Privacy-preserving Proxy Re-encryption with Decentralized Trust Management for MEC-empowered VANETs

Xu Han, Daxin Tian, *Senior Member, IEEE*, Jianshan Zhou, Xuting Duan, Zhengguo Sheng, *Senior Member, IEEE*, and Victor C.M. Leung, *Life Fellow, IEEE*

***Abstract*—Multi-access edge computing (MEC) technology is widely deployed at the edge of Vehicular Ad hoc Networks (VANETs) to enhance their communication and computational capabilities. However, existing security and privacy preservation solutions for MEC applications in VANETs face several challenges, such as the risk of privacy exposure of vehicle authentication, increased overhead due to cryptographic algorithms, as well as resource occupation and malicious attacks on edge servers. In this paper, we propose an aggregated security solution for the confidential, efficient, and trustworthy sharing of data while safeguarding the privacy of vehicle identities. Firstly, we present a broadcast proxy re-encryption scheme based on cubic spline interpolation that ensures the security of the VANET system and the identity privacy of large-scale vehicles. The re-encryption system is designed to prioritize the reduction of re-encryption computation time rather than focusing on the sizes of re-encryption keys and ciphertexts. We further model the aggregation overhead in terms of communication and computation. Additionally, we propose an efficient protocol based on Practical Byzantine Fault Tolerant (PBFT) consensus to facilitate decentralized trust management for edge proxy servers. Our security analysis demonstrates that the proposed scheme satisfies the security and confidentiality requirements for data sharing in VANETs. Finally, we provide extensive simulations that reveal the performance and effectiveness of our solution.**

***Index Terms*—Vehicular edge computing, Proxy re-encryption, Blockchain, Identity privacy-preserving, Trust management.**

I. Introduction

Due to the iterative updates and advancements in related state-of-the-art technologies such as autonomous driving and artificial intelligence [1]–[4], traditional VANETs are insufficient to meet the increasingly prominent requirements for high-speed computation and communication for vehicular applications [5]. To address these challenges, MEC technology is being widely deployed at macro-base stations (MBS), small base stations (SBS), roadside units (RSU), and other edge service network facilities due to its remarkable storage and computing capabilities. This helps to reconcile the high mobility, high bandwidth, and low latency problems of VANETs [6]. However, the characteristics of geographical location leave MEC servers subject to frequent attacks and sabotage, as they are vulnerable to leaking the identity, location and other sensitive data of nearby vehicle users. Therefore, effective encryption or desensitization techniques are crucially required in MEC-empowered VANETs.

Existing literature has extensively discussed various encryption, re-encryption and signature schemes that have been applied in VANETs to tackle security and privacy concerns [7]–[9]. The basic difference between encryption and re-encryption lies in their respective purposes and mechanisms. Encryption safeguards the confidentiality of data by converting plaintext to ciphertext using an encryption algorithm and a secret key, while re-encryption modifies the access rights by delegating a trusted third party to re-encrypt the previously encrypted ciphertext. In practice, re-encryption algorithms tend to have higher computational demands. However, in MEC-empowered VANETs, where the roadside servers possess greater computational power, enabling them to handle the computational process of ciphertext conversion effectively alleviates the burden of frequent encryption and decryption operations on the vehicles. At the same time, the application of proxy re-encryption enhances the reliability and confidentiality of data on roadside edge servers. Maiti *et al.* [10] propose an identity-based broadcast proxy re-encryption scheme supported by a roadside semi-trusted proxy server while innovatively enabling the hiding of a group of vehicles' identities via interpolation-based approach. To the best of our knowledge, this is the only proxy re-encryption scheme that effectively protects vehicular identity privacy in MEC-empowered VANETs. However, like most studies in this area, their research is still restricted to limited comparisons of the performance of re-encryption algorithms in isolation from practical VANETs application scenarios. It is essential to consider the inherent characteristics of computation and communication when designing re-encryption solutions for VANETs, as they are closely related to the efficiency of implementation.

In addition, even though proxy re-encryption safeguards data security, attention also remains to be paid to the trustworthy sharing of re-encrypted cipher-texts throughout the entire roadside edge server system, as large-scale authorized vehicles travelling at high speeds demand real-time and consistent

This research was supported by the National Key Research and Development Program of China under Grant No. 2022YFC3803700. (corresponding author: Daxin Tian.)

X.Han, D.Tian, J.Zhou and X.Duan are with State Key Lab of Intelligent Transportation System, China, School of Transportation Science and Engineering, Beihang University, Beijing 100191, China (e-mail: 13661382800@163.com; dtian@buaa.edu.cn; jianshanzhou@foxmail.com; duanxuting@buaa.edu.cn).

Z. Sheng is with Department of Engineering and Design, the University of Sussex, Richmond 3A09, U.K. (e-mail: z.sheng@sussex.ac.uk).

V. C. M. Leung is with Computer Science and Software Engineering, Shenzhen University, Shenzhen 518060, China, and also with the University of British Columbia, Vancouver, BC V6T 1Z4, Canada (e-mail: vleung@ieee.org).

access to re-encrypted packets from the roadside proxy server. Since data requests and interactions in the VANETs usually occur between the vehicles and multiple roadside servers [11], the revolutionary blockchain platform, with its decentralization and immutability properties, derives extensive security and trust frameworks designed to support VANET services [6], [12]. Furthermore, benefiting from the high adaptability of blockchain in MEC-empowered VANET scenarios, block validation applications achieve faster and more efficient consensus mechanisms [13], [14].

MEC-empowered VANETs have to some extent addressed the issue of limited and constrained resources when executing secure re-encryption solutions, as the edge server can bear the significant computational cost of re-encryption algorithms. However, there is a dearth of research on proxy re-encryption for security and privacy protection that optimises the exploitation of communicative and computational resources. Besides, although extensive research has been carried out on both the security and privacy of MEC-empowered VANETs, no single study exists comprehensively considers the identity privacy of vehicles in proxy re-encryption and the trust management of roadside proxy edge servers.

In this paper, our aim is to address the aforementioned challenges to secure and trusted sharing of data while protecting vehicle identity privacy in MEC-empowered VANETs. The main contributions of our work are summarized as follows:

- We propose a privacy-preserving proxy re-encryption model for MEC-empowered VANETs, in which a cubic spline is used in re-key generation and re-encryption algorithms to protect the identity privacy of a group of vehicles.
- We construct a blockchain system for the roadside edge servers with a PBFT-based consensus mechanism to facilitate the trusted sharing of re-encrypted ciphertexts. Proxy re-encryption's confidentiality enables the consensus process to validate the digest instead of the complete ciphertext, enhancing efficiency.
- We theoretically analyse the security and privacy of the proposed scheme and evaluate the communication and computational integration costs in practical VANETs scenarios. The extensive simulations demonstrate the advantages of our solutions.

The rest of this paper is organized as follows. Section II provides an overview of the related works. Section III introduces the necessary preliminaries. Section IV presents the system model including a re-encryption system and a blockchain system, as well as corresponding consistency and security model. In section V, we define and construct a vehicular identity privacy-based proxy re-encryption scheme and a PBFT-based consensus protocol, followed by the theoretical analysis in Section VI. The performance of the proposed scheme is verified by simulations in Section VII. Finally, Section VIII concludes this paper.

II. Related Work

A. Identity-Based Broadcast Proxy Re-Encryption

Since it was proposed in 1996, proxy re-encryption(PRE) [15] has emerged as a widely used cryptographic primitive. The subsequent introduction of identity-based PRE (IPRE) [16] eliminated the administration of certificates thus making it possible to share data securely, efficiently and flexibly. To overcome the limitation that IPRE cannot generate re-encryption keys for multiple receivers, Xu *et al.* [17] presented identity-based broadcast PRE (IBPRE), which as a broadcast encryption scheme using identity as the public key, enabled the sender to effectively multicast ciphertext to a large number of receivers while only authorized receivers can decrypt the ciphertext. At present, IBPRE-derived solutions were deployed extensively in cloud computing scenarios, in which Huang *et al.* [18] enabled data owners to share and transmit data adaptively according to conditional access policies and time trapdoors in the ciphertext, Ge *et al.* [19] granted the proxy server the flexibility to revoke authorization to a set of receivers from the re-encryption key, Deng *et al.* [20] allowed the newly added user groups to be flexibly authorized and gave them access to the original data through the proposed ciphertext conversion mechanism, and Hu *et al.* [21] realized efficient proxy re-encryption under the constraint of the computation capacity of a receiver. In addition, proxy re-encryption has been shown to have the potential to be extended to edge computing scenarios [22] and VANETs [8], [23] for secure sharing and privacy preserving of data. Unfortunately, there was still a neglect of research on proxy re-encryption in edge computing-empowered VANETs.

B. Blockchain and Consensus

With continuous innovation and convergence, blockchain has now been considered to be an effective and feasible technology to provide a trustworthy environment for secure sharing and synchronization in VANETs [24]. Extensive studies have focused on the single or hybrid implementation of advanced consensus mechanisms such as Proof of Authority (PoA) [25], Proof of Work (PoW) [26], PoS (Proof of Stake) [26], [27], Byzantine Fault Tolerant (BFT) [28], [29], etc. Where some works enabled higher-level trust management in VANETs by constructing decentralized blockchain systems at the roadside [25], [26]. Kang *et al.* [27], based on PoS mechanism, proposed a voting scheme oriented to the reputation of miner candidates and an interaction scheme inspired by the contract theory, further coordinated to realize optimal management of consensus and prevention of voting collusion. Whereas Sowmya *et al.* [29], based on Practical Byzantine Fault Tolerant (PBFT) mechanism, achieved an efficient and extensible blockchain system in large-scale public transportation networks which regarding the mobility of vehicles and resource constraints of onboard devices.

While the above efforts took into account security issues, there were also some works which contribute to enhancing the safety of VANETs from a privacy perspective [30]–[33]. Among these studies, Lee *et al.* [31] suggested two blockchains in a VANET which consisted of a local short-term blockchain and a global reputation blockchain supported by location-based PBFT. In this system, disposable public keys were applied by vehicles in the system beyond the local short-term traffic information interaction to mitigate the risk of their identity privacy exposure. There were also other forefront approaches [32], [33], differently, conducted location privacy protection while trust management by performing a combination of consensus mechanisms and a k-anonymity scheme. However, the development of quantum computer, with its more powerful computing performance, posed a threat to the above privacy-enhanced blockchains protected by asymmetric cryptographic algorithms, making them potentially cracked [34]. Vehicle communication was considered as the main target of quantum cryptography application, and a wide range of quantum [35] and post-quantum [36] signature schemes have been proposed.

C. Comprehensive Security and Privacy

Along with the application of multiple advanced technologies as well as the expansion of various edge-based computing scenarios, security and privacy issues of VANETs have always been of extensive attention from academia and industry [37], [38]. Considerable research was devoted to exploring comprehensive approaches to ensure both security and privacy. He *et al.* [39] proposed an identity based signature scheme without bilinear pairing with lower communication and computation overhead, which was deployed in VANET to achieve secure and efficient vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communications along with identity privacy protection for vehicles. Zhang *et al.* [40] innovatively introduced hierarchical aggregation-verification technology for the verification of certificates and signatures within secure messages in VANET systems, thus guaranteeing the security and privacy of VANETs. Additionally, security and privacy protection solutions based on technologies such as digital twins [41] and federated learning [42] have also received widespread attention. There were also inspiring studies that combine proxy re-encryption with blockchain technology [43]. By incorporating these innovative technologies, VANETs can provide better protection for sensitive information and ensure the privacy and security of data transmission and computing.

III. Preliminaries

A. Bilinear Pairing

For two multiplicative groups $\mathbb{G}$ and $\mathbb{G}_\mathbb{T}$, with q denoting their prime order, we output the parameters $(q, \mathbb{G}, \mathbb{G}_\mathbb{T}, e)$ for a bilinear map. The mapping $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_\mathbb{T}$ meets following properties: 1) $\forall a, b \in \mathbb{Z}_q^*$, and $(g, t) \in \mathbb{G}^2$, $e(g^a, t^b) = e(g, t)^{ab}$, 2) $\forall g, t \neq 1_\mathbb{G}$, there exists $e(g, t) \neq 1_{\mathbb{G}_\mathbb{T}}$, 3) $\forall g, t \in \mathbb{G}$, $e(g, t)$is efficiently computable.

B. Cubic Spline

The segmental definition of a cubic spline $S(x)$ takes the following form [44].

$$S_i(x) = a_i + b_i(x - x_i) + c_i(x - x_i)^2 + d_i(x - x_i)^3, \quad i = 1, 2, \ldots, n-1 \tag{1}$$

where a_i, b_i, c_i, d_i represent the $4(n-1)$ unknown coefficients. The articulation conditions to be satisfied between each segment function are as follows.

$$\begin{cases} S_i(x_i) = y_i, where\ i = 1, 2, \ldots, n \\ S_i(x_{i+1}) = S_{i+1}(x_{i+1}) = y_{i+1}, where\ i = 1, 2, \ldots, n-2 \\ S_i'(x_{i+1}) = S_{i+1}'(x_{i+1}), where\ i = 1, 2, \ldots, n-2 \\ S_i''(x_{i+1}) = S_{i+1}''(x_{i+1}), where\ i = 1, 2, \ldots, n-2 \end{cases} \tag{2}$$

Let step length $h_i = x_{i+1} - x_i$, $m_i = S_i''(x_i) = 2c_i$, then we obtain

$$\begin{aligned} &h_i m_i + 2(h_i + h_{i+1}) m_{i+1} + h_{i+1} m_{i+2} \\ &= 6 \left[\frac{y_{i+2} - y_{i-1}}{h_{i+1}} - \frac{y_{i+1} - y_i}{h_i} \right] \end{aligned} \tag{3}$$

When natural boundary conditions are adopted, there are no external impacts at either end of the cubic spline (i.e. $S_1''(x_1) = 0$, and $S_{n-1}''(x_n) = 0$), we are able to obtain $m_0 = 0$ and $m_n = 0$. Therefore, the equations required to be solved can be written in (4).

IV. System and Security Model

A. System Model

We consider a MEC-empowered vehicular network where a cloud centre is integrated with a private key generator (PKG), a registration authority(RA) and a remote service provider (RSP) to provide services including authorization and remote computing. Meanwhile, there coexist a number of roadside clouds consisting of edge proxy service providers (EPSPs). With the support of edge computing architectures, data owners (e.g., intelligent mobile devices and vehicles) could transmit their contents directly to edge clouds. Vehicles in different groups aim to achieve a quick content request at near-edge locations while guaranteeing their own identity privacy.

As illustrated in Fig.1, we take into account the following scenarios, where PKG generates private keys for all participants, after which data owner OID generates initial ciphertext C_{OID} for original data M(e.g., software update packets) with its private key sk_{OID} and transfers it to roadside EPSPs instead of remote RSP while the channel is unoccupied. As they are not authorized, EPSPs and vehicles do not have access

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 \\ h_1 & 2(h_1+h_2) & h_2 & 0 & 0 & 0 & \cdots & 0 \\ 0 & h_2 & 2(h_2+h_3) & h_3 & 0 & 0 & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & 0 & 0 & 0 & h_{n-2} & 2(h_{n-2}+h_{n-1}) & h_{n-1} \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ \vdots \\ m_{n-1} \\ m_n \end{bmatrix} = 6 \begin{bmatrix} 0 \\ \frac{y_3-y_2}{h_2} - \frac{y_2-y_1}{h_1} \\ \frac{y_4-y_3}{h_3} - \frac{y_3-y_2}{h_2} \\ \vdots \\ \frac{y_n-y_{n-1}}{h_{n-1}} - \frac{y_{n-1}-y_{n-2}}{h_{n-2}} \\ 0 \end{bmatrix} \tag{4}$$

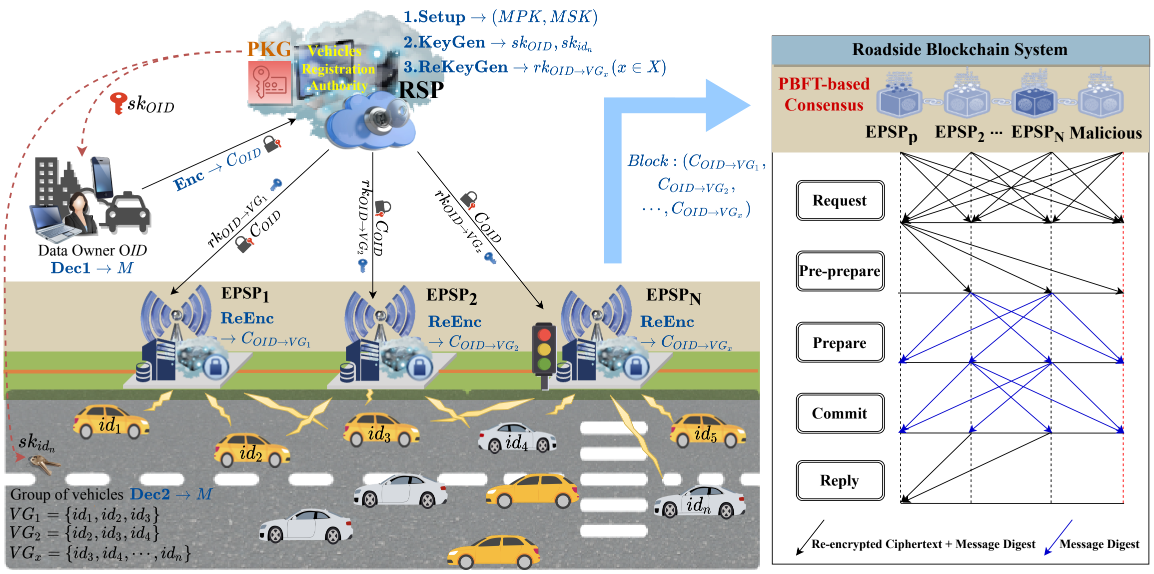


Fig. 1. System model with integrated proxy re-encryption and blockchain.

to M from C_{OID}. RSP is then responsible for broadcasting a profile of C_{OID} to all participants and further maintaining a register table that contains the identities of vehicles that requested the packet C_{OID}. Subsequently, RSP allocates access rights of C_{OID} to different groups of requested vehicles (e.g. $VG_1 = \{id_1, id_2, id_3\}$ and $VG_2 = \{id_2, id_3, id_4\}$) based on system conditions such as the status of wireless channel and the computational capacities of edge servers, which is performed by generating and sending re-encryption keys $rk_{OID} \to VG_1$ and $rk_{OID} \to VG_2$ to edge proxy service provider EPSP$_1$ and EPSP$_2$ respectively according to the private keys sk_{id_n} of requested vehicles. Once EPSP$_1$ re-encrypts the initial ciphertext C_{OID} with the re-encryption key $rk_{OID} \to VG_1$ and sends the re-encrypted packet C_{VG_1} to a specific vehicle group VG_1, it is possible for any vehicle in VG_1 (i.e. id_1, id_2, id_3) to decrypt the packet C_{VG_1} using its own private key (i.e. $sk_{id_1}, sk_{id_2}, sk_{id_3}$), thereby obtaining the original data M. The same operation can be performed by EPSP$_1$ for VG_2.

Furthermore, we consider a blockchain system for securely sharing re-encryption packets among N EPSPs on the roadside, where the action of sharing a re-encryption packet through the blockchain system is defined as a "transaction". Each EPSP maintains a cache list of the re-encryption packets which are output by its execution of the **ReEnc** algorithm which will be explained in detail later. Besides, two independent discrete-time slot systems are employed in this paper, the re-encryption time slot system and the blockchain time slot system, whose time is divided into discrete time periods $T^{reen} = \{1, \cdots, t, \cdots T\}$ and $T^{bc} = \{1, \cdots, t', \cdots T'\}$ respectively, where time periods t and t' have constant durations $\dot{T}$ and $\dot{T}'$ respectively. Suppose that in the re-encryption interval $\dot{T}$, each EPSP outputs $\mathcal{K}$ re-encryption packets and updates its cache list. Meanwhile, assume that within a block interval $\dot{T}'$, each EPSP chooses K re-encryption packets to be shared from its cache list, thus generating $N \cdot K$ transactions. In particular, $\mathcal{K}$ and K take various values in different time periods to characterize the time-varying of wireless networks. Based on the proposed re-encryption scheme, which ensures the confidentiality of plaintexts against EPSPs, the role of the blockchain is to establish a decentralized trust mechanism among EPSPs. This mechanism aims to mitigate the impact of malicious EPSPs, ensuring that every edge proxy server provider in roadside sharing system retains the ability to access all of the re-encryption packets for requests from vehicles. Whoever holds the earliest of $N \cdot K$ packets above will be appointed as the primary EPSP and perform the role of block producer. After a PBFT-based consensus, the primary EPSP appends the consensus block to the blockchain. PBFT is able to guarantee security and liveness in the presence of $F < (N-1)/3$ faulty EPSPs [45].

B. Assumptions and System Requirements

The proposed scheme assumes that the RSP, RA, and PKG operating in the trusted cloud center are entirely trustworthy and will not be compromised or collude with other malicious attackers. EPSPs, likewise, are not involved in any malicious manipulations such as attacking, deciphering, or tampering with the initial encrypted data received from the cloud center. However, EPSPs may exhibit a certain level of curiosity about the privacy of the identity of requested vehicles, which could lead to potentially malicious behavior when sharing re-encrypted ciphertexts among themselves. Therefore, several key system requirements must be met.

- Consistency of re-encryption. If vehicle id_i in $VG = \{id_1, id_2, \ldots, id_n\}$ is an authorized receiver from RA, it is able to recover the original data M from the re-encrypted packet $C_{OID\to VG}$.
- Consistency of blockchain. To ensure the trustworthy sharing of correctly held re-encrypted ciphertexts by EPSPs with roadside blockchain systems, it is essential that malicious EPSPs are no more than $F < (N-1)/3$.

- Security of data. It is not possible for For any polynomial time adversary (e.g., semi-trusted EPSP and intended receiver who is not authorized by RA) to recover original data M from initial ciphertext C_{OID} or any re-encrypted packet $C_{OID \to VG}$.
- Privacy of receivers. EPSPs cannot derive the identities of an authorized vehicle group from ciphertext or re-encryption key. Besides, a legitimate receiver id_i in a group VG of a re-encrypted packet $C_{OID \to VG}$ cannot recover the identity of another legitimate receiver id_j in group VG.

V. System Definitions

A. Vehicular Identity Privacy-based Proxy Re-encryption

Definition 1 (**VIPPR: Vehicular Identity Privacy-based Proxy Re-encryption**). *Let $VG = \{id_1, id_2, \ldots, id_n\}$ be the set of vehicle identities in the receiver group, and $n \in \mathbb{N}$ is the total number of vehicles in VG. A fully developed VIPPR scheme includes seven algorithms as follows.*

- **Setup**: System setup algorithm is executed by cloud centre with input $\alpha \in \mathbb{N}$, which is a security parameter determined by the security level of system. And its outputs are a system public key MPK and a system secret key MSK.
- **KeyGen**: PKG generates secret keys for all system users by running this algorithm. Without loss of generality, consider one data owner O as a system user. Leading to this algorithm with inputs MSK and identity OID of data owner. Accordingly, the output of this algorithm is a private key sk_{OID} corresponding to identity of data owner. Besides, OID will be used as the public key of data owner in the next algorithms.
- **Enc**: The inputs of this algorithm are MPK, OID and original data M as a plaintext. This algorithm is performed by data owner to produce a VIPPR initial ciphertext C_{OID}.
- **ReKeyGen**: The inputs of this algorithm are MPK, OID, sk_{OID} and a set of identities VG. The output of this algorithm is a re-encryption key $rk_{OID \to VG}$. This algorithm is invoked by the RSP.
- **ReEnc**: The inputs of this algorithm are MPK, $rk_{OID \to VG}$ and C_{OID}. The output is a re-encrypted VIPPR ciphertext $C_{OID \to VG}$. This algorithm is performed by the EPSP.
- **Dec1**: The inputs of this algorithm are MPK, sk_{OID} and C_{OID}. This algorithm is performed by data owner to result the original data M.
- **Dec2**: The inputs of this algorithm are MPK, a identity id_i of any one of the vehicles in VG, corresponding secret key sk_{id_i} and re-encrypted ciphertext $C_{OID \to VG}$. This algorithm can be executed by each vehicle in VG to obtain the decrypted original data M.

In addition, for any system public key MPK, any original data M, any **KeyGen**$(MSK, OID) \to sk_{OID}$ and **KeyGen**$(MSK, id_i) \to sk_{id_i}$ corresponding to a data owner's identity OID and a request vehicle's identity id_i where $id_i \in VG$, this scheme always satisfy:

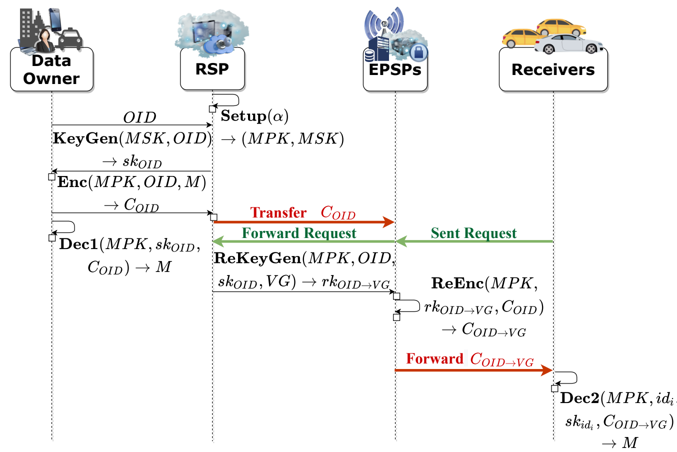


Fig. 2. Algorithm procedure of VIPPR.

- **Dec1**$(MPK, sk_{OID}, $**Enc**$(MPK, OID, M)) \to M$
- **Dec2**$((MPK, id_i, sk_{id_i}, $**ReEnc**$(MPK, $**ReKeyGen**$(MPK, OID, sk_{OID}, VG), $**Enc**$(MPK, OID, M))) \to M$

B. Construction of VIPPR

The proposed VIPPR scheme is constructed following the algorithm procedure in Fig.2.

- **Setup**$(\alpha) \to (MPK, MSK)$ takes a security parameter $\alpha \in \mathbb{N}$ as input, from which it constructs a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$, where $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are two multiplicative group with prime order $q(|q| = \alpha)$. This algorithm outputs a system public key MPK and a system secret key MSK below

$$MPK = (q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, v, t, t^{\beta}, u, u^{\beta}, \mathbb{H}_1, \mathbb{H}_2) \tag{5}$$

$$MSK = (g, \beta) \tag{6}$$

where secret parameter $\beta \in \mathbb{Z}_q^*$ and generators $(g, t, u) \in \mathbb{G}^3$ are randomly selected, and $v = e(g, t)$. Additionally, two cryptographic hash functions $\mathbb{H}_1 : \{0, 1\} \to \mathbb{Z}_q^*$ and $\mathbb{H}_2 : \mathbb{G}_{\mathbb{T}} \to \mathbb{G}$ are selected to map any length $\{0, 1\}$ strings to $\mathbb{Z}_q^*$ and $\mathbb{G}_{\mathbb{T}}$ to $\mathbb{G}$, respectively.

- **KeyGen**$(MSK, OID) \to sk_{OID}$ adopts MSK and user ID to output a corresponding private key to the user. For example, the private key of data owner O is

$$sk_{OID} = g^{\frac{1}{\beta + \mathbb{H}_1(OID)}} \tag{7}$$

- **Enc**$(MPK, OID, M) \to C_{OID}$ outputs the original ciphertext C_{OID} in the following form

$$C_{OID} = \langle \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3 \rangle$$
$$where \begin{cases} \mathrm{C}_1 = t^{\gamma(\beta + \mathbb{H}_1(OID))} \\ \mathrm{C}_2 = v^{\gamma} \cdot M \\ \mathrm{C}_3 = u^{\gamma\left[\frac{\beta + \mathbb{H}_1(OID)}{\mathbb{H}_1(OID)}\right]} \end{cases} \tag{8}$$

where $\gamma \in \mathbb{Z}_q^*$ is chosen randomly.

- **ReKeyGen**$(MPK, OID, sk_{OID}, VG) \to rk_{OID \to VG}$. For a group of authorized vehicles $VG = \{id_1, id_2, \ldots, id_n\}$, this algorithm first constructs n

nodes in the form of $\{(x_i, y_i), i = 1, 2, \cdots, n\}$, where $x_i = \mathbb{H}_1(id_i)$ and $y_i = t^{\delta(\beta+\mathbb{H}_1(id_i))}$ in which $\delta \in \mathbb{Z}_q^*$ is randomly selected. The step length of the cubic spline interpolation is following considered, which is $h_i = x_{i+1} - x_i, (i = 1, 2, \cdots, n-1)$. Further substituting (x_i, y_i) and $h = \{h_1, h_2, \cdots, h_{n-1}\}$ into (4) and solve the matrix to obtain $m = \{m_1, m_2, \cdots, m_{n-1}\}$. Finally, the coefficients in (5) are calculated respectively as $a_i = y_i$, $b_i = \frac{y_{i+1}-y_i}{h_i} - \frac{h_i}{2} m_i - \frac{h_i}{6}(m_{i+1} - m_i)$, $c_i = \frac{m_i}{2}$ and $d_i = \frac{m_{i+1}-m_i}{6h_i}$, where $i = 1, 2, \cdots, n-1$. In this way, a re-encryption key $rk_{OID\to VG}$ is generated as

$$rk_{OID\to VG} = \langle \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3 \rangle$$
$$where \begin{cases} \mathrm{R}_1 = \begin{Bmatrix} a_1, b_1, c_1, d_1 \\ a_2, b_2, c_2, d_2 \\ \cdots \\ a_{n-1}, b_{n-1}, c_{n-1}, d_{n-1} \end{Bmatrix} \\ \mathrm{R}_2 = \mathbb{H}_2(v^\delta) \cdot t^\varepsilon \\ \mathrm{R}_3 = sk_{OID} \cdot u^{\frac{\varepsilon}{\mathbb{H}_1(OID)}} \end{cases} \tag{9}$$

- **ReEnc**$(MPK, rk_{OID\to VG}, C_{OID}) \to C_{OID\to VG}$ is employed to calculate the re-encrypted ciphertext based on $\mathrm{C} = (\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3)$ and $rk_{OID\to VG} = (\mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3)$.

$$C_{OID\to VG} = \langle \mathrm{C}'_1, \mathrm{C}'_2, \mathrm{C}'_3, \mathrm{C}'_4 \rangle$$
$$where \begin{cases} \mathrm{C}'_1 = \mathrm{R}_1 \\ \mathrm{C}'_2 = \mathrm{R}_2 \\ \mathrm{C}'_3 = \mathrm{C}_3 \\ \mathrm{C}'_4 = \mathrm{C}_2 \cdot e(\mathrm{R}_3, \mathrm{C}_1)^{-1} \end{cases} \tag{10}$$

- **Dec1**$(MPK, sk_{OID}, C_{OID}) \to M$ is used to implement the decryption of initial ciphertext.

$$M = \frac{C_2}{e(sk_{OID}, C_1)} \tag{11}$$

- **Dec2**$(MPK, id_i, sk_{id_i}, C_{OID\to VG}) \to M$ implements the decryption of re-encrypted ciphertext. Each vehicle id_i in the group VG is entitled to carry out this algorithm depending on the computable $x_i = \mathbb{H}_1(id_i)$ and $y_i = a_i + b_i(x - x_i) + c_i(x - x_i)^2 + d_i(x - x_i)^3$, where the coefficients a_i, b_i, c_i, d_i are available in R_1 which comes from $C_{OID\to VG} = \langle \mathrm{R}_1, \mathrm{R}_2, \mathrm{C}_3, \mathrm{C}_2 \cdot e(\mathrm{R}_3, \mathrm{C}_1)^{-1} \rangle$ in (10).

$$M = \mathrm{C}'_4 \cdot e\left(\mathrm{C}'_3, \frac{\mathrm{C}'_2}{\mathbb{H}_2\left(e(sk_{id_i}, y_i)\right)}\right) \tag{12}$$

C. PBFT-based Consensus Protocol

As noted in IV-A, a consensus protocol based on PBFT is applied to a blockchain system consisting of N EPSPs, of which a selected primary EPSP is the block producer. This section defines in detail the consensus process for sharing re-encryption packets via blockchain.

Definition 2 (**PBFT-based Consensus Protocol**). *For a time period t' of duration $\dot{T}'$, let $N^{t'} = \{1, 2, \ldots, N\}$ be the set of EPSPs in a blockchain system, $K^{t'} = \{1, 2, \ldots, K\}$ be the set of transactions in each EPSP, F be the maximum number of malicious EPSPs that the system is capable of tolerating and $EPSP_p$ be the primary EPSP (where $p \in N$). A fully developed PBFT-based consensus protocol includes five stages as follows.*

- **Request**: N EPSPs broadcast **Request** messages which primarily comprise their public-key signatures, message authentication codes (MACs), respective K transactions and corresponding message digest to the blockchain system via backhaul links between each other. Subsequently, $EPSP_p$ verifies the signature and MAC of each **Request** message. If all of the verifications are valid, these $N \cdot K$ transactions are generated into a block by $EPSP_p$.
- **Pre-prepare**: Primary $EPSP_p$ signs the new block and multicasts it to other EPSPs along with $N-1$ different **Pre-prepare** messages, where each **Pre-prepare** message mainly includes the ID of $EPSP_p$, a block signature, a block MAC, $N \cdot K$ signed intact transactions as well as digest messages. After receiving the **Pre-prepare** message, every EPSP except $EPSP_p$ verifies a total of $N \cdot K + 1$ signatures and $N \cdot K + 1$ MACs for one block and $N \cdot K$ transactions, respectively.
- **Prepare**: After $N-1$ other EPSPs have verified the new block, all EPSPs sign and send **Prepare** message to each other, which contains their message digests for $N \cdot K$ transactions. Then each of them is responsible for verifying the signatures and MACs of **Prepare** messages, further comparing the message digests between **Pre-prepare** message and **Prepare** message of the same EPSP until $2F$ consistent results are achieved.
- **Commit**: Each EPSP signs and sends a **Commit** message that includes $N \cdot K$ message digests to $N-1$ other EPSPs after it has reached $2F$ consistency results. Each recipient EPSP then validates the **Commit** messages and stops further validation when $2F$ **Commit** messages have been successfully validated. The completion of the above process means that the EPSP is consensus on the generation of the new block.
- **Reply**: Each EPSP signs the new consensus block and sends a **Reply** message to the primary $EPSP_p$ which contains $N \cdot K$ intact transactions and $N \cdot K$ digest message of each transaction. While $EPSP_p$ appends the new consensus block to the blockchain once it receives and verifies $2F$ **Reply** messages.

VI. Theoretical Analysis

A. Cost of Re-encryption System

In the proposed re-encryption system, the permission to generate the re-encryption secret key is delegated to EPSPs. For this reason, we assume that the processes that occur after the vehicles request the re-encryption packets (i.e. below the green arrows in Fig.2) lead to the cost of re-encryption system in a practical application scenario, which are the communication or computation costs of re-encryption key generation, re-encrypt operation and re-encrypted packets transmission. We ignore the decryption cost by vehicle because it does not affect the performance of the system.

Let Ξ_e be the CPU cycles required to perform an exponent operation in $\mathbb{G}$ or $\mathbb{G}_T$, $\{|\mathbb{G}|, |\mathbb{G}_\mathbb{T}|, |\mathbb{Z}|\}$ be the sizes of $\{\mathbb{G}, \mathbb{G}_\mathbb{T}, \mathbb{Z}_q^*\}$ respectively (in bits), and Ξ_p be the CPU cycles for operating a single bilinear pairing. As the execution of other mathematical operations takes far fewer CPU cycles than Ξ_e and Ξ_p, they are usually negligible. In addition, suppose that the data is requested by a vehicle in a group VG of n vehicles. The re-encryption cost $T_{V_j}^{RE}$ of a single request from V_j is expressed as

$$\begin{aligned} T_{V_j}^{RE} &= T_{cp}^{\textbf{ReKeyGen}} + T_{cm}^{re-key} + T_{cp}^{\textbf{ReEnc}} + T_{cm}^{re-ciphertext} \\ &= \frac{6\Xi_e}{f^{RSP}} + \frac{3\left|\mathbb{G}\right| + (n-1)\left|\mathbb{Z}\right|}{r_{R,E}} + \frac{\Xi_e + \Xi_p}{f_i^{EPSP}} \\ &+ \frac{3\left|\mathbb{G}\right| + \left|\mathbb{G}_{\mathbb{T}}\right| + (n-1)\left|\mathbb{Z}\right|}{r_{E_i,V_j}} \end{aligned} \tag{13}$$

where $r_{R,E}$ refers to the transmission rate from RSP to EPSPs, r_{E_i,V_j} is the transmission rate from an $EPSP_i(i \in N)$ to a vehicle $id_j(id_j \in VG)$, f^{RSP} and f^{EPSP_i} are the CPU frequencies of RSP and $EPSP_i$, respectively.

B. Cost of Blockchain System

To evaluate the cost resulting from sharing re-encryption packets via roadside EPSPs blockchain system, we assume that the CPU cycles for generating or verifying a signature, and generating or verifying a MAC are Γ and Θ [46]. In addition, suppose that the adopted message digest is implemented by Message-Digest Algorithm 5 (MD5) [47], which outputs a unique and irreversible 128-bit hash. As each of the five stages in Definition 2 incurs a communication cost for transferring the messages as well as a computation cost for verifying the signatures and MACs, the cost of PTFB-based consensus protocol is analysed as follows.

- **Request**: Based on Definition 2, it is assumed that every EPSP holds a certain number of transactions, denoted by K. When N EPSPs broadcasts their respective signed K transactions and K message digests, the total number of transactions to be packed into the block is $N \cdot K$. Thereby, the communication cost T_{cm}^{req} at this stage is expressed as

$$T_{cm}^{\text{req}} = \frac{\max_{i \in N, j \in K}(\mathcal{D}_{ij}) + \mathcal{D}_{digest}}{r^{EPSP}} \tag{14}$$

  where $\mathcal{D}_{ij}$ is the size of j^{th} transaction of $EPSP_i$, $\mathcal{D}_{digest}$ is the size of a message digest, and r^{EPSP} is the back-haul rate between EPSPs.
  Assume that the CPU frequency of $EPSP_p$ is f^{EPSP_p}. $EPSP_p$ is responsible for verifying $N \cdot K$ signatures and $N \cdot K$ MACs on the request messages from all EPSPs, including itself. Therefore, the computation cost T_{cp}^{req} caused by $EPSP_p$ verifying $N \cdot K$ transactions at the request stage is

$$T_{cp}^{\text{req}} = \frac{N \cdot K(\Gamma + \Theta)}{f^{EPSP_p}} \tag{15}$$

- **Pre-prepare**: The message to be transferred during the pre-prepare stage consists mainly of a new block integrating $N \cdot K$ transactions and their message digest. So that the communication cost T_{cm}^{pre} is denoted as

$$T_{cm}^{\text{pre}} = \frac{\sum_{\substack{1 \le i \le N \\ 1 \le j \le K}} \mathcal{D}_{ij} + N \cdot K \cdot \mathcal{D}_{digest}}{r^{EPSP}} \tag{16}$$

  The computation cost T_{cp}^{pre} of this stage is affected by two parts which are $EPSP_p$ signing block and each $EPSP_i(i \in N \cap i \neq p)$ verifying the block and transactions.

$$T_{cp}^{\text{pre}} = \frac{\Gamma + (N-1)\Theta}{f^{EPSP_p}} + \max_{i \in N \cap i \neq p} \left\{ \frac{(N \cdot K + 1)(\Gamma + \Theta)}{f^{EPSP_i}} \right\} \tag{17}$$

- **Prepare**: Different from traditional PTFB consensus scheme, the transactions shared in our blockchain system are re-encryption packets, which are inherently secure and cannot be decrypted by EPSPs. Therefore, it is sufficient for ensuring consistency of transactions in prepare stage to transmit and verify just the message digests instead of the full text of transaction. The communication cost T_{cm}^{prep} is expressed as

$$T_{cm}^{\text{prep}} = \frac{N \cdot K \cdot \mathcal{D}_{digest}}{r^{EPSP}} \tag{18}$$

  All EPSPs except $EPSP_p$ are required to generate a signature and $N-1$ MACs for the prepare message, then all EPSPs have to verify $2F$ prepare messages, which leads to the following computational cost

$$T_{cp}^{\text{prep}} = \max_{i \in N \cap i \neq p} \left\{ \frac{\Gamma + (N-1)\Theta}{f^{EPSP_i}} \right\} + \max_{i \in N} \left\{ \frac{2F(\Gamma + \Theta)}{f^{EPSP_i}} \right\} \tag{19}$$

- **Commit**: Due to EPSPs only broadcasting their authenticated message digests as stated in **Prepare** stage, accordingly, the communication cost of commit stage is $T_{cm}^{\text{com}} = T_{cm}^{\text{prep}}$. Besides, the maximum time consumption of each EPSP to generate a signature and $N-1$ MACs as well as verify $2F$ commit messages is considered to be the computation cost at this stage, which is represented as

$$T_{cp}^{\text{com}} = \max_{i \in N} \left\{ \frac{\Gamma + (N-1)\Theta + 2F(\Gamma + \Theta)}{f^{EPSP_i}} \right\} \tag{20}$$

- **Reply**: Since the reply message needs to transfer the same intact block content as **Pre-prepare** message, the communication cost of reply stage is $T_{cm}^{\text{rep}} = T_{cm}^{\text{pre}}$. Meanwhile, the computation cost T_{cp}^{rep} caused by $EPSP_i$ (where $i \in N \cap i \neq p$) signing the consensus block and $EPSP_p$ verifying $2F$ reply messages is

$$T_{cp}^{\text{rep}} = \max_{i \in N \cap i \neq p} \left\{ \frac{N \cdot K(\Gamma + \Theta)}{f^{EPSP_i}} \right\} + \frac{2F \cdot N \cdot K(\Gamma + \Theta)}{f^{EPSP_p}} \tag{21}$$

Therefore, the total cost of sharing the re-encryption packets through the blockchain system is

$$\begin{aligned} & T^{BC} = T_{cm}^{BC} + T_{cp}^{BC} \\ & where \left\{ \begin{array}{l} T_{cm}^{BC} = T_{cm}^{\text{req}} + T_{cm}^{\text{pre}} + T_{cm}^{\text{prep}} + T_{cm}^{\text{com}} + T_{cm}^{\text{rep}} \\ T_{cp}^{BC} = T_{cp}^{\text{req}} + T_{cp}^{\text{pre}} + T_{cp}^{\text{prep}} + T_{cp}^{\text{com}} + T_{cp}^{\text{rep}} \end{array} \right. \end{aligned} \tag{22}$$

C. Consistency Analysis

1) Consistency of Re-encryption: The consistency of suggested VIPPR scheme, cf. [10], entails that the owner of original data can correctly decrypt the initial ciphertext by using its private key. Meanwhile, each of the authorized receivers should also decrypt accurately the re-encryption packet generated by the appropriate encryption steps using their own private key, ultimately obtaining the original data. To be specific, consistency is illustrated by the following theorems.

Theorem 1. *For any properly executed algorithms **KeyGen** $(MSK, OID) \rightarrow sk_{OID}$ and **Enc** $(MPK, OID, M) \rightarrow C_{OID}$, the algorithm **Dec1**$(MPK, sk_{OID}, C_{OID}) \rightarrow M$ is consistently valid, i.e., **Dec1** always outputs the desired original data M.*

Proof. Given that $sk_{OID} = g^{\frac{1}{\beta+\mathbb{H}_1(OID)}}$ defined in equation (7) is the output of algorithm **KeyGen** while $C_{OID} = \langle \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3 \rangle$ defined in equation (8) is the output of algorithm **Enc**, where $\mathrm{C}_1 = t^{\gamma(\beta+\mathbb{H}_1(OID))}$, $\mathrm{C}_2 = v^{\gamma} \cdot M$. Since algorithm **Dec1**(MPK, sk_{OID}, C_{OID}) (where $MPK = (q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, v, t, t^{\beta}, u, u^{\beta}, \mathbb{H}_1, \mathbb{H}_2)$ is constructed in (4)) requires to calculate $\frac{C_2}{e(sk_{OID}, C_1)}$, we have $e(sk_{OID}, C_1) = e(g^{\frac{1}{\beta+\mathbb{H}_1(OID)}}, t^{\gamma(\beta+\mathbb{H}_1(OID))}) = e(g,t)^{\gamma} = v^{\gamma}$, hence $\frac{C_2}{e(sk_{OID}, C_1)} = \frac{v^{\gamma} \cdot M}{v^{\gamma}} = M$.

Above process proved that the algorithm **Dec1** can be executed to obtain the correct original data M. □

Theorem 2. *If $VG = \{id_1, id_2, \ldots, id_n\}$ is a group of authorized vehicles and $id_i \in VG$ represents any vehicle in VG, then the algorithm **Dec2**$(MPK, id_i, sk_{id_i}, C_{OID \rightarrow VG}) \rightarrow M$ is consistently valid once the algorithms **KeyGen**$(MSK, OID) \rightarrow sk_{OID}$, **KeyGen**$(MSK, id_i) \rightarrow sk_{id_i}$, **Enc**$(MPK, OID, M) \rightarrow C_{OID}$, **ReKeyGen**$(MPK, OID, sk_{OID}, VG) \rightarrow rk_{OID \rightarrow VG}$ and **ReEnc**$(MPK, rk_{OID \rightarrow VG}, C_{OID}) \rightarrow C_{OID \rightarrow VG}$ are executed properly in sequence, i.e., algorithm **Dec2** always outputs the desired original data M.*

Proof. We are given that $sk_{OID} = g^{\frac{1}{\beta+\mathbb{H}_1(OID)}}$ and $sk_{id_i} = g^{\frac{1}{\beta+\mathbb{H}_1(id_i)}}$ are the private keys that the PKG generates for data owner OID and authorized vehicle id_i respectively by performing the algorithm **KeyGen**. Besides, $C_{OID} = \langle \mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3 \rangle$ defined in equation (8) is the output of algorithm **Enc** (where $\mathrm{C}_1 = t^{\gamma(\beta+\mathbb{H}_1(OID))}$, $\mathrm{C}_2 = v^{\gamma} \cdot M$ and $\mathrm{C}_3 = u^{\gamma\left[\frac{\beta+\mathbb{H}_1(OID)}{\mathbb{H}_1(OID)}\right]}$), $rk_{OID \rightarrow VG} = \langle \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3 \rangle$ defined in equation (9) is the output of algorithm **ReKeyGen** (where $\mathrm{R}_2 = \mathbb{H}_2(v^{\delta}) \cdot t^{\varepsilon}$ and $\mathrm{R}_3 = sk_{OID} \cdot u^{\frac{\varepsilon}{\mathbb{H}_1(OID)}}$), $C_{OID \rightarrow VG} = \langle \mathrm{C}_1', \mathrm{C}_2', \mathrm{C}_3', \mathrm{C}_4' \rangle$ defined in equation (10) is the output of algorithm **ReEnc** (where $\mathrm{C}_2' = \mathrm{R}_2$, $\mathrm{C}_3' = \mathrm{C}_3$ and $\mathrm{C}_4' = \mathrm{C}_2 \cdot e(\mathrm{R}_3, \mathrm{C}_1)^{-1}$). Since **Dec2**$(MPK, id_i, sk_{id_i}, C_{OID \rightarrow VG}) \rightarrow M$ (where $MPK = (q, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, e, v, t, t^{\beta}, u, u^{\beta}, \mathbb{H}_1, \mathbb{H}_2)$ is constructed in (4)) requires to calculate $\mathrm{C}_4' \cdot e\left(\mathrm{C}_3', \frac{\mathrm{C}_2'}{\mathbb{H}_2(e(sk_{id_i}, y_i))}\right)$, we have

$$
\begin{aligned}
\mathrm{C}_4' &= \mathrm{C}_2 \cdot e(\mathrm{R}_3, \mathrm{C}_1)^{-1} = v^{\gamma} \cdot M \cdot e(sk_{OID} \cdot u^{\frac{\varepsilon}{\mathbb{H}_1(OID)}}, \mathrm{C}_1)^{-1} \\
&= v^{\gamma} \cdot M \cdot e(sk_{OID}, \mathrm{C}_1)^{-1} \cdot e(u^{\frac{\varepsilon}{\mathbb{H}_1(OID)}}, \mathrm{C}_1)^{-1} \\
&= v^{\gamma} \cdot M \cdot v^{-\gamma} \cdot e(u^{\frac{\varepsilon}{\mathbb{H}_1(OID)}}, t^{\gamma(\beta+\mathbb{H}_1(OID))})^{-1} \\
&= M \cdot e(u,t)^{-\frac{\varepsilon\gamma(\beta+\mathbb{H}_1(OID))}{\mathbb{H}_1(OID)}}
\end{aligned}
$$

Furthermore, given that $y_i = t^{\delta(\beta+\mathbb{H}_1(id_i))}$ where $id_i \in VG$,

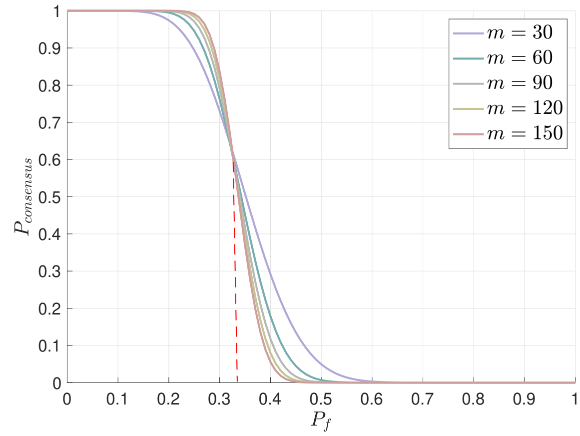


Fig. 3. Analytical result of FPD model.

we have

$$
\begin{aligned}
\frac{\mathrm{C}_2'}{\mathbb{H}_2(e(sk_{id_i}, y_i))} &= \frac{\mathbb{H}_2(v^{\delta}) \cdot t^{\varepsilon}}{\mathbb{H}_2\left(e(g^{\frac{1}{\beta+\mathbb{H}_1(id_i)}}, t^{\delta(\beta+\mathbb{H}_1(id_i))})\right)} \\
&= \mathbb{H}_2(v^{\delta}) \cdot t^{\varepsilon} / \mathbb{H}_2(v^{\delta}) = t^{\varepsilon}
\end{aligned}
$$

Therefore, we obtain

$$
\begin{aligned}
\mathrm{C}_4' \cdot e\left(\mathrm{C}_3', \frac{\mathrm{C}_2'}{\mathbb{H}_2(e(sk_{id_i}, y_i))}\right) &= \mathrm{C}_4' \cdot e\left(u^{\gamma\left[\frac{\beta+\mathbb{H}_1(OID)}{\mathbb{H}_1(OID)}\right]}, t^{\varepsilon}\right) \\
&= M \cdot e(u,t)^{-\frac{\varepsilon\gamma(\beta+\mathbb{H}_1(OID))}{\mathbb{H}_1(OID)}} \cdot e(u,t)^{\frac{\varepsilon\gamma(\beta+\mathbb{H}_1(OID))}{\mathbb{H}_1(OID)}} = M
\end{aligned}
$$

Consequently, we proved that the algorithm **Dec2** can be executed to obtain the correct original data M. □

2) Consistency of PBFT-based blockchain : In this study, we employed a classic PBFT consensus as a benchmark, where re-encrypted ciphertexts are recorded in the roadside blockchain, validated by the EPSPs consensus committee, and supervised by other entities. As we were only lightweight the signature and ciphertext, the proposed blockchain system is considered to inherit the safety and trust advantages of PBFT consensus, which can tolerate no more than $(N-1)/3$ faulty nodes.

Theorem 3. *In PBFT-based blockchain system with N EPSPs, the security threshold for achieving consistency is $\frac{m}{3}$ (where $m = N - 1$).*

Proof. To evaluate the consistency performance of the PBFT consensus mechanism across various blockchain systems, we adopt the faulty probability determined (FPD) model [45]. By assuming that all EPSPs except $EPSP_p$ are independent and possess an identical failure probability P_f, the consensus success rate of the system ($P_{consensus}$) can be expressed as

$$P_{consensus} = \sum_{i=0}^{\frac{m}{3}} C_m^i (1-P_f)^{m-1} {P_f}^i \tag{23}$$

As illustrated in Fig.3, the $P_{consensus}$ curve exhibits a sharp increase in slope as the system scale increases, particularly near the $P_f = \frac{1}{3}$ point. This trend suggests that the faulty tolerance of PBFT approaches $\frac{1}{3}$ as the number of EPSPs (or equivalently, the size of the system) grows infinitely large. Therefore, we can conclude that the proposed consensus mechanism achieves faulty tolerance convergence at $\frac{1}{3}$ in an infinite system scale. In other words, the system achieves a 100 percent consensus success rate when the maximum number of tolerable faulty nodes is $\frac{m}{3}$. $\square$

D. Security and Privacy Analysis

1) Security of data: We refer to the notions in [10], [17] to illustrate that the re-encrypted ciphertexts are secure against chosen plaintext attacks (CPA) by describing a game of interaction between challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

- Initialization. Adversary $\mathcal{A}$ chooses an id^* as the challenge vehicle identity and sends id^* to challenger $\mathcal{C}$.
- Setup. $\mathcal{C}$ runs **Setup**$(\alpha) \rightarrow (MPK, MSK)$ algorithm and transfers the system public key MPK to $\mathcal{A}$.
- Phase 1. Adversary $\mathcal{A}$ is permitted to query for the private key of id^* and a re-encryption key that corresponds to a group of vehicle identities VG.
  - If $OID \neq id^*$, $\mathcal{A}$ is able to conduct private key query $\mathcal{Q}^{SK}(OID)$ for data owner O . Challenger $\mathcal{C}$ runs **KeyGen**$(MSK, OID) \rightarrow sk_{OID}$ algorithm and transfers the private key sk_{OID} to $\mathcal{A}$.
  - If $OID = id^*$, $\mathcal{A}$ can conduct re-encryption key query $\mathcal{Q}^{RK}(OID, VG)$ and cannot query $\mathcal{Q}^{RK}(OID, id')$ and $\mathcal{Q}^{SK}(id')$ at the same time for any $id' \in VG$. Challenger $\mathcal{C}$ runs **KeyGen**$(MSK, OID) \rightarrow sk_{OID}$ algorithm followed by **ReKeyGen**$(MPK, OID, sk_{OID}, VG) \rightarrow rk_{OID\rightarrow VG}$ algorithm, then sends the re-encryption key $rk_{OID\rightarrow VG}$ to $\mathcal{A}$.
- Challenge. Adversary $\mathcal{A}$ delivers two challenge data M_0 and M_1 to challenger $\mathcal{C}$. $\mathcal{C}$ runs **Enc**$(MPK, id^*, M_b) \rightarrow C^*$ algorithm to generate a challenge ciphertext C^*, where $b \in \{0, 1\}$ is a randomly chosen coin. After that, C^* is passed back to $\mathcal{A}$.
- Phase 2. Perform the same queries as in Phase 1.
- Guess. Adversary $\mathcal{A}$ develops a guess $b' \in \{0, 1\}$. $\mathcal{A}$ wins if $b' = b$ with $Adv^{\mathcal{A}}_{VIPPR} = \left|Pr\left[b' = b\right] - \frac{1}{2}\right|$ as the advantage to win the game.

Assuming that adversary $\mathcal{A}$ has the advantage to break VIPPR in the selective security model. The security of the proposed VIPPR scheme relies on the CPA security of IBB [48] and P2B [10] schemes. Since it is proofed in [10], the P2B scheme is CPA secure in the random oracle (RO) model under the IBB secure assumption [48], where the hash function is assumed to be completely random, both $Adv^{\mathcal{A}}_{IBB}$ and $Adv^{\mathcal{A}}_{P2B}$ are negligible. Therefore, $Adv^{\mathcal{A}}_{VIPPR}$ is also negligible, which indicates that the proposed VIPPR is secure against CPA secure.

2) Privacy of receivers: The privacy of vehicle receivers in our scheme is proved through the following theorem.

Theorem 4. *In VIPPR, neither the EPSPs nor the members of the group VG have access to the identity id_i of a receiver vehicle i, where $i \in VG$.*

Proof. RSP runs **ReKeyGen** algorithm to generate re-encryption key $rk_{OID\rightarrow VG} = \langle \mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3 \rangle$ for a data owner with identity OID, where $VG = \{id_1, id_2, \ldots, id_n\}$, $\mathrm{R}_1, \mathrm{R}_2, \mathrm{R}_3$ are detailed display in (9). In particular, the coefficients a_i, b_i, c_i, d_i of the cubic spline $y_i = a_i + b_i(x - x_i) + c_i(x - x_i)^2 + d_i(x - x_i)^3$ are available in R_1. **ReKeyGen** calculates $x_i = \mathbb{H}_1(id_i)$ and $y_i = t^{\delta(\beta + \mathbb{H}_1(id_i))}$ for each $id_i \in VG$.

EPSPs run **ReEnc** algorithm to produce re-encrypted ciphertext $C_{OID\rightarrow VG} = \langle \mathrm{C}'_1, \mathrm{C}'_2, \mathrm{C}'_3, \mathrm{C}'_4 \rangle$, where $\mathrm{C}'_1, \mathrm{C}'_2, \mathrm{C}'_3, \mathrm{C}'_4$ are detailed display in (10).

Receiver i with identity id_i operates **Dec2** to achieve plaintext $M = \mathrm{C}'_4 \cdot e\left(\mathrm{C}'_3, \frac{\mathrm{C}'_2}{\mathbb{H}_2\left(e(sk_{id_i}, y_i)\right)}\right)$. In practical terms, Receiver i can obtain $x_i = \mathbb{H}_1(id_i)$ and sk_{id_i}. Then, because of $id_i \in VG$, the related y_i is available from R_1 which comes from $C_{OID\rightarrow VG}$. Finally, the ciphertext is decrypted based on the above statements.

If receiver i is curious about whether a vehicle with identity id_j belongs to the same group VG as itself, $x_j = \mathbb{H}_1(id_j)$ and corresponding cubic spline curve $y_j = a_j + b_j(x - x_j) + c_j(x - x_j)^2 + d_j(x - x_j)^3$ according to $C_{OID\rightarrow VG}$ must be obtained. Obviously, it is not achievable. Furthermore, receiver i does not know the private key sk_{id_j} of receiver j and thus cannot perform an exact bilinear pairing operation. In other words, receiver i is unable to find out whether there are any other receivers in the group VG, which proves the effectiveness of the proposed VIPPR scheme with respect to the privacy of the receiver's identity. $\square$

VII. Performance Evaluation

A. Performance Analysis of Re-encryption system

We summarize the computation and communication costs brought by supporting the function of VIPPR and other identity based broadcast re-encryption schemes (i.e., Xu15 [17], Huang18 [18], and Maiti20 [10]) in Table I.

Firstly, regarding the computation cost, we make a comparison of computation overheads of our proposal with those of Xu15, Huang18 and Maiti20 for the three algorithms **ReKeyGen**, **ReEnc** and **Dec2**. The proposed VIPPR scheme inherits the computational cost advantage of the Maiti20 scheme in its **ReEnc** and **Dec2** algorithms, which amounts to $\Xi_e + 2\Xi_p$. Consequently, the computational cost required for the receiver to decrypt data packets encrypted by the **ReEnc** algorithm by running **Dec2** is lower than that of the Xu15 and Huang18 schemes. In particular, the computation overhead of **ReKeyGen** algorithm in VIPPR is significantly reduced from that of Maiti20, as it eliminates the n exponent operations in the re-encryption key generation phase. Besides, in cases where the size of a vehicle group is more than 4 (this condition is generally satisfied in practical application scenarios), our scheme provides better computational performance than any other scheme. Secondly, regarding the communication cost, we analyze the sizes of original ciphertext, re-encryption key and re-encrypted ciphertext of the above schemes. Just like Maiti20, we do not specify the scale of the receiver in the initial encryption phase **Enc**, so accordingly, the original ciphertext size of VIPPR is smaller than that of Xu15 and Huang18. Meanwhile, the sizes of re-encryption keys in Huang18 and VIPPR ($n\,|\mathbb{G}|$ and $3\,|\mathbb{G}| + (n-1)\,|\mathbb{Z}|$, respectively) are typically larger than their counterparts in Xu15 and Maiti20 due to their dependence on the scale

TABLE I
COMPARISON OF COMMUNICATION AND COMPUTATION COSTS

Schemes	Computation Cost (in CPU cycles)			Communication Cost (in bits)		
	ReKeyGen	**ReEnc**	**Dec2**	Original ciphertext size	Re-encryption key size	Re-encrypted ciphertext size
Xu15 [17]	$(n+2)\Xi_e$	$(n+1)\Xi_e+2\Xi_p$	$(n+2)\Xi_e+3\Xi_p$	$3\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert$	$4\lvert\mathbb{G}\rvert$	$4\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert$
Huang18 [18]	$(n+8)\Xi_e+\Xi_p$	$(n+3)\Xi_e+\Xi_p$	$3\Xi_e+2\Xi_p$	$(n+2)\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert+\lvert\mathbb{Z}\rvert$	$n\lvert\mathbb{G}\rvert$	$4\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert$
Maiti20 [10]	$(n+6)\Xi_e$	$\Xi_e+\Xi_p$	Ξ_e+2Tp	$2\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert$	$3\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert+\lvert\mathbb{Z}\rvert$	$3\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert+\lvert\mathbb{Z}\rvert$
VIPPR	$6\Xi_e$	$\Xi_e+\Xi_p$	$\Xi_e+2\Xi_p$	$2\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert$	$3\lvert\mathbb{G}\rvert+(n-1)\lvert\mathbb{Z}\rvert$	$3\lvert\mathbb{G}\rvert+\lvert\mathbb{G}_{\mathbb{T}}\rvert+(n-1)\lvert\mathbb{Z}\rvert$

of receiving vehicle group. In addition, VIPPR and Maiti20 provide independently decryptable re-encrypted ciphertexts for a group of vehicles, resulting in larger communication costs. Furthermore, compared with the other three schemes, the proposed VIPPR produces the largest re-encrypted ciphertext.

It is not negligible that the EPSPs deployed on the roadside in practical scenarios usually hold heterogeneous communication and computational capabilities, therefore we will investigate the integration cost for computation and communication of the above schemes with numerical simulations.

B. Scalability Analysis

1) Response time: Response time refers to the duration that elapses between the time a request is generated and the moment the system responds with a result. If the response time of the blockchain system increases concurrently with the number of EPSPs, it is possible that the scalability of system may be compromised. Therefore, optimizing the response time of the blockchain system is crucial to promote its scalability and ability to handle a growing workload. The reduced response time $\triangle T$ of our aforementioned solution compared to traditional encryption based blockchain system is calculated as follows.

$$\triangle T = \overline{T^{BC}}_{\{\text{Enc}\}} - \overline{T^{BC}}_{\{\text{VIPPR}\}} \tag{24}$$

where $T^{BC}_{\{\text{Enc}\}}$ and $T^{BC}_{\{\text{VIPPR}\}}$ represent the response times of blockchain systems for sharing original encrypted ciphertext and re-encrypted ciphertext generated by the VIPPR scheme, respectively. The values of $\overline{T^{BC}}_{\{\text{Enc}\}}$ and $\overline{T^{BC}}_{\{\text{VIPPR}\}}$ are averages calculated based on different ciphertext sizes. Notably, the computation of $T^{BC}_{\{\text{Enc}\}}$ is based on the approach presented in [46], while $T^{BC}_{\{\text{VIPPR}\}}$ is equivalent to T^{BC} which is provided in (22). The results in Table II show that as the number (i.e. N) of EPSPs participating in consensus increases, the value of $\triangle T$ consistently rises. This finding suggests the proposed solution's effectiveness in improving the blockchain system's scalability.

2) Throughput: Throughput is used to evaluate the capacity of a blockchain system to process transactions within a specific duration. Typically, a system is considered well scalable if its throughput increases proportionally to the growing number of vehicles and EPSPs. Assuming that N EPSPs in a blockchain system are all holding K ciphertexts as transactions, where the ciphertexts are generated for a group of vehicles of size n, the throughput of traditional blockchain and VIPPR-based blockchain systems are respectively represented as

$$TPS_{\{\text{VIPPR}\}} = \frac{N \cdot K \cdot (3\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_{\mathbb{T}}\rvert + (n-1)\lvert\mathbb{Z}\rvert)}{T^{BC}_{\{\text{VIPPR}\}}} \tag{25}$$

$$TPS_{\{\text{Enc}\}} = \frac{N \cdot K \cdot (2\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_{\mathbb{T}}\rvert)}{T^{BC}_{\{\text{Enc}\}}} \tag{26}$$

Fig.4 depicts the advantages of our proposed solution in terms of system throughput. Firstly, as demonstrated by the curved surface in the upper half of the figure, it is evident that the VIPPR-based blockchain system's throughput tends to increase more significantly as the number of vehicles increases. Secondly, although both two systems experience a decrease in throughput as the number of EPSPs increases, our proposed VIPPR-based blockchain system consistently achieves a greater throughput compared to the traditional encryption based blockchain system.

TABLE II
THE RESPONSE TIME OF SYSTEMS UNDER DIFFERENT BLOCKCHAIN DIMENSIONS

	$\overline{T^{BC}}_{\{\text{Enc}\}}$ [s]	$\overline{T^{BC}}_{\{\text{VIPPR}\}}$ [s]	$\triangle T$ [ms]
$N = 10$	38.81	38.63	**175.85**
$N = 40$	327.77	327.01	**762.03**
$N = 70$	874.55	873.20	**1348.21**
$N = 100$	1679.14	1677.21	**1934.39**

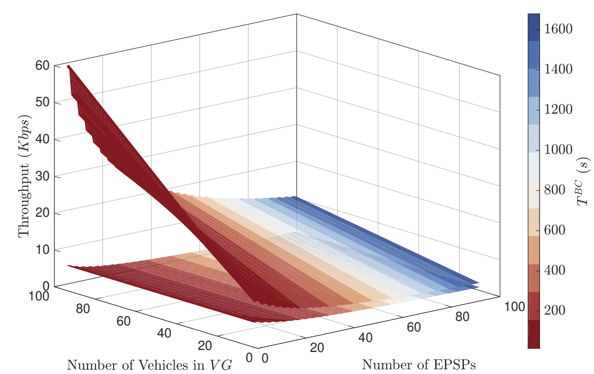
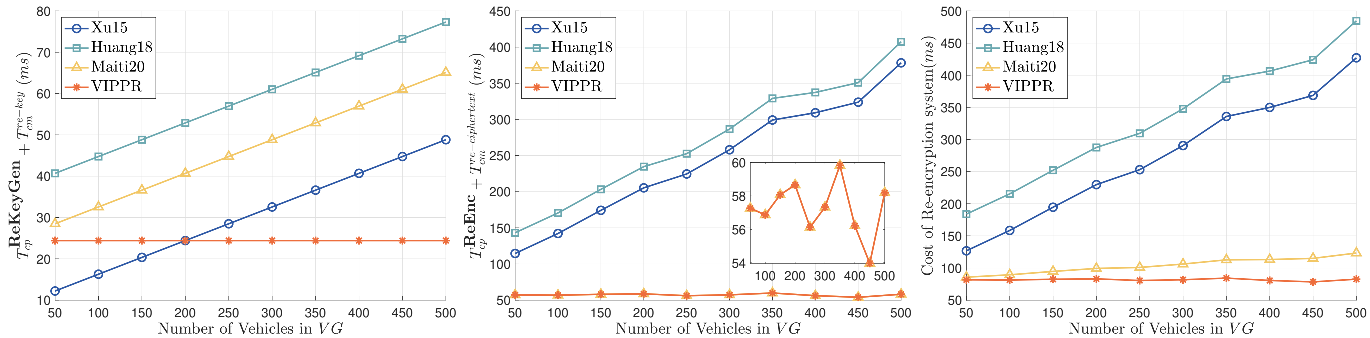


Fig. 4. Response time and throughput evaluation.



(a) $T_{cp}^{\textbf{ReKeyGen}} + T_{cm}^{re-key}$ (b) $T_{cp}^{\textbf{ReEnc}} + T_{cm}^{re-ciphertext}$ (c) Cost of Re-encryption system

Fig. 5. The cost of re-encryption system under different numbers of vehicle in a group VG in (19). a) Computation cost of **ReKeyGen** algorithm and communication cost of transferring re-key from RA to an EPSP; b) Computation cost of **ReEnc** algorithm and communication cost of transferring re-ciphertext from an EPSP to a requesting vehicle; c) The integration cost of re-encryption system.

C. Numerical Simulations

In this section, we first compare the integration cost of re-encryption system with the three methods mentioned in VII-A. In order to contrast and analyse, it is assumed that a 160-bit prime-order bilinear group based on the elliptic curve over a 512-bit finite field is adopted in re-encryption system [18]. The proposed consensus mechanism is then implemented between the roadside EPSPs on the basis of re-encryption system to further compare the time consumption of blockchain systems under various re-encryption methods. In addition, simulations in two scenarios are conducted with ns-3 simulators [49] and Simulation of Urban MObility (SUMO) [50] to verify the efficiency of the proposed scheme. Without specification, the parameters of system configuration are shown in Table III.

TABLE III
SIMULATION PARAMETERS [18], [46]

Parameter	**Value**
Simulation area in scenarios	$30m \times 1500m$,$1500m \times 1500m$
Simulation time in scenarios	100 s, 330 s
Mobility of vehicles in scenarios	20 m/s, Trace with 0 $\sim$ 20 m/s
Number and Position of EPSPs	5, arranged equidistantly in a line
Transmission power of EPSPs	20 dBm
Data size of M	512 bytes $\sim$ 2048 bytes
Wireless protocol	802.11p
Propagation loss model	TwoRayGroundPropagation
PhyMode	OfdmRate6MbpsBW10MHz
Routing protocol	AODV
Size of autherized vehicle group n	100
Size of message digest D_{digest}	16 bytes
Transmission rate $r_{R,E}$	1 Gbps
CPU frequency f^{RSP}	2.4 GHz
CPU frequency f^{EPSP_i}	1 GHz
CPU cycles for $\{\Xi_e, \Xi_p, \Gamma, \Theta\}$	$\{10, 10, 1, 10\}$ Mcycles
Size of $\{\mathbb{G}, \mathbb{G}_{\mathbb{T}}, \mathbb{Z}_q^*\}$	$\{512, 512, 160\}$ bits

In the first comparison, the CPU frequency f^{EPSP_i} of an $EPSP_i$ is chosen randomly between 0.1GHZ and 1GHZ, and the transmission rate r_{E_i,V_j} from $EPSP_i$ to a request vehicle V_j is randomly chosen between 1Mbps and 10Mbps, to demonstrate the heterogeneity of the computation and communication capabilities of EPSPs, respectively. After repeating the simulation 1000 times, the average numerical results are given in Fig.5. In particular, Fig.5(a) shows the cost of RA to generate as well as transmit a re-key for the group of vehicles VG, which consists of the time consumption by Executing **ReKeyGen** and the latency of forwarding the re-encryption key. As can be seen from the figure, the proposed VIPPR differs from the comparison algorithms in that it maintains a constant consumption around 10ms at this phase and outperforms both schemes Huang18 and Maiti20. In addition, it provides better performance than Xu15 when the size of receiving vehicle group is over 200. Fig.5(b) displays the cost of an EPSP to re-encrypt an initial cipher and broadcast its corresponding result, including the time consumption to implement **ReEnc** and the latency to forward the re-ciphertext to a requesting vehicle. The cost of VIPPR at this phase stays between 54ms and 60ms, which is roughly the same as Maiti20 and significantly less than the cost of Xu15 and Huang18 approaches at this phase. Fig.5(c) shows the integration cost of re-encryption system which is detailed stated in VI-A. It can be seen from the figure that the integrated performance of VIPPR for generating re-encryption packets for a group of vehicles is superior to that of existing schemes. Significantly, VIPPR improves the approach to generating a group of re-encryption keys on the basis of Maiti20, which reduces the **ReKeyGen** algorithm execution time by compromising the size of re-ciphertext, thereby realizing a decrease in the integration cost of re-encryption system in MEC-empowered VANET. Besides, the integration cost of VIPPR is minimally affected by the growing size of the vehicles group, which grants it an advantage in terms of system stability. We further implement a roadside blockchain system among five heterogeneity EPSPs, where the PBFT-based consensus is accordingly able to accommodate no more than one faulty EPSP. Fig.6(a) displays the costs of the blockchain system for the above comparison algorithms for increasing sizes of vehicle groups, with 1000 simulations in average. Disregarding the outliers in Fig.6(a), the median costs of the blockchain system incurred by executing four comparison schemes are

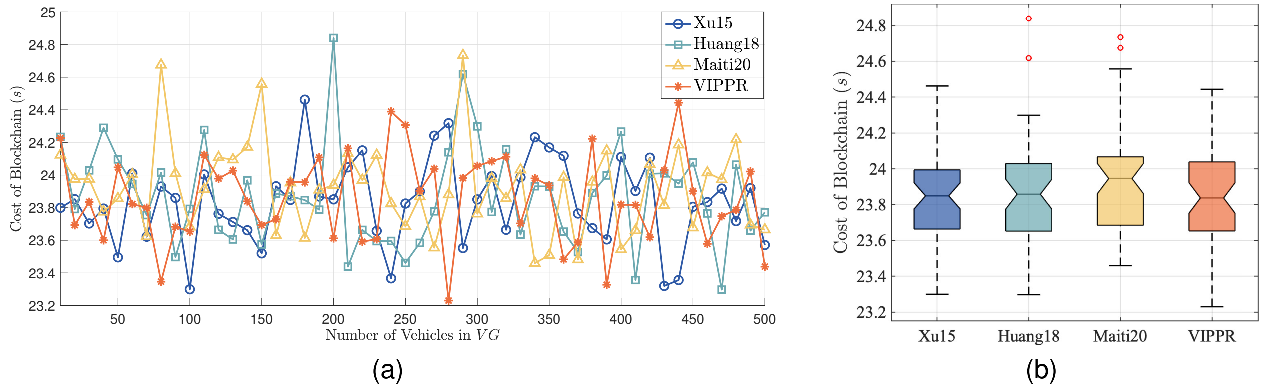


Fig. 6. The cost of PBFT-based blockchain system under different numbers of vehicle in a group VG in (22).

illustrated in Fig.6(b). Obviously, all medians fall between 23.8s and 24s, which indicates that sharing the re-encrypted packets generated by Xu15, Huang18, Maiti20 and VIPPR in the roadside blockchain results in approximately equal system cost, which is taken into account simplistically as block generation time in our simulations. The finding provides evidence to support the further assumption in our simulation of practical scenarios. Without loss of generality, we employ $T^{BC} = 24s$ in our subsequent implements.

To evaluate the effects of implementing the proposed security and privacy operations on network performance, particularly on average end-to-end delay, throughput, and packet delivery ratio, we conducted simulations in two scenarios. In **scenario 1**, vehicles are distributed with different densities and travelling at constant speed on a $30m \times 1500m$ range highway, where 10% of the vehicles in a same group send requests for original ciphertext simultaneously. And **scenario 2** is an urban scenario corresponding to a square area of size $1500m \times 1500m$ with the traffic information generated by SUMO. Other simulation parameters are given in Table III.

There are four comparison experiments conducted in **scenario 1** as shown in Fig.7. The first experiment involved a VANET system that utilized the basic encryption scheme (cf. the encryption algorithm in [10]). The second experiment employed identity-based proxy re-encryption (IBPRE), as explained in [17]. The third experiment deployed our proposed VIPPR scheme in the VANET system. Finally, a MEC-empowered VANET system with VIPPR deployed was implemented. We subsequently discuss the performance of the network in different configurations of VANETs. Fig.7(a) provides the average end-to-end delay of network under different simulations with the increase of vehicle density. In an encryption or IBPRE-based VANET, when all vehicles attempt to access the data, they are required to send their requests individually to the EPSP. Consequently, this process leads to a significant increase in communication overhead. Conversely, by employing the VIPPR scheme, the VANET system allows data sharing between vehicles within the same group, extending beyond the scope of the evaluated system. This approach ensures security and privacy while excluding the consideration of interaction delays between vehicles during the evaluation. As can be seen from the figure, the third experiment demonstrates the lowest average end-to-end delay, with a maximum of no more than 15ms. The fourth experiment takes it a step further than VIPPR by achieving trusted sharing of re-encryption packets between roadside EPSPs, utilizing the PBFT consensus based of blockchain. Due to the blockchain system's design, the MEC-empowered VANET enables requesting vehicles to access their desired

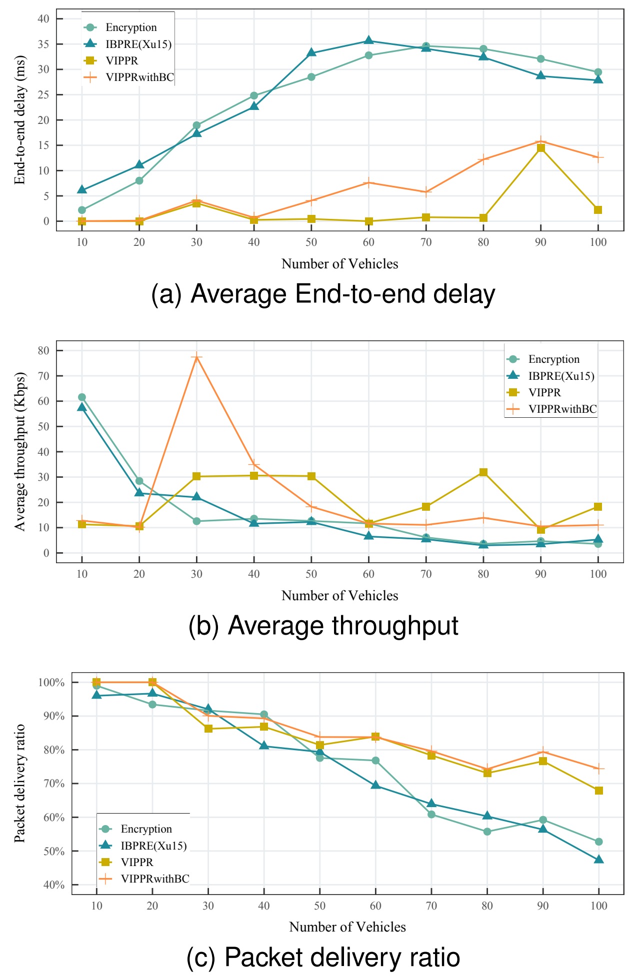


Fig. 7. Network performance in highway simulation area with different vehicle densities, where 10% of the vehicles in a same group send requests for original ciphertext simultaneously.

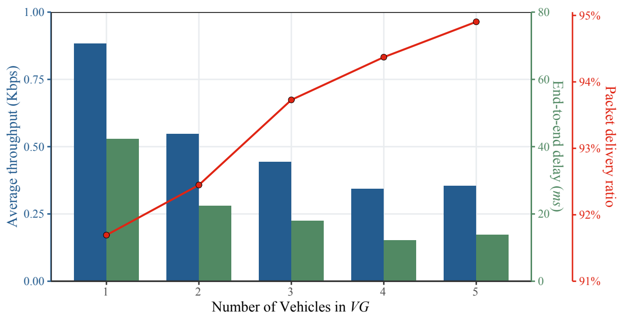


Fig. 8. Network performance in urban scenario.

data (which undergoed re-encryption) at any EPSP within the preset system. However, it also leads to an inevitable increase in the average end-to-end delay as the number of requests rises, as illustrated by the orange curve in Fig.7(a). Expanding the previous analysis, Fig.7(b) displays the average throughputs in different experiments. The maximum average throughputs for the four VANET systems exhibit 61.57 Kbps, 57.31 Kbps, 31.97 Kbps and 77.46 Kbps respectively, which indicates that the VANET system deployed with the VIPPR scheme features the most excellent parallel processing capacity. Fig.7(c) shows the packet delivery ratios in different experiments. It is obvious that MEC-empowered VANET system with VIPPR deployed (i.e., VIPPRwithBC) has almost always kept the highest packet delivery ratio at different vehicle densities. By averaging the results of multiple simulations, we can draw the following conclusions: Joint deployment of a VIPPR-based re-encryption system and a roadside PBFT-based blockchain system ensures the maximisation of network performance.

In conclusion, we deploy our proposed comprehensive security and privacy protection scheme in a real-world city-traffic environment involving 28 vehicles in **scenario 2**. In this simulation, the size of the authorized vehicle group, denoted by n, ranges from 1 to 5. Specifically, there are 28, 14, 10, 7, and 5 vehicle groups in the network, resulting in corresponding re-encryption packet sizes of 2048 bits, 2208 bits, 2368 bits, 2528 bits, and 2688 bits, respectively, generated by VIPPR. Assuming each group randomly picks a vehicle to request data, the corresponding network performances are shown in Fig.8. It can be observed from the figure that, with the expansion of the group size in VIPPR encryption scheme, the end-to-end delay and average throughput of VANET reduce in general, while the packet delivery ratio is completely on a rising trend to 94.91%. Of course, the primary reason for this result is that the number of requests is gradually decreasing. However, when $n = 4$, the simulation produces the lowest end-to-end delay of 12.13ms. This leads to the following inspiration: the authorized group size of proposed scheme cannot be increased arbitrarily in practice, it needs to match the scale of the network. For example, in this scenario, if the end-to-end delay is the main optimisation target, the size of authorized vehicles group in VIPPR should be set to $n = 4$.

VIII. Conclusions

This paper presents an efficient and trustworthy approach to ensure the security of data sharing and the privacy protection of vehicle identities in MEC-empowered VANTEs. The proposed scheme combines the security and privacy features of a novel privacy-preserving proxy re-encryption with the trust advantages of a blockchain based on PBFT consensus. Our VIPPR re-encryption scheme is demonstrated to consistently outperform comparable schemes in terms of communication and computation costs in VANET simulation scenarios. Although the re-encryption and consensus operations result in non-negligible latency, the proposed integrated scheme still achieves significant improvements in average end-to-end delay, average throughput, and packet delivery ratio compared to traditional re-encryption schemes applied independently to VANETs. In future work, we aim to achieve secure and sustainable data sharing in more complex VANET scenarios, such as when vehicles belong to multiple groups and simultaneously request edge servers to generate re-encrypted ciphertext for different groups. Additionally, we intend to investigate the potential applications of quantum technology in our proposed schemes.

References

[1] L. Chen, Y. Li, C. Huang, B. Li, Y. Xing, D. Tian, L. Li, Z. Hu, X. Na, Z. Li, S. Teng, C. Lv, J. Wang, D. Cao, N. Zheng, and F.-Y. Wang, "Milestones in autonomous driving and intelligent vehicles: Survey of surveys," *IEEE Trans. Intell. Veh.*, pp. 1–13, 2022.

[2] L. Chen, Y. Zhang, B. Tian, Y. Ai, D. Cao, and F.-Y. Wang, "Parallel driving os: A ubiquitous operating system for autonomous driving in cpss," *IEEE Trans. Intell. Veh.*, vol. 7, no. 4, pp. 886–895, 2022.

[3] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C.-H. Hsu, "Efficient and secure routing protocol based on artificial intelligence algorithms with uav-assisted for vehicular ad hoc networks in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4757–4769, 2021.

[4] N. Lyamin, D. Kleyko, Q. Delooz, and A. Vinel, "Ai-based malicious network traffic detection in vanets," *IEEE Netw.*, vol. 32, no. 6, pp. 15–21, 2018.

[5] S. Chen, J. Hu, Y. Shi, L. Zhao, and W. Li, "A vision of c-v2x: Technologies, field testing, and challenges with chinese development," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3872–3881, 2020.

[6] E. Jayatunga, A. Nag, and A. D. Jurcut, "Security requirements for vehicle-to-everything (v2x) communications integrated with blockchain," in *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)*. IEEE, 2022, pp. 208–213.

[7] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (v2x) communication platforms," *IEEE Trans. Intell. Veh.*, vol. 5, no. 4, pp. 693–713, 2020.

[8] S. Jiang, J. Liu, L. Wang, Y. Zhou, and Y. Fang, "Esac: An efficient and secure access control scheme in vehicular named data networking," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 10 252–10 263, 2020.

[9] Y. Liu, D. He, Z. Bao, H. Wang, M. K. Khan, and K.-K. R. Choo, "An efficient multilayered linkable ring signature scheme with logarithmic size for anonymous payment in vehicle-to-grid networks," *IEEE Trans. Intell. Veh.*, 2022, doi: 10.1109/TIV.2022.3216949.

[10] S. Maiti and S. Misra, "P2b: Privacy preserving identity-based broadcast proxy re-encryption," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5610–5617, 2020.

[11] S. Chen, J. Hu, Y. Shi, and L. Zhao, "Lte-v: A td-lte-based v2x solution for future vehicular network," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 997–1005, 2016.

[12] H. El-Sayed, H. Alexander, P. Kulkarni, M. A. Khan, R. M. Noor, and Z. Trabelsi, "A novel multifaceted trust management framework for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 20 084–20 097, 2022.

[13] P. Lang, D. Tian, X. Duan, J. Zhou, Z. Sheng, and V. C. M. Leung, "Cooperative computation offloading in blockchain-based vehicular edge computing networks," *IEEE Trans. Intell. Veh.*, vol. 7, no. 3, pp. 783–798, 2022.

[14] P. Lang, D. Tian, X. Duan, J. Zhou, Z. Sheng, and V. C. Leung, "Blockchain-based cooperative computation offloading and secure handover in vehicular edge computing networks," *IEEE Transactions on Intelligent Vehicles*, 2023, doi: 10.1109/TIV.2023.3271367.

[15] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation." in *Proc. 3rd ACM Conf. on Computer and Communications Security*, 01 1996, pp. 48–57.

[16] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Applied Cryptography and Network Security: 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007. Proceedings 5*. Springer, 2007, pp. 288–306.

[17] P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity-based broadcast proxy re-encryption and its application to cloud email," *IEEE Trans. Comput.*, vol. 65, no. 1, pp. 66–79, 2015.

[18] Q. Huang, Y. Yang, and J. Fu, "Secure data group sharing and dissemination with attribute and time conditions in public cloud," *IEEE Trans. Serv. Comput.*, vol. 14, no. 4, pp. 1013–1025, 2018.

[19] C. Ge, Z. Liu, J. Xia, and L. Fang, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 3, pp. 1214–1226, 2019.

[20] H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang, and Y. Zhou, "Identity-based encryption transformation for flexible sharing of encrypted data in public cloud," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3168–3180, 2020.

[21] H. Hu, Z. Cao, and X. Dong, "Autonomous path identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Access*, vol. 10, pp. 87 322–87 332, 2022.

[22] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.

[23] M. A. Ferrag and A. Ahmim, "Esspr: an efficient secure routing scheme based on searchable encryption with vehicle proxy re-encryption for vehicular peer-to-peer social network," *Telecommunication Systems*, vol. 66, no. 3, pp. 481–503, 2017.

[24] Z. Zhu, X. Wang, Y. Zhao, S. Qiu, Z. Liu, B. Chen, and F.-Y. Wang, "Crowdsensing intelligence by decentralized autonomous vehicles organizations and operations," *IEEE Trans. Intell. Veh.*, vol. 7, no. 4, pp. 804–808, 2022.

[25] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, "Blockchain-based secure data storage for distributed vehicular networks," *Applied Sciences*, vol. 10, no. 6, p. 2011, 2020.

[26] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, 2019.

[27] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2906–2920, 2019.

[28] S. Kim and A. S. Ibrahim, "Byzantine-fault-tolerant consensus via reinforcement learning for permissioned blockchain-empowered v2x network," *IEEE Trans. Intell. Veh.*, vol. 8, no. 1, pp. 172–183, 2023.

[29] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based vanet," *Information Sciences*, vol. 545, pp. 170–187, 2021.

[30] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionless blockchain: A survey," *Digital Communications and Networks*, vol. 7, no. 3, pp. 295–307, 2021.

[31] S. Lee and S.-H. Seo, "Design of a two layered blockchain-based reputation system in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 1209–1223, 2022.

[32] B. Li, R. Liang, W. Zhou, H. Yin, H. Gao, and K. Cai, "Lbs meets blockchain: An efficient method with security preserving trust in sagin," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5932–5942, 2022.

[33] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in vanet," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3765–3775, 2021.

[34] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," 2018.

[35] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 1–17, 2020.

[36] K.-A. Shim, "A survey on post-quantum public-key signature schemes for secure vehicular communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 14 025–14 042, 2021.

[37] C. Xu, H. Wu, H. Liu, W. Gu, Y. Li, and D. Cao, "Blockchain-oriented privacy protection of sensitive data in the internet of vehicles," *IEEE Trans. Intell. Veh.*, 2022, doi: 10.1109/TIV.2022.3164657.

[38] L. Chen, Y. Li, C. Huang, Y. Xing, D. Tian, L. Li, Z. Hu, S. Teng, C. Lv, J. Wang, D. Cao, N. Zheng, and F.-Y. Wang, "Milestones in autonomous driving and intelligent vehicles—part 1: Control, computing system design, communication, hd map, testing, and human behaviors," *IEEE Trans. Syst., Man, Cybern., Syst.*, pp. 1–17, 2023.

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

[40] L. Zhang, B. Kang, F. Dai, Y. Zhang, and H. Liu, "Hybrid and hierarchical aggregation-verification scheme for vanet," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 11 189–11 200, 2022.

[41] J. Yang, F. Lin, C. Chakraborty, K. Yu, Z. Guo, A.-T. Nguyen, and J. J. P. C. Rodrigues, "A parallel intelligence-driven resource scheduling scheme for digital twins-based intelligent vehicular systems," *IEEE Trans. Intell. Veh.*, 2023, doi: 10.1109/TIV.2023.3237960.

[42] Y. Tian, J. Wang, Y. Wang, C. Zhao, F. Yao, and X. Wang, "Federated vehicular transformers and their federations: Privacy-preserving computing and cooperation for autonomous driving," *IEEE Trans. Intell. Veh.*, vol. 7, no. 3, pp. 456–465, 2022.

[43] L.-Y. Yeh, N.-X. Shen, and R.-H. Hwang, "Blockchain-based privacy-preserving and sustainable data query service over 5g-vanets," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 9, pp. 15 909–15 921, 2022.

[44] S. McKinley and M. Levine, "Cubic spline interpolation," *College of the Redwoods*, vol. 45, no. 1, pp. 1049–1060, 1998.

[45] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Trans. Parallel Distrib. Syst.*, vol. 32, no. 5, pp. 1146–1160, 2020.

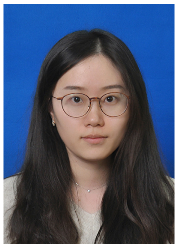
[46] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu, and V. C. M. Leung, "Adaptive resource allocation in future wireless networks with blockchain and mobile edge computing," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1689–1703, 2020.

[47] R. Rivest, "Rfc1321: The md5 message-digest algorithm," 1992.

[48] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *Advances in Cryptology–ASIACRYPT 2007: 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007. Proceedings 13*. Springer, 2007, pp. 200–215.

[49] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in *Modeling and tools for network simulation*. Springer, 2010, pp. 15–34.

[50] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using sumo," in *2018 21st international conference on intelligent transportation systems (ITSC)*. IEEE, 2018, pp. 2575–2582.



Xu Han received her B.E. and M.Sc. degrees in Software Engineering from Jilin University. She is currently working towards the Ph.D. degree with the School of Transportation Science and Engineering, Beihang University, Beijing, China. Her current research interests are focused on wireless communication, privacy protection in Internet of Vehicles, and intelligent transportation systems.

Daxin Tian (Senior Member, IEEE) received his Ph.D degree in computer application technology from Jilin University, Changchun, China, in 2007. He is currently a professor with the School of Transportation Science and Engineering, Beihang University, Beijing, China. His research is focused on intelligent transportation systems, autonomous connected vehicles, swarm intelligent and mobile computing. He was awarded the Changjiang Scholars Program (Young Scholar) of Ministry of Education of China in 2017, the National Science Fund for Distinguished Young Scholars in 2018, and the Distinguished Young Investigator of China Frontiers of Engineering in 2018. He is also a sensor member of the IEEE ans served as the Technical Program Committee member/Chair/Co-Chair for several international conferences including EAI 2018, ICTIS 2019, IEEE ICUS 2019, IEEE HMWC 2020, GRAPH-HOC 2020, etc.

Jianshan Zhou received the B.Sc.,M.Sc., and Ph.D. degrees in traffic information engineering and control from Beihang University, Beijing, China, in 2013, 2016 and 2020, respectively. From 2017 to 2018, he was a Visiting Research Fellow with the School of Informatics and Engineering, University of Sussex, Brighton, U.K. He is currently an associate professor with the School of Transportation Science and Engineering, Beihang University. He is the author or coauthor of more than 20 international scientific publications. His research interests include the modeling and optimization of vehicular communication networks and air–ground cooperative networks, the analysis and control of connected autonomous vehicles, and intelligent transportation systems.

Xuting Duan received the Ph.D degree in Traffic Information Engineering and Control from Beihang University, Beijing, China. He is currently an associate professor with the School of Transportation Science and Engineering, Beihang University. His current research interests include vehicular ad hoc networks, cooperative vehicle infrastructure system and internet of vehicles.

Zhengguo Sheng (Senior Member, IEEE) received the B.Sc. degree from the University of Electronic Science and Technology of China, Chengdu, China,in 2006, and the M.S. and Ph.D. degrees from Imperial College London, London, U.K., in 2007 and 2011, respectively. He is currently a Reader with the University of Sussex, Brighton, U.K. Previously, he was with UBC, Vancouver, BC, Canada, as a Research Associate and with Orange Labs as a Senior Researcher. He has more than 120 publications. His research interests cover IoT, vehicular communications, and cloud/edge computing.

Victor C. M. Leung (Life Fellow, IEEE) is a Distinguished Professor of Computer Science and Software Engineering at Shenzhen University, China. He is also an Emeritus Professor of Electrical and Computer Engineering and Director of the Laboratory for Wireless Networks and Mobile Systems at the University of British Columbia (UBC), Canada. His research is in the broad areas of wireless networks and mobile systems, and he has published widely in these areas. Dr. Leung is serving on the editorial boards of the IEEE Transactions on Green Communications and Networking, IEEE Transactions on Cloud Computing, IEEE Transactions on Computational Social Systems, IEEE Access, IEEE Network, and several other journals. He received the 1977 APEBC Gold Medal, 1977-1981 NSERC Postgraduate Scholarships, IEEE Vancouver Section Centennial Award, 2011 UBC Killam Research Prize, 2017 Canadian Award for Telecommunications Research, 2018 IEEE TCGCC Distinguished Technical Achievement Recognition Award, and 2018 ACM MSWiM Reginald Fessenden Award. He coauthored papers that won the 2017 IEEE ComSoc Fred W. Ellersick Prize, 2017 IEEE Systems Journal Best Paper Award, 2018 IEEE CSIM Best Journal Paper Award, and 2019 IEEE TCGCC Best Journal Paper Award. He is a Life Fellow of IEEE, and a Fellow of the Royal Society of Canada (Academy of Science), Canadian Academy of Engineering, and Engineering Institute of Canada. He is named in the current Clarivate Analytics list of Highly Cited Researchers.