Broadcast Encryption Scheme for V2I Communication in VANETs

Hong Zhong, Shuo Zhang, Jie Cui, Lu Wei, and Lu Liu

***Abstract*—Information dissemination in vehicular ad hoc networks (VANETs) is inseparable from the interaction between vehicles and infrastructure. The trust authority (TA) often plays a pivotal role in VANETs and requires interaction with multiple vehicles. However, when the TA sends the same message to multiple vehicles, there are many redundancies, as it needs to negotiate with each vehicle and send them different ciphertexts. This greatly reduces the work efficiency of the TA. To the best of our knowledge, there is no research on the problem of redundancy that occurs when the same message is sent to multiple vehicles in VANETs. The proposed scheme adopts identity-based broadcast encryption (IBBE) technology, which is a secure data-sharing scheme suitable for the vehicle-to-infrastructure communication mode, in VANETs for the first time. Thus, with only one encryption, the TA can generate a fixed-length ciphertext for a group of vehicles. When there are new vehicles that subsequently request a service, the TA can assign encryption tasks to the proxy server. In terms of security, our scheme meets the particular requirements of VANETs. The encryption overhead of the sender and the length of the ciphertext were comparatively analyzed. The results demonstrated that the performance of the scheme improved significantly. Thus, our scheme can prevent redundancies and effectively improve the work efficiency of TA.**

***Index Terms*—Broadcast encryption, vehicle to infrastructure (V2I), multi-receiver, proxy server.**

I. Introduction

With the development of science and technology, vehicles can easily obtain information from the outside world. The vehicle-related information, which is generated during driving, can be transmitted through a wireless communication device called the on-board unit (OBU) [1]. There are several interactive modes, such as vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-cloud. All of them form a huge information interaction network. While exchanging information, the privacy and integrity of participating vehicles and messages must be protected to ensure secure communication. Based on security, the efficiency of communication can be improved to achieve secure and efficient data sharing. Many schemes have been proposed to improve the efficiency of data sharing in VANETs in terms of various aspects [2]–[6].

Typically, there are three communication modes for data sharing: one-to-one, one-to-many, and many-to-many. Many communication schemes in VANETs are based on one-to-one. When one-to-many and many-to-many modes are implemented, their essence is still divided into many one-to-one direct communication modes [7], [8]. When a data owner wants to send the same message to a group of vehicles, the traditional solution is to split the multi-receiver to allow the data owner to interact with each vehicle of the group (using the one-to-one communication mode). The number of relevant ciphertexts and receivers is the same, and the length of the ciphertext increases linearly with the number of receivers [9]. This method can also achieve the ultimate purpose of secure data sharing. However, this has caused many redundancies for data owners.

The TA usually plays an important role in VANETs. As a third party, the TA may be the local traffic administration, which controls local vehicle information, road conditions, and other related service information [10], [11]. Furthermore, the TA can be a nationwide general manager. In this scheme, the TA is considered a regional manager (not nationwide). In an area, it is very common for the TA to have one-to-many communication with vehicles. For example, the vehicles at the scene of an accident send the collected relevant information to vehicle administrations. Some vehicles request local vehicle administrations for information related to their driving schedules. The TA sends local traffic conditions to vehicles arriving at the same destination or those passing through the same sections of a road. All situations involve the (redundancy) problem of sending duplicate messages. Multiple vehicles may want to request information related to this route because they have the same destination during a period. At this time, the TA (as the management of information) needs to send the same related data to the vehicles [12], [13]. If the communication mode is split into one-to-one, the messages need to be encrypted multiple times, which will create multiple redundant messages, particularly when the number of receivers is relatively large. As the traditional solution in VANETs does not provide a corresponding scheme to prevent the problem of redundancy in one-to-many communication, formulating an effective solution is essential [14].

To solve this problem, it is necessary to fix the length of the ciphertext by generating the same ciphertext for multiple receivers. Through investigation, we found that the IBBE can solve these problems efficiently. Broadcast encryption can achieve the effect of broadcasting, namely, one-to-many communication. It can generate a public, fixed-length ciphertext for a group of receivers using identity-based information. Next, the receivers use their broadcast encryption private keys to decrypt this ciphertext and obtain information in

H. Zhong, S. Zhang, J. Cui, and L. Wei are with the Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Computer Science and Technology, Anhui University, Hefei 230039, China, the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China, and the Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China (e-mail: cuijie@mail.ustc.edu.cn).

L. Liu is with the School of Informatics, University of Leicester, LE1 7RH, UK (email: l.liu@leicester.ac.uk).

plaintext. Generally, the purpose of broadcast encryption is to negotiate a common key shared by the sender and multiple receivers. Subsequently, secure data sharing can be achieved using public-key encryption. IBBE has many advantages; for example, flexibility. The data owner can choose the data being sent and has control over the group S(a group of authorized receivers). It can also negotiate a common short key with the receivers in group S. Then, the data owner uses a short key to encrypt the long dataset. Thus, it can obtain a large amount of data effectively in scenarios where vehicular interactions take more time than usual [15].

To further improve the efficiency of data sharing in the system, the proxy server is introduced to construct the optimization phase. The proxy server can reduce the encryption burden of the TA. TA can assign encryption tasks to vehicles (in group S) and proxy servers. At the same time, the proxy server can also reduce the decryption cost of the vehicle. By using proxy re-encryption technology [16], the proxy server can convert the IBBE ciphertext into an identity-based encryption (IBE) ciphertext. When a new vehicle wants to interact with the TA in the next period, the TA does not need to encrypt the plaintext data by itself; however, it forwards the encryption authority and the received request to the vehicle which has obtained the data access authority (in group S). The proxy server can use the intermediate key to convert the original ciphertext into a new ciphertext. The new ciphertext is encrypted with the public key of the authorizer in the proxy re-encryption process. During the conversion process, no information related to the plaintext is disclosed. This makes the proxy re-encryption technology very effective and secure in a scenario where there is a semi-trusted third party [17], [18]. Next, the vehicles in group S will generate a new intermediate key related to the identity of the new vehicle and send the intermediate key and IBBE ciphertext to the proxy server. The proxy server can convert the IBBE ciphertext into IBE ciphertext and send it to the new vehicle [19]. IBE has lightweight characteristics and does not need to manage cumbersome public key certificates [20]. This case is considered unique and special (IBBE with only one receiver). Therefore, the IBE ciphertext is chosen as the converted ciphertext to the new vehicle.

Note that the sender here is changed from TA to a certain vehicle user in the original group S. As the proxy server uses IBBE ciphertext and has no decryption authority, the proxy server will not receive any message about the plaintext. This can reduce the cost of the original sender TA (subsequent vehicle requests can be completely conducted by members of the proxy server and the group S), as well as the receiver. The sender and receiver do not need to be online at the same time. Thus, our data owner TA can eliminate subsequent requests after sending encrypted data for the first time. The TA transfers the authorization task to the vehicle in group S and the encryption task to the proxy server. Thus, it can significantly reduce the cost of the sender. Moreover, since the vehicle receives the IBE ciphertext and the cost of decrypting the data is negligible, the overall efficiency can be improved.

A. Contributions

To the best of our knowledge, no scheme uses broadcast encryption technology to prevent redundancies in one-to-many communication in VANETs. The main contributions of this study are as follows.

- To address the problem of redundancies in the one-to-many communication mode (between vehicles and infrastructure), a new scheme is proposed for VANETs. In our scheme, the IBBE technology is used by the sender TA, and the IBE technology is used by new vehicles. Our scheme improves the efficiency of the TA, helps prevent redundant encryption operations, and optimizes the decryption cost of the vehicle.
- A comprehensive security analysis is presented based on the security goals of VANETs. Based on a specific security analysis it is observed that our scheme is secure.
- Through experimental comparison and analysis, it is observed that our scheme can reduce the encryption redundancy of the sender TA, improve the communication efficiency between TA and vehicles, and ensure secure data sharing. In addition, the converted IBE ciphertext can greatly reduce the cost of the receiver owing to its lightweight characteristics.

B. Organization of the Rest Paper

In Section II, related work is introduced. In Section III, we briefly introduce the basic knowledge, system model, and security goals that need to be met in VANETs. The structure of the scheme is detailed in Section IV. Section V provides a comprehensive explanation and analysis of security goals. The experimental results of a comprehensive analysis are presented in Section VI. Section VII presents the conclusions.

II. Related Work

In recent years, many schemes have been proposed to solve the problem of secure data sharing in VANETs [21], [22]. They have improved the efficiency of data interaction in different aspects. Sookhak et al. [23] proposed a more efficient data sharing scheme between vehicles by using proxy re-encryption technology. In this scheme the cloud re-encrypt the data uploaded by the data owner and then sent it to the newly joined receivers. Liu et al. [24] proposed a real-time scheme between vehicles by using the evolutionary fuzzy game. The vehicle and its neighboring vehicle can cooperatively decide whether data is distributed out or cached locally. Compared with the non-cooperative data sharing scheme, the transmission delay and speed in this scheme are improved. Pan et al. [25] proposed a cross-domain data sharing scheme based on edge computing. The edge vehicle can forward data to the receiver to reduce RSU load and delay. Shen et al. [26] proposed a scheme that improves the efficiency of key updating and supports dynamic changes of members. This scheme use the symmetric balanced incomplete block design (SBIBD) algorithm and the concept of indistinguishable confusion. The SBIBD algorithm is improved to eliminate its complicated structure. However, these schemes do not consider

the redundancy problem of the encryption phase, and they do not improve the efficiency of communication.

Broadcast encryption was proposed by Fiat et al. [27]. The idea is to negotiate a common short key between a sender and multiple receivers. Then the sender uses this short key to encrypt data through symmetric encryption technology. For each member of the receiver, the ciphertext constructed by the sender is the same. The receiver can use its private key to decrypt the key ciphertext, as long as the receiver is authorized. And broadcast encryption has the characteristics of fixed-length ciphertext, which greatly reduces communication cost and computational cost. Subsequently, many broadcast encryption schemes were constructed based on this idea. In terms of security, Gentry et al. [28] elaborated the related issues of achieving adaptive security. Boneh et al. [29] proposed functional encryption to achieve the purpose of forming a fixed-length ciphertext and adaptive security. Then he proposed two construction methods based on multi-linear mapping [30]. However, the overhead of multi-linear mapping is too high and is not suitable for practical applications. Kim et al. [31] proposed a complete identity-based broadcast encryption scheme that has the fixed-length ciphertext and satisfies adaptive security. Because the computational complexity depends on the number of receivers, the scheme has huge overhead. Ge et al. [32] improved the performance of traditional broadcast encryption and realized effective revocation management for members in S. Only users who have not been revoked can decrypt the ciphertext. However, due to the use of attribute-based encryption, the computation cost is relatively large.

In recent years, broadcast encryption has been widely used in the Internet of Things, such as pay-TV, video conferencing, and other common applications in daily life. Li et al. [33] proposed a broadcast encryption scheme with fixed decryption cost. Based on leakage resilience identity encryption, the scheme gave a formal definition and security model of continuous leakage resilience IBBE. This scheme can resist adaptive selection ciphertext attacks. However, higher security brings much higher overheads. Kim et al. [34] discussed the IBBE technology that is more suitable for lightweight decryption devices in the context of edge computing. Under the original IBBE technology, interim nodes are introduced to convert the original IBBE ciphertext into a more lightweight ciphertext. After adding the outsourced partial decryption function, the scheme is more suitable for edge devices with limited computing resources. Chen et al. [35] proposed a broadcast encryption scheme with personalized information. In actual applications, the broadcast message related to the user can be personalized. Combined with the broadcast encryption technology, the personalized message is encrypted and transmitted with a shared key. However, due to the use of bilinear pairing operations, the decryption cost becomes very large.

The above is the development of broadcast encryption technology. Weng et al. [36] proposed a scheme using identity-based broadcast encryption technology in the environment of software-defined Internet of Vehicles. When SDN applications want to access network resources, the broadcast encryption mechanism enables network administrators to achieve dynamic access control. At the same time, the purpose of protecting the privacy of transmitted data is achieved. However, this scheme cannot solve the efficiency problem. Bunese et al. [37] evaluated group broadcast encryption in the VANETs. Compared with traditional symmetric encryption and asymmetric encryption, the author conclude that using group broadcast encryption can simplify the encryption phase and reduce the number of messages in the network.

A sender can use the multi-receiver encryption scheme or the broadcast encryption scheme to interact with multiple receivers. However, the multi-receiver encryption scheme does not reduce the encryption burden of sender. Bellare et al. [38] proposed multi-receiver encryption, which has the same scenario as broadcast encryption. The sender can generate identity-based ciphertexts for certain selected receivers. If the receiver is in the selected group, it can decrypt the ciphertext, and the receiver does not know the identity of other receivers except itself. Thus, the privacy of the receiver can be protected. Hung et al. [39] proposed a new certificateless multi-receiver anonymous encryption (CLMRE) scheme using bilinear pairing technology. In this scheme, the decryption cost is fixed and very low, while the encryption cost increases with the number of receivers. He et al. [40] improved the previous CLMRE scheme without using bilinear pairing technology. Even if the length of the ciphertext increases linearly with the number of receivers, the encryption cost is still much lower than the previous scheme. Deng et al. [41] proposed a new CLMRE scheme applied to the management of community services. The security of this scheme proved under the standard model is higher than the previous random oracle model.

Zeng et al. [42] proposed a deniable ring authentication scheme in VANETs. Here, the main purpose of using multi-receiver encryption is to hide the identity of the sender in a group of receivers to achieve the anonymity. This scheme protects the privacy of the sender and satisfies CCA2 security. It also shows that this scheme can be used to protect location privacy in VANETs. However, its excessive encryption operation do not solve the problem of sender's overhead.

None of the existing schemes solve the redundancy problem in one-to-many communication based on the Internet of Vehicles environment. The ciphertext length in traditional schemes is too long to satisfy the delay requirement. Therefore, our scheme uses the method of IBBE [15], which has the characteristics of short key and fixed ciphertext length. According to the scheme of Bunese et al. [37], it can be concluded that the scheme uses broadcast encryption technology to satisfy the security requirements of the Internet of Vehicle. It can reduce the encryption cost of the sender and improve the efficiency of data interaction.

III. BACKGROUND

Firstly, a brief review of some basic security knowledge is described to have a better understanding of the proposed scheme. Secondly, the model of vehicular network is introduced. There are four main components, TA, the proxy server (PS), roadside fixed unit (RSU), and vehicles equipped with the on-board unit (OBU). Finally, the security goals of our scheme are stated.

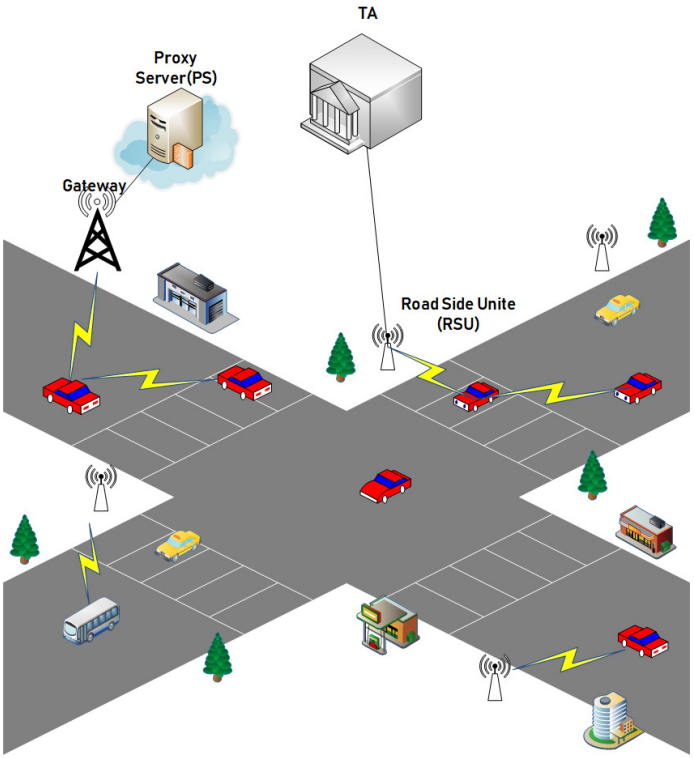


Fig. 1. System model of network

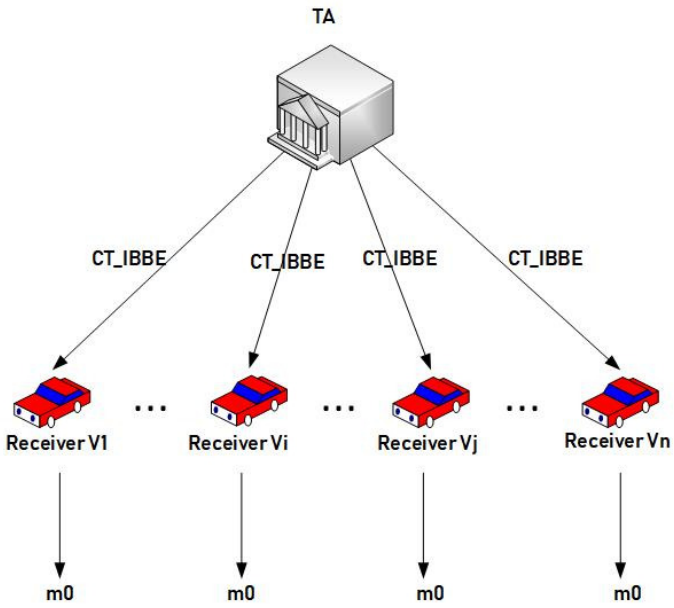


Fig. 2. System interaction model of IBBE

A. Bilinear Pairing

They are two cyclic groups noted by G_1, G_T, where p is the prime order of G_1. Let g be a generator of G_1, and there is a bilinear mapping on these two groups $e : G_1 \times G_1 \longrightarrow G_T$ has the following properties:

- Bilinearity: $\forall g_1, g_2 \in G_1, a, b \in Z_p$, we have $e({g_1}^a, {g_2}^b) = e(g_1, g_2)^{ab}$.
- Non-degeneracy: $\exists g_1, g_2 \in G_1$, it has $e(g_1, g_2) \neq 1$.
- Computability: $\forall g_1, g_2 \in G_1$, there exists an efficient algorithm to compute $e(g_1, g_2)$.

B. Network Model

Fig. 1 shows the vehicular network model considered in our framework. The details of the various components of the network are described below.

- TA: TA is a trusted third party with huge storage capacity and strong computing power. It is trusted completely in the system. The main functions of TA are to register public and private keys for vehicles joining the system, generate public parameters. Then TA loads these parameters into the vehicle's tamper-proof device (TPD) in advance. And it generates IBBE ciphertexts for the vehicle in group S to communicate with them efficiently.
- PS: The proxy server located on the cloud has the same powerful computing and huge storage capabilities as TA. However, it is half trusted. Therefore, only the encrypted data can be given to the proxy server instead of the plaintext information. The main function of the proxy server in this scheme is to perform conversion tasks. By using the intermediate key, the proxy server can convert the IBBE ciphertext into IBE ciphertext, even if the plaintext data is not known.
- RSU: The RSU is a wireless communication device located on the roadside between TA and the vehicle. It is connected to TA through a wire. In our scheme, RSU only acts as a transmission medium to forward vehicle information to TA or proxy server.
- Vehicle: The vehicle equipped with TPD is the broadest participant in the system can act as both a data owner and a data receiver. We assume that the TPD will never be attacked successfully. So, no information will be leaked. Therefore, the TPD can store the private key and other information obtained from TA securely. Then it can generate the pseudo identity of vehicle securely. The vehicle communicates with TA wirelessly through OBU and RSU.

In our system, the one-to-many communication scenario of V2I is carried out in the IBBE phase. To prevent confusion caused by too much information, it is assumed that the same vehicle only requests one message from TA in a period. A vehicle user has only one identity, whether it is an IBBE user or an IBE user.

C. Security Goals

In VANETs, security and privacy are the basic requirements for secure communication. A secure Internet of Vehicles scheme should meet the following basic security goals [43]:

- Message Authentication and Integrity: When the vehicle gets the message, it will verify the source of the message to ensure it is from the legitimate requested sender. Then the vehicle will verify whether the message is complete to ensure it is not modified or forged during the transmission process.

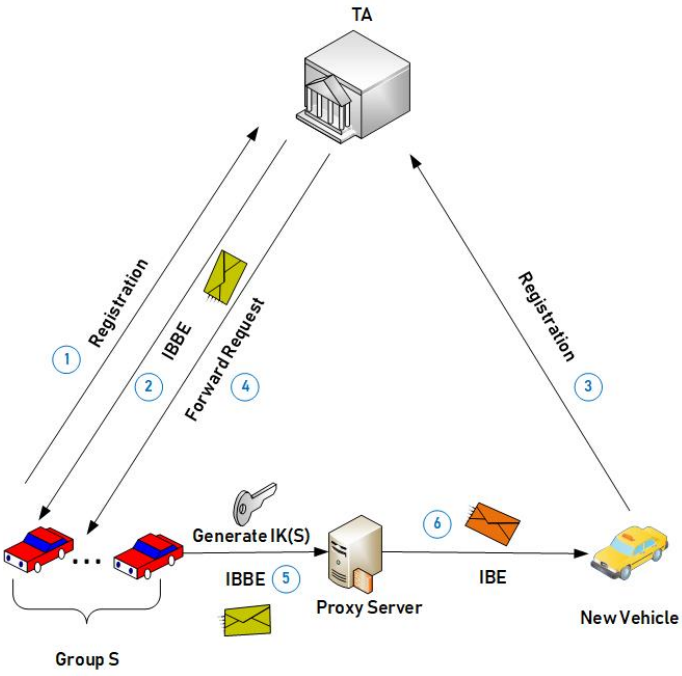


Fig. 3. System interaction model with proxy server

TABLE I
NOTATIONS

Notations	Definitions
TA	Trust authority
PS	Proxy server
S	A group of receiver vehicle
G	A cyclic group
g	The generator of group G
e	A bilinear map:$G_1 \times G_1 \rightarrow G_T$
q	Large prime number
rid	The real identity of the vehicle
T_i	The timestamp of message
$V_{i,j}$	The vehicle of scheme
h, Q_1, Q_2	Random elements in G
pid_i	A pseudo identity of vehicle
$pid_{i,j}$	A part of the pid_i, such that $pid_i = \{pid_{i,1}, pid_{i,2}\}$
pk	System public key
sk_i	A private key of the vehicle V_i
$sk_{i,j}$	A part of the sk_i, such that $sk_i = \{sk_{i,1}, sk_{i,2}\}$
msk	The master key of TA
BK_{ID_i}	The broadcast encryption key of V_i
IK	The intermediate key to converting the IBBE ciphertext
m_i	The requested message to TA from V_i
m_0	The encrypted symmetric key
$H(\cdot)$	A hash function such as $H : 0, 1^* \rightarrow Z_q^*$
$H_2(\cdot)$	A coding function such as $G_T \rightarrow G_1$
h_1, h_2	Two simple one-way hash functions
$\|\|$	Message concatenation operation

- Identity Privacy Protection: The vehicle continuously sends requests which contain identity information. To achieve the purpose of protecting their privacy, the vehicle uses pseudo identity instead of real identity. And the vehicle maintains unlinkability by changing the pseudo-identity regularly. No third party can obtain the true identity of the vehicle through any method except TA.
- Traceability and Conditional Privacy Protection: In some special cases, to track the specific vehicle, TA needs to reveal the true identity. When necessary, the vehicle needs removing from the communication system.
- Unlinkability: After the vehicle sends so many messages, no adversary can reveal the vehicle-related information by collecting and analyzing the massive messages.
- Resist Common Attacks: The scheme needs to resist common attacks, such as simulation attacks, replay attacks, modification attacks, and man-in-the-middle attacks in VANETs.

IV. The Proposed Scheme

In this section, the structure of the scheme is described in detail. A complete communication system is established here. First, the vehicle that wants to participate in the communication needs to interact with TA. The vehicle can participate in the subsequent communication after being authenticated by TA. The IBBE technology is used when TA sends messages to the vehicles in group S, which can reduce the number of redundant encryption of the sender. TA needs to send the same ciphertext to the vehicles in group S. Fig. 2 shows the interaction model of the IBBE phase.

Further, when a new vehicle wants to obtain data in the future, TA will no longer encrypt the plaintext data in person, but forward the new vehicle request and the data encryption authority to the vehicle in group S. Fig. 3 shows the overall framework of the IBE phase. The vehicle in group S only needs to generate an intermediate key, and then send the intermediate key and the IBBE ciphertext to the proxy server. Then it outsources the data encryption operation to the proxy server. The proxy server uses re-encryption technology to convert the IBBE ciphertext into the IBE ciphertext and send the ciphertext to the designated receiving vehicle. The main notations in this scheme are listed in Table I.

A. System Setup

Let G_1, G_T are two cyclic groups. Here, g is the generator of G and q is the order of G and G_T.

- TA randomly chooses $r_1, r_2 \in Z_q^*, \beta \in Z_q^*, h, Q_1, Q_2 \in G$, let $msk = (g, \beta)$ be the system master key.
- TA chooses hash function $H : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : G_T \rightarrow G_1$, and h_1, h_2 are two simple one-way hash functions as well. Then TA computes $pub_1 = g^{r_1}, pub_2 = g^{r_2}, g_0 = g, h^{\beta}, h^{\beta^2}, ..., h^{\beta^m}$, we set public key $pk = (pub_1, pub_2, e(g,h), g_0, H(\cdot), H_2(\cdot))$. Let $pk_{ibe} = \big(g_0, e(g,h), g^{\beta}, H(\cdot), H_2(\cdot)\big)$, $pk_{ibbe} = pk_{ibe}$. Here, m as the maximal size of the group S.
- TA securely preloads parameter r_1, r_2 into the vehicle's TPD.

B. Request Signing and Verification

1) When a vehicle wants to join the system, TA must authenticate the identities of all vehicles. Then, only vehicles that pass TA's authentication can obtain the broadcast key generated by TA. Here, the method of generating pseudonyms by on-board temper-proof device is adopted. TPD randomly chooses $s \in Z_q^*$,

compute Pseudo-identity $pid_i = \{pid_{i,1}, pid_{i,2}\}$ and $sk_i = \{sk_{i,1}, sk_{i,2}\}$, where

$$pid_{i,1} = g^s,$$

$$pid_{i,2} = rid_i \oplus H({pub_1}^s),$$

$$sk_{i,1} = {pid_{i,1}}^{r_1},$$

$$sk_{i,2} = {Q_1}^{r_2 h_2(pid_{i,1}||pid_{i,2}||T_i)} \cdot {Q_2}^{h_1(pid_{i,1})}.$$

We use $sk_{i,1}$ and $sk_{i,2}$ to generate the signature on m_i.

2) After the vehicle generates the relevant parameters, it will send a request m_i to TA to obtain a specific message. The vehicle selects the pseudo-identity pid_i related to the latest timestamp T_i and sk_i to sign the request m_i, it computes

$$\delta_i = sk_{i,1} \cdot {sk_{i,2}}^{h_1(m_i)}$$

where m_i is the request, then the vehicle sends tuple $(pid_i, m_i, \delta_i, T_i)$ to TA.

3) After TA receives the message, the first thing is to check the T_i is valid or not. If $T_c - T_i < T_\Delta$, it means that this message is valid, then TA verify this message through the following equation. Otherwise, TA will reject this message.

$$\begin{aligned} e(\delta_i, g) = e(pid_{i,1} \cdot {Q_2}^{h_1(pid_{i,1})}, pub_1) \\ \cdot e({Q_1}^{h_1(m_i)h_2(pid_{i,1}||pid_{i,2})}, pub_2) \end{aligned}$$

TA accepts the request only if this equation is correct. Then the batch verification is introduced, the tuple $\{pid_i, m_i, \delta_i, t_i\}_{i=1}^n$ denoted as the message will be verified. Then TA chooses a vector $Vt = (Vt_1, Vt_2, ..., Vt_n)$ with small value, where $V_i \in [1, x]$. Here, x is a small value. The batch verification equation is as follows.

$$\begin{aligned} e(\sum_{i=1}^{n}(Vt_i)^2\delta_i, g) = e(\sum_{i=1}^{n} Vt_i pid_{i,1} Q^{h_1(pid_{i,1})}, pub_1) \\ \cdot e(\sum_{i=1}^{n} {Q_1}^{h_1(m_i)h_2(pid_{i,1}||pid_{i,2})}, pub_2) \end{aligned}$$

After V_i is verified by TA, TA will uncover the vehicle's real identity by computing

$$rid_i = pid_{i,2} \oplus H({pid_{i,1}}^{r_1}),$$

which is used to compute the broadcast key BK_{ID_i} for vehicles.

$$BK_{ID_i} = g^{\frac{1}{\beta + H(rid_i)}}$$

Here, the BK_{ID_i} is uesd to decrypt the IBBE ciphertext for Vi. Then, it is loaded into the TPD on the vehicle.

C. Generate IBBE Ciphertext

After TA receives the vehicle's data request, it divides the group $S = \{H(pid_i)\}_{i=1}^n$ by itself and generates a fixed-length IBBE ciphertext for these receiving vehicles. Then TA broadcasts the IBBE ciphertext. Based on the public key PK, the identity hash collection S, and $m_0 \in G_T$ (the shared symmetric key to be encrypted), TA will generate ciphertext CT_{IBBE} for the vehicle in group S. The process is as follows:

1) TA chooses a random integer $r \in Z_p^*$ to compute ciphertext for vehicle in group S. The IBBE ciphertext $CT_{IBBE} = (CT_0, CT_1, CT_2)$ where

$$CT_0 = m_0 e(g, h)^r,$$

$$CT_1 = g_0^{-r},$$

$$CT_2 = h^{r\prod_{i=1}^{n}(\beta + H(rid_i))}.$$

2) TA broadcasts the message (CT_{IBBE}, S, T_i) to vehicles.

D. Generate IBE Ciphertext

A data file has been encrypted into IBBE ciphertext and sent to the vehicle group S. The original vehicle in group S can decrypt the IBBE ciphertext with its private key. When a new vehicle user rid requests this message, a user rid_j with access permission (a vehicle user in the group S) can authorize the newly joined vehicle to obtain data. First, TA still verifies the new vehicle's identity and then forwards the new user's identity hash value $H(rid_j)$ to the user V_j. V_j needs to generate an intermediate key for the newly joined vehicle. and then send the intermediate key to the proxy server. The proxy server uses the received intermediate key to transform the original IBBE ciphertext into IBE ciphertext and then sends the IBE ciphertext to the new vehicle user.

1) Intermediate key Generation: At this time, the authorization task of the data is transferred from TA to the vehicles in group S. We assume that the authorization task is performd by the user V_j with identity rid_j. Based on the identity hash value of the new vehicle, V_j can generate an intermediate key. V_j chooses a random element $k \in G_T$ and computes

$$BK'_{ID_j} = BK_{ID_j} \cdot H_2(k)^{\prod_{i=1 \neq j}^{n} H(rid_i)}.$$

V_j chooses random number $t \in Z_q^*$ and computes

$$IK_0 = ke(g, h)^r, IK_1 = h^{r(\beta + H(rid))}.$$

Among them, IK_0 and IK_1 are the parameters needed to generate the converted ciphertext. Finally, V_j outputs the intermediate key $IK = (BK_{ID_j}, IK_0, IK_1)$ and send it to PS.

2) Transformed Ciphertext Generation: According to the intermediate key K, the proxy server can convert the IBBE ciphertext CT_{IBBE} into an IBE ciphertext CT_{IBE}. The proxy server generates CT_{IBE} by using the intermediate key and CT_{IBBE}. First, according to the public key PK, CT_{IBBE}, and IK, the proxy server can compute

$$K = \left[e(CT_1, h^{p_{j,S}(\beta)}) \cdot e(BK'_{ID_j}, CT_2)\right]^{\frac{1}{\prod_{i=1, i \neq j}^{s} H(rid_i)}}$$

where

$$p_{j,S}(\beta) = \frac{1}{\beta}(\prod_{i=1,i\neq j}^{n}(\beta + H(rid_i)) - \prod_{i=1,i\neq j}^{n} H(rid_i)).$$

Then the proxy server uses K to compute

$$CT_0' = CT_0/K = m_0/e(H_2(k), CT_2).$$

Finally, the proxy server outputs

$$CT_{IBE} = (CT_0', CT_2, IK_0, IK_1).$$

Here proxy server can not compute $p_{j,S}$ directly, so we take apart the formula.

$$\begin{aligned}\prod_{i=1,i\neq j}^{n} H(rid_i) &= H(rid_1)H(rid_2)...H(rid_n)\\ &= R_0\end{aligned}$$

$$\begin{aligned}p_{j,S} &= \frac{1}{\beta}\left(\prod_{i=1,i\neq j}^{n}(\beta + H(rid_i)) - R_0\right)\\ &= \frac{1}{\beta}\left[(\beta + H(rid_1))...(\beta + H(rid_n)) - R_0\right]\\ &= \frac{1}{\beta}([\beta^2 + (H(rid_1) + H(rid_2))\beta + H(rid_1)\\ &\cdot H(rid_2)]...(\beta + H(rid_n)) - R_0)\\ &= \frac{1}{\beta}(\beta^n + R_{n-1}\beta^{n-1} + ... + R_1\beta + R_0 - R_0)\\ &= \beta^{n-1} + R_{n-1}\beta^{n-2} + ... + R_1\end{aligned}$$

Since $H(rid_i)$ is a positive integer, it can be known that R_i is a positive integer as well. Then the value of $(h^{\beta}, h^{\beta^2}, ..., h^{\beta^m})$ can be obtained from the public parameters. The public parameter can be used to compute $h^{p_{j,S}(\beta)}$. Of course, the overhead becomes relatively large because there are n times of cumulative multiplication operations.

E. Vehicle Decryption Phase

In this phase, there are two types of vehicle users, one belongs to the original group S, and the other is a new vehicle.

1) Upon receiving the IBBE ciphertext, the vehicle in group S can use the broadcast private key BK_{ID_i} to decrypt the ciphertext. Then the vehicle can obtain the symmetric key m_0. Finally the vehicle use the symmetric key to obtain the data. The vehicle computes

$$\begin{aligned}m_0' &= \left[e(CT_1, h^{p_{j,S}(\beta)}) \cdot e(BK_{ID_j}, CT_2)\right]^{\frac{1}{\prod_{i=1,i\neq j}^{s} H(rid_i)}}\\ &= e(g,h)^r.\end{aligned}$$

Then the vehicle uses m_0' to decrypt CT_0.

$$m_0 = CT_0/m_0'$$

2) When a new vehicle joins the system, it receives the converted IBE ciphertext CT_{IBE}. The vehicle needs to download the IBE ciphertext from the proxy server. Similarly, the vehicle reveals the ciphertext CT to obtain the symmetric key, and then uses the symmetric key to recover the plaintext data. IBE ciphertext decryption is described as follows. First, the new vehicle V_j uses the broadcast key to compute

$$k = IK_0/e(BK_{ID}, IK_1).$$

Then V_j uses parameter k to obtain

$$m_0 = CT_0' \cdot e(H_2(k), CT_0).$$

V. Security Analysis

In this section, combined with the specific security goals in VANETs, the comprehensive security analysis is presented to show the security of our scheme. The security proof can refer to the structure in [19].

First, we introduce the Computational Diffie-Hellman (CDH) problem. There is a cyclic group G with order p, and g is the generator of G. For $g, g^a, g^b \in G$, if the algorithm $\mathcal{A}$ can output $g^{ab} \in G$ with probability $Pr[\mathcal{A}(g, g^a, g^b) = g^{ab}]$, it is defined that $\mathcal{A}$ can solve the CDH in G where

$$Pr[\mathcal{A}(g, g^a, g^b) = g^{ab}] \geq \epsilon.$$

The probability is over the random choice of $g \in G$, $a, b \in Z_p^*$, and the random bits of $\mathcal{A}$.

Definition 1: The CDH hard problem holds in G if no adversary in probabilistic polynomial time can output g^{ab} with probability at least ϵ.

1) Message Authentication and Integrity: In the vehicle registration phase, TA can verify whether the signature comes from a legitimate message $(pid_i, m_i, \delta_i, T_i)$ through Equation $e\left(\sum_{i=1}^{n}(Vt_i)^2\delta_i, g\right) = e\left(\sum_{i=1}^{n} Vt_i \cdot pid_{i,1}Q^{h_1(pid_{i,1})}, pub_1\right) \cdot e\left(\sum_{i=1}^{n} Q_1^{h_1(m_i)h_2(pid_{i,1}||pid_{i,2})}, pub_2\right)$. According to the scheme [44], it can be seen from its security definition that no adversary can successfully break the difficult problem of CDH in polynomial time, so the signature cannot be successfully forged. The security proof of scheme [15] shows that $Adv_{IBBE}^{ind}(t,n)$ (the probability of an adversary breaking the IBBE scheme) is negligible, so IBBE ciphertext cannot be forged, either. At the conversion ciphertext phase, the probability of forging the conversion ciphertext is the same as breaking the IBBE scheme. It is also impossible to forge the conversion ciphertext because the IBBE scheme cannot be broken. Therefore, in this scheme, TA can authenticate the message from the vehicle and check its integrity. At the same time, when the vehicle receives the ciphertext, our scheme can also ensure that the received ciphertext comes from a legitimate sender, and the integrity is not destroyed.
2) Identity Privacy Protection: When the vehicle requests a message from TA, the vehicle hides its real identity by calculating $pid_{i,1} = g^s$ and $pid_{i,2} = pid_i \oplus H(pub_1^s)$. TA can recover the real identity of the vehicle by calculating $rid_i = pid_{i,2} \oplus H(pid_{i,1}^{r_1})$. Since the master keys r_1 and r_2 are only owned by TA, even if a third party obtains the pseudo identity of the vehicle during

the communication process, the real identity cannot be recovered. The real identity of the vehicle is hidden through the hash function as $S = H(rid_i)$. So, the malicious third party cannot disclose the real identity of the vehicle even if it intercepts the ciphertext.

3) Traceability and Conditional Privacy Protection: The vehicle sends a request message m_i to TA, then TA can use its private key r_1 to restore the true identity of the vehicle. In this way, TA can achieve the purpose of tracking malicious vehicles in the system. Whether it is an IBBE user or an IBE user, it must be authenticated by TA before entering the system to communicate. So that TA can control all vehicles in the system, and any malicious vehicle can be tracked once it is found.
4) Unlinkability: In our scheme, the vehicle chooses a random number r to generate pseudo-identities $pid_{i,1} = g^s$ and $pid_{i,2} = pid_i \oplus H(pub_1^s)$. When the timestamp expires, the vehicle will choose a new random number to compute the pseudo identity of the vehicle. So, the pseudo identity of the vehicle is dynamically updated. Therefore, even if the adversary intercepts multiple messages, it is impossible to analyze whether the messages $m_1, m_2, ..., m_i$ are from the same vehicle. After joining the system, the vehicle uses the value of $H(rid_i)$ to participate in the computation process. So the real identity of the vehicle cannot be linked by the adversary in the communication process.
5) Resist Common Attacks:
   - Replay Attack: The tuple is sent by the vehicle to TA, where T_i is the timestamp, so both TA and the proxy server can verify the freshness of the message by checking the timestamp. Once a malicious vehicle sends a message requested previously, it will be found that this message is invalid by checking the timestamp. In this way, the scheme can prevent replay attacks.
   - Simulation Attack: According to $sk_{i,1} = {pid_{i,1}}^{r_1}$ and $sk_{i,2} = Q_1^{r_2 h_2(pid_1||PID_2||T_i)} \cdot Q_2^{h_1 pid_{i,1}}$, if anyone wants to forge the signature, they have to obtain r_1 and r_2. Since r_1 and r_2 are private keys of TA and loaded in the vehicle's TPD securely, the adversary cannot obtain them. So the vehicle's signature cannot be forged.
   - Man-in-the-middle Attack Protection: Since the adversary cannot forge the signature of the message m_i successfully, the message cannot be simulated. So this scheme can resist man-in-the-middle attacks.

VI. Performance Analysis and Comparison

In this section, we carry out a series of analyses and provide comparisons with four related schemes [35], [39], [40] and [41]. These four related schemes have been introduced in section II. Our scheme is different from these comparison schemes. It is in the scenario of the Internet of Vehicles. It also includes the registration phase of the vehicle and the certification phase of the vehicle from TA. These phases ensure the security of the scheme in a special scenario. Therefore, we focus on the encryption phase (the encryption of the message during one-to-many communication) and the decryption phase (the decryption after the vehicle receives the ciphertext). For the vehicle registration phase and the subsequent phase, we perform a separate analysis in the same experimental environment. The subsequent phase is introduced to optimize the decryption cost of the vehicle.

TABLE II
Execution Time of Single Operation

Symbol	Description	Time/ms
T_{bpo}	The bilinear pairing operation	5.086
T_{eo}	The exponentiation operation in G or G_T	0.694
T_{smo}	The scale multiplication operation in G	0.3218

Based on the bilinear pairing $e : G_1 \times G_1 \to G_T$, which is built for achieving the security level of 80 bits, the IBBE and IBE schemes are constructed. The G_1 is a cyclic group with the order q on the supersingular elliptic curve $E : y^2 = x^3 + x$ mod g. Here g is a 512-bit prime number and q is a 160-bit Solinas prime number. Then each single operation time on the platform of 3.4 GHZ i7-4770 with the MIRACL library is tested. Table II lists the execution time of the cryptographic operations. Here, the exponentiation operation time, scale multiplication time, and pairing time were computed.

A. Computation Cost Analysis

Here, a corresponding analysis for the encryption and decryption phases of each scheme is conducted. Finally, we get a comparison of the total cost of each scheme. In the scheme of Chen et al. [35], when generating the header information Hdr, exponentiation operation is used to compute the relevant parameters K_i for each user. So the encryption cost here is $(3n + 3)T_{eo} + 2nT_{smo}$. In the decryption phase, the user only needs one pairing operation, six exponentiation operations, and four scalar multiplication operations. Then the total computation cost is $(3n + 9)T_{eo} + (2n + 4)T_{smo} + T_{bpo} \approx 2.7256n + 25.1112$ ms. In the scheme of Hung et al. [39], because the sender uses bilinear pairing technology and exponentiation operations to generate the relevant parameter Ki for each receiver, the overhead of this part is proportional to the number of receivers. In the encryption part, the sender requires n pairing operations, n exponentiation operations, and $n + 1$ scalar multiplication operations. In the decryption phase, users only need to compute some parameters related to themselves. Then only one pairing operation and one scalar multiplication operation are needed. Then the total operation is $(n+1)T_{bpo}+nT_{eo}+(n+2)T_{smo} \approx 6.1018n+5.7296$ ms. In the scheme of Deng et al. [41] bilinear pairing operations are also used. Then the overhead is very high. In the encryption phase, the sender needs $(2n + 3)$ scalar multiplication operations and n pairing operations. In the decryption phase, the receiver also needs a pairing operation and an exponentiation operation. So, the total cost is $(n + 1)T_{bpo} + (2n + 3)T_{smo} + T_{eo} \approx 5.7296n + 7.7108$ ms. He et al.'s scheme [40] didn't use bilinear pairing operations, then the computation cost in the encryption phase will be lower than the other schemes. It only requires $(3n + 1)$ scalar multiplication operations

TABLE III
COMPUTATION COMPARISON

Schemes	Encryption	Decryption	Total cost
Chen et al. [35]	$(3n+3)T_{eo}+2nT_{smo}$	$T_{bpo}+6T_{eo}+4T_{smo}$	$(3n+9)T_{eo}+(2n+4)T_{smo}+T_{bpo}$
Deng et al. [41]	$(2n+3)T_{smo}+nT_{bpo}$	$T_{bpo}+T_{eo}$	$(n+1)T_{bpo}+(2n+3)T_{smo}+T_{eo}$
Hung et al. [39]	$nT_{bpo}+nT_{eo}+(n+1)T_{smo}$	$T_{bpo}+T_{smo}$	$(n+1)T_{bpo}+(n+2)T_{smo}+nT_{eo}$
He et al. [40]	$(3n+1)T_{smo}$	$2T_{smo}$	$(3n+3)T_{smo}$
Our scheme	$3T_{eo}+T_{bpo}$	$2T_{bpo}+nT_{eo}$	$3T_{bpo}+(n+3)T_{eo}$

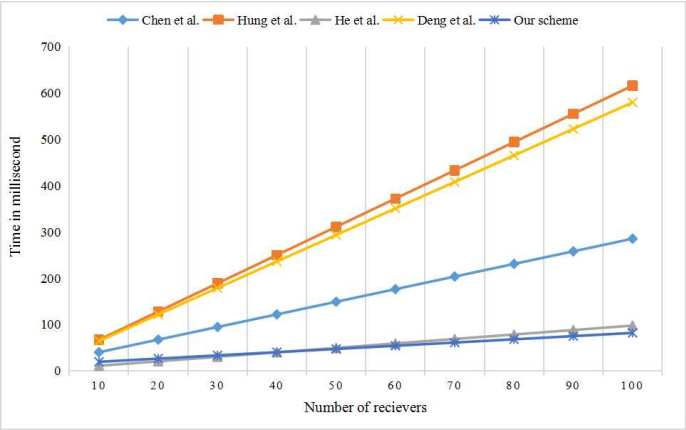


Fig. 4. Comparison of computation cost

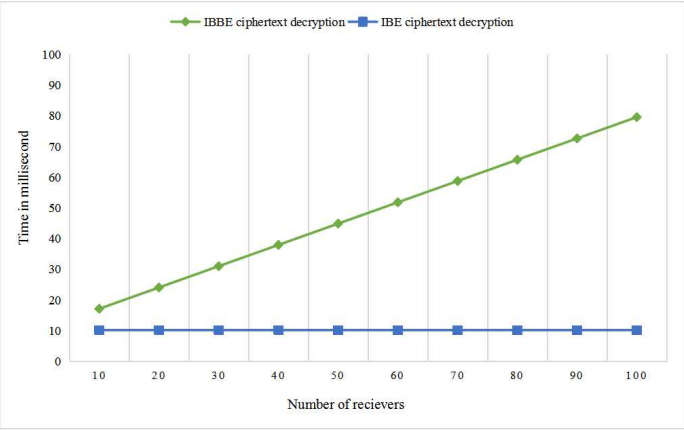


Fig. 5. Comparison of decryption cost

in the encryption phase. Here, the decryption cost is only requires two scalar multiplication operations, so the total cost is $(3n+3)T_{smo} \approx 0.9654n + 0.9654$ ms.

Finally, in our scheme, unlike the original IBBE scheme, the master private key β is owned by the sender. So the sender can directly use the private key to compute the ciphertext, and the encryption phase requires three exponentiation operations. However, in the decryption phase, because the receiver does not know the value of β, it needs to be computed based on the public key, which generates high computation cost. The decryption phase requires n exponentiation operations and two pairing operations, so the total cost of this scheme is $(n+3)T_{eo}+2T_{bpo} \approx 0.694n + 12.254$ ms. The total computation cost of the related schemes is listed in Table III. To see the comparison between our scheme and the other four schemes more intuitively, we draw a line chart in which the number of vehicles ranges from 10 to 100. According to Fig. 4, it can be seen that even if our scheme uses bilinear pairing technology, it has reached the same computational cost as He et al. [40]. As the number of receivers continues to grow, the cost of our scheme still be lower than He et al. [40]. By comparing the communication cost below, it shows that only our scheme has a fixed-size ciphertext. The ciphertext length of the other schemes, including He et al.'s scheme [40], increases linearly. So, although the scheme [40] has low cost, our scheme has better performance.

As shown in the previous analysis, the cost of the vehicle in the decryption phase of this scheme increases linearly with the number of receivers. The computing power of the OBU is also greatly improved with the development of technology, and the IBBE ciphertext decryption time in this scheme is acceptable in VANETs. A proxy server is also introduced to

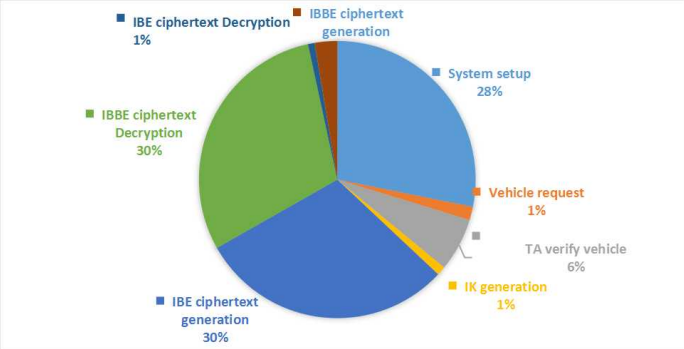


Fig. 6. The percentage of computation cost

reduce the decryption cost of the receiver further. However, the comparison scheme does not have the optimization phase introduced in our scheme. So we will analyze the decryption cost of the ciphertext before conversion and the decryption cost of ciphertext after conversion separately. From Fig. 5, we can see that the decryption cost of the vehicle is reduced significantly after the proxy server is introduced. According to the decryption phase of the IBE ciphertext, it can be known that this part only requires two pairing operations. Then the efficiency of decryption is greatly improved.

At the same time, since this scheme is a system for the vehicular networks, there will be other vehicle-related phases. we analyze the proportion of computation cost in different phases to total cost. Here, we set 100 vehicle users in the system. In Fig. 6, it can be seen that the cost of the proxy server in the ciphertext conversion phase accounts for about 30% of the entire computation cost, indicating that the cost of this part is not very low. As part of the computing tasks

TABLE IV
COMPARISON OF CIPHERTEXT LENGTH

Scheme	The ciphertext format CT	Length/byte
Chen et al. [35]	$(C_{01}, C_{02}, C_{03}, C_{11}, ..., C_{1n}, C_2)$	212+138n
Deng et al. [41]	$(C, U, V, z, g_{n-1}, ..., g_1, g_0)$	178+4n
Hung et al. [39]	$(C_1, C_2, ..., C_t, V, U, \wedge)$	102+20n
He et al. [40]	$(C_1, C_2, ..., C_t, T, v, \beta)$	102+20n
Our scheme	(CT_0, CT_1, CT_2)	484

are transferred to the proxy server, the cost of IBE ciphertext decryption is reduced. Here, the computing power of the proxy server is relatively strong. Different from TA, the number of the proxy server is not limited. There can be many proxy servers in different regions. So the computation cost of the proxy server is within the acceptable range. When there are 100 vehicles in the system, the cost of the intermediate key generation phase is about 3 ms, the cost of the IBE ciphertext generation phase is about 80 ms, and the cost of the IBE ciphertext decryption is about 2 ms. From vehicle sending the request to the decrypting, the toal cost is about 85 ms. Based on the analysis, we can conclude that the computation cost of our proposed scheme is smaller than that of the related schemes.

B. Communication Cost Analysis

Here, we have conducted a analysis of the communication cost of each scheme. We can get the communication cost by analyzing the ciphertext structure of each scheme. Here the generator of G_1 is g, which the size is 64 bytes, and the random element in group G_1 is 128 bytes. The hash function outputs a 20 bytes bit string. The size of the timestamp is 4 bytes. The comparison of communication costs is presented in Table IV.

In Chen et al. [35] scheme, the form of the ciphertext is $(C_{01}, C_{02}, C_{03}, C_{11}, C_{12}, ..., C_{1n}, C_2)$, where C_{1i} is composed of two parts, one is the output value of the hash function, and the other is the value of bilinear pairing, the length of ciphertext is $64 \times 3 + (w/8 + 128)n + 2L/8$ bytes. The length of w, L is not specified in this scheme, here we analyze it according to the security level of 80 bits and the result is $212 + 138n$ bytes. In Deng et al.'s [41] scheme, the form of the ciphertext is $(C, U, V, z, g_{n-1}, ..., g_1, g_0)$, where C is the result of the hash function H_5. The output of H_5 is a bit string of length $L1+L2$, and a 0,1-bit string w of length $L2$ is connected. Here we analyze it according to the security level of 80 bits, then the length of C is 30 bytes. Among the remaining parameters, a function $f(x)$ is constructed to decrypt the relevant parameter. The necessary parameters $g_0, ..., g_{n-1}$ of the constructor need to be sent. The length of parameters $g_0, ..., g_{n-1}$ is $4n$ bytes, so the length of ciphertext CT is $30+64\times2+20+4n = 178+4n$ bytes. In the scheme of Hung et al. [39], the ciphertext form is $(C_1, C_2, ..., C_t, V, U, \wedge)$, where C_i is the connection of the output values of the two hash functions. So the output length is $2w/8 = 20$ bytes. It is also worth noting that the parameter $V = Esk(m)$. Hung et al.'s [39] scheme did not specify the security level of the symmetric encryption. Here, the 128-bit secure AES encryption algorithm is used, so the length of V is 16 bytes. Finally, the length

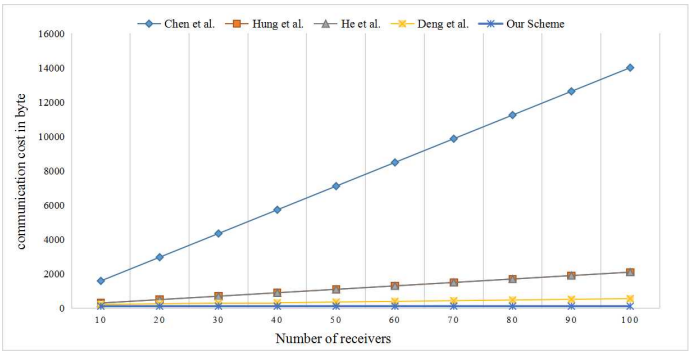


Fig. 7. Comparison of ciphertext length

of the ciphertext is $20n + 16 + 64 + 20 = 100 + 20n$ bytes. In the scheme of He et al. [40], the ciphertext form is $(C_1, C_2, ..., C_t, T, v, \beta)$, where C_i is the same length as C_i in scheme [39]. Respectively, the length of C_i is 20 bytes and the length of V is 16 bytes. Then the length of the ciphertext is $20n+16+64+20 = 100+20n$ bytes. Finally, in our scheme, the structure of ciphertext is (CT_0, CT_1, CT_2), and the length of each parameter is 128 bytes. So, the size of the ciphertext in our scheme is $128 \times 3 = 484$ bytes. As shown in Fig. 7, it can be seen intuitively that the size of the ciphertext of our scheme is smaller than the related schemes [35], [39]–[41]

VII. CONCLUSION

In widespread scenarios, where there is an infrastructural need to share secure data with multiple vehicles in VANETs, our scheme can help the TA prevent redundancies. During the encryption phase, the TA uses identity-based broadcast encryption technology to improve the encryption efficiency. At the same time, to further release the encryption burden of the TA, a proxy server is introduced to convert the original ciphertext. In terms of security, our scheme meets the special security requirements of VANETs. Compared with the existing one-to-one communication scheme, ours has more advantages as many vehicles need to interact with the TA simultaneously. In the future, we will continue to work on improving the efficiency of one-to-many communication in VANETs. Furthermore, we will try to combine more secure and lightweight technologies to construct a more efficient scheme for VANETs.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China under Grant 61872001, Grant 62011530046, and Grant U1936220 and in part by the Special Fund for Key Program of Science and Technology of Anhui Province, China under Grant 202003A05020043. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

REFERENCES

[1] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in vanets," *Vehicular Communications*, vol. 22, p. 100228, 2020.

[2] Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: a novel reputation framework for identifying denial of traffic service in internet of connected vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3901–3909, 2019.

[3] M. Shafiq, Z. Tian, A. K. Bashir, A. Jolfaei, and X. Yu, "Data mining and machine learning methods for sustainable smart cities traffic classification: A survey," *Sustainable Cities and Society*, vol. 60, p. 102177, 2020.

[4] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, and H. Duan, "A fluid mechanics-based data flow model to estimate vanet capacity," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 6, pp. 2603–2614, 2019.

[5] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Iot malicious traffic identification using wrapper-based feature selection mechanisms," *Computers & Security*, vol. 94, p. 101863, 2020.

[6] J. Cui, J. Chen, H. Zhong, J. Zhang, and L. Liu, "Reliable and efficient content sharing for 5g-enabled vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2020.

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

[8] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "Corrauc: A malicious bot-iot traffic detection method in iot network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2021.

[9] S.-J. Horng, C.-C. Lu, and W. Zhou, "An identity-based and revocable data-sharing scheme in vanets," *IEEE Transactions on Vehicular Technology*, 2020.

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

[11] J. Cui, X. Zhang, H. Zhong, J. Zhang, and L. Liu, "Extensible conditional privacy protection authentication scheme for secure vehicular networks in a multi-cloud environment," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1654–1667, 2020.

[12] H. Zhong, J. Ni, J. Cui, J. Zhang, and L. Liu, "Personalized location privacy protection based on vehicle movement regularity in vehicular networks," *IEEE Systems Journal*, pp. 1–12, 2021.

[13] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682–4696, 2020.

[14] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, "Data communication in vanets: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016.

[15] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2007, pp. 200–215.

[16] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security (TISSEC)*, vol. 9, no. 1, pp. 1–30, 2006.

[17] D. Nuñez, I. Agudo, and J. Lopez, "Proxy re-encryption: Analysis of constructions and its application to secure access delegation," *Journal of Network and Computer Applications*, vol. 87, pp. 193 – 209, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1084804517301078

[18] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing*, pp. 1–1, 2016.

[19] H. Deng, Q. Wu, B. Qin, W. Susilo, J. Liu, and W. Shi, "Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015, pp. 393–404.

[20] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Annual international cryptology conference*. Springer, 2001, pp. 213–229.

[21] U. Javaid, M. N. Aman, and B. Sikdar, "Drivman: Driving trust management and data sharing in vanets with blockchain and smart contracts," in *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. IEEE, 2019, pp. 1–5.

[22] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, H. Duan, and Q. Zeng, "Accessibility analysis and modeling for iov in an urban scene," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4246–4256, 2020.

[23] M. Sookhak, F. R. Yu, and H. Tang, "Secure data sharing for vehicular ad-hoc networks using cloud computing," in *Ad Hoc Networks*. Springer, 2017, pp. 306–315.

[24] J. Liu, X. Wang, G. Yue, and S. Shen, "Data sharing in vanets based on evolutionary fuzzy game," *Future Generation Computer Systems*, vol. 81, pp. 141–155, 2018.

[25] J. Pan, J. Cui, L. Wei, Y. Xu, and H. Zhong, "Secure data sharing scheme for vanets based on edge computing," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–11, 2019.

[26] J. Shen, T. Zhou, J. Lai, P. Li, and S. Moh, "Secure and efficient data sharing in dynamic vehicular networks," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8208–8217, 2020.

[27] A. Fiat and M. Naor, "Broadcast encryption," in *Annual International Cryptology Conference*. Springer, 1993, pp. 480–491.

[28] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2009, pp. 171–188.

[29] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in *Theory of Cryptography Conference*. Springer, 2011, pp. 253–273.

[30] D. Boneh, B. Waters, and M. Zhandry, "Low overhead broadcast encryption from multilinear maps," in *Annual Cryptology Conference*. Springer, 2014, pp. 206–223.

[31] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 679–693, 2015.

[32] A. Ge and P. Wei, "Identity-based broadcast encryption with efficient revocation," in *IACR International Workshop on Public Key Cryptography*. Springer, 2019, pp. 405–435.

[33] J. Li, Q. Yu, and Y. Zhang, "Identity-based broadcast encryption with continuous leakage resilience," *Information Sciences*, vol. 429, pp. 177–193, 2018.

[34] J. Kim, S. Camtepe, W. Susilo, S. Nepal, and J. Baek, "Identity-based broadcast encryption with outsourced partial decryption for hybrid security models in edge computing," in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, 2019, pp. 55–66.

[35] L. Chen, J. Li, and Y. Zhang, "Anonymous certificate-based broadcast encryption with personalized messages," *IEEE Transactions on Broadcasting*, vol. 66, no. 4, pp. 867–881, 2020.

[36] J.-S. Weng, J. Weng, Y. Zhang, W. Luo, and W. Lan, "Benbi: Scalable and dynamic access control on the northbound interface of sdn-based vanet," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 822–831, 2018.

[37] E. E. Bunese, E. Todt, and L. C. P. Albini, "Vanet security through group broadcast encryption," *Journal of Computer and Communications*, vol. 8, no. 8, pp. 22–35, 2020.

[38] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2000, pp. 259–274.

[39] Y.-H. Hung, S.-S. Huang, Y.-M. Tseng, and T.-T. Tsai, "Efficient anonymous multireceiver certificateless encryption," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2602–2613, 2015.

[40] D. He, H. Wang, L. Wang, J. Shen, and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Computing*, vol. 21, no. 22, pp. 6801–6810, 2017.

[41] L. Deng, "Anonymous certificateless multi-receiver encryption scheme for smart community management systems," *Soft Computing*, vol. 24, no. 1, pp. 281–292, 2020.

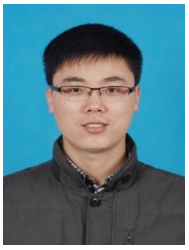
[42] S. Zeng, Y. Chen, S. Tan, and M. He, "Concurrently deniable ring authentication and its application to lbs in vanets," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, pp. 844–856, 2017.

[43] M. Raya and J.-P. Hubaux, "The security of vanets," in *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 93–94. [Online]. Available: https://doi.org/10.1145/1080754.1080774

[44] Z. Jianhong, X. Min, and L. Liying, "On the security of a secure batch verification with group testing for vanet," *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.

Hong Zhong was born in Anhui Province, China, in 1965. She received her PhD degree in computer science from University of Science and Technology of China in 2005. She is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). She has over 150 scientific publications in reputable journals (e.g. IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Mobile Computing, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Multimedia, IEEE Transactions on Vehicular Technology, IEEE Transactions on Network and Service Management, IEEE Transactions on Cloud Computing and IEEE Transactions on Big Data), academic books and international conferences.

Shuo Zhang is now a research student in the School of Computer Science and Technology, Anhui University. Her research focuses on the security of vehicle ad hoc networks.



Jie Cui was born in Henan Province, China, in 1980. He received his Ph.D. degree in University of Science and Technology of China in 2012. He is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has over 120 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Mobile Computing, IEEE Transactions on Computers, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Cloud Computing and IEEE Transactions on Multimedia), academic books and international conferences.

Lu Wei is currently a Ph.D. student in the School of Computer Science and Technology, Anhui University, Hefei, China. His research interests include vehicular ad hoc networks and applied cryptography. He has nearly 10 scientific publications in reputable journals (e.g. IEEE Transactions on Information Forensics and Security, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Intelligent Transportation Systems).

Lu Liu is the Professor of Informatics and Head of School of Informatics in the University of Leicester, UK. Prof Liu received the Ph.D. degree from University of Surrey, UK and MSc in Data Communication Systems from Brunel University, UK. Prof Liu's research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society (BCS).