An Efficient Anonymous Authentication Protocol for Secure Vehicular Communications *

YOUNGHO PARK, CHUL SUR, CHAE DUK JUNG AND KYUNG-HYUNE RHEE*

Division of Electronic, Computer and Telecommunication Engineering
Pukyong National University
Busan, 608-737 Korea

As vehicular communications bring the promise of improved road safety and optimized road traffic through cooperative systems applications, it becomes a prerequisite to make vehicular communications secure for the successful deployment of vehicular ad hoc networks. In this paper, we propose an efficient authentication protocol with anonymous public key certificates for secure vehicular communications. The proposed protocol follows a system model to issue on-the-fly anonymous public key certificates to vehicles by road-side units. In order to design an efficient authentication protocol, we consider a key-insulated signature scheme for certifying anonymous public keys of vehicles to the system model. We demonstrate experimental results to confirm that the proposed protocol has better performance than other protocols based on group signature schemes.

Keywords: vehicular network, security, authentication, anonymous public key certificate, key-insulated signature

1. INTRODUCTION

Vehicular ad hoc network (VANET) is an emerging type of network in which mobile vehicles and fixed road-side units (RSU) participate in the communication by means of wireless communication technologies, and vehicles equip with on-board unit (OBU) which provides wireless communication capability as well as several processors and storage. Vehicular communication is usually developed as a part of Intelligent Transport Systems (ITS) which seeks to achieve safety and productivity through intelligent transportation. As vehicular communications bring the promise of improved road safety and optimized road traffic through cooperative systems applications, VANET have been received a great deal of attention from both academia and industry.

Considering such useful applications in VANET, one of the prerequisites for the successful deployment of VANET is to make vehicular communications secure. For example, life-critical information do not have to be illegally inserted or modified by an attacker in safety applications, and the identity and location privacy of the driver must be protected as far as possible. Therefore, it becomes a fundamental requirement to provide anonymous message authentication for secure vehicular communications. Moreover, there is a common need for a security infrastructure for establishing mutual trust and enabling cryptographic protocols. The security infrastructure includes all technical and organizational measures and facilities needed to provide for the security goals.

Received March 31, 2009; accepted September 30, 2009.
Communicated by Chih-Yung Chang, Chien-Chung Shen, Xuemin (Sherman) Shen, and Yu-Chee Tseng.
* This study was financially supported by Pukyong National University in the 2008 Post-Doc. program. This work was partially supported by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2008-521-D00454).
+ Corresponding author.
1.1 Related Work

Although various security requirements have been considered for secure vehicular networks [8, 10], we just briefly examine some existing authentication protocols [5, 6, 9] in this section since our work focuses on authentication.

Raya et al. proposed some building blocks for secure vehicular communication including anonymous message authentication [9]. As a straightforward solution in their protocol, each vehicle possesses a set of anonymous keys to sign a message and these keys are periodically changed to avoid being tracked. However, it has some critical disadvantages; it requires a large number of anonymous public key certificates, and hence less efficient in storage costs. Moreover, it requires a long revocation list and takes a long time to update the certificate revocation list due to the large number of public keys.

Lin et al. proposed a secure and privacy preservation protocol using group signature scheme, named GSIS [5], to resolve the requirement of a large number of public key certificates. In their work, vehicles possess only their own group signing key issued by a trusted group manager, and each vehicle signs a message by using group signature scheme to be authenticated as a legitimate sender of the message. However, although it does not require a large storage space, the time for message verification accompanied with revocation check grows linearly to the number of revoked vehicles. Thus, each vehicle must spend much time in message verification when the number of revoked vehicles increase, and hence less efficient in computational cost.

Lu et al. proposed a system model for efficient conditional privacy preservation protocol, named ECPP [6], which also use a group signature scheme. Compared with the GSIS, instead of using group signature scheme for anonymous message authentication, each RSU, on vehicle’s request, issues a short-time anonymous public key certificate signed by group signature scheme. Since the RSU checks the validity of the requesting vehicle during the public key certificate issuance phase on the road, such revocation check among vehicles themselves of GSIS is not required. Therefore, message verification is more efficient than GSIS.

1.2 Contribution and Organization

It is evident that Lu et al. introduced a somewhat reasonable system model in ECPP for implementing a practical short-time anonymous public key certificates management on VANET. However, although efficient group signature schemes have been proposed in cryptographic literatures, group signature inherently needs much time consuming operations. Hence, we suggest that key-insulated signature (KIS) scheme be an alternative solution suitable for such a system model. Originally, KIS is a cryptographic primitive to reduce the damage caused by the exposure of a secret signing key stored in an insecure device [3]. Specifically, in a KIS scheme, temporary secret signing keys for insecure devices are generated by a master secret key stored in a physically secure device, but the single corresponding public signature verification key remains unchanged. Our protocol was motivated by this feature of KIS scheme, so we can design a more efficient public key certificate management in VANET.

For example, checking a public key certificate is to verify certificate issuer’s digital signature included in the public key certificate, so it requires the knowledge of certificate
issuer’s public key. Since there are lots of RSUs on VANET, if vehicles are given their anonymous public key certificates from various RSUs, then vehicles have to know the public keys of all RSUs to verify a certificate of any vehicle issued from any RSU. Thus, we intend to resolve this requirement by using KIS scheme in our system model in which only a single public signature verification key of a trusted authority is needed although every RSU has a different secret signing key to issue certificates. Furthermore, KIS is less time consuming than group signature scheme.

Based on these motivations, we propose an efficient anonymous authentication protocol (EA²P) on VANET in this paper. Our system model is similar to that of ECPP, but we consider the KIS scheme as our cryptographic building blocks to issue on-the-fly short-time anonymous public key certificates by RSUs, and take into account the revocation of RSUs signing keys.

In our system, a trusted authority (TA) maintains a master secret key and the corresponding public key, and assigns KIS signing keys to RSUs for a given time period. Then, each RSU uses the KIS signing key to sign and issue an anonymous public key certificate on vehicle’s request during the time period. Inspired by the KIS scheme, however, vehicles do not need to know all public keys of all RSUs on VANET to verify a public key certificate issued by any RSU because only TA’s public key is used in certificate verification.

The rest of this paper is organized as follows: We describe our system architecture and security goals for secure safety message applications in section 2, and we present the proposed protocols in section 3. We analyze the performance of the protocol as comparing with ECPP in section 4 and discuss security of the proposed protocol in section 5. Finally, we conclude in section 6.

2. SYSTEM MODEL

2.1 Network Architecture

As shown in Fig. 1, VANET in our system consists of three entities which have the following roles, respectively.

TA: TA, such as Governmental Transportation Authority, is in charge of the registration of RSUs deployed on the road side and vehicles equipped with OBU. The TA can reveal the real identity of a message originator by incorporating with its subordinate RSUs when a disputed situation is occurred.

RSU: RSUs are controlled by the TA and responsible for issuing short-time anonymous public key certificates for vehicles by using KIS scheme. RSUs assist the TA to track the identity of any message sender. RSUs will not disclose any inner information without the authorization of the TA.

OBU: OBUs installed on vehicles mainly communicate with each other for sharing local traffic information to improve the safety driving conditions, and with RSUs for requesting a short-time anonymous public key certificate.
In most VANET environments, we assume that RSUs can establish a secure channel with the TA by the Internet or any other reliable communication links, and the TA can inspect all the RSUs by an intrusion detection mechanism. Hence, once an RSU is compromised in one time period, the TA can detect and take an action to recover it in the next time period.

2.2 Design Goals

In this paper, we consider the following objectives to design secure VANET:

- **Anonymous Authentication**: The sender of a safety message should be authenticated to guard against the impersonation and message forgery attacks, but the real identity of the sender should not be disclosed from the message authentication protocol in order to preserve sender’s privacy.

- **Vehicle Tracing**: The authorities should be able to trace the sender of a message by revealing the identity in case of any disputed situation such as liability investigation. That is, privacy preservation protocols in VANET must be conditional by way of precaution against problematic situations.

- **Efficient Protocol**: Security schemes should be efficient in terms of message size and message authentication time for communication and computation efficiency, respectively.

2.3 Basic Safety Message Protocol

Because safety applications on VANET are in the beginnings and the primary VANET’s goal is to increase road safety, we also consider a simple public safety message application.

- We assume that each vehicle periodically broadcasts safety messages over a single hop every 300 millisecond (ms) according to the DSRC specification [12].

- To authenticate a sender of message and to guarantee the integrity of a message, each sender should provide a digital signature for the safety message accompanied with its public key certificate. Safety message may include vehicle’s position, current time, direction, speed, acceleration/deceleration and any other traffic-related events of the ve-
vehicle etc., but the identity of message sender is not included for anonymity in our protocol.

Upon receiving the message, each receiver first verifies the certificate and digital signature. If it holds, then the OBU accepts the message, otherwise drops it.

3. PROPOSED PROTOCOL: EA²P

The proposed EA²P consists of the followings; system initialization, short-time anonymous public key certificate issuance, message authentication using the anonymous public key, and vehicle tracing. In order to design concrete protocols, we consider the key-insulated signature scheme [7] and the ID-based key agreement scheme based on bilinear pairings [1]. Table 1 shows the notations used in our protocols.

<table>
<thead>
<tr>
<th>Notations</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_1, G_2, G_T$</td>
<td>cyclic groups of the same prime order $q$.</td>
</tr>
<tr>
<td>$\hat{e}: G_1 \times G_2 \rightarrow G_T$</td>
<td>bilinear map from $G_1 \times G_2$ to $G_T$.</td>
</tr>
<tr>
<td>$g_1 \in G_1, g_2 \in G_2$</td>
<td>generators of $G_1$ and $G_2$, respectively.</td>
</tr>
<tr>
<td>$K_{TA}$</td>
<td>TA’s secret key for message encryption.</td>
</tr>
<tr>
<td>$PID_i$</td>
<td>pseudo-id for a real vehicle identity $VID_i$.</td>
</tr>
<tr>
<td>$RSU_j$</td>
<td>identity of an RSU.</td>
</tr>
<tr>
<td>$OBU_i$</td>
<td>on-board unit of a vehicle with $VID_i$.</td>
</tr>
<tr>
<td>$ok_i, rk_j \in G_i$</td>
<td>ID-based private keys for $OBU_i$ and $RSU_j$, respectively.</td>
</tr>
<tr>
<td>$kk_j \in G_1$</td>
<td>$RSU_j$’s secret KIS signing key.</td>
</tr>
<tr>
<td>$t$</td>
<td>short-time period for anonymous public key.</td>
</tr>
<tr>
<td>$sk_{i,j}, pk_{i,j}$</td>
<td>$OBU_i$’s short-time private and public key pair, respectively.</td>
</tr>
<tr>
<td>$Cert_{i,j}$</td>
<td>short-time anonymous public key certificate for $pk_{i,j}$.</td>
</tr>
<tr>
<td>$Enc_K(), Dec_K()$</td>
<td>encryption and decryption under the key $K$, respectively.</td>
</tr>
<tr>
<td>$MAC_K()$</td>
<td>message authentication code under the key $K$.</td>
</tr>
</tbody>
</table>

| $H_1: \{0, 1\}^* \rightarrow G_1$ | cryptographic one-way hash functions.                                    |
| $H_2: G_1 \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ |                                                                       |
| $H_3: G_1^3 \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ |                                                                       |

3.1 System Initialization and Registration

TA chooses random numbers $s_0, x, x' \in Z_q^*$ and sets $s_0 = x - x'$ as the master secrets for ID-based private key extraction and KIS key extraction, respectively. TA calculates $y_0 = g_0^{s_0}, y_1 = g_1^{s_0}$ and $y'_1 = g_1'^{s_0}$, and then publishes system parameters $(G_1, G_2, G_T, q, g_1, g_2, \hat{e}, y_0, y_1, y'_1, H_1, H_2, H_3)$. Here, $(y_1, y'_1)$ is the public KIS verification key to be used for verifying short-time anonymous public key certificate issued by an RSU. TA issues ID-based private keys and KIS signing keys according to the initial registration process of Fig. 2. We assume that those keys are distributed through an out-of-band channel.
Upon receiving the request, mutual authentication, and the other is a short-time anonymous public key certificate, it is necessary to renew its anonymous public key certificate in its time anonymous public key certificate. On the other hand, if the registering entity is an RSU, RSU’s private key $r_k$ is derived from $H_i(RSU)\phi$, and the TA also assigns a secret KIS signing key $kk$ and partial public key $v_j$ used for issuing a Cert. Note, in KIS signing key generation steps, that $c_j = H_2(v_j, T)$ makes fine-grained revocation possible with respect to RSU’s signing key. We will discuss this in section 5.3.

### 3.2 Short-time Anonymous Public Key Certificate Issuance

Instead of having a large number of pre-issued set of short-time anonymous public key certificates, each vehicle can obtain a Cert from an RSU when the vehicle is necessary to renew its anonymous public key certificate in its OBU. Fig. 3 shows the certificate issuance protocol. This protocol largely consists of two phases. One is authenticated key agreement between the OBU and the RSU using their ID-based private keys for mutual authentication, and the other is a short-time anonymous public key certificate generation using KIS scheme by the RSU.

The detailed protocol steps are described as follows:

1. When a vehicle with $OBU_i$ requests a Cert to RSU, OBU and RSU should authenticate each other to convince whether $OBU_i$ (to RSU) or RSU (to OBU) is a legal entity admitted by the TA. First, $OBU_i$ chooses a random value $a \in Z_p^*$ to compute $g_i^a$ and $\phi_i = H_i(PID_i)$, and then sends a request together with $(g_i^a, \phi_i)$ to RSU.
2. Upon receiving the request, RSU chooses a random value $b \in Z_p^*$ and sets $g_2^b$ and $\phi_i = H_i(RSU_j)$. RSU calculates $k = e(\phi_i^b, y_0) \cdot e(r_k, g_2^b)$ to compute $\pi = MAC(RSU_j, \phi_i, g_2^a, g_2^b)$, and then sends $(g_2^b, \pi)$ to the OBU as a response.
3. The $OBU_i$ computes $k = e(\phi_i, g_2^b) \cdot e(\phi_i^a, y_0)$, and checks $\pi_i = MAC_i(RSU_j, \phi_i, g_2^a, g_2^b)$ to authenticate the RSU. If it holds, the $OBU_i$ selects private/public key pair $(sk_i, pk_i)$ and short-time period $t$ ($t < T$). Then $OBU_i$ requests a Cert for the public key $pk_i$ to be used for the time period $t$ by providing $\pi_i = MAC_i(PID_i, RSU_j, \phi_i, g_2^a, g_2^b, pk_i, t)$ to RSU. In this case, the time period $t$ should be reasonable.
To verify the validity of the

\[ \text{Certi}_i \]

3. \( \phi_i = H_1(\text{RSU}_j) \)
\[ k = \hat{e}(\phi_i, g_3^b) \cdot \hat{e}(\sigma_j, \gamma_j) \]
check \( \pi_j = \text{MAC}_d(\text{RSU}_j, \phi_i, \phi_j, g_3^a, g_3^b) \)
choose \( \text{sk}_{k,j}, \text{pk}_{k,j}, t \)
\[ C_i = \text{Enc}_d(\text{PID}_i, \text{pk}_{k,j}, t) \]
\[ \pi_i = \text{MAC}_d(\text{PID}_i, \text{RSU}_j, \phi_i, \phi_j, g_3^a, g_3^b, \text{pk}_{k,j}, t) \]

4. \( \text{req2}: C_i, \pi_i \)
\[ \langle \text{PID}_i, \text{pk}_{k,j}, t \rangle = \text{Dec}_c(C_i) \]
check \( \pi_i = \text{MAC}_d(\text{PID}_i, \text{RSU}_j, \phi_i, \phi_j, g_3^a, g_3^b, \text{pk}_{k,j}, t) \)
\[ u_j = Z_q, w_j = g_3^{a_j} \]
\[ z_j = H_2(v_j, w_j, \text{pk}_{k,j}, t) \]
\[ \sigma_j = u_j z_j + k (\text{mod } q) \]
\[ \text{Cert}_{j} = \langle \text{pk}_{k,j}, t, \sigma_j, z_j, v_j \rangle \]
store \( \langle \text{PID}_i, \text{Cert}_{j} \rangle \)

5. \( c_j = H_2(v_j, T) \)
check \( z_j = H_2(v_j, (g_3^a(y_j y'_j)^{-1})^{1/2}) \)
\( \text{pk}_{k,j}, t \)

Fig. 1. Short-time anonymous public key certificate issuance protocol between OBU and RSU.

to cope with a message tracing attack by a pervasive attacker. We will discuss this situation in section 5.2.

4. When receiving a certificate request, \( \text{RSU}_j \) first decrypts \( C_i \) to get \( \text{OBU}_i \)'s pseudo-id \( \text{PID}_i \), public key \( \text{pk}_{k,j} \), and \( t \), and then looks up the up-to-date revocation list retrieved from the TA to check the validity of the given \( \text{PID}_i \). If the \( \text{PID}_i \) is revoked one, the \( \text{RSU}_j \) refuses to issue a short-time public key certificate. Otherwise, \( \text{RSU}_j \) verifies \( \pi_i = \text{MAC}_d(\text{PID}_i, \text{RSU}_j, \phi_i, \phi_j, g_3^a, g_3^b, \text{pk}_{k,j}, t) \). If it holds, the \( \text{OBU}_i \) is ultimately authenticated, and then \( \text{RSU}_j \) generates a \( \text{Cert}_{j} = \langle \text{pk}_{k,j}, t, \sigma_j, z_j, v_j \rangle \) by using \( \text{RSU}_j \)'s KIS signing key \( k_k \). In fact, \( \langle \sigma_j, z_j, v_j \rangle \) is \( \text{RSU}_j \)'s digital signature of KIS scheme for certifying the given public key \( \text{pk}_{k,j} \). In the end, \( \text{RSU}_j \) issues the \( \text{Cert}_{j} \) to \( \text{OBU}_i \) and stores \( \langle \text{Cert}_{j}, \text{PID}_i \rangle \) in its local certificate list for assisting TA by way of provision against a liability investigation. Note, in certificate generation, that no identity-related information is included in \( \text{Cert}_{j} \).

5. To verify the validity of the \( \text{Cert}_{j} \), \( \text{OBU}_i \) computes \( c_j = H_2(v_j, T) \) for the current time period \( T \) and checks \( z_j = H_2(v_j, (g_3^a(y_j y'_j)^{-1})^{1/2}) \) by using \( \text{TA} \)'s KIS public key \( \langle y_j, y'_j \rangle \). If it holds, the vehicle comes to possess the private/public key pair \( \langle \text{sk}_{k,j}, \text{pk}_{k,j} \rangle \) and the corresponding anonymous public key certificate \( \text{Cert}_{j} \). Then, \( \text{OBU}_i \) can use
YOUNGHO PARK, CHUL SUR, CHAE DUK JUNG AND KYUNG-HYUNE RHEE

3.3 Anonymous Message Authentication

Once obtaining a \(\text{Cert}_{t,j}\), \(\text{OBU}_i\) can send safety messages in authenticated manner during the short-time period \(t\). With the proposed protocol, \(\text{OBU}_i\) which intends to send a safety message \(\text{msg}\) composed of traffic-related information without vehicle’s identity can run the following steps:

1. \(\text{OBU}_i\) signs the \(\text{msg}\) under short-time signing key \(\text{sk}_i\) for digital signature \(\text{sig}_i = \text{Sig}(\text{sk}_i, \text{msg})\), where \(\text{Sig()}\) is ordinary digital signature algorithm such as ECDSA, and forms the message \(\text{Msg} = [\text{msg} | \text{sig}_i | \text{Cert}_{t,j}]\), and then broadcasts \(\text{Msg}\) over wireless channel.

2. Upon receiving a safety message, each receiving \(\text{OBU}\) first checks the validity of the signature \(\langle \text{σ}_j, \text{z}_j, \text{v}_j \rangle\) in the \(\text{Cert}_{t,j}\) by using TA’s KIS public key \(\langle y_1, y'_1 \rangle\) for the current date \(T\). Here, the same verification procedure in step 5 of Fig. 3 is used. If the \(\text{Cert}_{t,j}\) is valid, then the receiver retrieves the public key \(\text{pk}_{i,j}\) from the \(\text{Cert}_{t,j}\) and verifies the signature \(\text{sig}_i\) using the \(\text{pk}_{i,j}\). If \(\text{sig}_i\) is verified as valid, the safety message is accepted, otherwise discarded.

3.4 Vehicle Tracing

When we deploy vehicular safety applications, liability requirement should be considered in addition to privacy preservation requirement. Hence, anonymity should be conditional depending on scenarios such as law enforcement. In our EA\(^2\)P, if a disputed circumstance occurs to a safety message \(\text{Msg} = [\text{msg} | \text{sig}_i | \text{Cert}_{t,j}]\), TA is involved in tracing the originator of this message.

The detailed protocol steps are described as follows:

1. TA first retrieves the partial public key \(\text{v}_j\) from the \(\text{Cert}_{t,j}\) and searches its trace list to find the \(\text{RSU}_j\) for the \(\text{v}_j\), then requests the pseudo-id of the \(\text{Cert}_{t,j}\) holder to the \(\text{RSU}_j\).

2. On TA’s demand, the \(\text{RSU}_j\) retrieves the pseudo-id corresponding to the \(\text{Cert}_{t,j}\) by searching its local certificate list and returns the pseudo-id \(\text{PID}_i\) to the TA.

3. Then, the TA can finally recover the real identity from the returned pseudo-id by \(\text{VID}_i = \text{Dec}_{k_\text{TA}}(\text{PID}_i)\).

4. PERFORMANCE EVALUATION

In order to evaluate the performance of our protocol in terms of RSU valid serving ratio and efficient message verification, we compare our EA\(^2\)P with ECPP of Lu et al.’s [6] in this section. For fairness in comparisons, we selected the same security measures of Lu et al.’s: We assumed an MNT curve of embedding degree \(k = 6\) and \(|q| = 160\) bits for bilinear pairing implemented on Pentium IV 3.0GHz [11]. Lu et al. implemented their own digital signature scheme for message authentication. On the other hand, we do not put restriction to any digital signature scheme, but we assume the ECDSA adopted
by IEEE1609.2 standard [13] for message authentication. Tables 2 and 3 show the measures to estimate and to compare our EA²P with ECPP, respectively.

### Table 2. Cryptography operation time.

<table>
<thead>
<tr>
<th>Description</th>
<th>time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_{pair}$</td>
<td>4.5</td>
</tr>
<tr>
<td>$T_{mul}$</td>
<td>0.6</td>
</tr>
<tr>
<td>$T_{ECDSA}$</td>
<td>1.28</td>
</tr>
</tbody>
</table>

### Table 3. Protocol execution time and message size.

<table>
<thead>
<tr>
<th>Description</th>
<th>ECPP</th>
<th>EA²P</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T_{gen}$</td>
<td>34.8</td>
<td>20.4</td>
</tr>
<tr>
<td>$T_{cert}$</td>
<td>18.9</td>
<td>2.4</td>
</tr>
<tr>
<td>$T_{sig}$</td>
<td>1.2</td>
<td>1.28</td>
</tr>
<tr>
<td>$</td>
<td>\text{Sig}</td>
<td>$</td>
</tr>
<tr>
<td>$</td>
<td>pk</td>
<td>+</td>
</tr>
</tbody>
</table>

#### 4.1 RSU Serving Ratio

The main operation of an RSU is to issue anonymous public key certificates to vehicles on requests within RSU’s valid coverage range ($R_{rng}$), so RSU’s performance always depends on vehicles density ($d$) and speed ($v$) within the coverage range. To measure RSU valid serving ratio, we follow Lu et al.’s analysis method [6]. Then, the valid serving ratio $S_{ratio}$, which is the fraction of the number of actually processed certificates to the number of requests, can be measured by the following formula where $\rho$ is the probability for each vehicle to request a certificate.

$$S_{ratio} = \begin{cases} 1, & \text{if } \frac{R_{rng}}{T_{gen} \cdot v} \cdot \frac{1}{d \cdot \rho} \geq 1 \\ \frac{R_{rng}}{T_{gen} \cdot v} \cdot \frac{1}{d \cdot \rho}, & \text{otherwise.} \end{cases}$$

Fig. 4 shows RSU valid serving ratio under EA²P and ECPP with different vehicle density and different vehicle speed within $R_{rng} = 300m$ and $\rho = 0.8$. In this estimation, the time overhead of EA²P certificate issuance protocol was measured by $T_{gen} = 4T_{pair} + 4T_{mul} = 20.4ms$ and that of ECPP measured by $T_{gen} = 6T_{pair} + 13T_{mul} = 34.8ms$, respectively. In Fig. 4, the bold-lined region means that RSU valid serving ratios are 1 under both EA²P and ECPP. From these results, we can observe that RSU under our EA²P can efficiently process vehicle’s short-time anonymous public key certificate request in most scenarios. On the other hand, ECPP cannot effectively process vehicle’s request in some cases. Therefore, our EA²P has the advantage in computational efficiency for certificate issuance service of RSU than ECPP.
4.2 Efficiency of Message Authentication

When we authenticate a safety message, we need to verify the public key certificate and digital signature for the safety message. Therefore, the required time cost under EA²P is $T_{E^2P} = T_{sig} + T_{cert} = 3.68\text{ms}$, and that of ECPP is $T_{ECPP} = T_{sig} + T_{cert} = 20.1\text{ms}$. The gains of computational cost of EA²P against ECPP is inherited from the efficient certificate verification because our EA²P is based on key-insulated signature scheme to generate short-time anonymous public key certificate while ECPP is based on group signature scheme which requires relatively much computations.

In a safety application in which vehicles periodically broadcast safety message, each vehicle is supposed to receive a lot of messages from many other vehicles within the same communication range. Therefore, it is required to measure the throughput of received messages. Suppose that there are $n$ vehicles sending $k$ messages every second within the same communication range and the processing time per received message is $T_p$. In the worst case, where all vehicles contend for the channel, $n_{msg} = n \times k$ messages are received per second, then the message processing ratio is measured by $1/(T_p \times n_{msg})$.

The left figure in Fig. 5 shows the bounds of message processing ratio under EA²P and ECPP for 300ms message interval (i.e., 3.3msg/sec) with different vehicle density. Considering the message verification time $T_p = T_{E^2P}$ and $T_p = T_{ECPP}$, EA²P and ECPP can process about maximum 212msg/sec and 49msg/sec, respectively.

The right figure in Fig. 5 shows the message processing ratio in a highway scenario assuming the uniform distribution of vehicles along each lane to each direction with 300m communication range. We adjusted the inter-vehicle distance as 1m/(km/hr) depending on a vehicle speed. For example, inter-vehicle distance is 100m if a vehicle speed is 100km/hr. Therefore, the higher vehicle speed means the lower vehicle density which causes less message traffics within a communication range, and our EA²P can rather effectively performs message authentication protocol than ECPP.

4.3 Simulated Performance

Furthermore, in order to consider some actual vehicular communication on a real city road environment, we simulated message transmission by using network simulator. We used TraNS with ns2-2.33 [16] and IEEE 802.11p configuration [15]. Our simulation parameters and the city road map are presented in Table 4 and Fig. 6, respectively.

For simulation, we put total 916 vehicles which move with a maximum speed of
EA²P FOR SECURE VEHICULAR COMMUNICATIONS

Fig. 5. Message processing ratio with different vehicle density, and speed in a highway scenario.

Table 4. Configurations for simulation.

<table>
<thead>
<tr>
<th>Dimension Space</th>
<th>13,473m × 12,315m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicle Density</td>
<td>1-80 vehicles in radio</td>
</tr>
<tr>
<td>Max. Vehicle Speed</td>
<td>22.3 m/s</td>
</tr>
<tr>
<td>Nominal Radio Range</td>
<td>300m</td>
</tr>
<tr>
<td>Message Interval</td>
<td>300ms</td>
</tr>
<tr>
<td>Wireless Protocol</td>
<td>802.11p</td>
</tr>
<tr>
<td>Channel Bandwidth</td>
<td>6Mbps</td>
</tr>
<tr>
<td>Payload Size of Message</td>
<td>100 byte</td>
</tr>
</tbody>
</table>

22.3m/s (i.e., 80km/hr) during the simulation, and we made each vehicle broadcast a message every 300ms within 300m nominal wireless communication range. We set the bandwidth to 6Mbs which is one of DSRC channel type and set the payload size of a safety message to 100byte according to [14]. In addition, we appended the fields necessary for digital signature and public key certificate as shown in Table 3, and also adjusted the message timeout to compensate for the delay of cryptographic operations under EA²P and ECPP as shown in Table 2, respectively. We simulated message broadcast over a single-hop, and then we measured received packet size and message authentication processing ratio to the number of received messages per vehicle during 200 seconds simulation.

Fig. 7 shows the number of messages and the number of bytes received by a vehicle during every simulation time period, respectively. From these results, although vehicles
received about 6.8% more messages under EA²P than ECPP (right figure in Fig. 7), we can observe that our EA²P causes about 24.8% less packet overhead than ECPP (left figure in Fig. 7) because the size of a public key certificate of EA²P appended to a safety message is smaller than that of ECPP.

Fig. 8 shows the results of average message processing ratio. Observing the Fig. 8, we can see that EA²P verifies about minimum 95% to the received messages (see Fig. 7) during the simulation while ECPP verifies about maximum 63% to the received messages which is much less than EA²P. In other words, EA²P based message authentication protocol suffers less message loss than ECPP based protocol because the verification of the public key certificate in our EA²P is faster than ECPP. As a result, we can conclude that the proposed EA²P is more practical.

5. DISCUSSION

5.1 Security

In short-time anonymous public key certificates issuance protocol, the authenticity of \( OBU_i \) and \( RSU_j \) is assured by checking the legitimacy of their ID-based private keys issued by the TA. As shown in Fig. 3, because the shared key for message authentication
code is established by the ID-based authenticated key agreement scheme [1]. OBU$_i$ and RSU$_j$ can be authenticated only if they possess their valid ID-based private key. Therefore, when we assume the security of the underlying ID-based key agreement scheme, no one can launch an impersonation attack unless the entity is registered to the TA.

Then, the RSU$_j$ issues anonymous public key certificate Cert$_i$ signed by RSU$_j$’s secret KIS signing key $kk_j$ only if the given vehicle’s PID$_i$ is not revoked by checking up-to-date revocation list from the TA. Even though PID$_i$ is known to the RSU$_j$, RSU$_j$ cannot reveal the real identity $VID_i$ from the PID$_i$ because PID$_i$ is the encryption of $VID_i$ under TA’s secret key $K_{TA}$.

Once OBU$_i$ is given a short-time anonymous public key certificate from an RSU$_j$, it can use this certificate in safety message authentication protocol. A remarkable feature in this protocol is how we can verify the certificate included in a safety message. As shown in the protocol description, the Cert$_i$ is verified by using TA’s KIS public key $\langle y_1, y_1' \rangle$ while OBU$_i$’s public key is signed by RSU$_j$’s secret KIS signing key $kk_j$. If the signature in the Cert$_i$ is valid, it implicitly means that a legitimate RSU$_j$, which obtains valid KIS signing key for the current time period $T$ from the TA, issued the certificate Cert$_i$. And hence, if the signature sig$_i$ for the safety message is verified as valid by using the public key $pk_i$ in the Cert$_i$, the owner of $pk_i$ can be consecutively authenticated as a legitimate sender of the message during the time period $t_i$. In addition, because safety message does not contain identity information of message sender and the Cert$_i$ does not contain any identity information of $pk_i$ owner, the sender can be anonymously authenticated in our protocol.

5.2 Time Period for Anonymity

Although anonymous certificates do not contain any identity-related information about the key owner, privacy can still be hijacked by tracing and linking the messages containing the same public key. Therefore, anonymous keys should be changed in such a way that a pervasive observer cannot track the owner of the key. To decide the key changing interval, Raya et al. proposed a key changing algorithm that can preserve privacy in their work [9]. Thus, the bound for the short-time period $t_i$ for anonymous public key in our EA$^2$P can be determined following Raya et al.’s algorithm.

According to [9], the bound for the key changing interval $T_{key}$, and the number of messages $N_{msg}$ to be sent are defined as follows (we can refer to [9] for detailed derivation):

\[
\min(T_{key}) = \frac{d_v + 2d_v}{v_t} \text{ seconds}
\]

\[
\max(T_{key}) = \frac{d_{att}}{v_t} \text{ seconds}; \text{ if } d_{att} > d_v + 2d_v
\]

\[
N_{msg} = \lceil r_m \times T_{key} \rceil \text{ messages}
\]

where, $v_t$ is the speed of target vehicle $V$, $d_v$ is $V$’s transmission range, $d_v$ is distance over which $V$ does not change its speed, $d_{att}$ is the distance for message collection by an attacker, and $r_m$ is the message rate.
Therefore, the time duration for a public key should not exceed the max(Tkey) or OBU should change its public key every Nmsg messages.

5.3 Fine-grained Revocation of RSU Signing Keys

Although RSUs are managed by the TA, we do not exclude a possibility that RSUs may be compromised by an attacker because RSUs are generally located at physically unprotected and public road side. Therefore, vehicles need to check whether RSU’s signing key is revoked or not when vehicles obtain their anonymous public key certificates. The simple and traditional way is to use revocation list, such as certificate revocation list (CRL) in PKI. However, it is not always possible for vehicles to get the revocation list in VANET because vehicles may not keep the direct connection to the TA.

Therefore, we considered fine-grained revocation scheme [2] in this paper. Our EA2P based on key-insulated signature scheme makes fine-grained revocation of RSUj’s signing key possible by combining with time or date-stamps. For example, if the TA sets the time period T as current date to compute \( c_j \) = \( H_j(v_j, T) \), RSUj’s secret signing key \( k_{ki} = c_j r_j + x_0 + x' \) (mod q) is generated as the function of \( c_j \), and OBUs can also use the current date to check the validity of RSUj’s signature in a certificate in step 5 of Fig. 3. Therefore, RSUj’s signing key is naturally useless after the day, and RSUj must obtain a new secret signing key from the TA. Moreover, the damage of the compromise of RSUj’s signing key is restricted to the end of the day and TA can renew RSUj’s signing key for the next day.

However, this has an unfortunate consequence of having to periodically re-issue all private keys in the system, so the shorter time period requires the more frequent key re-issue. Nevertheless, every day signing key renewal of the TA is insignificant operation because only hash function and multiplication are used for key renewal and furthermore, pre-computations are also possible.

6. CONCLUSION

In this paper, we have proposed an efficient and effective anonymous authentication protocol based on the system model which on-the-fly short-time anonymous public key certificate for a vehicle is issued by an RSU on vehicle’s request when it needed. To implement a concrete protocol, we considered a key-insulated signature scheme to issue anonymous public key certificate by RSUs. By doing so, our protocol is more efficient and effective in RSU valid serving capability and message verification than those of group signature-based protocols. We have demonstrated, through the performance evaluation, that the proposed protocol could achieve much better performance than ECPP based on group signature scheme. As a result, the proposed protocol can be properly applied for practical secure vehicular communications.

REFERENCES

2. X. Ding and G. Tsudik, “Simple identity-based cryptography with mediated RSA,”


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 worked as 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 and applied cryptography to communication security; authentication, key management, secure wireless ad hoc network including vehicular ad hoc network.
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. course student in Department of Computer Science, Pukyong National University. His research interests are related with applied cryptography, network security, and secure e-commerce.

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. course student 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.

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, University of Tokyo, and University of California, Irvine, respectively. 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 digital rights management.