Journal of Korea Multimedia Society Vol. 13, No. 6, JUNE 2010(pp. 865-874)

An Efficient Anonymous Authentication and Vehicle Tracing Protocol for Secure Vehicular Communications

Young Shin Park[†], Chae Duk Jung[††], Youngho Park[†††], Kyung-Hyune Rhee[††††]

ABSTRACT

Recently, Hao et al. proposed a privacy preservation protocol based on group signature scheme for secure vehicular communications to overcome a well-recognized problems of secure VANETs based on PKI. However, although efficient group signature schemes have been proposed in cryptographic literatures, group signature itself is still a rather much time consuming operation. In this paper, we propose a more efficient privacy preservation protocol than that of Hao et al. In order to design a more efficient anonymous authentication protocol, we consider a key-insulated signature scheme as our cryptographic building block. We demonstrate experimental results to confirm that the proposed protocol is more efficient than the previous scheme.

Key words: VANET, anonymity authentication, privacy, key-insulated signature

1. INTRODUCTION

Vehicular ad-hoc networks (VANETs) have attracted great extensive attentions in recent as a promising technology for revolutionizing the transportation systems. VANETs consist of entities including On Board Units (OBUs) and infrastructure Road Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are two basic communication modes, which respectively allow OBUs to communicate with each other and with the infrastructure RSUs. Furthermore, Vehicular communications bring the promise of improved road safety and location based services. For example, vehicles are able to communicate with each others in order to exchange some valuable traffic information among them, such as roadway conditions, accidents on the road, and so forth[1-8].

Considering the useful VANET applications, it is necessary to develop secure mechanisms to make VANET applications viable. To prevent several possible attacks such as message modification, movement tracking, impersonation, and so on in VANET, it is essential to authenticate the entities which take part in the communication. In particular, privacy is a very important issue in the VANET. Therefore, it becomes the fundamental requirement to provide anonymous message authentication for secure vehicular communications [4,5,7-10].

※ Corresponding Author : Kyung-Hyune Rhee, Address : (608-737) Daeyeon 3-dong, Nam-gu, Busan, Korea, TEL : +82-51-626-4887, FAX : +82-51-626-4887, E-mail: khrhee@pknu.ac.kr
Receipt date : Dec. 17, 2009, Revision date : Feb. 25, 2010
Approval date : Feb. 25, 2010
† Department of Information Security, Pukyong National University
(E-mail : yspark09@pknu.ac.kr)
†† Department of Information Security, Pukyong National University
(E-mail : jcd0205@pknu.ac.kr)
††† Department of IT Convergence and Application Engineering, Pukyong National University
(E-mail : pyhoya@pknu.ac.kr)
†††† Department of IT Convergence and Application Engineering, Pukyong National University
※ Following are results of a study on the "Human Resource Development Center for Economic Region Leading Industry" Project, supported by the Ministry of Education, Science & Tehnology(MEST) and the National Research Foundation of Korea(NRF).

1.1 Related Work

There have been several proposals for privacy preservation in VANETs. Gerlach et al.[3] proposed some building blocks for protecting the real identity of a vehicle or a driver by using pseudonyms. Moreover, Freudiger et al.[2], Huang, et al.[6], and Sampigethava et al.[11] have been proposed variant location privacy protection schemes enhancing the pseudonym-based scheme, respectively. However, pseudonym only schemes are not enough to support the secure functionality of authentication, integrity, and anonymity. To achieve the security requirements, Raya et al.[9] propose a PKI based security and privacy preserving protocol, where each vehicle should be preloaded with a huge number of anonymous public and private key pairs and the corresponding public key certificates issued by a trusted authority. However, this scheme has some disadvantages. Raya et al.'s scheme requires a large number of anonymous public key certificates, which incurs inefficiency for certificate management. To overcome the problem of pre-loading a large number of anonymous key materials in each vehicle, Lin et al. proposed an efficient anonymous public key management by using a group signature scheme in the VANET[7]. In their work, each vehicle possesses only single group signing key issued by a trusted group manager. However, although Lin et al.'s protocol does not require a large storage space, the overhead of message verification accompanied with revocation check grows linearly with the number of revoked vehicles, and hence less efficient in computational cost.

On the other hand, Hao et al.[5] proposed a distributed key management scheme in which RSUs issue private group signing keys dynamically to vehicles in the coverage area of the RSUs, instead of a trusted authority. 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) scheme[12,13] may be an alternative solution suitable for this network architecture.

1.2 Contribution and Organization

In this paper, we propose an efficient anonymous authentication and vehicle tracing protocol for secure vehicular communication on VANETs. Our system model and roles of each entity on VANETs are similar to the Hao et al.'s protocol[5]. However, we employ the KIS scheme as our cryptographic building block to issue on-the-fly signing key by RSUs. More specifically, all the vehicles within the coverage area of an RSU form a same communication domain, and the RSU acts as the KIS signing key distributor in the domain. When a vehicle approaches an RSU, it will get a KIS signing key from the RSU dynamically, then vehicle can authenticate each others by using a KIS scheme. Furthermore, although each vehicle has a different KIS secret signing key, only RSU's single KIS public key is used in signature verification. That is one of our motivations. Besides, our proposed protocol provides unlinkability by renewing vehicle's pseudonym whenever a communication domain is changed. Our scheme has an advantage in efficient authentication as comparing with Hao et al.'s protocol. We demonstrate experimental results to confirm that our protocol has better performance than Hao et al.'s protocol.

The rest of this paper is organized as follows. In Section 2, we introduce the security requirements in VANET. The proposed efficient anonymous authentication and vehicle tracing protocol is introduced in Section 3, followed by the security requirements analysis and the performance analysis in Section 4. Finally, we conclude the paper in Section 5.

2. SECURITY REQUIREMENTS

In this section, we define some security require-

ments for our proposed protocol. 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 some RSUs are compromised by an attacker, 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. In addition, 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 not be traceable yet. Moreover, even though the adversary compromised RSUs, it cannot link information stored in the RSUs as the same OBU.
- Traceability : The authority 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.

3. EFFICIENT ANONYMOUS AUTHENTICATION AND VEHICLE TRACING PROTOCOL

3.1 System Model

Entities in our proposed protocol are classified into three categories: Membership Manager(MM), Road Side Units(RSUs), and On Board Units (OBUs) as shown in Figure 1. The detailed description of the system components is as follows.

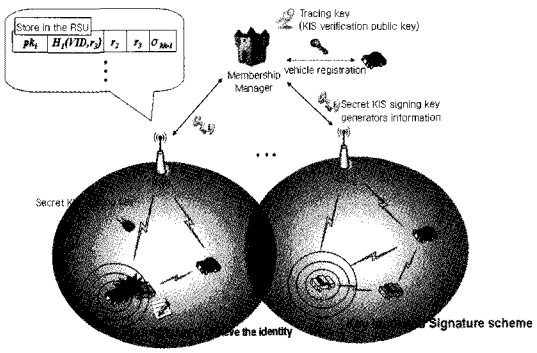


Fig. 1. System Architecture.

- MM (Membership Manager) is a public agency or corporation with administrative powers in a specific field; for example, city or state transportation authorities. The MM establishes and manages system parameters and system roles for secure VANET. In addition, the MM should be able to reveal the identities of message senders in case of a disputed events.
- RSUs (Road Side Units) are controlled by the MM and responsible for issuing secret KIS Signing keys to OBUs. When an RSU received a request message from the MM in order to reveal the identity of an accused message, it sends vehicle's information to the MM.
- OBUs (On Board Units) are installed on the vehicles and periodically send traffic messages signed by KIS scheme.

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

- The MM is fully trusted by all parties in the system, and it is infeasible for any attacker to compromise the MM.
- RSUs are immobile and subordinated by the MM in the most scenarios. Without the authorization of the MM, RSUs will not disclose any inner information. RSUs are assumed to connect with the MM by wired links or any other links with high bandwidth, low delay and low bit er-

ror rates[14].

- OBUs are mobile and moving most of the time, and could be easily compromised by a malicious attacker. When Each OBU enters a new RSU region, each OBU gets KIS signing key from the RSU. Each OBU has a unique electronic identity, e.g., ELP (Electronic License Plate).

3.2 Proposed Protocol

We apply the KIS scheme to our short-time anonymous signing key generation protocol. Table 1 shows the notations used in our proposed protocol.

Table 1. Notation and Description

Notation	Description
$g_1 \in Z_q^*$	Generators of Z_q^*
VID_i	Identity of an OBU_i
RID_j	Identity of an RSU_j
PID_i	Pseudonym for a real vehicle identity VID_i
OBU_i	On-board unit of vehicle VID_i
$kk_i \in Z_q^*$	KIS signing key of an OBU_i
$Enc_K() / Dec_K()$	Encryption/Decryption under the key K
$sig_K()$	Signature function under private key K
sk_i, pk_i	Private/Public key pair of entity i
$H_1 = \{0,1\}^* \rightarrow Z_q^*$	Cryptographic one-way hash function

[Setup] The MM randomly chooses its master secrets $s_0, s_1, s \in Z_q^*$. The MM selects a random number $r_1 \in Z_q^*$ and calculates $x = H_1(RID_j \| s_0 \| r_1)$, $x' = H_1(RID_j \| s_1 \| r_1)$, $x_0 = x - x'$ as the key-insulated signing key extraction. After that, the system parameters will be published, which include $\langle q, q_1, H_1 \rangle$. Here, $\langle x, x' \rangle$ is the master key of KIS signature.

[OBU registration] All OBUs need to be registered to the trusted MM and pre-loaded with public system parameters and their own secret quantities before joining VANET. Then, the MM generates OBU_i's signature $sig_{sk_{MM}}(pk_i)$ with long-term public key. The MM sends $sig_{sk_{MM}}(pk_i)$ to OBU_i.

[RSU registration] The MM generates RSU_j's long-term private/public key pair (sk_j, pk_j), RSU_j's signature $sig_{sk_{MM}}(pk_j)$ with long-term public key, and $SK_{ID-RSU} = H_1(RID_j)^s$. Here, SK_{ID-RSU} is a value to be used in checking an RSU_j's specific region by the MM in vehicle tracing procedure. Then, the MM sends $\langle sk_j, pk_j, sig_{sk_{MM}}(pk_j), SK_{ID-RSU}, x, x' \rangle$ to RSU_j through a secure channel.

[KIS Signing Key Generation] When an OBU_i enters the coverage region of the RSU_j, the RSU_j issues a KIS private signing key to the OBU_i. The generation of KIS private key works as follows.

1. Each RSU_j periodically broadcasts a beacon message containing $\langle RID_j, pk_j, sig_{sk_{MM}}(pk_j) \rangle$ in order to inform vehicles of RSU_j's existence.
2. When the OBU_i enters a RSU_j's region, the OBU_i receives the RSU_j's beacon message. Then, the OBU_i sends OBU_i's public key and corresponding signature encrypted under RSU_j's public key for requesting a valid KIS signing key.
3. Upon receiving the requesting message, the RSU_j decrypts the message and verifies the signature. If it holds, the RSU_j selects a random number $r_2 \in Z_q^*$ and computes a KIS signing key $kk_i = c_j \gamma_j + x_0 + x' \pmod q$ for the OBU_i, where $\gamma_j = H_1(SK_{ID-RSU} \| r_2)$, $v_j = g_1^{\gamma_j}$, and $c_j = H_1(v_j)$. At the same time, the RSU calculates $\langle y_0, y' \rangle = \langle y_0 = g_1^{x_0}, y' = g_1^{x'} \rangle$, where $\langle y_0, y' \rangle$ is the public KIS verification key to be used for checking signature. Then, the RSU_j sends $< Enc_{pk_j}(kk_i, v_j, r_2, sig_{sk_j}(kk_i, v_j, r_2)), y_0, y' >$ encrypted under OBU_i's public key to the OBU_i.

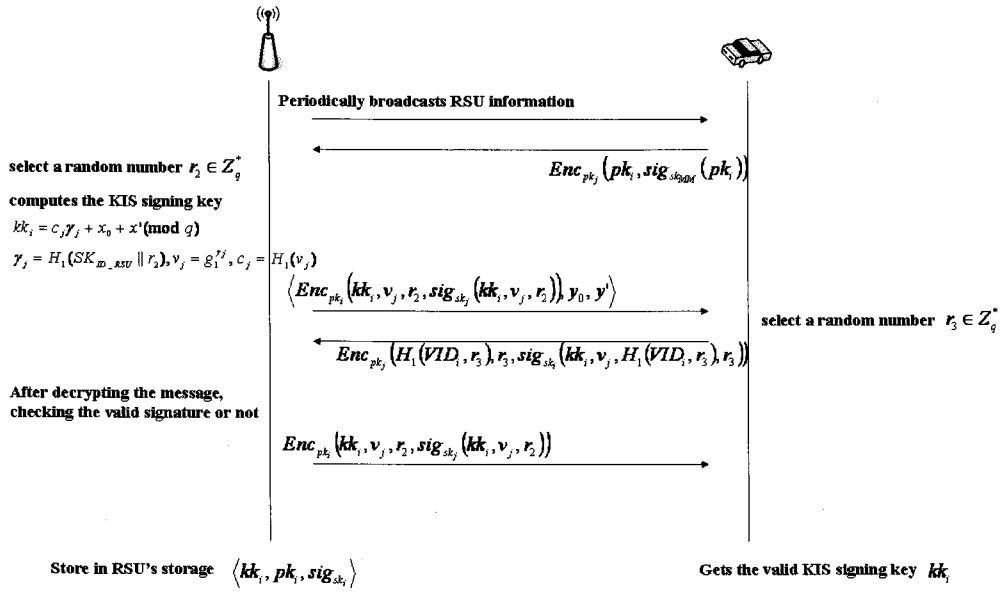


Fig. 2. KIS signing key issuance protocol between OBU_i and RSU_j.

4. When the OBU_i receives the message since the OBU_i decrypts the message and verifies RSU_j's signature. If it holds, the OBU_i chooses a random number $r_3 \in Z_q^*$, and the OBU_i sends $Enc_{pk_j}(H_1(VID_i, r_3), r_3, sig_{sk_i}(kk_i, v_j, H_1(VID_i, r_3), r_3))$ encrypted under RSU_j's public key to the RSU_j.
5. After receiving the message, the RSU_j decrypts the message and verifies the signature $sig_{sk_j}(kk_i, v_j, H_1(VID_i, r_3), r_3)$. If the signature is valid, the RSU_j encrypts $Enc_{pk_i}(kk_i, v_j, r_2, sig_{sk_j}(kk_i, v_j, r_2))$ under OBU_i's public key and transmits the message to the OBU_i, otherwise discarded.
6. Finally, the OBU_i gets a KIS signing key kk_i by decrypting the received message. Then, the OBU_i finishes registration protocol after it gets the valid KIS signing key. Meanwhile, the RSU_j stores the information of the OBU_i, as shown in table 2, in the local database.

Table 2. A Registration Record stored in the RSU_j

pk_i	$H_1(VID_i, r_3)$	r_2	r_3	σ_{kk_i}

[Message Authentication] Once obtaining a KIS signing key, OBU_i can broadcast traffic information message in authenticated manner during the short-time period t_i by using the KIS signing key. The message format is shown in Table 3, and the authentication protocol is performed as follows.

Table 3. Message Format for Broadcasting

RID_j	msg	$\langle y_0, y' \rangle$	r_2	σ_{kk_i}	v_j

1. The sender OBU_i sets $u_i = Enc_{pk_{TMA}}(VID_i \| r_3)$ as OBU_i's pseudonym.
2. In addition, the sender OBU_i computes $w_i = g_1^{u_i}$ and $z_i = H_1(msg, \gamma_j, v_j, w_i, t_i)$, where t_i is the timestamps.
3. As a result, the sender OBU_i computes $\sigma_{kk_i} = u_i z_i + kk_i$ and sets the signature $\sigma_{kk_i, v_j} = \langle t_i, \sigma_i, z_i, v_j, \gamma_j \rangle$. Then the sender OBU_i broadcasts traffic information including the signature.
4. Upon receiving a signed message, each receiving OBU first checks the validity of the signature. To verify the validity of the σ_{kk_i, v_j}, the

receiver OBU_i computes $c_j = H_1(v_j)$ and checks $z_i = H_1(msg, \gamma_j, v_j, (g_1^{\sigma_i}(v_j^{c_j} y_0 y')^{-1})^{1/z_i}, t_i)$ by using RSU_i's KIS public key $\langle y_0, y' \rangle$. If $\sigma_{kk_i v_j}$ is verified as valid, the message can be accepted, otherwise discarded.

[Vehicle Tracing] In case of any disputed situation, an OBU_i reports the traffic information message to the MM in order to resolve the real identity of the sender for the dispute message.

Table 4. Message Format for Accusation

RID_j	msg	$Reasons$	$\langle y_0, y' \rangle$	r_2	$\sigma_{kk_i v_j}$

In the table 4, msg means the message causing dispute situation. Vehicle tracing is processed by extracting the real identity from the $\sigma_{kk_i v_j}$ according to the following procedure.

1. The MM computes $SK_{ID-RSU} = H_1(RID_j)^s$, $\gamma_j = H_1(SK_{ID-RSU} \| r_2), v_j = g_1^{\gamma_j}$, and $c_j = H_1(v_j)$ by the disputed message. Therefore, the MM can compute KIS signing key $kk_i = c_j \gamma_j + x_0 + x' \pmod q$. Moreover, the MM can derive both value kk_i and z_i, and finally can compute $u_i = \sigma_{kk_i} - kk_i / z_i$ since z_i is also included in $\sigma_{kk_i z_i}$.
2. Finally, the MM can obtain the real identity VID_i by decrypting $u_i = Dec_{sk_{MM}}(PID_i)$.

4. ANALYSIS

4.1 Security Analysis

We analyze how the proposed protocol satisfies the security requirements stated in Section 2.1.

- Authentication : Because we applied the key-insulated signature scheme[13] which was proven to secure against adaptive chosen message attack, an adversary cannot launch a forgery attack and an impersonation attack to an OBU.
- Anonymity : Since an OBU's real identities are encrypted by using pk_{MM} and encrypted ciphertexts are used as pseudonyms, a malicious attacker cannot disclose a real identity from pseudonyms in signatures without knowing sk_{MM}.
- Unlinkability : A wide eavesdropper cannot link the safety messages since most safety message consists of different pseudonyms. Even if RSUs are compromised, the malicious attacker does not obtain any information from the compromised RSUs since each OBU generates and transmits different pseudonyms to RSUs in signature generation.
- Traceability : In dispute cases, the MM can trace a real identity of OBU_i corresponding pseudonym PID_i by using its own private key sk_{MM}. Even if some RSUs are compromised, the MM is able to trace OBUs since the trace procedure in the proposed protocol is executed by the MM without cooperations with RSUs.

4.2 Performance Analysis

In this section, we compare the proposed protocol with Hao et al.'s protocol to show that our protocol is efficient in terms of message verification. For fairness in comparisons, we select a bilinear pairing of 80-bit security level as the same security measures of Hao et al.'s protocol; We assumed an MNT curve of embedding degree $k=6$, and $|q| = 160\ bits$ on Pentium IV 3.2 GHz[15] for implementing a group signature and a key-insulated signature scheme. We do not put restriction to any digital signature scheme in key issuing protocol, but we assume the ECDSA adopted by IEEE 1609.2 standard[16]. Table 5 and Table 6 show the measures to estimate and to compare our proposed protocol with Hao et al.'s protocol[5], respectively.

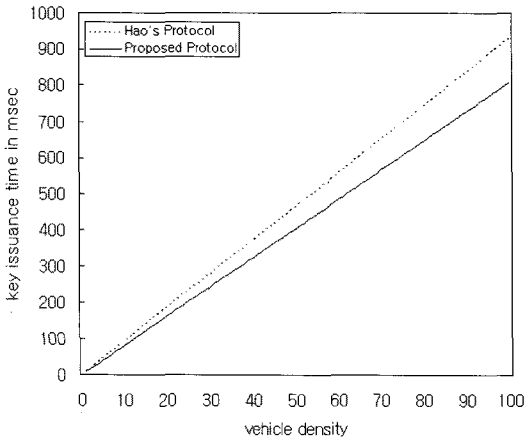


Fig. 3. Time for sign key issuance.

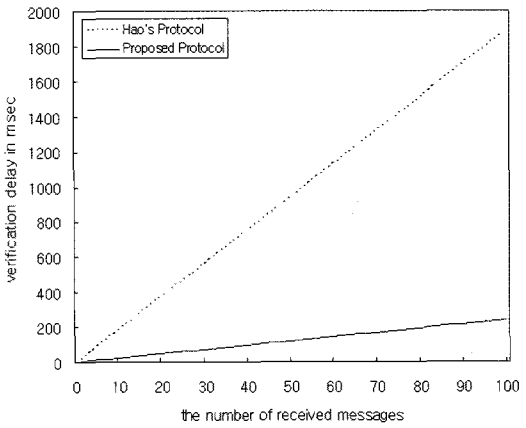


Fig. 4. Time for signature verification.

Table 5. Cryptographic operation time

Cryptographic operation time	Time(ms)
$\hat{e}$ Bilinear pairing operation	4.5
Point multiplication on G_1	0.6
ECDSA signature verification	1.2
Exponentiation on Z_q	2.1

Table 6. Protocol execution time

	Description	Hao et al.'s protocol	Proposed Protocol
$T_{\geq n}$	Time for signing key issuance protocol	9.3ms	8.1ms
T_{sig}	Time for signature verification	18.9ms	2.4ms

Table 7. NS-2 Simulation Parameters

Simulation area	13.5 Km × 12.3 Km
Simulation time	30 sec
Maximum OBU speed	60 Km/h
OBU transmission range	300 m
OBU information dissemination interval	300 $msec$

When we authenticate a safety message, it requires to verify the signature of the safety message. Therefore, the our protocol requires the time cost $T_{sig} = 2.4ms$, and that of Hao et al.'s protocol requires $T_{sig} = 18.9ms$. Figure 4 shows that our proposed protocol is more efficient than Hao et al.'s in the aspects of the signature verification cost. It is the reason that we considered KIS scheme for message verification, while Hao et al. applied group signature scheme.

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 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 numeri-

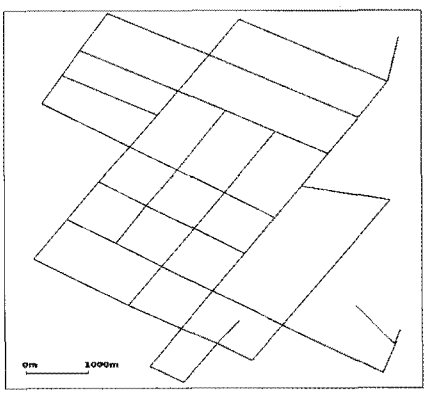
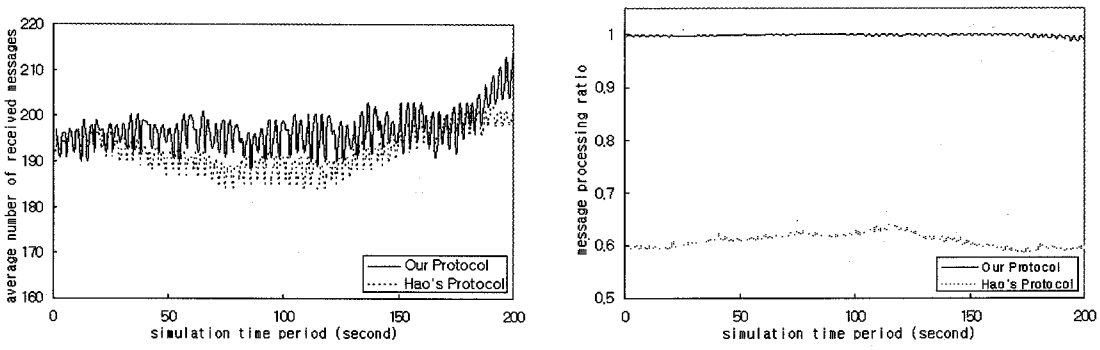


Fig. 5. A city street simulation scenario.



(a) average number of messages

(b) average message processing rate

Fig. 6. Average message processing rate of 900 vehicles for the received messages during 200 seconds simulation.

cally 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 ratio. Figure 6 shows these results. We used TraNS with ns2-2.34[17,18] and IEEE 802.11p parameters for ns2[19]. We put total 900 vehicles on a road of 13.5km×12.3km rectangular size. Each vehicle moves with a maximum speed of 16.7m/s (i.e., 60km/hr) and sends out a message every 300ms withn 300m nominal radio range. The simulation was run for 200 seconds and we measured the received messages every second[20-23].

From Figure 6, we can observe that our protocol and Hao et al.'s protocol received similar number of messages during the simulation, but our protocol shows about minimum 95% message processing rate while Hao et al.'s protocol processes about minimum 58% and maximum 65%, which is much less than our protocol. As a result, we can conclude that the proposed protocol is more practical.

5. CONCLUSION

In this paper, we have proposed an efficient anonymous authentication and vehicle tracing protocol based on pseudonym and a key-insulated signature scheme for secure vehicular communications on VANET. In our system model, on-the-fly short-time group signing key is issued by RSUs on OBU's request. By using the KIS scheme, we could implement a more efficient message verification protocol than Hao et al.'s protocol based on group signature scheme. We have demonstrated, through the performance evaluation, the proposed protocol has comparable performance to Hao et al.'s in terms of OBU's computational cost. As a result, our protocol can efficiently verify messages.

REFERENCES

[1] F. Dotzer, "Privacy issues in vehicular ad hoc networks," Proceedings of the Workshop on Privacy Enhancing Technologies 2005, LNCS 3856, pp.197-209, 2005.

[2] J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix Zones for Location Privacy in Vehicular Networks," WiN-ITS 2007, 2007.

[3] M. Gerlach and F.Guttler, "Privacy in VANETs using changing pseudonyms - ideal and real," VTC 2007, pp.2521-2525, 2007.

[4] J. P. Hubaux, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, Vol.2, pp. 49-55, 2004.

[5] Y. Hao, Y. Cheng, and K. Ren, "Distributed Key Management with protection Against RSU Compromise in Group Signature Based VANETs," IEEE GLOBECOM 2008, pp. 4951-4955, 2008.

[6] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," IEEE WCNC, Vol.2, pp.1187-1192, 2005.

[7] X. Lin, X. Sun, P.H. Ho and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications," *IEEE Transaction on Vehicular Technology*, Vol.56, No.6, pp. 3442-3456, 2007.

[8] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicle communications," IEEE INFOCOM 2008, pp.1229- 1237, 2008

[9] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, Vol.15, No.1, pp.39-68, 2007.

[10] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity based batch verification scheme for vehicular sensor networks," IEEE INFOCOM 2008, pp. 246-250, 2008.

[11] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," Proceedings of International workshop on Vehicular ad hoc networks (VANET), 2006.

[12] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," *Advances in Cryptology* - Eurocrypt 2002, LNCS 2332, pp. 65-82, 2002.

[13] G. Ohtake, G. Hanaoka, and K. Ogawa, "An efficient strong key-insulated signature scheme and its application," The 5th European PKI Workshop: Theory and Practice (EuroPKI2008), LNCS5057, pp.150-165, Springer, 2008.

[14] Y. Peng, Z. Abichar, and J. M. Chang, "Roadside-aided routing(RAR) in vehicular networks," IEEE ICC 2006, Vol.8, pp. 3602-3607, 2006.

[15] M. Scott, "Efficient Implementation of Cryptographic Pairings," ECRYPT Ph.D. Summer School on Cryptanalysis-Emerging Topics in Cryptographic Design and Cryptanalysis, 2007, Available : http://ecrypt-ss07.rhul.ac.kr/Slides/Thursday/mscott-samos07.pdf/.

[16] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International Journal of Information Security*, Vol.1, No.1, pp. 36-63, 2001.

[17] "The network simulator - ns-2." Available : http://nsnam.isi.edu/nsnam/index.php/User Information/.

[18] "Traffic and network simulation environment - TraNS." Available : http://trans.epfl.ch/.

[19] IEEE 802.11p parameters for NS2, Available : http://dsn.tm.uni-karlsruhe.de/Overhaul_NS-2.php/.

[20] "Dedicated Short Range Communications (DSRC)," Available : http://www.leearmstrong.com/dsrc/dsrchomeset.htm/.

[21] "SAFESPOT: Cooperative vehicles and road infrastructure for road safety," Available : http://www.safespot-eu.org/pages/page.php/.

[22] IEEE Standard 1609.2 - IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, July, 2006.

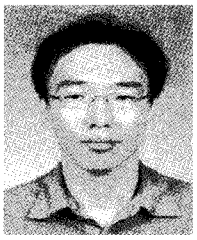
[23] U.S. Department of Transportation, "National highway traffic safety administration," Vehicle Safety Communications Project, Final Report, Appendix H: WAVE/DSRC Security, April 2006.

Young Shin Park

received the B.S. degree from Tongmyung University, Busan, Republic of Korea in 2009. He is currently the M.S. degree course student in the Department of Information Security of Pukyong National University. His research interests are in the areas of cryptographic algorithms, network security, and VANET.

Chae Duk Jung

received his Ph.D. and M.S. degrees in information security from Pukyong National University, Busan, Republic of Korea, in 2010 and 2007, respectively, and his B.S. degree from Dong-eui University, Busan, Republic of Korea in 2005. His research interests are in the areas of cryptographic algorithms, information security, VANET and PKI.



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 Department of IT Convergence and Application 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.