A Robust and Efficient Anonymous Authentication Protocol in VANETs

Chae Duk Jung, Chul Sur, Youngho Park, and Kyung-Hyune Rhee

Abstract: **Recently, Lu *et al*. proposed an efficient conditional privacy preservation protocol, named ECPP, based on group signature scheme for generating anonymous certificates from roadside units (RSUs). However, ECPP does not provide unlinkability and traceability when multiple RSUs are compromised. In this paper, we make up for the limitations and propose a robust and efficient anonymous authentication protocol without loss of efficiency as compared with ECPP. Furthermore, in the proposed protocol, RSUs can issue multiple anonymous certificates to an OBU to alleviate system overheads for mutual authentication between OBUs and RSUs. In order to achieve these goals, we consider a universal re-encryption scheme and identity-based key establishment scheme as our building blocks. Several simulations are conducted to verify the efficiency and effectiveness of the proposed protocol by comparing with those of the existing ECPP.**

Index Terms: **Authentication, conditional privacy, group signature, identity-based key establishment, movement tracking, universal re-encryption, vehicular ad-hoc network (VANET).**

I. INTRODUCTION

In the near future, vehicles will be equipped with on-board processing and wireless communication modules, which enable vehicle-to-vehicle and vehicle-to-infrastructure communications based on short-range wireless technology, e.g., IEEE 802.11p [1]. That is called a vehicular ad-hoc network (VANET). VANET mainly consists of on-board units (OBUs) and roadside units (RSUs) [2], where OBUs are installed on vehicles to provide wireless communication capability, while RSUs are deployed to provide access point to vehicles within their radio coverages. By this organization, VANET can provide useful functions such as cooperative driving and probe of vehicle data. For example, a vehicle can warn other vehicles about traffic accidents or traffic jam.

Considering the useful VANET applications, it is necessary to develop a suit of elaborate and carefully designed security mechanisms to make VANET applications viable [3]–[11]. To prevent several possible attacks in VANET, such as impersonation attack and message modification attack, it is necessary to authenticate the broadcasted safety message by OBUs. Besides, the increasing demand for privacy issue has brought additional requirements for privacy preservation in VANET such as anonymous message authentication. Therefore, conditional privacy preservation, which private information is not disclosed to other entities while the authorities should legally trace user-related information in case of a disputed event, becomes one of the main requirements for secure VANET. To supply conditional privacy preservation in VANET, issuing on-the-fly anonymous certificates from RSUs to OBUs has received plenty of attention from the research community in recent year.

A. Related Work and Motivation

Since our work focuses on anonymous authentication for conditional privacy preservation, we just examine some existing anonymous authentication protocols for secure VANET [9], [12], [13] in this section.

In [9], with a pool of around 43,800 certificates, each OBU randomly chooses one of the available certificates for signing the message at one time in order to meet the driver's privacy requirement. However, in case of any dispute, the authority has to exhaustedly search in a very huge database to find the identity related to the anonymous public key. Moreover, it occurs a system overhead to revoke 43,800 certificates in the OBU. As a result, it requires a long revocation list and a long time to update the certificate revocation list (CRL) due to the large number of public keys in a compromised OBU.

Lin *et al*. [13] proposed a conditional privacy-preserving authentication protocol for VANET by integrating the techniques of group signature in [14], [15] and identity-based signature in [16]. Group signature is used to secure the communication between OBUs and OBUs, and identity-based signature is adopted at RSUs to digitally sign each message launched by RSUs to ensure its authenticity. However, in [13], even though the authors reduced CRL size, their protocol needs the management of certificate revocation information in OBUs. Hence, each vehicle must spend much time in message verification when the number of revoked vehicles is increased.

Recently, Lu *et al*. [12] proposed an efficient conditional privacy preservation protocol, named ECPP, which issues on-the-fly short-time anonymous certificate to OBUs by using a group signature scheme in [17]. Since RSUs can check the validity of the requesting vehicle during the short-time anonymous certificate generation phase, such revocation check by an OBU itself of [13] is not required. However, ECPP provides unlinkability and traceability under the unrealistic assumption that most RSUs will not disclose any inner information without the authorization of the trusted authority. In general, due to the fact that there exist a large number of RSUs, cost considerations prevent the RSUs from having sufficient protection facilities against ma-

Manuscript received April 28, 2009.

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2008-521-D00454).

C. D. Jung is with the Department of Information Security, Pukyong National University, Republic of Korea, email: jcd0205@pknu.ac.kr.

C. Sur is with the Department of Computer Science, Pukyong National University, Republic of Korea, email: kahlil@pknu.ac.kr.

Y. Park and K.-H. Rhee are with the Division of Electronic, Computer & Telecommunication Engineering, Pukyong National University, Republic of Korea, email: {pyhoya, khrhee}@pknu.ac.kr, corresponding author: K.-H. Rhee.

licious attacks. Therefore, it is possible for an attacker to access RSUs and disclose the information in the RSUs. When multiple RSUs are compromised in ECPP, an attacker is able to track the movement trace of a vehicle by using the information stored in the compromised RSUs [18], because each RSU stores unchanged pseudonyms for OBUs. As a result, ECPP does not provide unlinkability of OBUs when some RSUs were compromised. Furthermore, since the trace procedure in ECPP is run by incorporating with an RSU which issued a certificate corresponding to a disputed message, it is impossible to trace OBUs belong to compromised RSUs. Consequently, ECPP does not provide traceability when multiple RSUs are compromised.

Moreover, even though ECPP runs mutual authentication between OBUs and RSUs, it requires validity check of RSUs by using up-to-date revocation list in anonymous certificate generation phase by considering an attacker who can disclose inner information in the compromised RSUs.

As a result, it is necessary to design a robust and efficient anonymous authentication protocol that not only provides unlinkability and traceability even if multiple RSUs are compromised, but also reduces system overheads for validity check of RSUs in anonymous certificate generation phase.

B. Contribution and Organization

In this paper, we propose a robust and efficient anonymous authentication protocol that provides unlinkability and traceability even if multiple RSUs are compromised without loss of efficiency as compared with ECPP. To efficiently resolve the problem of certificate revocation in traditional PKI, the proposed protocol employs the concept of on-the-fly short-time anonymous certificate. Furthermore, to reduce system overheads for mutual authentication between OBUs and RSUs in anonymous certificate generation phase, RSUs issue multiple anonymous certificates to an OBU based on universal re-encryption scheme [19]. In addition, our protocol employs identity-based key establishment scheme [20] to eliminate the validity checks of RSUs in OBUs when OBUs verify the issued multiple anonymous certificates.

The rest of the paper is organized as follows. In Section II, we describe our design objectives and define conditional privacy level for secure VANET. We outline our system architecture in Section III. Section IV presents the proposed robust and efficient anonymous authentication protocol. In Section V, the security and efficiency of the proposed protocol are evaluated. Finally, we conclude the paper in Section VI.

II. SECURITY REQUIREMENTS

In this paper, we aim at achieving the following security objectives:

- **Authentication:** The origin of the messages should be authenticated to guard against impersonation attack. Also, even though an attacker compromises some RSUs, the attacker cannot forge a signature on safety message in a compromised RSU's communication range.
- **Anonymity:** The identities of vehicles should be hidden from normal message receivers during the safety message authentication process. Moreover, even if an attacker obtains inner information of compromised RSUs, the attacker cannot disclose the real identities of OBUs.
- **Unlinkability:** When an adversary has collected several safety messages from an OBU, the OBU should be still not traceable. Moreover, even though the adversary compromised RSUs, it cannot link information stored in the RSUs as the same OBU.
- **Traceability:** Theauthority should be able to trace the sender of a safety message by revealing the identity in case of any disputed situation such as liability investigation. In addition, even if multiple RSUs are compromised, the authority should be able to trace the real identities of pseudonyms in anonymous certificates without assistances of compromised RSUs.

Following the above goals, we revise the definition of conditional privacy level in [12] as Table 1.

Table 1. Definition of conditional privacy level.

	Authentication & anonymity	Unlinkability	Traceability
Level 1	✓	×	×
Level 2	✓	✓	×
Level 3	✓	✓	✓

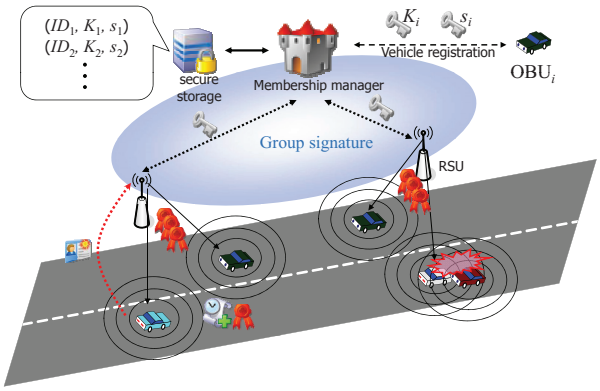

Fig. 1. System architecture.

Note that, ECPP does not provide unlinkability of an OBU since the compromised RSUs store the same pseudonym for the same OBU. Moreover, since the trace procedure in ECPP is run by the trust authority with an RSU (certificates generator), it is impossible to trace the real identities of OBUs belong to damaged RSUs. As a result, ECPP provides level 1 privacy in Table 1.

III. SYSTEM MODEL

In this section, we describe our system model, in which communication nodes are either membership manager, RSUs, or OBUs as shown in Fig. 1. The detailed description of system components is as follows:

- **Membership manager** is public agencies or corporations with administrative powers in a specific field; for example, city or state transportation authorities. The membership manager establishes and manages system parameters and

system roles for secure VANET. In addition, the membership manager should be able to reveal the identities of safety message senders in case of disputed traffic events.

- **RSUs** belong to the membership manager. When an RSU receives a request message for certificate issue from an OBU, it checks the validity of the OBU with the membership manager. If the OBU is legal, the RSU issues multiple anonymous certificates to the OBU by using universal re-encryption scheme and group signature scheme.
- **OBUs** periodically send safety messages by using its own short-time anonymous certificate. When an OBU needs anonymous certificates, it requests certificate issue to a nearby RSU. If the OBU is legitimate, it is able to get new multiple short-time anonymous certificates from the RSU.

To make our model more clear, we assume the followings.

- Each OBU has a unique electronic identity, e.g., ELP (Electronic License Plate).
- OBUs change its own short-time anonymous certificates within 1 minute (min) as a result of [7].
- RSUs can establish a secure channel with the membership manager by the Internet or any other reliable communication links with high bandwidth, and the medium used for vehicular communications is IEEE 802.11p incorporated with DSRC [21].
- Membership manager can inspect all RSUs at high level and maintain the compromised entities list.

The proposed anonymous authentication protocol consists of the following 6-phases:

1. Setup: The membership manager sets up its own master key and system parameters based on identity-based group signature scheme [17], universal re-encryption scheme [19] and identity-based key establishment scheme [20].
2. OBU registration: The membership manager assigns MAC keys and long-term secret keys to OBUs. At the same time, the membership manger stores the pairs ⟨OBU's real ID, MAC key, long-term secret key⟩ in his secure storage.
3. RSU registration: The membership manager assigns group signing key and long-term secret key to RSUs.
4. Multiple anonymous certificates generation: When an OBU requests anonymous certificates for a given time period, it generates a session key and transmits a request message including new pseudonym and encrypted public keys to a nearby RSU. After validity check for the OBU and the RSU by membership manager, the RSU issues multiple short-time anonymous certificates to the OBU by using the received partial session key from the membership manager. Finally, the OBU verifies the issued certificates by using the session key and public key of group signature.
5. Safety message authentication: OBUs periodically sign traffic information by using conventional digital signature scheme under its own short-time signing key, and then broadcast a traffic information attached with the signature and the short-time anonymous certificate. Before accepting the received traffic information, each receiver verifies the signature with sender's certificate.
6. OBU's real ID trace: In case of problematic happening, the membership manager traces the real identity of generator for a safety message by using its own private key.

Table 2. Notations.

Notation	Description
GS_{mk}	Master key of group signature
GS_{pk}	Public key of group signature
GS_{params}	System parameters of group signature
sk_{MM}, pk_{MM}	Private/public key pair of membership manager
H, H_0	Cryptographic hash functions
K_i	MAC key for OBU_i
ID_i	Real identity of entity i
ID'_i	Pseudonym of OBU_i
$ID'_{i,*}$	Short-time pseudonym of OBU_i
$Cert_{i,*}$	Short-time anonymous certificate of OBU_i
s_i	Long-term secret key for ID_i
$s_{i,j}$	Session key between ID_i and ID_j
$sk_{i,*}, pk_{i,*}$	OBU_i's short-time private/public key pair
t	Validity period for short-time certificate
$H_K()$	MAC function under the key K
$GSig()$	Group signature function
$E(), D()$	Encryption and decryption function of universal re-encryption, respectively
$Re()$	Re-encryption function of universal re-encryption
$SE(), SD()$	Encryption and decryption function of symmetric encryption, respectively

IV. ROBUST AND EFFICIENT ANONYMOUS AUTHENTICATION PROTOCOL

In this section, we propose a robust and efficient anonymous authentication protocol based on universal re-encryption scheme [19], identity-based group signature scheme [17] and identity-based key establishment scheme [20]. Table 2 describes the notations used in the proposed protocol.

A. Setup

The membership manager generates the required bilinear groups and system parameters in [17]. Given security parameter k, the membership manager chooses a k-bit prime number p, bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2)$ of order p. The membership manager randomly picks generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ be a bilinear pairing. The membership manager selects $\gamma \in \mathbb{Z}_p^*$ and sets $GS_{pk} = g_2^{\gamma}$. After that, the membership manager chooses secure cryptographic hash functions $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ and $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_2^2$. The system parameter GS_{params} and master key GS_{mk} of the membership manager are set up as follows: $GS_{params} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, \hat{e}, p, g_1, g_2, H, H_0, GS_{pk})$, $GS_{mk} = \gamma$.

To use the identity-based key establishment system in [20], the membership manager chooses four primes p_1, p_2, p_3, p_4 and computes $N(= p_1p_2p_3p_4)$ in $\mathbb{Z}_q$. Then, the membership manager selects a secret random multiplier $\alpha \in \mathbb{Z}_{\phi(N)}^*$, where $\phi()$ is the Euler's totient function.

In addition, the membership manager selects its own private key $sk_{MM} \in \mathbb{Z}_q^*$ and computes public key $pk_{MM} = g_3^{sk_{MM}}$, where g_3 is a generator for the underlying group for the ElGamal

cryptosystem in [22].

B. OBU Registration

All OBUs need to be registered from the trusted membership manager and pre-loaded with public system parameters and their own secret quantities before joining VANET. Thus, the membership manager randomly chooses a MAC key K_i, and computes a long-term secret key $s_i = \alpha log_{g_4}(ID_i^2)(mod\ \phi(N))$, where g_4 is a primitive element in $GF(p_j)$, for $1 \leq j \leq 4$. After that, the membership manager transmits (K_i, s_i) to OBU_i over a secure channel and stores $\langle ID_i, K_i, s_i \rangle$ in secure storage.

C. RSU Registration

The membership manager issues a group signing key to each RSU for generating anonymous certificates. To generate a group signing key, the membership manager selects $x_j \in \mathbb{Z}_p^*$ such that $\gamma + x_j \neq 0$, and then sets $A_j = g_1^{1/\gamma + x_j}$. After that, the membership manager computes $s_j = \alpha log_{g_4}(ID_j^2)(mod\ \phi(N))$, where ID_j is location information of RSU_j. Finally, the membership manager sends $\langle (A_j, x_j), s_j \rangle$ to RSU_j over a secure channel.

D. Multiple Anonymous Certificates Generation

When an OBU_i wants to get new multiple anonymous certificates for given time period from a nearby RSU_j, OBU_i and RSU_j run a multiple anonymous certificate generation protocol as Fig. 2. The detailed steps are as follows.

Step 1 An OBU_i encrypts its real identity ID_i based on universal re-encryption under the membership manager's public key to generate a new pseudonym ID_i'. At the same time, the OBU_i randomly selects a short-time validity period t and multiple signing keys $sk_{i,1}, \cdots, sk_{i,n}$, and then computes corresponding public keys (note that, each public key is formed by signature scheme in safety message authentication phase). After that, the OBU_i computes a session key $s_{i,j} = (ID_j^2)^{s_i h(t||K_i)}$ by using a location information of a nearby RSU_j and identity-based key establishment scheme in [20]. Finally, the OBU_i computes MAC value $MAC_{ID_i'} = H_{K_i}(ID_i'||PK'||t)$, where $PK' = SE_{s_{i,j}}(PK)$, and then transmits $\langle ID_i', PK', t, MAC_{ID_i'} \rangle$ to the RSU_j for obtaining n anonymous certificates, where PK is a list of public keys.

Step 2 The RSU_j checks the valid period t since a long period will cause the risk of continued circulation of an invalid certificate by an attacker. If t is a short valid period, RSU_j transmits the received message to the membership manager for checking a validity of OBU_i. The membership manager decrypts the received pseudonym ID_i' for getting real identity ID_i and searches (K_i, s_i) corresponding to ID_i when the RSU_j is unrevoked. If $MAC_{ID_i'}$ is valid and the OBU_i is legal, the membership manager computes a partial session key $g_4^{vs_i h(t||K_i)}$ and sends it with the permission message to the RSU_j, where $v \equiv \alpha^{-1}(mod\ \phi(N))$.

Step 3 If the RSU_j receives the permission message and the partial session key $g_4^{vs_i h(t||K_i)}$, which used to decrypt encrypted public key list PK', from the membership manager, it repeatedly executes a re-encryption algorithm in [19] with the pseudonym ID_i' to obtain n pseudonyms $ID_{i,1}', \cdots, ID_{i,n}'$ for OBU_i. At the same time, the RSU_j computes the session key $s_{i,j} = (g_4^{vs_i h(t||K_i)})^{s_j}$ to get the set of public key PK. After decrypting $SD_{s_{i,j}}(PK')$, the RSU_j computes each $\sigma_l = GSig(ID_{i,l}'||pk_{i,l}||t)$ by using group signature scheme in [17] under its own group signing key and forms each anonymous certificate $Cert_{i,l} = \{ID_{i,l}', pk_{i,l}, t, \sigma_l\}$, where $l = 1, \cdots, n$. Finally, the RSU_j transmits encrypted multiple anonymous certificates $CERT = SE_{s_{i,j}}(Cert_{i,1}, \cdots, Cert_{i,n})$ to the OBU_i.

Step 4 If public keys in the decrypted $Cert_i$ are equal to PK, the OBU_i verifies received certificates by using GS_{pk}. Finally, the OBU_i accepts the issued certificates if all the checks are valid.

E. Safety Message Authentication

OBU_i signs a traffic information m by using a conventional digital signature scheme such as ECDSA under its own short-time signing key $sk_{i,l}$ for generating signature σ_m. Then, the OBU_i forms the safety message $Msg = \{m, \sigma_m, Cert_{i,l}\}$ and broadcasts Msg. Upon receiving a safety message, each receiver first checks the validity of $Cert_{i,l}$ by using GS_{pk}. If the $Cert_{i,l}$ is valid, the receiver retrieves $pk_{i,l}$ from the $Cert_{i,l}$ and verifies σ_m using the $pk_{i,l}$. If σ_m is valid, the traffic information can be accepted, otherwise discarded.

F. OBU's Real ID Trace

In case of any disputed situation, it is necessary to extract the real identity of generator of the broadcasted safety message by the membership manager. Since pseudonyms $ID_{i,l}' = Re(ID_i')$ of OBU_i are computed by re-encryption scheme of [19] with $ID_i' = E_{pk_{MM}}(ID_i)$, the pseudonyms were formed as ciphertexts for OBU's real identity under the pubic key of the membership manager. Note that, due to the property of universal re-encryption, the membership manager can output real identities from pseudonyms in the safety message by using its own private key sk_{MM}.

V. EVALUATION

A. Security

We analyze how the proposed protocol satisfies the security requirements stated in Section II.

- **Authentication.** Since the signature is generated by a conventional digital signature scheme with respect to a pseudonym and a corresponding public key, which was proven to secure against adaptive chosen message attack, no adversary can launch a forgery attack and an impersonation attack to an OBU.
- **Anonymity.** Since OBUs' real identities are encrypted under pk_{MM} and re-encrypted ciphertexts are used as pseudonyms, an attacker who compromised multiple RSUs cannot disclose a real identity from pseudonyms in certificates without knowing sk_{MM} due to the property of universal re-encryption.

OBU_i	RSU_j	Membership manager
1. Set $ID'_i \leftarrow E_{pk_{MM}}(ID_i)$ Choose time period t Compute $sk_{i,1}, \cdots, sk_{i,n}$ and $s_{i,j}$ Set $PK = \{pk_{i,1}, \cdots, pk_{i,n}\}$ $PK' \leftarrow SE_{s_{i,j}}(PK)$ $MAC_{ID'_i} \leftarrow H_{K_i}(ID'_i \| PK' \| t)$ $\xrightarrow{ID'_i, PK', t, MAC_{ID'_i}}$		
2.	Check t $\xrightarrow{ID'_i, PK', t, MAC_{ID'_i}}$	If RSU_j is valid, $ID_i \leftarrow D_{sk_{MM}}(ID'_i)$ Search K_i, s_i If $MAC_{ID'_i}$ is valid, If OBU_i is legal, Compute $g_4^{vs_ih(t\|K_i)}$
	$\xleftarrow{Permission\ message, g_4^{vs_ih(t\|K_i)}}$	
3.	$ID'_{i,1}, \cdots, ID'_{i,n} \leftarrow Re(ID'_i)$ Compute $s_{i,j} = (g_4^{vs_ih(t\|K_i)})^{s_j}$ $PK \leftarrow SD_{s_{i,j}}(PK')$ $\forall\, l, \sigma_l \leftarrow GSig(ID'_{i,l} \| pk_{i,l} \| t)$ Issue $Cert_{i,1}, \cdots, Cert_{i,n}$ $CERT \leftarrow SE_{s_{i,j}}(Cert_{i,1}, \cdots, Cert_{i,n})$	
	$\xleftarrow{CERT}$	
4. $\{Cert_{i,1}, \cdots, Cert_{i,n}\} \leftarrow SD_{s_{i,j}}(CERT)$ If $\forall\, l, pk_{i,1} \in Cert_{i,l}$ are equal to PK, If $\forall\, l, Cert_l$ are valid, Accept n certificates		

Fig. 2. Multiple anonymous certificates generation.

- **Unlinkability.** An eavesdropper cannot link the safety messages since most safety messages consist of different pseudonyms and public keys independently. Even though multiple RSUs are compromised, the attacker does not obtain any information from the compromised RSUs since each OBU generates and transmits different pseudonyms to RSUs during certificate generation protocol.
- **Traceability.** In dispute cases, the membership manager is able to trace the real identity of OBU_i corresponding to pseudonym $ID'_{i,*}$ by using its own private key sk_{MM}. Even if some RSUs are compromised, the membership manager is able to trace OBUs since the trace procedure in the proposed protocol is executed without cooperations with RSUs.

As a result, the proposed protocol provides level 3 privacy in Table 1.

Moreover, since the membership manager issues the partial session key to an RSU in step 2 of the proposed multiple anonymous certificates generation phase if the RSU is uncompromised entity, valid anonymous certificates of an OBU should be made by the valid RSU. That is, there is no necessity to check the validity of the RSU by an OBU in multiple anonymous certificates generation phase. In addition, if the RSU is compromised entity, in contrast to ECPP, the OBU can run multiple anonymous certificates generation protocol with other RSUs by using pre-computed short-time private/public key pairs, because the compromised RSU does not know a list of OBU's public keys.

B. Efficiency

In this section, we compare the proposed protocol with ECPP to show that our protocol provides reasonable efficiency in terms of OBU's computational costs and RSU valid serving ratios. For fairness in comparisons, we selected a bilinear pairing of 80-bit security level as the same security measures of ECPP as follows; degree $k = 6$, $|\mathbb{G}_1| = 160$ bits and $|q| = 1024$ bits. Tables 3 and 4 show the measures to estimate and to compare our protocol with ECPP, respectively. Note that ECPP_M is ECPP's multiple certificates issue type as shown in Table 5.

To measure the valid number of requesting certificates at once per vehicle, we assume that all OBUs in an RSU range request n_V anonymous certificates to the RSU and the average speed of vehicles varies from 10 m/s $\sim$ 40 m/s (or 36 km/hr$\sim$144 km/hr). Therefore, n_V depends on vehicle density d, which

Table 3. Cryptographic operation time (implemented on Pentium IV 3.0 GHz).

Cryptographic operation time	Time(ms)
$\hat{e}$ bilinear pairing operation	4.5
Point multiplication on $\mathbb{G}_1$	0.6
Exponentiation on $\mathbb{Z}_q$	2.1

Table 4. Protocol execution time (implemented on Pentium IV 3.0 GHz, $N_R = |RL|$).

unit: ms

Execution time	ECPP$_M$	Proposed protocol
n certificates issue	20.4+14.4n	12.6+18.6n
n certificates verification	17.1n	17.1n
Validity check of RSU	$9N_R$	no need

Table 5. Modification to multiple-ECPP.

Phase	ECPP$_M$
Public key generation	$\forall\, i \le n, x_i \in \mathbb{Z}_q^*,\ Y_i = x_i P$
Certificate check	check $\forall\, i \le n, Cert_i$
RSU validity check	revocation check (using RL)

Table 6. The maximum number of requesting certificates n_V.

	Lane numbers N_L				
Speed v	2	4	6	8	10
10 m/s	53.4	26.5	17.6	13.1	10.4
20 m/s	53.4	26.5	17.6	13.1	10.4
30 m/s	53.4	26.5	17.6	13.1	10.4
40 m/s	53.4	26.5	17.6	13.1	10.4

means the number of OBUs in an OBU's communication range, that is computed by 2-second rule which drivers maintain as much distance between vehicles, as the vehicle would travel in 2 second. That is, we have $d = R_{\text{range}} \times N_L/(v \times 2)$ where R_{range} is RSU's valid coverage, N_L is the number of lane and v is vehicle speed. Since $T_R \ge T_G \times d$ where $T_R (= R_{\text{range}}/v)$ is passing time through an RSU range and $T_G (= 12.6 + 18.6 n_V)$ is the time overhead for generating n_V certificates, n_V can be measured as follow:

$$n_V \le \frac{T_R}{18.6d} - 0.3 = \frac{R_{\text{range}}}{18.6vd} - 0.3.$$

Table 6 shows the maximum n_V with different vehicle speeds and different lane numbers where $R_{\text{range}} = 300$ meters. As we can see, each OBU can request about $10 \sim 50$ anonymous certificates to an RSU depending on vehicle density.

Fig. 3 shows computational costs of the proposed multiple certificates generation protocol, ECPP$_M$ and ECPP with different N_R and different n. Then, we can observe that the proposed protocol has reasonable efficiency to ECPP$_M$ in the matter of OBU's computational costs. Furthermore, when the number of the compromised RSUs are increased, the proposed protocol has more efficiency than both ECPP$_M$ and ECPP.

Let $|R|_n$ be the minimal number of passed RSUs for n minutes (min), and ρ_n be the probability for each OBU to issue a request for n min. Therefore, an OBU could request n certificates to an RSU among $|R|_n$ RSUs. Then, we have $\rho_n = 1/|R|_n$

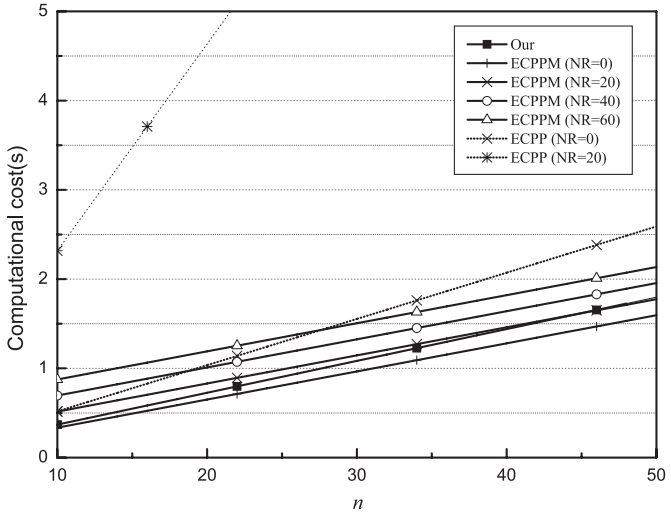

Fig. 3. Computational costs of OBU.

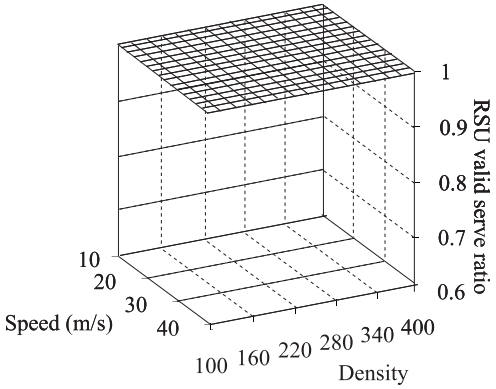

Fig. 4. RSU valid serving ratio.

(note that, since $|R|_n$ is a minimal value, we consider that ρ_n is maximal probability). When we assume that an RSU is allocated every 500 meters on the road, $|R|_1$ and ρ_1 are (10 m/s $\times$ 60 s)/500 m=1.2 and 0.8, respectively. In addition, we have $|R|_n = n|R|_1$. As a result, ρ_n can be measured as follow;

$$\rho_n = \frac{1}{|R|_n} = \frac{1}{n|R|_1} = \frac{1}{n}\rho_1 = \frac{0.8}{n}.$$

To measure RSU valid serving ratio S_{RSU}, we follow Lu *et al.*'s analysis method in [12]. Then, S_{RSU} can be defined by

$$S_{RSU} = \begin{cases} 1, & \text{if } \frac{R_{\text{range}}}{T_K \rho_n v d} \ge 1 \\ \frac{R_{\text{range}}}{T_K \rho_n v d}, & \text{otherwise} \end{cases}$$

where T_K is a time overhead to generate n anonymous certificates and d is the number of OBUs in an RSU's communication range.

Fig. 4 shows RSU valid serving ratios of the proposed protocol for $n \ge 10$. As you can see, RSUs can efficiently manage multiple certificates requests in most traffic scenarios.

Finally, we show the valid serving ratio of the membership manager for OBUs' requests. In our protocol, the main operation of the membership manager is to decrypt OBUs' pseudonyms at

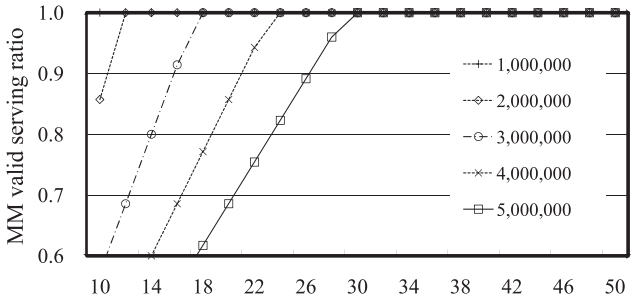

Fig. 5. Membership manager valid serving ratio with different N_{OBU}.

each n min, so the membership manager's performance always depends on the size of n. Then, S_{MM}, the valid serving ratio of the membership manager, can be defined by

$$S_{MM} = \begin{cases} 1, & \text{if } \frac{T_{ms}}{T_{MM}(T_{\mathrm{avg}}/n)N_{\mathrm{OBU}}} \geq 1 \\ \frac{T_{ms}}{T_{MM}(T_{\mathrm{avg}}/n)N_{\mathrm{OBU}}}, & \text{otherwise} \end{cases}$$

where T_{ms} is a total time for a day, T_{MM} is a time overhead for authenticating an OBU, T_{avg} is an average driving time per day and N_{OBU} is the number of OBUs.

Fig. 5 shows the valid serving ratio of the membership manager with different N_{OBU} and different n, where $T_{MM} = 4.2$ ms and $T_{\mathrm{avg}} = 120$ min. From this result, we can observe that the membership manager can efficiently manage multiple certificates requests in most of cases. As a result from Figs. 4 and 5, the proposed multiple anonymous certificates generation protocol is feasible.

VI. CONCLUSION

In this paper, we have proposed a robust and efficient anonymous authentication protocol based on universal re-encryption scheme, identity-based group signature scheme and identity-based key establishment scheme in VANET. Compared with ECPP, the proposed protocol can provide unlinkability and traceability even if an attacker compromises multiple RSUs. Furthermore, to avoid frequent certificate requests and to reduce computational overhead for mutual authentication between OBUs and RSUs in certificate generation phase, RSUs can issue multiple anonymous certificates to an OBU. Moreover, the proposed protocol eliminates validity check in OBUs by using identity-based key establishment scheme. We have demonstrated, through the performance evaluation, that the proposed protocol has comparable performance to ECPP in terms of OBU's computational costs and RSU valid serving ratios.

REFERENCES

[1] U. Varsheney, "Vehicular mobile commerce," *IEEE Computer Magazine Online*, 2004.
[2] Y. Peng, Z. Abichar, and J. M. Chang, "Roadside-aided routing (RAR) in vehicular networks," in *Proc. IEEE ICC*, vol. 8, 2006, pp. 3602–3607.
[3] J. Blum and A. Eskandarian, "The threat of intelligent collisions," *IT Professional*, vol. 6, no. 1, pp. 22–29, 2004.
[4] J.-P. Hubaux, S. Capkun and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy Mag.*, vol. 2, no. 3, pp. 49–55, 2004.
[5] J. Luo, and J.-P. Hubaux, "A survey of inter-vehicle communication technical report," EPFL Tech. Rep. IC/2004/24, 2004.
[6] B. Parno and A. Perrig, "Challenges in securing vehicular networks," *HotNets-IV*, 2005.
[7] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proc. SASN*, 2005, pp. 11–21.
[8] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *Proc. STRC*, 2005.
[9] M. Raya and J.-P. Hubaux, "Securing vehicle ad hoc networks," *J. Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.
[10] K. Ren, W. Lou, R. H. Deng, and K. Kim, "A novel privacy preserving authentication and access control scheme in pervasive computing environments," *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373–1384, 2006.
[11] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Medium access control protocol design for vehicle-vehicle safety messages," *IEEE Trans. Veh. Technol.*, vol. 56, no. 2, pp. 499–518, 2007.
[12] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, 2008, pp. 1903–1911.
[13] X. Lin, X. Sun, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp.3442–3456, 2007.
[14] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. Advances in Cryptology-Crypto, LNCS 3152*, 2004, pp. 41–55.
[15] D. Chaum and E. van Heijst, "Group signatures," in *Proc. Advances in Cryptology-Eurocrypt*, LNCS 576, 1991, pp. 257–265.
[16] A. Shamir, "Identity-based cryptosystem and signature Schemes," in *Proc. Advances in Cryptology-Crypto*, LNCS. 196, 1984, pp. 47–53.
[17] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. CCS*, 2004, pp. 168–177.
[18] J. Freudiger, M. Raya, and M. Felegyhazi, "Mix-zones for location privacy in vehicular networks," in *Proc. WiN-ITS*, 2007.
[19] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, "Universal re-encryption for mixnets," in *Proc. CT-RSA*, LNCS 2964, 2004, pp. 163–178.
[20] U. M. Maurer and Y. Yacobi, "A non-interactive public-key distribution system," *Designs, Codes, and Cryptography*, pp. 305–316, 1996.
[21] Dedicated Short Range Communications (DSRC). [Online]. Available: http://www.leearmstrong.com/dsrc/dsrchomeset.htm
[22] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, 1985.
[23] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," *Advances in Cryptology-Eurocrypt 2003, LNCS 2656*, pp. 614–629, 2003.
[24] P. Kamat, A. Baliga, and W. Trappe, "Secure, pseudonymous, and auditable communication in vehicular ad hoc networks," in *Proc. Security Comm. Networks*, 2008, pp. 233–244.

Chae Duk Jung received the B.S. degree from Dongeui University, Busan, Republic of Korea in 2005, and the M.S. degree from Pukyong National University, Busan, Korea in 2007. He is currently a Ph.D. candidate in the Department of Information Security of Pukyong National University. His research interests are in the areas of cryptographic algorithms, information security, VANET, and PKI.

Chul Sur received his B.S. and M.S. degrees in Department of Computer Science from Pukyong National University, Busan, Republic of Korea in 2000 and 2004, respectively. He is currently a Ph.D. candidate in Department of Computer Science, Pukyong National University. His research interests are related with applied cryptography, network security, and secure e-commerce.

Youngho Park received his Ph.D. and M.S. degrees in Information Security and Computer Science from Pukyong National University, Busan, Republic of Korea, in 2006 and 2002, respectively, and his B.S. degree in computer science from Pukyong National University, in 2000. He was a post-doctor course researcher in the Department of Information Engineering, Pukyong National University from Mar. 2008 to Feb. 2009. His research interests are related with information security, applied cryptography and network security; authentication, key management, secure mobile ad hoc network including vehicular ad hoc network.

Kyung-Hyune Rhee received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology (KAIST), Daejon, Republic of Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute (ETRI), Daejon, Korea from 1985 to 1993. He also worked as a visiting scholar in University of Adelaide in Australia, University of Tokyo in Japan, University of California at Irvine in USA and Kyushu University in Japan, respectively. He has also worked for Colombo Plan Staff College of Technician Education (CPSC) in Manila, Philippines as a director of Information and Communication Technology during 2002 through 2003. He is currently a Professor in the Division of Electronic, Computer and Telecommunication Engineering of Pukyong National University, Republic of Korea. His research interests are related to cryptography and its applications, wireless communication security and multimedia encryption and authentication, IT convergence security, etc.