A framework using IBC achieving non-repudiation and privacy in vehicular network.

Amira Bradai, Afifi Hossam

A Framework Using IBC Achieving Non-Repudiation and Privacy in Vehicular Network

Amira Bradai and Hossam Afifi.
Telecom & Management South Paris,
RS2M department Evry, France
{amira.bradai, hossam.afifi }@it-sudparis.eu

Abstract— **In vehicular communications, a balance between privacy and anonymity from one side and responsibility and non repudiation from the other side is very important.**
In this paper, a security framework for VANETs to achieve privacy and non-repudiation is proposed.

We present the safety requirements in the context of accident and reporting problem. We build a platform to provide security to safety messages in an accident scenario based on Identity-based cryptography (IBC).

An analytical evaluation and performance measurement are achieved to validate this platform.
This study confirms that identity-based cryptography and elliptic curves are very useful to make light communications.

***Index Terms*— Security, Privacy, Identity-based Encryption (IBE), Tracing, Non-repudiation, Vehicle communication**

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) technologies attract considerable interest in the fields of research, industry and normalization, owing to their applications in roadway scenarios.
An important challenge facing vehicular ad hoc networks is user privacy. In vehicular communication, due to its broadcasting nature, overhearing identity-specific information could happen frequently. However, one entity should have the ability to retrieve a vehicle's real identity from its pseudo identity when a dispute happens or when the content of a message is bogus.

The remainder of this paper is organized as follows: The next section gives a brief history about Identity-based cryptosystem. Section III presents related works. Section IV describes the solution. In Section V we present the security analysis. A framework implementation and evaluation is presented in Section VII. Finally, we conclude the paper in Section VIII and highlight some points for future work.

II. BRIEF OVERVIEW OF THE IDENTITY-BASED CRYPTOSYSTEM

Identity-based cryptography is a public-key encryption system in which the public key of a user is generated from his/her identity (e.g. a user's email address, the physical IP address, etc.)
Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. IBC cannot have any meaningful usage until it is linked to a well-known non-repudiable entity. This non-repudiable domain is known as Private Key Generator (PKG). It is a theoretical anchor point that other parties trust for its unforgeable nature. To operate the system, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the owner of the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID.
Fig. 1 illustrates the different functions in IBC in mail scenario.

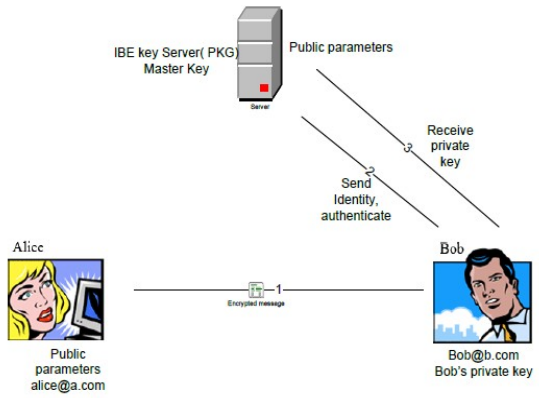

Fig. 1. IBE in mail scenario

- **Setup**: The Private Key Generator (PKG) is a trusted central authority that creates its parameters, including a master secret S used to generate the private keys for users. These parameters are used for the keys generation. The system parameters are: the order q, the

978-1-4577-0737-7/11/$26.00 ©2011 IEEE

prime number p, the generator point P, PKG public point P_{pub}= S.P and the hash functions.

- **Encryption:** When Alice wishes to send an encrypted message to Bob***(1)***, she encrypts the message ***M*** using Bob public key, P_{Bob} and obtains cipher message ***C.***
- **Key Extraction:** Bob authenticates himself (2) to the PKG and obtains the secret key S_{Bob} (3).
- **Decryption**: When Bob receives S_{Bob}, he decrypts the cipher message ***C*** to obtain the message ***M***.

This concept (IBC) was first proposed by **Shamir** [1] in 1984. In 2001, **Dan Boneh** and **Matthew K.Franklin** [2] developed an efficient approach of the identity-based system which employs weil pairing on elliptic curves, its security is based on the bilinear Diffie Hellman problem (BDHP).

Many other identity- based cryptographic schemes appeared in the literature. Apart from Boneh and Franklin's seminal work**, Cocks**[3] proposed a solution based on quadratic residuosity. However, it is generally considered very costly in terms of communication overheads due to the significant message expansion.

McCullagh and Barreto [4] proposed an authenticated key agreement protocol. Their protocol operates in two modes, with or without escrow. It is implemented using the conventional Tate pairing over elliptic curves. It achieves a perfect forward security, but provides no resistance to Key-compromise impersonation attack (KCI attack). The goal of a KCI attacker who has obtained the private key of an honest party is to impersonate a user to establish a valid session key with the corrupted party. **Wang et al** proposed an improved version of McCullagh-Barreto protocol in terms of resistance against of this KCI attack [5].

III. RELATED WORKS

In this section, we give an overview on the proposed security schemes in VANETs. The predominant approach uses asymmetric crypto rather than symmetric key architectures.

In general, the solutions with PKI infrastructure provide strong security features but they require extra communications to manage the Certificate Revocation Lists (CLRs) and high storage overheads.

Raya et al [6] proposed certain recommended mechanisms to achieve security issues in VANETs. Raya proposed to set up an Event Data Recording (EDR) machine and tamper-proof hardware in vehicles and to establish vehicular public key infrastructure.

Many security frameworks using PKI have been proposed but they still require extra communication and have heavy overheads. So another set of solutions are based on IBC have been introduced.

In [7], **Kamat et al**. used the ID-based signcryption. The base station manages CRLs of vehicles and issues new pseudonym IDs and secret keys using RSA. It stores CRL entries that are less than a year old. The proposed scheme offers privacy using short-lived, authenticated and unforgeable pseudonyms. The advantage of this scheme is that the communication between system entities is not tracked by parties and that the Trust Arbiter (TA) is able to verify trail in case of a dispute. There is no special storage required in either the vehicles or the infrastructure for each pseudonym.

In [8], based on non-interactive ID-based public key cryptography, blind signature and one way hash chain, **Li et al** proposed a protocol that is secured against eavesdropping and impersonating attacks. This work fixed the VANET architecture and analysed the communications between vehicles, between vehicles and roadside devices step by step. It also defined how to realise the access authorization phase and the access service phase. This scheme is efficient but it doesn't consider non- repudiation.

In these schemes, the Key Generation Center can abuse its access ability and cause the key escrow. That's why, in [9], **Jaeduck Choi** and **Souhwan Jung** proposed a new approach to assure strong non repudiation and conditional privacy. The advantage of this framework is that the third party who verifies the vehicle's ID never knows the user's private key. In fact, in this scheme, the vehicle itself generates the traditional RSA key pair, and the public key is then certified by the TA using an ID-based signature scheme. The third party, TA, generates only the signature value (Γ) for the user's ID and RSA public key. When car accidents and crimes occur, the RTA can trace the user by computing the PID with the public parameters of PID and all ID's registered in the RTA. The proposed security architecture is efficient in terms of signature and verification time but doesn't explain the case of non-repudiation.

In [10], **Sun et al** proposed a privacy preserving defence and pseudonym-based scheme to assure vehicle user privacy and traceability. This mechanisms guarantee authentication, non-repudiation, message integrity, and confidentiality.

In [11] and [12], **Lin et al.** introduced conditional privacy preservation with Group Signature and Identity-based Signature (GSIS) in 2007 and then with (Efficient Conditional Privacy Preservation (ECPP) in 2008.

In [13], **Chun-I e al**. proposed a mechanism based on bilinear mapping to improve the efficiency, the management cost, the performance and the certificate management. The EPPKI (Efficient Pseudonymous Public Key Infrastructure) assures the setup of the system with the parameters, the registration of the vehicle with the Certificate Authority (CA), signing, verification, tracing and revocation.

However, in all the existing security frameworks using an ID-based cryptosystem in VANETs, the private/public keys are assigned to vehicles or roadside devices by the PKG, which causes a problem because the PKG can cause an attack. Therefore, security framework providing strong security to be used in VANETs is required.

IV. DESCRIPTION OF THE SOLUTION

A. Preliminaries

To setup ECC, we first select a particular elliptic curve E over GF(p), where p is a big prime number. We also denote P as the base point of E and q as the order of P, where q is also a big

prime. We then pick a secret key x, and the corresponding public key y, where y = x.P, and a cryptographic hash function h(.). Finally, we have the secret key x and public parameters (y, P, p, q, h(.)). We denote encrypting a message m using public key y as EccEncrypt(m, y). The resulting ciphertext is denoted by c. The decryption of ciphertext c using the secret key x is given as EccDecrypt(c, x). The algorithms for EccEncrypt and EccDecrypt are found in Alg. 1 and Alg. 2 respectively.

Algorithm 1 **EccEncrypt(m, y)**
1: Generate a random number r ∈ GF(p). Encrypt m with r, $E_r(m)$
2: Calculate $A_r = h(r).\ y$
3: Calculate $B_r = h(r).\ P$
4: Calculate $\alpha_r = r \oplus \chi(Ar)$, where $\chi(Ar)$ is the x coordinate of A_r
5: Return ciphertext $c = (\alpha_r, B_r, E_r(m))$

Algorithm 2 **EccDecrypt(c, x)**
1: Calculate $x .B_r = x .\ h(r) .P = h(r) .\ y = A_r$
2: Determine the x coordinate, $\chi(A_r)$
3: Derive symmetric key r with $\alpha_r \oplus \chi(A_r) = r \oplus \chi(A_r) \oplus \chi(A_r) = r$
4: Apply r to $E_r(m)$ to return m.

B. *Motivations and contributions*

We are motivated to propose a security system that considers the given conflicting goals of privacy and traceability, and the challenges in designing a privacy preserving defense scheme for VANETs.

Specifically, our new identity-based system includes:

- new entities distribution,
- new algorithms to encrypt and decrypt message,
- pseudonym-based scheme to assure vehicle user privacy,
- new pseudonym generation and update of the private key,
- assuring non-repudiation of vehicle's owners in case of dispute,
- securing Vehicle to Infrastructure(V2I) communications,
- avoiding attacks .

The use of IBE in vehicular ad-hoc network has been proposed as mentioned in related work section. However, conventional IBE schemes cannot be secure and have large data computation times. We design a protocol based on identity-based encryption (IBE) where we provide total privacy protection to a vehicle. We propose on-demand-puzzled IBE sharing two properties with conventional IBE: the ability to use an arbitrary string to generate a public key and the ability to generate a public key separately from the corresponding secret key.

The first new idea behind our solution is to let an OBU independently generate a public key on-the-fly using an arbitrary string. The latter is used by the OBU to derive a public key, ***y*** to encrypt the message and send it to the RSU. At first, the OBU cannot create the secret key needed to decrypt the message.

When the OBU must release this information to the tracing manager or emergency procedures, it can derive the corresponding secret key, $\boldsymbol{x_{str}}$ by using the same string. This simplifies the key management, since the OBU can generate the secret key on-demand.

The second idea targets security: Instead of generating a single secret key, our protocol generates ***n*** secret keys and ***n*** corresponding public keys.

C. *Description of the proposed VANETs System*

The system consists of three network entities as shown in figure 1: the trusted authority (TA), the immobile RSUs at the road side and the mobile OBUs on the running vehicles.

- **TA**: is in charge of the registration of immobile RSUs(Road Side Units) and mobile OBUs(on board units) equipped on the vehicles.

- **RSU**: subordinated by the TA and connected to the Internet backbone to support diversified services.
  It holds storage units for storing data from vehicles (storage site).

- **OBU**: installed on the running vehicles, which mainly communicate with each for sharing local traffic information to improve the whole safety driving conditions, and with RSUs for requesting.

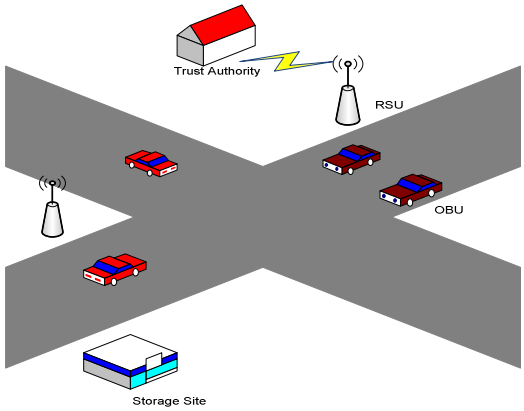

Fig. 2: The network model

D. *Steps of our protocol*

We describe first the initialization phase followed by the encryption phase which outlines how an OBU encrypts its data describing events in the system. The transfer phase describes how the OBU transfers data to the storage site. When a dispute occurs the quering phase is triggered when the tracing manager needs to obtain data from the storage site and knows the

location of the OBU and its identity. Finally, when the private key is compromised, we put the update phase.

Initialization phase:
Trust Authority select an elliptic curve E over GF(p) where ***p*** is a big prime number. We also denote ***P*** as the base point of ***E*** and ***q***, big prime, as the order of P.
The master secret key $X=(x_1 \ldots x_n)$ a set of n secret keys.
The master public key $Y= (y_1 \ldots .y_n)$ Where $y_i=x_i.P$.

Vehicles are preloaded with those parameters ***Y, P, q, p*** and ***h(.).*** Once the vehicle is in the network, TA assigns pseudonym to vehicles travelling in their home domain and vehicles from other domains. This pseudonym allows vehicles to authenticate with RSUs and others vehicles.
To generate a Pseudonym IDentity (PID), we have ***r*** as a random number $PID_i=str + r_i.h(P)$
For the communication Vehicle to vehicle (V2V) and for communication with the RoadSide infrastructure, the vehicle needs to generate a pseudonym for particular session and after a period of time, it need to generate a new one $PID_{i+1} =PID_i+r_{i+1}. h(P)$
Encrypt:
Derive the string ***str***, generate a random ***n***. Calculate m=(flag|n), where flag is a known bitstring. To encrypt a message ***m*** using a public key derived from string ***str***, the OBU does Encrypt (m, str) to determine the ciphertext ***c***.
1: Determine string ***str*** using agreed upon syntax.
2: Generate public key y_{str} where $y_{str} = \sum h_i(str) .y_i$
3: Execute EccEncrypt(m, y_{str}) to obtain c

Transfer:
Periodically, OBUs transfers data to the storage site (unicast/broadcast) using its PID.
Querying:
In figure 3, the querying phase is explained like follows:
An OBU transfers data to the storage site. At the moment of accident, OBU runs Keygen(str) = x_{str}, $X_{str}=\sum h_i(str).x_i$, where $h_i(str)$ is the i-th bit of h(str), to derive the corresponding secret key x_{str} needed to decrypt data of the accident event.
A tracing manager or emergency wishing to obtain data will first contact the TA for permission. Then, they contact the storage site and retrieve the data. The Tracing manager executes EccDecrypt(c, x_{str}) to obtain the original message ***m*** which was encrypted using a secret key derived from ***str***.
Update phase:
In many systems, when the private key is compromised, the user must have a new key through a secure channel and that make network overhead and security problems.

So, we think that the private key must have a short period time ***T*** such as few hours. The private key will be valid only during this designated lifetime. OBUs compute keygen(str_i) with $str_i = str_{i-1} || T_{current}$ and send to the TA to be registered. The TA verifies the current time and the previous update of the key to respect the expiration period.

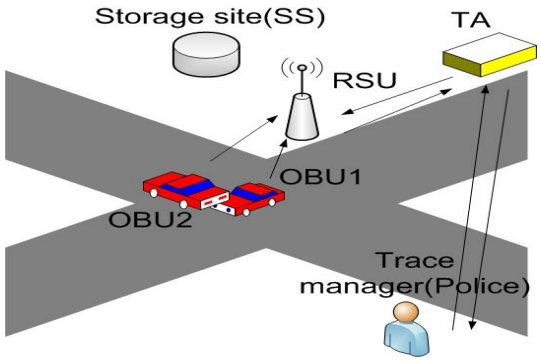

Fig. 3. Solving dispute scenario

V. SECURITY ANALYSIS

To verify the robustness of our system, we begin by examining the basic primitives, followed by an analysis of the protocol.

A. Analysis of Basic Primitives

The setup procedure is similar to the ECC 'one except knowing only one x_{str} and *h(str)*, the Tracing manager cannot determine the vehicle's master secret ***X*** since there are ***n*** unknown x_i. The Tracing manager is only able to determine ***X*** when he has in possession ***n*** different secret keys $x_1, \ldots, x_n$.

The use of the pair (x_{str}, y_{str}) as the private key and public key derived from string ***str*** does not violate the discrete logarithm property of ECC where, given a ***y = x. P***, it is infeasible to determine ***x*** given ***y*** and ***P***, since both are simply the result of addition of points. Also, both Encrypt and Decrypt procedures are secure since both rely on well-established ECC encryption and decryption methods.

B. Analysis of the protocol

Our protocol protects the privacy of the vehicle identity and location by encrypting all the information before forwarding the data to the storage site. Since all messages are in ciphertext, the storage site learns nothing about the vehicle's data.
When the Tracing manager receives permissions to access data encrypted under the string, he receives the secret key x_{str}, which cannot be used to decrypt any other ciphertext not encrypted using y_{str}.
The message ***c*** contains a random number ***n*** generated by the vehicle so the adversary cannot predict the value of ***n***. When he tries to match by creating many public keys, his/her attack will fail.
A compromised vehicle does not allow the adversary to obtain any useful data from the storage site since the vehicle only stores the publicly known parameters.
Finally, our protocols provide flexibility, the string ***str*** can be used to specify access to the data, without using additional certificates and this is the most known advantage of the IBE method.
For instance, we consider the string str={Monday|paris|1} used to encrypt data. An authority willing to obtain the corresponding secret key will have to convince the TA that he is indeed a tracing manager by signature. The process of

specifying what string to construct can be programmed by the vehicle without additional permissions from the TA.

C. *Efficiency Analysis*

The advantage of this scheme is that no special storage is required in either the vehicles or the infrastructures but only in the storage site. This scheme reduces the computation cost in comparison with other schemes where the keygen of the secret key is necessary. Therefore, the proposed protocol is highly efficient in term of computational overheads.

D. *Open Discussion and non-repudiation*

As mentioned earlier, a tracing manager or a man in the middle in general knowing one x_{str} and h (str) cannot determine the master secret ***X***. However, when the Tracing manager receives n secret keys x^1_{str}, …., x^n_{str}, he is able to solve for ***X***. We can prevent such an attack by selecting ***n*** to be large enough and periodically rekeying.

For non-repudiation, in case of a dispute one can try to locate the cause of the incident based on the messages exchanged between vehicles and RSUs and the secret key that is demanded in this case only.

VI. IMPLEMENTATION AND PERFORMANCE

Our goal is to have a first evaluation on the feasibility of the proposed solution before integrating it in a real platform.

So we did separate performance evaluations for our approach and we measured the speed of IBE (generation of TA's parameters, generating private and public keys) and the time needed to get the identity of the responsible of the accident by the tracing manager.

In order to evaluate the speed of the cryptographic operations, we used the IBE provided with "**Miracl** library", we modified it and we implement the communications between entities.

We used the elliptic curve $y^2=x^3+1$ mod p where p is 25-bits prime number.

We can see clearly the communication process among the system entities using the fig. 4 and fig. 5.

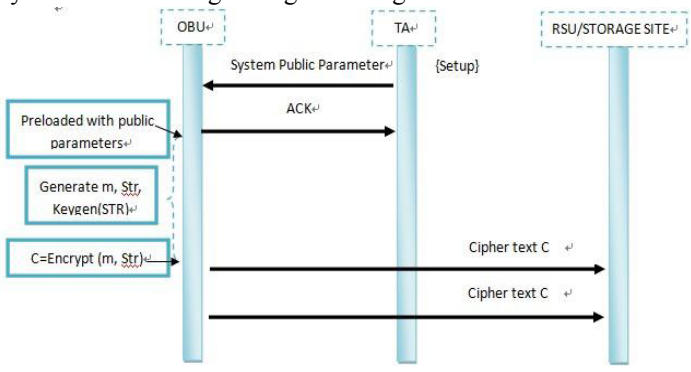

Fig. 4. Exchanges before the accident

When there is no accident happens on the road, TA broadcast the system public parameters (Y, P, p, q, h(.)) to all the OBUs on the road inside the broadcast range. OBUs preloaded with public parameters, the pseudonym identity, generate m, str, Keygen(str) and encrypt his date and get. OBUs send the cipher text to RSU/Storage Site (SS).

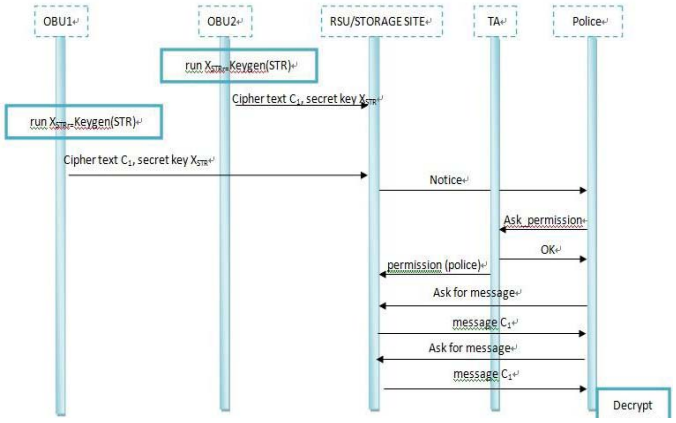

Fig. 5. Exchanges after the accident

When there is an accident happened between OBU1 and OBU2, OBU executes Keygen to derive X_{str} automatically. Then, it sends his own information of accident (time, location) in cipher text C with the secret key X_{str} to RSU/SS. The police (the tracing manager) asks the TA for permission (authentication). When he is authenticated, he can get the cipher text ***C*** which is stored in RSU/SS and uses the key to decrypt the message.

We analyze the previous points in order to evaluate the performance of our solution. We tried to observe the execution time for all the entities executed during the simulation and also for the executed time of functions. For each of these functions, the executed time is displayed as follows:

For each of functions, Setup: 7ms, Keygen: 28ms, Encrypt : 3ms and Decrypt : 2ms

For the execution time of each entity, we can clearly see from the execution time that the proposed cryptosystem is feasible in VANETs.

In scenario one (figure 4): TA : 30MS, OBU : 69MS

In scenario two (figure 5): OBU1 : 20MS, OBU2 : 21MS, TA : 20MS, RSU : 60MS and POLICE : 17MS

From the above data, we can find that the whole execution time for one accident is quite small and this is important because this application in VANET don't tolerate delay.

From our analysis, we believe that IBE performance is the most critical point that can influence the deploying of our solution. The identity based cryptography is also more secure using 160-bits key. The global performance of our solution needs to include the network interaction between the entities (vehicle, TA, RSU and police).

There are still some points that we can be changed to enhance the execution time. For example, we can improve the algorithm generating the PKG parameters and the generation of the keys because it introduces some delay.

VII. CONCLUSION

In this paper, we presented on-demand-puzzled IBE, an identity based encryption. It is considered to be light and suitable for vehicular communications. We also designed a

protocol based on this modified IBE system to assure privacy support and legal tracing. We evaluated our protocol using security analysis and by validating it in a platform for the accident scenario. We plan to ameliorate the system by including some additional authentication, signing and communication to make the simulation and the implementation more practical.

REFERENCES

[1] A. Shamir, "Identity Based Cryptosystems and Signature Schemes". In: Blakely,G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, Springer, Heide lberg 1985.

[2] D. Boneh and M. Franklin. "Identity-based encryption from the Weil pairing". In J. Kilian, editor, Advances in Cryptology - Proceedings of CRYPTO 2001, pages 213{229. Springer-Verlag LNCS 2139,

[3] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues". In IMA Int. Conf, pages 360-363, Springer-Verlag,2001.

[4] N. McCullagh and P. S. L. M. Barreto, "*A new two-party* identity-*based authenticated key agreement"*, Cryptology ePrint Archive, Report 2004/122, CT-RSA 2005.

[5] Y. Wang, "Efficient Identity and Authenticated Key Agreement Protocol", 2005

[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] P. Kamat, A. Baliga, and W. Trappe, ″An Identity-based security framework for VANETs,″ in Proc. VANET06, pp. 94-95, Sept. 2006.

[8] L. Chun-Ta, H. Min-Shiang , CHU Yen-Ping, " A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks", In Computer Communications archive Volume 31 , Issue 12, Pages: 2803-2814, 2008.

[9] J. Choi , S. Jung, "A security framework with strong non-repudiation and privacy in VANETs", In Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference table Las Vegas, NV, USA, Pages: 835-839, 2009.

[10] J. Sun, C. Zhang, and Y. Fang, ″An ID-based framework achieving privacy and non-repudiation in vehicular ad hoc networks,″ in Proc. MILCOM 2007, Oct. 2007.

[11] X. Lin, X. Sun, P.H. Ho, and X. Shen, ″GSIS: A secure and privacy preserving protocol for vehicular communications,″ IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442-3456, 2007.

[12] X. Lin, R. Lu, C. Zhang, H. Zhu, and P.H. Ho, ″Security in vehicular ad hoc networks,″ IEEE Commun. Mag., vol. 46, no. 4, pp. 88-95, Apr. 2008.

[13] Chun-I Fan, Ruei-Hau Hs, Chun-Hao Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks", Proceedings of the International Conference on Mobile Technology Applications and Systems, September 10-12, 2008, Yilan, Taiwan