This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2008 proceedings.

An Efficient Identity-based Batch Verification Scheme for Vehicular Sensor Networks

Chenxi Zhang, Rongxing Lu, Xiaodong Lin, Pin-Han Ho, and Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
Email: c14zhang@engmail.uwaterloo.ca, {rxlu, xdlin, pinhan, xshen}@bbcr.uwaterloo.ca

***Abstract*—With the adoption of state-of-the-art telecommunication technologies for sensing and collecting traffic related information, Vehicular Sensor Networks (VSNs) have emerged as a new application scenario that is envisioned to revolutionize the human driving experiences and traffic flow control systems. To avoid any possible malicious attack and resource abuse, employing a digital signature scheme is widely recognized as the most effective approach for VSNs to achieve authentication, integrity, and validity. However, when the number of signatures received by a Roadside Unit (RSU) becomes large, a scalability problem emerges immediately, where the RSU could be difficult to sequentially verify each received signature within 300 ms interval according to the current Dedicated Short Range Communications (DSRC) broadcast protocol. In this paper, we introduce an efficient batch signature verification scheme for communications between vehicles and RSUs (or termed vehicle-to-Infrastructure (V2I) communications), in which an RSU can verify multiple received signatures at the same time such that the total verification time can be dramatically reduced. We demonstrate that the proposed scheme can achieve conditional privacy preservation that is essential in VSNs, where each message launched by a vehicle is mapped to a distinct pseudo identity, while a trust authority can always retrieve the real identity of a vehicle from any pseudo identity. With the proposed scheme, since identity-based cryptography is employed in generating private keys for pseudo identities, certificates are not needed and thus transmission overhead can be significantly reduced.**

I. Introduction

With the advancement and wide deployment of wireless communication technologies, car manufactures and telecommunication industries recently gear up to equip each vehicle with wireless devices that allow vehicles to communicate with each other as well as with the roadside infrastructure in order to enhance driving safety and improve drivers' driving experiences [1]. Such vehicular communication networks, which are also referred to as Vehicular Ad Hoc Networks (VANETs), inherently provide us a perfect way to collect dynamic traffic information and sense various physical quantities related to traffic distribution with very low cost and high accuracy. Such functionalities simply turn a VANET into a Vehicular Sensor Network (VSN) [2], which is considered essential for achieving automatic and dynamic information collection and fusion in an Intelligent Transportation System (ITS) [3]. VSNs have been envisioned to have a great potential to revolutionize human's driving experiences and create a fresh new framework in metropolitan-area traffic flow control, and will undoubtedly take an important part of the future wireless metropolitan-area networks.

According to the Dedicated Short Range Communications (DSRC) [4] protocol, each vehicle in a VANET broadcasts a traffic safety message every 100-300 ms, which keeps the vehicle's driving related information, such as location, speed, turning intention, and driving status (e.g., regular driving, waiting for a traffic light, traffic jam, etc.), to other vehicles. With multi-hop forwarding, the messages will be either terminated by an RSU or dropped when exceeding over their lifetimes. When receiving a message, the RSU can either react to it if the sending vehicle of the message is nearby with some requests that can be handled locally (e.g., requesting to turn the traffic light to green in case no any traffic from the other direction of the intersection, and requesting for local map information, etc.), or deliver the information to a traffic control center if the message is considered to contain any possible useful information. The RSU can also monitor and summarize the traffic situation of where it is located and report it to the traffic control center. With all the collected traffic related information, the traffic control center can generate an optimized control and management strategy for traffic light control by analyzing the current traffic load in each intersection. In addition to traffic information collection for traffic flow analysis and control, VSNs can equip current transportation systems with many new value-added functionalities, such as serving as a virtual "black box" for each vehicle which keeps the driving record for resolving any possible traffic dispute and reconstructing scene of accidents.

Although VANETs that support VSNs have been taken as the candidate for implementing the future context-aware intelligent traffic information collection system, many challenging security and privacy issues in VANETs have been identified [5]–[15], which have to be well addressed before the implementation of VSNs can be put in a practical scenario for vehicular sensor networking purposes. To ensure both identity authentication and message integrity in VSNs, one appealing solution is to sign each message with a digital signature technique before the message is sent. However, conventional signature schemes that verify the received messages one after the other may fail to satisfy the stringent time requirement of the vehicular communication applications. Note that an RSU could communicate with hundreds of On Board Units (OBUs) [16] (the communication devices on the vehicles), each sending a safety related message to the RSU every 100-

978-1-4244-2026-1/08/$25.00 © 2008 IEEE

300 ms. In this case, verifying a large number of signatures sequentially could take a long time and will certainly become the processing bottleneck at the RSUs. For instance, in a high density traffic scenario, there could be roughly 180 vehicles keeping within the communication range of an RSU, and each vehicle is sending a message every 300 ms. This means a verifier (such as an RSU) has to verify 600 messages per second, which is obviously a tough requirement for any current digital signature scheme. In addition, the maintenance of public key certificates under the traditional Public Key Infrastructure (PKI) also incurs huge communication overhead.

In order to tackle the above mentioned problems and make VSNs suitable for the intelligent traffic systems, this paper introduces an efficient batch signature verification scheme for the communications between vehicles and RSUs. Our scheme has the following unparalleled features: 1) Multiple signatures can be verified at the same time instead of one after the other as that in the previously reported approaches. Therefore, the signature verification speed can be significantly improved such that the computational workload of the RSUs can be alleviated; 2) By generating distinct pseudo identities and the corresponding private keys for signing each message with a tamper-proof device, privacy regarding user identity and location of the vehicles can be protected; 3) The identities of the vehicles can be uniquely revealed by the trusted authorities under exceptional cases; and 4) Since identity-based cryptography is employed by the tamper-proof device, efforts on certificate management and the transmission overhead can be significantly reduced.

The remainder of the paper is organized as follows. In Section II, background and preliminary knowledge related to the proposed research is given, including the network model, pairing technique, batch verification, and security requirements. In Section III, the proposed batch verification scheme is described in details. In Section IV, the security of the proposed scheme is analyzed. In Section V, the performance evaluation is presented. Section V surveys the related work. Finally, Section VII concludes the paper and presents future work.

II. Background and Preliminaries

A. Network Model

We introduce a two-layer vehicular network model, as shown in Figure 1. The lower layer is composed of vehicles and RSUs. The communication among them is based on the DSRC protocol. Each vehicle has its own public keys and private keys, with which all messages are signed and then sent to its neighboring RSU. Each RSU receiving the traffic related information is responsible for verifying the digital signatures of the messages.

In general, the top layer is comprised of application servers (such as traffic control analysis center), and a Trust Authority (TA). The RSUs communicate with an application server and TA using a secure transmission protocols, such as the wired Transport Layer Security (TLS) protocol. The RSUs are responsible for forwarding the valid messages received from OBUs to the application server. The application server is responsible for making further analysis and/or giving feedbacks to RSUs after collecting the traffic related information such as current time, location, traffic accidents, traffic distribution, and road weather information [17] from the RSUs. For instance, the application server can aid to gather and analyze the traffic density of a whole city, and predict the traffic distribution in order to optimize the traffic light control. We assume that the TA is always trusted and can never be compromised, which is responsible for assigning master private keys for the OBUs.

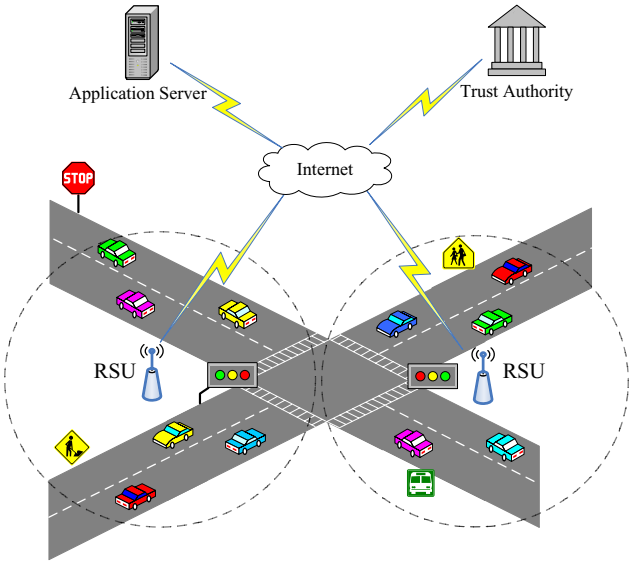

Fig. 1. The network model

B. Security Requirements

The vehicles to RSUs communication scenario is subject to the following three security requirements: *message authentication*, *identity privacy preserving*, and *traceability*, which are further discussed as below.

Message authentication: Messages from vehicles have to be authenticated to confirm that they are indeed sent unaltered by legitimate entities for the RSUs. In addition, when the number of vehicle increases, the speed of RSUs for signature verification should be faster in order to avoid any possible performance bottleneck.

Identity privacy preserving: In vehicular communication, due to its broadcasting nature, overhearing an identity-specific information could happen frequently. If the employed signature scheme is an ordinary digital signature, the signature would easily leak one's identity information [18]. Even though a pseudo identity is employed as a mask, an outside observer can also link multiple signatures to one vehicle through traffic analysis. This issue is called linkability, which may incur a location privacy violation problem [19]. Therefore, identity privacy preserving is required.

Traceability: The TA should have the ability to retrieve a vehicle's real identity from its pseudo identity when the

signature is in dispute or when the content of a message is bogus.

In this paper, we aim to address all the aforementioned issues.

C. Bilinear Maps

Since bilinear maps work as the basis of our proposed scheme in this paper, we briefly introduce the bilinear maps in this section.

Let $\mathbb{G}$ be a cyclic additive group generated by P, and $\mathbb{G}_T$ be a cyclic multiplicative group. $\mathbb{G}$ and $\mathbb{G}_T$ have the same prime order q, i.e., $|\mathbb{G}| = |\mathbb{G}_T| = q$. Let $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be an bilinear map, which satisfies the following properties:

- *Bilinear*: For all $P,\ Q,\ R \in \mathbb{G}$, and $a, b \in \mathbb{Z}$, $\hat{e}(Q, P + R) = \hat{e}(P + R, Q) = \hat{e}(P, Q) \cdot \hat{e}(R, Q)$. In particular, $\hat{e}(aP, bP) = \hat{e}(P, bP)^a = \hat{e}(aP, P)^b = \hat{e}(P, P)^{ab}$.
- *Non-degenerate*: There exist $P,\ Q \in \mathbb{G}$ such that $\hat{e}(P, Q) \neq 1_{\mathbb{G}_T}$.
- *Computable*: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P,\ Q \in \mathbb{G}$.

Such an bilinear map $\hat{e}$ is called an admissible pairing, and can be constructed by the modified Weil [20] or Tate pairings [21] on elliptic curves. The group that possesses such a map $\hat{e}$ is called a bilinear group, on which the Decisional Diffie-Hellman (DDH) problem is easy to solve while the Computational Diffie-Hellman (CDH) problem is believed hard [22]. For example, given $P, aP, bP, cP \in \mathbb{G}$ and any $a, b, c \in \mathbb{Z}_p$, there exists an efficient algorithm to determine whether $ab = c \bmod q$ by checking $\hat{e}(aP, bP) \stackrel{?}{=} \hat{e}(P, cP)$, while there exists no algorithm that can compute $abP \in \mathbb{G}$ with non-negligible probability within polynomial time.

D. Batch Verification

With the pervasiveness of telecommunication applications, the demand and requirement on authentication for communication security become more stringent. The delay caused by verification of a bulk of signatures may dramatically impede transmission throughput and impair the system applicability. In order to speed up the process of verification, a batch verification scheme should be a good alternative solution since it can verify all the signatures received in a time window with rather short time compared to verify each signature one after the other. The batch cryptography based on RSA was introduced by Fiat [23] in 1989. Some other batch signature schemes were proposed later [24]–[28]. The latest batch verification scheme proposed in [29] is based on the CL signature scheme [30], and is the first solution on batch verification without using random oracles, in which the computation efficiency can be significantly improved. For instance, 3 pairing operations are required to verify a single signature. With the batch verification scheme of [29], verifying n signatures also takes 3 pairing operations instead of $3n$ pairing operations. In other words, the verification time of the dominant operation (i.e., paring) is independent of the number of signatures to verify. Therefore, the batch verification can dramatically decrease the time spent on verifying a large number of signatures, which can achieve much better scalability. In this paper, we propose an efficient identity-based batch verification scheme based on the improved CL signature scheme in [29].

III. Batch Verification for Traffic Information Messages

In this section, we propose a novel Identity-based Batch Verification (IBV) scheme for traffic related message transmission. The proposed scheme includes the following four phases: the key generation and pre-distribution phase, the pseudo identity and private key generation phase, the message signing phase, and the batch verification phase. The notations throughout this paper are listed in Table I.

TABLE I
NOTATIONS

Notation	Descriptions
V_i:	The *i*th vehicle
RSU:	A roadside unit
TA:	A trust authority
$\mathbb{G}$:	A cyclic additive group
$\mathbb{G}_T$:	A cyclic multiplicative group
P:	The generator of the cyclic additive group $\mathbb{G}$
$\hat{e}$:	A bilinear map: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$
q:	The order of the group $\mathbb{G}$
r:	A random nonce
s_i:	The *i*th private master key of the tamper-proof device, where *i* is equal to 1 or 2
P_{pubi}:	The *i*th public key of the TA, where *i* is equal to 1 or 2
RID:	The real identity of the vehicle
PWD:	A password or authentication credential used to activate a tamper-proof device
ID^i:	A pseudo identity of the vehicle V_i
ID^i_j:	A part of the ID^i, such that $ID^i = (ID^i_1, ID^i_2)$
SK_i:	A private key of the vehicle V_i
SK^i_j:	A part of the SK^i, such that $SK^i = (SK^i_1, SK^i_2)$
$\mathcal{M}_i$:	A message sent by the vehicle V_i
$h(.)$:	A one-way hash function such that SHA-1 [31]
$H(.)$:	A MapToPoint hash [22] function such as $H : \{0,1\}^* \rightarrow \mathbb{G}$
$\|\|$:	Message concatenation operation, which appends several messages together in a special format

A. Key Generation and Pre-distribution

Firstly, let each vehicle be equipped with a tamper-proof device, which is secure against any compromise attempt in any circumstance. With the tamper-proof device on vehicles, an adversary cannot extract any data stored in the device including key material, data, and code [5], [7]. We assume that there is a trust authority (TA) which is in charge of checking the vehicle's identity, and generating and pre-distributing the private master keys of the vehicles. Prior to the network deployment, the TA sets up the system parameters for each RSU and OBU as follows:

- Let $\mathbb{G}$ be a cyclic additive group generated by P, $\mathbb{G}_T$ be a cyclic multiplicative group, and $\mathbb{G}$ and $\mathbb{G}_T$ have the same order q. Let $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a bilinear map.
- The TA first randomly chooses $s_1, s_2 \in \mathbb{Z}^*_q$ as its two master keys, and computes $P_{pub1} = s_1 P, P_{pub2} = s_2 P$

as its public keys. These two master keys of the TA are then loaded in the vehicles' tamper-proof device.

- Each RSU and vehicle are preloaded with the public parameters $\{\mathbb{G}, \mathbb{G}_T, q, P, P_{pub1}, P_{pub2}\}$. In addition, the tamper-proof device of each vehicle is preloaded with the parameters $\{s_1, s_2\}$.
- To activate the tamper-proof device, each vehicle is assigned with a real identity, denoted as $RID \in \mathbb{G}$, and a password, denoted as *PWD*, where the *RID* uniquely identifies the vehicle, while the *PWD* is required in the authentication process by the tamper-proof device. Therefore, an adversary cannot take advantages of the tamper-proof device even if the vehicle is stolen.

B. Pseudo Identity Generation

To achieve privacy preservation, we exploit to use the tamper-proof device, which is responsible for generating random pseudo identities and corresponding private keys based on identity-based cryptography [20]. The tamper-proof device is composed of three secure modules: an authentication module, a pseudo identity generation module, and a private key generation module as shown in Figure 2, which are further described in details as follows.

Authentication module: The authentication module works as an access control mechanism. A vehicle inputs its unique real identity *RID* and the password *PWD* to initiate the device, where the *PWD* can be the signature of the *RID* signed by the TA. If the *RID* and *PWD* successfully pass the verification of the authentication module, the *RID* is delivered to the next module, the pseudo identity generation module. Otherwise, the device denies providing services for the vehicle. Obviously, the authentication module enhances the security of the tamper-proof device since a malicious adversary cannot take advantages of it even though the tamper-proof device is physically held by the adversary.

Pseudo identity generation module: This module is responsible for generating a list of random pseudo identities from the authenticated *RID*. Each pseudo identity *ID* is composed of ID_1 and ID_2. In this module, the ElGamal encryption algorithm [32] over the ECC [33] is employed to encrypt the *RID* as shown in Figure 2. The two items of the cipher texts are taken as ID_1 and ID_2, respectively. In other words, we have $ID_1 = rP$, and $ID_2 = RID \oplus H(rP_{pub1})$, where r is a random nonce. r is changed each time and guarantees the distinction of ID_1 and ID_2 for each pseudo *ID*. $\oplus$ is an Exclusive-OR (XOR) operation. Here, P and P_{pub1} are the public parameters preloaded by the TA. After the encryption, ID_1 and ID_2 are delivered to the private key generation module.

Private key generation module: In this module, identity-based cryptography [20] is employed. Since a pseudo identity has two parts (i.e., ID_1 and ID_2), the private key generation module is responsible for computing a private key based on ID_1 and ID_2. Thus, the resultant private key also contains two parts, which are denoted as SK_1 and SK_2, respectively. As shown in Figure 2, SK_1 and SK_2 are equal to $s_1 ID_1$ and $s_2 H(ID_1 || ID_2)$, respectively.

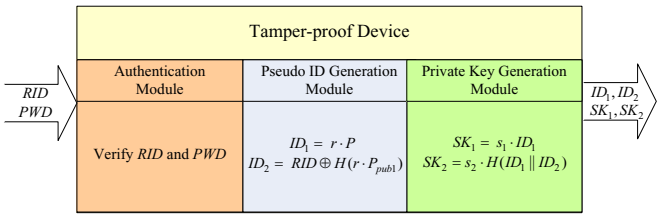

Fig. 2. The tamper-proof device

Finally, a vehicle can obtain a list of pseudo identities ID=(ID_1,ID_2) along with the corresponding private keys SK=(SK_1,SK_2). Note that the pseudo identities and the private keys can be generated offline by the tamper-proof device; thus, no delay will be caused in the signing messages at the OBU side due to this process.

C. Message Signing

When vehicles are traveling on the road, they periodically broadcast traffic related information that may potentially affect the decision making and traffic distribution optimization at the traffic control center. To ensure the integrity of the messages, each message sent by a vehicle should be signed and verified when being received. With the proposed IBV scheme, the message signing phase is presented as follows.

1) A vehicle, denoted by V_i, first generates the traffic related message denoted by $\mathcal{M}_i$.
2) V_i picks a pseudo identity ID^i=(ID_1^i,ID_2^i) and the corresponding private key SK^i=(SK_1^i,SK_2^i) by way of the tamper-proof device.
3) With the private key SK^i=(SK_1^i,SK_2^i), V_i can compute the signature σ_i of the message $\mathcal{M}_i$, where
$$\sigma_i \quad = \quad SK_1^i + h(\mathcal{M}_i) SK_2^i \ .$$
4) Subsequently, V_i sends the final message $\langle ID^i, \mathcal{M}_i, \sigma_i \rangle$ to its neighboring RSU.
5) These steps are repeated every 100-300 ms according to the DSRC [4].

The signature of the proposed IBV scheme has the following merits. Firstly, the signature overhead is very low. Compared with the ECDSA signature scheme of IEEE1609.2 [34], which is the current standard for VANETs, the length of a signature in the IBV scheme is a half of that of the ECDSA, i.e., $|\sigma_i| = 161$ bits ≈ 21 bytes.[1] However, the IBV scheme does not need any signature certificate to be sent along with the message due to the adoption of identity-based cryptography; instead, only a short-length pseudo identity is sent, which is of a length 42 bytes, i.e., $|ID^i| = |ID_1^i| + |ID_2^i| = 42$ bytes. In contrast, the ECDSA scheme has to incorporate a certificate in the message, which is 125 bytes long in the case of using the

[1]Note that with the IBV scheme, in order to get a short signature, we use an MNT curve [35] with 160-bit q, where the bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is asymmetric, $\mathbb{G}_1 \neq \mathbb{G}_2$, and elements in $\mathbb{G}_1$ are 161 bits long.

certificate presented in IEEE 1609.2 Standard [34]. We will further compare our proposed IBV scheme with the ECDSA scheme in terms of the communication overhead in Section V.

Secondly, from the perspective of signing speed, the proposed IBV scheme does not add any extra signature generation delay compared with that in ECDSA, where both of them need two multiplication operations on an elliptic curve. At last, the signature of the IBV scheme does not leak any real identity information of the vehicle because a pseudo identity is used in the scheme. Furthermore, since all the messages are signed with different pseudo identities, thus none of the two messages can be connected to a single vehicle with the IBV signature scheme, which is expected to successfully address the issue of privacy preservation in VANETs.

D. Batch Verification

Based on the network architecture as described in Section II, once an RSU receives a traffic related message from a vehicle, the RSU has to verify the signature of the message to ensure that the corresponding vehicle is not attempting to impersonate any other legitimate vehicle or disseminating bogus messages, which may result in tremendous impairment. For ease of presentation, we first introduce the single signature verification process, followed by the presentation on the batch verification of multiple signatures signed by distinct vehicles on different messages.

Single signature verification: Given the system public parameters $\{\mathbb{G},\ \mathbb{G}_T, q, P, P_{pub1}, P_{pub2}\}$ assigned by the TA and the message $\langle ID^i, \mathcal{M}_i, \sigma_i\rangle$ sent by the vehicle V_i, the signature σ_i is valid if $\hat{e}(\sigma_i, P) = \hat{e}(ID_1^i, P_{pub1}) \cdot \hat{e}(h(\mathcal{M}_i)H(ID_1^i||ID_2^i), P_{pub2})$, as verified below.

$$\begin{aligned} & \hat{e}(\sigma_i, P) \\ = \ & \hat{e}(SK_1^i + h(\mathcal{M}_i)SK_2^i, P) \\ = \ & \hat{e}(SK_1^i, P)\hat{e}(h(\mathcal{M}_i)SK_2^i, P) \\ = \ & \hat{e}(s_1ID_1, P)\hat{e}(h(\mathcal{M}_i)s_2H(ID_1^i||ID_2^i), P) \\ = \ & \hat{e}(ID_1^i, s_1P)\hat{e}(h(\mathcal{M}_i)H(ID_1^i||ID_2^i), s_2P) \\ = \ & \hat{e}(ID_1^i, P_{pub1})\hat{e}(h(\mathcal{M}_i)H(ID_1^i||ID_2^i), P_{pub2}) \end{aligned}$$

Therefore, the computation cost by the RSU for verifying a single signature is dominantly comprised of one MapToPoint hash [22], one multiplication, and three pairing operations. Note that the computation cost of a pairing operation is much higher than the cost of a MapToPoint hash and a multiplication operation.

Batch verification: Given n distinct messages denoted as $\langle ID^1, \mathcal{M}_1, \sigma_1\rangle$, $\langle ID^2, \mathcal{M}_2, \sigma_2\rangle$, ..., $\langle ID^n, \mathcal{M}_n, \sigma_n\rangle$, respectively, which are sent by n distinct vehicles denoted as V_1, V_2, ..., V_n, all signatures, denoted as σ_1, σ_2, ..., σ_n, are valid if $\hat{e}(\sum_{i=1}^n \sigma_i, P) = \hat{e}(\sum_{i=1}^n ID_1^i, P_{pub1}) \cdot \hat{e}(\sum_{i=1}^n h(\mathcal{M}_i)H(ID_1^i||ID_2^i), P_{pub2})$. Let HID^i denote $H(ID_1^i||ID_2^i)$. This batch verification equation follows since

$$\begin{aligned} & \hat{e}(\textstyle\sum_{i=1}^n \sigma_i, P) \\ = \ & \hat{e}(\textstyle\sum_{i=1}^n (SK_1^i + h(\mathcal{M}_i)SK_2^i), P) \\ = \ & \hat{e}(\textstyle\sum_{i=1}^n SK_1^i, P)\hat{e}(\textstyle\sum_{i=1}^n h(\mathcal{M}_i)SK_2^i, P) \\ = \ & \hat{e}(\textstyle\sum_{i=1}^n s_1ID_1^i, P)\hat{e}(\textstyle\sum_{i=1}^n s_2h(\mathcal{M}_i)HID^i, P) \\ = \ & \hat{e}(\textstyle\sum_{i=1}^n ID_1^i, s_1P)\hat{e}(\textstyle\sum_{i=1}^n h(\mathcal{M}_i)HID^i, s_2P) \\ = \ & \hat{e}(\textstyle\sum_{i=1}^n ID_1^i, P_{pub1})\hat{e}(\textstyle\sum_{i=1}^n h(\mathcal{M}_i)HID^i, P_{pub2}). \end{aligned}$$

Thus, this batch verification can dramatically reduce the verification delay, particularly when verifying a large number of signatures. From the above batch verification equation, the computation cost that the RSU spends on verifying n signatures is dominantly comprised of n MapToPoint hash, n multiplication, $3n$ addition, n one-way hash, and 3 pairing operations. This appealing property demonstrates that the verification time for multiple signatures is constant regardless of the size of the batch. Thus, the time for an RSU to verify a large number of signatures sent by the surrounding vehicles can be dramatically reduced, which can apparently reduce the message loss ratio due to the potential bottleneck of signature verification at the RSU. Another advantage is that the RSU can aggregate multiple signatures as one signature and deliver it to an application server, which can perform the batch verification on the aggregate signature. Thus, the workload of application server will also be reduced. In our scheme, the aggregate signature is equal to $\sum_{i=1}^n \sigma_i$, given n distinct signatures, σ_1, σ_2, ..., σ_n.

IV. Security Analysis

In this section, we analyze the security of the proposed batch verification scheme in terms of the following three aspects: the message authentication, the user identity privacy preservation, and the traceability by the TA.

- *Message authentication.* The message authentication is one of the basic security requirements in vehicular communications. In the proposed IBV scheme, the signature $\sigma_i = SK_1 + h(\mathcal{M})SK_2$ is actually a one-time identity-based signature. Without knowing the private key SK_1 and SK_2, it is infeasible to forge a valid signature. Because of the NP-hard computation complexity of Diffie-Hellman problem in $\mathbb{G}$, it is difficult to derive the private keys SK_1 and SK_2 by way of ID_1, P_{pub1}, P, and $H(ID_1||ID_2)$. At the same time, because $\sigma_i = SK_1 + h(\mathcal{M})SK_2$ is a Diophantine equation, by only knowing σ and $h(\mathcal{M})$, it is still difficult to get the private keys SK_1 and SK_2. Therefore, the one-time identity-based signature is unforgeable, and the property of message authentication is achieved.
- *Identity privacy preserving.* In the proposed scheme, the real identity *RID* of a vehicle is converted into two random pseudo identities ID_1 and ID_2, where $ID_1 = rP$ and $ID_2 = RID \oplus H(rP_{pub})$ for unknown r. Note that the pseudo identity pair (ID_1, ID_2) is actually an ElGamal-type ciphertext, which is semanticly secure under the chosen plaintext attacks. Therefore, without knowing the *master-key* (s_1, s_2), it is infeasible for anyone to tell the real identity from the pseudo identity pair. Also, the

linkability does not exist because the pseudo identities (ID_1, ID_2) in each signature instance is distinct. Therefore, the identity privacy preservation can be guaranteed.

- *Traceability.* Given the pseudo identity pair ID_1 and ID_2, only the TA, given the *master-key* (s_1, s_2), can trace the real identity of the vehicle by computing $ID_2 \oplus H(s_1 ID_1) = RID \oplus H(rP_{pub}) \oplus H(s_1 rP) = RID$. Therefore, once a signature is in dispute, the TA has the ability to trace the vehicle from the disputed message, in which the traceability can be well satisfied.

V. Performance Evaluation

In this section, we evaluate the performance of the IBV scheme in terms of verification delay and transmission overhead. Since the proposed scheme focuses on the signature verification process at the RSUs, it does not matter whether the VANETs support vehicle-to-vehicle communications or not. In the following evaluation, we assume all the vehicles can communication directly with the RSU.

A. Verification Delay

We define and compute the time cost of the cryptographic operations required in each verification by the proposed IBV scheme. Let T_{mul} denote the time to perform one point multiplication over an elliptic curve, T_{mtp} the time of a MapToPoint hash operation, and T_{par} the time of a pairing operation. Since these operations dominate the speed of a signature verification, we only consider these operations and neglect all the other operations such as additive and one-way hash function. We adopt the experiment in [37], which observes processing time for an MNT curve [35] of embedding degree $k = 6$ and 160-bit q, running on an Intel Pentium IV 3.0 GHZ machine. The following results are obtained: T_{mul} is 0.6 ms and T_{par} is 4.5 ms.

Next, we compare the proposed IBV scheme with ECDSA and BLS [22], [36] in terms of the verification delay. Here, the ECDSA scheme is the signature algorithm adopted by IEEE1609.2 standard [34], while BLS is a short signature scheme, which can also be used to perform signature aggregation. Table II shows the combination of the dominant operations of the three signature schemes in terms of verifying a single signature and n signatures, respectively. From the batch verification equation in Section III-V, we observe that the time to verify n distinct signatures is $3T_{\mathsf{par}}+nT_{\mathsf{mtp}}+nT_{\mathsf{mul}}$. According to [36], with BLS, the time spent on verifying n signatures is equal to $(n+1)T_{\mathsf{par}} + nT_{\mathsf{mtp}}$; while with the ECDSA, verifying distinct n signatures requires $2nT_{\mathsf{mul}}$. Since ECDSA and BLS are not identity-based signature schemes, additional operations are needed to verify the public key's certificate. Thus, the overall message verification time for ECDSA and BLS should be doubled[2] as shown in Table II.

[2]With the IBV scheme, each message sent by a vehicle corresponds to a distinct identity. Thus, to achieve the same privacy level as the IBV's, the vehicle using the public key based schemes also needs to change an identity for each sending message. That is the reason why verification time for ECDSA and BLS should be doubled in this paper.

TABLE II
Comparisons of the speed of three signature schemes (ms)

	Verify a single signature	Verify n signatures
IBV :	$3T_{\mathsf{par}} + T_{\mathsf{mtp}} + T_{\mathsf{mul}}$	$3T_{\mathsf{par}} + nT_{\mathsf{mtp}} + nT_{\mathsf{mul}}$
BLS :	$4T_{\mathsf{par}} + 2T_{\mathsf{mtp}}$	$(2n+2)T_{\mathsf{par}} + 2nT_{\mathsf{mtp}}$
ECDSA :	$4T_{\mathsf{mul}}$	$4nT_{\mathsf{mul}}$

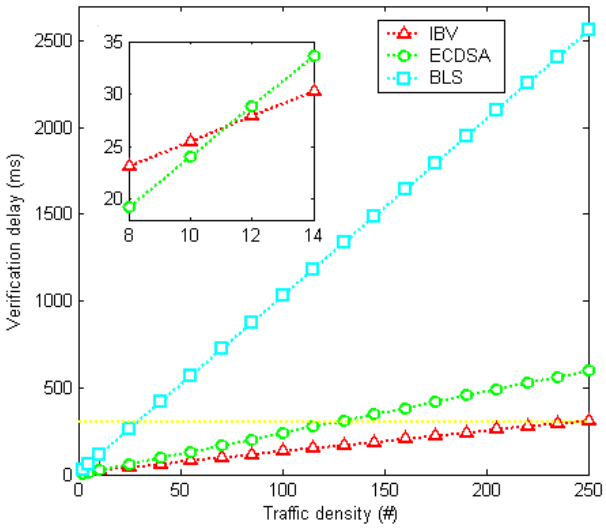

Fig. 3. Verification delay *vs.* Traffic density

In our analysis, we assume the communication coverage of an RSU is one square kilometer, and each vehicle periodically broadcasts a traffic related message every 300 ms. The traffic density is taken as the number (#) of vehicles within an RSU's radiation range. We compare the performance by using IBV, ECDSA, and BLS to verify the signatures at an RSU.

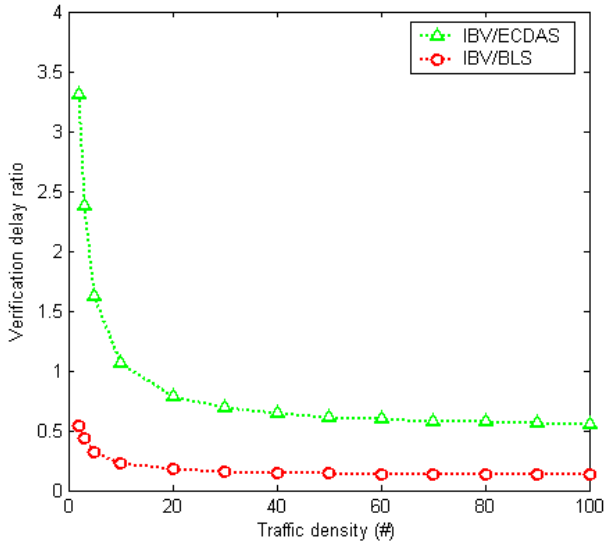

Fig. 4. Verification delay ratio *vs.* Traffic density

Figure 3 shows the relationship between the verification delay and the number of vehicles within an RSU's radiation

range. The embedded small figure is a local zoom-in with the traffic load ranging from 8 to 14. From Figure 3, we can observe that the verification delay by using BLS is always the largest no matter how many messages are received by an RSU. Another interesting result is that when the number of messages received within 300 ms is smaller than 11, the ECDSA scheme achieves the smallest message verification latency; however, when the number of messages is greater than 11, the IBV scheme yields much less verification latency. Figure 3 also shows that within a 300 ms interval, the maximum number of signatures that can be verified by the RSU is equal to 29, 125, and 239 when the BLS, ECDSA, and IBV schemes are adopted, respectively. In other words, when the number of incoming messages is greater than these maximal thresholds, some messages will be lost accordingly. Obviously, the IBV scheme can verify the largest number of signatures, which is observed to achieve the lowest message loss ratio when the traffic load increases.

One solution for the scenario when the number of messages is larger than the maximal threshold is that the RSU can leave the verification of the extra signatures to an application server, which is supposed to have powerfully parallel processors and can verify all of the leftover signatures. In this way, the RSU can relieve the computation workload by passing the unverified signatures to the application server. This solution, nonetheless, is at the expense of additional communication overhead by transmitting those signatures. This issue on the communication overhead will be tackled in the next subsection.

We compare the message verification delay of these three schemes in terms of the ratio of the verification delays as shown in Figure 4. We can see that the delay ratio between IBV and ECDSA approaches to a constant, which is approximately 0.641 when the number of messages in one interval is greater than 40. The delay ratio between IBV and BLS is approximately 0.157 when the number of messages is larger than 30. In other words, the speed of IBV is 35.6% faster than that of ECDSA, and is 84.3% faster than that of BLS.

B. Transmission Overhead

In this section, we compare the transmission overhead of the three schemes. The comparison is in terms of the following two aspects: the transmission overhead incurred by delivering the messages from a vehicle to an RSU, and the overhead incurred by delivering a message from an RSU to an application server. Here, the transmission overhead includes a signature and a certificate appended to the original message, while the message itself is not counted.

TABLE III
COMPARISONS OF TRANSMISSION OVERHEAD OF THREE SCHEMES (MS)

	Send a single message	Send n messages
IBV :	21+42 bytes	21+42n bytes
BLS :	21+125 bytes	21+125n bytes
ECDSA :	42+125 bytes	42n+125n bytes

For IBV and BLS, the length of a signature is 21 bytes, while the length for ECDSA is 42 bytes. When we use BLS or ECDSA, a certificate must be transmitted along with a signature. If we use the certificate presented in IEEE 1609.2 Standard [34], which has 125 bytes in length, the total transmission overhead of the BLS and ECDSA scheme is 21+125 bytes and 42+125 bytes, respectively, as shown in Table III. Since the proposed IBV scheme is based on identity-based cryptography, only a short pseudo identity with 42 bytes is transmitted along with the original message. Thus, the total transmission overhead of IBV is 21+42 bytes as shown in Table III.

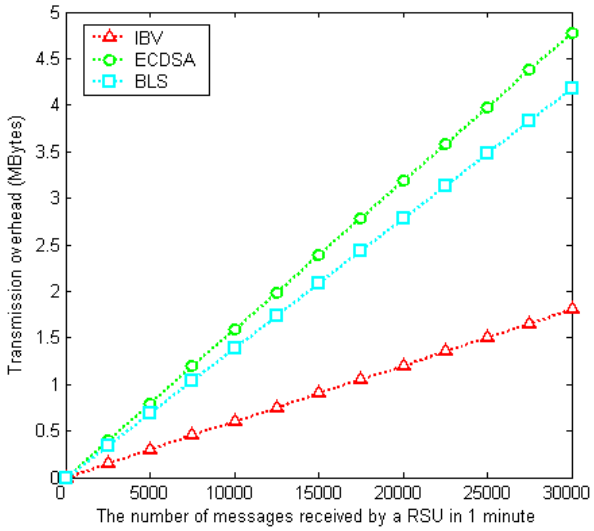

Fig. 5. Transmission overhead *vs.* the number of messages received by an RSU in 1 minute (between vehicles and an RSU)

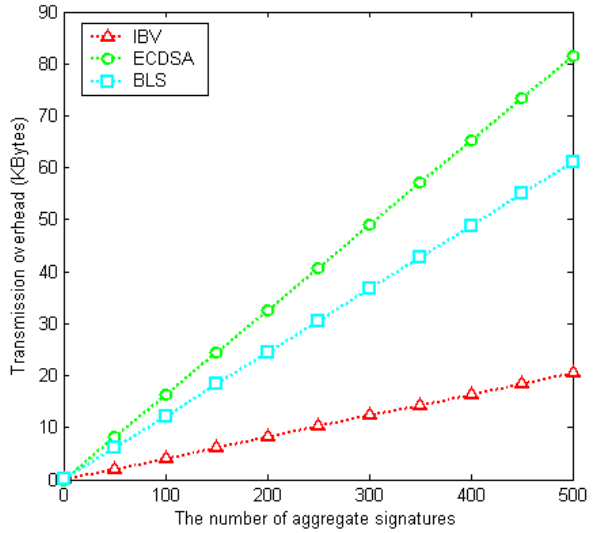

Fig. 6. Transmission overhead *vs.* the number of aggregate signatures (between an RSU and an application server)

Figure 5 shows the relationship between the transmission overhead and the number of messages received by an RSU in 1 minute. Obviously, as the number of messages increases,

the transmission overhead increases linearly. The transmission overheads of ECDSA is the largest among the three schemes, and the transmission overhead of the IBV is much smaller than the other two. We can further observe that the transmission overhead of the IBV scheme is 43.2 percent of that of BLS and 37.7 percent of that of ECDSA. On the other hand, as shown in Figure 5, within the observation window of 1 minute, when the number of messages increases up to 30000, IBV saves 2.37 Mbytes and 2.98 Mbytes of bandwidth compared with BLS and ECDSA, respectively. Here, 30000 corresponds to the number of messages sent by 150 vehicles in 1 minute.

On the other hand, when the number of messages received by an RSU in a 300 ms interval exceeds the maximal threshold, the RSU needs to pass the unverified signatures to an application server in order to mitigate the message loss problem. (Note, if an RSU is able to verify all signatures in a 300 ms, the RSU does not need to transmit the signature and its corresponding certificate of a message and instead it only needs to transmit the context of a message in order to reduce communication overhead.) Therefore, we discuss the transmission overhead from an RSU to the application server for those unverified signatures. As shown in Table III, let the RSU send n distinct signatures to the application server. With the ECDSA scheme, the transmission overhead is in proportion to the number of signatures, namely (42+125)n bytes. In contrast, since BLS and IBV can aggregate signatures, only one aggregate signature is sent upward. In addition to the signatures, the BLS scheme needs to transmit a certificate with the length of 125 bytes for each message, while the IBV only needs to transmit a pseudo identity with the length of 42 bytes for each message. Thus, the total transmission overhead is 21+125n and 21+42n for the BLS and IBV, respectively. Figure 6 shows the comparisons. The transmission overhead of all the schemes is proportional to the number of aggregate signatures. Compared with ECDSA, BLS is subject to lower transmission overhead; nonetheless, the advantage gained in BLS is not obvious because the certificate dominates the length of the overhead. On the other hand, since no certificate for each message is required in IBV, the advantage gained in the proposed scheme is obvious. From Figure 6, we can see the transmission overhead of the IBV scheme is 33.6 percent of that by BLS and only 25.1 percent of that by ECDSA.

VI. Related Work

Security and privacy issues on VANETs have attracted extensive attentions from both academia and industry. J. Hubaux *et al.* [5], [6] first identified the issues of security and privacy preservation in VANETs by claiming that an appropriate Public Key Infrastructure (PKI) must be well devised to protect the transited information and to mutually authenticate among network entities. To address the privacy issue, they suggested to relying on temporary pseudonyms to achieve anonymity.

Raya *et al.* [7] proposed an anonymous-key-based (HAB) security protocol, which can achieve anonymous message authentication and conditional privacy preservation. With the HAB solution, a huge set of anonymous keys are preloaded in each vehicle, and each vehicle randomly takes one of the keys in the set to sign a safety message. To further prevent movement tracking, each anonymous key has a short lifetime. The HAB scheme presented an efficient and straightforward way in solving the privacy issues, while the central authority simply keeps all the anonymous certificates of all the vehicles in a certain area in order to maintain the traceability. Once a malicious message is detected, the authority has to exhaustedly search in a very huge database (probably 43,800 times millions of cars) to find the real identity related with the compromised anonymous public key which incurs tremendous complexity for the identity and certificate management. Lin *et al.* [10] proposed an efficient security protocol called GSIS, which is based on the group signature scheme [38]. With this protocol, only a private key and the group public key are stored in the vehicle, and the messages are signed according to the group signature scheme without revealing any identity information to the public. This assures that the trusted authority is equipped with the capability of exposing the sender identity of a message. However, the verification of each group signature requires at least two pairing operations which might not be scalable when the density of the traffic is increasing.

Raya *et al.* [9] proposed a secure traffic aggregation scheme to minimize the communication overhead and initiate a trade-off between the security and efficiency. Under their design, firstly, cells are defined and predetermined according to the physical location. When vehicles are located in a cell, the vehicle that is physically closest to the center of the cell is automatically taken as the group leader of the vehicles in the cell, which is delegated to aggregate messages for the whole group when the message is going to be relayed to the leader of the neighbor groups. The aggregation of messages can achieve a significant reduction in the overhead for vehicle to vehicle communications. However, the vehicle closest to the center of a cell could change frequently, leading to a frequent update of the group leader of a cell (e.g., once in a few seconds), which indicates that the approach can be further improved in terms of its efficiency and practical applicability.

Unlike all the previous works, the proposed IBV scheme can meet all the security and efficiency requirements for vehicle to RSU communications, such as the verification speed, transmission overhead, management efficiency, anonymity, and traceability, which have been verified and analyzed in details through the paper.

VII. Conclusions and Future Work

We have proposed a novel Identity-based Batch Verification (IBV) scheme for VANETs in the application of sensing and collecting traffic flow related information, which has been identified to be capable of meeting the most important and emerging design requirements on security and privacy preservation ever reported in the literatures. In particular, the proposed IBV scheme can significantly improve the system performance by fully taking advantages of verifying multiple message signatures at once instead of the verification of one after the other. Our scheme has also addressed the identity

privacy and traceability issues in vehicular networks, where the signature of a message is signed according to a pseudo identity pair and private keys that are generated by the tamper-proof device. Furthermore, the IBV scheme enables the Trusted Authority (TA) to retrieve the real identity of a vehicle from any message signature, such that conditional privacy preservation can be achieved. Extensive analysis and evaluation have been conducted to demonstrate that the IBV scheme can achieve excellent operational efficiency for vehicle to RSU communications in terms of signature verification delay and communication overhead, in comparison with two recently reported counterparts, namely ECDSA and BLS.

To the best of our knowledge, this is the first paper to address both fast verification and privacy issues in VSNs. In our future work, we will continue our efforts to address other security issues in VSNs, such as Denial of Service (DoS) attack. Since a DoS attack is hard to defend and particularly fatal to our batch verification scheme, efficiently thwarting the DoS attack is not only a challenging task but also an urgent work in the future research. In addition, we will extend our identity-based batch verification scheme in V2V communication and will conduct more performance evaluation on message end-to-end delay and message loss ratio in V2V communication.

ACKNOWLEDGMENT

The research is financially supported by Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

[1] J. A. Misener, "Vehicle-infrastructure integration (VII) and satety: rubber and radio meets the road in california," *Intellimotion*, Vol. 11, No. 2, pp. 1-3, 2005.

[2] U. Lee, E. Magistretti, B. Zhou, M. Gerla, P. Bellavista, and A. Corradi, "Mobeyes: smart mobs for urban monitoring with a vehicular sensor network," *IEEE Wireless Communications*, Vol. 13, No. 5, pp. 52-57, 2006.

[3] F. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: an IEEE intelligent transportation systems society update," *IEEE Pervasive Computing*, Vol. 5, No. 4, pp. 68-69, 2006.

[4] Dedicated Short Range Communications (DSRC), [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html

[5] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy Magazine*, Vol. 2, No. 3, pp. 49-55, 2004.

[6] M. Raya and J. P. Hubaux, "Security aspects of inter-vehicle communications," in *Proceedings of Swiss Transport Research Conference*, 2005.

[7] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, Vol. 15, No. 1, pp. 39-68, 2007.

[8] M. Raya, P. Papadimitratos, and J. P. Hubaux, "Securing vehicular communications" *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, Vol. 13, No. 5, pp. 8-15, 2006.

[9] M. Raya, A. Aziz, and J. P. Hubaux, "Efficient secure aggregation in VANETs," in *Proceedings of International workshop on Vehicular ad hoc networks*, pp. 67-75, 2006.

[10] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Transaction on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, 2007.

[11] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Vehicle-to-vehicle safety messaging in DSRC," in *Proceedings of International workshop on Vehicular ad hoc networks*, pp. 19-28,Oct. 2004.

[12] X. Yang, J. Liu, F. Zhao, and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proceedings of IEEE MobiQuitous*, pp. 114-123, Aug. 2004.

[13] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks", in *Proceedings of IEEE International Conference on Communications*, Beijing, China, 2008.

[14] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proceedings of IEEE International Workshop on Vehicle Communication and Applications*, pp. 1-8, 2006.

[15] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks", *IEEE Communications Magazine*, to appear.

[16] U.S. Department of Transportation, National Highway Traffic Safety Adimistrtation, Vehicle Safety Communications Project, Final Repot, Apr. 2006.

[17] Road Weather Management. [Online]. Available: http://www.itsoverview.its.dot.gov/RWM.asp

[18] K. Ren, W. Lou, R. H. Deng, and K. Kim, "A novel privacy preserving authentication and access control scheme in pervasive computing environments," *IEEE Transactions on Vehicular Technology*, Vol. 55, No. 4, pp.1373-1384, 2006.

[19] K. Sampigethava, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: providing location privacy for VANET," in *Proceedings of International workshop on Vehicular ad hoc networks*, 2006.

[20] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing,", in *Proceedings of Crypto*, LNCS, Vol. 2139, pp. 213-229, 2001.

[21] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction," *IEICE Transactions on Fundamentals*, Vol. E84-A, No. 5, pp. 1234-1243, 2001.

[22] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of Asiacrypt*, Vol. 2248, pp. 514-532, 2001.

[23] A. Fiat, "Batch RSA," in *Proceedings of Crypto*, pp. 175-185, 1989.

[24] D. Naccache, D. M'Raïhi, S. Vaudenay, and D. Raphaeli, "Can D.S.A be improved? complexity trade-offs with the digital signature standard," in *Proceedings of EUROCRYPT*, LNCS, Vol. 950, pp. 77-85, 1994.

[25] J. C. Cha and J. H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *Proceedings of Public Key Cryptography*, pp. 18-30, 2003.

[26] F. Zhang, R. Safavi-Naini, and W. Susilo, "Efficient verifiably encrypted encrypted signature and partially blind signature from bilinear pairings," in *Proceedings of Indocrypt*, LNCS, Vol. 2904, pp. 191-204, 2003.

[27] F. Zhang and K. Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings," in *Proceedings of ACISP*, LNCS, Vol. 2727, pp. 312-323, 2003.

[28] H. Yoon, J. H. Cheon, and Y. Kim, "Batch verification with ID-based signatures," in *Proceedings of Information Security and Cryptology*, pp. 233-248, 2004.

[29] J. Camenisch, S. Hohenberger, and M. ∅. Pedersen, "Batch verification of short signatures," in *Proceedings of EUROCRYPT*, LNCS, Vol. 4514, pp. 246-263, 2007.

[30] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps," in *Proceedings of Crypto*, LNCS, Vol. 3152, pp. 56-72, 2004.

[31] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," IETF RFC 3174, 2001.

[32] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. 31, No. 4, pp. 469-472, 1985.

[33] V. S. Miller, "Use of elliptic curves in crytography," in *Proceedings of Advance in Cryptology*, pp. 417-426, Aug. 1985.

[34] IEEE Standard 1609.2 - IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, 2006.

[35] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE Transactions on Fundamentals*, Vol. E84-A, No. 5, pp. 1234-123, 2001.

[36] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," In *Procedings of Eurocrypt*, LNCS, Vol. 2656, pp. 416-432, 2003.

[37] M. Scott, "Efficient implementation of crytographic pairings," [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/ Slides/Thursday/mscott-samos07.pdf

[38] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology*, LNCS, Vol. 3152, pp. 41-55, 2004.