http://dx.doi.org/10.21172/ijiet.123.08

# PPAS: A Privacy Preservation Authentication Scheme for Vehicular Communication Networks

Ming-Chin Chuang[1], Chao-Lin Chen[2]
[1]*Department of CSIE, China University of Technology, Taipei, Taiwan, R.O.C.*
[2]*Smart System Institute, Institute for Information Industry, Taipei, Taiwan, R.O.C.*

**Abstract- Security issues related to vehicular ad hoc networks (VANETs) have attracted a great deal of attention recently. In this paper, we propose a privacy preservation authentication scheme (PPAS) for vehicle-to-infrastructure (V2I) communication environments. PPAS has low computation costs since we only use symmetric cryptography, an XOR operation, and a hash function to resolve the high computation problem of the public key infrastructure (PKI). The authentication process of PPAS is performed locally without returning to the trust authority (TA) to reduce the authentication latency. Moreover, PPAS satisfies the following security requirements: anonymity, location untraceability, mutual authentication to prevent server spoofing attack, stolen-verified attack resistance, replay attack resistance, and session key agreement.**
**Keywords – VANET, Security, Anonymity, Authentication**

## I. INTRODUCTION

With the rapid development of wireless technologies, vehicular ad hoc networks (VANETs) have become increasingly popular. The main components of VANETs are the wireless on-board unit (OBU) and the roadside unit (RSU). OBUs are installed in vehicles to provide wireless communication capability, while RSUs are deployed throughout the roadside as the infrastructure to provide information or access to the Internet for vehicles within their radio coverage. In the IEEE 802.11p task group, the Dedicated Short Range Communications (DSRC) [1] supports two kinds of communication environments: vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. The trust authority (TA) is responsible for the authentication procedure in VANETs.

A number of studies [2] [3] have focused on the problem of data dissemination in VANETs. However, in recent years, the security issues, especially in the privacy aspect, have attracted increasing attention from both industry and academia [4]. For example, to ensure user anonymity, a basic solution is to use a temporary identity or alias for a mobile user instead of his real identity. However, this solution cannot satisfy the required privacy requirement because since an adversary can still track the trajectory of a vehicle by collecting multiple messages [5]. Consequently, many related studies have focused on security and privacy preservation in VANETs [6]-[11]. To achieve both message authentication and ensure anonymity, Raya et al. [6] pre-load each vehicle with a large number of anonymous public and private key pairs, as well as the corresponding public key certificates, each of which contains a pseudo identity. Traffic messages are signed with a public key-based scheme, and each pair of public and private key has a short lifetime to preserve its privacy. However, the approach works with high computation cost, high storage cost, and high communication overhead. Zhang et al. [7] proposed a batch signature verification scheme to protect users' privacy in V2I communications; while Freudiger et al. [8] and Sampigethava et al. [9] proposed schemes that protect location privacy. However, all schemes in [7] [8] [9] do not consider the resultant communication overhead. Lu et al. [10] introduced an efficient conditional privacy preservation (ECPP) protocol for VANETs and defined three levels of user privacy, which are required to achieve authentication, anonymity, and untraceability. Under ECPP, RSUs are responsible for issuing temporary public key certificates to vehicles. But the packet length of ECPP is dramatically increased due to the signatures and public key certificates attached to each message. Zhang et al. [11] proposed an RSU-aided messages authentication scheme (RAISE), which uses the symmetric key hash message authentication code (HMAC), instead of a public key infrastructure (PKI) based message signature, to reduce the signature cost. However, in RAISE, the authentication scheme and key agreement process also use asymmetric cryptography, which leads to a high computation cost. As mentioned above, although the PKI can be used to prevent the attacks, it incurs a huge computation cost and communication overhead for most OBUs. Thus, to design a security and privacy preservation authentication scheme in VANET remains a major challenge.

In this paper, we focus on the anonymous authentication for the V2I communication in VANETs. We propose a privacy preservation authentication scheme (PPAS) to reduce the computation cost and provide better security in VANETs. PPAS has the following characteristics. (1) The computational cost is low, since it only uses symmetric

cryptography, an XOR operation, and a hash function to resolve the high computation problem of PKI. (2) The authentication process of PPAS is performed locally without returning to the trust authority (TA) to reduce the authentication latency. (3) The authentication scheme fulfills the following security requirements for an authentication scheme: anonymity, location untraceability, mutual authentication to prevent server spoofing attacks, stolen-verified attack resistance, replay attack resistance, and session key agreement.
The remainder of this paper is organized as follows. Section II introduces some preliminaries. In Section III, we describe PPAS in detail. An analysis of the security and computation costs is presented in Section IV. Then, in Section V, we summarize our conclusions and consider future research avenues.

## II. PRELIMINARIES

### *2.1 Attack Models*

The following possible attack models can be used during the authentication procedure.
Message replay attack: The adversary resends valid messages sent previously in order to disturb the traffic flow.
Movement tracking: Since wireless communication is based on a shared medium, an adversary can easily eavesdrop on any traffic. After intercepting a significant number of messages in a certain region, the adversary could trace the physical position and movement patterns of a vehicle by simply analyzing the information.
Impersonation attack: The adversary pretends to be a valid OBU or even the RSU/TA to cheat the OBUs.
Server stolen-verified attack: If the authentication server stores the verification table, the authentication scheme will be vulnerable to a stolen-verifier attack. A intruder can forge a valid identity after the intruder somehow succeeds in stealing the stored verifier.

### *2.2 Security Requirements*

Since an authentication scheme is susceptible to be attacked by adversaries, our objective is to design a scheme that is robust to such attacks. Based on related studies [6]-[11], we define the following key requirements for securing VANETs.
Identity anonymity: Anonymous authentication involves verifying that an OBU is legitimate without knowing the real identity of the OBU.
Location untraceability: The vehicle has a dynamic identity to prevent an adversary from tracking it when the OBU performs the authentication procedure.
Mutual authentication: A mutual authentication process is needed. The RSU needs to verify that the OBU is a legal user, and the OBU needs to ensure that the RSU is not a forgery.
Efficiency: The computation and communication costs on vehicles must be as low as possible.

## III. PRIVACY PRESERVATION AUTHENTICATION SCHEME (PPAS)

In this section, we describe the privacy preservation authentication scheme (PPAS) for VANETs in V2I communication environments. The preliminary version of this work was published in IEEE CECNET 2011 [14] and it only discusses the authentication process. However, in this paper, we describe the proposed scheme in detail. We review more related work and compare them. Moreover, we add more simulations to evaluate the performance of PPAS. The main operations of PPAS include the initial registration and the authentication procedures. Before the vehicles join a vehicular ad hoc network, every OBU must register with the TA. When the OBU joins a VANET or wants to access the Internet via an RSU, it has to perform the authentication procedure.

### *3.1 Initial Registration Procedure*

Before an OBU joins a vehicular ad hoc network, it needs to perform the initial registration procedure, which is executed via a secure channel, as shown in Fig. 1. The steps of the procedure are as follows.
OBU➔TA: The OBU sends its chosen public identification (i.e., IDOBU) to the TA. (Note that, in VANETs, IDOBU is a unique identification.)
Let sv denote a secret value of the TA, IDRSU denote the public identification of RSU, IDTA denote the public identification of TA, EK(M) denote the encrypted message M using key K with symmetric cryptography, h( ) denote a public one-way hash function, and "||" denote the combination of strings. After receiving the identification, the TA computes the values x, y, z, and k, as shown in step 2 of Fig. 1, We assume that GK denotes a group key pre-shared among RSUs and the TA.
TA➔OBU: TA stores the parameters (i.e., IDTA, x, y, z, k, h( )) in the OBU via an IC or smart card.

Note that, under this procedure, the TA does not need to store the verification information (e.g., user's password) about the OBU. Therefore, we can avoid the possibility of a stolen-verified attack. In addition, the registered OBU

cannot fabricate a valid user successfully when the OBU obtains these parameters (i.e., IDTA, x, y, z, k, h( )). This is because the OBU does not know the secret value of the TA (i.e., sv).

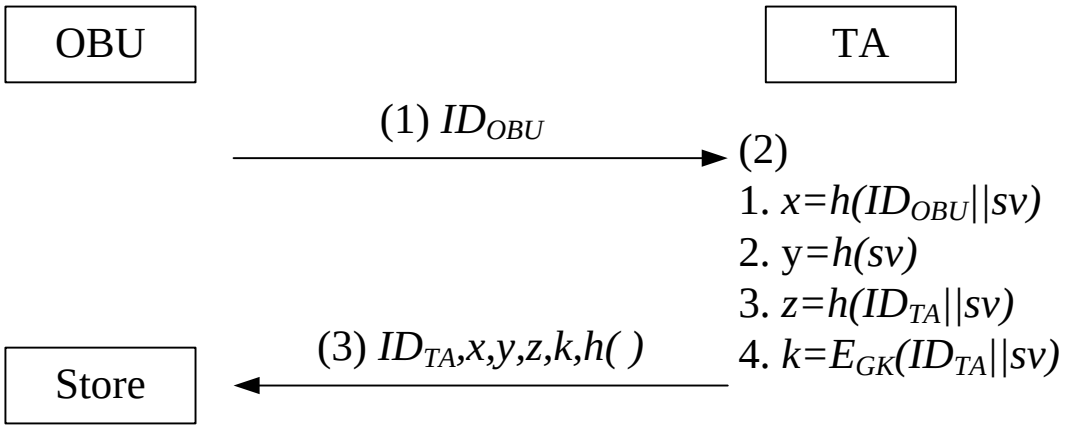


Figure 1. The initial registration procedure

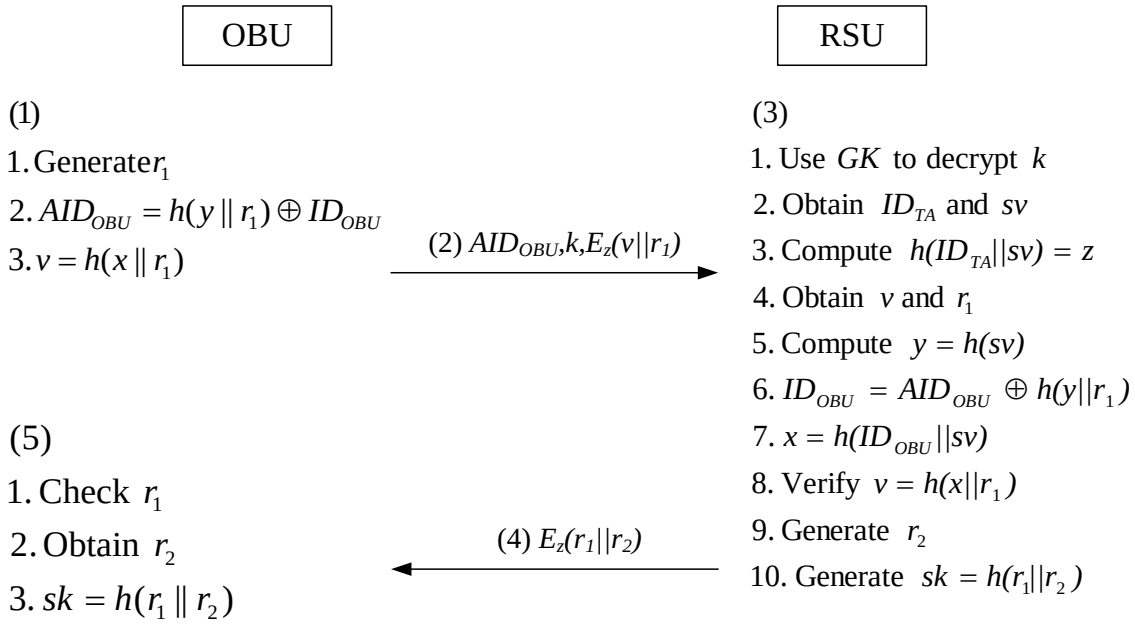


Figure 2. The authentication procedure

*3.2 Authentication Procedure*

When a vehicle joins a VANET, it performs the authentication procedure via an RSU. Our scheme belongs to a local authentication mechanism whereby authentication can be performed locally (i.e., by an RSU without involving the TA in this authentication). The steps of the authentication procedure are listed below and presented diagrammatically in Fig. 2.

The OBU generates a random number r1, computes the alias AIDOBU as h(y||r1) $\oplus$ IDOBU, and generates the authentication vector v as h(x||r1), where x and y are obtained from the initial registration procedure. OBU formats the authentication information as AIDOBU,k,Ez(v||r1). The OBU always uses differently alias to authenticate because the generation of alias is based on a random number r1.

OBU➔RSU: The OBU sends the authentication request to the RSU.

The RSU verifies the OBU: On receipt of the authentication request (i.e., AIDOBU,k,Ez(v||r1)), the RSU uses a group key GK to decrypt k (i.e., EGK(IDTA||sv)) and then obtains IDTA and sv. However, GK cannot decrypt k successfully if the authentication request has been modified since the modified authentication request would have

the wrong value of k. Next the RSU computes the value of z by hashing IDTA and sv and decrypts Ez(v||r1) to obtain v and r1. Then it computes the value of y (i.e., h(sv)), the original identification of OBU as AIDOBU⊕h(y||r1) and the value of x as h(IDTA||sv). Finally, it can verify the value of the authentication vector v. If the value of v calculated as h(x||r1) is equal to that of decrypting Ez(v||r1), the OBU is valid and the RSU generates a random number r2 and a session key sk as h(r1||r2); otherwise, the RSU rejects the authentication request. Thus, even an adversary can intercept a number of messages during a certain period, but it still cannot obtain the real identification of the OBU. However, the RSU or the TA is capable of computing the real identification of the OBU to authenticate. RSU➔OBU: The RSU sends back the authentication reply message (i.e., Ez(r1||r2)) to the OBU. The OBU verifies the RSU: The OBU receives the authentication reply message and verifies the legitimacy of the RSU. After using z to decrypt the encrypted message to obtain r1 and r2, the OBU checks the value of r1. Then, it uses the random number r2 to generate the session key sk with the RSU.

## IV. ANALYSIS

### *4.1 Security Analysis*

In this subsection, we analyze the security of the proposed PPAS in terms of the following factors: anonymity, location untraceability, stolen-verified attack resistance, mutual authentication, replay attack resistance, and session key agreement.

Anonymity: Under the proposed scheme, the original identity of an OBU is converted into an alias that is based on a random number. Therefore, an adversary cannot determine the original identity of the OBU without knowing the random number chosen by OBU.

Stolen-verified attack resistance: In the authentication procedure, the TA and the RSU do not need to store the verification table. Therefore, even if an adversary manages to access the database of the TA or the RSU, he still cannot obtain the authentication information of OBUs.

Location untraceability: Even an adversary can intercept a number of messages during a certain period, he cannot trace a vehicle's physical position because our anonymity mechanism is a dynamic identification process, and generation of the session key is based on a random number. Therefore, PPAS is robust against movement tracking attack.

Mutual authentication to prevent server spoofing attacks: The RSU authenticates the OBU in step 3, and the OBU authenticates the RSU in step 5 of the authentication procedure. Thus, this mutual authentication scheme prevents server spoofing attack completely.

Resistance to replay attacks: To protect the OBU from replay attacks, we add a random number to the message. Hence, if an adversary intercepts the authentication message and tried to impersonate the valid OBU by immediately replaying the message, the RSU or OBU would obviously reject the request because the random number in the replayed messages would be invalid.

Session key agreement: In the V2I communication environment, we only use one round trip between the OBU and the RSU to generate the session key. Then, we can use the key to encrypt the following packets to ensure the communications are confidential.

### *4.2 Analysis of the Computation Cost*

In the analysis of the computational cost, we use the following notations: "-" means there is no computational cost in that phase; n: the number of OBUs in the VANETs; Ch: the cost of executing the one-way hash function; CXOR: the cost of executing the XOR operation; Csym: the cost of computing a symmetric encryption or decryption; and Cran: the cost of generating a random number. The computational cost of PPAS is shown in Table I. PPAS is efficient in computation cost because it is only based on symmetric cryptography, an XOR operation, and a hash function without PKI cryptography1.

Table I. Computational cost of the proposed scheme

| | OBU | RSU | TA |
|---|---|---|---|
| Initial registration procedure | - | - | n(3Ch+Csym) |
| Authentication procedure | 3Ch+2Csym+Cran +CXOR | 6Ch+2Csym+Cran+CXOR | - |

[1] The computation cost of PKI is 10 to 100 times that of symmetric cryptography and the hash function

*4.3 Advantages of Local Authentication*

The authentication process of PPAS is performed locally without returning to the TA. The property of local authentication has three advantages: it reduces the authentication latency, reduces the signaling cost, and provides a fault tolerant mechanism.

Low authentication latency (AL): Our PPAS authentication scheme has the property of local authentication because the TA and RSU pre-share some common secret information (e.g., the group key GK) to facilitate authentication. Consequently, the authentication procedure can be executed by an RSU without returning to the TA. The authentication latency of the local and normal authentication schemes can be represented as follows.

$$\begin{cases} AL_{Local} = 2D_{OBU-RSU} \\ AL_{Normal} = 2D_{OBU-TA} = 2D_{OBU-RSU} + 2D_{RSU-TA} \end{cases} \quad (1)$$

where DOBU-RSU, DOBU-TA and DRSU-TA are the average transmission delay between the OBU and the RSU, the OBU and the TA, and the RSU and the TA, respectively. Fig. 3 shows the differences in authentication latency between local and normal authentication schemes. We observe that the latency of the normal scheme increases sharply as the distance between the RSU and the TA increases.

Low signaling cost (SC): The signaling costs are defined the entire amount of authentication messages in VANETs. Morales-Andres and Villen-Altamirano [12] developed the fluid flow mobility model where the direction of an MN's movement is uniformly distributed in the range of $(0,2\pi)$. This mobility model is suitable for mobile users with high mobility, infrequent speed, and direction transformations. Suppose $\lambda$ is the number of RSU crossing. Then, we can calculate the value of $\lambda$ as follows:

$$\lambda = \left\lfloor \frac{2v}{\sqrt{\pi}R} \right\rfloor \quad (2)$$

where v is the average speed of the MN and R is the transmission range of RSU. In Eq. (2), all subnets have the same circular shape and size.

Then, the signaling cost of local authentication and normal authentication schemes can be expressed as below:

$$\begin{cases} SC_{Local} = SC_{Local}^{first} + SC_{Local}^{cross} = (2+2\lambda) \cdot AUTH \cdot SC_{OBU-RSU} \\ SC_{Normal} = SC_{Normal}^{first} + SC_{Normal}^{cross} = (2+2\lambda) \cdot AUTH \cdot \left(SC_{OBU-RSU} + SC_{RSU-TA}\right) \end{cases} \quad (3)$$

where $SC_{Local}^{first}$ and $SC_{Normal}^{first}$ are the initial authentication signaling costs of local and normal authentication schemes, respectively when the MN first enters to a new VANET. $SC_{Local}^{cross}$ and $SC_{Normal}^{cross}$ are the authentication costs occurred by the MN crossing the RSU in the same VANET. AUTH denotes the proportion of authentication packet size which is related to the length of encryption key. Let SCOBU-RSU and SCRSU-TA be the signaling cost between the OBU and the RSU, and RSU and the TA respectively.

We present the total cost as a function of session to mobility ratio (SMR). The SMR is the ratio of the session arrival rate to the mobility rate [13]. In the fluid flow mode, the SMR is defined as $\frac{S}{\lambda}$, where S is the session arrive rate. We vary $\lambda$ from 5 to 25 with S fixed at 1, which yields the SMR of 0.2 to 0.04. When the SMR indicates low value, the mobility rate is relatively higher than the session arrival rate. Fig. 4 shows the effect of SMR on the total signaling cost. We can see that the local authentication scheme reduces a lot of signaling costs when the SMR decreases.

In terms of fault tolerance, if the TA crashes, the authentication procedure can still work because every RSU can perform the authentication procedure.

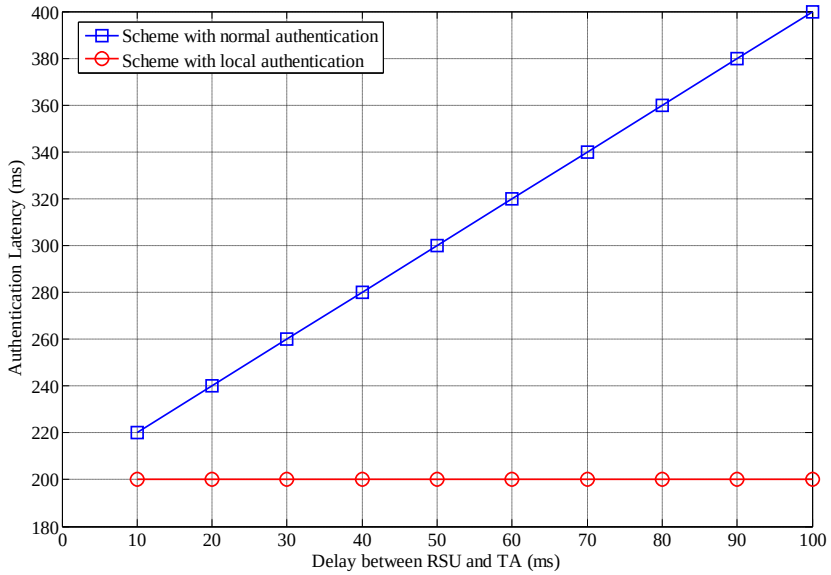


Figure 3. Authentication latency of local and normal authentication schemes (DOBU-RSU=100ms)

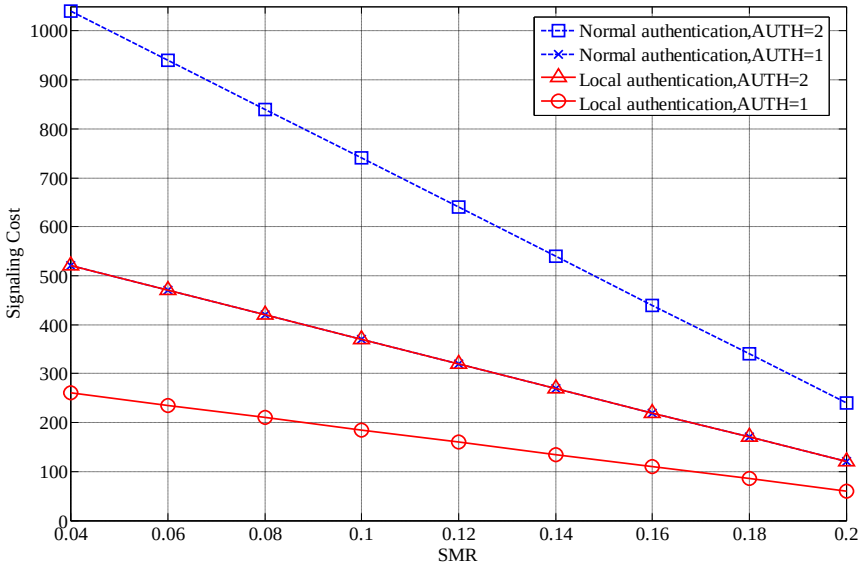


Figure 4. Signaling cost of local and normal authentication schemes (SCOBU-RSU=5,SCRSU-TA=5)

*4.4 Comparisons between Existing Mechanisms*

We summarize comparisons between our designed PPAS with ECPP and RAISE in Table II. In PPAS, the OBUs only perform symmetric cryptography, an XOR operation, and apply a hash function to achieve user anonymity and location untraceability. Moreover, PPAS needs a fewer message passing times. As shown in Table II, PPAS outperforms ECPP and RAISE.

Table II. Comparisons between authentication schemes for security properties

| | PPAS | ECPP | RAISE |
|---|---|---|---|
| Cryptography | Symmetric, XOR, Hash | Asymmetric, Symmetric | Asymmetric, HMAC |
| Total message passing times | 4 | 6 | 5 |
| Anonymity | Yes | Yes | Yes |

| | | | |
|---|---|---|---|
| Location untraceability | Yes | Yes | Yes |
| Stolen-verified attack resistance | Yes | No discussion | No discussion |
| Mutual authentication | Yes | Yes | Yes |
| Local authentication | Yes | Yes | Yes |
| Replay attack resistance | Yes | Yes | Yes |
| Session key agreement | Yes | No | Yes |

*4.5 Conclusions and future work*

In this paper, we propose an efficient authentication scheme called PPAS to protect the privacy of VANET users. The amount of cryptographic calculation under PPAS is substantially less than that of comparable schemes because PPAS only uses symmetric cryptography, an XOR operation, and a hash function. The scheme satisfies the following security requirements: anonymity, location untraceability, mutual authentication to prevent server spoofing attacks, stolen-verified attack resistance, replay attack resistance, and session key agreement. Moreover, our scheme has the property of local authentication, which reduces the authentication latency and network overhead, and ensures that the scheme is fault tolerant. In a future work, we will consider privacy preservation mechanisms in vehicle to vehicle communications.

## V. ACKNOWLEDGMENTS

This research was supported by the Ministry of Science and Technology, R.O.C., under grants MOST 107-2221-E-163-001-MY3.

## VI. REFERENCE

[1] Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.
[2] M. Nekovee and B. B. Bogason, "Reliable and Efficient Information Dissemination in Intermittently Connected Vehicular Ad hoc Networks," IEEE 65th Vehicular Technology Conference (VTC), pp. 2486-2490, 2007.
[3] Jing Zhao, Yang Zhang, and Guohong Cao, "Data Pouring and Buffering on the Road: A New Data Dissemination Paradigm for Vehicular Ad Hoc Networks," IEEE Transactions on Vehicular Technology, Vol. 56, No. 6, Part 1, pp. 3266-3277, 2007.
[4] J. P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy Magazine, Vol. 2, No. 3, pp. 49-55, 2004.
[5] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," ACM International workshop on Vehicular ad hoc networks (VANET), pp. 1-15, 2006.
[6] M. Raya and J. P. Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.
[7] Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," IEEE International Conference on Computer Communications (INFOCOM), pp. 246-250, 2008.
[8] J. Freudiger, M. Raya, and M. Feleghhazi, "Mix Zones for Location Privacy in Vehicular Networks," The First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS), pp. 1-7, 2007.
[9] K. Sampigethaya, Mi. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE Journal on Selected Areas in Communications (JSAC), Special issue on Vehicular Networks, Vol. 25, No. 8, pp. 1569-1589, 2007.
[10] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," IEEE International Conference on Computer Communications (INFOCOM), pp. 1229-1237, 2008.
[11] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and Pin-Han Ho, "RAISE: An Efficient RSU-Aided Message Authentication Scheme in Vehicular Communication Networks," IEEE International Conference on Communications (ICC), pp. 1451-1457, 2008.
[12] G. Morales-Andres and M. Villen-Altamirano, "An Approach to Modeling Subscriber Mobility in Cellular Radio Networks," The Forum Telecom'87, pp. 185-189, 1987.
[13] S. Pack., T. Kwon, and Y. Choi, "A Performance Comparison of Mobility Anchor Point Selection Schemes in Hierarchical Mobile IPv6 Networks," Computer Networks, Vol. 51. No. 6, pp. 1630-1642, 2007.
[14] Ming-Chin Chuang and Jeng-Farn Lee, "PPAS: A Privacy Preservation Authentication Scheme for Vehicle-to-Infrastructure Communication Networks," *IEEE CECNET*, pp.1509-1512, April 2011.