Efficient Anonymous Authentication Protocol Using Key-Insulated Signature Scheme for Secure VANET

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

Division of Electronic Computer and Telecommunication Engineering, Pukyong National University, 599-1 Daeyon 3Dong Nam-Gu, Busan, Republic of Korea
{pyhoya,kahlil,jcd0205,khrhee}@pknu.ac.kr

Abstract. In this paper, we propose an efficient authentication protocol with conditional privacy preservation for secure vehicular communications. The proposed protocol follows the system model to issue on-the-fly anonymous public key certificates to vehicles by road-side units. In order to design an efficient message authentication protocol, we consider a key-insulated signature scheme for certifying anonymous public keys of vehicles to such a 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, anonymous, authentication, key-insulated signature.

1 Introduction

As vehicular communications bring the promise of improved road safety and optimized road traffic through cooperative systems applications, vehicular ad hoc networks(VANET) have received a great deal of attention from both academia and industry. Considering the useful applications in VANET, a prerequisite for the successful deployment of VANET is to make vehicular communications secure first of all [6][8].

For example, it is essential to make sure that life-critical information cannot be illegally inserted or modified by an attacker in safety applications, and it should also protect the privacy of the drivers and passengers as far as possible. Therefore, it becomes 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 schemes. The security infrastructure includes all technical and organizational measures and facilities needed to provide for the security goals.

Raya et al. [7] proposed some building blocks for secure vehicular communication. 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

F. Granelli et al. (Eds.): MOBILIGHT 2009, LNICST 13, pp. 35–44, 2009.

a large number of anonymous public key certificates, and hence less efficient in storage costs. Moreover, it requires a long revocation list and a long time to update the certificate revocation list due to the large number of public keys.

Lin et al. [3] proposed a secure and privacy preservation protocol using group signature scheme, named GSIS, 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 with the number of revoked vehicles, and hence less efficient in computational cost.

Lu et al. [4] proposed a system model for efficient privacy preservation protocol, named ECPP, which also uses a group signature scheme. Compared with the GSIS, instead of using group signature scheme for anonymous message authentication, each RSU(Road Side Unit), on vehicle's request, issues on-the-fly short-time anonymous public key certificate to the requesting vehicle by using group signature scheme. Since the RSU checks the validity of the requesting vehicles during the short-time anonymous public key certificate issuance protocol, such revocation check by vehicle itself of GSIS is not required. Therefore, message verification is more efficient than GSIS.

It is evident that Lu et al., in ECPP, introduced a somewhat reasonable system model for implementing a practical short-time anonymous public key certificates management in VANET. However, although efficient group signature schemes have been proposed in cryptographic literatures, group signature itself is still a rather much time consuming operation. Hence, in our opinion, key-insulated signature(KIS) [2] scheme may be an alternative solution suitable for this network architecture.

Based on these observation, in this paper, we propose an efficient anonymous authentication protocol(EA^2P) in VANET. Our system model and roles of each entity on VANET are similar to ECPP's. However, we consider the KIS scheme to our system model as our cryptographic building blocks to issue on-the-fly short-time anonymous public key certificates by RSUs. We demonstrate experimental results to confirm that our protocol has better performance than other protocols based on group signature schemes.

The rest of this paper is organized as follows: We describe our system architecture in Section 2, and we propose our protocols in Section 3. We analyze the performance of our protocol as comparing with ECPP in Section 4, and conclude in Section 5.

2 System Model

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

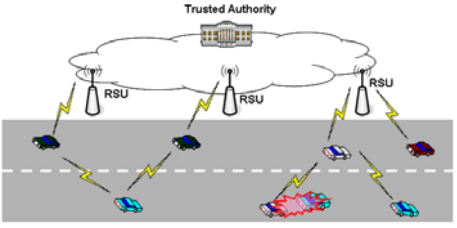


Fig. 1. Vehicular network model

message application using IEEE 802.11p incorporated with DSRC [9]. As shown in Figure 1, vehicular network consists of three entities and each entity has the following roles.

TA: TA(Trusted Authority), such as Governmental Transportation Authority, is in charge of the registration of RSUs deployed on the road side and OBUs equipped on the vehicles. 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 to OBUs by using KIS scheme. RSUs do not disclose any inner information without the authorization of the TA.

OBU: The OBUs are installed on the moving vehicles. They mainly communicate with each other for sharing local traffic information, and with RSUs for requesting the short-time anonymous public key certificate.

3 Proposed Protocol: EA^{2}P

We apply the key-insulated signature scheme [5] and key agreement scheme based on bilinear pairings [1] to our short-time anonymous public key certificate issuance protocol. Table 1 shows the notations used in our EA^{2}P.

3.1 System Initialization

TA chooses random numbers $s_0, x, x' \in Z_q^*$ and sets s_0 and $x_0 = x - x'$ as the master secrets for ID-based private key extraction and key-insulated signing key extraction, respectively. TA calculates $y_0 = g_2^{s_0}$, $y_1 = g_1^{x_0}$ and $y_1' = g_1^{x'}$, and then publishes system parameters $\langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, q, g_1, g_2, \hat{e}, y_0, y_1, y_1', H_1, H_2, H_3 \rangle$. Here, $\langle y_1, y_1' \rangle$ is the public KIS verification key to be used for checking short-time anonymous public key certificate. TA issues ID-based private keys and KIS signing keys according to the initial registration process of Figure 2. We assume that those keys are distributed through out-of-band channel.

Table 1. Notations for EA^{2}P

Notation	Description
$\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$	cyclic groups of the same prime order q.
$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$	bilinear map from $\mathbb{G}_1 \times \mathbb{G}_2$ to $\mathbb{G}_T$.
$g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$	generators of $\mathbb{G}_1$ and $\mathbb{G}_2$.
K_{TA}	TA's secret key for message encryption.
PID_i	pseudo-id for a real vehicle identity VID_i.
RSU_j	identity of an RSU.
OBU_i	on-board unit of a vehicle VID_i.
$ok_i, rk_j \in \mathbb{G}_1$	ID-based private keys for OBU_i and RSU_j respectively.
$kk_j \in \mathbb{G}_1$	RSU_j's secret KIS signing key.
sk_i, pk_i	OBU_i's short-time private/public key pair.
$Cert_i$	short-time anonymous public key certificate for pk_i.
$Enc_K()$, $Dec_K()$	encryption and decryption under the key K.
MAC_K	message authentication code using the key K.
$H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$	cryptographic one-way hash functions.
$H_2 : \mathbb{G}_1 \times \{0,1\}^* \rightarrow Z_q^*$	
$H_3 : \mathbb{G}_1^3 \times \{0,1\}^* \rightarrow Z_q^*$	

1. for OBU_i:
   (a) compute $PID_i = Enc_{K_{TA}}(VID_i)$.
   (b) set $ok_i = H_1(PID_i)^{s_0}$ as VID_i's ID-based private key for PID_i.
   (c) issue $\langle ok_i \rangle$ to OBU_i.
2. for RSU_j:
   (a) set $rk_j = H_1(RSU_j)^{s_0}$ as RSU_j's ID-based private key.
   (b) choose $r_j \in Z_q^*$ and compute $v_j = g_1^{r_j}$ and $c_j = H_2(v_j, T)$, where T is time period.
   (c) calculate $x_j = c_j r_j + x_0 \pmod q$.
   (d) set $kk_j = x_j + x' \pmod q$ as secret signing key.
   (e) store $\langle RSU_j, v_j \rangle$.
   (f) issue $\langle rk_j, kk_j, v_j \rangle$ to RSU_i.

Fig. 2. Initial registration and key issuance of the TA

3.2 Short-Time Anonymous Public Key Certificate Issuance

Instead of having a large number of pre-issued short-time anonymous public key certificates, each OBU_i can request a $Cert_i$ to the RSU_j within OBU_i's communication range when the OBU_i is necessary to renew its anonymous public key. Figure 3 shows the certificate issuance protocol.

The detailed protocol steps are described as follows.

1. When OBU_i with pseudo-id PID_i requests a $Cert_i$ to RSU_j, they should authenticate each other to determine whether the OBU_i can provide the RSU_j with its PID_i, and to convince the given RID_j and PID_i are valid.

	OBU_i		RSU_j
1.	$a \in Z_q^*$, g_2^a, $\phi_i = H_1(PID_i)$.		
		req1 : g_2^a, ϕ_i $\longrightarrow$	
2.			$b \in Z_q^*$, g_2^b, $\phi_j = H_1(RSU_j)$. $k = \hat{e}(\phi_i^b, y_0) \cdot \hat{e}(rk_j, g_2^a)$. $\pi_j = MAC_k(RSU_j, \phi_i, \phi_j, g_2^a, g_2^b)$.
		$\longleftarrow$ res1 : ϕ_j, g_2^b, π_j	
3.	$k = \hat{e}(ok_i, g_2^b) \cdot \hat{e}(\phi_j^a, y_0)$. check $\pi_j \stackrel{?}{=} MAC_k(RSU_j, \phi_i, \phi_j, g_2^a, g_2^b)$. choose sk_i, pk_i, t_i. $C_i = Enc_k(PID_i, pk_i, t_i)$. $\pi_i = MAC_k(PID_i, RSU_j, \phi_i, \phi_j, g_2^a, g_2^b, pk_i, t_i)$.		
		req2 : C_i, π_i $\longrightarrow$	
4.			$\langle PID_i, pk_i, t_i \rangle = Dec_k(C_i)$. check $\pi_i \stackrel{?}{=} MAC_k(PID_i, RSU_j, \phi_i, \phi_j, g_2^a, g_2^b, pk_i, t_i)$. $u_j \in Z_q^*$, $w_j = g_1^{u_j}$. $z_j = H_3(v_j, w_j, pk_i, t_i)$. $\sigma_j = u_j z_j + kk_j \pmod q$. $Cert_i = \langle pk_i, t_i, \sigma_j, z_j, v_j \rangle$. store $\langle PID_i, Cert_i \rangle$.
		$\longleftarrow$ res2 : $Cert_i$	
5.	$c_j = H_2(v_j, T)$. check $z_j \stackrel{?}{=} H_3(v_j, (g_1^{\sigma_j}(v_j^{c_j} y_1 y_1')^{-1})^{1/z_j}, pk_i, t_i)$.		

Fig. 3. Short-time anonymous public key certificate issuance protocol between OBU_i and RSU_j

OBU_i chooses a random value $a \in Z_q^*$ to compute g_2^a and $\phi_i = H_1(PID_i)$, and then sends a request with $\langle g_2^a, \phi_i \rangle$ to RSU_j.

2. Upon receiving the request, RSU_j chooses a random value $b \in Z_q^*$ and sets g_2^b and $\phi_j = H_1(RSU_j)^b$. RSU_j calculates $k = \hat{e}(\phi_i^b, y_0) \cdot \hat{e}(rk_j, g_2^a)$ to computes $\pi_j = MAC_k(RSU_j, \phi_i, \phi_j, g_2^a, g_2^b)$, and then sends $\langle g_2^b, \phi_j, \pi_j \rangle$ to the OBU_i as a response.
3. The OBU_i computes $k = \hat{e}(ok_i, g_2^b) \cdot \hat{e}(\phi_j^a, y_0)$, and checks $\pi_j \stackrel{?}{=} MAC_k(RSU_j, \phi_i, \phi_j, g_2^a, g_2^b)$ to authenticate the RSU_j. If it holds, the OBU_i selects its anonymous private/public key pair $\langle sk_i, pk_i \rangle$ and short-time period t_i ($t_i < T$). Then OBU_i requests a $Cert_i$ for the public key pk_i to be used for the time period t_i by providing $C_i = Enc_k(PID_i, pk_i, t_i)$ and $\pi_i = MAC_k(PID_i, RSU_j, \phi_i, \phi_j, g_2^a, g_2^b, pk_i, t_i)$.

4. When receiving certificate request, RSU_j first decrypts C_i to get OBU_i's pseudo-id PID_i, public key pk_i and t_i, and then looks up the up-to-date revocation list retrieved from the TA to check the validity of the given PID_i. If the PID_i is revoked one, the RSU_j refuses to issue the short-time public key certificate. Otherwise, RSU_j verifies $\pi_i \stackrel{?}{=} MAC_k(PID_i, RSU_j, \phi_i, \phi_j, g_2^a, g_2^b, pk_i, t_i)$. If it holds, the OBU_i is ultimately authenticated, and then RSU_j generates a $Cert_i = \langle pk_i, t_i, \sigma_j, z_j, v_j \rangle$ by using RSU_j's KIS signing key kk_j. In fact, $\langle \sigma_j, z_j, v_j \rangle$ is RSU_j's digital signature for certifying the given public key pk_i. In the end, RUS_j issues a $Cert_i$ to OBU_i and stores $\langle Cert_i, PID_i \rangle$ 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 the $Cert_i$.
5. To verify the validity of the $Cert_i$, OBU_i computes $c_j = H_2(v_j, T)$ for the current date T and checks $z_j \stackrel{?}{=} H_3(v_j, (g_1^{\sigma_j}(v_j^{c_j} y_1 y_1')^{-1})^{1/z_j}, pk_i, t_i)$ by using TA's KIS public key $\langle y_1, y_1' \rangle$. If it holds, the OBU_i comes to possess the private key sk_i and the corresponding anonymous public key certificate $Cert_i$. Then, OBU_i can use this key for the purpose of anonymous message authentication for the short-time period t_i in VANET.

3.3 Anonymous Message Authentication

Once obtaining a $Cert_i$, the OBU_i can send safety messages in authenticated manner during the short-time period t_i. With the proposed protocol, an OBU_i which intends to send a safety message msg composed of traffic-related information without OBU_i's identity can run the following steps.

1. OBU_i signs the msg with its short-time signing key sk_i for signature $sig_i = Sig(sk_i, msg)$, where $Sig()$ is ordinary digital signature algorithm such as ECDSA, and forms the message $Msg = [msg \mid sig_i \mid Cert_i]$, and then broadcasts Msg.
2. Upon receiving a safety message, each receiving OBU first checks the validity of the signature $\langle \sigma_j, z_j, v_j \rangle$ in the $Cert_i$ for the current date T by using TA's KIS public key $\langle y_1, y_1' \rangle$. Here, the same verification procedure in step 5 of Figure 3 is used. If the $Cert_i$ is valid, then the receiver retrieves the public key pk_i from the $Cert_i$ and verifies the signature sig_i using the pk_i. If sig_i is verified as valid, the safety message can be 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 $Msg = [msg \mid sig_i \mid Cert_i]$, TA is involved in tracing the originator of this message.

1. TA first retrieves the partial public key v_j from the $Cert_i$ and searches its trace list to find the RSU_j for the v_j, then requests the pseudo-id of the $Cert_i$ holder.
2. On TA's demand, the RSU_j retrieves the pseudo-id corresponding to the $Cert_i$ by searching its local certificate list and returns the pseudo-id PID_i to the TA.
3. Then, the TA can ultimately recover the real identity from the returned pseudo-id by $VID_i = Dec_{K_{TA}}(PID_i)$.

4 Performance Evaluation

In order to show the efficiency 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 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 3.0 GHz. We do not put restriction to any digital signature scheme, but we assume the ECDSA adopted by IEEE 1609.2 standard [10] for message authentication. Table 2 and Table 3 show the measures to estimate and to compare our EA^{2}P with ECPP, respectively.

Table 2. Cryptographic operation time

	Description	time
T_{pair}	bilinear pairing operation	4.5 ms
T_{mul}	point multiplication	0.6 ms
T_{ecdsa}	ECDSA signature verification	1.28 ms

Table 3. Protocol execution time and message size of EA^{2}P and ECPP

	Description	ECPP	EA^{2}P
T_{gen}	time for certificate issuance protocol	34.8 ms	20.4 ms
T_{cert}	time for certificate verification	18.9 ms	2.4 ms
T_{sig}	time for signature verification	1.2 ms	1.28 ms
$\|Sig\|$	signature size for a safety message	40 bytes	40 bytes
$\|pk\| + \|Cert\|$	public key certificate size	147 bytes	84 bytes

4.1 RSU Serving Ratio

RSU's main operation is to issue anonymous public key certificates to OBUs on requests within RSU's valid coverage (R_{rng}), so RSU's performance always depends on vehicles density(d) and speed(v) on the road. To measure RSU valid

serving ratio, we followed Lu et al.'s analysis method. 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 defined by

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

where ρ is the probability for each OBU to issue a certificate request.

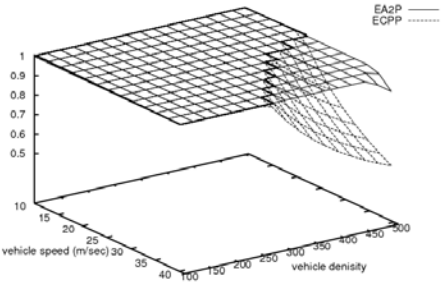


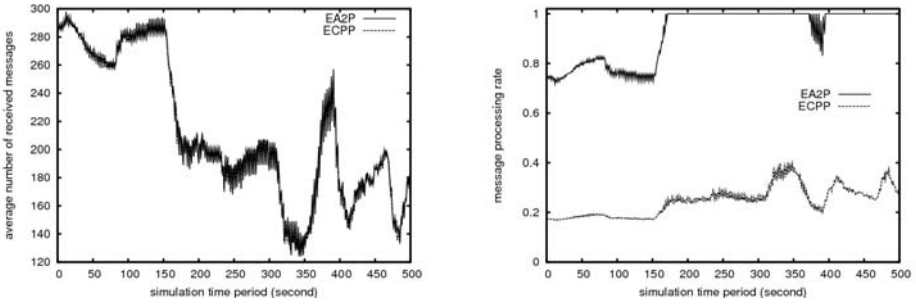
Fig. 4. RSU valid serving ratio of EA^{2}P and ECPP

Figure 4 shows RSU valid serving ratio of EA^{2}P and ECPP with different vehicle density and different vehicle speed for $R_{rng} = 300$m and $\rho = 0.8$. In this estimation, as shown in Table 3, $T_{gen} = 20.4$ms of EA^{2}P short-time anonymous public key certificate issuance protocol in Figure 3 was measured by $4T_{pair} + 4T_{mul}$, and 34.8ms of ECPP by $6T_{pair} + 13T_{mul}$ with respective. From these results, we can observe that RSU in our EA^{2}P can efficiently process OBUs' short-time anonymous public key certificate requests in most scenarios. On the other hand, ECPP cannot effectively process OBUs requests in some cases. Therefore, our EA^{2}P has the advantage in scalability for RSUs than ECPP.

4.2 Efficient Message Verification

When we authenticate a safety message, it requires to verify the certificate and signature of the safety message. Therefore, the required time cost of EA^{2}P is $T_{EA^2P} = T_{sig} + T_{cert} = 4.68$ms, and that of ECPP is $T_{ECPP} = T_{sig} + T_{cert} = 20.1$ms. The computational gains of EA^{2}P against ECPP is due to the certificate verification cost because our protocol considered key-insulated signature scheme to generate short-time anonymous public key certificate while ECPP applied group signature scheme which requires relatively much computations.

In actual vehicular communications, 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



(a) average number of messages (b) average message processing rate

Fig. 5. Average message processing rate of 400 vehicles for the received messages during 500 seconds simulation

communication range and the processing time per 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 rate per second is numerically calculated as $1/(T_p \times n_{msg})$.

In order to consider some actual vehicular communication on the road, we simulated message transmission on VANET by using network simulator, and then we traced the number of received messages and estimated the message processing rates. Figure 5 shows these results. We used TraNS [13] with ns2-2.33 [12] and IEEE 802.11p parameters for ns2 [11]. We put 400 vehicles on a grid-shape road of 600m×700m rectangular size. Each vehicle moves with a maximum speed of 16.7m/s (i.e., 60km/hr) and sends out a message every 300ms within 100m nominal radio range. The simulation was run for 500 seconds and we measured the received messages every second.

From Figure 5, we can observe that EA^{2}P and ECPP received similar number of messages during the simulation, but our EA^{2}P shows about minimum 72% processing rate while ECPP processes about minimum 17% and maximum 40% of received messages, which is much less than EA^{2}P's. As a result, we can conclude that the proposed EA^{2}P is more practical.

5 Conclusion

It is a fundamental security requirement to provide anonymous message authentication mechanism for secure vehicular communications. 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 is issued by an RSU on OBU'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 can achieve much better performance than ECPP based on group signature scheme. As a result, our protocol can be implemented for practical secure vehicular communications.

Acknowledgement

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).

References

1. Chen, L., Cheng, Z., Smart, N.P.: Identity-based key agreement protocols from pairings. International Journal of Information Security 6(4), 213–241 (2007)
2. Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-insulated public key cryptosystems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 65–82. Springer, Heidelberg (2002)
3. Lin, X., Sun, X., Shen, X.: GSIS: a secure and privacy preserving protocol for vehicular communications. IEEE Transaction on Vechicular Technology 56(6), 3442–3456 (2007)
4. Lu, R., Lin, X., Zhu, H., Ho, P.-H., Shen, X.: ECPP: Efficient conditional privacy preservation protocol for secure vehilce communications. In: Proceedings of The IEEE INFOCOM 2008, pp. 1229–1237 (2008)
5. Ohtake, G., Hanaoka, G., Ogawa, K.: An efficient strong key-insulated signature scheme and its application. In: Mjølsnes, S.F., Mauw, S., Katsikas, S.K. (eds.) EuroPKI 2008. LNCS, vol. 5057, pp. 150–165. Springer, Heidelberg (2008)
6. Parno, B., Perrig, A.: Challenges in securing vehicular networks. In: Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV) (2005)
7. Raya, M., Hubaux, J.-P.: Securing vehicular ad hoc networks. Journal of Computer Security 15(1), 39–68 (2007)
8. Zarki, M.E., Mehrotra, S., Tsudik, G.: Security Issues in a Future Vehicular Network. In: European Wireless 2002 (2002)
9. Dedicated Short Range Communications (DSRC), `http://www.leearmstrong.com/dsrc/dsrchomeset.htm`
10. IEEE Standard 1609.2 - IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages (July 2006)
11. IEEE 802.11p parameters for NS2, `http://dsn.tm.uni-karlsruhe.de/Overhaul_NS-2.php`
12. Network Simulator-NS2, `http://www.isi.edu/nsnam/ns/`
13. TraNS - Realistic Simulator for VANET, `http://trans.epfl.ch/`