sensors

MDPI

Article

A Secure and Efficient Group Key Agreement Scheme for VANET

Lianhai Liu [1,2], Yujue Wang [3], Jingwei Zhang [2,*] and Qing Yang [2]

[1] School of Information Science and Engineering, Central South University, Changsha 410006, China; liulianhai@csu.edu.cn

[2] School of Computer Science and Information Security, Guilin University Of Electronic Technology, Guilin 541004, China; gtyqing@hotmail.com

[3] Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China; yjwang@guet.edu.cn

* Correspondence: gtzhjw@gmail.com

Received: 8 November 2018 ; Accepted: 21 January 2019 ; Published: 24 January 2019

Abstract: A vehicular ad hoc network (VANET) is a special mobile ad hoc network that provides vehicle collaborative security applications using intervehicle communication technology. The method enables vehicles to exchange information (e.g., emergency brake). In VANET, there are many vehicle platoon driving scenes, where vehicles with identical attributes (location, organization, etc.) are organized as a group. However, this organization causes the issue of security threats (message confidentiality, identity privacy, etc.) because of an unsafe wireless communication channel. To protect the security and privacy of group communication, it is necessary to design an effective group key agreement scheme. By negotiating a dynamic session secret key using a fixed roadside unit (RSU), which has stronger computational ability than the on-board unit (OBU) equipped on the vehicle, the designed scheme can help to provide more stable communication performance and speed up the encryption and decryption processes. To effectively implement the anonymous authentication mechanism and authentication efficiency, we use a batch authentication scheme and a shared secret key mechanism among the vehicles, RSUs and trusted authority (TA). We design an efficient group secret key agreement scheme, which satisfies the above communication and security requirements, protects the privacy of vehicles, and traces the real identity of the vehicle at a time when it is necessary. Computational analysis shows that the proposed scheme is secure and more efficient than existing schemes.

Keywords: vehicular ad hoc network; group key agreement; bilinear maps; batch verification; authentication; shared secret key

1. Introduction

A VANET is a special mobile ad hoc network, which is mainly composed of OBUs installed on vehicles and RSUs. The VANET can be used to achieve vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication [1,2]. Vehicles in VANET can generate their own driving state information (acceleration, lane changing information, etc.) and collect traffic information such as traffic congestion and slippery road. These information can be used by the vehicles in VANET to improve driving comfort and safety.

Many traffic jams or traffic accidents are caused by the driver's inability to predict instantaneous and variable road conditions. Intervehicle communication can exchange information about road conditions and vehicle status in time, which helps the driver to determine the driving environment in advance. Thus, effective intervehicle communication can reduce traffic accidents and alleviate traffic congestion. There are three communication modes: unicast, multicast, and broadcast. On some occasions, the emergency message must only be forwarded to specific vehicles. If the message is forwarded by unicast, it takes much time to inform specific vehicles on a road section. If the message is forwarded by broadcast, it is easy to cause a broadcast storm. Multicast is a more efficient method to exchange messages in VANET. However, the wireless channel of VANET may be easily jammed and monitored, which results in data monitoring, tampering and replaying [3]. Some private information of vehicles such as the driver information, driving track, and parking position may be leaked on these channels [4], which would result in potential threats to the drivers and passengers [2]. Therefore, the security of VANET data transmitted on these communication channels must be enhanced.

With the development of group communication application in VANET, the group key agreement mechanism is widely studied. Because of the lower density and high mobility of vehicles [5], the secure and effective group key agreement mechanism for VANET becomes extremely important. Compared to mobile ad hoc networks (MANETs) [6], the vehicles in VANET have lower fixity, communication ability and computing power than the RSU. Therefore, to improve the efficiency of the group key agreement, people can use the advantages of the RSU to complete the computing and communication. The vehicles in VANET may move fast and must dynamically change the running route because there are always vehicles joining or leaving a communication group. A secure secret key agreement scheme must ensure that the legality of new vehicles should be verified before joining the communication group. In addition, when some vehicle leaves the communication group, the RSU can revoke its group key. Therefore, designing a secure and efficient group key agreement for VANET is the key to realize group communication.

In recent years, many studies have been conducted on group key agreement in VANET. A batch authentication scheme [7] was presented to improve the computation efficiency, but the integrity of the request messages were not checked before the batch authentication. Hai [8] proposed an authenticated group key agreement scheme using bilinear pairings, which satisfies all secure group communication requirements for VANET. However, this scheme authenticates vehicles using certificates, which results in low authentication efficiency. Therefore, it is a great challenge to design an efficient and secure group secret key agreement for VANET.

To address the aforementioned problems, we present a group secret key agreement scheme for VANETs with batch verification. Our main contributions are summarized as follows:

- The RSU is used at the main node in the group key agreement. Since the RSU has more powerful computing and communication capabilities than the vehicles, the communication cost can be reduced, and the key negotiation efficiency can be increased.
- The shared secret key mechanism is used among the vehicles, RSUs and TA to effectively implement the anonymous authentication mechanism.
- The RSU verifies a set of signatures in the batch, which greatly improves the authentication performance compared to individually verification.

The remainder of this paper is organized as follows. We describe the related works in Section 2. The system model and security requirements for VANET are defined in Section 3. We present a secure and efficient group key agreement (SEGKA) scheme in Section 4 and analyze the security and evaluate the performance for SEGKA in Section 5. Finally, the paper is concluded in Section 6.

2. Related Work

The VANET provides a series of applications, such as efficiency applications [9,10] (urban traffic management, path planning, etc.), commercial applications [11] (location-based services, path planning etc.), information entertainment applications (video sharing, social networks, etc.), and security applications [12–15] (rear end warning, road ice testing, etc.). However, the vehicles communicating in the wireless network are easily attacked, particularly when the vehicles have private messages to be shared with others in the same group. Therefore, VANET must build secure channels for group communication. The emergence of group-oriented communication applications has triggered research on group communication security and privacy protection. A difficult problem of group communication is to design an effective group membership authentication key agreement mechanism.

In VANET, the relative position among vehicles may fast and frequently changed, thus the vehicles are often dynamically divided into groups to perform broadcast communication, i.e., group communication. Vehicle group communication refers to communication among vehicles with the same attribute. A secure group communication scheme should be able to ensure that once a new vehicle joins the group and becomes a legitimate group member, it could receive or send messages in the group in time. Also, once some node moves far away, there should be a mechanism to let it leave the current group, so that it cannot continue to enjoy the rights of a legitimate group member and cannot continue to receive or send messages in this group. The group key agreement schemes can be divided into two types: a central node to assign a communication key to other members, and every group member provides a partial key and finally forms a group key. Although the communication mechanism using the asymmetric encryption technology can well satisfy this requirement, it is not suitable for VANET applications because it does not account for the vehicle's computation capability and complicated key management. To reduce the cost of computing and improve communication efficiency, it is preferable to use symmetrical key encryption in designing VANET communication schemes.

Because of the fast-moving speed and limited communication scope, the secure and effective group key agreement mechanism becomes extremely important. To handle the security and efficiency issues, Han, Hua and Ma [16] proposed a self-authentication and deniable efficient group key agreement (SADEGKA) protocol. The certification efficiency is improved with the group key transmission method without certification authority and prevents the attacker from attacking the legal vehicle through a deniable group key agreement method. However, this scheme is not scalable because every vehicle must verify other vehicles during the key agreement, which increases the verification delay. Chim et al. [17] studied privacy protection and presented a method to verify a batch of signatures within a short time period using two shared secrets. This method enables the existing vehicles to form a group for secure communications. Meanwhile, the RSU is involved in the signature verification process, which greatly mitigates the vehicle's computing burden. Our scheme also uses shared secrets for the group key agreement to improve the group key agreement efficiency. The RSU always has more powerful computation ability than vehicles; thus, it can speed up the vehicle legality certification. Lei, Yu and Xian [18] proposed an ID-based group authenticated key agreement protocol based on the DBDH assumption and considered the dynamic issue of group communication. In this scheme, the vehicles cannot be anonymous, and their privacy cannot be protected. Zheng et al. [19] introduced an ID-based authenticated group key agreement protocol without the management of certifications. However, both [18,19] have privacy protection problems.

3. Preliminaries

In this section, we briefly introduce the system model and bilinear maps. Some notations are shown in Table 1.

3.1. System Model

As shown in Figure 1, a typical VANET system includes three types of entities: OBU, RSU and TA.

- Each vehicle is equipped with an OBU, which is responsible for the communication with other neighbor OBUs or RSUs using the dedicated short range communication (DSRC) protocol. The OBU has limited computation and storage capabilities. Vehicles periodically broadcast messages of their driving state, e.g., emergency braking. Since the OBU is semicredible, it is necessary for vehicles to sign and authenticate messages transmitted in such unreliable transmission scenarios. Otherwise, the communication channel would be vulnerable to attacks from malicious attackers.

- RSUs are always distributed on both the roadside and intersections, which are responsible for the vehicle-to-infrastructure communication and infrastructure-to-TA communication. They periodically broadcast the road information (e.g., road congestion) and local environment (e.g., gas station and parking lot) to vehicles to improve the traffic condition. The RSU is also semicredible. The RSU has more powerful computation and communication capability than OBU; thus, it is notably suitable to authenticate vehicles and distribute keys to vehicles, which reduces the authentication latency and improves the communication efficiency [20].
- TA is a trustworthy third party, which is responsible for the generation and distribution of the private and public keys for OBUs and RSUs. The public key of every entity in the system is certified by a trusted party, so that the corresponding certificate can be publicly verified. This trusted party is also responsible for certificate managements. It also initializes the system and generates system parameters. Before performing the key agreement, OBUs and RSUs must be legally registered in TA. TA allocates the related authentication parameters to RSUs and OBUs. TA can trace the real vehicle identification when it is necessary to realize traceability [21].

Table 1. Notations.

Notations	Definitions
TA	Trusted authority
s	A master key of TA
P_{pub}	A public key of TA
PID_i	The pseudo identity of vehicle
TID_i	The true identity of vehicle
V_i	The vehicle number
VID_i	V_i's verification identity
$ENC_k(M)$	Encrypting function of M using key k
h	One secure one-way hash function
H	A MapToPoint hash function
PK_{RSU}	A public key for the RSU
SK_{RSU}	A private key for the RSU
T_i	The freshness of time
G_1	The cyclic additive group with prime order q
G_2	The cyclic multiplicative group with the prime order q

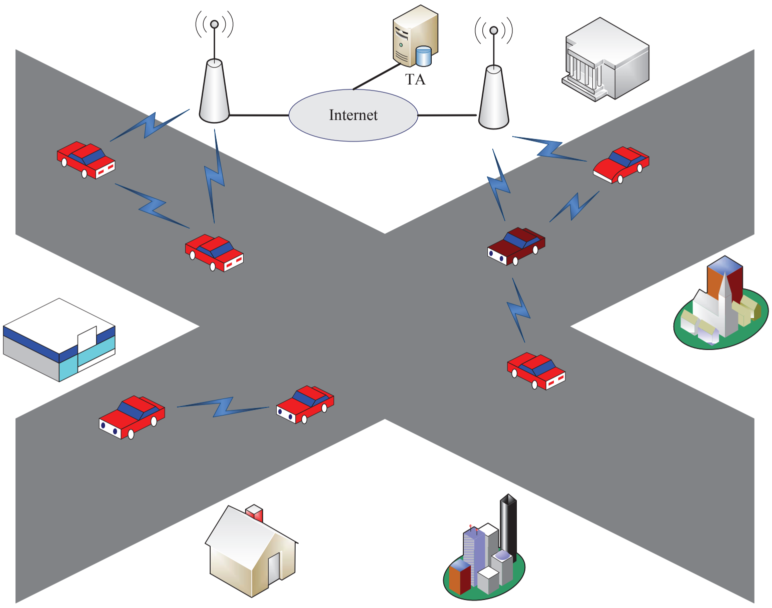

Figure 1. System model.

3.2. Bilinear Maps

Let G_1 be a cyclic additive group with prime order q and G_2 be a cyclic multiplicative group with the same prime order q. The bilinear map is denoted as the mapping $e : G_1 \times G_1 \rightarrow G_2$, which has the following properties:

(1) *Bilinearity*

$$e(aP, bQ) = e(P, Q)^{ab}$$

where $P, Q \in G_1, a, b \in_R Z_q^*$.

(2) *Nondegeneracy*

$$e(P, P) \neq 1$$

where P is the generator of G_1.

(3) *Efficiency*

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

3.3. Mathematical Assumptions

Definition 1. *Discrete Logarithm Problem (DLP): $\forall a \in {}_R Z_q^*$, given $P, aP \in G_1$, compute a.*

Definition 2. *Computational Diffie-Hellman Problem (CDHP): $\forall a, b \in {}_R Z_q^*$, given $P, aP, bP \in G_1$, compute abP.*

Definition 3. *Decisional Diffie-Hellman Problem (DDHP): $\forall a, b, c \in_R Z_q^*$, given $P, aP, bP, cP \in G_1$, decide whether $cP = abP$.*

4. Scheme Design

To address the security and privacy issues of VANET group communication, this paper designs a secure and efficient group key agreement scheme for VANET in bilinear groups. The vehicles will apply for their own group when registering with the TA. TA will authenticate them and assign relevant group identification according to vehicle attribute. The RSU computes the group key for the vehicles in its coverage according to the group identification. When vehicles are driving in the same RSU coverage area, they with the same group identification initiate group key negotiation due to communication needs. With the relatively fixed location, wide coverage, strong communication and computing capabilities, the RSU is selected as the manager of the group to complete the signature batch authentication of the vehicles and compute and distribute the group key. This can greatly improve the negotiation efficiency of the group key and reduce the communication delay. Figure 2 depicts the process of our group key agreement.

(1) TA initializes the system parameters and sends them to vehicles and RSUs.
(2) The RSU requests registration to TA.
(3) TA returns the verification information.
(4) Vehicle sends the vehicle registration information to TA.
(5) TA returns the verification information.
(6) TA sends the partial vehicle verification information (the shared key, etc.) to RSUs.
(7) Vehicle requests the group key agreement and sends its signature to the RSU.
(8) The RSU sends the final group key agreement result to vehicle according to the signature verification.

The scheme contains seven modules, i.e., parameter initialization, vehicle and RSU registration, vehicle signing, RSU verification, group key generation, group member joining, and group member leaving.

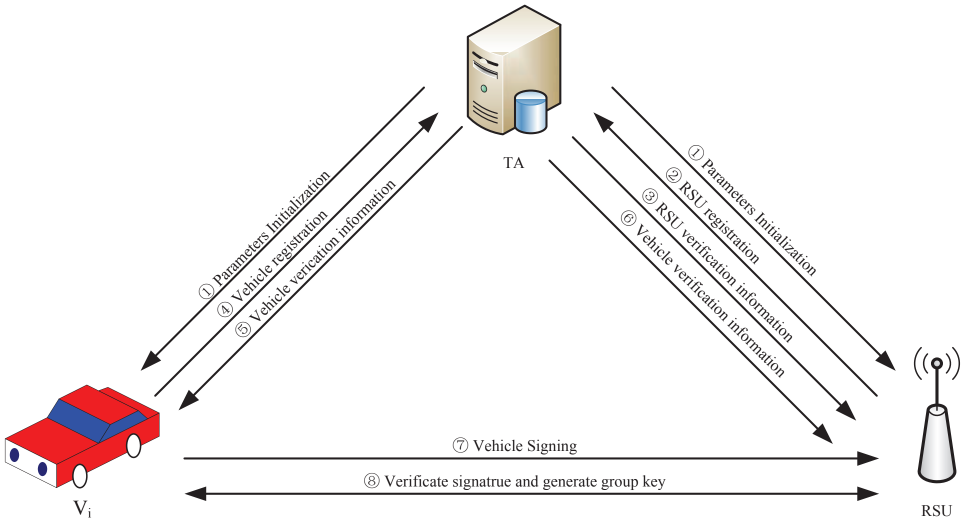
TA
① Parameters Initialization
④ Vehicle registration
⑤ Vehicle verication information
① Parameters Initialization
② RSU registration
③ RSU verification information
⑥ Vehicle verification information
⑦ Vehicle Signing
⑧ Verificate signatrue and generate group key
V_i
RSU

Figure 2. The process of group key agreement.

4.1. Parameter Initialization

TA generates some initial system parameters. This process must only be performed once for the entire system. However, TA may periodically update the system master key to enhance the security performance. The detailed processes are as follows.

(1) TA selects a cyclic additive group G_1 and a cyclic multiplicative group G_2 that have bilinear map properties.
(2) TA selects a random number $s \in_R Z_q^*$ as the system master key and computes $P_{pub} = sP$ as the corresponding public key.
(3) TA selects two cryptographic hash functions: $H : G_1 \to Z_q^*, h : \{0,1\}^* \to Z_q^*$.
(4) TA broadcasts the public parameters $paras = \{G_1, G_2, e, q, P, P_{pub}, H, h\}$ to all vehicles and RSUs, as shown in Figure 3.

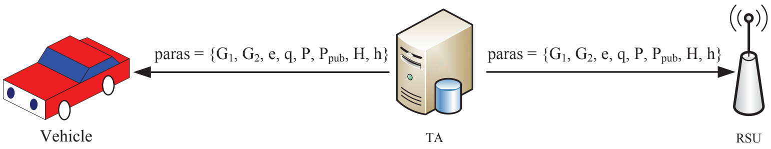
paras = {G1, G2, e, q, P, Ppub, H, h}
paras = {G1, G2, e, q, P, Ppub, H, h}
Vehicle
TA
RSU

Figure 3. Parameter initialization.

4.2. Vehicle and RSU Registration

The vehicle and RSU are registered at TA. TA assigns the corresponding registration information to them, as shown in Figure 4.

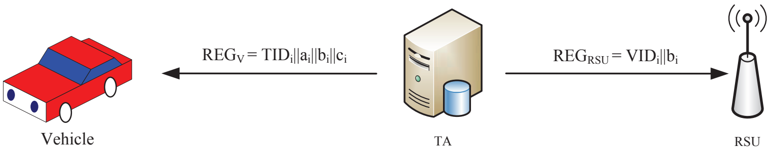

Figure 4. Vehicle and RSU registration.

TA assigns unique n-dimensional column vectors TID_i, a_i and b_i to every legitimate vehicle. TID_i denotes the vehicle's real identity, a_i is the shared secret between vehicle V_i and TA, and b_i is the shared secret between vehicle V_i and the RSU. TA computes $c_i = sH(a_i \oplus TID_i)$ and sends $REG_V = TID_i||a_i||b_i||c_i$ to vehicle V_i through a secure channel.

TA computes V_i's verification $VID_i = a_i \oplus TID_i$ and sends $REG_{RSU} = VID_i||b_i$ to the RSU through a secure channel.

4.3. Vehicle Signing

In this module, the RSU authenticates the vehicles to prepare for the group key agreement. The detailed processes are described below.

Vehicle V_i selects a random nonce r_i, which is used to prevent an attacker from tracing the vehicle. Then, it generates a pseudo identity PID_i that is composed of $PID_{i,1} = r_i P$ and $PID_{i,2} = VID_i \oplus H(b_i \cdot PID_{i,1})$

V_i calculates the signature $\sigma_i = c_i + b_i c_i h(M_i)$, where $M_i = PID_i || T_i$ and T_i is the signing time. Then, it provides the information $D_i = r_i || PID_i || \sigma_i || T_i$ to the RSU through a secure channel, as shown in Figure 5.

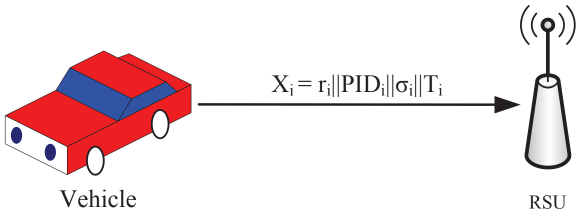

Figure 5. Vehicle signing.

4.4. RSU Verification

This module enables the RSUs to verify the vehicles' signatures. The verification can be performed as single verification and batch verification.

(1) Single verification

When the RSU receives the vehicle V_i's signature D_i, it decrypts D_i with its secret key SK_{RSU} and checks the freshness of time T_i. If T_i is fresh, that is, T_i is within the validity period, the RSU continues to find out V_i's verification public key VID_i and shared secret key b_i; then, it verifies whether the received $PID_{i,2}$ is equal to $VID_i \oplus H(b_i \cdot PID_{i,1})$. If it is true, the RSU verifies Equation (1):

$$e(\sigma_i, P) = e(H(VID_i)(1 + b_i h(M_i)), P_{pub}). \tag{1}$$

Proof of correctness:

$$\begin{aligned}
&L.H.S \\
&= e(c_i + b_i c_i h(M_i), P) \\
&= e(c_i, P) e(b_i c_i h(M_i), P) \\
&= e(sH(a_i \oplus TID_i), P) e(b_i sH(a_i \oplus TID_i) h(M_i), P) \\
&= e(H(VID_i), sP) e(b_i H(VID_i) h(M_i), sP) \\
&= e(H(VID_i), P_{pub}) e(b_i H(VID_i) h(M_i), P_{pub}) \\
&= e(H(VID_i)(1 + b_i h(M_i)), P_{pub}) \\
&= R.H.S
\end{aligned}$$

Therefore, Equation (1) holds.

(2) Batch verification

Assume the RSU receives a batch of signatures $D_1, D_2, \cdots, D_n$ from vehicles $V_1, V_2, \cdots, V_n$. First, the RSU checks the freshness of every time T_i $(1 \le i \le n)$. If all are fresh, then the RSU continues to find the vehicle's public verification key and the shared secret key and checks whether the second part of the pseudo identity is valid. If all are valid, the RSU verifies the signatures in the batch by checking Equation (2).

$$e(\sum_{i=1}^{n} \sigma_i, P) = e(\sum_{i=1}^{n} H(VID_i)(1 + b_i h(M_i)), P_{pub}). \tag{2}$$

Proof of correctness:

$$\begin{aligned}
& L.H.S \\
& = e(\sum_{i=1}^{n} (c_i + b_i c_i h(M_i)), P) \\
& = e(\sum_{i=1}^{n} c_i, P) e(\sum_{i=1}^{n} b_i c_i h(M_i), P) \\
& = e(\sum_{i=1}^{n} sH(a_i \oplus TID_i), P) \\
& \quad e(\sum_{i=1}^{n} b_i sH(a_i \oplus TID_i) h(M_i), P) \\
& = e(\sum_{i=1}^{n} H(VID_i), sP) e(\sum_{i=1}^{n} b_i H(VID_i) h(M_i), sP) \\
& = e(\sum_{i=1}^{n} H(VID_i), P_{pub}) e(\sum_{i=1}^{n} b_i H(VID_i) h(M_i), P_{pub}) \\
& = e(\sum_{i=1}^{n} H(VID_i)(1 + b_i h(M_i)), P_{pub}) \\
& = R.H.S
\end{aligned}$$

Therefore, Equation (2) holds.

4.5. Group Key Generation

After the vehicles are authenticated, the RSU generates the group key for the vehicles. The detailed processes are as follows.

(1) The RSU randomly selects a random nonce $d_{RSU} \in {}_R Z_q^*$, computes $D_i = d_{RSU} PID_{i,1}$, and computes the group key K_{RSU} as follows:

$$K_{RSU} = e(\sum_{i=1}^{n} D_i, d_{RSU} P) \tag{3}$$

(2) The RSU computes its signature $\sigma_{RSU} = SK_{RSU} H(D)$, where $D = D_1 || D_2 || \cdots || D_n$. Then, it broadcasts $Z = \sigma_{RSU} || D$ to the vehicles, as shown in Figure 6.

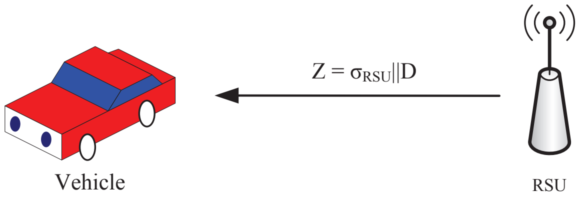

Figure 6. Group key generation.

(3) After vehicle V_i receives Z, it first verifies the signature of the RSU by checking Equation (4) as follows.

$$e(\sigma_{RSU}, P) = e(H(D), PK_{RSU}). \tag{4}$$

(4) If the signature of the RSU is valid, vehicle V_i computes group key K_i as follows.

$$K_i = e(\sum_{i=1}^{n} D_i, r_i^{-1} D_i) \tag{5}$$

4.6. Group Member Joining

Suppose that $V_1, V_2, \cdots, V_n$ have a group key as described. The detailed process of a new vehicle V_a joining the group is described as follows.

(1) V_a selects a random nonce r_a and generates a pseudo identity $PID_a = (PID_{a,1}, PID_{a,2})$, where $PID_{a,1} = r_a P, PID_{a,2} = VID_a \oplus H(b_a \cdot PID_{a,1})$. Then, V_a calculates the signature $\sigma_a = r_a H(PID_a) + b_a c_a H(T_a)$ and sends $D_a = ENC_{PK_{RSU}}(r_a || PID_a || \sigma_a || T_a)$ to RSU.

(2) When the RSU receives signature D_a of vehicle V_a, it decrypts D_a with its secret key SK_{RSU} and checks the freshness of time T_a. If the time is fresh, the RSU continues to find the public verification key VID_a of V_a and shared secret key b_a. The RSU verifies whether the received $PID_{a,2}$ is equal to $VID_a \oplus H(b_a \cdot PID_{a,1})$. If it holds, the RSU verifies V_a's signature as shown in Equation (1). If the signature is valid, the RSU allows for vehicle V_a to join the group. Then, the RSU reselects a random nonce $d'_{RSU} \in_R Z_q^*$ and recomputes $D'_i = d'_{RSU} PID_{i,1} (1 \leq i \leq n)$ and $D_a = d'_{RSU} PID_{a,1}$. The RSU computes the group key K'_{RSU} as follows.

$$K'_{RSU} = e(\sum_{i=1}^{n} D'_i + D_a, d'_{RSU} P) \tag{6}$$

(3) The RSU computes its signature $\sigma'_{RSU} = SK_{RSU} H(X')$, where $X' = D'_1 || D'_2 || \cdots || D'_n || D_a$. Then, it broadcasts $Z' = \sigma'_{RSU} || X'$ to all vehicles in the group.

(4) When vehicles including V_a receive Z', they verify the signature of the RSU as defined in Equation (4). If the signature is valid, they compute a new group key K'_i as follows.

$$K'_i = e(\sum_{i=1}^{n} D'_i + D_a, r_i^{-1} D'_i) \tag{7}$$

4.7. Group Member Leaving

Suppose that $V_1, V_2, \cdots, V_n$ have a group key as described above. Let V_n be a vehicle leaving the group. The RSU should update the group key for the remaining $n-1$ vehicles. The detailed process of the group key updating is described as follows.

(1) The RSU selects a random nonce $d'_{RSU} \in_R Z_q^*$ and computes $D'_i = d'_{RSU} PID_{i,1}$ $(1 \leq i \leq n-1)$. The RSU computes the group key K'_{RSU} as follows.

$$K'_{RSU} = e(\sum_{i=1}^{n-1} D'_i, d'_{RSU} P) \tag{8}$$

(2) The RSU computes the signature $\sigma'_{RSU} = SK_{RSU} H(X')$, where $D' = D'_1 || D'_2 || \cdots || D'_{n-1}$. Then, it broadcasts $Z' = \sigma'_{RSU} || X'$ to the vehicles.

(3) After the vehicles receive Z', they verify the signature of the RSU as shown in Equation (4). If the signature is valid, they compute a new group key K'_i as follows.

$$K'_i = e(\sum_{i=1}^{n-1} D'_i, r_i^{-1} D'_i) \tag{9}$$

5. Scheme Analysis

In this section, we analyze the correctness, security and performance of our proposed dynamic group key agreement scheme.

5.1. Correctness Analysis

Given the group secret keys K_i and K_j generated by two vehicles V_i and V_j, we have:

$$PID_{i,1} = r_i P, D_i = d_{RSU} PID_{i,1}$$

$$PID_{j,1} = r_j P, D_j = d_{RSU} PID_{j,1}$$

Thus,

$$r_i^{-1} D_i = d_{RSU} P$$
$$r_j^{-1} D_j = d_{RSU} P$$

$$\begin{aligned} &K_i \\ &= e(\sum_{k=1}^{n} D_i, r_i^{-1} D_i) \\ &= e(\sum_{k=1}^{n} D_i, d_{RSU} P) \\ &= e(\sum_{k=1}^{n} D_i, r_j^{-1} D_j) \\ &= K_j \end{aligned}$$

Therefore, the two keys K_i and K_j are identical.

5.2. Security

In this section, we present detailed analyses on the security and privacy protection of our scheme.

5.2.1. Forward Security

Forward security indicates that even if an attacker can obtain the previous group secret key, it cannot calculate the secret keys of the group in future. In other words, when some vehicle leaves the communication range of the RSU, the RSU will regenerate a random number d_{RSU} for the group key generation and recalculate a secret key from the remaining vehicles D_i. Thus, the proposed scheme offers forward security.

5.2.2. Backward Security

Backward security indicates that even if the attacker holds the current group key, it cannot calculate the group keys before it joins the group. In other words, before the vehicle enters the communication range of the RSU, it does not hold the previous random number d_{RSU} for the part of the group key, which implies that it cannot calculate the previous group keys. Therefore, the scheme offers the backward security.

5.2.3. Replay Attack Resistance

In the scheme, D_i generated by the RSU is different from the secret keys of the vehicles, where a notably strong collision-resistant one-way function H is used. Therefore, the group key negotiated is highly independent. In addition, because of the difficulty of $CDHP$, it is not feasible for any attacker to calculate the secret keys in polynomial time.

5.2.4. Anonymity

$PID_i = PID_{i,1}||PID_{i,2}$ is a pseudo identity, which contains two random numbers b_i and r_i generated by TA and the vehicle, respectively. Thus, PID_i can well protect the vehicle's privacy. Since the attacker cannot calculate the true identity $TID_i = a_i \oplus PID_{i,2} \oplus H(b_i \cdot PID_{i,1})$, the proposed scheme supports anonymity.

5.2.5. Traceability

The true identity of the vehicle can only be extracted by TA. Since TA has stored (TID_i, a_i, b_i, VPK_i) during the vehicle registration phase, it can verify the given pseudo identity $PID_i = PID_{i,1}||PID_{i,2}$. The verification process is shown as follows.

$$\begin{aligned} & a_i \oplus PID_{i,2} \oplus H(b_i \cdot PID_{i,1}) \\ & = a_i \oplus VPK_i \\ & = TID_i \end{aligned}$$

Therefore, the proposed scheme enables TA to trace the true identities of the vehicles.

5.2.6. Replay Attack Resistance

There is a timestamp T_i in the signature generated by vehicle, which enables the RSU to check the freshness of T_i to prevent the replay of request for group key generation. Therefore, the proposed scheme can satisfy the replaying resistance.

5.3. Performance and Comparison

In this section, the proposed scheme is compared with existing schemes [8,16,22] in terms of computation overhead. Jiang, Zhu and Wang [22] proposed a conditional privacy (ACP) scheme based on anonymized batch authentication in vehicular ad hoc networks. Hai [8] proposed an authenticated group key Agreement (AGKA) scheme for mobile communication based on bilinear. For comparison, only the time-consuming multiplication/division and bilinear pairing operations are considered, and the other efficient operations such as point addition are omitted. Let T_{par} be the execution time of a pairing operation, T_{mul} be the execution time of performing a scale multiplication over an elliptic curve, Terminal be the user terminal node, and ACS be the access control server. The comparison is summarized in Table 2. As shown in Table 2, every procedure of our scheme enjoys constant computing costs, whereas the costs of existing schemes are linear with the group size. With the increase of the number of vehicles, the advantages of our scheme are more and more obvious, that is, the computation costs would not increase. Since both our scheme and ACP use the batch verification method, RSU takes less computations than the other two schemes. Note that OBU in [22] should take n multiplications, which requires more computation resources than our scheme. Although the computation cost of OBU in [8] is the same as that of our scheme, there requires a complicated certificate management mechanism, which affects the overall secret key negotiation efficiency.

Table 2. Computation Overhead Comparison.

Scheme	OBU/Terminal	RSU/ACS
ACP [22]	nT_{mul}	$3T_{par} + (2n+1)T_{mul}$
AGKA [8]	$3T_{par} + T_{mul}$	$(2n-1)T_{par} + (n+1)T_{mul}$
SADEGKA [16]	$2nT_{par} + 5nT_{mul}$	$2nT_{par} + 4nT_{mul}$
Our scheme	$3T_{par} + T_{mul}$	$3T_{par} + T_{mul}$

We conducted experiments on a system with Intel(R) Core(TM) i5-5200U CPU at 2.20 GHz and 8.00 MB memory, using Pairing Based Cryptography Library (PBC) [23]. The elliptic curve is of Type A ($y^2 = x^3 + x$), where the element size of group G is 256 bits and the size of order p is 160 bits. We use Network Simulator 3 (NS3) as communication protocol simulator and follow the IEEE 802.11p standard. Our vehicle mobility model is based on the statistical analysis of the real GPS traces, which includes 360,000 records for a 1043 vehicles network. We extract 50 vehicle traces for delay evaluations. We deployed RSU and TA in the vehicles network. We assume that the OBU, RSU, and TA have completed parameter initialization and registration, and stored related group key negotiation information, such as VID, signature key, etc. The default parameter settings are listed in Table 3

Table 3. Default parameter settings.

Parameter	Default Value
Vehicles number	50
Communication range	250 (m)
Average speed	40 (kph)
Slot time	1.3×10^{-5} (s)

Figure 7 depicts the whole delay in group key negotiation, which includes computation delay and communication delay. In the simulation, we statistically analyzed the average delay of n vehicles initiating the negotiation group key. As shown in Figure 7, with the increase of the number of vehicles, the number of channel collisions increases, thereby increasing the communication delay. The communication efficiency of our scheme outperforms other ones, since the computation delay of our scheme is lower than that of other ones. When a new vehicle enters the communication range of RSU to apply for a new session key, the vehicle only needs to send its own group identity and signature to the RSU. Other existing n vehicles do not need to resend their pseudo identities and signatures again. The RSU computes a new group key according to the newly added vehicle information and broadcasts it. In this procedure, only $n + 2$ messages are exchanged. Thus, this phase only requires two rounds to update group key. When a vehicle leaves the communication range of some RSU, the RSU only needs to recalculate the group key based on the information about the remaining $n - 1$ vehicles. In this procedure, only $n - 1$ messages are transferred. This phase only requires one round in updating group key.

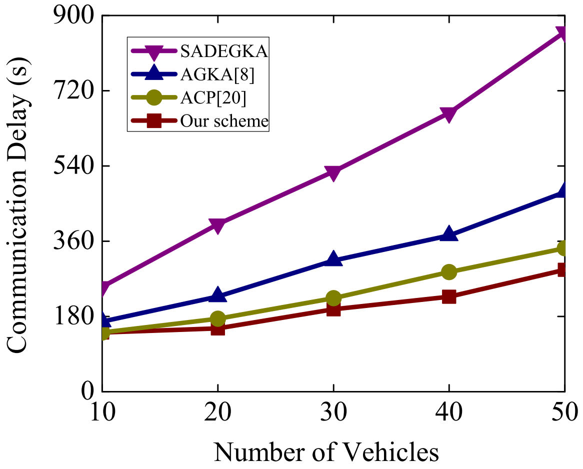

Figure 7. Number of vehicles versus computation delay.

6. Conclusions

This paper has proposed an authenticated group key agreement scheme for VANET in bilinear groups. The scheme selects the RSU as the main node in group key agreement, adopts the idea of shared secret keys, and realizes the identity authentication of each vehicle. Thorough analyses and comparison demonstrate that the proposed scheme provides privacy protection, traceability and revocability requirements and improves the performance compared to other schemes.

Author Contributions: conceptualization, L.L. and Y.W.; methodology, L.L.; software, L.L.; validation, Y.W., J.Z.; formal analysis, L.L.; investigation, Q.Y.; resources, J.Z.; data curation, L.L. and J.Z.; writing original draft preparation, L.L.; writing review and editing, L.L. and Y.W.; visualization, Q.Y.; supervision, L.L.; project administration, L.L. and J.Z; funding acquisition, J.Z.

Funding: This research was funded by the National Natural Science Foundation of China (Nos. 61462017, 61662015, 61862013, 61662013, U1501252, U1711263, 61562014, 61862012), the Guangxi Key Lab of Wireless Wideband Communication and Signal Processing (GXKL061508), the Guangxi Young Teachers' Basic Ability Improvement Program under Grant 2018KY0194, Guangxi Innovation-Driven Development Project (Science and Technology Major Project, AA17202024), and the Guangxi Natural Science Foundation (Nos. 2018GXNSFAA281232, 2017GXNSFAA198035, 2017GXNSFAA198372, 2016GXNSFAA380149, 2016GXNSFAA380043).

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

References

1. Paridel, K.; Balen, J.; Berbers, Y.; Martinovic, G. VVID: A delay tolerant data dissemination architecture for VANETs using V2V and V2I communication. In Proceedings of the International Conference on Mobile Services, Resources, and Users, Venice, Italy, 21–26 October 2012; pp. 151–156.
2. Kim, J.Y.; Choi, H.K.; Copeland, J.A. An Efficient Authentication Scheme for Security and Privacy Preservation in V2I Communications. In Proceedings of the IEEE 72nd Vehicular Technology Conference—Fall, Ottawa, ON, Canada, 6–9 September 2010; pp. 1–6. [CrossRef]
3. Lu, X.; Xu, D.; Xiao, L.; Wang, L.; Zhuang, W. Anti-Jamming Communication Game for UAV-Aided VANETs. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2018; pp. 1–6.
4. Abuelela, M.; Olariu, S.; Ibrahim, K. A Secure and Privacy Aware Data Dissemination for the Notification of Traffic Incidents. In Proceedings of the VTC Spring 2009—IEEE 69th Vehicular Technology Conference, Barcelona, Spain, 26–29 April 2009; pp. 1–5. [CrossRef]
5. Abbasi, I.; Khan, A.; Ali, S. Dynamic Multiple Junction Selection Based Routing Protocol for VANETs in City Environment. *Appl. Sci.* **2018**, *8*, 687. [CrossRef]
6. Dorronsoro, B..E.; Ruiz, P.; Danoy, G.; Pigne, Y.; Bouvry, P. *Introduction to Mobile Ad Hoc Networks*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2014; pp. 1–26.
7. Song, C.; Zhang, M.; Peng, W. Efficient pairing-based batch anonymous authentication scheme for VANET. *J. China Univ. Posts Telecommun.* **2018**, *25*, 85–94.
8. Hai, Z. An Authenticated Group Key Agreement Scheme for Mobile Communication Based on Bilinear Pairing. *Comput. Appl. Softw.* **2012**, *29*, 151–155.
9. Maslekar, N.; Boussedjra, M.; Mouzna, J.; Labiod, H. A stable clustering algorithm for efficiency applications in VANETs. In Proceedings of the 2011 7th International Wireless Communications and Mobile Computing Conference, Istanbul, Turkey, 4–8 July 2011; pp. 1188–1193.
10. Liu, L.; Wang, J.; Huang, J.; Feng, Q.; Min, G. Encounter Prediction-based Data Forwarding for High Reliability in Bus Networks. *Ad Hoc Sens. Wirel. Netw.* **2018**, *41*, 137–164.
11. Bhakthavathsalam, R.; Nayak, S.; Srikumar, M.G. Expediency of penetration ratio and evaluation of mean throughput for safety and commercial applications in VANETs. In Proceedings of the International Conference on Ultra Modern Telecommunications & Workshops, St. Petersburg, Russia, 12–14 October 2009; pp. 1–5.
12. Wang, Y.; Ding, Y.; Wu, Q.; Wei, Y.; Qin, B.; Wang, H. Privacy-Preserving Cloud-based Road Condition Monitoring with Source Authentication in VANETs. *IEEE Trans. Inf. Forensics Secur.* **2018**. [CrossRef]
13. Lee, J.L.; Hwang, J.; Park, H.; Kim, D. On latency-aware tree topology construction for emergency responding VANET applications. In Proceedings of the IEEE INFOCOM 2018—IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; pp. 57–63. [CrossRef]
14. Wagan, A.A.; Jung, L.T. Security framework for low latency vanet applications. In Proceedings of the International Conference on Computer and Information Sciences, Kuala Lumpur, Malaysia, 3–5 June 2014; pp. 1–6.
15. Qian, Y.; Moayeri, N. Design of Secure and Application-Oriented VANETs. In Proceedings of the VTC Spring 2008—IEEE Vehicular Technology Conference, Singapore, 11–14 May 2008; pp. 2794–2799.
16. Han, M.; Hua, L.; Ma, S. A Self-Authentication and Deniable Efficient Group Key Agreement Protocol for VANET. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 3678–3698.

17. Chim, T.W.; Yiu, S.M.; Hui, L.C.K.; Jiang, Z.L.; Li, V.O.K. *SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 189–203.
18. Lei, L.J.; Yu, H.H.; Xian, A.L. Novel Group Authentication Key Agreement Scheme. *Comput. Eng.* **2012**, *38*, 132–134.
19. Zheng, J.; Yang, C.; Xue, J.; Zhang, C. A Dynamic ID-based Authenticated Group Key Agreement Protocol. In Proceedings of the 4th National Conference on Electrical, Electronics and Computer Engineering, Xi'an, China, 12–13 December 2015.
20. Chuang, M.C.; Lee, J.F. PPAS: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks. In Proceedings of the 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), XianNing, China, 16–18 April 2011; pp. 1509–1512. [CrossRef]
21. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1711–1720. [CrossRef]
22. Jiang, S.; Zhu, X.; Wang, L. A conditional privacy scheme based on anonymized batch authentication in Vehicular Ad Hoc Networks. In Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 2375–2380.
23. PBC Library. Available online: http://crypto.stanford.edu/pbc/ (accessed on 6 March 2018).