Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs

Toward an RSU-unavailable lightweight certificateless key agreement scheme for VANETs

J. Song, C. He, L. Zhang, Shanyu Tang, and H. Zhang

Abstract

Vehicle ad-hoc networks have developed rapidly these years, whose security and privacy issues are always concerned widely. In spite of a remarkable research on their security solutions, but in which there still lacks considerations on how to secure vehicle-to-vehicle communications, particularly when infrastructure is unavailable. In this paper, we propose a lightweight certificate less and one-round key agreement scheme without pairing, and further prove the security of the proposed scheme in the random oracle model. The proposed scheme is expected to not only resist known attacks with less computation cost, but also as an efficient way to relieve the workload of vehicle-to-vehicle authentication, especially in no available infrastructure circumstance. A comprehensive evaluation, including security analysis, efficiency analysis and simulation evaluation, is presented to confirm the security and feasibility of the proposed scheme.

Keywords: vehicle ad-hoc network; security and privacy; lightweight authentication; certificateless key agreement

I. Introduction

Vehicle ad-hoc networks (VANETs) have got unprecedented attentions from both industry and academia in these years. Dedicate Short Range Communications (OSRC) and Wireless Access in Vehicular Environments (WAV E) in 802.11p [1], through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications at 5.9 GHz, enable a self-organizing, easy deployment, low cost, open architecture of mobile ad-hoc network. We can expect that vehicular networks applications and value-added service will play an even more important role in easing traffic pressure, in- creasing the driving comfort, avoiding traffic accidents, online payment and online infotainment, etc. It is well known that vehicular networks are unique features in the following two aspects, namely the dynamic network topology and the short-range and unstable communication environment. Thus it may not be desirable or feasible to simply utilize those existing solutions to handle with VANET security issues.

Due to the mobile and dynamic topology nature, vehicular networks have brought some challenging security and privacy issues that still remain to be addressed. Although there is a remarkable research for VANET key agreement solutions in the literature, the previous work did not specifically optimize the security implementations considering the properties of infrastructure inaccessible scenarios. For instance, in areas where traffic is concentrated, the distribution of infrastructures is generally intensive and well-organized so that vehicles can mutually authenticate in real-time online methods. However, in places where infrastructures are sparsely deployed or infrastructures cannot be accessed, the method of online authentication does not work properly, such as highway environment, suburb, or disaster areas where infrastructures were destroyed.

To address the concerns, in this paper, we propose a secure lightweight certificateless authentication key agreement scheme (CL- AKA) especially for the purpose of securing V2V communication when without available road-side infrastructures. The main contributions of this study are threefold. First, we present a strong certificateless key agreement protocol following a practical approach and fully addressing the aforementioned security issues under a dynamic and insecure vehicular environment. Second, we implement one CL- AKA scheme and show its construction pro- cesses based on defined strong security model. Third, this paper gives the security proof of the proposed CL-AKA scheme and evaluates its performance through comparing with other schemes. Security analyses and performance results show that the proposed scheme is a well-optimized CL-PKA scheme whose efficiency and performance are advantageous for the V2V authentication communication scenarios.

The rest of this paper is organized as follows. Section II overviews the related work. Section III describes the system model and the security model for VANETs. Section IV presents our security protocol. Followed by security analysis and performance results in section V, the last part is our further discussions and conclusion in section VI.

II. Related Work

Generally, there are mainly four kinds of key agreement scheme so far, that is, the tradition- al PKI-based or the Certificate (CA)-based key agreement schemes, the identification (ID)-based key agreement schemes [5,6], or others, including the

certificateless public key agreement [2, 3], the Lite-CA based key agreement schemes[4], and the self-certificate public key based key agreement schemes. It is worth noting that CA-based key agreement scheme usually requires the attendance of a public key infrastructure. Besides that, the IO-based cryptosystem [5] often exists a key escrow issue.

In 2005, AI-Riyami and Paterson [7] introduced a certificateless public-key encryption (CL-PKE) that gets rid of the requirement of public key infrastructure. Roughly speaking, it combines the ideas and methods from the traditional public key encryption and identity-based encryption. Distinguished from 10-based cryptosystems, user's partial private key originates from its own identity information and KGC, and a secret value generated by the user itself. In 2008, Dent [8], in one survey paper, notes that two obvious advantages of certificateless public key encryption scheme. First, it has no requirement of certificates, which is unlike a traditional public key encryption scheme. Furthermore, it voids the direct threat from attackers to compute the full private key.

In 2009, Lippold et al. [3] proposed the first one-round CL-AKE scheme proven secure in the random oracle model. This paper gives a detailed secure proof and a generic model to design a strong secure key agreement proto- col. However, its process of key agreement is complex and time-consuming with at least five modular exponentiation and ten bilinear pairing operations. In 2011, Yang et al. [9] proposed the first proven strongly secure CL-KE protocol without pairing. It requires less computation cost than Lippold’s scheme because of no expensive pairing operations. These certificateless key agreement schemes, in general, have three main secrets, that is, the ID-based key, the secret value and the ephemeral key. Both papers use the random oracle model to prove their security that, as long as one of the three secrets is

unrevealed, the scheme is considered secure [3, 9]. However, these studies are not feasible in securing V2V communication when considering of less computation and communication overhead.

Song et al. [2] proposed a strong certificateless key agreement protocol following a practical approach and fully addressing the aforementioned security issues under common VANET attacks. This scheme has four rounds to achieve the three-way handshake. Thus it is still inefficient for vehicle-to-vehicle key agreement communication. Dong and Cao [4] proposed an efficient lite-CA-based encryption scheme for data forwarding in VANETs. This proposed scheme has less computational over- head and provides an efficient way to relieve workload and deployment of certificates as well.

Inspired by previous works, this paper pro- poses a certificateless key agreement scheme which is addressed in a dynamic and insecure vehicular environment, particularly for V2V authentication communication in the scenario without available road-side infrastructures.

III. SYSTEM MODEL AND SECURE MODEL

3.1 System model

This paper addresses the VANETs scenario as Figure 1. As seen from the figure, there are usually three components: Regional Trusted Authority (RTA), Road Side Unit (RSU) and On Board Unit (OBU). In this paper, the main concern is the secure

authentication key agreement communication between vehicles, as well as the registration before communication.

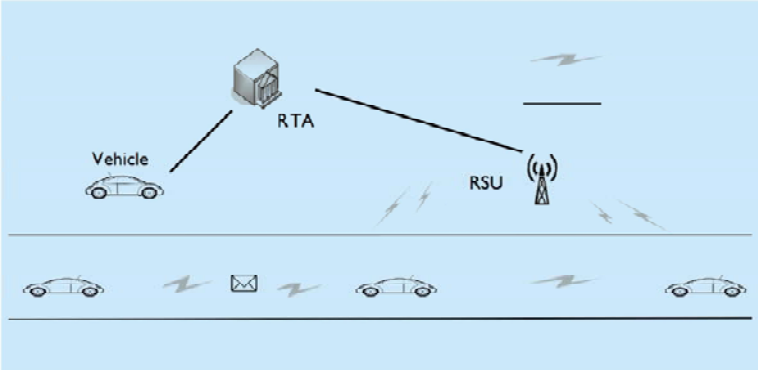

Fig.1 System model

a) RTA: is a regional trusted authority. There is usually only one RTA which is always trusted. In our system model, RTA has two main functions: one is that RTA computes the master key for the key agreement and publishes the requisite public parameters; the other is that when vehicles come into its communication range, RTA controls the registration pro- cess of vehicles and computes the pseudonym for vehicles.

b) RSU: is a trusted roadside unit which connects with RTA through wired channel and communicates with OBU via wireless channel; meanwhile, it has a wireless Access Point (AP) for all OBUs in its communication range. RSUs have two roles, data warehouse and pro- cessing center authorized by CA. So RSUs are important to act as the secure proxy between RTA and OBU. They are generally deployed in an

optimized way for high utilization due to their high cost. Therefore, once the RSUs are unavailable in some areas, the V21 communications will be invalid or infeasible.

c) OBU: is deployed on the vehicles as a trusted platform module (TPM). OBUs can communicate with RSUs through wireless channel. OBUs should register to RTA and obtain key materials in advance. Before OBUs communicate with each other, they exchange public keys and compute the session keys for encrypting the subsequent messages.

3.2 Secure model

Inspired by the extended Canetti-Krawcyzk (eCK) model [ll], this paper designs a novel lightweight certificateless key agreement scheme which is provably secure in the random oracle model. We present their cryptography properties as followings.

The proposed scheme consists of the following probabilistic polynomial time algorithms:

Setup(l^k) : with the input of the security parameters k, it outputs the global parameters {g, q, G} as well as the hash functions.

MasterKeyGen(l^k): with the k as the security parameter input, it returns the master private key s and the corresponding master public key S.

ID-basedKeyGen(s, ID): with the input of the master private key s and the identity ID of a user, it returns the ID-based key d_{ID} of the user.

SecretValueGen (1^k): with the input of the security parameters *k*, it outputs the secret value X_i of user $_i$.

CertificatelessPublicKeyGen(x_i): with the input of the secret value X_i of user i, it outputs the certificateless public key X_i.

EphemeralKeyGen(1^k) : with the input of the security parameters k, it outputs the ephemeral key r_i and R_i of user i.

SessionKeyGen(*sid*, pk_i, pk_j, sk_i, sk_j): with the input of the parameters sid, pki' pkj' sk;, skj, where sid is the identity of the session, pki is the set of user i's public keys, pkj is the set of user j's public keys, Ski is the set of user i's private keys, skj is the set of user j's private keys, the algorithm outputs the session key SK between user i and}.

Let U = U_1, U_2, U_3, …, U_n be a set of vehic1es. The protocol is run between any two of these vehicles. For each vehicle, an ID-based private key can be obtained from the RTA through a secure channel. Other keys, such as their secret value, ephemeral key and certificateless public key are generated by themselves.

The adversary A has the ability to control the communication channel over which the vehicles exchange their messages. IT i,' j denotes the *t*th protocol session running between the user i and user}. In addition, the adversary is allowed to replace the certificate less public key unless the corresponding private key is unrevealed, and vice versa. A session IT i, 'j may enter an accepted state with having computed a session key S K;'J or terminate without entering into an accepted state. We assumed that the information that whether a session is terminated with entering into an accepted state or not is public. Each session ITi, j is identified with a session ID sid which contains the identity of user i and user j. The transcript of the message is exchanged between

user i and user } during the session. Two sessions IT i,'j and IT i, k j are considered to be a match if they have the same sid.

The game runs in two phases. During the first phase, the adversary is allowed to issue the following queries in any order:

Send(IT i,' j, x): if the Send query is allowed, the adversary controls all the communication and can cancel and modify the existing messages, insert new ones as well. If the Send query is not allowed, the adversary can only passively eavesdrop the message sent by the parties after the authenticated communication.

Reveal master key: by this query, A learns the master key s.

Reveal ID-based secret: by this query, A learns a user's ID-based key dm.

Reveal secret value: by this query, A learns a user's long term secret key X_U.

Reveal ephemeral key: by this query, A learns a user's ephemeral secret key r_U in session ITi, I I

Replace public key: by this query, A replaces a user's public key Xu to be X□, and V will use X;; as its public key.

Reveal session key: by this query, A learns the session key SK of session IT i,'I Once the first phase is over, the adversary chooses a fresh session IT i,1j and issues the T est(IT i,1j) query.

Test(ITi,'j): input a fresh session ITi,' j and a bit b E { 0, I} is chosen. If b = 0, the adversary is given the session key S K i, 1 j, otherwise, the adversary gets session key randomly chosen from the set of the valid session key.

After the second phase, the adversary outputs a guess fj for b. If fj = b, we consider the adversary wins the game, and the advantage that the adversary wins the game is defined as:

$$Adv^{M}(k)[\Pi] = |Pr[M_{win}] - 1/2|$$

IV. SECURITY PROTOCOL DESIGN

In this section, we propose the preliminaries for the certificateless key agreement scheme, and then design a lightweight certificateless key agreement scheme by using five following cryptographic primitives. It is noted that this scheme can be easily extended and further optimized by one kind of improvement design. Finally, we present their proofs on consistency and security.

4.1 Preliminaries

Due to the page limit, we only review part of the definitions and theorems that are closely related to our proposed protocol.

Definition: Z_q^* is multiplicative group, where q is a prime integer; G is a cyclic group of prime order q, generated by g∈; $G^* = G \setminus 1$, where 1 is the identity of G.

Computational Diffie-Hellman (*CDH*) Problem: [12] given g^a, $g^b \in G$, where a, b ← Z, compute g^{ab}.

Cap Diffie-Hellman (CDH) Problem: [13] given g^a, g^b, $g^c \in G^*$, where a, b, c $\leftarrow$ Z, it is easy to decide whether c=ab, but cannot compute a, b.

Cap Diffie-Hellman (CDH) Signature: [13] let secret key x $\leftarrow Z_q^*$, the public key v = g^x given x and a message M $\in \{0, 1\}^*$, compute h = H(M), and the signature $\sigma = h^x$, where H: $\{0, 1\}^* \rightarrow G^*$. The verification is to compute h = H(M), and verify that (g, v, h, σ) is a valid Diffie-Hellman tuple.

Dual (exponential) Challenge-Response (DCR) signature: [14] let public keys A = g^a and X = g^x, B = g^b and Y = g^y. The OCR signature (OS) of A and B on message ml, m2 is a tuple of values X, Y, and DSA'B' respectively. Here, the same signature can be exchanged to compute (and verify) as follows:

$$DS_{A,B}(m_1,m_2,X,Y) = g^{(x+da)(y+eb)} = (YB^e)^{x+da} = (XA^d)^{y+eb}$$

where d and e denote H(X, ml) and H(Y, m2).

Twin Diffe-Hellman (TDH) Trapdoor Theorems: [1 3] using the above notations, suppose Xl E G' r, s E Z' and := g'/X;. Y,Zj,ZC are random variables in G and defined as functions of Xl and X2• Then, I) X2 is uniformly distributed over G; 2) Xl and X2 are independent; 3) if Xj = g" and Xc = g", the probability that the value of Z Z2 = Y' does not agree with the value of Zj = yx, 1\ Z2 = yxo is at most I/q (if the latter holds, the former certainly holds).

4.2 Protocol design

In this section, we present a concrete certificateless key agreement scheme for V2V communication. The new scheme consists of the following PPT algorithms.

Setup(l^k) : input a security parameter 1 k, the RTA runs the Setup algorithm as following steps: determines (g, q, G), where q is a k-bit prime, G is a cyclic group with order q and generator g, and then, choose three hash functions: $H : \{0,1\}^* \to \mathbb{G},\ H_1 : \{0,1\}^* \to \mathbb{Z}_q^*,\ H_2 : \{0,1\}^* \times \{0,1\}^* \times \mathbb{G}^{11} \to \{0,1\}^n$. RTA publishes the global parameter param = {q, g, G, H, H_1, H_2}.

MasterKeyGen(l^k): input a param-secuntyeter 1^k, the RTA chooses $s \leftarrow Z_q$, and computes $S = H(TA)^s$ where TA is the identity of RTA, s is the master private key and public key, respectively.

ID-basedKeyGen(*s, ID*): run by the RTA. To register via the RTA, the vehicle sends its real identity ID to the RTA. RTA computes the pseudonym ID' and the ID-based key for the vehicle. After that, the RTA returns (lD', d_{ID}) to the vehicle, where d_{ID} is a Diffie-Hellman signature by the RTA.

VerifyID-basedKey: get (lD', d_{ID}) from the RTA, the vehicle can verify whether (, , d_{ID}) is a valid Diffie-Hellman tuple by verifying the key d_{ID}.

SecretValueGen(l^k) : input a security parameter l^k, the vehicle runs the algorithm to generate the secret value x_U, $x_U \leftarrow Z_q$. The x_U is the long-term secret.

CertijicatelessPublicKeyGen(x_{ij}): with the secret value x_U, the vehicle runs this algorithm to compute the certificateless public key x_U.

EphemeralKeyGen(1^k) : input a security parameter 1^k, the vehicle chooses $r_U \leftarrow Z_q$, and computes $R_U = g^{ru}$.

MessageExchange: Before user A and user B run the SessionKeyGen algorithm, they exchange the following message:

$$A \rightarrow B : A', E_A = (X_A \| R_A), Tcur_A, Lcur_A$$
$$A \leftarrow B : B', E_B = (X_B \| R_B), Tcur_B, Lcur_B$$

where, A', B' are the pseudonym identities of the user A and user B, $Tcur_A$, $Tcur_B$ are the time-stamps, and $Lcur_A$, $Lcur_B$ are location information.

SessionKeyGen(*sid*, pk_A, pk_B, sk_A, sk_B): input the parameters *sid*, pk_A, pk_B, sk_A, sk_B, this algorithm returns the session key *SK*. Here, *sid* is the identity of the session, and $sid = \{A', B', E_A, E_B\}$, $sk_A = \{x_A, r_A, d_A\}$, $pk_A = \{X_A, R_A\}$, $sk_B = \{x_B, r_B, d_B\}$, $pk_B = \{X_B, R_B\}$. To generate the session key, A, B do the following computation:

A computes

$$\lambda_1 = R_B^{r_A}, \lambda_2 = X_B^{x_A}, \lambda_3 = X_B^{r_A}, \lambda_4 = R_B^{x_A}, \quad \lambda_5 = X_B^{x_A} d_A^{H_1(B)}, \lambda_6 = R_B^{r_A} d_A^{H_1(B)}, \lambda_7 = d_A^{H_1(B)}$$

B computes

$$\lambda_1 = R_A^{r_B}, \lambda_2 = X_A^{x_B}, \lambda_3 = R_A^{x_B}, \lambda_4 = X_A^{r_B}, \quad \lambda_5 = X_A^{x_B} d_B^{H_1(A)}, \lambda_6 = R_A^{r_B} d_B^{H_1(A)}, \lambda_7 = d_B^{H_1(A)}$$

Above computations can be easily verified as:

$$\lambda_1 = g^{r_A r_B}, \lambda_2 = g^{x_A x_B}, \lambda_3 = g^{r_A x_B}, \lambda_4 = g^{x_A r_B},$$
$$\lambda_5 = g^{x_A x_B + sH_1(A)H_1(B)}, \lambda_6 = g^{r_A r_B + sH_1(A)H_1(B)}, \lambda_7 = g^{sH_1(A)H_1(B)}$$

So the session key SK is:

$$SK = H_2(Sid, \lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6, \lambda_7)$$

As mentioned above, we show a proposed certificateless key agreement process, which fits for Lippold's secure model [3]. Further- more, this proposed scheme

computes more easily and keeps minimization principle from the cryptography primitives.

V. SECURITY ANALYSIS AND PERFORMANCE RESULTS

In this section, we demonstrate that the proposed protocol is secure, practical and feasible by analyzing its security properties, computational cost and communication overhead.

5.1 Security analysis

We first prove that the proposed certificateless key agreement scheme is secure in random oracle under the CDR assumption. The advantage of any PPT, Oli -valued adversary A in solving CDH Problem referred in section 4. 1 can be defined as:

$$Adv^{A}(k)[CDH] = Pr[A(g, g^{x}, g^{y}, g^{xy}) = 1 : x, y \in \mathbb{Z}_{q}]$$

And CDH Assumption is: $Adv^{A}(k)[CDH]$ is negligible.

$Test(\Pi i_{i}^{'}, j)$: the input session is fresh [3], and a bit b $\in$ {0, 1} is randomly chosen. If b = 0, the adversary A learns the session key SK, otherwise it randomly chooses a session key from the set of valid session keys for A. We say that our certificate less

authentication key agreement scheme is secure if for any PPT adversary A to guess b for 'jj, the advantage A breaks up our scheme is a negligible function of k, which we denote as:

$$Adv^{A}(k)[\Pi] = | Pr[A(\hat{b} = b)] - 1/2 |$$

Before $Test(\Pi i_i^{'}, j)$, the challenger B tries to guess the test session, and he randomly chooses two indices i, J E {I, 2,· . . q}, tE {I, 2, . . · q'} and i *' J, i, J represent the *i'h* and the *j'h distinct* query. i, J' and t denote the *t,h* test oracle ITi, j. Where, q is the most of users, and q' is the most sessions.

So, the probability of B choosing the right i, j is:

$$\frac{1}{q(q-1)} > \frac{1}{q^2}$$

and then the probability of guess the $\Pi_i^{'}, j$ correctly is:

$$\Pr[B(\hat{i} = i, \hat{j} = j, \hat{t} = t,)] = \frac{1}{q^2}\frac{1}{q^{'}}$$

Since there are three secrets *(drm Xu, ru)* kept in each party, we say that our scheme is secure as long as there is still one secret unrevealed for each party. So there are 9 situations that each party still keeps one secret. For the 9 situations, there are 9 strategies for B to abort the game, illustrated in Table I and AdvA(k)[CDH] > Pr[B(i = i, J = j,t= t)]Adv(k)[IT]. So, the advantage of any adversary A against our protocol is limited by:

$$Adv^{A}(k)[\Pi] \le 9q'q^2 Adv^{A}(k)[CDH]$$

Table I The Nine Situations and Strategies

Strategies	Secrets						Embedded in
	$d_{ID'}$		x_U/X_U		R_U		
1	×	×	×	×	√	√	λ_1
2	×	×	√	√	×	×	λ_2
3	×	×	×	√	√	×	λ_3
4	×	×	√	×	×	√	λ_4
5	√	×	×	√	×	×	λ_5
6	×	√	√	×	×	×	λ_5
7	√	×	×	×	√	×	λ_6
8	×	√	×	×	×	√	λ_6
9	√	√	×	×	×	×	λ_7

1) Strategy 1. The adversary learned the ID- based key dr and d.r of party I and J through revealing mastered key query or through10- based key query, and also learned the secret value Xr and XJ through revealing secret value or replacing the public key and X"I through replacing public key query. The only remained secrets are rJ and So, the adversary has to guess the right session IIi,'j and then to solve the CDR problem to compute rA and rB if he wants to compute Al for the session key. So the advantage of the adversary is limited to:

$$Adv^A(k)[\Pi] \le q'q^2\, Adv^A(k)[CDH]$$

2) Strategy 2: the adversary learned the 10- based key dl and dJ through revealing mastered key query or revealing ID-based key query of party I and J, and also learned the ephemeral key rl and rJ through revealing ephemeral key query in session IIi, I The unrevealed secrets are Xu and Xu. Therefore, the adversary has to

guess the right party I and J and then to solve the CDR problem to compute XI and XJ if he wants to compute A2 for the session key. So, the advantage is limited by:

$$Adv^{A}(k)[\Pi] \le q^{2} Adv^{A}(k)[CDH]$$

3) Strategy 3 and 4: the adversary learned the IO-based key dl and dJ through revealing mastered key query or revealing ID-based key query of party I and J, moreover, the adversary learned the secret value through revealing secret value or replacing the public key through replacing public key query of either of party and learned the ephemeral key of either party through revealing ephemeral key query in session IIi, I Each party keeps a secret of xr/Xu or ru safety. If the adversary wants to compute A3 or A4 for the session key, he must guess the right party I and J and the right session IIi, j and then to solve the CDR problem. So, the advantage is limited by:

$$Adv^{A}(k)[\Pi] \le q' q^{2} Adv^{A}(k)[CDH]$$

4) Strategy 5 and 6: the adversary learned the IO-based key and secret value of either party or replaced the pubic key of either party, and also learned the ephemeral key of both parties in session IIi, I. The uncorrupted key of each party is an IO-based key or a x_u/X_u or r_u. The adversary has to guess the right party I and J and then to solve the DCR signature to compute As if he wants to compute the session key. So, the advantage is limited by:

$$Adv^{A}(k)[\Pi] \le q^{2} Adv^{A}(k)[DCR]$$

5) Strategy 7 and 8: the adversary learned the ID-based key and ephemeral key of either party, and also learned the secret value or re-placed the public key of both parties. The safety secret in each party is an ID-based key or an ephemeral key. The adversary has to guess the right party I and J and the right session IIi, j, and then to

solve the DCR signature to compute A6 if he wants to compute the session key. So, the advantage is limited by:

$$Adv^{A}(k)[\Pi] \le q'q^{2}\, Adv^{A}(k)[DCR]$$

6) Strategy 9: the adversary learned the secret values and ephemeral keys of both parties and replaced the public keys of both parties. The unrevealed secrets are ID-based keys of both parties. The adversary has to guess the right party I and J and then to solve the CDR problem to compute XJ and if he wants to compute A9 for the session key. So, the advantage is limited by:

$$Adv^{A}(k)[\Pi] \le q^{2}\, Adv^{A}(k)[CDH]$$

5.2 Performance results

In this section, we will evaluate our proposed certificateless key agreement scheme from the aspect of efficiency and network performance.

1) *Efficiency Analysis*: In this part, we evaluate and compare the performance of our protocol with the other protocols, which offer similar security and privacy properties even though different schemes were adopted, i.e., discrete logarithm in our protocol and elliptic curve cryptosystem in theirs. We measure the computation overhead of the following five different operations based on the original source code in the Miracl library[15], which is a well-known free software for non-commercial use and implements efficient Big Number Cryptography. The experimentation results of the crypto overhead are listed in Table II.

Table II Crypto Overhead

Operations	From	Time(ms)	
		Naive	Comba
Pairing e	$e(aP, bP)$	22.641	
Point Multiplication E_1	xP	1.8444	0.4124
Modular Exponentiation E_2	$g^x \bmod n$	3.2028	0.7070
Multiplication M	$ab \bmod n$	0.0334	
Map-to-Point Hash Function H	$H: \{0,1\}^* \rightarrow G$	0.9180	

The experiment platform used in this paper is a commodity PC with a dual-core 3.4 GHz CPU, and 2 GB RAM, and we used the Miracl big number library. Without loss of generality, the total computation for each party in our scheme is nine 1024-bit modular exponent Mod_{exp} operations, four 1024-bit big number multiplication $Mul_{1024/prime}$ operations, two 1024-bit big number modular addition ADD/Mod_{1024} operations, and six 512- bit hash operations. We compare our protocol with several existing CL-AKA protocols we have referred above in Table III. As shown in Figure 2, Figure 3 and Figure 4, we can see that our scheme have obvious advantage in computation efficiency after multi-times key agreement.

Table III Comparison of Different Protocol

Protocol	Computation	Time(ms)	
		Naive	Comba
Huang	$3E_1 + 2e$	50.8125	46.5192
Lippold	$5E_1 + 10e + 2H$	237.468	230.308
Song	$16E_2 + 4M$	51.3784	11.4456
Yang	$9E_2 + 3M$	28.9254	6.4632
Our	$9E_2 + 2M$	28.8920	6.4298

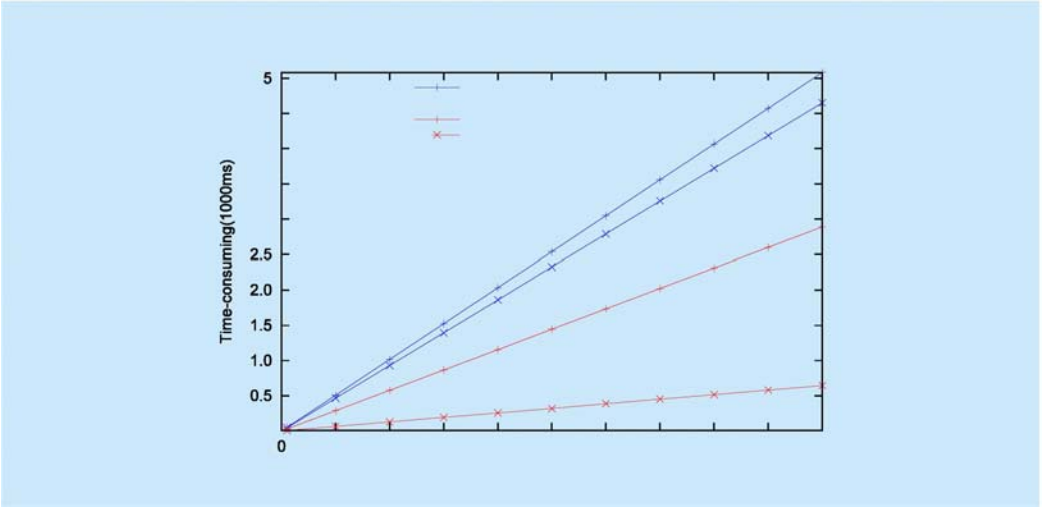

Fig. 2 Compared with Huang s schemes

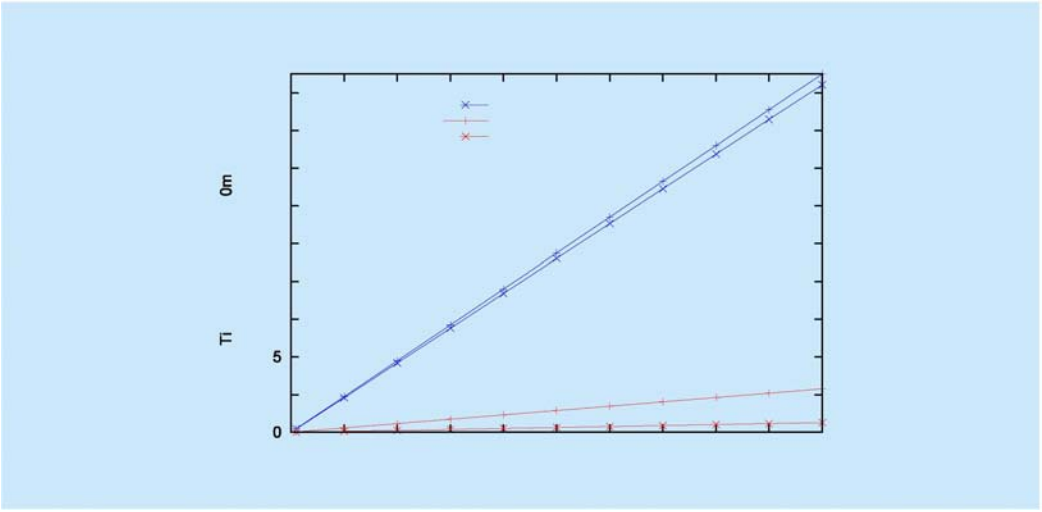

Fig. 3 Compared with Lippolds schemes

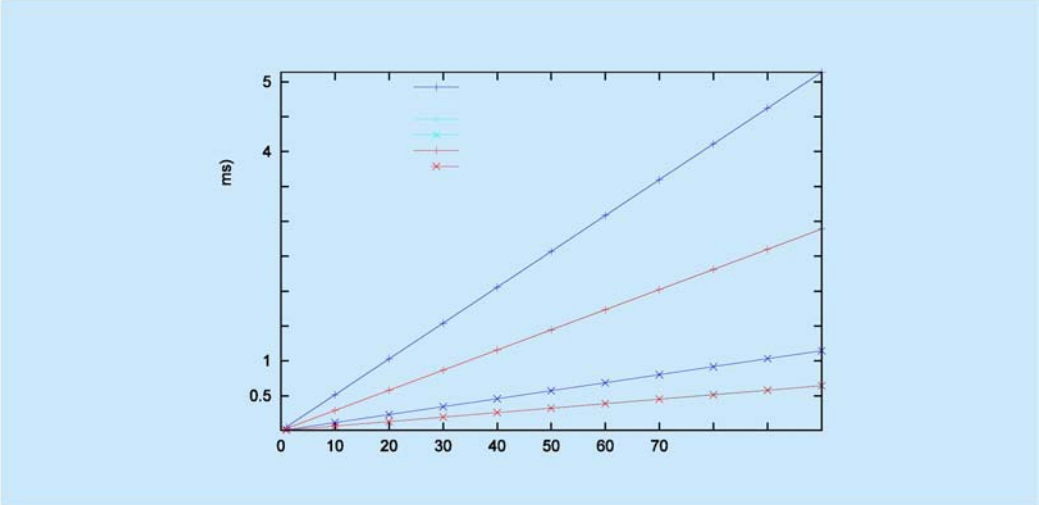

Fig. 4 Compared with Song and Yang s schemes

2) *Network Performance*: In this section, we present the performance evaluation of the proposed protocol. There are several metrics that can be used to measure the performance of a routing protocol, but we use the most widely accepted ones: the packet delivery ratio (PDR), end-to-end delay (E2ED).

We evaluate the computation overhead of the proposed scheme in NS3 with a cross-layer weighted position-based routing protocol (CLW PR) [16], which is designed for urban VANET environment. CLWPR uses cross-layer information, such as SNIR from PRY layer and frame error rate from MAC layer to improve the efficiency of routing.

The scenario is a 5x5 Manhattan Grid network with 200 nodes, with mean speed varying from 0 to 35mls in bonnmotion-2.0[17]. For each scenario, 10 concurrent

connections are created in NS3.11 using UDP connections to get the PDR, E2ED, hop counts and total dropped packets. We run several Monte Car- lo simulations, and use 50 different mobility trace files for each scenario. Each vehicle is equipped with a proper wireless interface. The communication range is set to be 500m according to the IEEE 802.11p standard with RTS/CTS mechanism and the used propagation model is Two-Ray-Ground.

The results are shown in Figure 5, Figure 6. In both figures, the x-axis indicates the mean speed of the 200 vehicles in the scenario. In each figure, there are three curves, the red line with + point stands for the PDR or E2ED of the CLWPR protocol without our proposed secure key agreement scheme, the green line with x point stands for the PDR or E2ED of the CLWPR protocol with our proposed secure key agreement scheme, and the time of our scheme is computed by the naive algorithm in Miracle, the last curve of blue line with x point is the PDR or E2ED of the CLWPR protocol with our proposed secure key agreement scheme testing in the comba algorithm in Miracle.

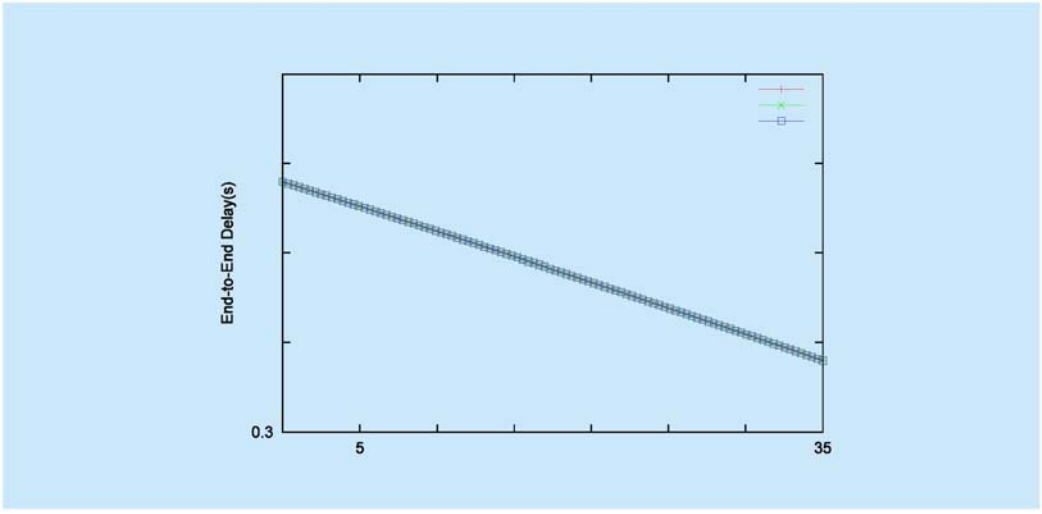

Fig.5 Packet delivery rate results

In Figure 5, the y-axis indicates the pack- age delivery rate, which means the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

$$PDR = \frac{\sum Numberofpacketreceive}{\sum Numberofpacketsend}$$

From Figure 5, we can see that the three curves are very similar, and they are nearly overlapped. Therefore, the proposed scheme does not decrease the packet delivery rate and does not add much network overhead.

In Figure 6, the y-axis indicates the end- to-end delay, E2ED means the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only these data packets are successfully delivered to destinations count.

$$E2ED = \frac{\sum arrive\ time - send\ time}{\sum Number\ of\ \ connections}$$

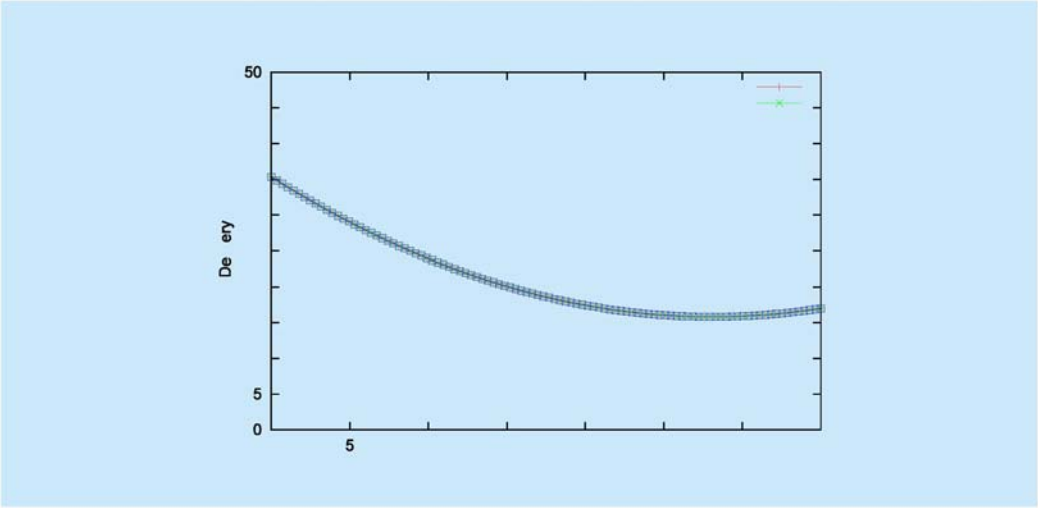

Fig.6 End-ta-end delay results

From Figure 6, we can see that the pro- posed scheme increases a little extra end-to-end delay, but the addition in E2ED is negligible because the three curves are quite close. We can conclude that our proposed certificate- less key agreement scheme is efficient which shows a good network performance.

VI. CONCLUSIONS

In this paper, we focus on a practical and safe certificateless key agreement scheme special to secure V2V communication without available RSU. Firstly, we utilize Gap Diffie-Heilman Signature for RTA to sign the ID-based key d_{ID}, which makes it possible to build our scheme free from a secure channel between RTA and vehicles. Secondly, considering securing forward property, the ephemeral key pairs, i.e., r_U and

R_U, which is only used in one certain key exchange process, is embedded into the session key. Thirdly, in order to enhance the efficiency and robustness of the proposed scheme, we embed DCR signature in session key evidences and reduced the key agreement interactions to one-round. Finally, we evaluate the computational cost and the network overhead of the proposed scheme by the existing routing protocol CLWPR in NS3. Besides that, we also use the classical reduction approach to prove that the proposed scheme is secure as long as there is still one secret uncompromised in the random oracle model. Performance comparisons with other schemes show that our proposed key agreement schemes are efficient and suitable for vehicle-to-vehicle authentication communication services.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported in part by the National Natural Science Foundation of China under Grant No. 61170217, 61272469, 61303212, 61332019, and Grant No.U1l35004, and by the Fundamental Research Founds for National University, China University of Geosciences (Wuhan).

References

[1] Weigle M. Standards: WAVE/DSRC/802.11p [J]. Vehicular Networks CS, 2008, 795-895.

[2] Song J, Zhuang Y, Pan J, et al. Certificate less Secure Upload for Drive-thru Internet [ClII Communications (ICC), 2011 IEEE International Conference on Communications. Kyoto, Japan, June 2011, 1-6.

[3] Lippold G, Boyd C, Nieto J G. Strongly secure certificateless key agreement [MlI/Pairing-Based Cryptography-Pairing 2009. Springer Berlin Heidelberg. Palo Alto, CA, USA, August 2009, 206-230.

[4] Dong X, Wei L, Zhu H, et al.: An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Vehicular Ad Hoc Networks [J]. Vehicular Technology, IEEE Transactions on, 2011, 60(2): 580-591.

[5] Shamir A. Identity-based cryptosystems and signature schemes [ClII Advances in cryptology. Springer Berlin Heidelberg, 1985: 47-53.

[6] Huang H, Cao Z. An ID-based authenticated key exchange protocol based on bilinear Diffie-Heilman problem[C]II Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. ACM, 2009: 333-342.

[7] AI-Riyami S, Paterson K G. CBE from CL-PKE: A generic construction and efficient schemes [M]11 Public Key Cryptography-PKC 200S. Springer Berlin Heidelberg, 2005: 398-41S.

[8] Dent A W. A survey of certificateless encryption schemes and security models [J]. International Journal of Information Security, 2008, 7(5): 349-377.

[9] Yang G, Tan C H. Strongly secure certificateless key exchange without pairing [ClII Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, 2011: 71-79.

[10] Hartenstein H, Laberteaux K P. A tutorial survey on vehicular ad hoc networks [J]. Communications Magazine, IEEE, 2008, 46(6): 164-171.

[11] LaMacchia B, Lauter K, Mityagin A. Stronger security of authenticated key exchange[M]11 Provable Security. Springer Berlin Heidelberg, 2007: 1-16.

[12] Bao F, Deng R H, Zhu H. Variations of diffie-hell- man problem [MlI/ Information and Communications Security. Springer Berlin Heidelberg, 2003: 301-312.

[13] Cash D, Kiltz E, Shoup V. The twin Diffie-Heil-man problem and applications [MlI/ Advances in cryptol-2008: 127-14S.

[14] Sarr A P, Elbaz-Vincent P, Bajard J C. A secure and efficient authenticated diffie-hellman protocol [M]II Public Key Infrastructures, Services and Applications. Springer Berlin Heidelberg, 2010: 83-98.

[1S] Scott M. Miracl-multiprecision integer and rational arithmetic c/c+ + library[J]. Shamus Soft- ware Ltd, Dublin, Ireland, 2003.

[16] Katsaros K, Dianati M, Tafazolli R, et al. CLW- PR-A novel cross-layer optimized position based routing protocol for VANETs [ClI/ Vehicular Networking Conference (VNC), 2011 IEEE. IEEE, 2011: 139-146.

[17] Aschenbruck N, Ernst R, Gerhards-Padilla E, et al. Bonnmotion: a mobility scenario generation and analysis tool [c]II Proceedings of the 3rd International ICST

Conference on Simulation Tools and Techniques. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2010: 51.

[18] Lu R, Lin X, Zhu H, et al. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications [Cl// INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. Phoenix, AZ, USA, April 2008.

[19] Cheng Z, Nistazakis M, Comley R, et al. On The Indistinguishability-Based Security Model of Key Agreement Protocols-Simple Cases [J]. IACR Cryptology ePrint Archive, 2005, 2005: 129.

[20] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[M]II Advances in Cryptology-ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 514-532.