ge ², Yikang Yang ², Qinglei Qi ¹ and He Li ^{1,*}

¹ Department of College of Artificial Intelligence and Henan Province Intelligent Emergency Service and Support Engineering Research Center, The University of Nanyang Normal University, Nanyang 473061, China; zhaocong@nynu.edu.cn (C.Z.); qiqinglei@nynu.edu.cn (Q.Q.)

² Department of College of Artificial Intelligence, The University of Nanyang Normal University, Nanyang 473061, China; s20560140110@nynu.edu.cn (X.G.); 21631922848@nynu.edu.cn (Y.Y.)

* Correspondence: lihe@nynu.edu.cn

Abstract

Vehicular ad hoc networks (VANETs), as a key communication component of the Internet of Vehicles (IoV), enable vehicles and roadside infrastructure to exchange information efficiently, thereby supporting road safety and traffic management. However, because these communications take place over open wireless channels, VANETs are exposed to message forgery, replay, identity disclosure, and unauthorised access by revoked vehicles. To address these issues, this paper proposes EPAF, an efficient privacy-preserving batch authentication scheme with revocation support for fog-enabled VANETs. EPAF uses roadside fog nodes to distribute update keys and report information related to misbehaving vehicles, thereby reducing reliance on remote centralised processing. Rather than assuming ideal tamper-proof devices that store system-wide secrets, EPAF requires protected storage only for vehicle-local certificates, limiting the impact of compromising an individual vehicle device. The scheme employs batch verification to authenticate multiple messages from different vehicles in a single procedure, reducing verification overhead in message-intensive traffic conditions. It further introduces an update-key mechanism through which legitimate vehicles obtain current authentication keys, whereas revoked vehicles are prevented from generating valid authentication messages in subsequent revocation periods. Under the honest-authority model, the security analysis establishes the EUF-CMA security of an authentication packet in the random-oracle model and separately addresses conditional identity privacy, traceability, and unlinkability across different pseudonym periods. Performance evaluation examines the trade-off among authentication efficiency, communication overhead, and revocation performance, showing that EPAF is a practical solution for fog-enabled vehicular communication.

Keywords: batch authentication; conditional privacy-preserving; fog computing; revocation; VANETs



Academic Editor: Jose I. Moreno Novella

Received: 27 May 2026

Revised: 20 July 2026

Accepted: 28 July 2026

Published: 30 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

With the rapid development of the Internet of Things (IoT), Vehicular Ad Hoc Networks (VANETs) have become an important communication component of intelligent transportation systems (ITSs) and the Internet of Vehicles (IoV) [1,2]. By enabling real-time information exchange among vehicles and roadside infrastructure, VANETs support road-safety applications, improve traffic management, and provide drivers with value-added services [3].

A typical VANET consists of On-Board Units (OBUs), roadside units (RSUs), and a trusted authority (TA) [4]. Vehicles communicate directly with one another through Vehicle-to-Vehicle (V2V) technology and interact with roadside infrastructure through Vehicle-to-Infrastructure (V2I) technology. TA is responsible for system initialization, credential management, and authorised identity tracing. RSUs provide roadside communication support and relay information between vehicles and TA. Each vehicle is equipped with an OBU that exchanges traffic conditions, accident warnings, and other road-related information over short-range wireless links, such as Dedicated Short-Range Communication (DSRC) [5].

Despite these benefits, the open and broadcast nature of wireless communication exposes VANETs to serious security and privacy risks. Attackers may intercept, modify, replay, or fabricate vehicular messages, thereby launching man-in-the-middle, impersonation, or replay attacks [6]. They may also analyse transmitted messages to infer sensitive information, including vehicle identities, locations, and movement trajectories. Protecting both message security and user privacy has therefore become a fundamental requirement for VANETs [7]. At the same time, privacy must be balanced with accountability: when a vehicle distributes false information or behaves maliciously, authorised entities should be able to identify and revoke it [8].

Authentication is central to achieving this balance. It allows receivers to verify the origin and integrity of transmitted messages while supporting privacy-preserving communication through pseudonyms. However, VANETs are characterised by rapid topology changes and frequent message broadcasts, particularly in dense traffic conditions. In such environments, verifying each message independently may impose substantial computational delay and limit system scalability [9]. Batch authentication therefore provides a practical approach by enabling a verifier to process multiple messages together and reduce repeated verification operations [10].

Although many authentication schemes have been proposed, several practical limitations remain. Centralised architectures may increase communication latency and create dependence on remote processing. Some schemes also assume ideal tamper-proof devices (TPDs) that securely store system-wide master secrets; once such assumptions fail, the consequences for system security and vehicle privacy can be severe. In addition, conventional revocation list (RL)-based mechanisms may require frequent dissemination and checking of revocation information, increasing communication and storage costs as the network scales [11].

Fog computing provides a promising means of addressing these limitations. By placing computing and communication support closer to vehicles, roadside fog nodes can assist with local authentication processing and key-update distribution, thereby reducing reliance on distant central servers [12–14]. In this setting, fog-enabled VANETs offer a suitable architecture for supporting timely authentication and practical revocation management in dynamic vehicular communication environments.

Motivated by these observations, this paper proposes an Efficient Privacy-Preserving Authentication Scheme for Fog-Enabled VANETs (EPAF) with batch verification and revocation support. EPAF is designed for the VANET communication component of the IoV. It uses roadside fog nodes to assist authentication and update-key distribution, employs efficient batch verification to reduce authentication overhead, and introduces a tree-based update-key mechanism to prevent revoked vehicles from generating valid authentication messages in subsequent revocation periods. Rather than relying on ideal TPDs that store system-wide secrets, EPAF assumes protected storage only for vehicle-local certificates. Its main contributions are summarised as follows.

- (1) EPAF introduces a fog-assisted authentication architecture for vehicular communication. By allowing roadside fog nodes to support local authentication processing, the proposed architecture reduces reliance on remote centralised servers and improves scalability in message-intensive traffic environments. In addition, EPAF employs an elliptic-curve-based batch verification mechanism that enables a receiver to authenticate multiple messages efficiently.
- (2) EPAF provides a tree-based revocation mechanism in which update keys are distributed to legitimate vehicles for each revocation period. Once the current update keys have been distributed, a revoked vehicle cannot derive the valid authentication key required to generate acceptable messages in subsequent communications. This design supports practical revocation management without requiring each verifier to maintain and repeatedly check a complete revocation list.
- (3) EPAF supports conditional identity privacy under separated authority roles. Rather than relying on ideal tamper-proof devices that store system-wide master secrets, the scheme assumes protected storage only for vehicle-local certificates, thereby limiting the impact of compromising an individual vehicle device. Security analysis examines message authentication, traceability, and unlinkability across different pseudonym periods, while performance evaluation considers the trade-off among authentication efficiency, communication overhead, and revocation support.

The remainder of this paper is organized as follows. Sections 2 and 3 present the related work and preliminaries, respectively. Section 4 describes the efficient privacy-preserving authentication scheme in detail. System analysis is elaborated in Section 5. Section 6 presents the performance analysis. Finally, Section 7 summarizes the paper.

2. Related Work

The classification of existing privacy-preserving authentication schemes is based on mechanisms applied using public key, identity, certificateless, and group signature [15,16].

Public Key-based Authentication. The authentication schemes, which are based on public key cryptography, adopt a trusted authority (TA) to generate and distribute public–private key pairs and certificates for vehicles. Vehicles authenticate with each other through certificates and signatures. Traceability is achieved by certificates issued by TA. However, they generally incur considerable overhead in certificate management, signature verification, and revocation. Although existing schemes have reduced part of this overhead through anonymous certificate self-generation, dynamic key management, physical-attack resistance, and fog-assisted processing [17–19], they essentially shift the burden to trusted hardware, trusted authorities, revocation maintenance, or resource-rich RSUs. To improve efficiency, Azees et al. [17] proposed EAAP, which enables vehicles and RSUs to generate anonymous certificates locally, but still relies on pairing operations and TPDs. Aghabagherloo et al. [18] developed a physically secure authentication scheme with tamper detection and key updating to protect privacy under individual OBU compromise. Ali et al. [19] further proposed a fog-assisted CLC-to-PKI signcryption scheme that supports batch verification at RSUs to reduce authentication delay. Nevertheless, existing schemes still face limitations in jointly achieving efficient authentication, lightweight revocation, and robust privacy protection under partial device compromise.

Identity-based Authentication. In identity-based authentication schemes, a trusted authority issues pseudo-identities derived from the real identity (e.g., license plate number) for vehicles. Moreover, TA uses its master key to generate private keys corresponding with vehicles' pseudo-identities for each vehicle. Identity-based authentication schemes avoid the certificate management overhead of conventional PKI-based approaches and improve authentication efficiency in VANETs. However, although existing studies reduce the cost

of certificate maintenance, batch verification, or pseudonym generation [16,20–23], they often shift the burden to trusted authorities, roadside infrastructure, trusted hardware, or revocation management. To improve practicality, Liu et al. [21] proposed a distributed conditional privacy-preserving scheme based on identity-based cryptography and short-lifetime regional certificates, reducing the reliance on online trusted authorities and ideal TPDs. Kang et al. [20] developed a randomized authentication protocol that enables vehicles to self-generate unlinkable identities through homomorphic encryption, but requires collaborative authentication servers. Zhang et al. [23] designed an ECC-based anonymous batch authentication scheme with hash-chain-based pseudonyms and rapid identity revocation, while still relying on TA for tracing and revocation support. Cui et al. [22] proposed a pairing-free mutual authentication scheme that periodically updates sensitive information stored in TPDs to mitigate side-channel attacks. More recently, Maurya and Chaurasiya [16] proposed an ECC-based anonymous batch authentication scheme in which RSU-distributed parameters support pseudonym generation and efficient batch verification. Nevertheless, these schemes still face limitations in jointly achieving low-latency authentication, lightweight revocation, and robust privacy preservation under partial device compromise.

Certificateless-based Authentication. Certificateless authentication schemes eliminate certificate management in PKI-based approaches and alleviate the key escrow problem in identity-based schemes. However, although existing schemes improve communication and verification efficiency through aggregate signatures and pairing-free constructions [24–27], their security and efficiency remain limited in practical VANETs. Kumar et al. [24] proposed certificateless signature and aggregate signature schemes to reduce bandwidth and verification overhead, but their construction relies on costly bilinear pairing operations. Zhu et al. [25] developed a pairing-free CLAS-based authentication scheme with conditional privacy preservation to improve efficiency and resist multiple adversaries. Subsequently, Yang et al. [26] showed that Zhu et al.’s scheme remains vulnerable to public-key replacement and coalition attacks, and proposed an enhanced pairing-free scheme. Wenjie Yang et al. [27] further identified forgery vulnerabilities in existing CLAS schemes and designed an aggregate authentication mechanism with public verification and improved signature validity assurance. Nevertheless, these schemes mainly focus on aggregate-signature security and verification efficiency, while lightweight revocation and privacy preservation under partial device compromise remain insufficiently addressed.

Group Signature-based Authentication. Group-based authentication schemes improve authentication efficiency and privacy preservation by enabling vehicles to authenticate and communicate as group members rather than as independent entities. However, although existing schemes reduce repeated authentication and group management overhead through batch verification, dynamic group keys, and group pseudonyms [28–33], they often shift the burden to expensive cryptographic operations, key-update procedures, trusted infrastructures, or blockchain-assisted management. Lai et al. [30] proposed SEGM, which supports dynamic group maintenance and lightweight access authentication, but depends on integrated VANET-cellular infrastructure. Xu et al. [29] developed BAGKD by combining batch authentication with distributed group key management; however, its bilinear mapping operations still incur considerable computational cost. Sun et al. [31] proposed an ECC-based anonymous authentication and key agreement scheme using group keys and realistic TPDs, while Zhang et al. [28] employed CRT-based group key updates to reduce authentication overhead; nevertheless, both schemes still require group-key maintenance. Jayashree and Kumar [32] further proposed a certificateless group-signature-based verification scheme using ECC-based aggregate signatures to improve authentication efficiency. More recently, Xia et al. [33] introduced a blockchain-assisted cross-domain

group authentication scheme for vehicle platoons, but its operation relies on additional blockchain and cross-domain infrastructures.

EPAF adopts the tree-based subset-cover component from prior work (KUNode) [34]. Its contribution is the protocol-level binding of the current-period KUNode update key to the effective ECC authentication key and verification equation. Under the designated separation of responsibilities, KGC disseminates update-key items through fog nodes, and only a vehicle whose path intersects the current minimum update-node set can derive the effective key used for authentication. This shifts the overhead of proving non-revocation from the verifier to the authentication initiator, thereby increasing the willingness of verifiers to cooperate. This construction couples revocation state with direct V2V/V2I batch authentication, whereas the closest schemes in Table 1 provide only a subset of these functions or rely on a complete revocation-list check at the verifier. EPAF provides an integrated design under the established trust and device-protection assumptions, rather than treating authentication, key updating, and revocation as separate procedures. Table 1 compares some classic authentication schemes in VANETs from different aspects. In summary, while many authentication mechanisms have been proposed, the reliance on centralized servers, tamper-proof devices, RLs, and resource-intensive cryptographic techniques limits their scalability, efficiency, and robustness. These challenges motivate the need for more efficient, scalable, and privacy-preserving authentication schemes, which is the focus of this paper.

Table 1. Comparison of the state-of-the-art authentication schemes.

Cryptography	Schemes	C1	C2	C3	C4	C5
Public key	[17]	✓	✓	×	R	×
	[18]	✓	×	✓	R	✓
	[19]	×	×	✓	I	×
Identity	[20]	×	×	✓	R	✓
	[21]	✓	×	×	R	×
	[22]	✓	×	×	I	✓
	[16]	✓	✓	✓	I	×
	[23]	×	×	✓	R	✓
Certificateless	[24]	✓	✓	✓	R	×
	[25]	✓	×	✓	I	×
	[26]	✓	×	✓	I	×
	[27]	✓	×	✓	I	×
	EPAF	✓	×	✓	R	✓
Group Signature	[29]	✓	✓	✓	I	×
	[30]	×	×	✓	R	×
	[28]	✓	×	✓	I	×
	[31]	×	×	×	R	×
	[32]	✓	×	✓	I	×
	[33]	✓	✓	✓	I	×

1. C1, C2, C3, C4, and C5 represent V2I and V2V, bilinear pairing, batch verification, TPD, and revocation, respectively. 2. ✓ denotes that the property is achieved, and × denotes that the property is not achieved. 3. R denotes realistic, and I denotes ideal.

3. Preliminaries

3.1. KUNode Algorithm

A binary tree BT is defined as containing n nodes, with the root node denoted by $root$. Each non-leaf node contains a left child node x_l and a right child node x_r . For a leaf node n , $Path\{n\}$ represents the set of nodes on the path from $root$ to n . The number of nodes in a given set is represented by $|set|$. Each registered vehicle is assigned one leaf. At current time T , the effective revocation set is $RL_T = \{(v_i, T_i) \in RL : T_i \leq T\}$, where v_i denotes

the revoked vehicle and T_i denotes the corresponding revocation timestamp. Algorithm 1, adapted from the KUNode procedure in [34], outputs a minimum update-node set $MSet$ such that every unrevoked leaf has an ancestor in $MSet$, whereas no revoked leaf does. All revoked nodes are marked in red, while all ancestors of the non-revoked nodes are marked in black and subsequently output, at which point the black nodes are distributed with the updated keys.

Algorithm 1 KUNode Algorithm

Input: $BT, RL, T;$ **Output:** $MSet;$

```

1:  $RL_T \leftarrow \{(v_i, T_i) \in RL : T_i \leq T\};$ 
2:  $X, MSet \leftarrow \emptyset;$ 
3: if  $|RL_T| = 0$  then
4:   add root to  $MSet$ ;
5: else
6:   for each  $(v_i, T_i) \in RL_T$  do
7:      $X \leftarrow X \cup \text{Path}(v_i);$ 
8:   end for
9:   for each  $x \in X$  do
10:    if  $x_l$  exists and  $x_l \notin X$  then
11:      add  $x_l$  to  $MSet$ ;
12:    end if
13:    if  $x_r$  exists and  $x_r \notin X$  then
14:      add  $x_r$  to  $MSet$ ;
15:    end if
16:  end for
17: end if
18: return  $MSet$ ;

```

Two examples are shown in Figure 1. Suppose that users $u_1, u_2, \dots, u_8$ are assigned to leaf nodes 8, 9, $\dots$, 15, respectively. When RL_T is empty, Algorithm 1 returns $\{\text{root}\}$, as shown in Figure 1a. When u_1 is revoked, the algorithm returns $MSet = \{3, 5, 9\}$, as shown in Figure 1b; none of these update nodes is an ancestor of the revoked leaf. If every leaf is revoked, every child encountered by the algorithm belongs to X , and the valid output is $MSet = \emptyset$.

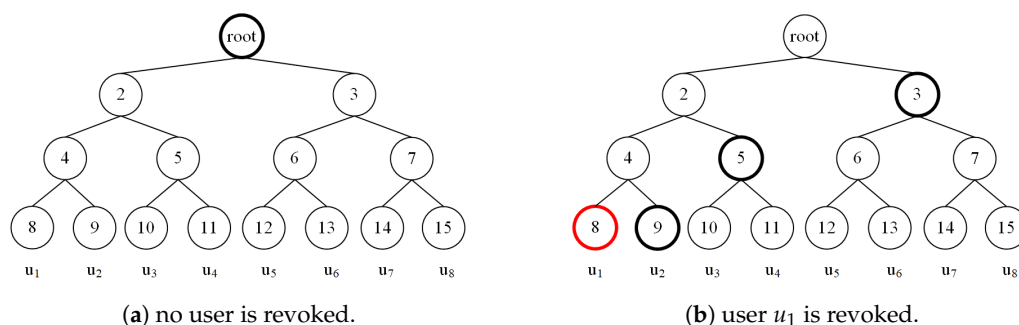


Figure 1. Examples of the KUNode algorithm.

3.2. Elliptic Curve Cryptography

The elliptic curve cryptography (ECC) was proposed independently by Neal Koblitz and Victor Miller in 1985. The main advantage of ECC is that it provides incredibly high efficiency and relatively good security using a smaller key than other methods, such as RSA cryptography [35]. ECC can be perfectly adopted for VANETs due to its shorter key length and lower computation overhead.

Over a finite field F_q , consider a non-singular elliptic curve $E : y^2 = x^3 + ax + b \pmod{q}$, where $a, b \in F_q$ and $4a^3 + 27b^2 \neq 0$.

Definition 1. *Elliptic Curve Discrete Logarithm Problem (ECDLP):* Given a generator P of an elliptic-curve group G and a point $Q = xP$, determine the scalar x . The ECDLP assumption states that no probabilistic polynomial-time algorithm solves this problem with non-negligible probability for the selected group parameters.

3.3. System Model

According to Figure 2, the system model in the proposed scheme includes a trusted authority, a Key Generation Center, roadside units, and On-Bord Units.

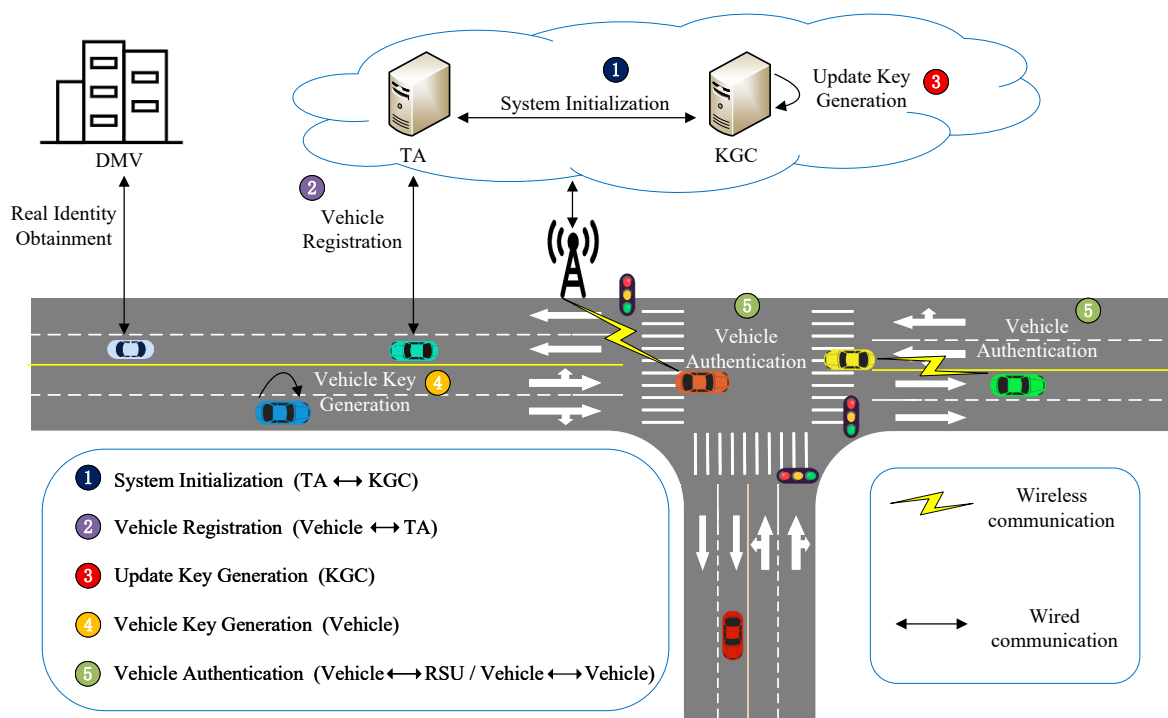


Figure 2. Overview of EPAF.

The trusted authority (TA) and Key Generation Center (KGC) are considered as trusted third authorities. TA and KGC cooperate for system initialization, vehicle registration, binary tree maintenance, and malicious user revocation. In addition, TA is responsible for managing the revocation list, and KGC is responsible for key updates. TA communicates with KGC through a secure wired channel. TA and KGC both have high computation capacity and sufficient storage capacity. TA and KGC are assumed to execute the protocol honestly, not to collude with the adversary, and not to disclose their master secrets or internal registration and update-key-generation states.

Roadside units (RSUs) are communication devices installed along roadsides and act as fog nodes (FNs). RSUs are connected to TA and KGC with a secure wired channel. The main functions of RSUs are to broadcast update keys from KGC and report malicious

vehicles. RSUs communicate with vehicles within their communication range using DSRC protocol.

Each vehicle is equipped with On-Board Units (OBUs) that enable vehicles to communicate with neighbouring vehicles and RSUs through DSRC protocol. Its computation and storage capacities are less than those of RSUs. OBUs are composed of Tamper-Proof Devices (TPDs), Global Positioning Systems (GPSs), network devices, and sensors. Surrounding information is gathered and transmitted to OBUs by the GPS and other sensors. OBUs monitor the collected information and broadcast traffic-related information.

3.4. Adversary Model and Security Objectives

In the proposed EPAF scheme, the trusted authority (TA) and the Key Generation Center (KGC) are assumed to be trusted and non-colluding authorities. They follow the protocol correctly and protect their respective master secrets. Fog nodes (FNs) are assumed to be honest-but-curious: they correctly perform authentication-related operations and distribute update keys, but may attempt to infer vehicle information from the data they process. Vehicles equipped with On-Board Units (OBUs) may behave maliciously. A malicious vehicle may attempt to obtain information about nearby vehicles or broadcast false traffic messages. In addition, because vehicles communicate through open wireless channels using DSRC, external attackers may eavesdrop on, modify, replay, or fabricate transmitted messages.

Under this adversary model, EPAF is designed to protect message authenticity and vehicle identity privacy while enabling authorised accountability and revocation. Based on the security requirements of privacy-preserving authentication in fog-enabled vehicular networks, EPAF aims to satisfy the following properties [15]:

- (1) **Message authentication and integrity:** A receiver should be able to verify that a received message was generated by a vehicle holding valid current certificates and that the message has not been modified during transmission.
- (2) **Conditional identity privacy:** During normal communication, external attackers and fog nodes should not be able to recover a vehicle's real identity from its authentication messages. When a vehicle is confirmed to be malicious, its real identity should be recoverable through an authorised procedure involving both TA and KGC.
- (3) **Unlinkability:** An external observer should not be able to determine that authentication messages generated under different pseudonyms originate from the same vehicle without the cooperation of the trusted authorities. Messages transmitted under the same active pseudonym period may remain linkable.
- (4) **Distributed identity resolution and revocation:** TA and KGC should cooperate to recover the real identity of a misbehaving vehicle and initiate its revocation. Neither authority should independently obtain all information required for identity resolution during normal operation.
- (5) **Resistance to message-level attacks:** Under the stated adversary model, EPAF should resist impersonation, message modification, and replay attacks.

4. The Proposed Scheme

This section presents an efficient privacy-preserving batch authentication (EPAF) scheme supporting revocation in fog-enabled VANETs. Figure 2 illustrates an overview of EPAF, which consists of the following phases:

- (1) *System Initialization:* Given a security parameter κ , TA and KGC output system parameters.

- (2) *Vehicle Registration*: For each registered vehicle, TA and KGC generate partial keys $\{\alpha, A_i, A_i', \hat{a}_i\}_{\alpha \in \text{Path}(\mu)}$ and certificates $\{R_i, \text{psk}_i, \text{PID}_i, \Delta T_i\}$ by taking the binary tree BT , vehicles' identity RID and private keys $\{s_1, s_2\}$ as input.
- (3) *Update key Generation*: KGC executes this phase periodically with the minimum node set $MSet$ and the private key s_2 as input and generates update keys $\{\beta, B, B', \hat{b}\}_{\beta \in MSet}$ for unrevoked vehicles.
- (4) *Vehicle Key Generation*: Given partial keys $\{\alpha, A_i, A_i', \hat{a}_i\}_{\alpha \in \text{Path}(\mu)}$ and the update key $\{\beta, B, B', \hat{b}\}_{\beta \in MSet}$, the vehicle $\mathcal{V}$ generates a vehicle key $\{e, C\}$ for subsequent authentication.
- (5) *Vehicle Authentication*: Given certificates $\{R_i, \text{psk}_i, \text{PID}_i, \Delta T_i\}$ and a vehicle key $\{e, C\}$, the vehicle $\mathcal{V}$ generates a signature based on the message msg , then sends a packet $\{\sigma, F, E, \text{PID}, R, \Delta T, T_{RL}, ts, msg\}$ to authentication with FNs or vehicles.

The sequence of these phases is shown in Figure 3. In addition, the identity inspection is shown in Figure 3. Fog nodes (FNs) forward tuples obtained from misbehaving vehicles to TA. TA and KGC cooperate to inspect real identities of misbehaving vehicles to achieve conditional privacy-preserving. The notations appearing in the scheme are described in Table 2.

Table 2. Notations and descriptions.

Notations	Descriptions
P_{pub1}, s_1	The public and private key of TA
P_{pub2}, s_2	The public and private key of KGC
F, f	The public and private key of the vehicle
H_0, H_1, H_2, H_3, H_4	Hash functions
RID	Real identity of the vehicle
PID	Pseudonym of the vehicle
ΔT	The valid period of the pseudonym
RL	The revocation list
T_{RL}, ts	The timestamp of RL and message
msg	The message
$\oplus$	The exclusive-OR operation

4.1. System Initialization

The trusted authority (TA) and the Key Generation Center (KGC) cooperate to generate system parameters as follows.

- (1) Given security parameters k , TA and KGC choose two large primes p and q and construct a non-singular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$, where $a, b \in \mathbb{Z}_p^*$ and $4a^3 + 27b^2 \bmod p \neq 0$. Then TA and KGC define a cyclic group G with the order q on the elliptic curve E and choose a generator P of G .
- (2) TA randomly selects $s_1 \in \mathbb{Z}_q^*$ and computes $P_{pub1} = s_1 \cdot P$. KGC chooses a random number $s_2 \in \mathbb{Z}_q^*$ and computes $P_{pub2} = s_2 \cdot P$.
- (3) TA and KGC define five secure hash functions $H_0 : G \rightarrow \{0,1\}^\ell$, $H_1 : G \times G \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \mathbb{Z}_q^* \times G \times G \rightarrow \mathbb{Z}_q^*$, $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_4 : G \times \{0,1\}^* \times \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, where ℓ denotes the length of real identity of vehicles. The system parameters are $\{q, p, P, P_{pub1}, P_{pub2}, H_0, H_1, H_2, H_3, H_4\}$. TA and KGC publish the system parameters to all FNs and vehicles. Meanwhile, s_1 is only known to TA and s_2 is only known to KGC.
- (4) In addition, TA and KGC maintain a binary tree BT and TA manages a revocation list RL .

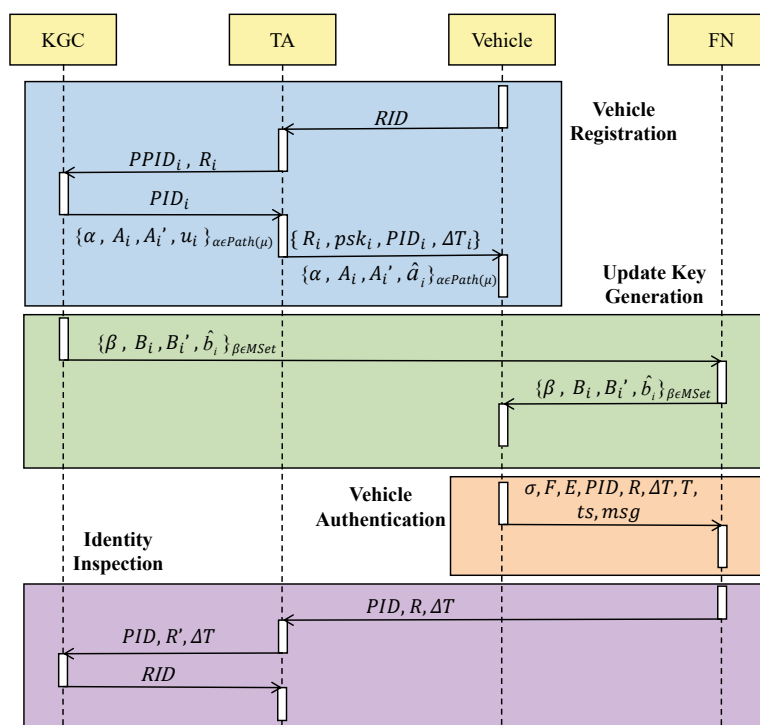


Figure 3. Sequence of the four phases in EAPAF.

4.2. Vehicle Registration

All vehicles have to register with TA and KGC through a secure channel before joining the networks.

- (1) The vehicle $\mathcal{V}$ first registers offline with the Department of Motor Vehicle (DMV) to obtain its real identity RID , then $\mathcal{V}$ sends RID to TA through a secure channel.
- (2) TA verifies the RID with the help of DMV. If the verification fails, TA discards the RID . Otherwise, TA randomly chooses an unsigned leaf node μ from the binary tree for the registered vehicle $\mathcal{V}$ and stores RID in the node.
- (3) Afterwards, TA randomly chooses $r_i \in \mathbb{Z}_q^* (i \in [1, l])$ and computes $R_i = r_i \cdot P$ and $PPID_i = RID \oplus H_0(s_1 \cdot R_i)$, where l denotes the number of pseudonyms issued by TA. TA sends $\{PPID_i, R_i\}$ to KGC for pseudonym generation.
- (4) KGC first calculates pseudonyms

$$PID_i = PPID_i \oplus H_0(s_2 \cdot R_i) \quad (1)$$

for the registered vehicle $\mathcal{V}$.

- (5) For each node $\alpha \in Path(\mu)$,
 - (i) If α is undefined, KGC randomly selects $x \in \mathbb{Z}_q^*$ and stores x in the node α .
 - (ii) Then KGC chooses random numbers $a_i, a_i' \in \mathbb{Z}_q^* (i \in [1, l])$.
 - (iii) KGC computes partial keys

$$\begin{aligned}
 A_i &= a_i \cdot P, \\
 A_i' &= a_i' \cdot P, \\
 h_2 &= H_2(x, P_{pub1}, P_{pub2}), \\
 u_i &= a_i + a_i' + xh_2 \pmod{q}.
 \end{aligned} \quad (2)$$

- (iv) KGC sends pseudonyms PID_i and partial keys $\{\alpha, A_i, A_i', u_i\}_{\alpha \in Path(\mu)}$ back to TA.

- (6) TA computes the proof of the pseudonym

$$\begin{aligned} h_{1_i} &= H_1(PID_i, R_i, \Delta T_i), \\ psk_i &= r_i + h_{1_i} s_1 \bmod q, \\ \hat{a}_i &= u_i + s_1 h_{1_i} \bmod q. \end{aligned} \quad (3)$$

where ΔT_i is the valid period of the pseudonym PID_i .

- (7) TA sends certificates $\{R_i, psk_i, PID_i, \Delta T_i\}$ and partial keys $\{\alpha, A_i, A_i', \hat{a}_i\}_{\alpha \in Path(\mu)}$ to $\mathcal{V}$ through secure channel.
 (8) Then $\mathcal{V}$ validates the received $\{R_i, psk_i, PID_i, \Delta T_i\}$ by computing

$$psk_i \cdot P = R_i + h_{1_i} \cdot P_{pub1} \quad (4)$$

where $h_{1_i} = H_1(PID_i, R_i, \Delta T_i)$. If the equation holds, $\mathcal{V}$ stores certificates $\{R_i, psk_i, PID_i, \Delta T_i\}$ and partial keys $\{\alpha, A_i, A_i', \hat{a}_i\}_{\alpha \in Path(\mu)}$. Otherwise, discard the received certificates and partial keys. The correctness is proved in 8.

4.3. Update Key Generation

To realize revocation and preserve network security, TA periodically generates a revocation list RL that includes the real identities of misbehaving users. In EPAF, KGC broadcasts update keys instead of the RL to improve the revocation efficiency. KGC generates update keys based on the binary tree BT , the revocation list RL , and the timestamp T_{RL} of the revocation list. Given $\{BT, RL, T_{RL}\}$, KGC executes **KUNode Algorithm** as described in Algorithm 1 to obtain the minimum node set $MSet$.

For each node $\beta \in MSet$,

- (1) KGC first retrieves x stored in β . If the node β is undefined, skip the process.
- (2) Then KGC chooses random numbers $b, b' \in Z_q^*$.
- (3) Next, KGC calculates

$$\begin{aligned} B &= b \cdot P, \\ B' &= b' \cdot P, \\ h_2 &= H_2(x, P_{pub1}, P_{pub2}), \\ h_3 &= H_3(T_{RL}), \\ \hat{b} &= b + s_2 h_3 + b' - x h_2 \pmod{q}. \end{aligned} \quad (5)$$

- (4) Finally, KGC publishes update keys $\{\beta, B, B', \hat{b}\}_{\beta \in MSet}$ to all vehicles in networks through FNs.

4.4. Vehicle Key Generation

Given update keys $\{\beta, B, B', \hat{b}\}_{\beta \in MSet}$ and partial keys $\{\alpha, A_i, A_i', \hat{a}_i\}_{\alpha \in Path(\mu)}$, the vehicle $\mathcal{V}$ calculates the vehicle key in advance.

- (1) If $Path(\mu) \cap MSet \neq \emptyset$, $\mathcal{V}$ arbitrarily chooses a node $\gamma \in Path(\mu) \cap MSet$.
- (2) Then $\mathcal{V}$ computes $e = \hat{a} + \hat{b} \bmod q$ as the vehicle key.
- (3) Meanwhile, $\mathcal{V}$ calculates $E = A + A' + B + B'$ for subsequent authentication.

4.5. Vehicle Authentication

For a message msg to be shared with nearby vehicles and FNs, $\mathcal{V}$ signs the message msg as follows:

- (1) $\mathcal{V}$ selects a random number $f \in Z_q^*$ as the private key.

- (2) Then $\mathcal{V}$ computes the public key F and the signature σ

$$\begin{aligned} F &= f \cdot P, \\ \sigma &= f + eh_m \bmod q, \end{aligned} \quad (6)$$

where $h_m = H_4(msg, F, ts)$ and ts is the current timestamp.

- (3) Afterwards, $\mathcal{V}$ sends authentication packet $\{\sigma, F, E, PID, R, \Delta T, T_{RL}, ts, msg\}$ to FNs or vehicles.
- (4) The receiver first verifies if ts is fresh or not. Assuming that the receiving time is ts' , the receiver continues the authentication if $ts' - ts < \Delta ts$, where Δts is a conjointly agreed transmission delay.
- (5) Suppose that the receiver receives multiple packets $\{\sigma_i, F_i, E_i, PID_i, R_i, \Delta T_i, T_{RL_i}, ts_i, msg_i\} (i \in [1, n])$ from different vehicles $\mathcal{V}_1, \mathcal{V}_2, \dots, \mathcal{V}_n$. The receiver first verifies whether Equation (7) is satisfied, where $h_{1_i} = H_1(PID_i, R_i, \Delta T_i)$, $h_{3_i} = H_3(T_{RL_i})$ and $h_{m_i} = H_4(msg_i, F_i, ts_i)$. If the equation holds, the receiver accepts the messages. The correctness is proved in (9).

$$\begin{aligned} \sum_{i=1}^n \sigma_i \cdot P &= \sum_{i=1}^n F_i + \sum_{i=1}^n (h_{m_i} \cdot E_i) \\ &+ \sum_{i=1}^n (h_{1_i} h_{m_i}) \cdot P_{pub1} + \sum_{i=1}^n (h_{3_i} h_{m_i}) \cdot P_{pub2} \end{aligned} \quad (7)$$

5. System Analysis

This section first proves the correctness of equations, then presents the security analysis of EPAF.

5.1. Correctness Proof

Theorem 1. In the vehicle registration phase, vehicles store certificates if verifications are successful.

Proof. Given certificates $\{R_i, psk_i, PID_i, \Delta T_i\}$, $\mathcal{V}$ stores them if Equation (4) holds. The proof process is as follows:

$$\begin{aligned} \sum_{i=1}^n psk_i \cdot P &= \sum_{i=1}^n (r_i + h_{1_i} s_1) \cdot P \\ &= \sum_{i=1}^n r_i \cdot P + \sum_{i=1}^n h_{1_i} s_1 \cdot P \\ &= \sum_{i=1}^n R_i + \sum_{i=1}^n h_{1_i} \cdot P_{pub1} \end{aligned} \quad (8)$$

□

Theorem 2. In the vehicle authentication phase, the receiver accepts messages if verifications are successful.

Proof. Given multiple packets $\{\sigma_i, F_i, E_i, PID_i, R_i, \Delta T_i, T_{RL_i}, ts_i, msg_i\}$ from different vehicles, the receiver accepts messages if Equation (7) holds. The proof process is shown in Equation (9). □

$$\begin{aligned}
 \sum_{i=1}^n \sigma_i \cdot P &= \sum_{i=1}^n (f_i + e_i h_{m_i}) \cdot P \\
 &= \sum_{i=1}^n F_i + \sum_{i=1}^n (\hat{a}_i + \hat{b}_i) h_{m_i} \cdot P \\
 &= \sum_{i=1}^n F_i + \sum_{i=1}^n (a_i + s_1 h_{1_i} + a_i' + x h_{2_i} + b_i \\
 &\quad + s_2 h_{3_i} + b_i' - x h_{2_i}) h_{m_i} \cdot P \\
 &= \sum_{i=1}^n F_i + \sum_{i=1}^n (a_i + b_i + a_i' + b_i') h_{m_i} \cdot P \\
 &\quad + \sum_{i=1}^n s_1 h_{1_i} h_{m_i} \cdot P + \sum_{i=1}^n s_2 h_{3_i} h_{m_i} \cdot P \\
 &= \sum_{i=1}^n F_i + \sum_{i=1}^n h_{m_i} \cdot (A_i + B_i + A_i' + B_i') \\
 &\quad + \sum_{i=1}^n (h_{1_i} h_{m_i}) \cdot P_{pub1} + \sum_{i=1}^n (h_{3_i} h_{m_i}) \cdot P_{pub2} \\
 &= \sum_{i=1}^n F_i + \sum_{i=1}^n (h_{m_i} \cdot E_i) \\
 &\quad + \sum_{i=1}^n (h_{1_i} h_{m_i}) \cdot P_{pub1} + \sum_{i=1}^n (h_{3_i} h_{m_i}) \cdot P_{pub2}
 \end{aligned} \tag{9}$$

5.2. Security Analysis

The communication in EPAF relies on wireless channels, and thus an adversary may intercept, modify, replay, or forge authentication packets. This subsection demonstrates that EPAF is secure against adaptive chosen-message attacks under the ECDLP assumption and in the random-oracle model. We assume that TA and KGC operate honestly, do not collude with the adversary, and never disclose their master secrets or internal states. A Type I adversary may issue adaptive hash and signature queries but cannot obtain the target effective private key. A Type II adversary may additionally compromise the private keys of non-target vehicles, but it cannot obtain the target vehicle's effective private key or replace the target authentication context.

The following game is played between challenger $\mathcal{C}1$ and a Type I PPT adversary $\mathcal{A}1$.

Setup: Given a security parameter, $\mathcal{C}1$ generates the system parameters $para$, the private key s_1 of TA, and the private key s_2 of KGC. It honestly generates and fixes the target context $ctx^* = (E^*, PID^*, R^*, \Delta T^*, T_{RL}^*)$. For this context, it sets $\tau_1^* = H_1(PID^*, R^*, \Delta T^*)$, $\tau_2^* = H_3(T_{RL}^*)$, and denotes the effective public key by $Y^* = E^* + \tau_1^* P_{pub1} + \tau_2^* P_{pub2} = e^* P$, where e^* is the effective private key known only to the target vehicle. Then, $\mathcal{C}1$ sends $para$ and the public target context to $\mathcal{A}1$. The values s_1 , s_2 , and e^* are not disclosed.

Queries: $\mathcal{A}1$ adaptively submits hash and signature queries. In particular, for each new query (msg_i, F_i, ts_i) , H_4 returns an independently and uniformly selected value in $\mathbb{Z}_q$ and records it in L_{H_4} ; a repeated query receives the recorded value. For a signature query on (msg_i, ts_i) under ctx^* , $\mathcal{C}1$ returns a valid authentication packet containing (σ_i, F_i) .

Output: $\mathcal{A}1$ outputs an authentication packet $\{\sigma^*, F^*, E^*, PID^*, R^*, \Delta T^*, T_{RL}^*, ts^*, msg^*\}$. It wins if the timestamp is admissible, (msg^*, ts^*) has not appeared in a signature query under ctx^* , and the individual verification equation $\sigma^* P = F^* + H_4(msg^*, F^*, ts^*) Y^*$ holds.

Definition 2. If any Type I PPT adversary $\mathcal{A}_1$ wins the above game with only negligible probability, EPAF is secure against adaptive chosen-message attacks for an individual authentication packet under the fixed target context.

Theorem 3. Suppose that the ECDLP assumption holds in the group G and that H_4 is a random oracle. Under the above honest-authority and fixed-target-context assumptions, EPAF is unforgeable for an authentication packet against a Type I adversary.

Proof. Assume that $\mathcal{A}_1$ wins the above game with a non-negligible probability ϵ . We construct a challenger $\mathcal{C}_1$ that uses $\mathcal{A}_1$ to solve an ECDLP instance $(P, Q = xP)$.

Setup: $\mathcal{C}_1$ executes the *System Initialization* phase and fixes τ_1^* and τ_2^* . It embeds the ECDLP instance into the target effective public key by setting

$$E^* = Q - \tau_1^* P_{pub1} - \tau_2^* P_{pub2}. \quad (10)$$

Therefore, $Y^* = E^* + \tau_1^* P_{pub1} + \tau_2^* P_{pub2} = Q$. Since Q is uniformly distributed in G , the resulting effective public key has the same distribution as an honestly generated effective public key. The target context remains fixed after this step.

Queries: $\mathcal{A}_1$ is permitted to query the following oracles.

- (1) H_1 oracle query: $\mathcal{C}_1$ maintains a list L_{H_1} . For a new query $(PID_i, R_i, \Delta T_i)$, it randomly chooses $\tau_{1_i} \in \mathbb{Z}_q$, records the tuple, and returns τ_{1_i} . A repeated query receives the recorded value.
- (2) H_3 oracle query: $\mathcal{C}_1$ maintains a list L_{H_3} . For a new query T_{RL_i} , it randomly chooses $\tau_{2_i} \in \mathbb{Z}_q$, records the tuple, and returns τ_{2_i} . A repeated query receives the recorded value.
- (3) H_4 oracle query: $\mathcal{C}_1$ maintains a list L_{H_4} . For a new query (msg_i, F_i, ts_i) , it randomly chooses $\tau_{3_i} \in \mathbb{Z}_q$, records the tuple, and returns τ_{3_i} . A repeated query receives the recorded value.
- (4) Signature query: Given (msg_i, ts_i) , $\mathcal{C}_1$ randomly chooses $\sigma_i, \tau_{3_i} \in \mathbb{Z}_q$ and computes

$$F_i = \sigma_i P - \tau_{3_i} Q. \quad (11)$$

If (msg_i, F_i, ts_i) has not been defined in L_{H_4} , $\mathcal{C}_1$ sets $H_4(msg_i, F_i, ts_i) = \tau_{3_i}$ and returns the authentication packet under ctx^* . This packet is valid because

$$F_i + \tau_{3_i} Y^* = \sigma_i P - \tau_{3_i} Q + \tau_{3_i} Q = \sigma_i P. \quad (12)$$

In a real packet, $F_i = f_i P$ is uniform and $\sigma_i = f_i + \tau_{3_i} e^* \bmod q$; hence the simulated packet has the same distribution as a real one. The simulation aborts only if the programmed H_4 input was previously assigned a different value.

Output: Eventually, $\mathcal{A}_1$ outputs a valid fresh authentication packet $\{\sigma^*, F^*, E^*, PID^*, R^*, \Delta T^*, T_{RL}^*, ts^*, msg^*\}$. Except with probability at most $1/q$, $\mathcal{A}_1$ must have queried $H_4(msg^*, F^*, ts^*)$; otherwise it can satisfy the verification equation only by guessing the random-oracle value.

Extraction: Let $\tau_3^* = H_4(msg^*, F^*, ts^*)$. By the General Forking Lemma, $\mathcal{C}_1$ reruns $\mathcal{A}_1$ with the same random tape and the same oracle answers before this critical H_4 query, but returns a different value $\tau_3^{*'} \neq \tau_3^*$ at that query. With the probability guaranteed by the forking lemma, the second run outputs another valid forgery with the same $(ctx^*, msg^*, F^*, ts^*)$:

$$\begin{aligned} \sigma^* P &= F^* + \tau_3^* Q, \\ \sigma^{*'} P &= F^* + \tau_3^{*'} Q. \end{aligned} \quad (13)$$

Subtracting the two equations gives

$$(\sigma^* - \sigma^{*'})P = (\tau_3^* - \tau_3^{*'})Q. \quad (14)$$

Since $Q = xP$ and $\tau_3^* \neq \tau_3^{*'}$, $C1$ obtains

$$x = (\sigma^* - \sigma^{*'}) (\tau_3^* - \tau_3^{*'})^{-1} \bmod q, \quad (15)$$

thereby solving the ECDLP instance.

Analysis: Let q_{H_4} and q_s denote the numbers of H_4 and signature queries, respectively, and define

$$\epsilon_0 = \epsilon - \frac{q_s q_{H_4}}{q} - \frac{1}{q}. \quad (16)$$

The term $q_s q_{H_4} / q$ bounds conflicts when programming H_4 , and $1/q$ bounds a successful forgery without the critical H_4 query. A standard form of the General Forking Lemma gives

$$\Pr[C1 \text{ solves ECDLP}] \geq \epsilon_0 \left(\frac{\epsilon_0}{q_{H_4}} - \frac{1}{q} \right). \quad (17)$$

If ϵ is non-negligible, the right-hand side is non-negligible, which contradicts the ECDLP assumption. Therefore, ϵ is negligible. $\square$

The following game is played between challenger $C2$ and a Type II PPT adversary $A2$.

Setup: $C2$ honestly generates the system parameters and the fixed target context, and sends the public parameters and public target context to $A2$. The private keys of TA and KGC and the target effective private key are not disclosed.

Queries: $A2$ may issue the same hash and target-context signature queries as $A1$. It may also request the private keys and public keys of non-target vehicles. The target vehicle's effective private key cannot be queried.

Output: $A2$ outputs a fresh authentication packet for the fixed target context. It wins if $\sigma^* P = F^* + H_4(\text{msg}^*, F^*, ts^*) Y^*$ holds and the corresponding (msg^*, ts^*) was not submitted to the target-context signature oracle.

Definition 3. If any Type II PPT adversary $A2$ wins the above game with only negligible probability, EPAF is secure against adaptive chosen-message attacks in the presence of non-target vehicle compromise.

Theorem 4. Suppose that the ECDLP assumption holds in the group G and that H_4 is a random oracle. Possession of the private keys of polynomially many non-target vehicles does not enable a Type II PPT adversary to forge an authentication packet for the fixed target context.

Proof. The challenger generates the keys of all non-target vehicles honestly and answers the corresponding corruption queries directly. These keys are independent of the target effective private key embedded in $Y^* = Q$. The target-context hash and signature queries are simulated as in the proof of Theorem 3. Therefore, a successful target-context forgery allows the challenger to obtain two related forgeries by the same forking procedure and extract the discrete logarithm of Q . This contradicts the ECDLP assumption. $\square$

The above reductions prove the unforgeability of an authentication packet.

Theorem 5 (Message integrity and authentication). Under the honest-authority and fixed-valid-context assumptions, EPAF supports message integrity and authentication for an individual authentication packet.

Proof. Let $\{\sigma, F, E, PID, R, \Delta T, T_{RL}, ts, msg\}$ be an accepted authentication packet under a pre-validated target context. The verifier checks

$$\sigma P = F + H_4(msg, F, ts)Y, \quad (18)$$

where $Y = E + H_1(PID, R, \Delta T)P_{pub1} + H_3(T_{RL})P_{pub2}$ is fixed by that context.

First, Equation (18) binds msg, F , and ts to σ and the fixed effective public key Y . If an adversary changes msg, F , or ts and nevertheless produces a fresh packet that passes verification, the resulting tuple is a valid forgery that was not returned by the signing oracle. If the adversary changes only σ while keeping the remaining values unchanged, validity would require $\sigma'P = \sigma P$. Since P generates the prime-order group, this implies $\sigma' = \sigma \bmod q$; hence a different signature value cannot pass verification.

Second, for a Type I adversary that has no target effective private key, any fresh valid modified packet contradicts the individual-packet unforgeability established in Theorem 3. Third, even if a Type II adversary obtains the private keys of polynomially many non-target vehicles, a fresh valid packet for the fixed target context contradicts Theorem 4, because those non-target keys are independent of the target effective private key. Therefore, except with negligible probability, an adversary cannot alter the protected packet fields and still cause acceptance, the proposed EPAF supports message integrity and authentication. $\square$

Theorem 6 (Unlinkability). *EPAF achieves unlinkability for authentication packets generated by the same vehicle in different pseudonym periods.*

Proof. In EPAF, the vehicle sends the authentication packet $\{\sigma, F, E, PID, R, \Delta T, T_{RL}, ts, msg\}$ to FNs or other vehicles. For two different pseudonym periods, TA selects r_i and r'_i , which generate different public values $R_i = r_iP$ and $R'_i = r'_iP$. The corresponding pseudonyms are computed as $PID_i = RID_i \oplus H_0(s_1s_2R_i)$ and $PID'_i = RID_i \oplus H_0(s_1s_2R'_i)$, respectively. Therefore, without the cooperation of TA and KGC, an external adversary cannot recover the real identity or determine whether the two pseudonyms belong to the same vehicle. The random values used in EPAF have different lifetimes. Specifically, r_i, a_i , and a'_i are generated for a given pseudonym during vehicle registration, whereas b_i and b'_i are refreshed during update-key generation for each revocation period. Only f_i is independently selected for each authentication message. Consequently, $F_i = f_iP$ and the signature σ_i vary across authentication messages, while PID_i, R_i , and ΔT_i remain unchanged within the same active pseudonym period. The unlinkability provided by EPAF is limited to authentication packets generated in different pseudonym periods. $\square$

Theorem 7 (Conditional privacy preserving). *EPAF guarantees conditional privacy-preserving on vehicles, assuming the ECDLP assumption holds.*

Proof. (1) Identity privacy-preserving: Suppose an adversary $\mathcal{A}$ obtains a tuple $\{PID, R, \Delta T\}$ in the network by eavesdropping, where $R = r \cdot P, PID = RID \oplus H_0(s_1s_2 \cdot R)$. The adversary can only retrieve the real identity of the vehicle by calculating $RID = PID \oplus H_0(s_1s_2 \cdot R)$. The system private keys s_1 and s_2 are secretly stored by TA and KGC, respectively. Due to the complexity of the ECDLP, the adversary $\mathcal{A}$ cannot disclose the RID . Therefore, identity privacy-preserving on vehicles can be protected even if there are adversaries trying to retrieve the real identities of vehicles.

(2) Traceability: For the misbehaving vehicle to be revoked, TA and KGC must cooperate to extract its real identity. If a vehicle is found to have any misbehaviour, a FN forwards the tuple $\{PID, R, \Delta T\}$ obtained from the misbehaving vehicle to TA. TA computes $R' = s_1 \cdot R$ and forwards $\{PID, R', \Delta T\}$ to KGC. Then KGC retrieves the real identity

$RID = PID \oplus H_0(s_2 \cdot R')$ of the misbehaving vehicle. In addition, TA adds the RID to the revocation list RL and KGC generates update keys based on the RL for unrevoked vehicles. Hence, the misbehaving vehicle's real identity can be traced.

In conclusion, identity privacy-preserving and traceability on vehicles are both satisfied. Therefore, EPAF guarantees conditional privacy-preserving. $\square$

Theorem 8 (Distributed resolution authority). *EPAF can provide distributed resolution authority for vehicle revocation.*

Proof. Vehicle revocation requires the participation of both KGC and TA. In the revocation phase, TA and KGC cooperate to retrieve the real identity of the misbehaving vehicle. Then TA adds the misbehaving vehicle to the revocation list RL . Therefore, only the cooperation between TA and KGC can register and revoke vehicles, which satisfies the distributed resolution authority. $\square$

Theorem 9 (Resist attacks). *EPAF can resist various attacks, such as impersonation attacks, tampering attacks, and replay attacks.*

Proof. (1) Impersonation attacks: Assume an impersonation attacker can generate a valid authentication packet $\{\sigma, F, E, PID, R, \Delta T, T_{RL}, ts, msg\}$, which satisfies the equation $\sigma \cdot P = F + (h_m \cdot E) + (h_1 h_m) \cdot P_{pub1} + (h_3 h_m) \cdot P_{pub2}$. However, according to Theorems 3 and 4, there is no PPT adversary that can forge a valid authentication packet. Hence, EPAF can resist impersonation attacks.

(2) Tampering attacks: Suppose an attacker tampers an authentication packet $\{\sigma, F, E, PID, R, \Delta T, T_{RL}, ts, msg\}$, which means the attacker can tamper the original authentication packet to another valid packet. According to Theorems 3 and 4, EPAF offers unforgeable authentication packets for any PPT attacker, which implies EPAF can withstand tampering attacks.

(3) Replay attacks: EPAF adopts the current timestamp ts to guarantee the message cannot be replayed. The signature σ contained in the authentication packet $\{\sigma, F, E, PID, R, \Delta T, T_{RL}, ts, msg\}$ is generated based on $h_m = H_4(msg, F, ts)$. Therefore, EPAF can withstand replay attacks outside the freshness window. $\square$

6. Performance Analysis

This section evaluates EPAF in terms of computational cost, communication overhead, authentication delay, packet loss ratio, and revocation performance. The computational and communication costs of EPAF are compared with those of ESCA [26], EPCP [27], EABA [16], EPP-GAS [33], and CSFC [19]. The revocation performance analysis covers revocation-list size and query throughput. These two metrics are compared with those of the three schemes C2RL [36], IMF-PR [37], and a conventional X.509 CRL [38].

6.1. Computation Overhead

To evaluate the computational efficiency of EPAF, we compare the costs of signature generation (SG), single-signature verification (SSV), and multiple-signature verification (MSV) with those of ESCA, EPCP, EABA, EPP-GAS, and CSFC [16,19,26,27,33]. The execution times of the required cryptographic operations are taken from the benchmark results reported in [39] to ensure a consistent comparison. The corresponding operation times are summarised in Table 3. Following common practice, we consider only cryptographic operations whose execution time exceeds 0.1 ms, while omitting comparatively inexpensive operations, such as elliptic-curve point addition and ordinary hash evaluation.

Table 3. Execution time of cryptographic operations.

Notations	Cryptographic Operations	Time (ms)
T_{bp}	Bilinear pairing	5.5852
$T_{bp.pm}$	Point multiplication associated with the bilinear pairing	0.817
$T_{ec.pm}$	Point multiplication associated with the elliptic curve	0.3476

Table 4 compares the computational costs of the considered authentication schemes in both V2I and V2V communication scenarios. Figure 4 further illustrates their computational costs in the V2I scenario. Since EPP-GAS [33] does not support single-signature verification (SSV), no SSV result is reported for this scheme.

Table 4. Comparison of computation overhead of various schemes.

Schemes	V2I			V2V		
	SG	SSV	MSV	SG	SSV	MSV
ESCA [26]	$T_{ec.pm}$	$4T_{ec.pm}$	$2nT_{ec.pm}$	$T_{ec.pm}$	$4T_{ec.pm}$	$2nT_{ec.pm}$
EPCP [27]	$T_{ec.pm}$	$5T_{ec.pm}$	$(4n + 1)T_{ec.pm}$	$T_{ec.pm}$	$5T_{ec.pm}$	$(4n + 1)T_{ec.pm}$
CSFC [19]	$5T_{ec.pm}$	$4T_{ec.pm}$	$4nT_{ec.pm}$	—	—	—
EPP-GAS [33]	$nT_{ec.pm}$	—	$(4n + 2)T_{ec.pm} + 4T_{bp}$	$3T_{ec.pm}$	—	$3nT_{ec.pm}$
EABA [16]	$3T_{ec.pm}$	$4T_{ec.pm} + 3T_{bp}$	$(2n + 3)T_{ec.pm} + 3T_{bp}$	$3T_{ec.pm}$	$4T_{ec.pm} + 3T_{bp}$	$(2n + 3)T_{ec.pm} + 3T_{bp}$
EPAF	$T_{ec.pm}$	$4T_{ec.pm}$	$(n + 3)T_{ec.pm}$	$T_{ec.pm}$	$4T_{ec.pm}$	$(n + 3)T_{ec.pm}$

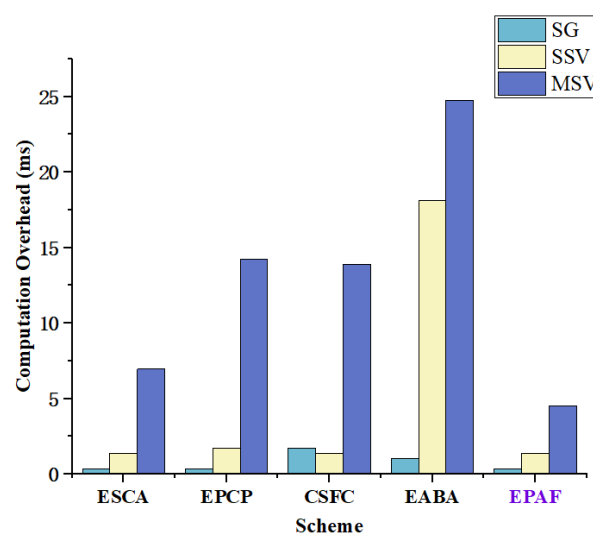


Figure 4. Computation overhead for schemes.

In the V2I scenario, EPAF, ESCA [26], and EPCP [27] incur the same signature generation (SG) cost, which is lower than those of CSFC [19], EPP-GAS [33], and EABA [16]. This result indicates that EPAF introduces limited computational burden for message signing at the vehicle side. For single-signature verification (SSV), EPAF has the same computational cost as ESCA and CSFC, and requires less computation than EPCP and EABA. More importantly, EPAF achieves the lowest multiple-signature verification (MSV) cost among the considered schemes, whereas EPP-GAS incurs the highest cost. This advantage results from the batch verification mechanism of EPAF, which allows a receiver to verify multiple authentication messages together and avoids repeated expensive cryptographic operations. Such an improvement is particularly beneficial in dense traffic environments,

where vehicles and roadside units must process a large number of safety messages within a short period.

In the V2V scenario, the computational cost of EPP-GAS is lower than that in the V2I scenario, but remains higher than that of EPAF. The other schemes that support both communication modes incur the same computational costs in V2V and V2I communications. CSFC is excluded from the V2V comparison because it does not support V2V authentication. In addition to verifying message validity, EPAF verifies whether the sender holds certificates corresponding to the current revocation period. Thus, the reported computation cost reflects not only authentication processing but also integrated revocation enforcement. Overall, EPAF achieves competitive SG and SSV costs and provides a clear efficiency advantage in MSV, making it suitable for message-intensive fog-enabled vehicular communication environments.

6.2. Communication Overhead

Communication overhead is a critical performance metric for authentication schemes in VANETs because vehicles transmit messages frequently over bandwidth-constrained wireless channels. To ensure a consistent comparison, we adopt the parameter settings reported in [40]. For pairing-based schemes at the 80-bit security level, the bilinear map is defined as $e : G_1 \times G_1 \rightarrow G_T$, where an element in G_1 occupies 64 bytes and an element in $\mathbb{Z}_q^*$ occupies 20 bytes. For ECC-based schemes at the same security level, an additive cyclic group G generated by a point P of order $\bar{q}$ is used, where an elliptic-curve point and an element in $\mathbb{Z}_{\bar{q}}^*$ each occupy 40 bytes and 20 bytes, respectively. In addition, the size of a timestamp is set to 4 bytes following [28].

According to the packet structure defined in Section 4.5, a vehicle in EPAF transmits $\{\sigma, F, E, PID, R, T_{RL}, ts, msg\}$, where the pseudonym validity period ΔT is included in the pre-issued pseudonym credential and is not retransmitted with each authentication message. Excluding msg , the communication overhead of EPAF is $3 \times 40 + 2 \times 20 + 2 \times 4 = 168$ bytes.

For ESCA [26], the transmitted authentication information requires 204 bytes under the adopted parameter settings. In EPCP [27], a vehicle transmits $\{PID_i, pk_i, m_i, \sigma_i, t_i\}$, where $\sigma_i = \{w_i, U_i\}$. Excluding m_i , its communication overhead is $4 \times 40 + 2 \times 20 + 2 \times 4 = 208$ bytes. For EABA [16], the authentication packet $\{PID_{v_j}, \sigma, m_j, Ts_{v_j}\}$ requires $40 + 3 \times 20 + 4 = 104$ bytes.

The communication overhead of EPP-GAS [33] differs between the V2I and V2V scenarios. In the V2I scenario, a vehicle transmits $\{H_M, Ts, R_i, \dots, R_N\}$ to an RSU, resulting in an overhead of $2n \times 40 + (3n + 1) \times 20 + (n + 1) \times 4 = 144n + 24$ bytes for n authenticated messages. In the V2V scenario, a vehicle broadcasts $\{pid_i, X_i, F_i, Y_i, Ts_i\}$, resulting in an overhead of $2 \times 40 + 3 \times 20 + 4 = 144$ bytes. For CSFC [19], the authentication packet contains $\{X, \lambda, c, t\}$, and its communication overhead is $40 + 2 \times 20 + 4 = 84$ bytes.

Table 5 summarises the communication overhead of the compared schemes. EPAF requires 168 bytes for each authentication message, which is lower than the 204 bytes and 208 bytes required by ESCA and EPCP, respectively. Compared with EABA and CSFC, EPAF introduces a larger packet size because it carries additional information required for update-key-based revocation. Although CSFC has the smallest communication overhead, it does not support V2V authentication and is therefore excluded from the V2V comparison.

The comparison with EPP-GAS depends on both the communication scenario and the number of processed messages. In the V2V scenario, EPP-GAS requires 144 bytes, which is slightly lower than the 168 bytes required by EPAF. In the V2I scenario, EPP-GAS requires $144n + 24$ bytes; its overhead is therefore equal to that of EPAF when $n = 1$ and higher than that of EPAF when multiple messages are authenticated together. This result indicates that EPAF is more communication-efficient than EPP-GAS for batch-oriented V2I authentication.

Table 5. Comparison on communication overhead of various schemes.

Schemes	V2V	V2I
ESCA [26]	204 bytes	204 bytes
EPCP [27]	208 bytes	208 bytes
EABA [16]	104 bytes	104 bytes
CSFC [19]	84 bytes	84 bytes
EPP-GAS [33]	144 bytes	(144n + 24) bytes
EPAF	168 bytes	168 bytes

Compared with EABA, EPAF increases the authentication packet size from 104 bytes to 168 bytes, corresponding to an increase of approximately 61.5%. This additional communication cost results from the parameters introduced to support revocation through current-period update keys. In return, according to the preceding computation comparison, EPAF reduces the multiple-signature verification cost by approximately 92% relative to EABA. Moreover, EPAF enables a verifier to determine whether a sender holds valid certificates for the current revocation period during authentication, without requiring each verifier to maintain and repeatedly check a complete revocation list.

Overall, EPAF is not designed solely to minimise packet size. Instead, it balances batch-verification efficiency, communication overhead, and update-key-based revocation. The following analysis therefore evaluates revocation-list size and query control-path throughput.

6.3. Revocation List Size Analysis

This subsection compares the revocation list size with the three comparison schemes: C2RL [36], IMF-PR [37], and a conventional X.509 CRL [38]. The number of revoked physical vehicles is varied from $R = 50$ to 500 across the vehicular system [41]. With an illustrative 30 min revocation-update interval and a 5 min pseudonym lifetime [42,43], each revoked vehicle contributes six pseudonyms, so the number of revoked pseudonym entries is $n_i = 6R$. The false-positive target of the filter-based schemes is $\epsilon = 0.001$, and the IMF-PR load factor is $\alpha = 0.5$, following the comparative parameter analysis in [37].

The conventional X.509 CRL explicitly stores every revoked pseudonym. A 39-byte entry represents the serial number, revocation date, reason and encoding overhead, while mandatory fixed fields occupy 400 bytes.

$$S_{X.509} = 400 + 39n_i = 400 + 234R. \quad (19)$$

C2RL replaces explicit entries with a Bloom-filter bit array [36]. With a 24-byte header, a 64-byte signature, and $m = -n_i \ln 2 \log_2 \epsilon$ filter bits, its size is

$$S_{C2RL} = 88 + \left\lceil \frac{-n_i \ln 2 \log_2 \epsilon}{8} \right\rceil \text{ bytes.} \quad (20)$$

IMF-PR stores fingerprints in an improved Morton-filter structure rather than storing complete revoked-pseudonym entries [37]. Under the parameter model used in its comparative analysis, the retained fingerprint space depends on both the false-positive target and load factor:

$$S_{IMF} = 88 + \left\lceil \frac{(\log_2 5 - \log_2 \epsilon)n_i}{32\alpha} \right\rceil \text{ bytes.} \quad (21)$$

EPAF generates update-key items for the minimum set of legitimate subtrees. Each item $\{\beta, B, B', \hat{b}\}$ occupies 104 bytes and the timestamp T_{RL} occupies 4 bytes; therefore,

$$S_{EPAF} = 4 + 104|MSet| \text{ bytes.} \quad (22)$$

Because $|\text{MSet}|$ depends on the locations of revoked leaves, we evaluate adjacent, uniformly random, and maximally dispersed placements. Following a recent tree-based revocation experiment that configures an 11-level complete binary tree to support $2^{10} = 1024$ users [44], EPAF is assigned a capacity of 1024 vehicle leaves. This citation provides a reproducible tree-capacity precedent, not evidence that 1024 is a metropolitan-scale VANET population. The plotted EPAF line is the mean of 1000 random placements, and the shaded region spans the adjacent and dispersed cases.

Figure 5 shows different scaling mechanisms. The conventional X.509 CRL grows by 234 bytes per revoked physical vehicle, whereas C2RL and IMF-PR grow with their compact filter representations. At $R = 300$, the X.509 CRL requires 70,600 bytes, C2RL requires 1643 bytes, and IMF-PR requires 1471 bytes. EPAF requires 524 bytes for adjacent revocations, 41,240.52 bytes on average, and 53,252 bytes for the dispersed case. Thus, EPAF benefits strongly from subtree aggregation but is not uniformly smaller than the probabilistic filters. At $R = 500$, the corresponding X.509, C2RL, IMF-PR, and EPAF random-mean values are 117,400, 2679, 2392, and 38,675.568 bytes, respectively. The slight decrease in EPAF's mean occurs because fully revoked subtrees require no update item for legitimate leaves.

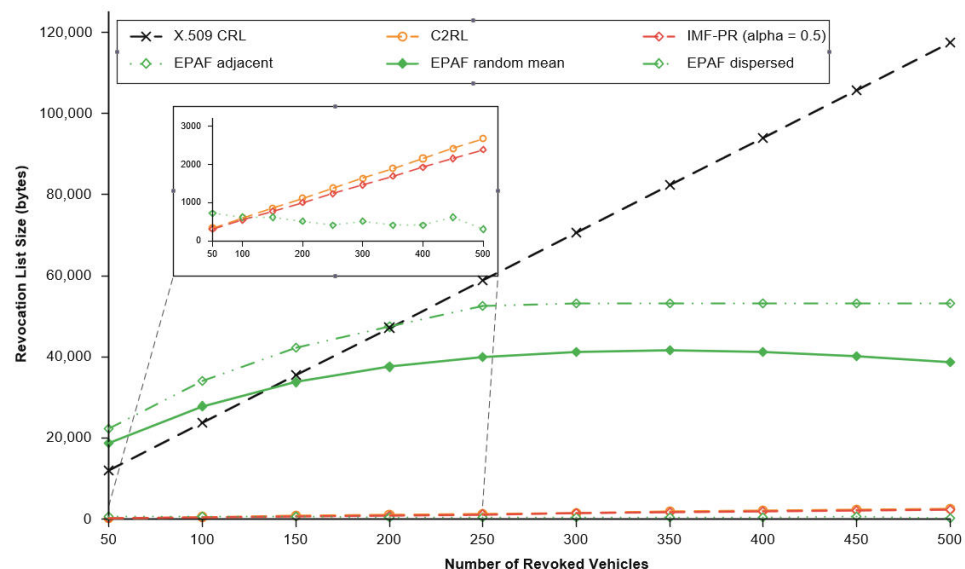


Figure 5. Revocation List size at TA/RSU side.

At the vehicle side, both filter-based schemes are assumed to retain the distributed filter used for local membership decisions, while the conventional X.509 CRL retains its full list. An EPAF vehicle instead selects one matching item satisfying $\text{Path}(\mu) \cap \text{MSet} \neq \emptyset$ and retains only that 104-byte item plus the 4-byte timestamp:

$$S_{\text{EPAF-vehicle}} = 4 + 104 = 108 \text{ bytes.} \quad (23)$$

As shown in Figure 6, EPAF retains a constant 108 bytes per legitimate vehicle under this protocol model. C2RL and IMF-PR remain much smaller than the conventional X.509 CRL, but their retained sizes increase with the number of revoked pseudonyms.

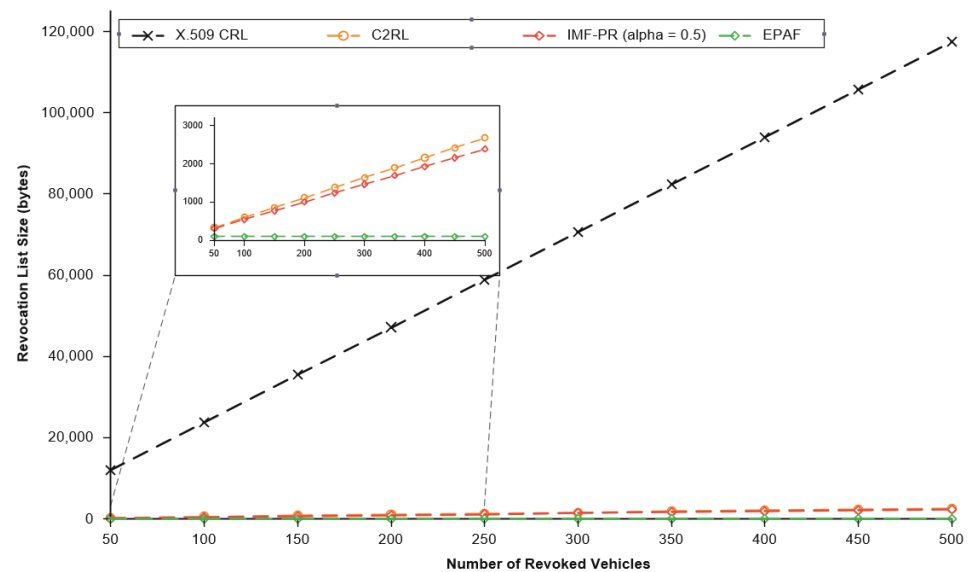


Figure 6. Revocation List size at vehicle side.

6.4. Query Throughput

Query throughput is the number of revocation membership decisions completed per second, $Q = N_q/t_q$. A common pure-Python 3.12 harness executes $N_q = 4096$ queries per repetition, with 50% present and 50% absent items, five warm-up runs, and 30 measured repetitions; the line reports the median. The same four schemes are compared as in Section 6.3. The conventional X.509 CRL performs a linear membership scan. C2RL performs Bloom-filter bit tests [36]; IMF-PR performs its Morton-style fingerprint lookup [37]; and EPAF searches the vehicle's tree path for a matching update node. Figure 7 therefore characterizes within-harness control-path cost. The y-axis interval from 1.5 to 2.5 million operations/s is omitted using a broken axis because no measured result lies in this range.

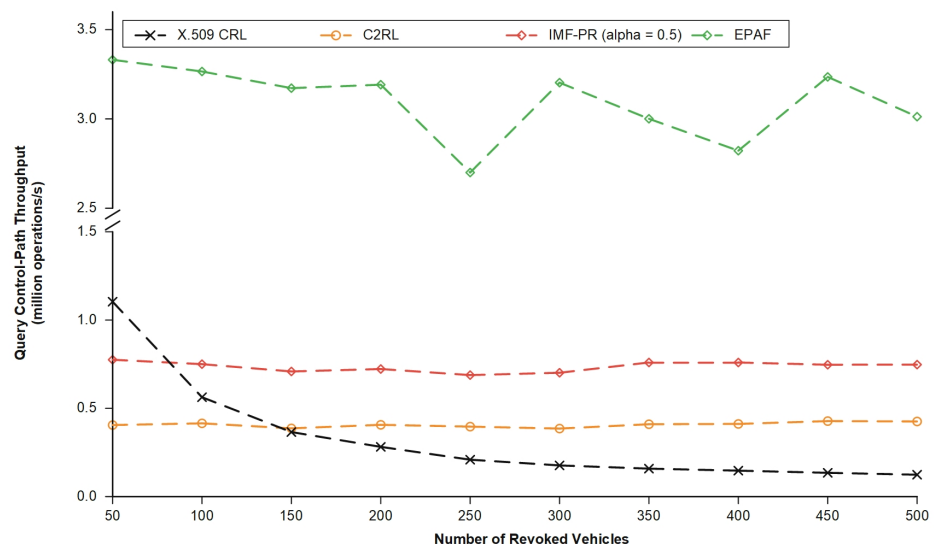


Figure 7. Query throughput versus number of revoked vehicles.

At $R = 300$, the median query throughputs are 0.177 million operations/s for the conventional X.509 CRL, 0.385 million for C2RL, 0.702 million for IMF-PR, and 3.203 million for the EPAF path-selection control path. At $R = 500$, the corresponding values are 0.124, 0.426, 0.748, and 3.012 million operations/s. The linear CRL scan slows as the list grows,

whereas the compact filters and EPAF tree lookup avoid a full entry scan. Within this harness, EPAF achieves the highest query throughput.

6.5. Simulation

The open-source Veins framework is used to evaluate the performance of EPAF and the compared authentication schemes [19,26,27,33]. Because CSFC [19] does not support V2V authentication, it is excluded from the V2V simulation comparison. In the simulation environment, SUMO generates vehicle mobility traces according to road layouts and traffic behaviour, while OMNET++ models wireless communication and message delivery among vehicles and roadside units. Veins integrates these two components to evaluate authentication performance under vehicular communication conditions. The main simulation parameters are listed in Table 6.

Table 6. Simulation parameters.

Parameter	Values
Hardware platform	CPU: 3.7GHz Intel(R) Core(TM) i7-8700K, 4 GB RAM
Operating system	Debian 9.4
Traffic generator	SUMO
Network simulator	OMNET++
Simulator	Veins
Map	Single local fog/RSU domain
Mobility model	SUMO-generated mobility traces
Simulator area	1000 m × 1000 m
Data transmission rate	6 Mbps
Transmission power	20 mW
Noise floor	−94 dBm
Number of vehicles	20–100 [45–47]
Time interval of the beacon	300 ms

The 1000 m × 1000 m area and the 20–100-vehicle range represent a local fog/RSU service domain rather than an entire urban road network [45–47]. The experiment is therefore a load-sensitivity analysis within one local domain.

6.5.1. Authentication Delay

To evaluate the practical efficiency of the compared schemes, we measure the average authentication delay in the V2V scenario, which reflects the combined effect of message transmission and authentication processing [48]. Let D_{au} denote the average time required for authentication messages generated by vehicles to be received and verified by their intended receivers. It is defined as

$$D_{au} = \frac{1}{N} \sum_{i=1}^N (T_g^i + T_t^i + T_w^i + T_v^i), \quad (24)$$

where N is the number of authentication messages, and T_g^i , T_t^i , T_w^i , and T_v^i denote the generation time, transmission time, waiting time, and verification time of the i -th message, respectively.

Figure 8 presents the average authentication delay D_{au} of EPAF, EABA [16], EPCP [27], EPP-GAS [33], and ESCA [26] under different vehicle densities. As the number of vehicles increases, more authentication messages are transmitted within the same communication area. This increase raises channel contention and verification workload, resulting in longer authentication delays for all compared schemes.

Among the compared schemes, EABA exhibits the most pronounced increase in authentication delay as vehicle density grows. This behaviour is mainly due to its relatively high verification cost, particularly the use of bilinear pairing operations, which becomes costly when many messages must be processed within a short time. EPCP also incurs a higher delay than EPP-GAS, while EPP-GAS requires more time than ESCA. These observations are consistent with the computational-cost comparison reported above.

EPAF achieves the lowest average authentication delay among the schemes evaluated in Figure 8. This result is primarily attributable to its batch verification mechanism and its use of comparatively efficient elliptic-curve operations, which reduce repeated authentication processing when multiple messages are received. The result indicates that EPAF is well suited to message-intensive V2V communication scenarios under the evaluated simulation settings.

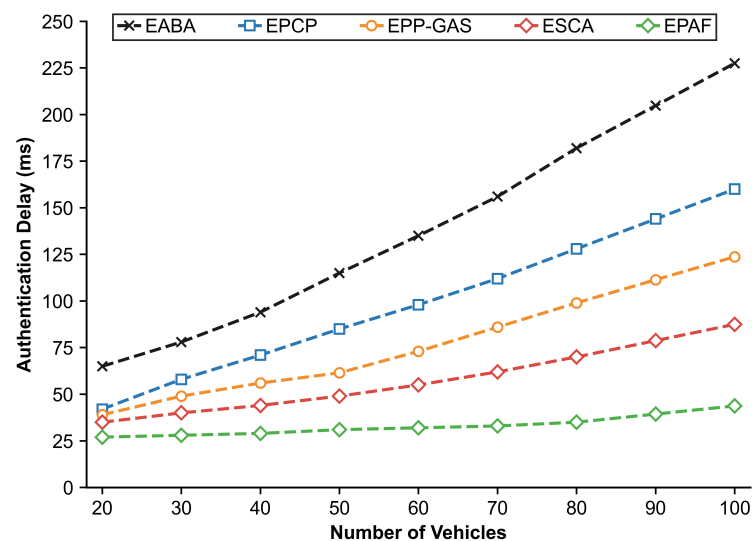


Figure 8. Average authentication delay versus number of vehicles.

6.5.2. Packet Loss Ratio

The packet loss ratio in V2V communication is used to assess the transmission performance of the compared schemes because both packet size and traffic load affect message delivery over a shared wireless channel [48]. Let P_l denote the proportion of authentication messages that are transmitted by vehicles but not successfully received by their intended receivers. It is defined as

$$P_l = 1 - \frac{N_r}{N_s}, \quad (25)$$

where N_s is the number of authentication messages sent by vehicles and N_r is the number of those messages successfully received by the intended receivers.

Figure 9 presents the packet loss ratio P_l of EPAF [27], EPCP [27], ESCA [26], EPP-GAS [33], and EABA [16] under different vehicle densities. As the number of vehicles increases, the packet loss ratio rises for all compared schemes. This trend is mainly caused by the growing number of authentication packets sharing the wireless channel, which increases channel contention and the probability of transmission collisions or delayed delivery.

EPAF achieves a lower packet loss ratio than EPCP and ESCA under the evaluated simulation settings. This result can be attributed to the combined effect of its packet size and authentication processing delay: efficient batch verification allows receivers to process incoming authentication messages more promptly, thereby reducing message accumulation under high traffic loads. However, EPAF incurs a slightly higher packet loss ratio than EABA and EPP-GAS. This difference is consistent with the larger authentication packet carried by EPAF to support update-key-based revocation.

The packet loss results should therefore be interpreted together with the security functions provided by each scheme. EPAF introduces additional authentication data so that a verifier can determine whether a sender holds valid certificates for the current revocation period during message authentication. However, because the revocation procedures of EABA and EPP-GAS are not evaluated under the same simulation model, this comparison does not claim that EPAF has lower total communication costs after all revocation-related exchanges are included. Instead, the results indicate that EPAF maintains an acceptable packet loss ratio while providing integrated revocation enforcement. Together with its authentication-delay results, EPAF offers a practical balance between transmission performance, verification efficiency, and revocation support in the evaluated V2V environment.

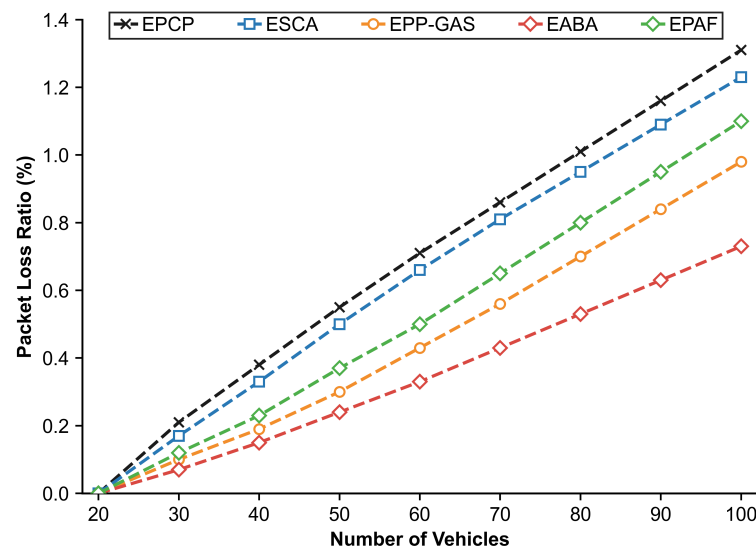


Figure 9. Average packet loss ratio versus number of vehicles.

7. Conclusions

This paper presents EPAF, an efficient privacy-preserving batch authentication scheme with revocation support for fog-enabled Vehicular Ad Hoc Networks (VANETs). By using roadside fog nodes to distribute update keys and forward reports on misbehaving vehicles, EPAF supports timely revocation management in dynamic vehicular communication environments. Rather than relying on ideal tamper-proof devices (TPDs) that store system-wide master secrets, EPAF assumes protected storage only for vehicle-local certificates, thereby limiting the impact of compromising an individual vehicle device. In addition, EPAF supports batch verification, enabling a receiver to authenticate messages from multiple vehicles efficiently and reduce repeated verification operations. To support revocation, EPAF introduces a tree-based update-key mechanism that distributes current authentication keys only to legitimate vehicles. Once the update keys for a new revocation period have been disseminated, revoked vehicles cannot generate authentication messages that are accepted under that period. The security analysis proves authentication packet EUF-CMA security in the random-oracle model under honest TA/KGC operation. It also addresses conditional identity privacy, traceability, and unlinkability across different pseudonym periods. The performance analysis shows that EPAF achieves the lowest multiple-signature verification cost and average authentication delay among the evaluated authentication schemes, while its authentication packet reflects the additional information required for integrated revocation. In the comparative evaluation of revocation performance against related schemes, EPAF offers a lightweight vehicle-side revocation state and the highest query throughput.

The security of EPAF relies on the trusted and non-colluding operation of TA and KGC, whereas roadside fog nodes are assumed to be honest-but-curious. EPAF does not require an RSU to participate in every V2V authentication. However, the proposed architecture uses roadside fog nodes to disseminate update keys and forward reports on misbehaving vehicles. Insufficient coverage, unstable connectivity, or delayed dissemination can therefore postpone revocation enforcement and can also cause temporary authentication unavailability or state inconsistency for legitimate vehicles that miss the current update. Future work will investigate vehicle-assisted key dissemination, adaptive update intervals, resilient update recovery, and more scalable distributed revocation mechanisms under larger, multi-domain traffic scenarios.

Author Contributions: Conceptualization, C.Z. and H.L.; methodology, C.Z. and X.G.; formal analysis, C.Z., Y.Y. and Q.Q.; writing—original draft preparation, C.Z. and X.G.; writing—review and editing, X.G., Y.Y., Q.Q. and H.L.; supervision, H.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Doctoral Research Funds for the Nanyang Normal University (Grant No. 2024ZX009), Key Scientific and Technological Research Projects in Henan Province (Grant No. 252102210247), Henan Province Key Scientific Research Projects for Higher Education Institutions (Grant No. 26B520033), and the Natural Science Foundation of Henan Province (Grant No. 262300420703).

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zhao, C.; Guo, N.; Gao, T. Efficient privacy-preserving authentication and group key agreement scheme in fog-enabled VANET. In *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*; Springer: Cham, Switzerland, 2022; pp. 161–171.
2. Guo, N.; Zhao, C.; Gao, T. An anonymous authentication scheme for edge computing-based car-home connectivity services in vehicular networks. *Future Gener. Comput. Syst.* **2020**, *106*, 659–671.
3. Dong, S.; Su, H.; Xia, Y.; Zhu, F.; Hu, X.; Wang, B. A comprehensive survey on authentication and attack detection schemes that threaten it in vehicular ad-hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 13573–13602.
4. B K, S.; Azam, F. Ensuring security and privacy in VANET: A comprehensive survey of authentication approaches. *J. Comput. Netw. Commun.* **2024**, *2024*, 1818079.
5. Kenney, J.B. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE* **2011**, *99*, 1162–1182.
6. Arif, M.; Wang, G.; Bhuiyan, M.Z.A.; Wang, T.; Chen, J. A survey on security attacks in VANETs: Communication, applications and challenges. *Veh. Commun.* **2019**, *19*, 100179.
7. AlMarshoud, M.; Sabir Kiraz, M.; Al-Bayatti, A.H. Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Comput. Surv.* **2024**, *56*, 1–39.
8. Zhu, D.; Guan, Y. Secure and lightweight conditional privacy-preserving identity authentication scheme for VANET. *IEEE Sens. J.* **2024**, *24*, 35743–35756.
9. Manasrah, A.; Yaseen, Q.; Al-Aqrabi, H.; Liu, L. Identity-based authentication in VANETs: A review. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 4260–4282.
10. Naskar, S.; Brunetta, C.; Zhang, T.; Hancke, G.; Gidlund, M. Authentication framework with enhanced privacy and batch verifiable message sharing in VANETs. *IEEE Trans. Veh. Technol.* **2025**, *74*, 18556–18571.
11. Shahrouz, J.K.; Analoui, M. Privacy-aware revocation in VANETs with a Blockchain using accumulator. *Veh. Commun.* **2025**, *53*, 100918.
12. Awais, S.M.; Yucheng, W.; Mahmood, K.; Alenazi, M.J.; Bashir, A.K.; Das, A.K.; Lorenz, P. Provably secure and lightweight authentication and key agreement protocol for fog-based vehicular ad-hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 21107–21116.
13. Liu, P.; He, Q.; Chen, Y.; Jiang, S.; Zhao, B.; Wang, X. A lightweight authentication and privacy-preserving aggregation for blockchain-enabled federated learning in VANETs. *IEEE Trans. Consum. Electron.* **2024**, *71*, 1274–1287.

14. Gao, J.; Cheng, T.; Shi, Q.; Yang, Z.; Zhu, J. Efficient Vehicle-fog-Cloud Anonymous Authentication and Group Key Agreement Scheme Based on QRNG in VANETs. *IEEE Internet Things J.* **2025**, *12*, 49366–49386.
15. Mundhe, P.; Verma, S.; Venkatesan, S. A comprehensive survey on authentication and privacy-preserving schemes in VANETs. *Comput. Sci. Rev.* **2021**, *41*, 100411.
16. Maurya, C.; Chaurasiya, V.K. Efficient anonymous batch authentication scheme with conditional privacy in the Internet of Vehicles (IoV) applications. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 9670–9683.
17. Azees, M.; Vijayakumar, P.; Deboarh, L.J. EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2467–2476.
18. Aghabagherloo, A.; Delavar, M.; Mohajeri, J.; Salmasizadeh, M.; Preneel, B. An efficient and physically secure privacy-preserving authentication scheme for vehicular ad-hoc NETWORKS (VANETs). *IEEE Access* **2022**, *10*, 93831–93844.
19. Ali, I.; Chen, Y.; Pan, C.; Chen, S. Cost-effective and secure scheme for fog computing-enabled internet of vehicles using CLC-to-PKI-based heterogeneous signcryption. *IEEE Trans. Intell. Veh.* **2024**. <https://doi.org/10.1109/TIV.2024.3455352>.
20. Kang, J.; Lin, D.; Jiang, W.; Bertino, E. Highly efficient randomized authentication in VANETs. *Pervasive Mob. Comput.* **2018**, *44*, 31–44.
21. Liu, Z.C.; Xiong, L.; Peng, T.; Peng, D.Y.; Liang, H.B. A Realistic Distributed Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE Access* **2018**, *6*, 26307–26317.
22. Cui, J.; Xu, W.; Han, Y.; Zhang, J.; Zhong, H. Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Veh. Commun.* **2020**, *21*, 100200.
23. Zhang, J.; Zhong, H.; Cui, J.; Xu, Y.; Liu, L. An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks. *IEEE Internet Things J.* **2020**, *7*, 3462–3473.
24. Kumar, P.; Kumari, S.; Sharma, V.; Li, X.; Sangaiah, A.K.; Islam, S.K.H. Secure CLS and CL-AS schemes designed for VANETs. *J. Supercomput.* **2019**, *75*, 3076–3098.
25. Zhu, F.; Yi, X.; Abuadba, A.; Khalil, I.; Huang, X.; Xu, F. A security-enhanced certificateless conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 10456–10466.
26. Yang, X.; Li, S.; Yang, L.; Du, X.; Wang, C. Efficient and security-enhanced certificateless aggregate signature-based authentication scheme with conditional privacy preservation for VANETs. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 12256–12268.
27. Yang, W.; Fan, J.; Song, K.; Zheng, Y.; Zhang, F. An efficient and practical conditional privacy-preserving aggregate authentication for vehicular ad-hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 20256–20267.
28. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 722–735.
29. Xu, G.; Li, X.; Jiao, L.; Wang, W.; Liu, A.; Su, C.; Zheng, X.; Liu, S.; Cheng, X. BAGKD: A Batch Authentication and Group Key Distribution Protocol for VANETs. *IEEE Commun. Mag.* **2020**, *58*, 35–41.
30. Lai, C.; Zheng, D.; Zhao, Q.; Jiang, X. SEGM: A secure group management framework in integrated VANET-cellular networks. *Veh. Commun.* **2018**, *11*, 33–45.
31. Sun, M.; Guo, Y.; Zhang, D.; Jiang, M.M. Anonymous Authentication and Key Agreement Scheme Combining the Group Key for Vehicular Ad Hoc Networks. *Complexity* **2021**, *2021*, 1–13.
32. Jayashree, S.; Kumar, S.S. An efficient group signature based certificateless verification scheme for vehicular ad-hoc network. *Wirel. Networks* **2024**, *30*, 3269–3298.
33. Xia, Y.; Zhu, S.; Liu, X.; Zhong, Q. EPP-GAS: An Efficient and Privacy-Preserving Cross Trust-Domain Group Authentication Scheme for Vehicle Platoon Based on Blockchain. *IEEE Trans. Intell. Transp. Syst.* **2024**, *25*, 19744–19756.
34. Yuan, J.; Zhao, Y.; Yu, J. A Conditional Privacy-Preserving Efficient Authentication Scheme with Revocability for Wireless Body Area Networks. *IEEE Internet Things J.* **2025**, *12*, 49942–49954.
35. Ye, X.; Xu, G.; Cheng, X.; Li, Y.; Qin, Z. Certificateless-Based Anonymous Authentication and Aggregate Signature Scheme for Vehicular Ad Hoc Networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1–16.
36. Höglund, J.; Furuheid, M.; Raza, S. Lightweight certificate revocation for low-power IoT with end-to-end security. *J. Inf. Secur. Appl.* **2023**, *73*, 103424.
37. Zhao, C.; Qi, J.; Gao, T.; Deng, X. IMF-PR: An improved Morton filter-based pseudonym revocation scheme in VANETs. *Sensors* **2023**, *23*, 4066.
38. Larisch, J.; Aqeel, W.; Lum, M.; Goldschlag, Y.; Kannan, L.; Torshizi, K.; Wang, Y.; Chung, T.; Levin, D.; Maggs, B.M.; et al. Hammurabi: A framework for pluggable, logic-based X.509 certificate validation policies. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 7–11 November 2022; pp. 1857–1870.
39. Cui, J.; Tao, X.; Zhang, J.; Xu, Y.; Zhong, H. HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs. *Veh. Commun.* **2018**, *14*, 15–25.
40. Thumbur, G.; Rao, G.S.; Reddy, P.V.; Gayathri, N.; Reddy, D.K.; Padmavathamma, M. Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. *IEEE Internet Things J.* **2020**, *8*, 1908–1920.

41. Liang, J.; Sadiq, M.; Yang, G.; Cheng, D. Bac-CRL: Blockchain-assisted coded caching certificate revocation list for authentication in VANETs. *J. Netw. Comput. Appl.* **2023**, *218*, 103716.
42. Scopelliti, G.; Baumann, C.; Alder, F.; Truyen, E.; Mühlberg, J.T. Efficient and timely revocation of V2X credentials. In Proceedings of the 2024 Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 26 February–1 March 2024.
43. Almani, D.; Muller, T.; Furnell, S. Leveraging reputation for enhanced decision accuracy in vehicle-to-vehicle communications under limited infrastructure. *Veh. Commun.* **2025**, *54*, 100927.
44. Xiao, P.; Yang, S.; Wang, H.; Zhang, Z.; Zou, C. Privacy-preserving revocable access control for LLM-driven electrical distributed systems. *Peer- Netw. Appl.* **2025**, *18*, 148.
45. Tang, H.; Rauf, A.; Lin, Q.; Dou, G.; Qin, C. Hybrid mutual authentication for vehicle-to-infrastructure communication without the coverage of roadside units. *Veh. Commun.* **2024**, *50*, 100850.
46. Audat, A.; Younes, M.B.; Yahia, M.; Ghoul, S. Confidential intelligent traffic light control system: Prevention of unauthorized traceability. *Big Data Cogn. Comput.* **2025**, *9*, 169.
47. Kaur, R.; Singla, C.; Singh, H.; Bhardwaj, R.; Sharma, P.; Aggarwal, A.; Alsekait, D.M.; Elminaam, D.S.A. A comprehensive framework for emergency message dissemination in urban VANET scenarios: A comparative analysis of clustering-based routing protocols. *IEEE Access* **2024**, *12*, 174284–174296.
48. Soleymani, S.A.; Goudarzi, S.; Anisi, M.H.; Zareei, M.; Abdullah, A.H.; Kama, N. A security and privacy scheme based on node and message authentication and trust in fog-enabled VANET. *Veh. Commun.* **2021**, *29*, 100335.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.