A Self-Authentication and Deniable Efficient Group Key Agreement Protocol for VANET

Mu Han[1], Lei Hua[1] and Shidian Ma[2]
[1] School of Computer Science and Communication Engineering, Jiangsu University
Zhenjiang, 212013, China
[e-mail: hanmu@ujs.edu.cn, hualei@ujs.edu.cn]
[2] School of Automotive Engineering Research Institute , Jiangsu University
Zhenjiang, 212013, China
[e-mail: masd@ujs.edu.cn]
*Corresponding author: Shidian Ma

Received December 21, 2016; revised March 30, 2017; accepted April 9, 2017; published July 31, 2017

Abstract

With the rapid development of vehicular ad hoc Network (VANET), it has gained significant popularity and received increasing attentions from both academics and industry communities in aspects of security and efficiency. To address the security and efficiency issues, a self-authentication and deniable efficient group key agreement protocol is proposed in this paper. The scheme establishes a group between road side units (RSUs) and vehicles by using self-authentication without certification authority, and improves certification efficiency by using group key (GK) transmission method. At the same time, to avoid the attacker attacking the legal vehicle by RSUs, we adopt deniable group key agreement method to negotiation session key (sk) and use it to transmit GK between RSUs. In addition, vehicles not only broadcast messages to other vehicles, but also communicate with other members in the same group. Therefore, group communication is necessary in VANET. Finally, the performance analysis shows superiority of our scheme in security problems, meanwhile the verification delay, transmission overheard and message delay get significant improvement than other related schemes.

Keywords: Vehicular ad hoc network (VANET), deniable, key negotiation, Group communication

A preliminary version of this paper appeared in IEEE ICC 2009, June 14-18, Dresden, Germany. This version includes a concrete analysis and supporting implementation results on MICAz sensor nodes. This research was supported by a research grant from the IT R&D program of MKE/IITA, the Korean government [2005-Y-001-04, Development of Next Generation Security Technology]. We express our thanks to Dr. Richard Berke who checked our manuscript.

https://doi.org/10.3837/tiis.2017.07.021 **ISSN : 1976-7277**

1. Introduction

Vehicular ad hoc Network (VANET) is an essential branch of Mobile Ad hoc Networks and is a promising approach to enhance transportation safety and efficient [1]. VANET has many promising features, such as vehicles' movement at high speed, rapid topological transformation, short interactive time between nodes and so on [2]. In addition, the nodes of VANET comprise two parts, the on-board units(OBUs) which is equipped in the vehicles, and the RSUs which is located on the road side. Due to the peculiar attribute of VANET, it can provide many services including traffic information, traffic safety warning and infotainment dissemination for drivers and passengers [3-6]. However, VANET also faces some challenges, such as the problem of information storage. Because of the large number of network nodes in the vehicular network, there is a large number of data information (e.g., identity information, key information, etc.). In the existing scheme, the purpose of mass information storage is realized by means of distributed storage [7]. In addition, there is a set of unique challenges of VANET. First, vehicles communicate with each other as well as RSUs through open wireless channel, in which attracters can easily monitor, alter and forge the information(e.g., users' identity, travel route) [8]. Sceond, vehicles are located in an open physical space, privacy leaking in VANET not only exposes privacy information, but also brings treat to the lives and properties of drivers and passengers [9,10]. Third, its short communication range as well as vehicles' high speed in VANET leads to the limited communication among RSUs and vehicles. Therefore, it is of great theoretical significance and application value to design a secure and efficient network communication protocol for the unique challenges in vehicular networks.

Primarily, a suitable communication protocol for VANET needs to meet some security requirements to resist security threats, for example:

- Message integrity and authentication: Vehicles should be able to verify that a message is indeed sent and received by another vehicle without being modified by anyone else.
- Privacy: Vehicle's true identity (TID) should not be linked to any message, and other vehicles or RSUs cannot achieve any vehicle's true identity by analyzing multiple messages sent from it.
- Confidentiality: The message sent to target vehicles should be readable only for the target receivers, other vehicles should be unable to decrypt the message.
- Non-repudiation: To avoid the circumstance that the sender denied that he had sent the message, trust authority (TA) should be able to obtain the vehicle's TID and associate this message with the sender.
- Forward-security and backward-security: The vehicles has left from the communication group should not be able to acquire the new group key and communicate with original group members. In addition, a new group member should be unable to learn the previous group key.

In the next place, due to the inconstancy of the network topology, short communication time and other characteristics, the efficiency of communication is equally important.

To solve the aforementioned problems, we design a self-authentication and deniable efficient group key agreement protocol to meet security requirements cited above and enhance the communication efficiency. Our main contributions are listed as follows:

- This paper proposed an anonymous authentication protocol which is without trusted center. It realized the authentication between vehicles and road-side units by the

geographical area parameters and random authentication parameters to reduce the cost of the authentication.

- This paper proposed the method that road-side units establish the communication group by the deny negotiation in hope of reducing the steps of authenticating vehicle through the transmission of group key and thus improving the authentication efficiency.
- This paper proposed a group key negotiation protocol. In this protocol, the nodes can communicate without key negotiation through the pseudonyms of the nodes in group broadcasted by RSUs and random key parameters. Therefore, the communication cost will not increase with the increase of the nodes' number in the group.
- According to the requirement of different scenarios, this paper designed a broadcast communication protocol, the point to point communication protocol between vehicles and the communication protocol between vehicle and road-side unit.

The reminder of the paper is organized as follows: Some related work is given in Section 2. Section 3 presents the system model, bilinear maps and hard problem. Section 4 proposed our scheme. Section 5 and Section 6 analyses security and performance of the proposed protocol. Finally, Section 7 concludes the paper.

2. Related Work

With the development of VANET, its communication technology has been gradually improved which mainly concentrates on two aspects: the communication between vehicles and RSUs, and the communication between vehicles. Because of the short communication range and the vehicles' high speed movement, the efficiency and security of communication in VANET become extremely significant. To handle the security problems, [8] and [11] produced the public and private keys by using PKI mechanism, and utilized digital signature certification to guarantee the validity of the vehicles. Nevertheless, the overhead of the signature, verification and transmission will increase rapidly with the increasement of nodes. [12-14] have been proposed to solve the problem of users' privacy. In [13], the authors proposed an efficient and secure anonymous communication scheme, which employed asymmetric cryptography to protect users' private information. A secure and efficient communication scheme is proposed [15] to protect the confidentiality of information and enhance the scalability. [16] suggested that every vehicle should be pre-loaded with a large number of anonymous public and private keys as well as the corresponding public key certifications. It avoids being tracked to a certain extent by using this method, but it will waste a lot of time on checking the list of canceled certificates. In [17], a spontaneous privacy-preserving protocol based on revocable ring signature with a feature for locally authenticating safety messages is proposed. However this protocol is not scalable because every vehicle needs to participate in message verification process. Aiming at the improvement of communication efficiency, [18] adopted identity-based cryptography, not only shortened the computation process of the public key certification, but also reduced the computation and transmission cost. A batch-based authentication scheme [19] was presented. In this scheme, the computation efficiency can be significantly improved , but they don't check the integrity of request messages before batch authentication. Therefore, once an invalid request caused by wireless channel interface, packet loss or a bogus message is in the batch, these schemes may lose their efficacy, or need some additional authentication delay for rebatch. [20] introduced "an efficient identity-based batch verification scheme", in which the efficiency of the vehicle certification can be improved but this scheme still has privacy issues. [21] proposed a broadcast authentication scheme to reduce communication and computation cost using fast

authentication and selective authentication method. [22] proposed a scheme using two kinds of traditional cryptographic schemes, asymmetric PKI and symmetric respectively. The asymmetric cryptography scheme is used to securely exchange the key and authentication process and symmetric cryptography scheme is used for low latency safety application. This scheme not only reduces the latency but also enhances the security.

3. Preliminaries

3.1 Network Model

As shown in **Fig. 1**, the network model of VANET consists of three entities: The Trust Authority (TA), RSU and OBU equipped on mobile vehicles.

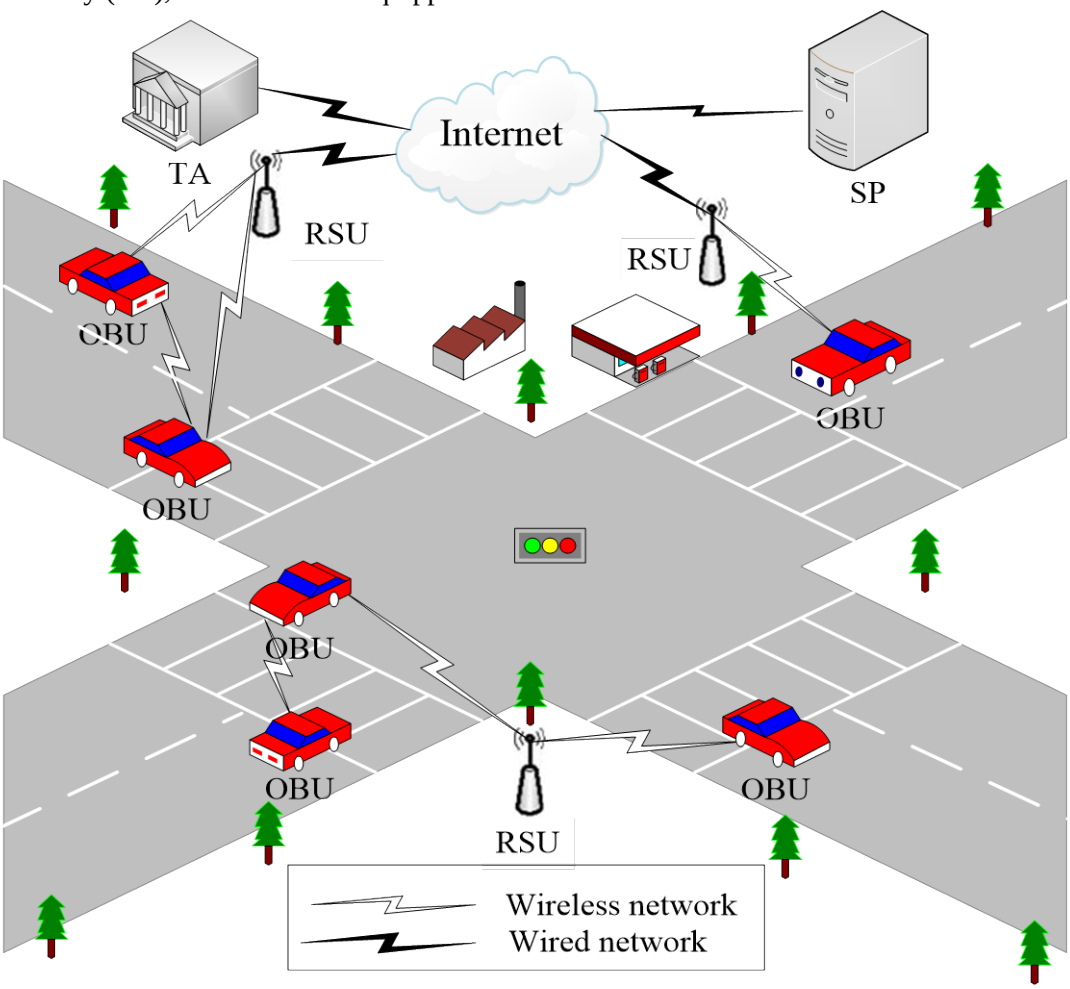

Fig. 1. System model

- TA: TA is a trustworthy certification center of the whole network. It responses to registers and manages all nodes in the VANET. In addition, it exposes TID of the valid vehicles and releases the information of the revoked vehicles. In this paper, TA allocates the certification parameters to RSU and vehicles. As usual, TA has a strong storage capability and is impossible to compromise with adversary.
- RSUs: RSUs are distributed on the roadside densely. They connect with TA by wired

links while wireless links are used between vehicles. In this protocol, RSUs are used to authenticate the validity of the vehicles and negotiate with the vehicles to form the group. In addition, it assists TA to condemn the vehicles which have illegal acts. Each RSU is able to know the public key (PK) of the one in its neighborhood and communicates with them.

- OBUs: Each vehicles are equipped with OBU, which periodically broadcast traffic related status information to improve the road environment, traffic safety, and infotainment dissemination for drivers and passengers [23].

3.2 Definitions and Assumptions

Definition 1: Bilinear Maps

Let G_1 be a cyclic additive group and G_2 is a cyclic multiplicative group. Both group G_1 and G_2 have the same prime order q (k bites, k is the safety parameters of the system). Let P be a generator of G_1, aP express P self-increase $a \in Z_q^*$ times. A mapping $e: G_1 \times G_1 \to G_2$ is called bilinear mapping if it satisfies the following properties.

Bilinearity： $e(aP, bQ) = e(P, Q)^{ab}$ for all $e(P, Q)$. $a, b \in Z_q^*$.

Nondegeneracy： $e(P, P) \neq 1$

Computability：There is an efficient algorithm to compute $e(P, Q)$, for any $P, Q \in G_1$.

Definition 2: Computational Diffie-Hellman problem in G_1 (CDH Problem)

Let P be the generator of G_1, for all $a, b \in Z_q^*$, give (P, aP, bP), output abP by the probabilistic polynomial time algorithm A.

The probability of A success is defined as:

$$Succ_{A,G_1}^{CDH} = \Pr[A(P, aP, bP) = abp : a, b \in_R Z_q^*]$$

CDH Assumption: $Succ_{A,G_1}^{CDH}$ is a negligible value for all the *PPT* algorithm A.

Definition 3: Decide Diffie-Hellman problem in G (DDH Problem)

Let G be a special cyclic multiplicative group, P is the safety parameter, and it satisfies $P = 2q + 1$. Let g be the generator of the cyclic group $G' =< g >$, G' is quadratic residue class of model P. Define the function $f: f(x) = \{^{x, if\ x<q}_{p-x, if\ q<x<p}$. Through function f, define $G: G = \{f(g^i) \mid i \in Z_q\}$. Define the exponent arithmetic in $G: a^b = \{f(a^b) \bmod p\}\ a, b \in G$.

The DDH problem in G is that for $(g, g^x, g^y, g^r): x, y, r \in_R G$, exist a *PPT* algorithm A which output is 0/1, output 1 when $r = xy$; Otherwise, output 0.

The advantage of A solves the DDH problem in G is defined as follows:

$$ADv_{A,G}^{DDH} = \Pr[A(g, g^x, g^y, g^{xy}) = 1] - \Pr[A(g, g^x, g^y, g^r) = 1] : x, y, r \in_R G.$$

DDH Assumption: $ADv_{A,G}^{DDH}$ is a negligible value for all the *PPT* algorithm A, which output is 0/1.

4. Proposed Scheme

In this section, we describe our scheme with the following process: 1) system initialization, 2) deniable group key negotiation of RSUs, 3) authentication between RSUs and Vehicles, 4) negotiation and update of the group key between RSUs and Vehicles, 5) communication among the group. **Table 1** provides a summary of the symbols used in this paper.

Table 1. Descriptions of symbols

Symbols	Descriptions
$V_i, TID_{V_i}, FID_{V_i}$	The true name,and pseudonym of Vehicle V_i,
RSU_i, TID_{RSU_i}	The true name of RSU_i
m	The message
Q_U, S_U	The certification parameters of the node U
TS	Time stamp
U	The node U ,vehicle or RSU
$RSU_{i\pm1}$	The RSU nearby RSU_i
(PK_U, SK_U)	The public and private key of the node U
$\sigma_{SK_U}(\cdot)$	The signature of the node U
GK	Group Key between RSUs and vehicles
$VVK_{i,j}$	The shared key among vehicle V_i and V_j
$HMAC_k(\cdot)$	The message authentication by symmetric key k
$E_k(\cdot)$	The encrypt by key k
pid	The set of all users' TID who participate in the process
sk	The session key in Group of RSU

4.1 System Initialization

- Given the parameters $(G_1, G_2, P, q, e, G, p, g)$,which satisfy the description in Section 3.2, TA initializes the system by the following steps:
  1) TA chooses a random number $\psi_{TA} \in Z_q^*$ as its private key SK_{TA} and compute the public key $PK_{TA} = g^{\psi_{TA}}$;
  2) TA chooses two cryptographic hash functions : $H_1 : \{0,1\} \to G_1, h : \{0,1\} \to Z_q^*$;
  3) TA chooses a security symmetric cryptographic $E_k(\cdot)$, and then TA publishes the system parameters, which include $(G_1, G_2, P, q, e, G, p, g, PK_{TA}, H_1(\cdot), h(\cdot), E_k(\cdot))$ and downloads these parameters into RSUs and Vehicles.
- RSUs require download the system parameters by TA before installing to the appropriate location. TA distributes TID_{RSU_i} to RSU_i and chooses a random $\xi_i \in Z_q^*$ as its private

key SK_{RSU_i} and computes the public key $PK_{RSU_i} = g^{\xi_i}$, the certification parameters $Q_{RSU_i} = H_1(TID_{RSU_i})$ and $S_{RSU_i} = \psi_{TA} Q_{RSU_i}$. Then download the public key, the private key and the certification parameters into RSU_i. At the same time, download other RSU_i's public keys which is located nearby regions.

- Vehicles also require to download the system parameters by TA before they used. TA distributes a true identity TID_{V_i} (each vehicle has a unique digital true identity e.g., the license plate number) to vehicle V_i, then TA computes the certification parameters $Q_{V_i} = H_1(TID_{V_i})$, $S_{V_i} = \psi_{TA} Q_{V_i}$ and downloads them into it. In order to ensure vehicles could not traced by the malicious nodes, when vehicles enter a new range of RSU, it will motivate the key generator to generate the private key $SK_{v_i} = \alpha_i, \alpha_i \in Z_q^*$, the public key $PK_{RSU_i} = g^{\alpha_i}$ and pseudonym $FID_{V_i} = TID_{V_i} \oplus H_1(\alpha_i * PK_{TA})$.

4.2 Deniable group key negotiation of RSUs

We adopted two-round deniable group key agreement protocol [24], which is used to establish a confidential channel for communications. Simultaneously, it allows participants to deny that they have ever participated in group key agreement. Firstly, we contract a group (it include all RSUs) and then generate the session key (sk) between RSUs by using deniable group key agreement, which is the preparatory work for the group key transmission mechanism. The purpose is to prevent the attacker tracking the legitimate vehicles from RSUs and ensure the security of group key transmission. The deniable group key negotiation of RSUs is as follows:

Step 1: RSU_j random select $x_j, r_j, t_j \in Z_q^*$ compute $X_j = g^{x_j}$, $R_j = g^{r_j}$, $T_j = g^{t_j}$, then broadcast message $M_j^1 : ((E_{SK_{RSU_j}}(TID_{RSU_j}, X_j, R_j, T_j))\sigma_{SK_{RSU_j}}(\cdot))$.

Step 2: RSU_i receives all the message $\{M_j^1\}_{j\in\{1,\cdots,n\}, j\neq i}$, decodes it and gets $\{X_j, R_j, T_j\}$, then proceeds as following types:

1. Compute $Y_i^L = X_{i-1}^{x_i}, Y_i^R = X_{i+1}^{x_i}, Y_i = Y_i^R / Y_i^L$.

2. Compute $v_i = H(Y_i^L \| Y_i^R \| X_1 \| X_2 \| \cdots \| X_n \| pid) : pid = h(TID_{RSU_1} \| TID_{RSU_2} \| \cdots \| TID_{RSU_n})$ and using $SK_{RSU_i} = \xi_i$ compute $s_i = r_i - v_i \cdot \xi_i$.

3. Using r_i compute $T_{i,j} = T_j^{r_i}$, $j = \{1, \cdots, i-1, i+1, \cdots, n\}$.

4. Broadcast $M_i^2 : (TID_{RSU_i} E_{SK_{RSU_i}}(Y_i, s_i, T_{i,1}, \cdots, T_{i,i-1}, T_{i,i+1}, \cdots, T_{i,n}))\sigma_{SK_{RSU_j}}(\cdot))$ Session key generation RSU_j receives all message $\{M_i^2\}_{j\in(1,\cdots,n), j\neq i}$, proceeds as follows:

1. Verify $T_{i,j} = R_i^{t_j} (i = \{1, \cdots, j-1, j+1, \cdots n\})$ holds or not. If it holds, continues, else, stop.

2. Compute $\hat{Y}_{j+1}^R = Y_{j+1} \cdot Y_j^R, \hat{Y}_{j+2}^R = Y_{j+2} \cdot \hat{Y}_{j+1}^R, \cdots, \hat{Y}_{j+(n-1)}^R = Y_{j+(n-1)} \cdot \hat{Y}_{j+(n-2)}^R$ and confirm $Y_j^L = \hat{Y}_{j+(n-1)}^R$. If it holds to all RSU_i, continues, else, cease.

3. All RSU_i compute $\hat{v}_i = H(\hat{Y}_{i-1}^R \| \hat{Y}_i^R \| X_1 \| \cdots \| X_n \| pid)$, verify $g^{s_i} (PK_{RSU_i})^{\hat{V_i}} = R_i$. If

it holds to all RSU_i, continues, else, cease.

4. Compute $sk = \hat{Y}_1^R \cdot \hat{Y}_2^R \cdots \hat{Y}_n^R = g^{x_1x_2+x_2x_3+\cdots+x_nx_1}$.

4.3 Authentication between RSUs and vehicles

The main function of the vehicle network is to provide the communication between vehicles and vehicles, vehicles and RSU, and then provide a variety of services for vehicles. Vehicles must be authenticated to ensure the legality of the vehicle before they obtain some services. However, the vehicle identity is the only legal identification of the vehicle, which is related directly to vehicles' information. Therefore, in the process of vehicle certification, there is a problem of vehicle privacy.

To solve the above problems, this paper designed a kind of anonymous authentication protocol in VANET. This authentication protocol without the participation of trusted center needs fewer times for legal vehicles authentication by using group key transmission mechanism. At the same time, the authentication protocol can meet the security requirements such as Mutual authentication of vehicles and RSU, anonymity and privacy of vehicle et al. The authentication between and vehicle is shown in **Fig. 2.**

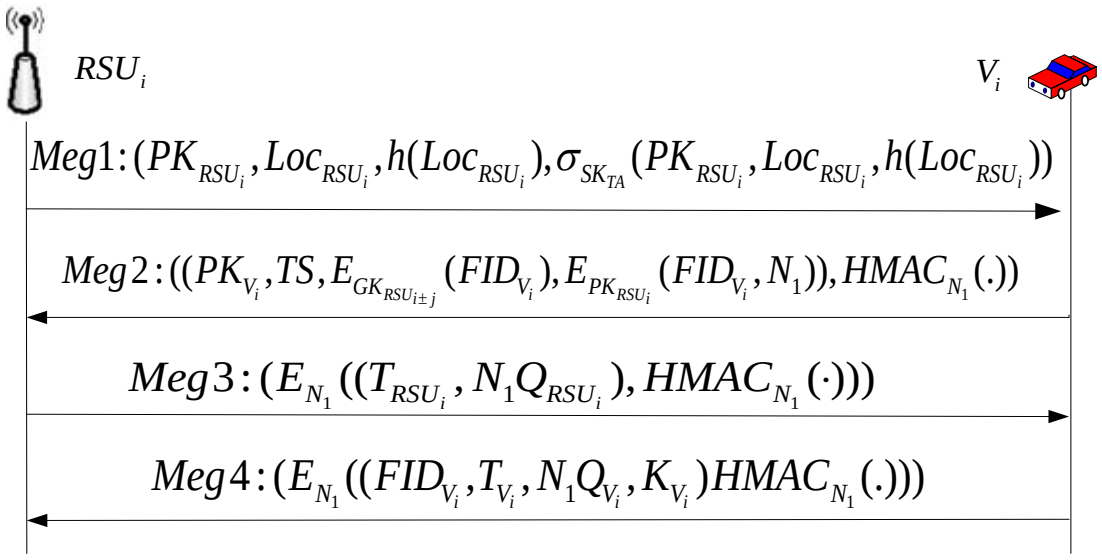

Fig. 2. Interactive model between RSU_i and V_i

Step 1: RSUs store the signing message $\sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$, which promulgate by TA. $h(Loc_{RSU_i})$ is the hash operation on location information of RSU_i. And RSU_i periodically broadcasts $Meg1:(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}), \sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$.

Step 2: When V_i gets into the communication scope of RSU_i, it needs to authenticate RSU_i. V_i authenticate RSU_i by using the flowing algorithm 1. Vehicle V_i receives $Meg1$,and gets $PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i})$, verifies $\sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i})$. If

$\sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$ is validated, computes $h'(Loc_{RSU_i})$ by using Loc_{RSU_i}. If formula (1) is set up, V_i completes the authentication of RSU_i, else, discards the message.

$$h(Loc_{RSU_i}) = h'(Loc_{RSU_i}) \tag{1}$$

Algorithm 1 The process of V_i authenticating RSU_i

Require: $PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}), \sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$

V_i Verifies $\sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$ by PK_{TA}.
if $\sigma_{SK_{TA}}(PK_{RSU_i}, Loc_{RSU_i}, h(Loc_{RSU_i}))$ is validated **then**
  V_i computes $h'(Loc_{RSU_i})$ by Loc_{RSU_i} ,and
  verifies $h(Loc_{RSU_i}) = h'(Loc_{RSU_i})$.
    if The equation holds
      V_i completes the authentication of RSU_i.
    end if
end if

Step 3: If vehicle V_i completed the step 2, then RSU_i needs to authenticate V_i. RSU_i authenticate V_i by using the flowing algorithm 2. V_i chooses a random number N_1 and sends message $Meg2:((PK_{V_i}, TS, E_{GK_{RSU_{i\pm j}}}(FID_{V_i}), E_{PK_{RSU_i}}(FID_{V_i}, N_1)), HMAC_{N_1}(\cdot))$ to RSU_i.

Step 4: RSU_i receives the message $Meg2$ to verify time stamp TS, and then calculates $\Delta t = CT - TS$ (CT is current time). If Δt meets the network delay, finishes the TS verification, else discards the message. By using private key to decrypt $E_{PK_{RSU_i}}(FID_{V_i}, N_1)$ and obtain N_1, FID_{V_i}. Then calculates $HMAC'_{N_1}(\cdot)$ and compares with $HMAC_{N_1}(\cdot)$, if them unequal, discards the message, else uses $GK_{RSU_{i\pm j}}$ to get FID'_{V_i} from $E_{GK_{RSU_{i\pm j}}}(FID_{V_i})$, then compares FID'_{V_i} and FID_{V_i}. If they are equal, it explains that V_i has authenticated by other RSU. Therefore, the authentication has completed and then executed the negotiation of the group key. Else RSU_i chooses a random number $\alpha_i \in Z_q^*$ to computes $T_{RSU_i} = \alpha P$, and sends $Meg3:(E_{N_1}((T_{RSU_i}, N_1Q_{RSU_i}), HMAC_{N_1}(\cdot)))$ to V_i.

Step 5: V_i receives $Meg3$, gets T_{RSU_i} and verifies $HMAC_{N_1}(\cdot)$. Then V_i chooses a random number $\beta_i \in Z_q^*$, computes $T_{V_i} = \beta P, K_{V_i} = e(\beta N_1 Q_{RSU_i}, PK_{TA})e(N_1 s_{V_i}, T_{RSU_i})$ and sends $Meg4:(E_{N_1}((FID_{V_i}, T_{V_i}, N_1Q_{V_i}, K_{V_i}), HMAC_{N_1}(\cdot)))$ to RSU_i.

Step 6: RSU_i receives $Meg4$ and obtains $FID_{V_i}, T_{V_i}, N_1Q_{V_i}, K_{V_i}$ from it, then verifies $HMAC_{N_1}(\cdot)$ and calculates $K_{RSU_i} = e(\alpha N_1 Q_{V_i}, PK_{TA})e(N_1 s_{RSU_i}, T_{V_i})$. If formula (2) holds, RSU_i finishes the authentication to V_i, else, discards the message.

$$e(\beta N_1 Q_{RSU_i}, PK_{TA})e(N_1 s_{V_i}, T_{RSU}) = e(\alpha N_1 Q_{V_i}, PK_{TA})e(N_1 s_{RSU_i}, T_{V_i}) \quad (2)$$

Algorithm 2 The process of RSU_i authenticating V_i

Require: $Meg2:(PK_{V_i}, TS, E_{GK_{RSU_{i\pm j}}}(FID_{V_i}), E_{PK_{RSU_i}}(FID_{V_i}, N_1)), HMAC_{N_1}(\cdot))$

$Meg3:(E_{N_1}((T_{RSU_i}, N_1 Q_{RSU_i}), HMAC_{N_1}(\cdot)))$

$Meg4:(E_{N_1}((FID_{V_i}, T_{V_i}, N_1 Q_{V_i}, K_{V_i}), HMAC_{N_1}(\cdot)))$

1: RSU_i receives $Meg2$, verifies TS and calculates $\Delta t = CT - TS$ (CT is current time).
2: **if** Δt meets the network delay **then**
3: RSU_i decrypts $E_{PK_{RSU_i}}(FID_{V_i}, N_1)$ and gets FID_{V_i}, N_1, computes $HMAC'_{N_1}(\cdot)$, and verifies $HMAC'_{N_1}(\cdot) \stackrel{?}{=} HMAC_{N_1}(\cdot)$.
4: **if** The equation holds **then**
5: RSU_i decrypts $E_{GK_{RSU_{i\pm j}}}(FID_{V_i})$ by $GK_{RSU_{i\pm j}}$, gets FID'_{V_i}, and compares FID'_{V_i} and FID_{V_i}
6: **if** FID'_{V_i} and FID_{V_i} are equal **then**
RSU_i finishes the authentication to V_i.
7: **else** RSU_i chooses a random number $\alpha_i \in Z_q^*$ to computes $T_{RSU_i} = \alpha P$, and sends $Meg3$ to V_i.
8: V_i receives $Meg3$, gets T_{RSU_i} and verifies $HMAC_{N_1}(\cdot)$.
9: **if** $HMAC_{N_1}(\cdot)$ is validated **then**
10: V_i chooses a random number $\beta_i \in Z_q^*$, computes, $T_{V_i} = \beta P$, $K_{V_i} = e(\beta N_1 Q_{RSU_i}, PK_{TA})e(N_1 s_{V_i}, T_{RSU_i})$, and sends $Meg4$ to RSU_i.
11: RSU_i receives $Meg4$, obtains $FID_{V_i}, T_{V_i}, N_1 Q_{V_i}, K_{V_i}$, verifies $HMAC_{N_1}(\cdot)$ calculates $K_{RSU_i} = e(\alpha N_1 Q_{V_i}, PK_{TA})e(N_1 s_{RSU_i}, T_{V_i})$ and verifies $e(\beta N_1 Q_{RSU_i}, PK_{TA})e(N_1 s_{V_i}, T_{RSU}) \stackrel{?}{=} e(\alpha N_1 Q_{V_i}, PK_{TA})e(N_1 s_{RSU_i}, T_{V_i})$
12: **if** The equation holds **then**
13: RSU_i finishes the authentication to V_i
14: **end if**
15: **end if**
16: **end if**
17: **end if**
18: **end if**

4.4 Negotiation and update of the group key

4.4.1 Negotiation of the group key

After completing the vehicle authentication, it is necessary to communicate with RSUs and other vehicles to get the road condition information, alarm information and so on. Therefore,

the vehicle needs to negotiate the group key (GK). The negotiation between RSU_i and V_i is shown in **Fig. 3.**

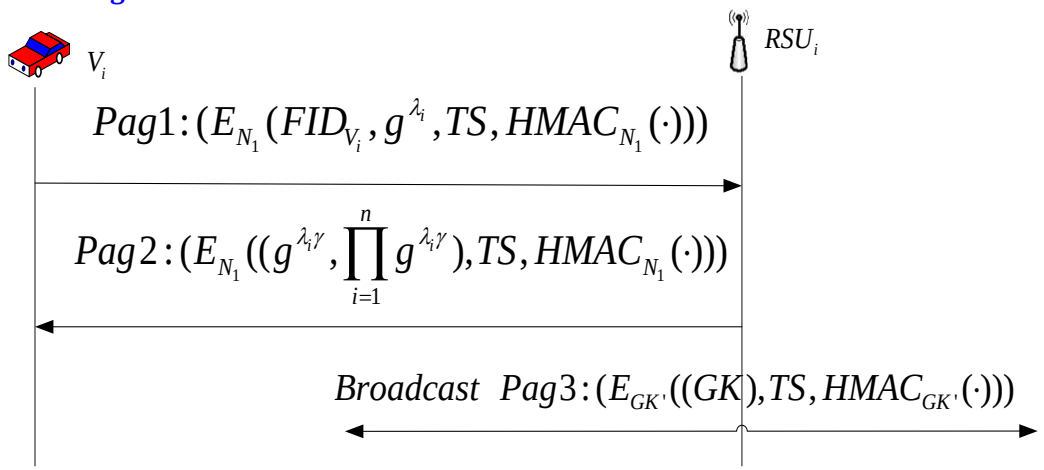

Fig. 3. The negotiation of the group key between RSU_i and V_i

Step 1: Vehicle V_i chooses a random number $\lambda_i \in Z_q^*$, computes g^{λ_i} and send $Pag1$: $(E_{N_1}(FID_{V_i}, g^{\lambda_i}, TS, HMAC_{N_1}(\cdot)))$ to RSU_i.

Step 2: RSU_i receives the message $Pag1$, get FID_{V_i}, g^{λ_i} from it. Then chooses a random number $\gamma \in Z_q^*$, computes $g^{\lambda_i\gamma}, \prod_{i=1}^{n} g^{\lambda_i\gamma}$, new group key $GK = g^{\gamma} * \prod_{i=1}^{n} g^{\lambda_i\gamma}$, and sends $Pag2:(E_{N_1}((g^{\lambda_i\gamma}, \prod_{i=1}^{n} g^{\lambda_i\gamma}), TS, HMAC_{N_1}(\cdot)))$ to V_i. At the same time, RSU_i broadcasts $Pag3:(E_{GK'}((GK), TS, HMAC_{GK'}(\cdot)))$ to the primary group members. Here GK' is the primary group key.

The group key transmission scheme: RSU_i sends $(E_{sk}(GK_{RSU_i}), TS, HMAC_{sk}(\cdot))$ to the nearby RSUs through the wire communication when GK has updated.

4.4.2 Update of the group key

In order to guarantee the communication quality of primary group members, the group key needs to update when vehicles join or leave the group. Mainly including:

Step 1: When vehicle V_j has left the scope of RSU_i, RSU_i chooses a random number $\gamma \in Z_q^*$, to computes $g^{\lambda_i\gamma}$ of every group members (except V_j) and their sum $\prod_{1}^{j-1}\prod_{j+1}^{n} g^{\lambda_i\gamma}$. Broadcast $Bm1:(E_{GK'}((g^{\lambda_1\gamma}, FID_{V_1}), \cdots, (g^{\lambda_{j-1}\gamma}, FID_{V_{j-1}}), (g^{\lambda_{j+1}\gamma}, FID_{V_{j+1}}), \cdots, (g^{\lambda_n\gamma}, FID_{V_n})), \prod_{1}^{j-1}\prod_{j+1}^{n} g^{\lambda_i\gamma}, TS, HMAC_{GK'}(\cdot)))$.

Step 2: The group member V_i receives $Bm1$ and gets $g^{\lambda_i\gamma}$, $\prod_{1}^{j-1}\prod_{j+1}^{n} g^{\lambda_i\gamma}$ by using the primary

group key GK' to decode it and according to FID_{V_i}. Then computes $g^{\gamma} = (g^{\lambda_i \gamma})^{-\lambda_i}$ and the new group key $GK = g^{\gamma} * \prod_{1}^{j-1} \prod_{j+1}^{n} g^{\lambda_i \gamma}$.

4.5 Communication among the group

When the legal vehicle joined in a group of RSU, it is necessary to communicate with other RSUs and vehicles in the group. Therefore, according to the needs of the scene, we designed three communication modes: group communication, one-to-one communication, and the communication between vehicle and RSU.

4.5.1 Broadcast communication

When the vehicle in-group needs to send a message to all the group members, e.g. RSU need to send traffic alarm messages to all vehicles, it can use broadcast communication.

Vehicle V_i broadcast $E_{GK}(m, FID_{V_1}, HMAC_{GK}(\cdot))$ if it wants to broadcast message m to other vehicles.

4.5.2 Communication between vehicles and RSUs

When the vehicle in-group wants to send a message to RSU, such as emergency road traffic accident: the vehicle informs the RSU and RSU can broadcast the news so as to remind the members of the group to drive safety and select the driving road.

When V_i wants to send a message m to RSU_i, it sends $((FID_{V_i}, E_{N_1}(m)), HMAC_{N_1}(.))$ to RSU_i.

4.5.3 Communication between vehicles

If V_i needs one-to-one communication with V_j, they are required to execute this communication process as shown in **Fig. 4.**

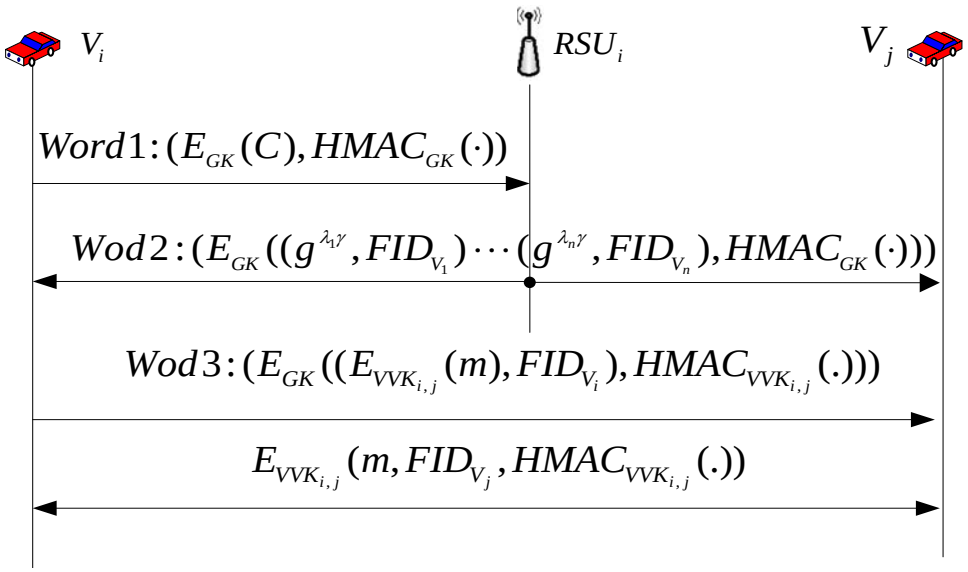

Fig. 4. Communication between V_i and V_j

Step 1: V_i sends $Word1:(E_{GK}(C),HMAC(.))$ to RSU_i, here C is a fixed value, it explains the request of one to one communication.

Step 2: RSU_i receives $Word1$ and obtains C by using GK decode it and according to C broadcast the message $word2:(E_{GK}((g^{\lambda_1 l},FID_{V_1})...(g^{\lambda_n l},FID_{V_n}),HMAC_{GK}(.)))$.

Step 3: V_i receives $word2$ verifies $HMAC_{GK}(.)$ and obtains $g^{\lambda_j \gamma}$ according to FID_{V_j}. And then computes $VVK_{i,j}=g^{\lambda_i\lambda_j\gamma}$ and sends $Wod3:(E_{GK}((E_{VVK_{i,j}}(m),FID_{V_i}),HMAC_{VVK_{i,j}}(\cdot)))$ to V_j.

Step 4: V_j receives $Wod2$ and $Wod3$ to obtain $g^{\lambda_j\gamma}$. Then computes $VVK_{i,j}=g^{\lambda_i\lambda_j\gamma}$ and verifies $HMAC_{VVK_{i,j}}(\cdot)$, if it is true, receives the message m.

5. Analysis of Proposed Scheme

In this section, we will analyze the scheme from the aspect of security requirements which have been referred in Introduction.

5.1 Message confidentiality

For the authentication and negotiation in section 4.4, messages are protected by the shared secret key N_1, the cipher text under symmetric encryption cannot leak any information about message. The broadcast in section 4.5 whose confidentiality is protected by the shared secret group key, while the confidentiality of one-to-one communication is protected by the shared secret key $VVK_{i,j}$ between vehicles.

5.2 Message integrity and authentication

This scheme uses $E_K(m)$ and $HMAC_K(m)$ to realize the message integrity and confidentiality of message m.

Assuming that the shared key k is held safely. When the message cannot be forged by an attacker, the forgery attack on the scheme is secure under random oracle. First, consider the Game between the challenger and the attacker.

Setup: The challenger starts by giving the attacker a set system parameters.

Challenge: The challenger asks the attacker to pick a random message m and sign it to generate $E_K(m)$ and $HMAC_K(m)$.

Guess: Finally, the attacker sends $E_K(m)$ and $HMAC_K(m)$ to the challenger.

The attacker's advantage is defined to be $E_K(m)$ and $HMAC_K(m)$ are valid signatures. The scheme is secure against existential forgery, adaptive chosen message attack if the attacker's advantage is negligible.

In section 4.3, $k=N_1$ is the shared key between V_i and RSU_i. V_i encodes N_1 by PK_{RSU_i} and transfers it to RSU_i. However, only RSU_i has SK_{RSU_i} to decode it and get ^{N_1}. So, only V_i and RSU_i know the key N_1. In section 4.5 the shared key between V_i and V_j is $VVK_{i,j}=g^{\lambda_i\lambda_j\gamma}$. However, $\lambda_i\lambda_j$ is respectively held by V_i and V_j, it do not be transferred.

According to the difficulty problem, it is known that only V_i and V_j can compute $VVK_{i,j}$.

The above analysis shows that the attacker cannot obtain the shared secret key, and cannot forge any valid message. Therefore, the attacker's advantage is negligible and our scheme is secure.

5.3 Identity privacy

The message which sent by V_i only contained pseudonym FID_{V_i}, the public key PK_{V_i} and $N_1Q_{V_i}$. Vehicles will generate a new random α_i, when it gets into the scope of RSUs. So pseudonym $FID_{V_i} = TID_{V_i} \oplus H_1(\alpha_i * PK_{TA})$ and the public key $PK_{V_i} = g^{\alpha_i}$ of one vehicle is diffident within the scope of different RSU. Therefore, the attacker cannot attack the vehicle by pseudonym and the public key. According to CDH problem which has been mention in section 3.2, the attacker cannot compute Q_{V_i} from $N_1Q_{V_i}$. However, $N_1Q_{V_i}$ is also different in the scope of different RSU. Therefore, the attacker also cannot attack the vehicle by $N_1Q_{V_i}$.

5.4 Non-repudiation

To avoid the vehicle deny ever sent the message which led to the accident, TA should be able to reveal TID of the sender from the message. In this scheme, TA can get the pseudonym from the message, and get the public key of the sender with RSUS' assist. Then, TA uses its private key PK_{TA}, the vehicle's the public key PK_{V_i} and the pseudonym to compute $TID_{V_i} = FID_{V_i} \oplus H_1(s * PK_{V_i}) = TID_{V_i} \oplus H_1(r_1 * PK_{TA}) \oplus H_1(s * PK_{V_i}) = TID_{V_i}$.

Finally, TA obtains TID_{V_i} of sender. In addition to TA and the vehicle itself, the other participants cannot know TID_{V_i}. Therefore, our scheme is non-repudiation.

5.5 Forward-security and backward-security

When the vehicle V_j has left the scope of RSU_i, RSU_i random selects $\gamma \in Z_q^*$ and computes the new group key is $GK = g^{\gamma} * \prod_{1}^{j-1}\prod_{j+1}^{n} g^{\lambda_i \gamma}$. The vehicle V_j only knows $g^{\lambda_1 \gamma}, \cdots, g^{\lambda_{j-1} \gamma} g^{\lambda_j \gamma}, \cdots, g^{\lambda_n \gamma}, g^{\gamma} * \prod_{1}^{j-1}\prod_{j+1}^{n} g^{\lambda_i \gamma}$, but could not know the new $g^{\lambda_i \gamma}$. According to the DDH problem, V_j cannot compute g^{γ} and the new group key. Therefore, our scheme is forward-secure.

When the vehicle V_i joined in the group, it received the message by RSUs to update the group key. However, the message is encode by the previous group key, vehicle cannot decode it and get the previous group key. Therefore, our scheme has to backward-secure.

6. Performance Evaluation

In this section, we compare with some related work from verification delay and transmission overheard and have a simulation on message delay by NS2.34.

6.1 Verification delay

The experiment is running on an Intel Pentium IV 3.0 GHZ machine. According to [24], the following results are obtained: the time of a pairing operation T_{par} is 4.5ms, the time of performing one point multiplication over an elliptic curve T_{mul} is 0.6ms and the time of a MapToPoint hash operation T_{mtp} is 0.6ms. The computation cost of the message certification mainly focus on the above three parameters, any other operations are not considered, such as each HMAC operation is assumed to take 0.006ms. **Table 2** shows the comparison of verification delay of other schemes.

Table 2. Comparison of verification delay

Scheme	Complete n verification	
	OBU	RSU
IBV [20]	$nT_{mul}+nT_{mtp}$	$(n+1)T_{mul}+nT_{mtp}+3T_{par}$
ECPP [26]	$4nT_{mul}+nT_{par}$	$2nT_{mul}+3nT_{par}$
RMAKA [27]	$4nT_{mul}$	$4nT_{mul}$
ACP [25]	nT_{mul}	$(2n+1)T_{mul}+3T_{par}$
Our scheme	$5nT_{mul}+nT_{mtp}+2nT_{par}$	$4nT_{mul}+2nT_{par}$

Notice that, **Table 2** shows the computations in once verification between RSUs and vehicles. In other compared schemes, legal vehicles need to conduct identity verification each time when vehicles pass a RSU, which results in frequent verifications. This paper only needs once verification for legal vehicles by using the group key transmission scheme, which reduces the times for legal vehicles' verification and thus enhance authentication efficiency as a whole.

Fig. 5 illustrates that the verification delay radio compared with others scheme for RSUs verify the vehicles when the illegal vehicles is 5%. From **Fig. 5,** with the increase of certified vehicles, the ratio of ACP, IBV are on the rise, but they are less than 1. Therefore, the verification delay of our scheme is less than them. And compared with the ECPP, RMAKA, the verification speed of our scheme is about 94% faster than that of ECPP and is about 75% faster than that of RMAKA.

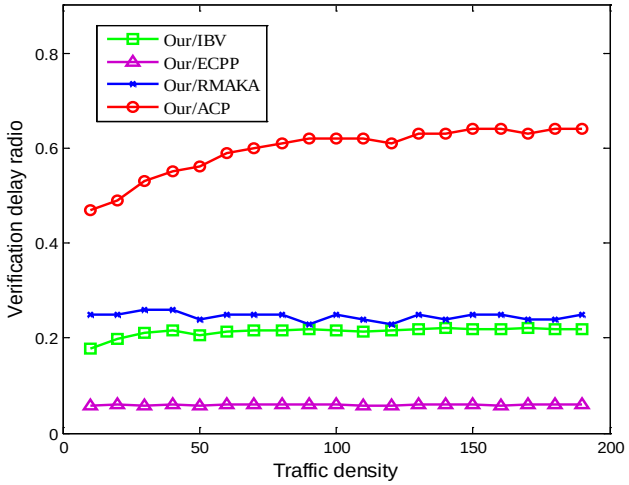

Fig. 5. Traffic density and Verification delay radio

6.2 Transmission overhead

Communication overhead is represented by the size of the transmission message. According to reference [28], each vehicle send message every 300ms. In this paper, the length of pseudonym is 42bytes and HMAC is 16bytes. Fig. 6 and **Table 3** illustrates that the transmission overhead of RMAKA, ABAKA, ARGBV and our scheme. From **Fig. 6**, we can see that the transmission overhead of our scheme is least.

Table 3. Comparison of transmission overhead

Scheme	Send n messages (bytes)
	$OBU \rightarrow RSU$
RMAKA [27]	167n
ABAKA [30]	84n
ARGBV [31]	63n
Our scheme	58n

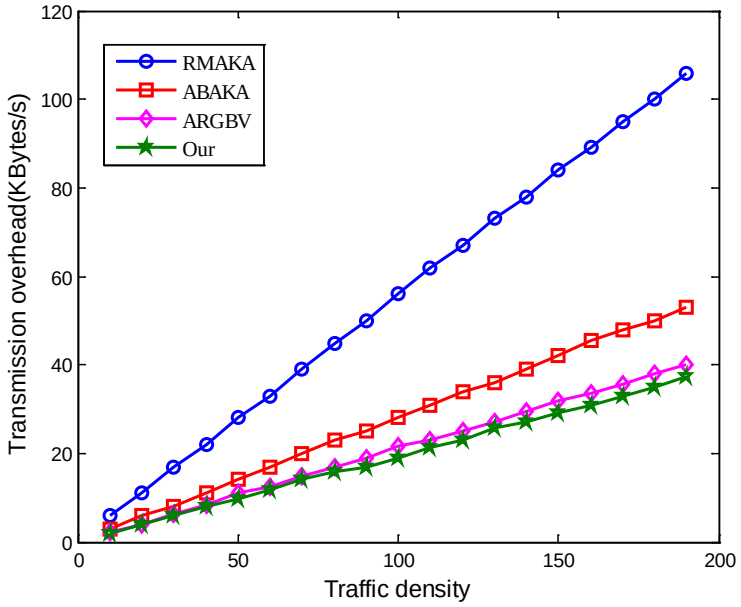

Fig. 6. Traffic density and Transmission overhead

6.3 Simulation

In order to reinforce experiment authenticity and feasibility, the road model and vehicle movement parameters in the map adopt the true data of California Emeryville city's 80th interstate on 2005 April 13 which is provide by Federal Highway Administration's next generation simulation project[29]. The road in experiment is 1000 meters long, which includes 5 lanes and an auxiliary road. Two RSUs are deployed at the 200 meters distance and 800 meters distance respectively. Our experiment adopts data from vehicles that move towards south from 14:40:00-14:45:00 of that day for that there are great traffic flow and high traffic density in this period thus to get more objective experiment results. Therefore, the road select is 1000m.

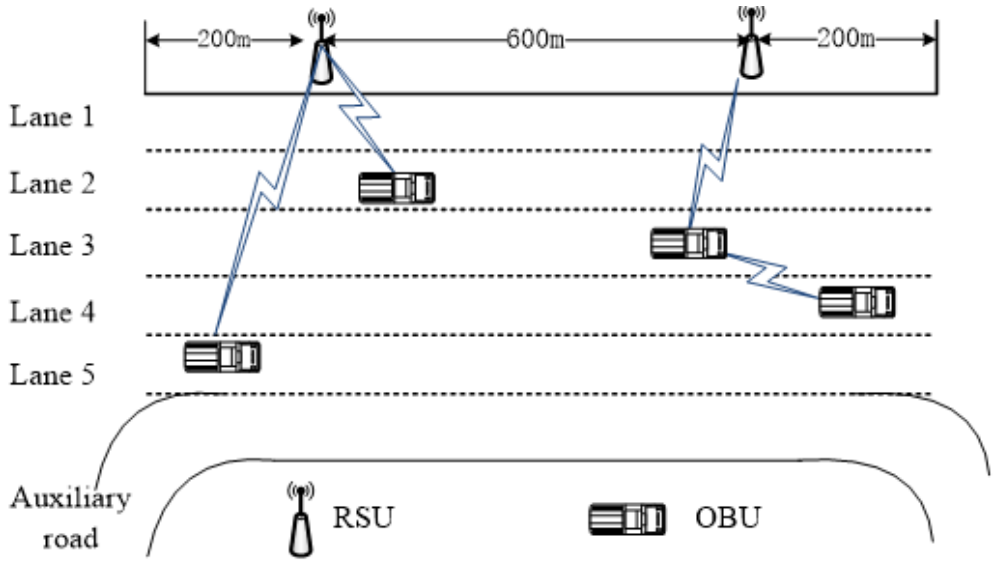

Fig. 7. Simulation experiment environment

The main simulation parameters are list in **Table 4**

Table 4. Simuliation parameters

Simulation parameters	Value
Road length	1000 m
Simulation time	20 s
Message size	200 bytes
Broadcast interval	300 ms
Interval variance	0.05 s
Communication Range of RSU and Vehicles	600 m
Communication Range of Vehicles	300 m
Bandwidth	6 Mbps

We define the average delay of a message as [25]:

$$Delay = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{M_i}\sum_{m=1}^{M}(T_{Creat}^{n\text{-}m} + T_{Transmission}^{n\text{-}m\text{-}k} + T_{verify}^{n\text{-}m\text{-}k}) \tag{3}$$

Here N is the number of the vehicles, M_i is the number of messages sent by vehicle V_i, $T_{Creat}^{n\text{-}m}$ is the time that the Vehicle or RSU create the message, $T_{Transmission}^{n\text{-}m\text{-}k}$ is the transmission time that entity n sent message to entity k, $T_{verify}^{n\text{-}m\text{-}k}$ is the time that entity k verify the message from entity n.

Fig. 8 illustrates the impact of vehicle's number versus average delay. In this paper, the communication of us divided on two aspects. One is between OBU, and another is between RSU and OBU. **Fig. 8** shows that the message delay also increase with the increase of vehicle number. The message delay of ABAKA, ARGBV and RMAKA are bigger than our scheme. Therefore, with the increase of vehicle quantity, the message delay of our scheme is least.

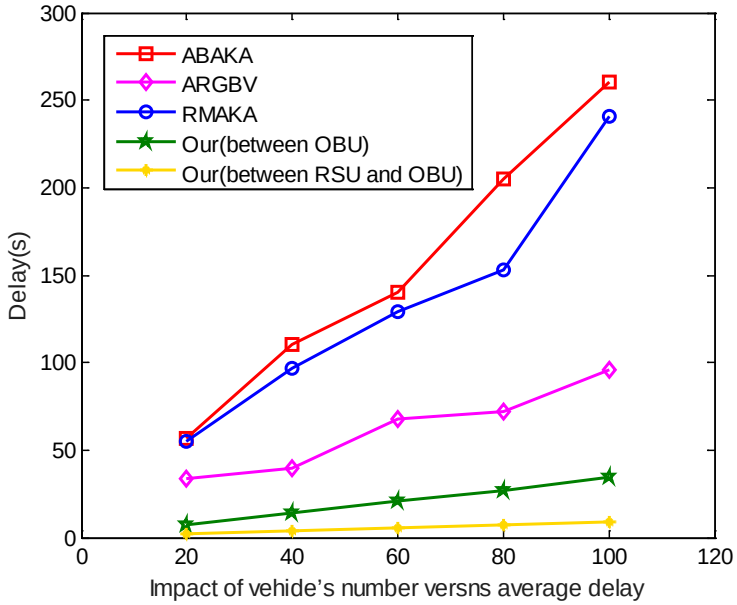

Fig. 8. The message delay and traffic density

7. Conclusion

In this paper, we propose a self-authenticated deniable efficient group key agreement scheme in VANET. The features of the scheme are as follows: (1) Employ the no certification public key system, the authentication process between vehicles and RSUs has no authentication center participated in, which prevents the time delay problem of TA certification. (2) Reduce the frequency of legal vehicles' certification and avoid tracking legal vehicles through RSUs by using the deniable group key transmission scheme. (3) In order to alleviate the workload of the group leader and eliminate the probability of failure problem for single point by using key negotiation instead of distributing group key by group leader. In the communication protocol proposed in this paper, the vehicle is authenticated by RSUs fixed on the road. However, in practical applications, the deployment of a large number of RSUs takes a large amount of cost, which is not conducive to the promotion and use of VANET. If the RSU is mobile, and even in the absence of RSU participation, 'how to authenticate the vehicle', will become a huge challenge of VANET in the future. Therefore, we will carry out a more in-depth research of the problems above in the future work.

Acknowledgement

This research is supported by the following funds: Natural Science Foundation of China (61300229), Six Talent Peaks Project of Jiangsu Province (DZXX-012), Natural science fund for colleges and universities in Jiangsu Province (Grant No.12KJD580002) and Traffic information fund of ministry of communications of China (Grant No. 2013-364-863-900).

References

[1] Akhtar R, Memon I, "Implementation of secure AODV in MANET[J]," in *Proc. of SPIE - The International Society for Optical Engineering*, 8768(2):03, 2013. Article (CrossRef Link).
[2] Liu J, Wan J, Wang Q, et al., "A survey on position-based routing for vehicular ad hoc networks[J]," *Telecommunication Systems*, 62(1):15-30, 2016. Article (CrossRef Link).
[3] Jiang S, Zhu X, Wang L., "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs[J]," *IEEE Transactions on Intelligent Transportation Systems*, 17(8): 2193-2204, 2016. Article (CrossRef Link).
[4] Arain Q A, Memon I, Deng Z, et al., "Location monitoring approach: multiple mix-zones with location privacy protection based on traffic flow over road networks[J]," *Multimedia Tools & Applications*, 1-45, 2017. Article(CrossRef Link).
[5] Arain Q A, Deng Z, Memon I, et al., "Privacy Preserving Dynamic Pseudonym-Based Multiple Mix-Zones Authentication Protocol over Road Networks[J]," *Wireless Personal Communications*,1-17, 2016. Article (CrossRef Link).
[6] Arain Q A, Uqaili M A, Deng Z, et al., "Clustering Based Energy Efficient and Communication Protocol for Multiple Mix-Zones Over Road Networks[J]," *Wireless Personal Communications*, 1-18, 2016. Article (CrossRef Link).
[7] Dai M, Chi S, Wang H, et al., "A New Zigzag-decodable Code with Efficient Repair in Wireless Distributed Storage[J]," 1-1, 2016. Article (CrossRef Link).
[8] Whaiduzzaman M, Sookhak M, Gani A, et al., "A survey on vehicular cloud computing[J]," *Journal of Network & Computer Applications*, 40(1):325-344, 2014. Article (CrossRef Link).
[9] Wang C, Shi D, Xu X, et al., "An anonymous data access scheme for VANET using pseudonym-based cryptography[J]," *Journal of Ambient Intelligence and Humanized Computing*, 7(1):63-71, 2016. Article (CrossRef Link).
[10] Wang M, Liu D, Zhu L, et al., "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication[J]," *Computing*, 98(7):685-708, 2016. Article (CrossRef Link).
[11] Ding Q, Li X, Jiang M, et al., "Reputation Management in Vehicular Ad Hoc Networks[C]," in *Proc. of International Conference on Multimedia Technology*, IEEE, 1-5, 2010. Article (CrossRef Link).
[12] Memon I, Arain Q A, Memon H, et al., "Efficient User Based Authentication Protocol for Location Based Services Discovery Over Road Networks[J]," *Wireless Personal Communications*, 1-20, 2017. Article (CrossRef Link).
[13] Memon I, Hussain I, Akhtar R, et al., "Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme[J]," *Wireless Personal Communications*, 84(2):1-22, 2015. Article (CrossRef Link).
[14] Memon I., "Authenticated Privacy Preserving for Continuous Query in Location Based Services[J]," *Journal of Computational Information Systems*, (9: 24):9857{9864, 2013. Article (CrossRef Link).
[15] Memon I., "A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks[J]," *Wireless Personal Communications*, 85(3):1167-1191, 2015. Article (CrossRef Link).
[16] Wasef A, Shen X., "MAAC: message authentication acceleration protocol for vehicular ad hoc networks[J]," 12(1):1-6, 2010. Article (CrossRef Link).

[17] Xiong H, Beznosov K, Qin Z, et al., "Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication[C]," in *Proc. of IEEE International Conference on Communications. arXiv*, 1-6, 2010. Article (CrossRef Link).
[18] 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[J]," *IEEE Transactions on Vehicular Technology*, 60(1):248-262, 2011. Article (CrossRef Link).
[19] Shim K A., "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks[J]," *IEEE Transactions on Vehicular Technology*, 61(4):1874-1883, 2012. Article(CrossRef Link).
[20] Zhang C, Lu R, Lin X, et al., "An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks[J]," in *Proc. of IEEE INFOCOM*, 246-250, 2008. Article (CrossRef Link).
[21] Wang X, Tague P., "ASIA: Accelerated secure in-network aggregation in vehicular sensing networks[C]," *Sensor, Mesh and Ad Hoc Communications and Networks. IEEE*, 514-522, 2013. Article (CrossRef Link) .
[22] Wagan A A, Jung L T., "Security framework for low latency vanet applications[C]," in *Proc. of International Conference on Computer and Information Sciences*, 1-6, 2014. Article (CrossRef Link).
[23] Zhu X, Jiang S, Wang L, et al., "Privacy-preserving authentication based on group signature for VANETs[C]," in *Proc. of IEEE GLOBECOM Workshops IEEE*, 4609-4614, 2013. Article (CrossRef Link).
[24] Chen Y, Ming-Xing H E, Zeng S K, et al., "Two-round Deniable Group Key Agreement Protocol[J]," *Journal of Cryptologic Research*, 2016. Article (CrossRef Link) .
[25] Jiang S, Zhu X, Wang L., "A conditional privacy scheme based on anonymized batch authentication in Vehicular Ad Hoc Networks[J]," 2375-2380, 2013. Article (CrossRef Link).
[26] Lu R, Lin X, Zhu H, et al., "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications[C]," in *Proc. of INFOCOM 2008. IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 13-18 April 2008*, Phoenix, Az, Usa. DBLP, 1229-1237, 2008. Article (CrossRef Link).
[27] Yang J H, Chang C C., "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem[J]," *Computers & Security*, 28(3-4):138-143, 2009. Article (CrossRef Link).
[28] Hu C, Chim T W, Yiu S M, et al., "Efficient HMAC-based secure communication for VANETs[J]," *Computer Networks*, 56(9):2292–2303, 2012. Article (CrossRef Link).
[29] Li J G, Lin Y P, Li R, et al., "Secure anonymous authentication scheme based on elliptic curve and zero-knowledge proof in VANET[J]," *Journal on Communications*, 34(5):52-61, 2013. Article(CrossRef Link).
[30] 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[J]," *IEEE Transactions on Vehicular Technology*, 60(1):248-262, 2011. Article (CrossRef Link).
[31] Wang L M, Xiaojun L I, Zhong H., "A revocable group batch verification scheme for VANET[J]," *Scientia Sinica*, 43(10) , 2013. Article (CrossRef Link).
[32] Huyen N T T, Jo M, Nguyen T D, et al., "A beneficial analysis of deployment knowledge for key distribution in wireless sensor networks[J]," *Security & Communication Networks*, 5(5):485-495, 2012. Article (CrossRef Link).
[33] Memon I, Mohammed M R, Akhtar R, et al., "Design and Implementation to Authentication over a GSM System Using Certificate-Less Public Key Cryptography (CL-PKC)[J]," *Wireless Personal Communications*, 79(1):661-686, 2014. Article (CrossRef Link).
[34] Memon I, Arain Q A., "Erratum to: Dynamic path privacy protection framework for continuous query service over road networks[J]," *World Wide Web-internet & Web Information Systems*, 1-33, 2016. Article (CrossRef Link).

[35] Akhtar R, Amin N U, Memon I, et al., "Implementation of secure AODV in MANET[C]," in *Proc. of International Conference on Graphic and Image Processing. International Society for Optics and Photonics*, 876803-876803-5, 2013. Article (CrossRef Link).
[36] Adu-Gyamfi D, Wang Y, Zhang F, et al, "Modeling the spreading behavior of passive worms in mobile social networks[C]," in *Proc. of International Conference on Information Management, Innovation Management and Industrial Engineering. IEEE*, 380-383, 2013. Article (CrossRef Link).

Mu Han received her Ph.D. degree from the School of Computer Science and Technology, Nanjing University of Science and Technology, China, in 2011. Currently she is an Associate Professor at the School of Computer Science and Communication Engineering, Jiangsu University. Her research interests include Cryptography, Security and Communication in vehicle ad hoc network (VANET) and Information Security, etc.

Lei Hua received her bachelor degree from Jiangsu University, China, in 2015. She is now a master degree candidate at the School of Computer Science and Communication Engineering, Jiangsu University, China. Her research direction is Security and Communication in VANET.

Shidian Ma received his master's degree from School of mechanical and automotive engineering, Hefei University of Technology, China, in 2005. He is currently an Associate Professor at School of Automotive Engineering Research Institute, Jiangsu University. His research interests are Automotive Electronic Control Technology, Road Traffic Active Safety Prevention and Control, Security and Communication in VANET.