Attribute-Based Proxy Re-encryption with Privacy Protection for Message Dissemination in VANET

Qiuming Liu, Zhexin Yao, Zhen Wu(✉), and Zeyao Xu

Jiangxi University of Science and Technology, School of Software Engineering, Nanchang, China
{liuqiuming,zxyao,6720200926}@jxust.edu.cn, wuzhen35@163.com

Abstract. Message dissemination between the infrastructures and vehicles is the most common operation in the vehicular ad hoc network (VANET). However, only some specific vehicles can access the disseminated message with keys. When other vehicles do need to access this message, they have to send requests to the infrastructures like the trusted authority (TA). TA negotiates with this vehicles and may produce many encryption redundancies for the same message, which costs extra communication and computation overhead. Thus, the proposed scheme adopts attribute-based proxy re-encryption (ABPRE) with privacy protection, which is suitable for one-to-many communication mode in VANET. By shifting the re-encryption work to roadside units (RSUs) and cloud servers, the computation overhead of the trusted authority (TA) is significant reduced. Besides, pseudonym and batch verification are introduced in authentication work to ensure the security. The security analysis shows that our scheme meets the secure requirements of VANET. The simulation evaluates the cost of each phase, which demonstrated that the scheme has a low computation cost and reduces the redundancy work.

Keywords: Vehicular ad hoc network (VANET) · Attribute-based proxy re-encryption (ABPRE) · Pseudonym · Message dissemination

1 Introduction

Vehicular ad hoc network (VANET) technology has been adopted in the modern transport system to improve traffic security and driving experience effectively [1]. VANET consists of vehicles and infrastructures like roadside units (RSUs) and trusted authority (TA). Vehicles are equipped with the onboard unit (OBU) plays the role of information generator and message transmitter. Message may include traffic information, road situation, and vehicle's status. Meanwhile, the

Supported by Natural Science Foundation of Jiangxi Province (Grant No. 20202BAB212003), Science and technology project of Jiangxi Provincial Department of Education(GJJ210853).

S. Goel et al. (Eds.): ICDF2C 2022, LNICST 508, pp. 387–402, 2023.
https://doi.org/10.1007/978-3-031-36574-4_23

vehicle can receive messages from other vehicles and infrastructures [2]. With real-time data sharing, the transport agency can predict some potential traffic accidents and vehicles can get the latest surrounding traffic situation.

As we all know, vehicles have the feature of high mobility and the communication among vehicles is conducted in the open wireless network [3]. Hence, security and efficiency must be ensured during message exchange. The security of VANET means the validity and privacy of participating entities must be protected. Besides, due to the mobility of vehicles, VANET must realize efficient data sharing. There have been many schemes proposed to improve the security and efficiency of VANET in message dissemination [4].

The communication modes in VANET can be divided into three kinds: one-to-one, one-to-many, and many-to-many. However, in the reality, one-to-many and many-to-many are formed by one-to-one mode [5]. Under one-to-one mode, the same message may has been encrypted for many times to match the different receivers. The computation and communication cost is quite unworthy and should be avoided. To solve this problem, Chen et al. [6] proposed a scheme that broadcasts ciphertext with a shared key to achieving one-to-many communication. Unfortunately, the encryption of ciphertext is based on bilinear maps, which causes a huge computation cost. Cui et al. [7] applied group key encryption with the method of self-healing key distribution in the scheme. Though the scheme using the elliptic curve cryptosystem to improve authentication efficiency, the risk of sharing the same group key in the same area shouldn't be ignored.

Ciphertext-policy attribute-based encryption (CP-ABE) can realize one-to-many encryption. CP-ABE has been applied for secure authentication and efficient communication in many VANET schemes. With CP-ABE, the data owner encrypts messages by access policy, and only receivers whose attributes satisfy the policy can get the plaintext. Liu et al. [8] proposed a message dissemination scheme in VANET with CP-ABE, which realizes secure and efficient communication. Based on that, Li et al. [9] proposed a VANET scheme adopting ABE to ensure security and privacy. Besides, the scheme outsources encryption and decryption to cloud servers to reduce computation overhead. Similarly, Horng et al. [10] proposed a CP-ABE data sharing scheme which also outsources encryption and decryption to third party.Furthermore, the scheme adopted identity revocation to keep secure authentication.

Above all, attribute-based encryption with fine-grained access control can be well applied with data dissemination in VANET. But the schemes mentioned above didn't consider the situation of ciphertext re-encryption.Consider this scenario (see Fig. 1): Vehicle A uploads a traffic message encrypted by access policy ('RSU1' and 'Jiefang Avenue') or ('RSU2' and 'Renmin Road'), which indicates vehicles in RSU1's area on the Jiefang Avenue or in RSU2's area on the Renmin Road can access the message. Vehicle B with attributes ('RSU2', 'Nanjing Road'), who will pass by Renmin Road, can't decrypt the ciphertext. But if the ciphertext includes the traffic accident information happened in Renmin Road, transport agency do need to disseminate the message to surrounding vehicles including vehicles. Otherwise, vehicles like B knowing nothing will drive into the Renmin Road normally, causing the traffic situation more serious. To avoid

that, the trivial solution is that transport agency request data owner A decrypts the original ciphertext and re-encrypts with designed access policy for vehicles like B. However, in this method, with the number of vehicles growing, the re-encryption phase would cost huge computation and the ciphertext would be encrypted redundantly.

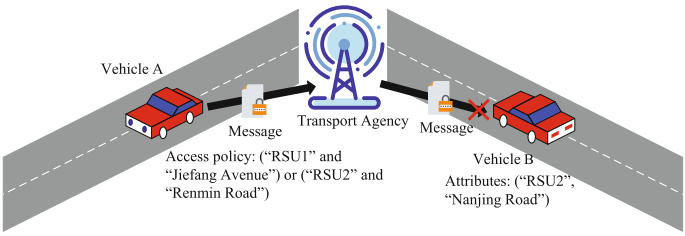

Fig. 1. Example of data sharing in VANET with ABE.

To improve efficiency, proxy re-encryption is introduced during data sharing. Ciphertext can be converted by proxy re-encryption. Zhong et al. [11] proposed a broadcast re-encryption scheme, which realizes the transformation from identity-based broadcast encryption (IBBE) to identity-based encryption (IBE). However, the design of the whole system sharing the same secret parameters r_1 and r_2 makes the privacy feeble. Liu et al. [12] proposed an attribute-based proxy re-encryption (ABPRE) scheme with multi-RSU, which achieves an efficient seamless handover and ciphertext conversion. However, this scheme ignores message verification and privacy protection. Furthermore, Ge et al. [13] proposed a verifiable and fair ABPRE scheme, which focuses on ciphertext verification during re-encryption, while this scheme ignores the message authentication during the uploading process.

Therefore, a scheme that adopts attribute-based proxy re-encryption (ABPRE) with privacy protection is proposed. In VANET, numbers of RSUs are distributed along the road in the coverage of TA. The proposed scheme makes RSUs and cloud servers conduct re-encryption work to reduce the computation overhead of TA. RSU also plays the role of attribute management in its coverage. Besides, to ensure privacy protection and security, pseudonyms and batch verification are adopted. The primary contributions of this paper are summarized as follows:

- To present an efficient and secure communication mode, a scheme that adopts attribute-based proxy re-encryption with privacy protection is proposed. Besides, batch verification is introduced during the message verification to improve working efficiency further.
- The detailed structure of the proposed scheme is introduced with the operation procedure. The security analysis proves that the scheme is confidential, privacy-preserving, and traceable.

– Through the performance evaluation and comparison, it is remarkable that the proposed scheme can achieve efficient one-to-many communication with privacy protection.

The rest structure of this paper is shown below. Section 2 introduces the preliminary knowledge, components' functions and security requirements. The detailed communication procedures are introduced in Sect. 3. Section 4 demonstrates the comprehensive security analysis of the proposed scheme. The comparison of different schemes and the simulation results are described in Sect. 5. Finally, Sect. 6 gives the summary of this paper.

2 Preliminaries

This section first introduces the mathematical knowledge adopted in this paper: linear secret sharing scheme, attribute-based proxy re-encryption. Then, the communication model is proposed with the description of the entities. Meanwhile, the security requirements are listed according to the communication model.

2.1 Linear Secret Sharing Schemes

A linear secret sharing scheme (LSSS) Π over a set of parties $\mathcal{P}$ (over $\boldsymbol{Z}_p$) is linear if:

– The share of each party is a vector over $\boldsymbol{Z}_p$.
– There exists a $l \times n$ matrix m and a function ρ, where $\rho(j) \in \mathcal{P}$ denotes jth row of M , $j \in \{1, 2, \cdots l\}$. Let r be a secret number and random numbers $r_2, r_3, \cdots, r_n \in \boldsymbol{Z}_p$. Construct a vector $\vec{v} = (r, r_2, \cdots, r_n)$, then $M \cdot \vec{v}$ is a vector of l shares of r according to Π and $M_j \cdot \vec{v}$ is a share belonging to $\rho(j)$.

Suppose that A is an authorized attribute set and J is a constant set that $J = \{j : \rho(j) \in A\} \subset \{1, 2, \cdots l\}$. The linear reconstruction of LSSS states that there exists a vector $\vec{\theta}$, such that $\{M_j\}_{j \in J} \cdot \vec{\theta} = (1, 0, \cdots, 0)^T$, $\vec{v} \cdot \{M_j\}_{j \in J} \cdot \vec{\theta} = r$.

2.2 Attribute-Based Proxy Re-encryption

Attribute-based proxy re-encryption (ABPRE) is an algorithm that combined CP-ABE and proxy encryption, which can achieve flexible access control and efficient ciphertext conversion [13]. The proposed scheme utilizes ABPRE in VANET for secure traffic information transmission.

– $Setup(\lambda, \boldsymbol{U})$: It takes the security parameter λ and the attribute universe $\boldsymbol{U}$ as input. Algorithm $Setup$ generates system public parameter pp and master secret key msk.
– $Key\_Gen(msk, \boldsymbol{A})$: It takes the master secret key msk and attribute set $\boldsymbol{A}$ as input. Then, it outputs secret key sk based on $\boldsymbol{A}$ for requesters.

- $Enc(m, (\boldsymbol{M}, \rho))$: It takes message m and access policy $(\boldsymbol{M}, \rho)$ as input and generates ciphertext CT based on $(\boldsymbol{M}, \rho)$.
- $Re\_Key\_Gen(sk, (\boldsymbol{M}', \rho'))$: This step inputs sk based on attribute and another access policy $(\boldsymbol{M}', \rho')$. Then, it generates a re-encrypted key rk to re-encrypt original ciphertext.
- $Re\_Enc(rk, CT)$: Based on re-encrypted key rk, it coverts the original ciphertext CT to re-encrypted ciphertext CT' without revealing plaintext.
- $Dec1(CT, sk)/Dec2(CT', sk)$: This step decrypts original ciphertext or re-encrypted ciphertext with attribute-based key sk and outputs message m.

2.3 Communication Model

The proposed vehicular network contains four entities including trusted authority (TA), roadside units (RSUs), cloud servers (CS), and vehicles carried with the on-board unit (OBU), where vehicles connected to other vehicles or RSUs by the dedicated short-range communication protocol (DSRC). Figure 2 illustrates the communication framework and the details of entities are described as follows.

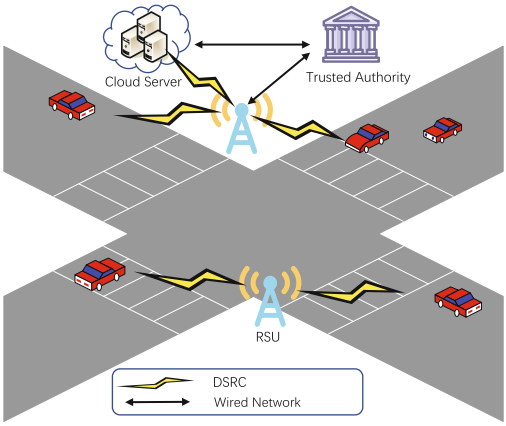

Fig. 2. Data sharing model in VANET

- TA: TA is considered a trusted traffic center with sufficient computing power and storage space. TA initiates the system by generating global parameters and takes charge of vehicle's registration. TA generates pseudonyms and secret keys for vehicles. Besides, TA can trace the real identities of vehicles for partial anonymity.
- RSU: RSUs are distributed along the road. RSU is also a gateway between vehicles and upper entities in the system. RSU takes charge of traffic message collection and dissemination in its coverage. In the network, RSU also plays the role of generating attribute-based key and re-encryption key for vehicles.

- CS: CS is a semi-trusted third party and equipped with sufficient computing power and huge storage space. In the proposed scheme, CS is also considered as a proxy server, which achieves ciphertext conversion without disclosing plaintext by re-encryption key from RSU.
- Vehicle: Each vehicle equips with an OBU to collect surrounding traffic information and transfer it to neighboring RSUs and other vehicles by DSRC. In the proposed scheme, vehicles carry a set of attributes and other private data, e.g., secret keys, pseudonyms.

2.4 Security Requirement

Security and privacy are two basic preconditions in a stable VANET. Besides, the proposed scheme should also meet other requirements listed below.

- Message Confidentiality: The message OBU collected may contain some sensitive information. Thus, the message must keep confidential during the communication.
- Message Authentication and Integrity: Receivers must verify the validity of the message transmitted in the VANET. On the one hand, the source of the message must be authenticated to ensure the validity. On the other hand, it is important to ensure the integrity of the message to prevent forgery.
- Identity Protection: Vehicles would transmit message with identity information in the public channel continuously. To protect identity privacy, the vehicle uses pseudonym instead of real identity.
- Traceability: Vehicles broadcast message and requests in VANET. But if the vehicle exists some malicious behavior, the real identity of the vehicle should be designed to traceable.
- Other Common Attacks: The scheme should also have the ability to resist some common attacks, such as replay attacks, simulation attacks and so on.

3 The Proposed Scheme

In this section, the procedures of the proposed scheme are described. TA plays the role of manager in the whole communication system. To reduce the computation pressure, TA's management area is divided into multiple pieces by RSUs. RSU takes charge of message authentication and assists re-encryption working in its coverage. Vehicle as the traffic information collector and receiver must register with TA and RSU to get further communication service. For secure and efficient message dissemination, traffic information is encrypted by ABE before uploading. And then during the dissemination, if the receiver's attribute set doesn't satisfy the designed access policy, it couldn't access the ciphertext. To deal with that, the proposed scheme adopts proxy re-encryption, where RSU generates re-encrypted key and CS utilizes the key for ciphertext re-encryption. The notations utilized in the proposed scheme are listed in in the Table 1.

Table 1. List of notations

Notations	Definition	Notations	Definition
$\boldsymbol{G}$, $\boldsymbol{G}_T$	Multiplicative group	key_{TA}	Private key of TA
r_1, r_2	Master private key	key_{id}	Identity-based key of vehicle
g	A generator of group G	key_{att}	Attribute-based key of vehicle
p	Large prime number	key_{re}	Key for re-encryption
Q_1, Q_2	Random generator in G	t_1, t_2	time stamp
$h(\cdot)$	One-way hash function	$\boldsymbol{A}, \boldsymbol{S}$	Attribute set
CT	Original ciphertext	CT'	Re-encrypted ciphertext

3.1 System Initialization

TA initializes the system by generating system public parameter pp and master secret key key_{TA} based on security number λ and attribute universe $\boldsymbol{U}$.

- TA generates two multiplicative groups $\boldsymbol{G}$ and $\boldsymbol{G}_T$ with the same prime order p, where g is a generator of $\boldsymbol{G}$. These two groups satisfy the bilinear map $e : \boldsymbol{G} \times \boldsymbol{G} \rightarrow \boldsymbol{G}_T$.
- TA picks two secret numbers $r_1, r_2 \in \boldsymbol{Z}_p$, $r_1 \neq r_2$ and computes auxiliary parameters $pub_1 = g^{r_1}$, $pub_2 = g^{r_2}$. Then, TA stores master secret key as $key_{TA} = (r_1, r_2)$.
- TA chooses two random generators $Q_1, Q_2 \in \boldsymbol{G}$ and five cryptographic hash functions: $h_1 : \boldsymbol{G} \rightarrow \{0,1\}^*$, $h_2, h_3 : \{0,1\}^* \rightarrow \boldsymbol{Z}_p$, $h_4 : \boldsymbol{G}_T \rightarrow \{0,1\}^*$ and $h_5 : \boldsymbol{G}_T \rightarrow \boldsymbol{Z}_p$.
- For each attribute x of $\boldsymbol{U}$, TA chooses a number $h_x \in \boldsymbol{Z}_p$ and computes $H_x = g^{h_x}$. Then, TA publishes $pp = (e, g, p, pub_1, pub_2, Q_1, Q_2, \{H_x\}_{\forall x \in U}, h_i(\cdot), \Delta t)$ to all entities, where Δt means the expected delay.

After the initialization of TA, RSU generates secret key key_{RSU} and publish its parameter rpp in its coverage.

- RSU chooses two random exponents $\alpha, a \in \boldsymbol{Z}_p$, and sets its secret key as $key_{RSU} = g^{\alpha}$.
- RSU computes $e(g,g)^{\alpha}$, g^a, and publishes parameter $rpp = (e(g,g)^{\alpha}, g^a)$.

3.2 Key Generation

Before joining the communication system, vehicle must register with TA. Vehicle v sends its unique real identity rid to TA. Then, based on the vehicle's identity, TA generates corresponding pseudo identity pid and identity-based private key key_{id}.

- TA picks a random number $k \in \boldsymbol{Z}_p$ and computes $pid_1 = g^k$, $pid_2 = rid \oplus h_1(pub_1^k)$. Set pseudo identity as $pid = (pid_1, pid_2, vp)$, where vp is the valid period of pid.

- Based on the pid, TA computes $sk_1 = pid_1^{r_1}$, $sk_2 = Q_1^{r_2 h_2(pid_1||pid_2||vp)} \cdot Q_2^{h_3(pid_1)}$. Set identity-based private key as $key_{id} = (sk_1, sk_2)$ for vehicle v.
- TA transmits tuple (pid, key_{id}) to vehicle in a secure channel and vehicle stores it in tamper-proof devices.

When vehicle v enters an RSU coverage, it picks a valid pid from identity pool. Then, v sends pid and its attribute set $\boldsymbol{A}$ to the RSU to request for attribute-based key key_{att}.

- RSU maintain a list of vehicles' pseudonyms and attribute sets. Receiving the key request from the vehicle, RSU first checks the validity of pid. Then, RSU checks whether pid and attribute set $\boldsymbol{A}$ already existing in the list. If not, RSU continues the next procedure.
- RSU picks a random number $b \in \boldsymbol{Z}_p$ and computes attribute-based key as $key_{att} = (\boldsymbol{A}, K_1 = g^{\alpha} g^{ab}, K_2 = g^b, \forall x \in \boldsymbol{A}, K_x = H_x^b)$.
- RSU sends key_{att} to the vehicle in a secure channel.

3.3 Message Encryption

To ensure confidentiality and integrity, the message must be encrypted and signed. Vehicle encrypts message by CP-ABE and signs the message with Algorithm 1.

Algorithm 1. Signature Algorithm $Sign()$

Input: Ciphertext CT; Identity based key $key_{id} = (sk_1, sk_2)$; Timestamp t_1;
Output: Signature σ;

1: compute hash value $w = h_3(CT||t_1)$;
2: compute signature $\sigma = sk_1 \cdot sk_2^w$;
3: **return** σ;

- v defines access policy $(\boldsymbol{M}, \rho)$, where $\boldsymbol{M}$ is a $l \times n$ matrix and ρ is a function associate each row of matrix to an attribute.
- v chooses a vector $\vec{\boldsymbol{u}} = (r, y_2, \cdots, y_n)^T \in \boldsymbol{Z}_p$, where r is the main security number. Then, vehicle computes $\vec{\boldsymbol{\lambda}} = \boldsymbol{M} \cdot \vec{\boldsymbol{u}} = \{\boldsymbol{M}_j\} \cdot \vec{\boldsymbol{u}} = (\lambda_1, \lambda_2, \cdots, \lambda_l)^T$, in which $\boldsymbol{M}_j$ represents jth row of matrix, $j \in [1, l]$.
- v randomly selects $b_j \in \boldsymbol{Z}_p$ for each $\boldsymbol{M}_j$, $j \in [1, l]$, and computes ciphertext as $CT = ((\boldsymbol{M}, \rho), C = m \oplus H(e(g, g)^{\alpha r}), C_1 = g^r, C_{2,j} = g^{a\lambda_j} H_{\rho(j)}^{-b_j}, C_{3,j} = g^{b_j}, j \in [1, l])$.
- v picks a valid pid and corresponding key_{id}, then signs ciphertext with Algorithm 1 generating signature σ. Vehicle sends (CT, σ, pid, t_1) to local RSU, where t_1 is timestamp to against replay attack.

3.4 Message Verification

RSU receives (CT, σ, pid, t_1) from vehicle v. First, RSU checks the validity of timestamp t_1. If $t_r - t_1 < \Delta t$, where t_r is the time the message arriving, RSU continues next verification steps; or, RSU would reject the message. Then, RSU check the validity of pseudo identity with vp. To keep efficient operation and

reduce computation overhead, RSU introduces batch verification technology. Assume that RSU receives messages as $\{CT_i, \sigma_i, pid_i, t_{i,1}\}_{i=1}^{n}$ and verifies these messages by Algorithm 2. If the result of verification is true, RSU transmits messages to CS to store. Otherwise, invalid signature search algorithm [14] is adopted.

Algorithm 2. Verification Algorithm $Verify()$

Input: messages $\{CT_i, \sigma_i, pid_i, t_{i,1}\}_{i=1}^{n}$; parameters (Q_1, Q_2, pub_1, pub_2);
Output: $True$ or $False$;

1: choose a vector $\vec{\boldsymbol{a}} = (a_1, a_2, \cdots, a_k)^T$,$a_i \in [1, 2^d]$;
2: check whether equation

$$\begin{aligned} e(\sum_{i=1}^{n} (a_i)^2 \sigma_i, g) &= e(\sum_{i=1}^{n} (a_i)^2 (sk_{i,1} \cdot sk_{i,2}^{w_i}), g) \\ &= e(\sum_{i=1}^{n} a_i pid_{i,1} Q_2^{h_3(CT_i||t_{i,1})h_2(pid_{i,1})}, pub_1) \\ &\cdot e(\sum_{i=1}^{n} a_i Q_1^{h_3(CT_i||t_{i,1})h_3(pid_{i,1}||pid_{i,2}||vp_i)}, pub_2) \end{aligned} \tag{1}$$

holds or not;
3: **return** $True$ or $False$;

3.5 Message Re-encryption

Vehicle sends its message request to RSU. If the vehicle's attributes don't satisfy the ciphertext's access policy, RSU then generates re-encryption key for the vehicle.

- RSU defines another access policy $(\boldsymbol{M}', \rho')$ which satisfies vehicle's attribute-based key $key_{att} = (\boldsymbol{A}, K_1 = g^{\alpha} g^{ab}, K_2 = g^b, \forall x \in \boldsymbol{A}, K_x = H_x^b)$.
- RSU randomly chooses $O \in \boldsymbol{G}_T$ and encrypts O with policy $(\boldsymbol{M}', \rho')$. The encryption procedure is the same as message encryption in Sect. 3.3. Set the ciphertext of O as C_0.
- RSU computes $\varphi = h_5(O)$ and sets re-encryption key as $key_{re} = (\boldsymbol{S}, RK_1 = K_1^{\varphi}, RK_2 = K_2^{\varphi}, \forall x \in \boldsymbol{S}, RK_x = K_x^{\varphi}, C_0)$, where $\boldsymbol{S}$ is the attribute set of RSU, and then RSU sends key_{re} to CS.

Once receiving re-encryption key key_{re} , CS re-encrypts the requested ciphertext. After a conversion without disclosing the plaintext, the re-encrypted ciphertext could be decrypted by initial requester.

- CS picks the original ciphertext CT in database. Let $\boldsymbol{J} = \{j | \rho(j) \in \boldsymbol{S}\} \subset \{1, \cdots, l\}$ be a constant set which denotes attribute satisfies access policy. Then, there exists a vector $\vec{\boldsymbol{\theta}} = (\theta_1, \theta_2, \ldots, \theta_j)^T$, $j \in \boldsymbol{J}$, $\theta_j \in \boldsymbol{Z}_p$, which

satisfies $\sum_{j\in \boldsymbol{J}} \boldsymbol{M}_j \vec{\boldsymbol{\theta}} = (1, 0, \ldots, 0)^T$. CS computes

$$\begin{aligned} C_p &= \frac{e(C_1, RK_1)}{\prod\limits_{j\in J} \left(e(C_{2,j}, RK_2) e(C_{3,j}, RK_x)\right)^{\theta_j}} \\ &= \frac{e(g^r, (g^{\alpha} g^{ab})^{\varphi})}{\prod\limits_{j\in J} \left(e(g^{a\lambda_j} H_{\rho(j)}^{-b_j}, g^{b\varphi}) e(g^{b_j}, H_x^{b\varphi})\right)^{\theta_j}} \\ &= e(g, g)^{\alpha r \varphi}. \end{aligned} \tag{2}$$

- Set $C' = C$, $C_1{}' = C_1$ and construct re-encrypted ciphertext as $CT' = ((\boldsymbol{M}', \rho'), C', C_1{}', C_0, C_p)$.
- CS utilizes Algorithm 1 to generate signature σ' of CT' and disseminates the re-encrypted message (CT', σ', pid, t_2) to the vehicles.

The re-encryption procedure can be summarized as Algorithm 3 describing the calculation and transmission details.

Algorithm 3. Ciphertext Re-encryption Algorithm

Input: Vehicles key_{att}; RSU attribute set $\boldsymbol{S}$; Ciphertext CT;
Output: Re-encrypted ciphertext CT';

if $R(\boldsymbol{A}, (\boldsymbol{M}, \rho)) = 0$ **then**
  $//R(\boldsymbol{A}, (\boldsymbol{M}, \rho)) = 0$ means $\boldsymbol{A}$ doesnt meet access policy $(\boldsymbol{M}, \rho)$.
  Define another policy $(\boldsymbol{M}', \rho')$;
else
  Attributes satisfy access policy, stop re-encryption!
end if
if $R(\boldsymbol{A}, (\boldsymbol{M}', \rho')) = 1$ **then**
  Randomly choose $O \in \boldsymbol{G}_T$; $Enc(O, (\boldsymbol{M}', \rho')) \rightarrow C_0$;
  Compute $\varphi = h_5(O)$,$RK_1 = K_1^{\varphi}, RK_2 = K_2^{\varphi}, RK_x = K_x^{\varphi}$;
  Set $key_{re} = (\boldsymbol{S}, RK_1, RK_2, \forall x \in \boldsymbol{S}, RK_x, C_0)$;
end if//Re-encryption key generation finished.
// Then, RSU transmits re-encryption key to CS.
if $R(\boldsymbol{S}, (\boldsymbol{M}, \rho)) = 1$ **then**
  Find $\boldsymbol{J} = \{j | \rho(j) \in \boldsymbol{S}\} \subset \{1, \cdots, l\}$;
  Compute $\sum_{j\in \boldsymbol{J}} \boldsymbol{M}_j \vec{\boldsymbol{\theta}} = (1, 0, \ldots, 0)^T \rightarrow \vec{\theta}$;
  Compute $C_p = \frac{e(C_1, RK_1)}{\prod\limits_{j\in J} \left(e(C_{2,j}, RK_2) e(C_{3,j}, RK_x)\right)^{\theta_j}}$;
end if
Set $C' = C$,$C_1{}' = C_1$;
return $CT' = ((\boldsymbol{M}', \rho'), C', C_1{}', C_0, C_p)$;

3.6 Message Decryption

In order to describing the decryption more specifically, the proposed scheme divides this procedure into two types, the decryption of original ciphertext and the decryption of re-encrypted ciphertext.

1) Vehicle receives original ciphertext (CT, σ, pid, t_1) from CS. Suppose that vehicle's attribute-based key is $key_{att} = (\boldsymbol{A}, K_1, K_2, \forall x \in \boldsymbol{A}, K_x)$ and attribute set $\boldsymbol{A}$ meets the access policy $(\boldsymbol{M}, \rho)$.
   - Vehicle verifies the integrity of the message by Algorithm 2 proposed in Sect. 3.4 and if the result is true, carries out the next procedure.
   - Let $J = \{j | \rho(j) \in \boldsymbol{A}\} \subset \{1, \cdots, l\}$ be a constant set which denotes attribute satisfies access policy.Then, find a vector $\vec{\boldsymbol{\theta}} = (\theta_1, \theta_2, \ldots, \theta_j)^T$, $j \in \boldsymbol{J}$,$\theta_j \in \boldsymbol{Z}_p$, which satisfies $\sum_{j \in \boldsymbol{J}} \boldsymbol{M}_j \vec{\boldsymbol{\theta}} = (1, 0, \ldots, 0)^T$.
   - Due to $(\vec{\boldsymbol{\lambda}})^T \cdot \vec{\boldsymbol{\theta}} = r$, Vehicle computes

$$\begin{aligned} \Theta &= \frac{e(C_1, K_1)}{\prod_{j \in J} \left(e(K_2, C_{2,j}) e(K_{\rho(j)}, C_{3,j})\right)^{\theta_j}} \\ &= \frac{e(g^r, g^{\alpha} g^{ab})}{\prod_{j \in J} \left(e(g^{a\lambda_j} H_{\rho(j)}^{-b_j}, g^b) e(g^{b_j}, H_x^b)\right)^{\theta_j}} \\ &= e(g, g)^{\alpha r} \end{aligned} \tag{3}$$

   and gets the original content by $m = C \oplus h_4(\Theta)$.
2) Vehicle receives re-encrypted message (CT', σ', pid, t_2) and checks the integrity of the message by Algorithm 2 first. Then, vehicle decrypts CT' by following steps.
   - Vehicle utilizes key_{att} to decrypt ciphertext C_0 and gets the result of decryption O. The decryption procedure is the same as the description above.
   - Then vehicle computes $\varphi = h_5(O)$ and $\Theta = (C_p)^{\frac{1}{\varphi}}$. After that, the original plaintext is $m = C' \oplus h_4(\Theta)$.

4 Security Analysis

In this section, the security analysis is presented. Based on the security requirement proposed in Sect. 2.4, the analysis shows the realization of security in the proposed scheme. Let's first introduce Computational Diffie-Hellman problem (CDHP) on Definition 1 and Discrete Logarithm assumption (DLA) on Definition 2.

Definition 1. *Given a cyclic group $\boldsymbol{G}$ with the order p and generator g. For $g, g^a, g^b \in \boldsymbol{G}$, the goal of CDHP is to find $g^{ab} \in \boldsymbol{G}$. The CDHP holds in $\boldsymbol{G}$, if there is no algorithm $\mathcal{B}$ who can output g^{ab} in a probabilistic polynomial time (PPT) with probability at least ε as: $\mathcal{P}r[g^{ab} \leftarrow \mathcal{B}(g, g^a, g^b) : a, b \in \boldsymbol{Z}_p] \geq \varepsilon$.*

Definition 2. *Based on a bilinear tuple $(e, \boldsymbol{G}, \boldsymbol{G}_T, g, g^{\beta}, p)$, $\beta \in \boldsymbol{Z}_p$, the DLA means that the time for an adversary $\mathcal{A}$ to find the integer β with the advantage of a probabilistic polynomial time (PPT) is negligible. Formally, the advantage of a PPT adversary $Adv_{DLA} = \mathcal{P}r(\mathcal{A}(e, \boldsymbol{G}, \boldsymbol{G}_T, p, g, g^{\beta}) = \beta)$ is negligible.*

- Message confidentiality: Messages are transmitted as the form of ciphertexts CT, where original text m is encrypted as $C = m \oplus H(e(g,g)^{\alpha r})$. Through the method of LSSS, plaintext is encrypted by the access policy $(\boldsymbol{M}, \rho)$ with the secret number r, which is CCA secure proved in [15]. Due to the DLA, even the adversary obtains the ciphertext, without r, the plaintext couldn't be disclosed.
- Message authentication and integrity: In the proposed scheme, only the registered vehicle can transmit message. Each message has the signature $\sigma = sk_1 \cdot sk_2^{h_3(CT||t_1)}$. The signature is produced by pseudonym pid, identity-based key key_{id} and ciphertext CT to ensure the authentication and integrity. After receiving the message, RSUs or vehicle could verify whether the signature satisfies the Equation $e(\sigma, g) = e(pid_1 Q_2^{h_3(CT||t_1)h_2(pid_1)}, pub_1) \cdot e(Q_1^{h_3(CT||t_1)h_3(pid_1||pid_2||vp)}, pub_2)$. According to [16], there is no adversary can solve the CDHP in polynomial time. Thus, if the message get forged, the equation would not hold. After the re-encryption, the message (CT', σ', pid, t_2) could also utilize the equation to check the integrity.
- Identity protection: In the proposed scheme, each message is transmitted with the pseudonym to protect the identity privacy. Pseudonym is designed as $pid = (pid_1 = g^k, pid_2 = rid \oplus h_1(pub_1^k))$. Due to the DLA, though the parameters like g and pub_1 is public, it is hard to compute secret number k from $pid_1 = g^k$. Without knowing k, the adversary couldn't disclose the real identity from $pid_2 = rid \oplus h_1(pub_1^k)$.
- Traceability: If there exists some malicious vehicles, the system should have the ability to trace the real identities. In the proposed scheme, pseudonym $pid_1 = g^k$ and $pid_2 = rid \oplus h_1(pub_1^k)$, where secret number k is randomly selected and stored in TA. Thus, TA has the ability to trace the real identity by $pid_2 = rid \oplus h_1(pub_1^k)$. But other entities in the scheme can't reveal the real identity of vehicles due to the DLA.
- Replay attack: The message (CT, σ, pid, t_1) contains valid time period vp of pid and time stamp t_1. Thus, the receivers could check vp timestamp t_1 to resist replay attacks.
- Simulation attack:The adversaries conduct simulation attacks by signature forgery. The signature is consisted by $sk_1 = pid_1^{r_1}$ and $sk_2 = Q_1^{r_2 h_2(pid_1||pid_2||vp)} \cdot Q_2^{h_3(pid_1)}$ and secret numbers r_1 and r_2 are stored in TA. Thus, the adversaries can't obtain the secret numbers, so the signature wouldn't be forged.

5 Performance Evaluation and Comparison

In this section, we conduct a series of comparisons with three related schemes [6, 11,13] introduced in the Sect. 2 and evaluate the performance of these schemes. Different from these three schemes, the proposed scheme also contains the phases of vehicle registration and message authentication, which are designed to ensure the security of data sharing. Hence, the performance evaluation mainly focuses on the message encryption phase, re-encryption phase and decryption phase.

Table 2. Execution Time of Three Operation

Notations	Description	Time(ms)
T_{bp}	The execution time of bilinear pairing	4.512
T_{eo}	The execution time of exponential operation	0.564
T_{smo}	The scale multiplication operation	0.313

First, the bilinear pairing algorithm $e : \boldsymbol{G} \times \boldsymbol{G} \rightarrow \boldsymbol{G}_T$ and the elliptic curve algorithm $E : Y^2 = X^3 + X$ are built with the same security level of 128 $bits$. Then, the group order is set as 160 $bits$. The simulation is operated on a laptop of 2.9 GHZ i5-10400 with the MIRACL library, 8 GB memory, Windows 10 operating system. The running time of the three phases are listed in Table 2.

5.1 Functionality Comparison

Table 3. Functionality comparison with [6,11] and [13]

Schemes	Mode	Encryption	Authentication	Re-encryption	Access control
Chen et al. [6]	One-to-many	IBE	×	×	×
Zhong et al. [11]	One-to-many	IBE	√	√	×
Ge et al. [13]	One-to-many	ABE	×	√	√
Ours	One-to-many	ABE	√	√	√

Here, a functionality comparison of the proposed scheme and schemes [6,11,13] is demonstrated. As is shown in the Table 3, these four schemes are all proposed for one-to-many communication mode. To keep confidentiality, schemes [6,11] adopt identity-based encryption (IBE), while our scheme and scheme [13] utilize attribute-based encryption (ABE). Compare with IBE, ABE has the advantage of flexible access control for ciphertext. Moreover, the computation cost of is not related to the number of vehicles. Different with scheme [13], our scheme also considers message authentication while communication.

5.2 Computation Cost Evaluation

Here, the corresponding computation cost evaluation in encryption step, re-encryption step and decryption step of each scheme is presented. The total computation cost is listed in the Table 4, where n represents the number of the vehicle and l represents the size of attribute set. In the scheme [6], the broadcaster has to calculate each receivers' personalized key K_i with exponentiation operation during encryption phase. So the computation cost is $(3n+3)T_{eo}+2nT_{smo}$. When decrypting ciphertext Hdr, receiver utilizes bilinear pairing with key $K_i^{'}$ and the cost here is $T_{bp} + 6T_{eo} + 4T_{smo}$. In the scheme of [11], the sender owns master

Table 4. Computation cost comparison with [6,11] and [13]

Schemes	Encryption	Re-encryption	Decryption
Chen et al. [6]	$(3n+3)T_{eo}+2nT_{smo}$	$\times$	$T_{bp}+6T_{eo}+4T_{smo}$
Zhong et al. [11]	$3T_{eo}+T_{bp}$	$4T_{bp}+(n+3)T_{eo}$	$2T_{bp}+nT_{eo}$
Ge et al. [13]	$(3l+5)T_{eo}$	$(3l+8)T_{eo}+(2l+3)T_{bp}$	$(2l+1)T_{bp}$
Ours	$(3l+2)T_{eo}$	$(4l+4)T_{eo}+(2l+1)T_{bp}$	$(2l+1)T_{bp}$

private key β, so the sender can directly calculate ciphertext and the computation cost is $3T_{eo}+T_{bp}$. During the re-encryption phase, the authenticated vehicle and cloud server take over the computation cost. The re-encryption cost related to the size of authenticated group S is $4T_{bp}+(n+3)T_{eo}$. In the decryption phase, receiver has to compute ciphertext with public parameters and the cost is $2T_{bp}+nT_{eo}$. Different with scheme [13], our scheme improves the re-encryption phase and the cost is lower.

Considering the realistic situation in VANET, the simulation sets the number of vehicles from 10 to 100. Besides, we set each vehicle with the size of attribute set as 5. During the encryption phase, as is shown in Fig. 3, the computation cost of Chen et al. [6] increases rapidly with the number of vehicles grow while the other three has no influence. Figure 4 shows that when the number of vehicles is small, the re-encryption cost of Zhong et al. [11] is least. However, the proposed scheme performs better while the number of vehicles is over 80. In Fig. 5, the decryption cost of Chen et al. [6] is the least among these schemes. Finally, the Fig. 6 shows the total cost of all cryptographic phases. As it shows, when the number of vehicles is below 20, the scheme of Chen et al. [6] performs best. When the number of vehicles is over 80, our scheme has the lowest computation cost. Above all, we can see if the number of the vehicle keeps small-scale, the scheme based on identity has less cost, while with the number of vehicle increasing, the advantage of attribute-based algorithm is more obvious.

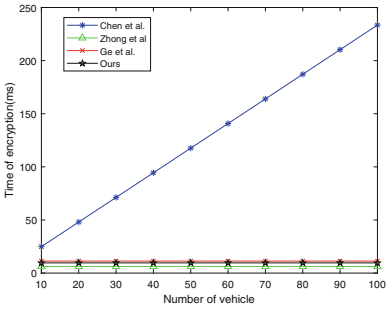

Fig. 3. Comparison of encryption cost

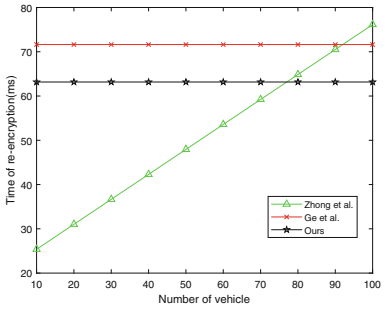

Fig. 4. Comparison of re-encryption cost

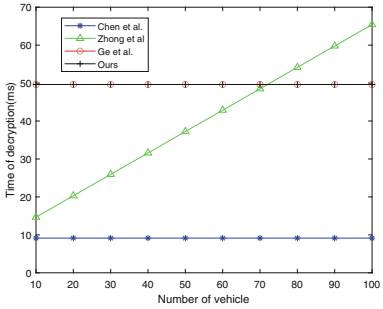

Fig. 5. Comparison of decryption cost

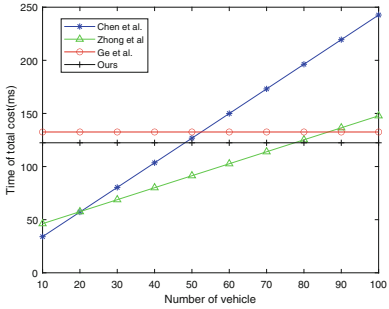

Fig. 6. Comparison of total cost

6 Conclusion

In daily VANET, the number of vehicle increasing rapidly and more traffic problems are following. Thus, it is urgent to adopt efficient and secure message dissemination in VANET to improve transport system. To solve the existing encryption redundancy problem, the proposed scheme utilizes ABPRE method for this one-to-many communication mode. Combined with proxy re-encryption, the proposed scheme reduces the computation cost of re-encryption significantly. To meet the secure requirements, pseudonyms and batch verification are applied in communication. Furthermore, in the future, we will try more efficient and lightweight technology and construct a more secure scheme for VANET.

References

1. Lieira, D.D., Quessada, M.S., Cristiani, A.L., De Grande, R.E., Meneguette, R.I.: Mechanism for optimizing resource allocation in VANETs based on the PSO bio-inspired algorithm. In: 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 283–290 (2022)
2. Goudarzi, S., et al.: A privacy-preserving authentication scheme based on elliptic curve cryptography and using quotient filter in fog-enabled vanet. Ad Hoc Netw. **128**, 102782 (2022)
3. Zhong, H., Han, S., Cui, J., Zhang, J., Xu, Y.: Privacy-preserving authentication scheme with full aggregation in VANET. Inf. Sci. **476**, 211–221 (2019)
4. Shafiq, M., Tian, Z., Bashir, A.K., Du, X., Guizani, M.: IoT malicious traffic identification using wrapper-based feature selection mechanisms. Comput. Secur. **94**, 101863 (2020)
5. Shafiq, M., Tian, Z., Bashir, A.K., Du, X., Guizani, M.: CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques. IEEE Internet Things J. **8**(5), 3242–3254 (2020)
6. Chen, L., Li, J., Zhang, Y.: Anonymous certificate-based broadcast encryption with personalized messages. IEEE Trans. Broadcast. **66**(4), 867–881 (2020)

7. Cui, J., Wu, D., Zhang, J., Xu, Y., Zhong, H.: An efficient authentication scheme based on semi-trusted authority in VANETs. IEEE Trans. Veh. Technol. **68**(3), 2972–2986 (2019)
8. Liu, X., Xia, Y., Chen, W., Xiang, Y., Hassan, M.M., Alelaiwi, A.: SEMD: secure and efficient message dissemination with policy enforcement in VANET. J. Comput. Syst. Sci. **82**(8), 1316–1328 (2016)
9. Huang, Q., Li, N., Zhang, Z., Yang, Y.: Secure and privacy-preserving warning message dissemination in cloud-assisted internet of vehicles. In: 2019 IEEE Conference on Communications and Network Security (CNS), pp. 1–8 (2019)
10. Horng, S.J., Lu, C.C., Zhou, W.: An identity-based and revocable data-sharing scheme in VANETs. IEEE Trans. Veh. Technol. **69**(12), 15933–15946 (2020)
11. Zhong, H., Zhang, S., Cui, J., Wei, L., Liu, L.: Broadcast encryption scheme for v2i communication in VANETs. IEEE Trans. Veh. Technol. **71**(3), 2749–2760 (2021)
12. Liu, X., Chen, W., Xia, Y.: Security-aware information dissemination with fine-grained access control in cooperative multi-RSU of VANETs. IEEE Trans. Intell. Transp. Syst. **23**, 2170–2179 (2020)
13. Ge, C., Susilo, W., Baek, J., Liu, Z., Xia, J., Fang, L.: A verifiable and fair attribute-based proxy re-encryption scheme for data sharing in clouds. IEEE Trans. Dependable Secure Comput. **19**, 2907–2919 (2021)
14. Huang, J.L., Yeh, L.Y., Chien, H.Y.: ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **60**(1), 248–262 (2011)
15. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 62–91. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_4
16. Jianhong, Z., Min, X., Liying, L.: On the security of a secure batch verification with group testing for VANET. Int. J. Netw. Secur. **16**(5), 351–358 (2014)