Journal of The Korea Institute of Information Security & Cryptology
VOL.24, NO.6, Dec. 2014
ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.6.1147

차량 네트워크에서 신원교환을 통해 프라이버시를 보호하는 방법*

후세인 라쉬드,[†] 오 희 국[‡]
한양대학교

Identity-Exchange based Privacy Preserving Mechanism in Vehicular Networks*

Rasheed Hussain,[†] Heekuck Oh[‡]
Hanyang University

요 약

차량과 통신기술의 발전으로 임시네트워크를 이용한 지능형 교통 시스템이 실현되었다. VANET은 지능형 교통 시스템의 한 예로써, 현재 배포단계를 눈앞에 두고 있다. 하지만 지능형 교통 시스템의 많은 장점에도 불구하고, 보안과 프라이버시 문제로 아직 대다수 차량에 설치되지 못하고 있다. 사용자들은 주변 차량이나 기반시설과의 통신을 위해 자신들의 프라이버시가 노출되는 것을 원치 않기 때문이다. 따라서 지능형 교통 시스템의 대중화를 위해 프라이버시 문제는 선결되어야 한다. 일반적인 임시네트워크나 VANET과 같은 특정 상황에서 프라이버시 문제를 해결하기 위한 여러 가지 기법들이 제안되었다. 대표적으로 다중 익명성을 이용한 기법이 있지만, 이를 비콘 메시지에 적용하더라도 공격자는 사용자를 특정 지을 수 있다. 따라서 임시네트워크에서 프라이버시를 보호하기 위한 새로운 기법이 필요하다. 본 논문에서는 VANET 환경에서 프라이버시를 조건부로 보장하는 신원교환 기법을 제안한다. 사용자는 자신의 가명을 이웃과 교환하고 메시지를 보낼 땐 이웃의 가명을 이용하여 보낸다. 제안하는 기법은 분쟁이 발생하는 경우 (권한이 있는) 기관이 메시지 송신자의 익명성을 철회할 수 있게 만듦으로써 프라이버시를 조건부로 제공한다.

ABSTRACT

Intelligent transportation system (ITS) is realized through a highly ephemeral network, i.e. vehicular ad hoc network (VANET) which is on its way towards the deployment stage, thanks to the advancements in the automobile and communication technologies. However, it has not been successful, at least to date, to install the technology in the mass of vehicles due to security and privacy challenges.

Besides, the users of such technology do not want to put their privacy at stake as a result of communication with peer vehicles or with the infrastructure. Therefore serious privacy measures should be taken before bringing this technology to the roads. To date, privacy issues in ephemeral networks in general and in VANET in particular, have been dealt with through

접수일(2014년 8월 8일), 수정일(2014년 10월 24일), 게재확정일(2014년 10월 24일)

* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학ICT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1015).

* 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학ICT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2014-H0301-14-1044).

* 이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2012R1A2A2A01046986).

* 이 논문은 2014년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2012R1A1A2009152).

† 주저자, rasheed@hanyang.ac.kr

‡ 교신저자, hkoh@hanyang.ac.kr(Corresponding author)

various approaches. So far, multiple pseudonymous approach is the most prominent approach. However, recently it has been found out that even multiple pseudonyms cannot protect the privacy of the user and profilation is still possible even if different pseudonym is used with every message. Therefore, another privacy-aware mechanism is essential in vehicular networks. In this paper, we propose a novel identity exchange mechanism to preserve conditional privacy of the users in VANET. Users exchange their pseudonyms with neighbors and then use neighbors' pseudonyms in their own messages. To this end, our proposed scheme conditionally preserves the privacy where the senders of the message can be revoked by the authorities in case of any dispute.

Keywords: VANET, VANET Clouds, Security, Conditional Privacy, Revocation, Route Tracing

I. Introduction

Over the last couple of decades, ample amount of research has been carried out in the field of ephemeral networks due to their rich set of applications. Ephemeral networks are short lived networks where the nodes come into contact for a relatively short amount of time. Mobile ad hoc networks (MANET) and its specialized breed vehicular ad hoc networks (VANET) are the famous examples of such networks and this paper focuses only on VANET. Researchers both from academia and industry have produced noteworthy results in the field of VANET [1-4]; however, ironically, VANET has not made it to the deployment stage so far. The reasons are several-fold: for instance, the upfront cost of the hardware and deployment is a nightmare for both governments and the service providers. They do not want their investment at stake before testing the waters for such promising yet unpredictable technology. On the other hand, security and privacy issues have been keeping the authorities and service providers at the bay from bringing this technology to the mass of vehicles.

Security and Privacy have been extensively studied and investigated in VANET from various angles. Both user and location privacy have been researched in a greater depth with promising results [5-8]. The reason for focusing on the privacy aspect of the security in VANET is to gain success among consumers. More precisely, VANET technology has to make sure that as a result of the use of this technology, users and their location privacy will not be violated. Therefore, the deployment of this technology will have huge economical and social impact on consumers.

The notion of privacy has been divided into two classes. Pure privacy is the term used for complete privacy where the trails cannot be traced back to the users in any circumstances. For instance, in VANET if a vehicle sends any message anonymously, then regardless of its originality, integrity, or credibility, it cannot be linked to the sender at any cost. Such level of privacy is questionable in VANET because it gives room to adversaries to penetrate and launch various kinds of attacks. In this paper, we only focus on the user privacy.

Among other approaches, temporary identities also known as pseudonyms somehow produced better results [7]. In this approach, the nodes use temporary identity for a specified amount of time and then change this identity either after regular or irregular intervals. However, the spatio-temporal information of pseudonym can lead the attacker to generate movement profiles. Therefore multiple pseudonyms are adapted and different pseudonyms are used with every message in order to mitigate the possibility of linkage to the user [8]. Recently it has been found out that even multiple pseudonyms are not much helpful in preserving users' privacy because they can still be linked to a particular user although without particular user information [9].

In the light of aforementioned privacy issues, we propose a new privacy preservation scheme which is based on a novel identity-exchange mechanism. The interested nodes exchange their temporary identities and then use the exchanged identity in their message, This way the message seems as if it was sent by the owner of that identity. Our privacy preserving mechanism is conditional where the identity of the immediate sender can be revoked by the revocation authorities in case of any dispute. The main contributions of this paper are given below:

1. We propose a traceable multiple pseudonyms approach to preserve the conditional privacy of the users.
2. Our proposed scheme is based on identity-exchange, where interested nodes exchange their identities with each other and use the other party's identity in their own message to preserve conditional privacy.
3. Our proposed scheme also guarantees revocation of the current user of the pseudonym in case of any dispute.

The rest of the paper is organized as follows. Section II outlines the state of the art regarding privacy preserving mechanisms in VANET and section III outlines the network and system model. We describe our proposed scheme in detail in section IV followed by evaluation in section V. In section VI, we give our concluding remarks.

II. State of the Art

In this section we outline the state of the art regarding privacy issues in VANET. In order to preserve privacy, to date, multiple pseudonymous strategy is adapted by the research community to preserve user and location privacy in VANET. As a result, an ample amount of research has been carried out based on multiple pseudonyms. In [7,8,10], authors put multiple pseudonyms into practice in order to preserve privacy whereas Ma et al. [11] discussed the refilling strategy for multiple pseudonyms-based schemes. Lu et al. [12] opted social spots for changing pseudonyms by the vehicles in order to preserve the privacy. Beresford et al. [13] proposed the concept of Mix Zone that is used as a hotspot for changing pseudonyms. Mix zone provides unlinkability among pseudonyms that are sent by the same vehicle. Whenever a vehicle passes through mix zone, it will have a chance to change its current pseudonym. Chaurasia et al. [14] proposed anonymity zone, a similar approach to mix zone where a vehicle needs to be silent for some fraction of time called silent period. Hussain et al. [15] proposed a conditional privacy preserving scheme through identityless beaconing mechanism. In their scheme, the vehicles broadcast beacon messages anonymously without any identity information.

Most of the work done on VANET privacy considers pseudonyms and their different variations. However, changing pseudonyms do not necessarily preserve the privacy. Recently, Wiedersheim et al. figured out that in multiple pseudonymous scenario, even if different pseudonym is used with every message; movement profiles could still be generated and the vehicles could be traced [9]. This led Eckhoff et al. [16] to propose an identity diffusion scheme where users swap their identities with neighbors using predefined time slots. However the time-dependent pseudonym swapping has an adverse effect on the privacy because the pseudonyms are bounded by the time window and the degree of anonymity depends upon the length of the time window.

Therefore for conditional privacy and anonymous communication, we proposes a new flexible identity-exchange mechanism, where the neighbors exchange identities among each other for privacy preservation. In case of any dispute, the revocation authorities can still trace back to the current user of the identity, if needed.

III. System Models

3.1 Network Model

Our VANET network model consists of two main entities from bird's view, managerial entities and the users. Managerial entities include department of motor vehicles (DMV) which is responsible for the initialization and registration of the on-board units (OBUs). The owners have to visit the DMV physically in order to get their OBU initialied and registered. Besides, there can be certification authorities as well but we only focus on the revocation authorities (RAs). Vehicular nodes are equipped with OBUs and tamper-resistant hardware. Every vehicle broadcasts beacon message for cooperative awareness according to dedicated short-range communication (DSRC) standard. They also exchange their pseudonyms after showing '*exchange interest*' in the beacons. However, the exchange history must be logged for the future revocation. One important requirement is that, a vehicle must not be able to frame other benign nodes and only the current user of the pseudonym must be subject to revocation.

3.2 System Initialization

We use ElGamal encryption algorithm [17] over the elliptic curve cryptography (ECC) [18] to encrypt K_{OBU} and K_{psu}. Let G be a cyclic group of prime order q where G is generated by P. DMV first chooses $s \in Z_q^*$ as its private key and computes $Pub = sP$ as its public key. DMV then uses threshold based secret sharing scheme [12] and divides s into k parts where k is the number of revocation authorities, each carries a share s_i and $s_i = (s_1, s_2, \ldots, s_k)$. In order to construct s from individual s_i, RAs must elect one of them to be group leader and construct s from the combination of individual s_i.

3.3 TRH Initalization

Only DMV has the authority to initialize and install OBU in the car and store the security paramters in it. Therefore, after confirming the credentials, DMV initializes the TRH and saves the system parameters including $\{G, q, P, Pub, \pi\}$, where $\pi = \{PS_1, PS_2, \ldots, PS_n\}$. DMV also saves vehicle's individual secret key K_{OBU} and pseudonym generation key K_{psu}.

3.4 Pseudonym Generation

DMV generates a pool of pseudonyms for each vehicle and saves it in the TRH. The pseudonyms are generated as follows:

$$PS_i = ((nonce)_{K_{psu}} \| (nonce \oplus VID)_{K_{OBU}} \| n_i)_{K_{DMV}^{-}}$$

nonce is the random number selected by DMV, n_i is the current count of the generated pseudonyms, and VID is the identity of the vehicle. DMV saves these pseudonyms in vehicle's TRH along with anonymous certificates, and sends the anonymous pseudonyms and certificates to RAs as well. DMV also indexes the stored pseudonyms with the value of n. For revocation purpose, TRH also encrypts K_{psu} and K_{OBU}, and sends the encrypted text to RAs which serves as a trapdoor for the revocation. Encryption of the aforementioned keys with the master public key of DMV is carried out as follows:

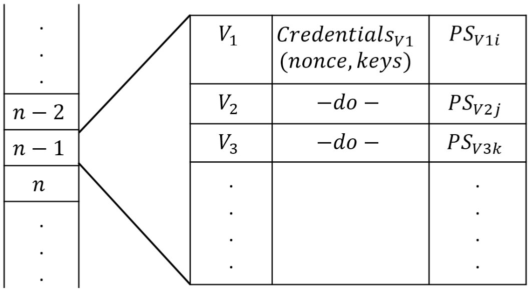
$$c_1 = rP,\ c_2 = (K_{psu} \| K_{OBU}) \oplus H(rPub)$$

r is a random number selected by TRH for the encryption. TRH sends (c_1, c_2) to DMV and RAs. However RAs can only decrypt the cipher text through colluding. When RAs agree to decrypt the cipher text, they collude and construct s from individual s_i. This way the RAs can get K_{psu} and K_{OBU}. Additionally DMV also sends hashed credentials including K_{psu} and K_{OBU} along with the pseudonyms to RAs which are in turn used to revoke the identity. Moreover DMV also maintains a database where it saves the credentials of the vehicle ($VID, nonce$).

IV. Proposed Identity-Exchange Scheme

4.1 Baseline

In VANET, every vehicle broadcasts beacon with certain frequency. Before starting communications, the vehicles must have received their pool of pseudonyms from DMV. DMV and RAs also save the pseudonyms in the form of pseudonyms table as shown in Fig. 1a and Fig. 1b respectively. Vehicles during the course of V2V communication may show their intention to exchange their identity(s) with other nodes. After successful exchange of identities with neighbors based on the intentions, they send the exchange history to the authorities. After that the vehicles communicate with each other through the exchanged identities. Whenever there is a dispute among the vehicles, they take it to the revocation authorities, where the culprits are revoked.



V_1	$Credentials_{V1}$ $(nonce, keys)$	PS_{V1i}
V_2	$-do-$	PS_{V2j}
V_3	$-do-$	PS_{V3k}

Fig.1(a). Pseudonym Table at DMV

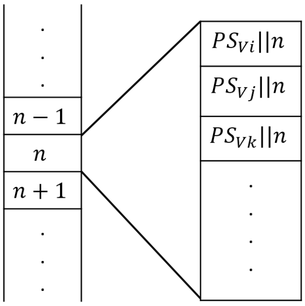


Fig. 1(b). Pseudonym Table at RAs

4.2 Pseudonym Exchange

Since multiple pseudonyms are enough to protect the privacy of the users, therefore it is essential to come up with another mechanism that not only protects the user privacy, but also enables authorities to revoke the culprits whenever needed.

According to DSRC standard, every vehicle in VANET broadcasts beacons with certain frequency defined by the standard. These beacons contain whereabouts information that includes current location, current speed, heading, and so forth. Vehicles that are interested in exchanging their pseudonyms, include their '*intent*' in their beacon message to exchange pseudonym(s) with the neighbors. Among the neighbors whoever has a mutual interest to exchange pseudonyms, replies with an '*intent-reply*' flag in the next scheduled beacon.

When a vehicle wants to exchange its pseudonym for privacy preservation, it shows its intention in its beacon messages. However, the neighbors who receive the beacon with intent flag set, have choice if they want their pseudonyms to be exchanged.

The generic beacon denoted by M_b is given by:

$$M_b = (B_{data} \| Sec.Parameters \| intent)$$

B_{data} is the beacon data that includes whereabouts information, $Sec.Paramters$ are the security parameters used for authentication, privacy, and non-repudiation, and $intent$ is the interest of the vehicle for exchanging pseudonym. The requirements that must be fulfilled prior to pseudonym exchange are anonymous mutual authentication of the exchanging entities, no-repudiation, privacy preservation, pseudonym validity, and verification. Kim et al.'s scheme is the most suitable scheme for pseudonym exchange in our proposed scheme [19]. We assume their scheme to be used in our pseudonym exchange process. Their scheme fulfills all aforementioned security primitives. It is worth noting that before exchanging pseudonyms, vehicles periodically receive pseudonym revocation list (PRL) from RSUs and check for the pseudonym validity beforehand.

Time	Source Pseudonym	Pseudonym Changed For:
t_i	PS_{Vx^i}	PS_{Vy^i}

Fig. 2. PEHT-Pseudonym exchange history table

After the exchange takes place, the report about the exchanged pseudonyms is sent to RAs anonymously. RAs maintain another database for the exchange history referred to as pseudonym exchange history table (PEHT) which contains time of the exchange, the source pseudonym and the destination pseudonym. This exchange information is used for revocation purpose which is explained in the next subsection in detail. The format of PEHT maintained by RAs is shown in Fig. 2.

4.3 Revocation

In order for RAs to revoke a user, RAs retrieve the beacons in questions from the storage. The storage can be anywhere, the details of which are out of the scope of this paper. When queried based on a time interval, the beacons storage entity provides RAs with the data related to the time interval provided in the query. After that RAs have to look into the n values of the message to figure out which pseudonym was used. RAs search the pseudonym related to value n and then searches the pseudonym exchange history table (PEHT) to figure out whether the pseudonym have been used by its original owner or exchanged with another user. PEHT will let the RAs know who to follow up. It is worth noting that there will be an incentives mechanism in place which will stimulate the pseudonym exchange report after the exchange takes place. After searching PEHT based on recent time value, RAs collude and construct s from individual s_i related to the pseudonym in question and the session leader decrypts the keys from cipher text (c_1,c_2) as follows:

$$PS_i = c_2 \oplus H(sc_1)$$
$$PS_i = (K_{psu} \| K_{OBU}) \oplus H(rPub) \oplus H(rsPub)$$

When RAs decrypt the keys K_{psu} and K_{OBU}, then RAs have to decrypt the *nonce* and extract VID from the pseudonym. It is worth noting that the PEHT is most critical module in our proposed scheme, because in case of a complex scenario, for instance a vehicle may exchange somebody else's pseudonym. In such case, the current node that used the pseudonym must be revoked, not the original owner of the pseudonym. This scenario could grow larger up to several levels where the originator and the user of the pseudonyms must be taken care of. To counter the complexity, we search the PEHT backwards with respect to time and take into account, only the latest best match with the suspected pseudonym. This way the current user of pseudonym in question is revoked.

V. Analysis and Evaluation

In this section we analyze and evaluate our proposed scheme from security, privacy, and communication cost standpoint.

Time	Time	Source Pseudonym	Changed For:
↓	t_1	PS_{A2}	PS_{B3}
	t_2	PS_{B4}	PS_{A1}
	t_3	PS_{A2}	PS_{C4}
	t_4	PS_{C4}	PS_{B2}

Fig. 3. PEHT example scenario

5.1 Security Analysis

The security requirements for our proposed pseudonym based scheme is dependent on both beacons security and the communication security while exchanging pseudonyms. The pseudonyms itself are secure as long as keys K_{psu} and K_{OBU} are not compromised. The compromise of these keys will have dire consequences. Since these keys have been used in pseudonym generation, the compromise of these keys (together) will let the adversary to not only find the original owner of the pseudonym, but also adversary can inject bogus information during the future communication where the aforementioned keys will be used.

Secondly, the security requirements for the pseudonym exchanged has already been outlined in the previous section and we assumed Kim et al.'s [19] scheme for the pseudonym exchange. The aforementioned scheme guarantees mutual authentication and other security requirements for the safe exchange of the pseudonyms, thereby it can be assumed that unless and until the security primitives have been compromised, it will be hard for adversary to gain valuable information from the pseudonym exchange process.

5.2 Privacy Preservation

Our proposed scheme guarantees privacy in the form of confusion for the adversaries, because with the help of pseudonym exchange at time t_i, let say PS_j is used by a vehicle V_k, but at time t_{i+1}, the same pseudonym PS_j will be used by another vehicle V_l. Therefore there are greater chances of false positive or true negative for the adversaries.

The pseudonyms also preserve privacy of the users because the pseudonyms are anonymous. VID is embedded in the pseudonyms as a trapdoor for revocation purpose. The pseudonym is the encrypted value with the two keys and signed by DMV. The pseudonym itself does not reveal the identity of the owner. Moreover in our case, it is also not sure, whether the pseudonym is the sender's own or exchanged with somebody else.

Theorem 1: *In the proposed scheme, RAs single out the immediate user of the pseudonym rather than the owner of the pseudonym.*

Proof: Let suppose, there are 4 cars A, B, C, and D. The cars have pseudonym sets $\{PS_{A1}, PS_{A2}, \ldots, PS_{An}\}$, $\{PS_{B1}, PS_{B2}, \ldots, PS_{Bn}\}$, $\{PS_{C1}, PS_{C2}, \ldots, PS_{Cn}\}$, and $\{PS_{D1}, PS_{D2}, \ldots, PS_{Dn}\}$. The pseudonym exchange that took place among these 4 nodes (according to Fig. 2), is shown in Fig. 3.

It can be seen in the table that at time t_1, A received PS_{B3} from B for an exchange of PS_{A2}. That means vehicle A is using PS_{B3}. If a message with PS_{B3} is under observation at time t_1, then vehicle A must be held responsible for that, not vehicle B. However, at time t_3, vehicle B exchanges PS_{A2} (originally owned by vehicle A) with C's pseudonym PS_{C4}. At this point in time if the message under observation after t_3 contains PS_{A2}, vehicle C must be held responsible. Hence the current sender of the pseudonym is traced by RAs. □

Theorem 2: *If the pseudonym exchange history is sound, then any culprit node will not get away with its malicious behavior.*

Proof: On the basis of assumption that the pseudonym exchange history is intact, if there is any malicious activity experienced by the node while either sending beacons or reporting message with a designated pseudonym PS_{yi} (i-th pseudonym of node y) will be used along with that message. Now there are two possibilities, the pseudonym may belong to the sender or it may have exchanged it with somebody else in the neighborhood. In the former case, searching PEHT will give zero hit for the RAs and RAs will revoke the identity in the pseudonym according to the revocation mechanism, in the latter case, PEHT will give the hit on the exchanging node, and thus RAs will revoke the original sender. □

5.3 Communication Overhead

We take into account the revocation overhead incurred by our proposed scheme. The cost of revocation is divided into two scenarios depending upon the usage of pseudonyms, i.e. direct and indirect revocation. In case of direct revocation, the cost denoted by $T_{dir-rev}$ is given by:

$$\begin{aligned} T_{dir-rev} &= S.T_{pseu} + S.T_{PEHT} + Ext(K_{psu}, K_{OBU}) \\ &\quad + Sym.Decryp \\ T_{dir-rev} &= 2T_{\epsilon} + 2T_{\mu l} + 2T_H + 2T_{sym-dec} \end{aligned}$$

$S.T_{pseu}$ is the time required for the search table operation for pseudonyms and the PEHT denoted by T_{ϵ}, Ext represents the cost incurred by the extraction cost of the keys, denoted by $(2T_{\mu l}+2T_H)$ and followed by the symmetric decryption denoted by $2T_{sym-dec}$.

Whereas in case of indirect revocation, RA has to examine all the current holders of the pseudonym in question that was used simultaneously. The revocation in such case consists of two steps: single out the nodes that possessed and used the pseudonym and then compare their trapdoor value sent in the beacons, which can be the hashed MAC value calculated with K_{OBU} with the pseudonym in question.

VI. Conclusion

In this paper we proposed a novel identity-exchange based mechanism to conditionally preserve the privacy of the users in vehicular ad hoc network (VANET). VANET is a highly ephemeral network where the vehicles have intermittent connection with each other. Vehicles have a pool of pseudonyms stored inside OBU and during communication, they exchange their pseudonym(s) with the neighbors and use neighbors' pseudonym for their communication. This way the privacy is preserved and the anonymity is increased. Moreover, in order to deal with the liability issues, we also proposed a revocation mechanism, where the messages can be traced back to immediate senders rather the owners of the pseudonyms. Our proposed scheme is secure, privacy-preserving and lightweight.

References

〔1〕 U. Lee, R. Cheung and M. Gerla, "Emerging Vehicular Applications," Vehicular Networks: from theory to practice, S. Olariu and M. C. Weigle, eds., BocaRaton, FL: Taylor and Francis, pp. 1-30, 2009.

〔2〕 M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal of Computer Security, vol. 15, pp. 39-68, 2007.

〔3〕 F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T. Ta-Vinh, G. Calandriello, A. Held, A. Kung, and J. P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," Communications Magazine, IEEE, vol. 46, pp. 110-118, 2008.

〔4〕 X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in Vehicular Ad Hoc Networks," IEEE Communications Magazine, vol. 46, no. 4, pp. 88-95, 2008.

〔5〕 J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, 2010.

〔6〕 R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in Proc. IEEE International Conference on Computer Communications (INFOCOM), pp. 1229-1237, 2008.

〔7〕 Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, 2010.

〔8〕 D. Huang, S. Misra, M. Verma, G. Xue, "PACP: An Efficient Pseudonymous

Authentication-Based Conditional Privacy Protocol for VANETs," Intelligent Transportation Systems, IEEE Transactions on, vol.12, no.3, pp.736,746, Sept. 2011.

〔9〕 B. Wiedersheim, Z. Ma, F. Kargl, P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on, pp.176,183, Feb. 2010.

〔10〕 E. Fonseca, A. Estag, R. Baldessari, R. L. Aguiar, "Support of Anonymity in VANETs - Putting Pseudonymity into Practice," Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE, pp.3400,3405, 11-15 March 2007.

〔11〕 Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications," in Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th. IEEE, pp. 1–5, 2008.

〔12〕 R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," Vehicular Technology, IEEE Transactions on, vol. 61, no. 1, pp. 86–96, 2012.

〔13〕 A. R. Beresford and F. Stajano, "Mix zones: User privacy in location aware services," in Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, pp. 127–131, 2004.

〔14〕 B. K. Chaurasia and S. Verma, "Maximizing anonymity of a vehicle through pseudonym updation," in Proceedings of the 4th Annual International Conference on Wireless Internet. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), p. 83, 2008.

〔15〕 R. Hussain, S. Kim, and H. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET," in Information Security Applications, Y. Heung Youl and Y. Moti, Eds., ed: Springer-Verlag, pp. 268-280, 2009.

〔16〕 D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in vanets: Identity diffusion using timeslots and swapping," in Vehicular Networking Conference (VNC), 2010 IEEE. IEEE, pp. 174–181, 2010.

〔17〕 T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," Information Theory, IEEE Transactions on, vol. 31, no. 4, pp. 469–472, 1985.

〔18〕 V. S. Miller, "Use of elliptic curves in cryptography," in Advances in Cryptology CRYPTO'85 Proceedings. Springer, pp. 417–426, 1986.

〔19〕 D. Kim, J. Choi, and S. Jung, "Mutual identification and key exchange scheme in secure vanets based on group signature," in Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE. pp. 1–2, 2010.

〈저자소개〉

후세인 라쉬드 (Rasheed Hussain) 학생회원
2007년 5월: NWFP University of Engineering and Technology, Peshawar, Pakistan 학사
2010년 8월: 한양대학교 컴퓨터공학과 석사
2011년 9월~현재: 한양대학교 컴퓨터공학과 박사과정
〈관심분야〉 정보보호, VANET, Cloud computing, VANET-Cloud

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과 학사
1989년: 아이오와주립대학 전자계산학과 석사
1992년: 아이오와주립대학 전자계산학과 박사
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안