A Security Framework with Strong Non-repudiation and Privacy in VANETs

Jaeduck Choi and Souhwan Jung
School of Electronic Engineering, Soongsil University, Korea
e-mail: cjduck@cns.ssu.ac.kr and souhwanj@ssu.ac.kr (corresponding author)

***Abstract*—This paper proposes a security framework with strong non-repudiation and privacy using new approach of ID-based cryptosystem in VANETs. To remove the overheads of certificate management in PKI, security frameworks using an ID-based cryptosystem are proposed. These systems, however, cannot guarantee strong non-repudiation and private communication since they suffer from the inherent weakness of an ID-based cryptosystem like the key escrow problem. The key idea of this paper is that the ID of the third-party is used as the verifier of vehicle's ID and self-generated RSA public key instead of using the ID of the peers. Our scheme provides strong non-repudiation and privacy preservation without the inherent weaknesses of an ID-based cryptosystem in VANETs. Also, the proposed scheme is efficient in terms of signature and verification time for safety-related applications.**

***Index Terms*—VANET, ID-based Cryptosystem, Key Escrow Problem, Non-repudiation, Privacy.**

I. Introduction

Among the various application services enabled by enhanced wireless communication technologies, Vehicular Ad-hoc Networks (VANETs) recently represent the most popular ones. Actually, in the USA there are several Intelligent Transportation System (ITS) standard organizations such as IEEE, ASTM, ANSI, etc., [1] and, in Europe, such industrial consortiums as Car 2 Car communication Consortium [2]. Vehicular scenarios have been classified into safety-related and non-safety-related applications. For example, safety-related services include collision avoidance, emergency vehicle signal preemption, intersection collision avoidance, and traffic management. Other applications include payment services and infotainment (e.g., Internet access).

There are several essential requirements to promote these services. Security functions must be supported to prevent potential attacks caused by the driver reacting dangerously as a result of receiving erroneous messages. Especially, the safety applications require a strong mutual authentication with non-repudiation because all safety-related messages may contain life-critical information. In other words, drivers sending safety-related information should not be able to deny the fact that they transmitted the message. For example, if an attacker diffuses wrong safety messages in the VANETs, other drivers receiving these messages would be faced with potentially dangerous situations.

Privacy preservation is another important issue for VANETs. Drivers don't want their private information such as name, position, moving route, and user data to be revealed. In the various applications such as collision avoidance and traffic management, the user must send messages related to these services to other vehicles or roadside devices, which violates the user's privacy regardless of his intention. Therefore, the anonymity of identity should be supported in VANETs. However, when car accidents or certain crimes occur, the identity information has to be revealed by the law authority to establish the liability of accidents or crimes.

To solve these problems, a number of studies for VANET security have been proposed. These studies can be classified into two classes: Public Key Infrastructure (PKI) proposals and the ID-based cryptosystem. There are a number of security frameworks using PKI for VANET [4]-[10]. Although they provide strong security features such as authentication, non-repudiation, and confidentiality, they are not likely to be widely available because they require extra communication to manage the Certificate Revocation Lists (CRLs) and have high storage overheads. These are the most critical drawbacks. To avoid these overheads, security schemes with privacy preservation through ID-based cryptosystem are proposed [12]-[16]. Unfortunately, in all the existing security frameworks, the private/public keys of VANET nodes are assigned by the Key Generation Center (KGC), which causes the inherent weakness such as the key escrow problem since the KGC issues their private keys using the master key of the KGC [17]-[19]. This cannot guarantee strong non-repudiation and private communication because the KGC can sign and decrypt any messages and abuse its access ability.

In this paper, we propose a security framework with strong non-repudiation and conditional privacy using new approach of an ID-based cryptosystem. We use the IDentity of Regional Transportation Authority (RTA) as the third party to verify a vehicle's ID and self-generated RSA public key. In our scheme, the vehicle itself generates the traditional RSA key pair, and the public key is then certified by the RTA using an ID-based signature scheme. The third party, RTA, generates only the signature value (**Γ**) for the user's ID and RSA public key. Therefore, the RTA never knows the user's private key. Note that the VANET nodes verify the signature **Γ** of each other using the RTA's ID. And then, they can use their RSA

978-1-4244-2309-5/09/$25.00 ©2009 IEEE

private/public keys to provide strong non-repudiation and private communication. For privacy preservation, in this paper the RTA generates the Privacy ID (PID) using the RTA's secret value and computes the signature value $\mathbf{\Gamma}$ including the PID and RSA public key. The proposed security architecture is efficient in terms of signature and verification time for safety-related messages in delay-sensitive applications.

This paper is organized as follows. The related works of VANET security are briefly reviewed in Section II. In Section III, we present the proposed security framework and secure applications in VANETs. The security and performance aspects of our scheme are discussed, and a comparison of security frameworks for VANET is shown in Session IV. Finally, the concluding remarks are presented in Section V.

II. Related Works

In [3], Zarki et al. presented the vehicular applications aimed at assisting drivers and security issues in VANETs. Furthermore, they proposed some potential security solutions: security architectures using the PKI and ID-based cryptosystem.

Actually, a number of studies for VANET security using the PKI have been proposed [4]-[10]. The IEEE P1609.2 standard specifies security services for the Wireless Access in Vehicular Environments (WAVE) networking and applications [4]. The standard proposed the issuance of short-lived certificates to reduce the overhead of CRLs. In [5] [6], Raya et al. explained the detailed threat and security requirements, and then proposed security architecture using PKI with related protocols. Specifically, they showed that PKI is suitable for VANETs through simulations of related overheads in [5]. In [6], they proposed a brief overview of novel certificate revocation protocols: Revocation Protocol of the Tamper-Proof Device (RTPD), Revocation protocol using Compressed Certificate Revocation Lists (RCCRL), and Distributed Revocation Protocol (DRP). Plößl et al. proposed security architecture that consists of three layers: basic security elements, single-hop-security, and multi-hop-security [7]. In [8], the security architecture proposed by Eichler represents a holistic approach proving all security requirements and system layer components. Wang et al. proposed authenticated session key distribution, pairwise and group keys, used in non-safety-related applications [9], which enhance the security of Raya and Hubaux's scheme [5]. The enhanced scheme provides both non-repudiation and confidentiality services. Plößl et al. also proposed an efficient security infrastructure that uses asymmetric as well as symmetric cryptosystem and tamper-resistant hardware [10]. As has been noted, although many security frameworks using PKI have been proposed, the system's availability will not be pervasive or feasible since such systems still require extra communication to manage the CRLs and have heavy overheads.

Recently, VANET security frameworks using ID-based cryptography have been introduced to avoid the overheads of PKI [12]-[16]. In ID-based cryptosystem [11], instead of certificates, the user's identifiers such as phone number and e-mail address can be used as his public key for verification and encryption. In other words, the ID-based cryptosystem simplifies the certificate management process. Kamat et al. proposed the practical ID-based security framework for VANETs [12]. They use the ID-based signcryption scheme to provide non-repudiation and confidentiality. In Kamat's scheme, a Base-Station (BS) manages CRLs of vehicles and issues new pseudonym ID and secret key using RSA encryption only if the vehicle's certificate has not been revoked. Sun et al. presented a security framework mainly consisting of privacy using the preloading pseudonym and non-repudiation assurance functionalities through an ID-based threshold signature scheme [13]. In [14][15], Lin et al. introduced conditional privacy preservation, which is called GSIS. GSIS employs the group signature between vehicles and an ID-based signature between vehicles and RSU. In [15], they also proposed the RSU-aided certificate revocation scheme. Li et al. proposed a secure and efficient communication scheme with authenticated key agreement and privacy preservation in vehicle-to-vehicle and vehicle-to-roadside device, which is called SECSPP [16]. SECSPP is based on non-interactive ID-based public-key cryptography, blind signature, and one-way hash chain. Their scheme is efficient in its implementation on vehicles, but it does not consider the need for non-repudiation between vehicles.

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 KGC, which causes the key escrow problem because the KGC issues the user's private key using the master key of the KGC [17]-[19]. Although one can provide some strong security features and prevent the need for the expensive PKI, an authorized third party can gain access to all cryptography keys. As a result, it does not perfectly guarantee the strong non-repudiation and private communication. Also, the third party can abuse its access ability. Therefore, security framework providing strong security to be used in VANETs is required.

III. A Proposed Security Architecture and Protocols

The security architecture proposed in this paper is shown Figure 1. We assume that there are vehicle registration sites and that vehicles should be registered to a RTA in the sites when they are sold. A vehicle registration site is managed by a RTA which can be a state, province, etc. Also, the vehicle should store its credential information $\mathbf{\Gamma}$ and the RTAs list including several RTA's ID and RTA's public parameter. Note that the

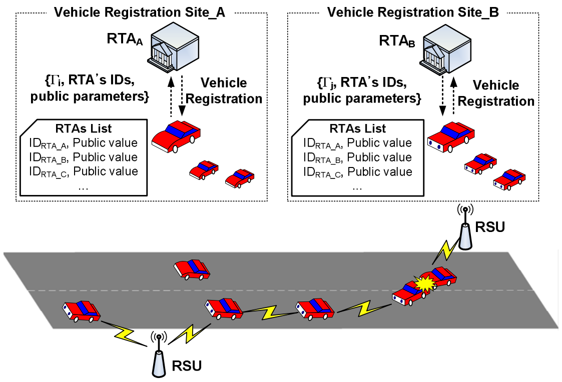
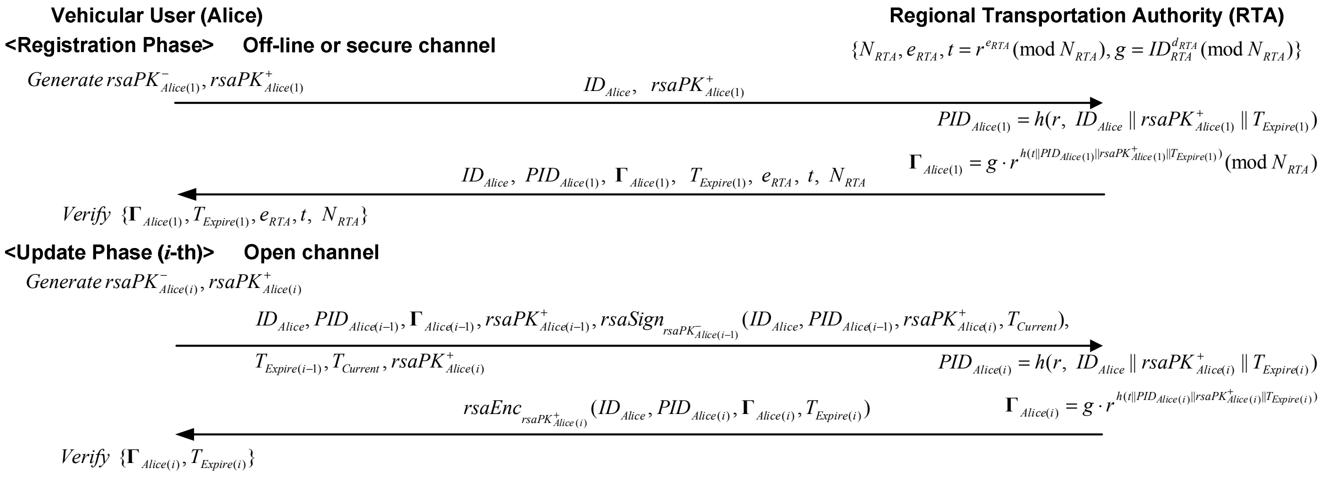

Vehicle Registration Site_A
RTA_A
{Γ_i, RTA's IDs, public parameters}
Vehicle Registration
RTAs List
ID_{RTA_A}, Public value
ID_{RTA_B}, Public value
ID_{RTA_C}, Public value
...
Vehicle Registration Site_B
RTA_B
{Γ_j, RTA's IDs, public parameters}
Vehicle Registration
RTAs List
ID_{RTA_A}, Public value
ID_{RTA_B}, Public value
ID_{RTA_C}, Public value
...
RSU
RSU

Fig. 1. Proposed security framework in VANETs.



Vehicular User (Alice)
Regional Transportation Authority (RTA)
<Registration Phase> Off-line or secure channel
$\{N_{RTA}, e_{RTA}, t = r^{e_{RTA}} (\text{mod } N_{RTA}), g = ID_{RTA}^{d_{RTA}} (\text{mod } N_{RTA})\}$
Generate $rsaPK^{-}_{Alice(1)}, rsaPK^{+}_{Alice(1)}$
$ID_{Alice}, \ rsaPK^{+}_{Alice(1)}$
$PID_{Alice(1)} = h(r, \ ID_{Alice} \parallel rsaPK^{+}_{Alice(1)} \parallel T_{Expire(1)})$
$\mathbf{\Gamma}_{Alice(1)} = g \cdot r^{h(t \parallel PID_{Alice(1)} \parallel rsaPK^{+}_{Alice(1)} \parallel T_{Expire(1)})} (\text{mod } N_{RTA})$
$ID_{Alice}, \ PID_{Alice(1)}, \ \mathbf{\Gamma}_{Alice(1)}, \ T_{Expire(1)}, \ e_{RTA}, \ t, \ N_{RTA}$
Verify $\{\mathbf{\Gamma}_{Alice(1)}, T_{Expire(1)}, e_{RTA}, t, \ N_{RTA}\}$
<Update Phase (i-th)> Open channel
Generate $rsaPK^{-}_{Alice(i)}, rsaPK^{+}_{Alice(i)}$
$ID_{Alice}, PID_{Alice(i-1)}, \mathbf{\Gamma}_{Alice(i-1)}, rsaPK^{+}_{Alice(i-1)}, rsaSign_{rsaPK^{-}_{Alice(i-1)}}(ID_{Alice}, PID_{Alice(i-1)}, rsaPK^{+}_{Alice(i)}, T_{Current}),$
$T_{Expire(i-1)}, T_{Current}, rsaPK^{+}_{Alice(i)}$
$PID_{Alice(i)} = h(r, \ ID_{Alice} \parallel rsaPK^{+}_{Alice(i)} \parallel T_{Expire(i)})$
$rsaEnc_{rsaPK^{+}_{Alice(i)}}(ID_{Alice}, PID_{Alice(i)}, \mathbf{\Gamma}_{Alice(i)}, T_{Expire(i)})$
$\mathbf{\Gamma}_{Alice(i)} = g \cdot r^{h(t \parallel PID_{Alice(i)} \parallel rsaPK^{+}_{Alice(i)} \parallel T_{Expire(i)})}$
Verify $\{\mathbf{\Gamma}_{Alice(i)}, T_{Expire(i)}\}$

Fig. 2. Registration and update phases.

list does not require much storage space since the number of RTAs managed by government is limited. In our framework, the ID-based cryptosystem is used to generate the vehicle's credential $\mathbf{\Gamma}$ and the self-generated RSA private/public keys are used for secure communications in vehicle-to-vehicle or vehicle-to-roadside environments. The use of Shamir's ID-based signature [11] in our scheme can significantly reduce the computational overhead in terms of signature and verification time in comparison with the ID-based schemes using pairing operations.

A. Preliminaries

- N: product of two large prime numbers
- e: integer satisfying $gcd(e,\varphi((N))=1$
- d: integer satisfying $ed \equiv 1(\text{mod } \varphi(N))$
- $h()$: strong one-way hash function
- ID_x: identity of node x
- PID_x: privacy identity of node x
- $rsaPK^{-}_{x}$: traditional RSA private key of node x
- $rsaPK^{+}_{x}$: traditional RSA public key of node x
- $\mathbf{\Gamma}_x$: signature value for PID_x and $rsaPK^{+}_{x}$
- $rsaSign$: RSA signature using $rsaPK^{-}_{x}$
- $rsaEnc$: RSA encryption using $rsaPK^{+}_{x}$
- T_{Expire}: validation period of the $\mathbf{\Gamma}_x$
- $T_{Current}$: current time

B. Registration Phase

The proposed system has two phases as shown in Figure 2. The RTA sets up the parameters $\{N_{RTA}, e_{RTA}, t = (r)^{e_{RTA}}, g = (ID_{RTA})^{d_{RTA}}\}$ and keeps the r, g, and d_{RTA} as the system secret key, where r is a random number. To perform the registration phase, Alice must register her vehicle to the RTA. Alice herself generates the RSA private/public keys and sends the public key with ID_{Alice} to the RTA. Receiving the parameters from Alice, the RTA computes the $PID_{Alice(1)}$ and signature $\mathbf{\Gamma}_{Alice(1)}$ by (1) and (2). The RTA does not need to maintain $PID_{Alice(1)}$ in its storage space since it can be computed by r and other public parameters. And then, the RTA sends the message including necessary data to Alice. Alice verifies the signature $\mathbf{\Gamma}_{Alice(1)}$ by (3). This registration phase is accomplished by an off-line or secure channel.

$$PID_{Alice(1)} = h(r, \ ID_{Alice} \parallel rsaPK^{+}_{Alice(1)} \parallel T_{Expire(1)}) \tag{1}$$

$$\mathbf{\Gamma}_{Alice(1)} = g \cdot r^{h(t \parallel PID_{Alice(1)} \parallel rsaPK^{+}_{Alice(1)} \parallel T_{Expire(1)})} (\text{mod } N_{RTA}) \tag{2}$$

$$(\mathbf{\Gamma}_{Alice(1)})^{e_{RTA}} \equiv ID_{RTA} \cdot t^{h(t \parallel PID_{Alice(1)} \parallel rsaPK^{+}_{Alice(1)} \parallel T_{Expire(1)})} (\text{mod } N_{RTA}) \tag{3}$$

C. Update Phase

We consider the update phase in which to issue the new vehicle's private and public keys. We define the lifetime T_{Expire}, for a shorter period, such as every few days of the week or every month. The private key will be valid only during the designated lifetime. In the existing security frameworks using an ID-based cryptosystem, if the user's private key is compromised, the user should obtain the new private key through a secure channel. However, our scheme allows vehicular user to update his/her signature $\mathbf{\Gamma}$ without requiring a secure channel.

When she wants to update her private and public keys, Alice herself generates the i-th RSA private/public key, computes the traditional RSA signature with ID_{Alice}, $PID_{Alice(i\text{-}1)}$, $rsaPK^{+}_{Alice(i)}$, and $T_{Current}$ using her private key $rsaPK^{-}_{Alice(i\text{-}1)}$, and sends the necessary parameters as shown in Figure 2 to the RTA through the open channel. The RTA checks the current time and verifies the $(i\text{-}1)$-th signature $\mathbf{\Gamma}_{Alice(i\text{-}1)}$ using its ID. If successful, the RTA verifies the RSA signature value including ID_{Alice}, $PID_{Alice(i\text{-}1)}$, and new public key $rsaPK^{+}_{Alice(i)}$ using Alice's previous public key $rsaPK^{+}_{Alice(i\text{-}1)}$. If successful, the RTA generates Alice's new $PID_{Alice(i)}$ as the (1). Also, the new public key $rsaPK^{+}_{Alice(i)}$ is certified by computing $\mathbf{\Gamma}_{Alice(i)}$ as the equation (2). The RTA encrypts the values $\{ID_{Alice}$, $PID_{Alice(i)}$, $\mathbf{\Gamma}_{Alice(i)}$, $T_{Expire(i)}\}$ using Alice's new public key and sends them to Alice. Receiving the message, Alice verifies the new credential $\mathbf{\Gamma}_{Alice(i)}$ by (3) and uses the new privacy ID and RSA key pair for their life time.

D. Secure Applications in VANETs

In this paper, we present secure applications such as collision avoidance and transmission of traffic information with strong non-repudiation and privacy. Also, we introduce emergency vehicle signal preemption with strong non-repudiation.

If a car accident occurs in front of Alice's vehicle, Alice simply broadcasts the alarm message *M* including the accident event. Upon receiving the secure flooding message, other vehicles authenticate Alice by verifying $\mathbf{\Gamma}_{Alice(i)}$ using the RTA ID and public parameters stored in their list of RTAs. If successful, they check the signature value using Alice's RSA public key and take appropriate action. Also, it is possible for Alice to provide the traffic information to the roadside unit (RSU). Note that Alice, using $PID_{Alice(i)}$, can notify other vehicles or RSU of these information without disclosing her original ID.

$$Alice \rightarrow * \;\; or \;\; Alice \rightarrow RSU :$$

$$PID_{Alice(i)}, \mathbf{\Gamma}_{Alice(i)}, ID_{RTA\_A}, rsaPK^{+}_{Alice(i)}, rsaSign_{rsaPK^{-}_{Alice(i)}}(M, T_{Current}), M, T_{Current}, T_{Expire(i)}$$

A Traffic Light (TL) can be controlled by an emergency vehicle (EV) such as ambulance, fire vehicle, and police car to provide traffic priority in emergency situations. In the case of emergency vehicle signal preemption, the traffic light has to authenticate the emergency vehicle requiring special traffic priority. In this case, it is not necessary to provide privacy to emergency vehicles and traffic lights. For these scenarios, emergency vehicles register themselves with their original ID to the special RTA such as a fire department and police headquarter. When emergency vehicles want to control a traffic light, the emergency vehicles and traffic light exchange authenticated control messages *M* using the their signature **Γ**.

$$EV \rightarrow TL :$$

$$ID_{EV}, \mathbf{\Gamma}_{EV(i)}, ID_{special\_RTA}, rsaPK^{+}_{EV(i)}, rsaSign_{rsaPK^{-}_{EV(i)}}(M, T_{Current}), M, T_{Current}, T_{Expire(i)}$$

$$TL \rightarrow EV :$$

$$ID_{TL}, \mathbf{\Gamma}_{TL(j)}, ID_{RTA\_C}, rsaPK^{+}_{TL(j)}, rsaSign_{rsaPK^{-}_{TL(j)}}(M, T_{Current}), M, T_{Current}, T_{Expire(j)}$$

IV. Discussion on Security and Performance

A. Security Considerations

The proposed scheme addresses the key escrow problem in comparison with the existing related proposals. In our scheme, the RTA which acts as the third party does not generate the private keys of vehicles and roadside devices. Instead, they make only the signature **Γ** of the user's public key using the ID-based signature scheme. Users then authenticate each other by verifying their IDs and RSA public keys using their RTA's ID. Therefore, our scheme ensures that strong non-repudiation and private communication are supported.

In the proposed scheme, an attacker could not abuse the user's private key after the lifetime of the **Γ** since the RSA private key of VANET node is frequently updated every T_{Expire}. It is possible for an attacker to renew the user's private key using the compromised private key. The legacy user, however, can perceive that his private key is compromised when the duplicate update procedure is performed by someone other than himself. There is an ID revocation problem in ID-based schemes. In existing ID-based systems, changing a vehicle's ID is required when its private key is compromised. But, the VANET node in our scheme updates only its new private and public keys without changing its ID.

Our scheme provides the conditional privacy function using the PID. The RTA generates the PID using its secret value *r*, user's original *ID*, user's public key, and T_{Expire} every update phase. It is impossible for other users to guess the user's original ID through PID since they do not know the secret value *r*. When car accidents and crimes occur, the RTA can trace the user by computing the PID with the public parameters of PID and all IDs registered in the RTA.

It is not necessary to establish a secure channel between the VANET nodes and RTA to update their private/public keys after the first registration phase. The value **Γ** plays an important role in the trust relationship among VANET nodes including the vehicle, roadside device, and RTA. To verify the **Γ**, all nodes have only the RTA's IDs and public parameters such as N_{RTA}, e_{RTA}, and *t*, which do not require any secure channel.

Although the proposed scheme solves the inherent weakness of IBC, it loses the advantage of IBC since a vehicle's ID can't be used as its public key.

B. Performance Considerations

It is important to reduce the signature and verification time of safety-related messages in delay-sensitive applications. We obtained time cost of cryptography operation by the experiment using MIRACL library [20] on a Pentium IV 3GHz in Table 1. Also, we compared the proposed scheme with the existing security architecture from the viewpoint of signature and verification time shown in Table 2. Li's scheme is excluded from our comparison since it does not provide the non-repudiation. Table 2 clearly shows that our scheme is a more efficient in terms of signature and verification time.

The proposed security architecture achieves low storage and communication overheads. The RTA has its secret key and public values, and the vehicles and roadside devices should store their RSA key pairs, the **Γ**, the RTA's ID list including the IDs and public parameters of RTA, none of which require much storage space. Also, extra communication with the RTA to query on the **Γ** status does not be required when VANET nodes are about to communicate with other nodes.

TABLE I
The Time Costs of Cryptography Operations (Security Size: 1024 bit)

T_E	T_{RS}	T_{RV}	T_M	T_P
0.463 ms	3.897 ms	0.206 ms	0.365 ms	12.628 ms

TABLE II
Comparison of Signature & Verification Time

Kamat *et al.*	$T_{sign} = 2T_M\,(1T_M)^*$ $T_{ver} = 2T_P$	$T_{total} = 25.986\ ms$ $(25.621\ ms)^*$
Sun *et al.*	$T_{sign} = 1T_P{+}1T_M\,(1T_M)^*$ $T_{ver} = 2T_P$	$T_{total} = 38.249\ ms$ $(25.621\ ms)^*$
Lin *et al.*	$T_{sign} = 1T_E{+}1T_M\,(1T_M)^*$ $T_{ver} = 1T_P{+}1T_E$	$T_{total} = 13.919\ ms$ $(13.456\ ms)^*$
Our scheme	$T_{sign} = 1T_{RS}$ $T_{ver} = 2T_{RV}{+}1T_E$	$T_{total} = 4.772\ ms$ $(4.772\ ms)^*$

T_M: Elliptic Curve point multiplication, T_P: tate pairing,
T_E: modular exponentiation, T_{RS}: RSA signature, T_{RV}: RSA verification,
*: optimized time cost by pre-computation

C. Comparison

In this subsection, we briefly compare the proposed security framework with other proposals except PKI-based schemes. All existing security frameworks suffer from the key escrow

TABLE III
COMPARISON ON SECURITY FRAMEWORKS IN V2V NETWORKS

	Kamat *et al.* [12]	Sun *et al.* [13]	Lin *et al.* [14]	Li *et al.* [16]	Our scheme
Key escrow problem	△	○	○	○	X
Secure key distribution problem	X	X	○	○	X
IBC private key revocation problem	X	X	○	○	X
ID revocation problem	X	X	○	○	X
Non-repudiation	○	○	○	X	○
Conditional privacy	○	○	○	X	○

problem. In [2], although the RTA does not store a vehicle's RSA private key, the private key of ID-based cryptosystem is generated by a base-station. Therefore, Kamat's scheme suffers from the key escrow problem when the vehicle uses ID-based cryptosystem for secure communication. Kamat et al. scheme does not require a secure channel to transmit the private key of ID-based cryptosystem since it uses a certificate based on PKI. However, our proposed framework is secure against these problems since it allows the vehicle to itself generate the RSA private/public key and to update its RSA key without requiring a secure channel. Therefore, all the existing security frameworks using an ID-based cryptosystem are limited to the small and closed networks in which the KGC is unconditionally trusted. Kamat's, Sun's, and our schemes provide the solution for two revocation problems. These systems employ the short-lived replenishment for the private key revocation and, to deal with the ID revocation problem, don't use a vehicle's original ID to generate its private key. Li's scheme focuses on authenticated key establishment and privacy without non-repudiation.

Kamat's, Sun's, and Lin's schemes using the pairing operation are computationally expensive and highly theoretical, while the proposed scheme is efficient in terms of signature and verification time since it employs the RSA algorithm instead of pairing operations.

V. CONCLUSION

This paper proposed a security framework with strong non-repudiation and privacy in VANETs. The key idea is that it uses a trusted third-party ID in ID-based cryptosystems to verify a vehicle's ID and self-generated RSA public key. Our scheme provides strong non-repudiation and private communication without an inherent weakness such as the key escrow problem. For privacy preservation, the RTA computes a privacy ID using its secret key. Also, the proposed security scheme is a more efficient security framework in terms of signature and verification time for safety-related applications.

ACKNOWLEDGMENT

This work was supported by the Korea Science and Engineering Foundation (KOSEF) grant funded by the Korea government (MEST) (No.R01-2007-000-11504-0), and partly supported by the IT R&D program of MKE/IITA [2008-F-015 -01, Research on Ubiquitous Mobility Management Methods for Higher Service Availability].

REFERENCES

[1] National ITS Architecture, <http://www.odetics-its.com/itsarch/html/standard/standard.htm>.

[2] Car 2 Car Communication Consortium, <http://www.car-2-car.org/>

[3] M.E. Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, ″Security issues in a future vehicular network,″ in *Proc. European Wireless 2002*, Feb. 2002.

[4] IEEE Std 1609.2, IEEE Trial-use standard for wireless access in vehicular environments - Security services for applications and management messages, 2006.

[5] M. Raya and J.P. Hubaux, ″The security of vehicular ad hoc networks,″ in *Proc. SASN 2005*, Nov. 2005.

[6] M. Raya, P. Papadimitratos, and J.P. Hubaux, ″Securing vehicular communications,″ *IEEE Wirel. Commun.*, vol. 13, no. 5, pp. 8-15, Oct. 2006.

[7] K. Plößl, T. Nowey, and C. Mletzko, ″Towards a security architecture for vehicular ad hoc networks,″ in *Proc. ARES2006*, 2006.

[8] S. Eichler, ″A security architecture concept for vehicular network nodes,″ in *Proc. 6th ICICS*, 2007.

[9] N.W. Wang, Y.M. Huang, and W.M. Chen, ″A novel secure communication scheme in vehicular ad hoc network,″ *Comput. Commun.*, Available online 16 December 2007: http://www. elsvier.com.

[10] K. Plößl and H. Federrath, ″A privacy aware and efficient security infrastructure for vehicular ad hoc networks,″ *Comput. Stand. Interfaces*, Available online 8 March 2008: http://www.elsvier.com.

[11] A. Shamir, ″Identity-based cryptosystems and signature schemes,″ in *Proc. CRYPTO'84*, *LNCS 196*, pp. 47-53, 1984.

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

[13] 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.

[14] 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.

[15] 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.

[16] C.T. Li, M.S. Hwang, and Y.P. Chu, ″A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks,″ *Comput. Commun.*, vol. 31, no. 12, pp. 2803-2814, July 2008.

[17] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo, ″A survey of Identity-based cryptography,″ in *Proc. AUUG 2004*, pp. 95-102, 2004.

[18] S. Al-Riyami and K. Paterson, ″Certificateless public key cryptography,″ in *Proc. Asiacrypt 2003*, *LNCS 2894*, pp. 452-473, Dec. 2003.

[19] C. Gentry, ″Certificate-based encryption and the certificate revocation problem,″ in *Proc. EUROCRYPT 2003*, *LNCS 2656*, pp. 272-293, May 2003.

[20] MIRACL, Multiprecision Integer and Rational Arithmetic C/c++ library, http://www.shamus.ie.