A study on anonymous identity-based security mechanism for the vehicular ad hoc network

Hsuan Heng Lai, *Henry Ker-Chang Chang

Chang Gung University, Department of Information Management, 259 Wen-Hwa 1st Road, Kwei-Shan Tao-Yuan, Taiwan, 333, R.O.C.

M9644022@stmail.cgu.edu.tw

*changher@mail.cgu.edu.tw

***Abstract*— In recent years, communication technologies have grown and matured, especially wireless technologies. Because of using wireless technologies, like the vehicle and transportation industry, have become more expandable. When wireless technology is attached to a vehicle, this vehicle becomes smarter than previous ones. These vehicles can now get various kinds of information which they need from other vehicles or communication infrastructures. Government can use this property to improve road safety, traffic management, and driver convenience and other related applications and services. In this article, we propose a secure anonymous identity generation mechanism and a secure anonymity trace mechanism. Anonymous identities combine with an identity-based cryptosystem to realize basic security requirement and privacy protection in VANETs. The anonymous property is attached to the proposed mechanism to protect personal privacy, but the user's real identity can be traced by police or law enforcement authorities when necessary.**

***Keywords*— VANETs, security, privacy, ID-based, anonymity**

1. INTRODUCTION

Traffic safety and management are serious issues that concern various countries concern all the time. Intelligent Transportation System (ITS) is an approach that can facilitate road safety, traffic management, and traffic information integration for drivers, passengers, and managers [15]. ITS integrates components such as electronic, communication, information and sensor technology. Telematic is an important part of ITS. It is an integrated application which focuses on telecommunication and informatics. By using telematic, people can not only get many kinds of traffic information, but they can also access entertainment, commerce, communication, convenience and information services. With telematic, ITS can be more powerful and increase road safety by giving drivers more time to react when there is danger. Safety-related information and traffic-related information also give drivers more time to make right decisions.

The wireless communication environment in telematic is called the vehicular ad hoc network (VANET) which is an important, complex, and dynamic communication network for telematic. With wireless communication technologies, various kinds of information can be transmitted between vehicles like cars, buses, trucks, and roadside units, and suitable communication protocols can realize many applications. The most general one is IEEE 802.11p (Wireless Access in the Vehicular Environment, WAVE) which is used MAC layer. 802.11p is an extended version of IEEE 802.11a and is made adaptive to the high mobility environments.

VANET is a wireless communication network based on mobile ad hoc network (MANET) topology. The topology of MANET changes frequently [9]. In VANET, nodes are presented by vehicles which have high speed (60km/h~300km/h). The MANET communication standards and protocols are not suitable for VANET because vehicles have no low energy power, low capability, and low memory problems. The potentially challenges are the high speed and large dimensions of VANET [11].

Many governmental ITS projects and researches have been proposed in many organizations such as the Taiwan Intelligent Transport Society, the U.S.A. Vehicle Safety Consortium [5, 7], the European Union Car-2-Car Communication Consortium [3], the European Road Telematics Implementation Coordination [4], the Japan Road and the Traffic Intelligence Society Organization [23]. IEEE Dedicate Short Range Communications (DSRC)

[1] research team proposed about 40 kinds of applications earlier on, as well as applications that are in sustainable development. VANET applications can be divided into two groups. They are safety related and non-safety related applications. Either group can then be divided into three sub groups which are vehicle-to-infrastructure (V-2-I), vehicle-to-vehicle (V-2-V), and vehicle-to-person (V-2-P) [19], [22]. Fig. 1 illustrates a safety-related application.

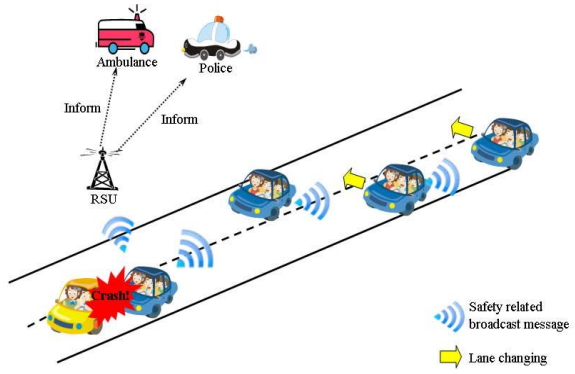

Fig. 1 Safety related application example - Intersection Collision Avoidance

In recent years, security has become the basic requirement of electrical applications especially network communications. Basic security requirements include access control, data confidentiality, node availability, data integrity, non-repudiation, and authentication. These requirements all have to be considered in VANET too [15]. Another important security issue was found to be personal privacy. When drivers want to acquire services from the service provider or want to broadcast safety-related messages, they might want to hide their real identity. Hiding one's real identity is a way to protect personal privacy because hackers can get our private information easily through general identifiers like our car license plates (LP) or our names [6]. Even though privacy protection is important, malicious anonymity might broadcast forged traffic information to endanger other drivers. An anonymous safety-related message has to be traceable if it is malicious.

If we can properly design a security mechanism and a secure architecture from the beginning of implementation, it will not difficult to prevent the security or privacy attacks. Raya [16] and Wang et al. [24] proposed using anonymous key pairs to protect personal privacy, but both ideas as of now are just a concept. They were not able to describe the details. In 2008, Lin et al. [11] pointed out the privacy- and identity-related problems in the IEEE standard 1609.2. We propose a mechanism based on identity-based cryptosystem in order to apply anonymous identities and corresponding key pairs. These key pairs can be used in secure communication schemes which have been proposed. The way, real identities of anonymities can also be tracked by police or law enforcement authorities legally.

2. RELATED WORK

In this chapter, we review some schemes that talk about how to secure VANET. In order to establish our proposed anonymous identity-based mechanism for VANET, we review some previously published cryptographic techniques and papers which discuss security issues in VANET.

2.1 Identity-Based Cryptosystem

Shamir [23] first proposed an Identity-Based Cryptosystem (IBC) concept in 1984. This system is different from general public key infrastructure (PKI) systems like the RSA cryptosystem. The characteristic of this system is that the sender can just use the receiver's identity information like name, email address, or phone number to encrypt the message and it does not have to verify each person's certificates during the procedure.

After Shamir proposed the concept, there are many other schemes were developed, but these schemes did not meet all of the requirements of IBC. For example, some schemes needed lots of calculation when it produced key pairs. In 2001, Boneh and Franklin [2] proposed an Identity-Based Encryption scheme that was based on the bilinear pairings property of an ellipse curve. In 2002, Paterson [13] proposed an Identity-Based Signature scheme that was also based on the bilinear pairings property of ellipse curve. These schemes can be used in practical applications. Let us review these schemes.

2.2 Boneh-Franklin's Identity-Based Encryption scheme

In 2001, Boneh and Franklin proposed an Identity-Based Encryption scheme from the Weil pairing [2]. There is a Key Generation Center (KGC) in this system. The KGC is responsible for issuing private keys, and the KGC hashes user's ID with a hash function to produce the user's public key. We show the properties of admissible bilinear pairing as below.

2.2.1 Admissible bilinear pairing

Let G_1 be an additive group of prime order q, and G_2 be a multiplicative group of the same order. Let P denote a generator of G_1. The discrete logarithm problem (DLP) in these groups is believed to be hard. A bilinear pairing is a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ with the following properties:

1. Bilinear:

$$\hat{e}(a \cdot Q_1, b \cdot Q_2) = \hat{e}(Q_1, Q_2)^{a b}, \text{ where } \forall Q_1, Q_2 \in G_1 \text{ and } a, b \in Z_q^* . \quad (1)$$

2. Non-degenerate:

$$\forall Q_2 \in G_1, \hat{e}(Q_1, Q_2) = 1 \text{ implies } Q_1 \equiv O, (O \text{ is the infinite}). \quad (2)$$

$$\forall Q_1 \in G_1, \hat{e}(Q_1, Q_2) = 1 \text{ implies } Q_2 \equiv O, (O \text{ is the infinite}). \quad (3)$$

$$\hat{e}(Q_1, Q_2) \neq 1; \text{ therefore it is a generator of } G_2. \quad (4)$$

3. Computable:

There is an efficient algorithm to compute $\hat{e}(Q_1, Q_2)$ where $\forall Q_1, Q_2 \in G_1$.

2.2.2 Encryption procedure

In the general implementation of G_1, there will be a group of points on an elliptic curve and G2 will denote a multiplicative subgroup on a finite field. Typically, the map ê will be derived from the Weil pairing on an elliptic curve over a finite field. Boneh and Franklin's scheme is given in the following four algorithms.

1. Setup:

The KGC specifies two groups, G_1 and G_2, and a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ between them. Let P denote a generator of G_1. It also specifies two one-way hash functions.

$$H_1 : \{0, 1\}^* \rightarrow G_1 \text{ (extract point from ID)} \quad (5)$$

$$H_2 : G_2 \rightarrow \{0, 1\}^n \text{ where n is the length of a plaintext message} \quad (6)$$

Then the KGC chooses a private key $s \in Z_q^*$ at random and computes for its public key $P_{Pub} = s \cdot P$, $Z_q^* = \{u \in Z_q \mid gcd(u, q) = 1\}$, P_{Pub} is the public key of the KGC, while $\{G_1, G_2, \hat{e}, n, P, P_{Pub}, H_1, H_2\}$ are the public parameters.

2. Extract:

If the user's identity is $ID \in \{0, 1\}^*$ then $Q_{ID} = H_1(ID) \in G_1$ is the public key of the user. The user's private key which was produced by the KGC is

$$D_{ID} = s \cdot Q_{ID} \quad (7)$$

3. Encryption:

If a sender wants to encrypt a message $M \in \{0, 1\}^n$ with the receiver's ID, the sender calculates the receiver's $Q_{ID} = H_1(ID) \in G_1$ first. Then the sender picks a random number $r \in Z_q^*$ and produces the cipher text

$$C = \{r \cdot P, M \oplus H_2(\hat{e}(Q_{ID}, P_{Pub})^r)\} = \{U, V\} \quad (8)$$

4. Decryption

Receiver can decrypt $C = \{U, V\}$ with his private key $D_{ID} = s \cdot Q_{ID}$. The calculation is

$$V \oplus H_2(\hat{e}(D_{ID}, U)) = M \quad (9)$$

Lemma: we want to improve that $V \oplus H_2(\hat{e}(D_{ID}, U)) = M$.

Proof:

$$\hat{e}(D_{ID}, U) = \hat{e}(s \cdot Q_{ID}, r \cdot P) = \hat{e}(Q_{ID}, P)^{sr} = \hat{e}(Q_{ID}, s \cdot P)^r = \hat{e}(Q_{ID}, P_{Pub})^r \quad (10)$$

then $V \oplus H_2(\hat{e}(D_{ID}, U))$

$= V \oplus H_2(\hat{e}(Q_{ID}, P_{Pub})^r)$

$= M \oplus H_2(\hat{e}(Q_{ID}, P_{Pub})^r) \oplus H_2(\hat{e}(Q_{ID}, P_{Pub})^r) = M$

2.3 Paterson's Identity-Based Signature scheme

In 2002, Paterson proposed an Identity-Based Signature scheme from the Weil pairing [13]. There is a Key Generation Center (KGC) in this system. The KGC is responsible for issuing private keys, and the KGC hashes the user's ID with a hash function to produce the user's public key. Paterson's scheme is given in the following three algorithms.

1. Setup:

KGC specifies two groups G_1 and G_2 and a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ between them and Let P denote a generator of G_1. If the user's identity is $ID \in \{0, 1\}^*$ then $Q_{ID} = H_1(ID) \in G_1$ is the public key of user. The user's private key which was produced by KGC is $D_{ID} = s \cdot Q_{ID}$ and $\{G_1, G_2, \hat{e}, P, P_{Pub}, H_1, H_3, H_4\}$ are public parameters. It also specifies three one way hash functions.

$$H_1 : \{0, 1\}^* \rightarrow G_1 \text{ (extract point from ID)} \quad (11)$$

$$H_3 : \{0, 1\}^* \rightarrow Z_q^* \quad (12)$$

$$H_4 : G_1 \rightarrow Z_q^* \quad (13)$$

2. Signatures generation:

If a sender wants to sign a message M, he/she has to generate a random number $k \in Z_q^*$ first. Then, the sender calculates for the signature (R, S) as below

$$R = k \cdot P,\ S = k^{-1}(H_3(M) \cdot P + H_4(R) \cdot D_{ID}),\ k^{-1} \text{ is the inverse of } k \quad (14)$$

3. Signatures verification:

When a receiver wants to verify a signature, he/she has to calculate for $\hat{e}(R, S)$ first. Then he compares $\hat{e}(R, S)$ with $\hat{e}(P,P)^{H_3(M)} \cdot \hat{e}(P_{Pub}, Q_{ID})^{H_4(R)}$. If both values are equal, this proves that the signature is legitimate.

Lemma: we want to improve that $\hat{e}(R, S) = \hat{e}(P,P)^{H_3(M)} \cdot \hat{e}(P_{Pub}, Q_{ID})^{H_4(R)}$.

Proof:

$$\begin{aligned} \hat{e}(R, S) &= \hat{e}(k \cdot P, k^{-1}(H_3(M) \cdot P + H_4(R) \cdot D_{ID})) \\ &= \hat{e}(P, H_3(M) \cdot P + H_4(R) \cdot D_{ID}) \\ &= \hat{e}(P, H_3(M) \cdot P) \cdot \hat{e}(P, H_4(R) \cdot D_{ID}) \\ &= \hat{e}(P,P)^{H_3(M)} \cdot \hat{e}(P, D_{ID})^{H_4(R)} \\ &= \hat{e}(P,P)^{H_3(M)} \cdot \hat{e}(P_{Pub}, Q_{ID})^{H_4(R)} \end{aligned} \quad (15)$$

2.4 Hash-based message authentication code (HMAC)

The purpose of a hash-based message authentication code (HMAC) is to ensure the integrity and the authentication of messages. The HMAC function can generate a unique value for the message just like a fingerprint, with the HMAC being a fixed-size value. A HMAC based on cryptographic hash functions is known as an HMAC. HMAC is also called keyed-hash message authentication code because of the use of a secret key, which is known to the sender and the receiver, and generates a fixed-size value. Detecting modification is the main objective of HMAC. What we want to use is the property of HMAC in which even an attacker can get a HMAC value, but can not check the HMAC without the key. Thererfore the attacker would not be able to compute for the original input. [21]

2.5 Secure communication schemes for VANETs

In 2006, Raya *et al.* [17] figured out the vulnerabilities in VANETs, vulnerabilities such as message forgery, impersonation, privacy violation, and on-board tampering. They proposed a secure architecture based on PKI which can meet the requirements of authentication as well as of the certificate revocation scheme. They also discussed privacy and identity related problems. In 2007, Raya *et al.* [16] described some security threats that might be happened in VANETs then proposed a secure communication scheme to fight against malicious attacks. The components of the scheme include digital signature, tamper-proof devices (TPDs), key management mechanism, anonymous key pairs. However there are still some security issues such as confidentiality problem in Raya's protocol, Wang *et al.* [24] proposed a more secure communication scheme to enforce and improve Raya's scheme.

2.5.1 The review of Wang's secure communication scheme

In this section we review on the pairwise session key establishment and the group session key establishment of Wang's secure communication scheme. Fig. 2 shows the pairwise session key establishment scheme of the scheme [24]. Before two vehicles start to communicate, they first have to exchange a session key through a secure way. Wang's scheme is based on the Diffie-Hellman key exchange. Using the Diffie-Hellman key exchange can ensure that a session key would only be known by A and B. Because all the key exchange messages are attached to the sender's signature, the middle attacks can be prevented.

For the group applications, establishing secure groups with secret group keys is a better solution. There is a group leader L in the center of the group cell. L distributes the group key SK to members by broadcasting and encrypting the SK with the member's public key. L also sends hash values of the receivers' public keys to help the receivers identify which encrypted group key to decrypt and sign a signature by L's private key to ensure the legality of key distribution messages.

The group session key establishment scheme is shown in Fig. 3.

$A \rightarrow B: M_1(\textit{ask B to communicate message with Diffie-Hellman parameter } a, q, Y_A),$
$Sig_{PrKA}[M_1 \mid T], Cert_A$

$B \rightarrow A: M_2(\textit{respond with Diffie-Hellman parameter } Y_B),$
$Sig_{PrKB}[M_2 \mid T], Cert_B, HMAC_{sk}(M_2)$

$A \rightarrow B: M_3(\textit{session key is built}), HMAC_{sk}(M_3)$

Transmit subsequent encrypted message with signature:

$A \rightarrow B: E_{sk}[m \mid Sig_{PrKA}[HMAC_{sk}(m)]]$

Fig. 2 Wang's pairwise session key establishment scheme

Distribute the group key SK to A, B and C:

$L \rightarrow *: H_A, \{SK\}_{PuKA}, H_B, \{SK\}_{PuKB}, H_C, \{SK\}_{PuKC}$
$Sig_{PrKL}[\textit{the whole message}]$

Using SK to encrypt message:

$L \rightarrow *: E_{SK}[m]$

Encrypted message with signature and HMAC:

$L \rightarrow *: E_{SK}[m \mid Sig_{PrKL}[HMAC_{SK}(m)]]$ or
$L \rightarrow *: E_{SK}[m], Sig_{PrKL}[HMAC_{SK}(E_{SK}[m])]$

When a new node D enter the group:

$L \rightarrow D: \{SK\}_{PuKD}, Sig_{PrKL}[\{SK\}_{PuKD}]$

Fig. 3 Wang's group session key establishment scheme

In both two kind of key establishment schemes, personal privacy can not be protected when necessary. The privacy of broadcast message sources should be considered, too.

2.6. Privacy-aware security schemes for VANETs

Privacy protection is another important security requirement for VANETs. There are some privacy-sensitive information like the driver's name, position, speed, driving route, and electronic license plate (ELP) in the message source which that could be revealed [6]. So, a safety-related message not only has to be authenticated by others, but it should also protect the privacy of the message source. A privacy-aware security infrastructure was proposed by Plöíl et al. [14]. In the proposed infrastructure, LP is a fixed pseudonym for vehicles, and only the governmental transportation authority (GTA) can link the real identities to their pseudonyms. The GTA then issues a vehicle-related identity, just like ELP, for the registered vehicle. But this infrastructure is weak in defending an inside attacker. If someone wants to know the real identity and personal information of an LP or an ELP, he/she can go to the GTA to buy personal information from an employee illegally, and there are many similar cases where governmental employees have sold personal profiles illegally for their own profit.

Raya *et al.* [16] and Wang *et al.* [24] also both also proposed a privacy preserve concept based on anonymous key pairs, but the generation scheme of anonymous key pairs can not be described explicitly and do not consider the traceability for getting the real identity of a person. And in [8], Lin et al. pointed out that the security communication standard, the IEEE 1609.2 security infrastructure, does not consider identity-related and privacy preservation problems.

In 2006, Kamat et al. [10] proposed an identity-based security framework for VANETs. The proposed framework uses the IBC concept and a pseudonym mechanism to protect personal privacy. When drivers need to hide their real identity, they have to find a base station to generate a pseudonym. In VANETs most safety-related applications occur in real time. If drivers do not apply a pseudonym at first, they cannot broadcast safety-related messages in time using a pseudonym identity.

Therefore, what we want to propose is a secure privacy preservation scheme which includes the generation scheme of anonymous key pairs, but the real identity of the user can be traced by police or law enforcement authorities when necessary. Inside attacks from governmental organizations or trusted third parties can also be prevented by a strong infrastructure. The IBC can realize the basic security requirement. The privacy preservation in VANETs is optional [11]. Even though the real identity of a user can be traced, it must have the privacy protection abilities to fight against other general people who would fight to trace message source's sensitive information.

3. ANONYMOUS KEY PAIR APPLICATION MECHANISM AND ANONYMITY TRACE MECHANISM

In the proposed mechanism, there are two sub mechanisms: the anonymous key pair application mechanism and the anonymity tracing mechanism. Our proposed mechanism is focuses on V-2-V communication. Anonymous identities combined with theIBC can realize basic security requirement and privacy protection.

3.1. Anonymous key pair application mechanism

In the proposed schemes, we assume that the KGC and the MVO are legal and secure for information protection. Fig. 4 illustrates the operations in the anonymous key pair apply apolication mechanism. When someone buys a new vehicle, the buyer has to apply a physical and unique LP to the new vehicle. The ELP and the anonymous key pair can be applied at the same time.

The purpose of the system is to generate anonymous key pairs securely and prevent inside attacks form the KGC or the MVO. The MVO applies anonymous key pairs from the KGC for applicant, but the applicant's real identities are only known by the MVO. The KGC can not get the real identities during the period of generating procedure. The MVO cannot know the anonymous key pairs even if these key pairs have to transmit the applicant through the MVO. Because of this, the anonymity can not be matched with the real identity by any one side. We assume that all of the network transportations are protected by security socket layer (SSL).

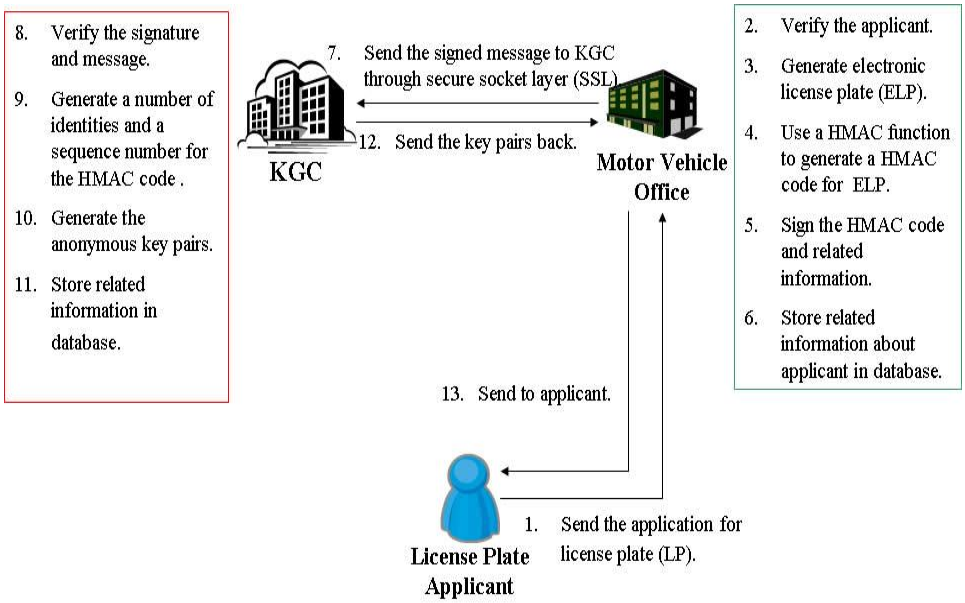

Fig. 4 Anonymous key pair apply mechanism description and architecture

The operation procedure and principle of the proposed mechanism are as follows:

1. The applicant takes or sends an application of the LP, an ex-factory statement and the manufacture's certificate of the vehicle to the MVO, along with the applicant's related information that can prove the applicant's real identity.
2. After receiving the related information and certificate from the applicant, the MVO verifies them first.
3. The MVO then generates a unique ELP for the corresponding LP. The ELP is an electronic data that can be stored in a smart car or in a hardware security module (HSM). An HSM is a physical device in the form of a plug-in card or an external security device that can be attached to general-propose computers. The HSM can secure generated data and secure store data, and use cryptographic or sensitive approaches. The HSM provides both logical and physical protection of data. Many HSM systems have means to securely backup the keys they handle either in a wrapped form via the computer's operating system or by externally using a smartcard.
4. The MVO uses an HMAC function with any one of applicant's real identities such as his/her name, phone number, e-mail address, or identification number to calculate a unique HMAC value for the ELP.

5. The MVO signs the HMAC value and the related information with the MVO's private key. The signature and the certificate can prove that the HMAC value and the messages are sent by the MVO.
6. The MVO stores the HMAC value and applicant's related information in their database securely.
7. The MVO sends the HMAC value and the information that the KGC needs to know to the KGC through a secure channel (SSL).
8. The KGC verifies the message by checking the signature and the certificate of the MVO.
9. The KGC generates one or more than one identities. These identities will combine with the ELP to produce a group of anonymous identities for the applicant.
10. The KGC uses these anonymous identities to generate corresponding key pairs. These anonymous key pairs will then be used in the identity-based VANET environment.
11. The KGC stores the HMAC, anonymous identities, and corresponding key pairs in their database securely.
12. The KGC signs these anonymous identities and corresponding key pairs with the KGC's private key then sends them back to the MVO. The signature and the certificate can prove that the message was sent by KGC. The most important thing is that the MVO just can see the HMAC value and the information which are not related to anonymous identities.
13. The MVO signs the message from the KGC and gives it to the corresponding applicant. After the applicant gets the anonymous identities and corresponding key pairs, he/she can use them in all communication applications.

3.1.1 Application phase

As shown in Fig. 5, applicant chooses two random numbers (r_1, r_2). These two numbers are used as secret keys so the MVO and the KGC can send the message back secretly and. It ensures that the MVO cannot see the context of the message which sent back by the KGC, and the context of the message sent to the applicant by the MVO can not be seen by others, too.

After the MVO verifies the applicant's identity and the vehicle's related information, the MVO then generates the *ELP*. Because we do not want the KGC to see the correct *ELP*, the MVO uses a HMAC function to encrypt the *ELP*. The MVO uses any one of the applicant's real identities as the encrypt key and uses a number (*RIN*) to record which real identity is the encrypt key. Table 3.1 shows an example of (*RIN*). The MVO uses an area code (*AC*) to record which MVO applies anonymous identities to the applicant. (*RIN*) and (*AC*) are used in trace mechanisms which we will describe in detail in Chapter 3.2.

TABLE 1
MECHANISM SYMBOLS

Symbol	Definition
G_1	An additive group of prime order q.
G_2	An multiplicative group of the same order q.
$\hat{e}$	Weil pairing function that can do $G_1 \times G_1 \rightarrow G_2$.
$H_1, H_2,$ H_3, H_4	Hash functions.
s	Secret key of KGC, $s \in Z_q^*$.
P	Generator of G_1.
P_{Pub}	Ppublic key of KGC, $P_{Pub} = s \cdot P$.
LA	LP application.
RID	Any one of the applicant's real identities.
$Cert_M, Cert_K$	Certificate of MVO and KGC.
PU_M, PR_M	Key pair of MVO.
PU_K, PR_K	Key pair of KGC.
PU_P, PR_P	Key pair of police or law enforcement authority.
k_K^P	Secret key known by police, law enforcement authority, and KGC.
k_M	Secret key only known by MVO.
AID_i, Q_{AID_i}	Key pair of an anonymity.
$ASD(), ASE()$	Asymmetrical decryption and encryption function.
$SD(), SE()$	Symmetrical decryption and encryption function.
SK	Group session key
$MAC()$	Hash MAC function based on SHA-2 hash algorithm.
$Sig(), Ver()$	Signature function and signature verification function.

$t_1 \sim t_7$	Timestamps.
AC	Area code of MVO
RIN	A number to record which real identity is the MAC key

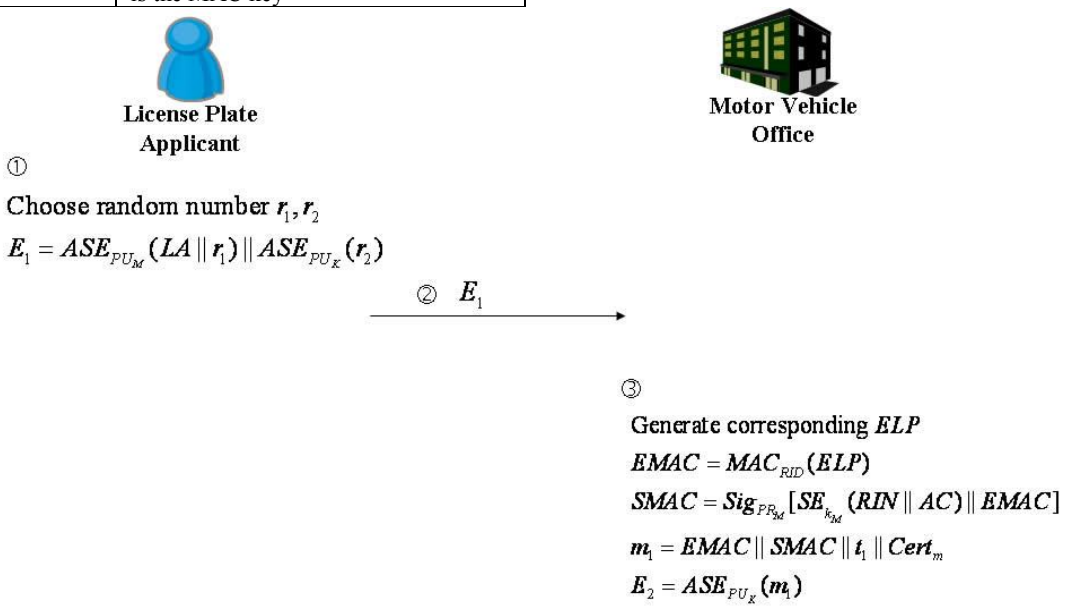

Fig. 5 Application phase

TABLE 2
EXAMPLE OF *RIN*

RIN	**1**	**2**	**3**	**4**	**5**
Real identities	Name	Phone number	Address	E-mail	Birthday

The *ELP* is unique so the HMAC value will also be unique. Because of the property of the MAC and the KGC will not know the HMAC encrypt key. Although the KGC has the HMAC value, it can not calculate for the correct *ELP*. The last operation in this phase is when the MVO sends the MAC value with a timestamp (t_1) and the MVO's certificate ($Cert_M$) to the KGC. Because we have to be sure of the confidentiality of the message, the message will be encrypted by the KGC's public key (PU_K) before it is transmitted.

3.1.2 Key generating phase

As shown in Fig. 6, the KGC will generate anonymous identities and corresponding key pairs for the applicant. After the KGC verifies the message and MVO's identity, it then generates a sequence number (*SN*) which is a record number and a group of user identities (UID_i). The parameter (i) is the order of (*UID*). The KGC uses a MAC function to calculate for MAC value for each (UID_i). The MAC encrypt key is the MAC value of the *ELP*.

For the propose of tracing in the future, police or law enforcement authorities can put a secret key in the KGC. The KGC uses a the secret key to encrypt the (*SN*) then concatenates it with the MAC value of (*UID*). The corresponding key pair will be generated by the scheme which we reviewed in Chapter 2.2 at the same time.

After the applicant gets the anonymous identities, he/she can optionally use his/her real identity or anonymous identities to require service or broadcast messages when he/she wants to be anonymous in order to prevent others form tracing the action. Anonymous key pairs can be stored in a smartcard or store in an intelligent car key to prevent impersonation if the vehicle is stolen.

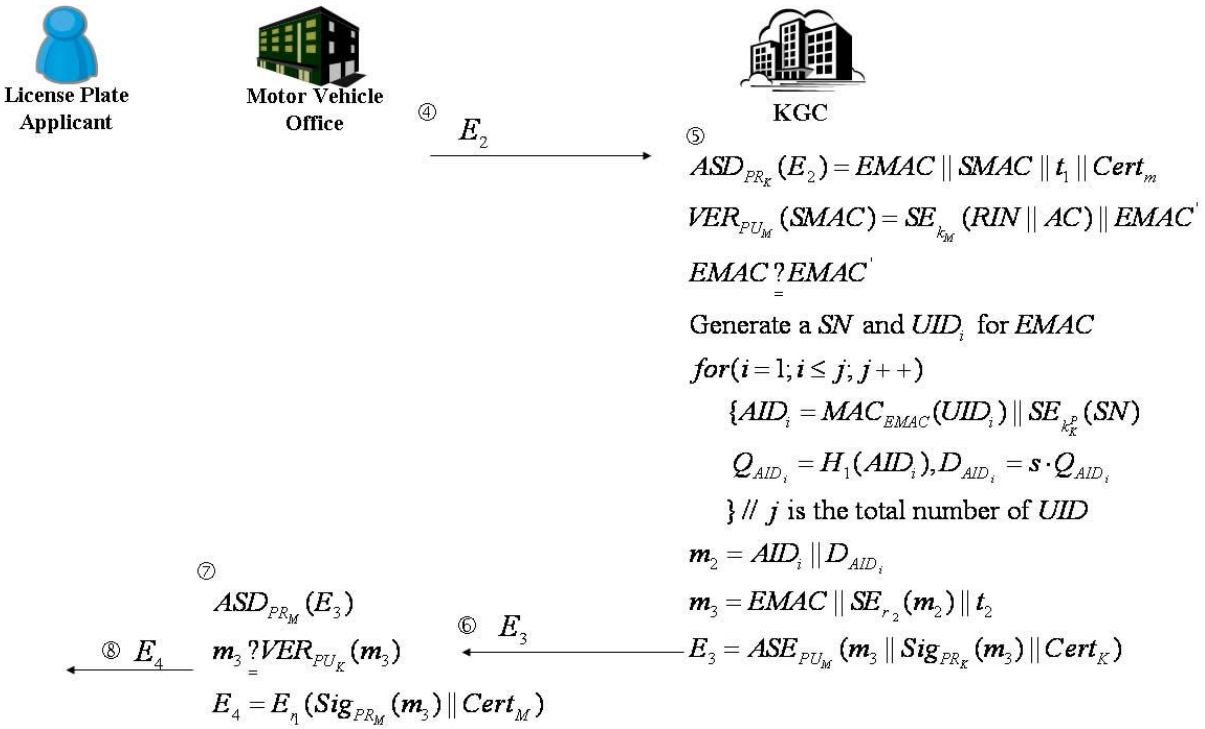

Fig. 6 Key generate phase

3.2 Anonymity trace mechanism

The police or law enforcement authorities, when necessary, can trace the user through safety-related broadcast messages by using this mechanism. Fig. 7 shows the proposed mechanism.

If the police or law enforcement authorities have had the message already, they can conduct the anonymity trace mechanism. The operation steps of the proposed trace mechanism are described as below:

1. The police or law enforcement authorities use the secret key which is shared with the KGC, which only records the sequence number (*SN*), then generates a request message. The request sender will make a signature for the request and hides the (*SN*) by encrypting it.
2. The police or law enforcement authorities send the complete request message (R_{KGC}) to the KGC.
3. The KGC verifies the signature and decrypts the ciphertext to get the (*SN*). Then , it finds the corresponding (*EMAC*) and ($SE_{k_M}(RIN \| AC)$) according to the (*SN*). Before it sends the message back, The KGC will make a signature for it and hidden the (*EMAC*) and ($SE_{k_M}(RIN \| AC)$) by encrypting it, too.
4. The KGC sends the response message (E_5) back to the request sender with secure protection.
5. The KGC gets the (*EMAC*) and ($SE_{k_M}(RIN \| AC)$) which matches the (*SN*) from (E_5). Then, it generates another request message (R_{MVO}). The request sender will also make a signature for the request and hides the (*EMAC*) and ($SE_{k_M}(RIN \| AC)$) by encrypting them.
6. The police or law enforcement authorities send the complete request message (R_{MVO}) to the MVO.
7. The MVO verifies the signature and decrypts the ciphertext to get (*EMAC, RIN, AC*). Then, it finds related information like real identities about the anonymity according to the (*EMAC, RIN, AC*). Before it sends them back, the MVO makes a signature for it and hides the related information by encrypting it.
8. The MVO sends the response message (E_6) back to the request sender with secure protection. Then the police or law enforcement authorities can get the information they want after verifying and decrypting (E_6).

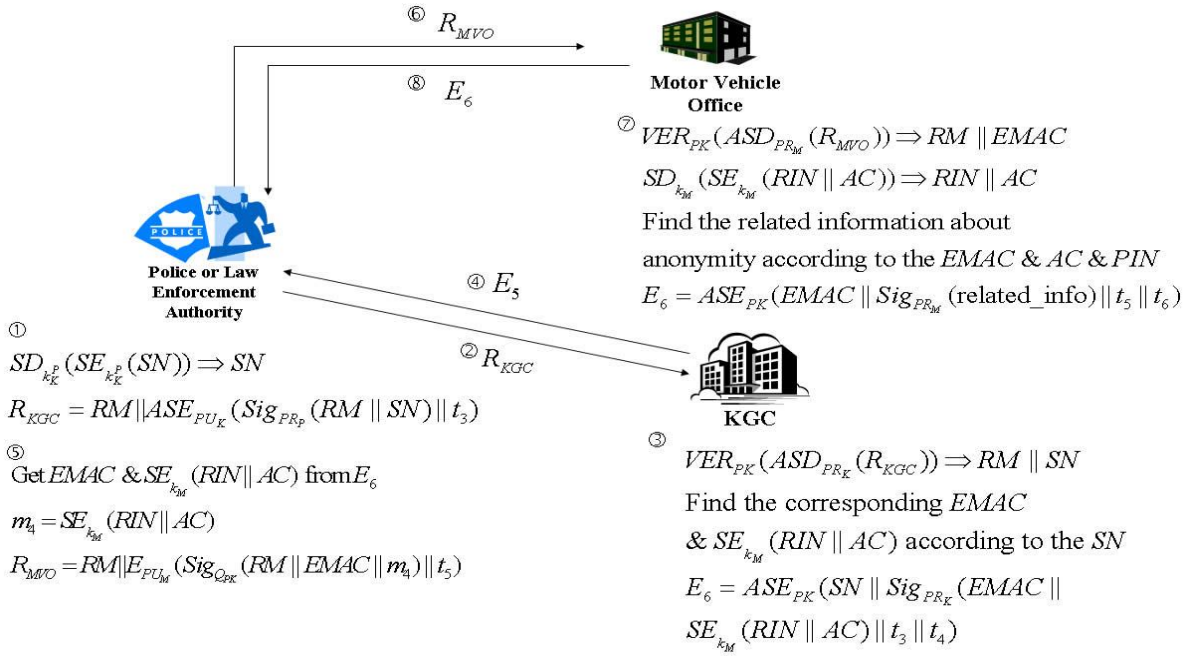

Fig. 7 Anonymity tracing mechanism

3.3 Application scenarios

In this section, we show how the safety-related applications and the group communication application operate with the proposed mechanism. Fig. 8 illustrates the scenario of a safety-related application with anonymity protection. The message broadcast source will choose an anonymous identity to make a signature for the message, and then broadcasts it with a timestamp and a hash value.

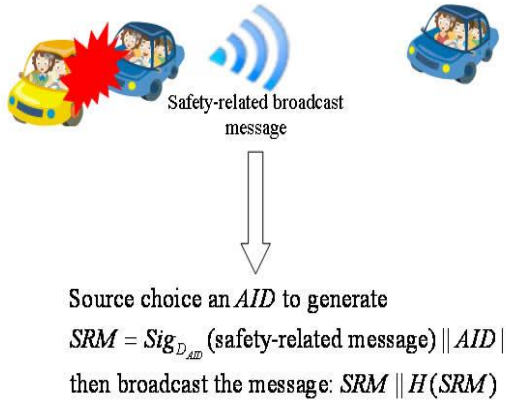

Fig. 8 Scenario of safety related application with anonymity protection

Fig. 9 illustrates the scenario of a group communication application with anonymity protection. This scenario occurs that when a group of vehicles want to discuss together or exchange information, but they don't want to expose their real identities. Before communication starts, the group members first choose the vehicle which is the geometric center of the network topology to be the master node first. The master node is responsible for distributing the group key which is a secret key only known by its members. After the master node is chosen, other group nodes send their (AID) to the master node. The master node then uses their (AID) to encrypt the group key and send it to them securely. The group key will have a lifetime (lt), which means that the group key has to be changed after an interval.

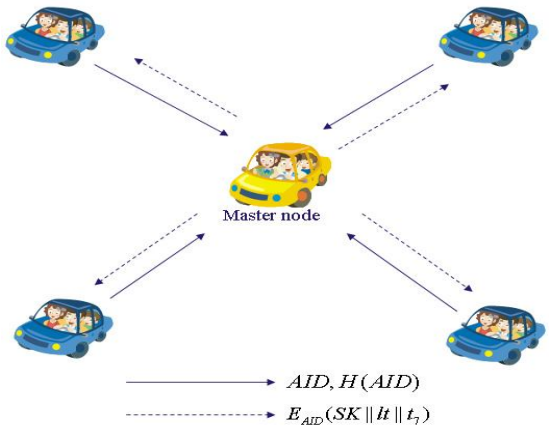

Fig. 9 Scenario of a group communication application with anonymity protection

4. SECURITY ANALYSIS

In this section we first analyze the security of the anonymous key pair generation mechanism and the anonymity tracing mechanism, and then analysis the security in VANETs communication by using anonymous key pairs, and compare this security with other schemes.

4.1 Security analysis for the anonymous key pair application mechanism

(1). Anonymity: The ELP is the material for anonymous key pairs, but the MVO blinds this material with the HMAC function. Even KGC has the HMAC value, but the KGC does not know the HMAC key and can not calculate for the original input (*ELP)*. So, the KGC does not know the real identity of the applicant.

(2). Unforgeability: The material of the anonymous key pairs will be signed by the MVO, so the KGC can verify the legality of the material. On the other hand, the MVO can verify the signature of KGC to ensure the legality of the anonymous key pairs.

(3). Authentication: Because the MVO and the KGC attach their certificates and signatures, they can recognize each other's identity.

(4). Confidentiality: All messages are protected through encryption and the security socket layer, so the confidentiality is ensured.

(5). Insider attack protection: Anonymity can not be matched with the real identity because of the functionality of (r_2) and the anonymity (1) of the mechanism. The random number (r_2) can be encrypted by the KGC's public key before the applicant transmits it, so the random number (r_2) can not be known by the MVO. After the anonymous key pairs are generated, the KGC encrypt them by using the secret key (r_2) before sending them back to the applicant through the MVO. Because of this, the anonymous key pairs cannot be seen by the MVO. When an inside attacker in any of the two departments would want to match the anonymity with the real identity, he/her must have the authority that the police or law enforcement authorities have. Oppositely, attackers can not get the information from two sides.

4.2 Security analysis for the anonymity tracing mechanism

(1). Authentication: Because the police or law enforcement authorities attach their certificates and signatures, they identities can be recognized.

(2). Confidentiality: All messages are protected by encryption, so the confidentiality can be ensured.

(3). Reply attack protection: This problem can be solved by using a timestamp.

4.3 Security analysis in VANETs communication by using anonymous key pairs

(1). Anonymity: Driver can randomly choose an anonymous identity to make a signature for messages before transmission.

(2). Authentication: An anonymous signature can be verified by the corresponding anonymous identity. If the signature cannot be verified, this proves the anonymous identity was not generated by the KGC under the IBC.

(3). Confidentiality: The sender can use the anonymous identity of the receiver to encrypt messages before transmits.

(4). Traceability: The police or law enforcement authorities can trace anonymities by using the anonymity tracing mechanism.

(5). Integrity: We use hash values to prevent that modify messages in the air.

(6). Non-repudiation: The broadcasted messages all have all been signed by the legal anonymous identity. If someone forges the traffic or safety-related message, the source's real identity can be traced by the forged message.

5 CONCLUSION

In this work, we proposed an anonymous key pair generation mechanism and an anonymity tracing mechanism that satisfies the security requirements with privacy preservation under the IBC of the VANETs. It makes the anonymous key pairs generating procedure secure. The anonymous identity can not be matched by insider attack easily, but it can be traced by the police or law enforcement authorities when necessary.

REFERENCES

[1] 5.9 GHz DSRC, http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Proc. Crypto 2001*, LNCS Vol. 2139, Springer, pp. 213-229, 2001.

[3] CAR 2 CAR Communication Consortium, http://www.car-2-car.org/
[4] European Road Telematics Implementation Coordination (ERTICO), http://www.ertico.com/
[5] Federal Highway Administration (FHWA), http://www.fhwa.dot.gov
[6] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo", The security and privacy of smart vehicles", *IEEE Security & Privacy*, Vol. 02, issue 3, pp. 49 - 55, June 2004.
[7] ITS America, http://www.itsa.org/
[8] Chun-Ta Li, Min-Shiang Hwang, and Yen-Ping Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad-hoc networks," *Computer Communications*, 2008.
[9] Nikos Komninos, Dimitris Vergados, and Christos Douligeris, "Layered security design for mobile ad-hoc networks," *Computers & Security*, Vol. 25, Issue 2, pp. 121-130, March 2006.
[10] Pandurang Kamat, Arati Baliga, and Wade Trappe, "An identity-based security framework for VANETs", *International Conference on Mobile Computing and Networking*, pp. 94-95, Los Angeles, California, USA, Sep. 2006.
[11] Xiaodong Lin, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-Han Ho, and Xuemin Shen., "Security in vehicular ad-hoc networks," *IEEE Communications Magazine*, Vol. 46, Issue 4, pp. 88-95, 2008.
[12] Intelligent Transport Systems of Taiwan, http://www.its-taiwan.org.tw/
[13] K. G. Paterson, "ID-based signatures from pairings on elliptic curves", *Electronics Letters*, Vol. 38, Issue 18, pp. 1025-1026, Aug. 2002.
[14] Klaus Plõíl, and Hannes Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," *Computer Standards & Interfaces*, Vol. 30, Issue 6, pp. 390-397, Aug. 2008.
[15] Yi Qian, and Nader Moayeri, "Design of secure and application-oriented VANETs," *Proceedings of IEEE VTC'2008-Spring*, Singapore, May 11-14, 2008.
[16] Maxim Raya, and Jean-Pierre Hubaux, "Securing vehicular ad-hoc networks", *Journal of Computer Security*, Vol. 15, pp. 39-68, 2007.
[17] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux, "Securing vehicular communications", *IEEE Wireless Communications Magazine*, 2006.
[18] W. Ren *et al.*, "ID-based secure routing framework for wireless ad-hoc networks," *In Proceeding of 4th International Conference on Information Technology*, pp. 102-110, 2007.
[19] Secure Vehicular Communication (SeVeCom), "VANETs Security Requirements Initial Version," http://www.sevecom.org/Pages/ProjectDocuments.html
[20] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptoloty-Crypto'84*, LNCS, Vol. 196, Springer-Verlag, pp. 47-53, 1984.
[21] William Stallings, "Cryptography and network security", Fourth edition, U.S.A. , Pearson Education International, 2006.
[22] U.S. Dept. of Transportation, "National Highway Traffic Safety Administration, Vehicle Safety Communications Project - Final Report," Apr. 2006.
[23] Vehicle, Road and Traffic Intelligence Society Organization, VERTIS, http://www.mlit.go.jp/road/ITS/j-html/
[24] Neng-Wen Wang, Yueh-Min Huang, and Wei-Ming Chen, "A novel secure communication scheme in vehicular ad-hoc networks", *Computer Communications*, to appear in 2008.