An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications

Yipin Sun, *Student Member, IEEE,* Rongxing Lu, *Student Member, IEEE,* Xiaodong Lin, *Member, IEEE,* Xuemin (Sherman) Shen, *Fellow, IEEE,* and Jinshu Su, *Member, IEEE*

***Abstract*—In this paper, we propose an efficient pseudonymous authentication scheme with strong privacy preservation, named PASS, for vehicular communications. Unlike traditional pseudonymous authentication schemes, the size of Certificate Revocation List (CRL) in PASS is linear with the number of revoked vehicles and irrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports Roadside Units-aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost irrelated to the number of the updated certificates. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries can not trace any vehicle even all Roadside Units have been compromised. Extensive simulations demonstrate that PASS outperforms previously reported ones in terms of the revocation cost and the certificate updating overhead.**

***Index Terms*—Vehicular communications, privacy preservation, anonymous authentication, revocation**

I. Introduction

VEHICULAR Ad Hoc Network (VANET), as a special instantiate of mobile ad hoc network, has been subject to extensive research efforts not only from the government, but also from the academia and automobile industry in recent years. Different from the traditional ad hoc networks, VANET contains not only mobile nodes — vehicles, but also stationary Roadside Units (RSUs). Due to this hybrid architecture, VANET opens a new door to facilitating road safety, traffic management, and providing multimedia services for vehicles on the road. According to the Dedicated Short Range Communications (DSRC) [1], in road safety-related applications, each vehicle equipped with On-Board Units (OBUs) will broadcast routine traffic messages with the information of position, current time, direction, speed, acceleration/deceleration, and traffic events, etc. With these information, drivers can get better awareness of their driving environment and take early actions to respond to an abnormal situation such as traffic accident. However, before putting this attractive application into practice, security and privacy issues in VANET must be resolved [2]–[5]. Without the security and privacy guarantees, an adversary in VANET can either forge bogus information to mislead other drivers and even cause deliberate traffic accident, or track the locations of the interested vehicles by collecting their routine traffic messages. Therefore, how to achieve anonymous authentication has become a fundamental requirement for securing VANET.

Over the past years, many anonymous authentication schemes have been reported [5]–[13], where both the group signature based schemes [6]–[8] and the pseudonymous authentication schemes [5,9]–[13] can well address most of the security and privacy concerns in VANET. However, due to the limitations of bandwidth and computation power, the applicabilities of these reported schemes are questionable in VANET. The size of Certificate Revocation List (CRL) and the checking cost are two important performance metrics for revocation mechanism in VANET. Unfortunately, the pseudonymous authentication schemes are prone to generate a huge CRL [5] while the checking cost in the group signature based schemes is unacceptable for the vehicles with limited computation power. Since CRL is usually transmitted by vehicle-to-vehicle communication [14,15], the quick increase of the CRL in the pseudonymous authentication schemes brings large communication cost. Moreover, the larger the CRL size, the longer the transmission delay to all vehicles during which period the misbehaving vehicles can compromise VANET continually. In the group signature based schemes [6]–[8], each checking operation that matching a message signature with respect to an identity in the CRL involves two pairing calculations, which causes obvious computation overhead for a vehicle, e.g., 10^{-2} sec in [8]. Given that CRL usually contains 10 revoked identities and a vehicle receives 20 messages per second, the total checking cost is 2 sec.

TABLE I
RSU DENSITY AND THE NUMBER OF THE CERTIFICATES THAT A VEHICLE HAS TO UPDATE ONCE IN NEW YORK CITY [12]

number of required RSUs	size of certificate set
176760	1
1473	120
589	300

Manuscript received December 16, 2009; revised March 29, 2010; accepted May 5, 2010. The associate editor coordinating the review of this paper and approving it for publication was Dr. J. Deng.

Y. Sun and J. Su are with the School of Computer Science, National University of Defense Technology, Changsha, P.R. China 410073 (e-mail: {ypsun,sjs}@nudt.edu.cn).

R. Lu and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada N2L 3G1 (e-mail: {rxlu,xshen}@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada L1H 7K4 (e-mail: xiaodong.lin@uoit.ca).

The distributed certificate service is a promising approach to decrease revocation cost [9]–[12]. In this way, vehicles can update theirs pseudonymous certificate sets from the certificate issuer by vehicle-to-RSU (V2R) communication on road. Once each certificate has a short-time period and is used in a specifically geographic region, the CRL that broadcasted in a region can decrease. However, the CRL size still depends on how many pseudonymous certificates are held by the revoked vehicles. Moreover, the certificate updating overhead becomes a heavy burden when the availability of an RSU is not pervasive, especially in the early stage of RSU deployment [5]. Recently, Wasef et al. [12] study the relationship between the RSU density in New York city and the number of the certificates that a vehicle has to update once, as shown in Table I. From the table, we can see that a vehicle has to update 120 pseudonymous certificates each time if 1473 RSUs had been built. Due to the limited wireless channel bandwidth, it is inefficient and difficult for an RSU to transmit hundreds of certificates for each passing-by vehicle while providing infotainment dissemination service at the same time. Furthermore, to generate so many certificates for tens of thousands requesters in a short time, the certificate issuer should have quite strong computation power which costs high expenditure. More seriously, some greedy users may send multiple requests to get more pseudonymous certificates, and legitimate users could also retransmit its request if the service latency becomes large. Subsequently, it will aggravate the service burden and even bring down the certificate issuer. To the best of our knowledge, how to optimize the certificate updating overhead in distributed certificate service has not been well addressed in previously reported works.

Another important issue in distributed certificate service is the privacy risk when each RSU acts as a sub certificate issuer [9,11,12]. To keep a centralized certificate issuer from being a bottleneck, an RSU is allowed to issue certificates for the vehicles. However, it brings a privacy risk when an RSU is compromised by the adversaries. Once the service records of an RSU are leaked, it is easy for the adversary to link the pseudonymous certificates which a vehicle has obtained from the compromised RSU. Especially, when the number of the compromised RSUs increases, it possibly provides a solution for the adversaries to revert the mobile trace of the interested vehicles. However, the privacy preservation against the RSUs is still an open issue to any scheme that supports the RSUs-aided distributed certificate service.

In this paper, to address both of the security and performance challenges in VANET, we propose an efficient Pseudonymous Authentication Scheme with Strong privacy preservation, named PASS, for vehicular communications. PASS supports RSUs-aided distribution certificate service that allows a vehicle to update its certificate set from an RSU on road. The contributions of this paper are four-fold.

- First, we design a novel scheme to generate the pseudo identities of the pseudonymous certificates belonging to the same owner based on one-way hash-chain technology. It is easy to revoke the unexpired certificates of an revoked user by only releasing two hash seeds. Therefore, unlike traditional pseudonymous authentication schemes, the CRL size in PASS is only linear with the number of revoked vehicles and irrelated to the number of pseudonymous certificates held by the revoked vehicles.
- Second, we propose an efficient certificate updating scheme. Although only the pseudonymous certificate issued by a legitimate RSU are valid in vehicular communication, PASS allows a vehicle to store a large set of pseudonymous certificates issued by the TA. Based the proxy re-signature cryptography technology [16] where a semi-trusted proxy with given some information can turn a user's signature on a message into another user's signature on the same message, the vehicle only needs to request the re-signature keys from an RSU and re-sign numbers of the certificates issued by the TA to be as same as ones issued by the RSU itself. In this way, the service overhead is almost irrelated to the number of the updated certificates.
- Third, we provide strong privacy preservation to the vehicles. Although the RSUs act as certificate issuers in PASS, they don't know what certificates are held by a vehicle. Therefore, the adversaries can not trace the interested vehicles even though they had compromised all RSUs.
- Finally, extensive simulations evaluate the proposed scheme and the previously reported ones on several performance metrics, such as authentication overhead, revocation overhead, and the certificate updating overhead on road.

The remainder of the paper is organized as follows. Section II surveys some related works. Section III presents the system model, the threat model and the research objectives. Section IV gives some preliminaries including secure hash function, bilinear pairings and Schnorr signature algorithm. Then, Section V presents the proposed PASS scheme, followed by the security analysis and performance evaluation in Section VI and Section VII, respectively. Finally, Section VIII draws our conclusions.

II. Related Work

Anonymous authentication is a very active topic for securing VANET and can be roughly divided into two categories: the group signature based schemes [6]–[8], and the pseudonymous authentication schemes [5,9]–[13]. Both of them can address the security requirements well, such as authentication, non-repudiation, identity revocation and conditional anonymity. In the group signature based schemes, utilizing group signature [17], any public entity won't reveal the originator identity of a routine traffic message [6,7]. However, one limitation that the cost for signing and verifying messages is far more than adopting traditional public key based signature. To reduce these overheads, Calandriello et al. [8] propose the Hybrid scheme that a vehicle can issue a certificate for itself by using a group key, and then sign its messages using public key based signature. In such a way, the average overhead of message authentication can decrease. From the viewpoint of revocation cost, the group signature based schemes have an advantage that the CRL size is linear with the number of revoked vehicles,

but the checking operation involves two pairing calculations which could take about 10^4 times of computation cost than a string comparison [8].

The pseudonymous authentication schemes [5,9]–[13] adopt traditional public key based digital signature. Raya et al. [5] propose the basic idea of pseudonymous authentication scheme (denoted as BP in the following context) that each vehicle is supposed to store a large set of pseudonymous certificates with pseudo identities, and randomly chooses one of the available pseudonymous certificates for signing a message at one time. However, when a vehicle is revoked, all the pseudo identities, e.g., 43,800 identities in [5], would be added into a CRL. So the CRL increases quickly. Two works investigate how to distribute the CRL efficiently by vehicle-to-vehicle communication [14,15]. However, due to the limited bandwidth of wireless communication and the high-speed mobility of vehicles, it is difficult to distribute a large CRL to all vehicles in a timely fashion. To decrease the CRL size, Bellur [10] suggests to segment a country into a number of geographic regions, and assign region-specific certificates with validity period to a vehicle. Lu et al. [9] develop the Efficient Conditional Privacy Preservation (ECPP) protocol which is the first one to support legitimate vehicles updating short-time pseudonymous certificates from the RSUs frequently. Under the most ideal condition that one RSU is deployed for 600 meters along each road, a vehicle takes only one pseudonymous certificate with a quiet short validity period so that it becomes unnecessary for the vehicles to have a copy of CRL. Wasef et al. [12] extend RSUs-aided distribute certificate service into a hierarchical authority architecture and propose an efficient Distributed Certificate Service (DCS) scheme that supports batch signature verification. Jiang et al. [13] propose a batch verification scheme based on binary authentication tree and analyze the message authentication cost when some received messages attach bogus signatures. However, the performance of the above distributed certificate service schemes [9]–[12] largely depends on the RSU density. The less the number of RSUs, the larger the revocation cost and the certificate updating cost.

Another privacy-related study in VANET focuses on strengthening the location privacy of drivers. Anonymous authentication can not prevent a vehicle from being traced if the adversary can eavesdrop the whole area. They can link traffic routine messages broadcasted by a same vehicle based on the spatial and temporal correlation between successive locations of the vehicle. Hence, to strengthen the location privacy, some studies [18]–[20] suggest constructing certain regions where the adversary can not eavesdrop the vehicular communication, called mix-zones. Then, vehicles can change certificates when passing through a mix-zone. Usually, mix zones should be placed in locations with high node density and unpredictable mobility.

Our proposed PASS is a pseudonymous authentication scheme and supports distributed certificate service. Compared with previously reported pseudonymous authentication schemes, it can optimize not only the revocation overhead but also the certificate updating overhead. More importantly, PASS is the first study on privacy preservation against the sub certificate issuer, i.e., the RSUs in this paper.

III. System Model, Threat Model and Research Objectives

In this section, we formalize the system model, the threat model, and identify the research objectives.

A. System Model

We consider a typical VANET, which consists of a top trusted authority (TA), some stationary RSUs deployed at the roadsides, and a large number of vehicles equipped with OBUs moving on the road, as shown in Fig. 1.

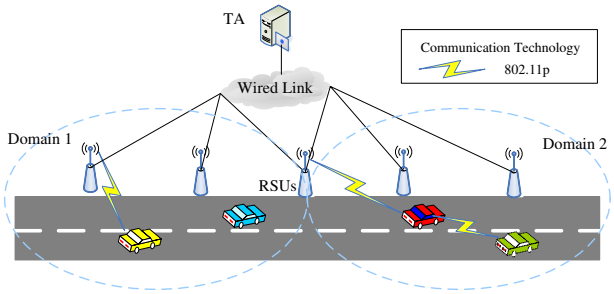


Fig. 1. System model

- *Trusted Authority (TA)*: TA is fully trusted by all parties in the system and in charge of the registration of RSUs and vehicles. The TA can divide its huge precinct into several domains and deploy RSUs at the boundary between these domains. The domain information is available to all entities. As usual, TA is assumed powered with sufficient storage capability and infeasible for any adversary to compromise [9].
- *RSUs:* RSUs act as the infrastructure of VANET and connect with the TA by wired links in the system. They provide service for information dissemination and certificate updating. In general, the density of RSU varies in different domains. Without loss of generality, the cantonal domains are supposed to have the similar RSU density while the domains in suburb may have a small number of RSUs. The pseudonymous certificates issued by an RSU can only be used in the domain where the RSU locates. As a distributed unit deployed on the roadside, an RSU has risk to be compromised. Although TA can detect a compromised RSU and take action to recover it [9], the records stored in the RSU maybe have been leaked.
- *Vehicle:* vehicles equipped with OBUs mainly communicate with each other for sharing local traffic information and improving the driving experience. A vehicle frequently requests the certificate service from an RSU and obtains enough certificates for the following period until passing by another RSU. Obviously, the number of the updated pseudonymous certificates depends on the RSU density [12]. The vehicle changes the pseudonymous certificates periodically to sign routine traffic messages.

B. Threat Model

We name any node to be an adversary or attacker if it deviates from the legitimate VANET protocols or infringes a driver's privacy. In addition, we refer to adversaries as misbehaving nodes in this paper. It is worth noting that an adversary may be an authenticated member of the network. Specifically, in our threat model, we consider an adversary could diffuse wrong information in the network to affect the behavior of other drivers or harm the infrastructure of VANET [2,5]. Moreover, an adversary can also launch tracking attacks by installing receivers on the roads to eavesdrop the messages broadcasted by the vehicles. Then, by trying to correlate some of the broadcasted certificates to a vehicle, the adversary may be able to track that vehicle of his interest [12].

C. Research Objectives

Since VANET is a large-scale wireless network scenario for public service, it faces serious security and privacy challenges. In the PASS scheme, we aim to achieve the following security and privacy objectives.

1) Authentication: It includes entity authentication and message integrity. Entity authentication enables receivers to check the authenticity of the sender, while message integrity ensures that the content of a message has not been altered in transit. All accepted messages should be from legal members and delivered unaltered;

2) Non-repudiation: Any entity can not deny the messages generated by itself. It is necessary for accident investigation that the malicious user should pay the fiddler for misleading the victims;

3) Identity revocation: It should be possible to exclude an unexpired membership from VANET. It is a fundamental requirement to defend the inside attacks and restore the security of VANET;

4) Conditional anonymity: It means the TA can reveal the real identity of the members while other entities could neither identify the real identity nor correlate these messages signed by the same member in a long term. In pseudonymous authentication schemes, conditional anonymity is supposed to be held if the validity period length of a pseudonymous certificate is less than a threshold (denoted as ΔT), e.g. 1 min [5]; and

5) Backward privacy: Once a membership was revoked, it should not reveal any information that decreases the conditional anonymity for the same member in the period before the revocation takes effect.

TABLE II
FORMAT OF THE SIGNED MESSAGE

protocol version	type	payload	certificate	signature

Moreover, by taking into consideration of the limited wireless bandwidth and valuable computation power, we also focus on the following performance objectives.

6) Authentication overhead: It mainly includes three parts, namely message signing cost, verification cost, and communication overhead includes the certificate and the signature as shown in Table II.

7) Revocation overhead: It can be evaluated by the CRL size and the checking cost against CRL. Compared with traditional pseudonymous authentication scheme, we hope to keep CRL size be linear with the number of revoked vehicles. Moreover, PASS is designed to support distributed certificate service to decrease CRL size; and

8) The overhead for certificate updating on the road: To solve a certificate updating request, the V2R communication overhead and the computation cost for the certificate issuer (RSU) is expected to be unrelated to the number of the updated certificates.

IV. PRELIMINARIES

In this section, we introduce some preliminaries, including secure hash chains, bilinear pairings [21] and Schnorr signature algorithm [22], which are the bases of our proposed PASS scheme. In addition, the notations used throughout the paper are given in Table III.

TABLE III
NOTATIONS

symbol	notation
ΔT	The privacy requirement on the validity period length of a pseudonymous certificate
TS_j	The j-th time slot
TW_k	The k-th time window that consists of L_w time slots
TA	The trust authority
R_x	The x-th RSU
V_i	The i-th vehicle
s	The master secret key of TA
P_{pub}	The master public key of TA
E	An arbitrary entity, which could be a vehicle, an RSU or the TA
$*$	The extra information declaration if it is not empty
$PK_{E,*}$, $SK_{E,*}$	The public key and secret key of E
$\mathsf{Cert}_{E_1,E_2,*}$	A certificate of E_2 issued by E_1
$\sigma_{E,*}$	A signature signed by E
VP_*	The certificate validity period
t_{stamp}	Time stamp
$h(.)$	A hash function such as SHA-1
$f(.)$	A hash function as $\{0,1\}^* \rightarrow \mathbb{G}$
$Enc_\kappa(.)$	A secure symmetric encryption algorithm with secret key κ
$\mathsf{Sign}(SK_E, M)$	Signing the message M by Schnorr signature algorithm with the secret key SK_E
$\mathsf{Verify}(PK_E, M, \sigma_{E,M})$	Verifying the Schnorr signature $\sigma_{E,M}$ of the message M with the public key PK_E
$\|$	Message concatenation operation, which appends several messages together

A. Hash Chains

A one-way hash function $h(.)$ is said to be secure if the following properties are satisfied [23]: *i*) $h(.)$ can take a message of arbitrary length as input and produce a message digest of a fixed-length output; *ii*) Given x, it is easy to compute $h(x) = y$. However, it is hard to compute $h^{-1}(y) = x$ given y; and *iii*) Given x, it is computationally infeasible to find $x^{'} \neq x$ such that $h(x^{'}) = h(x)$. Furthermore, suppose $h^i(x)$=$h(h^{i-1}(x))$, a hash chain of length L, $\{S_i\}$, is constructed by applying $h(.)$ recursively to an initial seed value SD, where $S_i = h^i(SD), i \in [1, L]$. Obviously, given S_i, it's easy to compute $S_j = h^{j-i}(S_i)$ $(j > i)$ but infeasible to obtain S_{i-1}.

B. Bilinear Pairing

Let $\mathbb{G}$ be a cyclic additive groups generated by P, and $\mathbb{G}_T$ be a cyclic multiplicative group of the same prime order q, i.e., $|\mathbb{G}| = |\mathbb{G}_T| = q$. An efficient admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ satisfies with the following properties: *i*) *Bilinear*: for all $P, Q, R \in \mathbb{G}$, and $a, b \in \mathbb{Z}_q^*$, $e(Q, P + R) = e(P + R, Q) = e(P, Q) \cdot e(R, Q)$. In particular, $e(aP, bQ) = e(P, Q)^{ab}$; *ii*) *Non-degenerate*: there exist $P, Q \in \mathbb{G}$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$; and *iii*) *Computable*: there is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in \mathbb{G}$. Such an admissible bilinear map e can be constructed by the modified Weil or Tate pairings on the elliptic curves [21]. The group that possesses such a map e is called a bilinear group, from which two problems are believed hard.

- *Elliptic Curve Discrete Logarithm Problem (ECDLP):* Given a point P of order q on an elliptic curve, and a point Q on the same curve. The ECDLP problem [21] is to determine the integer l, $0 \leq l \leq q - 1$, such that $Q = lP$.
- *Computational Diffie-Hellman problem (CDH):* Given two unknowns $a, b \in \mathbb{Z}_q^*$, the CDH problem [21] is given $P, aP, bP \in \mathbb{G}$, compute $abP \in \mathbb{G}$

C. Schnorr Signature Algorithm

The Schnorr signature algorithm [22] will be adopted as the basis of the signatures signed by the TA and vehicles, which is efficient and provably secure in the random oracle model. Suppose an entity E has the private secret key SK_E and the public key PK_E, where $SK_E \in \mathbb{Z}_q^*$ and $PK_E = SK_E \cdot P$. Let $\mathsf{Sign}(SK_E, M)$ denote the procedure that the entity E signs a signature $\sigma_{E,M}$ on message M, and $\mathsf{Verify}(PK_E, M, \sigma_{E,M})$ denote the procedure that other entities verify the Schnorr signature $\sigma_{E,M}$ of M signed by the entity E.

V. Our Proposed PASS Scheme

In this section, we will present our PASS scheme, which mainly consists of six phases: system initialization, RSU certificate issuing, vehicle pseudonymous certificate issuing, vehicle pseudonymous certificate updating, identity revocation and message signatures and verification.

A. System Initialization

Given the bilinear parameters $(q, \mathbb{G}, \mathbb{G}_T, e, P)$, the TA initializes the system by running the following steps:

(1) TA chooses one random number $s \in \mathbb{Z}_q^*$ as the master secret key, and computes the master public key $P_{pub} = sP \in \mathbb{G}$;

(2) TA chooses two one-way hash function $h(.)$, e.g., SHA-1, and $f(.) : \{0, 1\}^* \rightarrow \mathbb{G}$, and a secure symmetric encryption algorithm $Enc_\kappa(.)$; and

(3) TA chooses ΔT according to the privacy requirements of most vehicles, and set the validity period of pseudonymous certificate equal ΔT. Then, the TA estimates the number of the certificates that a vehicle has to update from an RSU once according to the RSU density in each domain [12], and selects a cut-point that satisfies the requirement of most cantonal domains, denoted as L_w. Furthermore, the updated certificates in a domain D_y will be counted by L_w, i.e., $N_y * L_w$, where $N_y \in \mathbb{N}$. In a suburb domain D_y that has fewer RSUs, $N_y > 1$. After that, the time domain is divided into serial time slots by ΔT and serial time windows by $L_w * \Delta T$, so a time window includes L_w time slots. In this way, a pseudonymous certificate can only be used in one time slot. Let TS_j denote the j-th time slot that ends at j$*\Delta T$, and TW_k denote the k-th time window that ends at k$*L_w * \Delta T$. TS_j is in TW_k if $j \in ((k-1) * L_w, k * L_w]$. Then, the system parameters will be published, which include $(q, \mathbb{G}, \mathbb{G}_T, e, P, P_{pub}, h(.), f(.), Enc_\kappa(.), \Delta T, L_w)$.

B. RSU Certificate Issuing

For an RSU R_x in the domain D_y, the TA issues a certificate Cert_{TA,R_x} as follows.

(1) TA chooses a random number $r \in \mathbb{Z}_q^*$, and sets the secret key $SK_{R_x} = r$, and the public key PK_{R_x}=rP;

(2) TA generates the signature σ_{TA,R_x} using Schnorr signature algorithm, where $\sigma_{TA,R_x} = \mathsf{Sign}(s, PK_{R_x} \| D_y)$; and

(3) TA securely delivers SK_{R_x} and Cert_{TA,R_x} to R_x, where $\mathsf{Cert}_{TA,R_x} = (PK_{R_x}, D_y, \sigma_{TA,R_x})$. Then it stores the mapping between the real ID of R_x and Cert_{TA,R_x}.

R_x and the other entities can verify the certificate Cert_{TA,R_x} by the procedure $\mathsf{Verify}(P_{pub}, PK_{R_x} \| D_y, \sigma_{TA,R_x})$.

C. Vehicle Pseudonymous Certificate Issued by TA

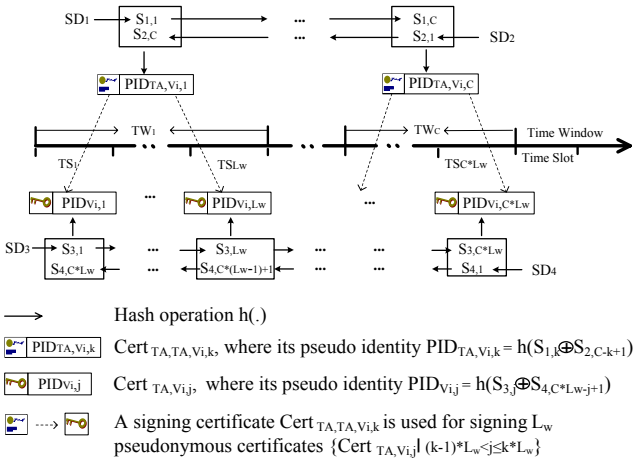


Fig. 2. The signing certificate $\mathsf{Cert}_{TA,TA,V_i,k}$ and the pseudonymous certificate $\mathsf{Cert}_{TA,V_i,j}$

PASS adopts prestore strategy that each vehicle can obtain a large set of pseudonymous certificates from the TA during the vehicle inspection. Suppose the TA issues $L_w * C$ pseudonymous certificates corresponding to the period from the time window TW_1 to TW_C for the vehicle V_i. Let $\mathsf{Cert}_{TA,V_i,j}$ denote V_i's pseudonymous certificate in the time slot TS_j ($j \in [1, L_w * C]$), where its validity period $VP_{V_i,j} = j$. As shown in Fig. 2, the pseudo identity of $\mathsf{Cert}_{TA,V_i,j}$ is calculated based on two hash chains with the random hash seeds SD_3 and SD_4, i.e., $PID_{V_i,j} = h(S_{3,j} \oplus S_{4,C*L_w-j+1})$, where $S_{3,j} =$

$h^j(SD_3)$, $S_{4,C*L_w-j+1} = h^{C*L_w-j+1}(SD_4)$, and $\oplus$ is XOR operation. In this way, all pseudonymous certificates of V_i can be easily revoked by releasing two hash seeds, the details of which will be presented in section V-E. However, without knowing the two seeds, it is infeasible to reveal the linkability among these certificates.

Different with issuing the certificate for an RSU, the TA does not use its master secret key to sign the pseudonymous certificates for a vehicle directly, but chooses a temporary secret key for such purpose in each time window. Let $SK_{TA,V_i,k}$ denote the signing secret key of the TA for issuing V_i's 's pseudonymous certificates in the time window TW_k , $PK_{TA,V_i,k}$ denote the corresponding public key, and $\mathsf{Cert}_{TA,TA,V_i,k}$ denote the corresponding certificate, named the signing certificate. As shown in Fig. 2, a signing certificate $\mathsf{Cert}_{TA,TA,V_i,k}$ is used for issuing L_w pseudonymous certificates $\{\mathsf{Cert}_{TA,V_i,j} \mid j \in ((k-1)*L_w, k*L_w]\}$. In addition, the pseudo identity of $\mathsf{Cert}_{TA,V_i,j}$ can also be calculated from two hash chains with the random hash seeds SD_1 and SD_2, i.e., $PID_{TA,V_i,k} = h(S_{1,k} \oplus S_{2,C-k+1})$, where $S_{1,k} = h^k(SD_1)$ and $S_{2,C-k+1} = h^{C-k+1}(SD_2)$.

The certificate issuing procedure is presented in Algorithm 1. Firstly, the TA generates the signing secret keys $\{SK_{TA,V_i,k}\}$ and the corresponding signing certificates$\{\mathsf{Cert}_{TA,TA,V_i,k}\}$ for itself based on Schnorr signature algorithm in lines 2-16, where k $\in [1, C]$. Secondly, the TA uses each secret key $SK_{TA,V_i,k}$ to sign L_w pseudonymous certificates based on short signature algorithm [24] in lines 17-33. After that, the TA sends the secret key set $\{SK_{V_i,j}\}$, the pseudonymous certificate set $\{\mathsf{Cert}_{TA,V_i,j}\}$ and the signing certificate set $\{\mathsf{Cert}_{TA,TA,V_i,k}\}$ securely to vehicle V_i. Finally, the TA stores the mapping relationship between the real identity of V_i and all these pseudo identities, and a 7-tuples $< V_i, 0, C, SD_1, SD_2, SD_3, SD_4 >$.

V_i and other entities can verify the signing certificate $\mathsf{Cert}_{TA,TA,V_i,k}$ by the procedure $\mathsf{Verify}(P_{pub}, PK_{TA,V_i,k} \| VP_{TA,V_i,k} \| PID_{TA,V_i,k}, \sigma_{TA,TA,V_i,k})$. Moreover, V_i can verify the pseudonymous certificate $\mathsf{Cert}_{TA,V_i,j}$ by $e(\sigma_{TA,V_i,j}, P) \stackrel{?}{=} e(f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), PK_{TA,V_i,k})$, where $j \in ((k-1)*L_w, k*L_w]$. The verification holds since

$$\begin{aligned} e(\sigma_{TA,V_i,j}, P) &= e(SK_{TA,V_i,k} \cdot f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), P) \\ &= e(f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), SK_{TA,V_i,k} \cdot P) \\ &= e(f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), PK_{TA,V_i,k}) \end{aligned}$$

Remarks:

- The TA can carry out the Algorithm 1 in advance, and then securely deliver these credentials to V_i during the vehicle inspection. In this way, certificate issuing is not a real-time procedure. Therefore, the TA can not become the bottleneck for the system.
- In PASS, a vehicle takes a large number of pseudonymous certificates but each pseudonymous certificate validates in different time slots. It can restrict the credential misuse. For example, without the strict validity period, a misbehaving vehicle may use all pseudonymous certificates in parallel to impersonate a number of vehicles and mount a Sybil attack [2]. A limitation of the proposed strategy is a vehicle has to take more certificates than it needs on driving. However, the storage overhead for a vehicle evaluated in section VII-D is accessible under the current storage capacity.

Algorithm 1: Certificate_issue(s,C)

Data: The master secret key s of TA, the time window span C
Result: The secret key and pseudonymous certificate set for vehicle V_i, and the signing certificate set of TA

1 **begin**
2 Select two random seed values SD_1 and SD_2
3 /⋆ generates two hash chains $\{S_{1,k}\}$ and $\{S_{2,k}\}$ ⋆/
4 **for** *each* $k \in [1, C]$ **do**
5 Set $S_{1,k} = h^k(SD_1)$, and $S_{2,k} = h^k(SD_2)$
6 **end**
7 /⋆ issues the signing certificates of TA ⋆/
8 **for** *each* $k \in [1, C]$ **do**
9 Set $PID_{TA,V_i,k} = h(S_{1,k} \oplus S_{2,C-k+1})$
10 /⋆ generates the signing secret key and public key used in TW_k ⋆/
11 Select a random number $r_1 \in \mathbb{Z}_q^*$
12 Set $SK_{TA,V_i,k} = r_1$,
13 $PK_{TA,V_i,k} = r_1 P$, and $VP_{TA,V_i,k} = k$
14 Calculate $\sigma_{TA,TA,V_i,k} =$ **Sign**$(s, PK_{TA,V_i,k} \| VP_{TA,V_i,k} \| PID_{TA,V_i,k})$
15 Set $\mathsf{Cert}_{TA,TA,V_i,k} = (PK_{TA,V_i,k}, VP_{TA,V_i,k}, PID_{TA,V_i,k}, \sigma_{TA,TA,V_i,k})$
16 **end**
17 Select two random seed values SD_3 and SD_4
18 /⋆ generates two hash chains $\{S_{3,j}\}$ and $\{S_{4,j}\}$ ⋆/
19 **for** *each* $j \in [1, L_w * C]$ **do**
20 Set $S_{3,j} = h^j(SD_3)$, and $S_{4,j} = h^j(SD_4)$
21 **end**
22 /⋆ issues the pseudonymous certificates of V_i ⋆/
23 **for** *each* $j \in [1, L_w * C]$ **do**
24 Set $PID_{V_i,j} = h(S_{3,j} \oplus S_{4,C*L_w-j+1})$
25 /⋆ generates the secret key and public key of V_i used in TS_j ⋆/
26 Select a random number $r_2 \in \mathbb{Z}_q^*$
27 Set $SK_{V_i,j} = r_2$,
28 $PK_{V_i,j} = r_2 P$, and $VP_{V_i,j} = j$
29 /⋆ signs with the signing secret key in TW_k that concludes TS_j ⋆/
30 Calculate $k = \lceil \frac{j}{L_w} \rceil$, and
31 $\sigma_{TA,V_i,j} = SK_{TA,V_i,k} \cdot f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j})$
32 Set $\mathsf{Cert}_{TA,V_i,j} = (PK_{V_i,j}, VP_{V_i,j}, PID_{V_i,j}, \sigma_{TA,V_i,j})$
33 **end**
34 **return** $\{SK_{V_i,j}, \mathsf{Cert}_{TA,V_i,j}, \mathsf{Cert}_{TA,TA,V_i,k} \mid j \in [1, L_w * C], k \in [1, C]\}$
35 **end**

D. Vehicle Pseudonymous Certificate Updating

Although a vehicle has a large set of pseudonymous certificates issued by the TA, it can not use these certificates directly in vehicular communication. In the domain D_y, only the certificates issued by an RSU R_x belonging to this domain are valid. However, a vehicle V_i doesn't request $N_y * L_w$ certificates from R_x directly. Instead, adopting the proxy re-signature cryptography technology [16], it only needs to request N_y re-signature key from R_x, and then re-signs the pseudonymous certificates issued by the TA to be as same as ones issued by R_x itself. As shown in Fig. 3, the whole

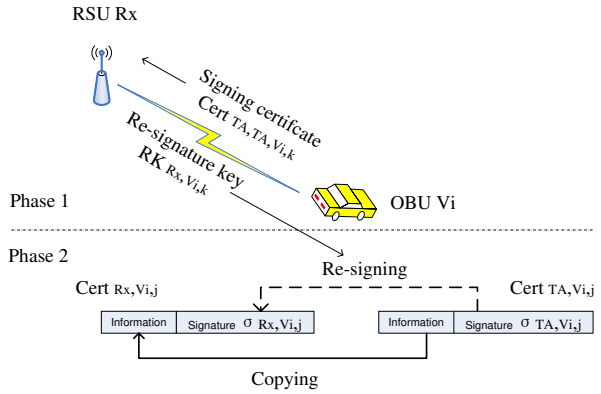


Fig. 3. Pseudonymous certificate updating

process can be divided into two phases:

Phase 1 Requesting re-signature key. Given that the current time window is TW_k, V_i can submit the signing certificates $SC \subseteq \{\mathsf{Cert}_{TA,TA,V_i,k'} | k' \in [k+1, k+N_y]\}$ to request the corresponding re-signature keys from the R_x.

(1) R_x broadcasts its certificate Cert_{TA,R_x} periodically, e.g., every 5 sec;

(2) If Cert_{TA,R_x} is valid, V_i selects a random number $r_3 \in \mathbb{Z}_q^*$, and calculates the shared secret key $\phi = r_3 \cdot PK_{R_x}$ and the hint $\psi = r_3 P$. Then, it sends the request message $(\psi, Enc_\phi(t_{stamp} \| SC)$ to R_x, and t_{stamp} is the time stamp;

(3) R_x calculates the shared secret key $\phi' = SK_{R_x} \cdot \psi$ to decrypt the request message, and checks whether t_{stamp} is fresh, and the signing certificates SC are valid during the period from TW_{k+1} to TW_{k+N_y}. If the verification is true, R_x calculates the re-signature key $RK_{R_x,V_i,k'} = \frac{1}{SK_{R_x}} \cdot PK_{TA,V_i,k'}$ for each $\mathsf{Cert}_{TA,TA,V_i,k'} \in SC$. After that, R_x sends $\{RK_{R_x,V_i,k'}\}$ back to V_i. Finally, R_x stores the service records that consist of the serial number of time window and the pseudo identity of signing certificate, i.e., $<k', PID_{TA,V_i,k'}>$;

(4) V_i verifies each re-signature key in $\{RK_{R_x,V_i,k'}\}$ by checking that

$$\begin{aligned} e(RK_{R_x,V_i,k'}, PK_{R_x}) &\stackrel{?}{=} e(\frac{1}{SK_{R_x}} \cdot PK_{TA,V_i,k'}, SK_{R_x} \cdot P) \\ &= e(PK_{TA,V_i,k'}, P) \end{aligned}$$

Phase 2 Re-signing pseudonymous certificates. The re-signature key $RK_{R_x,V_i,k'}$ can be used to re-sign L_w pseudonymous certificates that signed by $\mathsf{Cert}_{TA,TA,V_i,k'}$ primitively. i.e., $\{\mathsf{Cert}_{TA,V_i,j} | j \in ((k'-1)*L_w, k'*L_w]\}$. V_i transforms $\mathsf{Cert}_{TA,V_i,j} = (PK_{V_i,j}, VP_{V_i,j}, PID_{V_i,j}, \sigma_{TA,V_i,j})$ to the corresponding certificate $\mathsf{Cert}_{R_x,V_i,j}$ issued by R_x as follows.

(5) To re-sign $\sigma_{TA,V_i,j}$ to the signature $\sigma_{R_x,V_i,j} = \{\beta_0, \beta_1, \beta_2\}$ signed by R_x, V_i chooses a random number $r_4 \in \mathbb{Z}_q^*$, and calculates

$$\begin{cases} \beta_0 = r_4 \cdot \sigma_{TA,V_i,j} \\ \beta_1 = r_4 \cdot PK_{TA,V_i,k'} \\ \beta_2 = r_4 \cdot RK_{R_x,V_i,k'} \end{cases}$$

(6) V_i composes $\mathsf{Cert}_{R_x,V_i,j} = (PK_{V_i,j}, VP_{V_i,j}, PID_{V_i,j}, \sigma_{R_x,V_i,j}, \mathsf{Cert}_{TA,R_x})$.

To verify $\mathsf{Cert}_{R_x,V_i,j}$, other entities can first check that Cert_{TA,R_x} is valid, and then accept it if $e(\beta_0 + \beta_1, P) \stackrel{?}{=} e(\beta_1, f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}))\ e(PK_{R_x}, \beta_2)$. The verification holds since

$$\begin{aligned} e(\beta_0, P) &= e(r_4 \cdot \sigma_{TA,V_i,j}, P) \\ &= e(r_4 \cdot SK_{TA,V_i,k'} \cdot f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), P) \\ &= e(f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), r_4 \cdot SK_{TA,V_i,k'} \cdot P) \\ &= e(f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j}), r_4 \cdot PK_{TA,V_i,k'}) \\ &= e(\beta_1, f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j})) \\ e(\beta_1, P) &= e(r_4 \cdot PK_{TA,V_i,k'}, P) \\ &= e(r_4 \cdot \frac{SK_{TA,V_i,k'}}{SK_{R_x}} \cdot SK_{R_x} \cdot P, P) \\ &= e(SK_{R_x} \cdot P, r_4 \cdot \frac{SK_{TA,V_i,k'}}{SK_{R_x}} \cdot P) \\ &= e(PK_{R_x}, r_4 \cdot RK_{R_x,V_i,k'}) \\ &= e(PK_{R_x}, \beta_2) \end{aligned}$$

$$\begin{aligned} e(\beta_0 + \beta_1, P) &= e(\beta_0, P) e(\beta_1, P) \\ &= e(\beta_1, f(PK_{V_i,j} \| VP_{V_i,j} \| PID_{V_i,j})) e(PK_{R_x}, \beta_2) \end{aligned}$$

Remarks:

- The vehicle V_i can obtain at most N_y re-signature keys from R_x once. The greedy users cannot benefit more even through they retransmit the request many times. Compared to issue $N_y * L_w$ certificates, the service burden for R_x is trivial. Although N_y is larger than 1 in a suburb domain, the service cost is acceptable for an RSU because the traffic is small in suburb as well.
- It is worth noting that a misbehaving vehicle may try to create a pseudonymous certificate with an invalid pseudo identity to avoid being traced by the TA. However, due to the adopted re-signature cryptography technology, the vehicle cannot generate a correct signature for the forged pseudonymous certificate.
- R_x can issue pseudonymous certificates for the vehicles by itself. If the TA finds out a valid certificate issued by R_x without the corresponding record in its own database, it means R_x has been compromised.

E. Identity Revocation

In PASS, the TA publishes the CRLs to revoke the unexpired memberships in every domain. Let $CRL_{D(y),R}$ denote the CRL for the compromised RSUs in the domain D_y, and $CRL_{D(y),V}$ denote the CRL for the revoked vehicles in D_y. $CRL_{D(y),R}$ and $CRL_{D(y),V}$ would be broadcasted in D_y by vehicle-to-vehicle communication.

To revoke an RSU in D_y, the TA adds its certificate to $CRL_{D(y),R}$. In this way, all the pseudonymous certificate issued by the compromised RSUs would be revoked at the same time.

To revoke a vehicle V_i, the signing certificates stored in V_i should be informed to all RSUs, and the unexpired pseudonymous certificates which V_i had obtained by the re-signing service should be revoked at same time. In PASS, instead of revoking V_i thoroughly, the TA can just prevent it from accessing VANET for certain revocation period, e.g.,

from the current time window TW_n to the future one TW_m ($m \in (n, C]$). The procedure runs as follows.

(1) TA finds out the 7-tuples $< V_i,\ 0,\ C,\ SD_1,\ SD_2,\ SD_3,\ SD_4 >$, and calculates $S_{1,n} = h^n(SD_1)$, $S_{2,C-m+1} = h^{C-m+1}(SD_2)$. Then it sends the pseudo identity information of the revoked signing certificates $< n, m, S_{1,n}, S_{2,C-m+1} >$ to all RSUs;

(2) After receiving $< n, m, S_{1,n}, S_{2,C-m+1} >$, an RSU R_x calculates these pseudo identities PID_k ($k \in [n, m]$) of revoked signing certificates, where

$$\begin{cases} S_{1,k} = h^{k-n}(S_{1,n}) \\ S_{2,C-k+1} = h^{m-k}(S_{2,C-m+1}) \\ PID_k = h(S_{1,k} \oplus S_{2,C-k+1}) \end{cases}$$

R_x adds PID_k into the CRL used in the time window TW_k and will not provide the re-signature key for the signing certificate with the pseudo identity PID_k. R_x also check that whether it had issued the re-signature key for the revoked signing certificate with the pseudo identity $PID_{k'}$. If the record is not existed, set $k^{'}$ = 0. R_x sends $k^{'}$ back to TA;

(3) After receiving the responses from all RSUs in D_y, the TA finds out the maximum value of $\{k^{'}\}$, denoted as $k^{''}$. If the revoked vehicle V_i has the unexpired pseudonymous certificate in D_y, i.e., $k^{''} \neq 0$, the TA calculates $S_{3,(n-1)*L_w+1} = h^{(n-1)*L_w+1}(SD_3)$, and $S_{4,(C-k'')*L_w+1} = h^{(C-k^{''})*L_w+1}(SD_4)$. Then it adds the pseudo identity information of the revoked pseudonymous certificates $<(n-1) * L_w,\ k^{''} * L_w,\ S_{3,(n-1)*L_w+1},\ S_{4,(C-k'')*L_w+1} >$ to $CRL_{D(y),V}$. After that, $CRL_{D(y),V}$ will be distributed to all vehicles in the domain D_y by vehicle-to-vehicle communication [14];

(4) After receiving the updated information $<(n-1) * L_w,\ k^{''} * L_w,\ S_{3,(n-1)*L_w+1},\ S_{4,(C-k'')*L_w+1} >$ in $CRL_{D(y),V}$, any vehicle can calculate the pseudo identities PID_j ($j \in ((n-1) * L_w, k^{''} * L_w]$) of the revoked pseudonymous certificates, where

$$\begin{cases} S_{3,j} = h^{j-(n-1)*L_w-1}(S_{3,(n-1)*L_w+1}) \\ S_{4,C*L_w-j+1} = h^{k^{''}*L_w-j}(S_{4,(C-k'')*L_w+1}) \\ PID_j = h(S_{3,j} \oplus S_{4,C*L_w-j+1}) \end{cases}$$

Moreover, the vehicle would add PID_j to the local CRL used in time slot TS_j.

Remarks:

- No matter how many pseudonymous certificates a revoked vehicle has, only one item needs to be added into the CRL. Therefore, the CRL size is linear in terms of the number of revoked vehicles.
- Although the local CRL for each vehicle varies in different time slots, the constructing overhead can be omitted because the vehicle can construct CRL_j using the idle computation time in the time slot TS_{j-1}.

F. Message Signature and Verification

In the time slot TS_j, a vehicle V_i should use the pseudonymous certificate $\mathsf{Cert}_{R_x,V_i,j}$ to sign a message M by the Schnorr signature algorithm, i.e., the signature $\sigma_{V_i,M} = \mathsf{Sign}(SK_{V_i,j}, M)$.

After receiving the message (M, $\sigma_{V_i,M}$, $\mathsf{Cert}_{R_x,V_i,j}$) from V_i, the other entities first verify that whether $\mathsf{Cert}_{R_x,V_i,j}$ is valid, and then accept the message if $\mathsf{Verify}(PK_{V_i,j},\ M,\ \sigma_{V_i,M})$ is true.

Remarks: According to DSRC, a vehicle broadcasts routine traffic message every 300 msec. Because the validity period of a pseudonymous certificate is usually 1 min [8], it means that each certificate is used to sign about 200 messages. It is efficient for any vehicle to keep a public key buffer for the verified pseudonymous certificates so that the pseudonymous certificates of the neighboring vehicles only need to be verified once. Moreover, a vehicle can broadcast its pseudonymous certificate periodically, e.g., 1 sec, while it attaches the public key with every message instead of the whole certificate. It is good for reducing communication cost.

VI. Security Analysis

In this section, we discuss security issues of the proposed PASS scheme according to the security objectives presented in section III-C.

A. Authentication and non-repudiation

During routine vehicular communication, authentication and non-repudiation are achieved by the public key based digital signatures. First, the secret key of any entity in PASS is secure. It can be seen that finding the master secret key s from the master public key $P_{pub} = sP$ is an instance of the ECDLP problem. Similar analogy applies to find the secret key SK_E of any entity E from the corresponding public key PK_E, where $PK_E = SK_E \cdot P$. Second, based on the well-know signature algorithms such as Schnorr signature, Short signature and Re-signature technology, the signature generated by each entity is unforgeable. Therefore, entity authentication can be achieved by a digital certificate that consists of the owner's public key and the issuer's signature. Similarly, the message with a veritable signature can guarantee message integrity and non-repudiation.

In addition, weak authentication for certificate updating is secure. As presented in section V-D, the vehicle V_i uses a signing certificate of TA as the credential to get service from R_x. Although this authentication process is not as strong as the request message is supposed to attache V_i's signature, it achieves the tradeoff between efficiency and security. First, except the TA and V_i, the signing certificate is only explored to R_x because the communication between V_i and R_x is confidential. Finding the shared secret key ϕ from ψ and PK_{R_x} is an instance of the CDH problem: given P, $\psi = r_3 P$, and $PK_{R_x} = SK_{R_x} \cdot P$, find $\phi = r_3 \cdot SK_{R_x} \cdot P$. If R_x is compromised but not detected by the TA, the adversaries may utilize the received signing certificates to launch DoS attack against the other legitimate RSUs. However, with the help of the vehicles who own these signing certificates, the TA can easily discover the compromised RSU and revoke it. Second, the re-signature key generated for a signing certificate can only be used to re-sign these pseudonymous certificates that signed by the signing certificate. It is useless for the other entities except V_i. Therefore, the re-signature key can be transmitted

as a clear text. Finally, the time stamp that attached in the request messages can prevent the replay attack to an RSU.

B. Identity revocation

In PASS, the TA can exclude an entity from VANET by revoking its unexpired certificates with a CRL. Specially, to prevent a vehicle from accessing VANET, the TA releases only two hash elements that corresponding to the revocation period. Then, other entities can compute the pseudo identities of the pseudonymous certificates held by the revoked vehicle, and drop the messages signed by these certificates.

C. Conditional anonymity

In PASS, conditional anonymity is preserved by the following techniques.

- *Pseudonymous authentication:* A vehicle changes pseudonymous certificates frequently during vehicular communication. Moreover, other entities except the TA can not reveal the relationship between these certificates without knowing these two hash seeds. For example, given tow pseudo identities, $PID_{V,1}$ = $h(S_{3,1}\oplus S_{4,C*L_w})$ and $PID_{\overline{V},2}$ = $h(\overline{S}_{3,2}\oplus\overline{S}_{4,C*L_w-1})$, to verify their relationship, the adversary first computes $x = h^{-1}(PID_{V,1})$, and then computes $y = h^{-1}(x\oplus S_{3,1})$ for each possible value of $S_{3,1}$ until the verification is true, i.e., $h(h(S_{3,1})\oplus \mathrm{y}) \stackrel{?}{=} PID_{\overline{V},2}$. For a l-bits one-way hash function, the expected cost of solving h^{-1} is $O(2^{l-1})$. Moreover, suppose $PID_{V,1}$ and $PID_{\overline{V},2}$ really belong to the same user, the expected number of h^{-1} operation to confirm this relationship is 2^{l-1}. Therefore, the total cost is $O(2^{2l-2})$. Given a 160-bits one-way hash such as SHA-1, it is a hard computational problem to verify the relationship between two pseudo identities. In addition, to prevent a vehicle from being traced, it is better for the vehicle to change certificates in a mix-zone [18]–[20];
- *Anonymous authentication for certificate updating:* A vehicle requests service from the RSUs by the different signing certificates of TA. Similar as the above analysis, without knowing two hash seeds, RSUs can not find out the relationship between these pseudo identities of the signing certificates submitted by the interested vehicle.
- *Certificate updating based on re-signature technology:* Although an RSU R_x acts as the certificate issuer for a vehicle V_i, it has no idea to infringe V_i's privacy. First, R_x doesn't know the pseudo identity of the pseudonymous certificates held by V_i because the re-signing operation is implemented by V_i itself. Second, although the new certificate signature $\sigma_{R_x,V_i,j}$ is generated with the re-signature key $RK_{R_x,V_i,k'}$ issued by R_x, it's impossible to tell the relationship between the signature $\sigma_{R_x,V_i,j}$ and $RK_{R_x,V_i,k'}$ without knowing the random number r_4.

D. Backward privacy

In PASS, after a vehicle is revoked, it is still difficult for any entity to reduce the pseudo identities of pseudonymous certificates used by the revoked vehicle in the past. For example, suppose $S_{3,j}$ and $S_{4,1}$ are released to revoke a vehicle V_i from the time slot TS_j. To compute V_i's pseudo identity in the time slot TS_{j-1}, i.e., $PID_{V_i,j-1}$=$h(S_{3,j-1}\oplus S_{4,C*L_w-j+2})$, the adversary has to know $S_{3,j-1}$ = $h^{-1}(S_{3,j})$ at first. Given a 160-bits one-way hash such as SHA-1, it is hard to find out $S_{3,j-1}$ from $S_{3,j}$.

Among the previously reported works, the group signature based schemes can not achieve the backward privacy while the pseudonymous authentication schemes can achieve the above objectives basically if they use short-time pseudonymous certificates. However, the schemes that adopt RSUs-aided distributed certificate service can not achieve conditional anonymity against the RSUs. For example, in ECPP, a vehicle requests pseudonymous certificates from an RSU by its invariable credential. Therefore, when the service records stored in an RSU is leaked, the adversary can find out all the certificates that the RSU has issued for the interested vehicle. In DCS, a vehicle obtains the RSU service by a pseudonymous certificate issued by the other RSUs. In this way, the adversary doesn't know which vehicle requests the service, but it can correlate the pseudonymous certificates belonging to the same user. Here we develop a probabilistic model to analyze the risk that the knowledge of an RSU is used to track an interested vehicle.

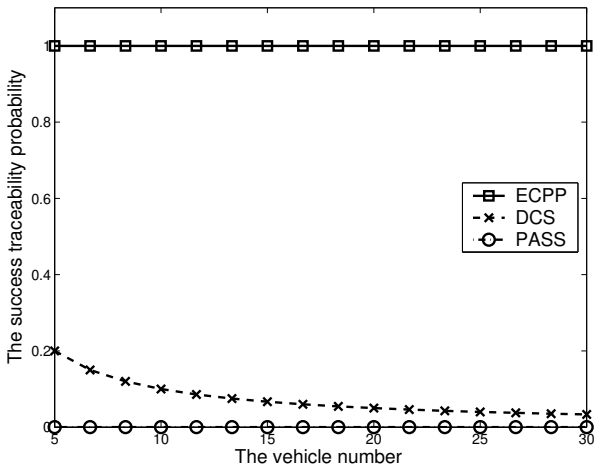


Fig. 4. The success traceability probability when the RSU is compromised

Suppose there is an RSU, an adversary and λ vehicles in a certain region. The adversary gathers some traffic routine messages during ξ time slots and tries to analyze the mobile route of an interested vehicle. In each time slot, the adversary has recorded the certificates used by these vehicles. Let $Pr(\theta)$ denote the probability that the adversary distinguishes the pseudonymous certificate of the interested vehicle from θ candidate certificates, where $Pr(\theta)$=$1/\theta$. If the adversary can correlate ξ certificates of the interested vehicle, the tracing analysis succeeds. Let SP denote the success traceability probability. When the RSU is in secure state, the adversary has to find out every certificate of the interested vehicle from λ certificates at each time slot. Therefore, SP= $1/\lambda^{\xi}$. In PASS, when the RSU is compromised, the adversary cannot get any useful information, so SP_{PASS} = SP. In ECPP, the adversary

TABLE IV
THE SIZE OF RSU AND TA SIGNING CERTIFICATES

(a) RSU certificate

parameter	size in bytes
PK_{R_x}	21
D_y	4
σ_{TA,R_x}	42
total	67

(b) TA signing certificate

parameter	size in bytes
$PK_{TA,V_i,k}$	21
$VP_{TA,V_i,k}$	4
$PID_{TA,V_i,k}$	20
$\sigma_{TA,TA,V_i,k}$	21
total	66

TABLE V
THE SIZE OF VEHICLE PSEUDONYMOUS CERTIFICATES

(a) Issued by TA

parameter	size in bytes
$PK_{V_i,j}$	21
$VP_{V_i,j}$	4
$PID_{V_i,j}$	20
$\sigma_{TA,V_i,j}$	21
total	66

(b) Issued by RSU R_x

parameter	size in bytes
$PK_{V_i,j}$	21
$VP_{V_i,j}$	4
$PID_{V_i,j}$	20
$\sigma_{R_x,V_i,j}$	63
Cert_{TA,R_x}	67
total	175

can directly find out the pseudonymous certificates of the interested vehicle, so SP_{ECPP} = 1. In DCS, the adversary has to confirm just one certificate of the interested vehicle, so SP_{DCS} = $1/\lambda$. Given ξ=10, Fig. 4 plots the success traceability probability vs. the vehicle numbers in the region. It can be seen that PASS provides the best privacy preservation.

VII. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed PASS with BP, ECPP, DCS and Hybrid schemes. The classical PKI digital signature approach, ECDSA [23], is adopted in BP. Suppose the vehicle inspection is an annul check [2], and the certificate validity period ΔT =1 min [5,8]. We consider the implementation of Tate pairing on an MNT curve [25] with embedding degree 6, where $\mathbb{G}$ is represented by 161 bits, and the order q is represented by 160 bits. Moreover, the used hash function $h(.)$ is SHA-1. In this way, Tables IV and V give the corresponding size in bytes for the certificates presented in this paper. Let T_{mul} denote the time to perform one point multiplication in $\mathbb{G}$, and T_{par} the time of a pairing operation. Since T_{mul} and T_{par} dominate the speed of message signing and signature verification, we only consider these operations to evaluate all anonymous authentication schemes. For simplicity, the vehicles and RSUs are supposed to equip an Intel Pentium IV 3.0 GHZ machine and run the same implementation of Tate pairing in [25]. Then, the following simulation adopts the measured processing time in [25], i.e., T_{mul} = 0.6 msec, and T_{par} = 4.5 msec.

A. Revocation Overhead

1) The updated CRL size: The updated CRL will be transmitted to all vehicles by vehicle-to-vehicle communication. The smaller the CRL, the better it is for VANET.

Table VI presents the CRL size to revoke one vehicle. In BP, ECPP and DCS, all the pseudo identities of unexpired certificates belonging to the revoked vehicle should be added into the CRL. Since the maximal size of short-time pseudonymous certificate set in both ECPP and DCS is L_w, the average number of unexpired certificates is $(L_w+1)/2$. In PASS, two hash seeds and the corresponding time windows numbers will be added into the CRL, while the secret key of the revoked vehicle should be disclosed in Hybrid. So the CRL size in PASS and Hybrid is constant.

TABLE VI
CRL SIZE FOR REVOKING ONE VEHICLE

method	unit size	item number	total (in bytes)
BP	21	48830	1025430
ECPP	21	$(L_w+1)/2$	$10.5*(L_w+1)$
DCS	8	$(L_w+1)/2$	$4*(L_w+1)$
Hybrid	21	1	21
PASS	48	1	48

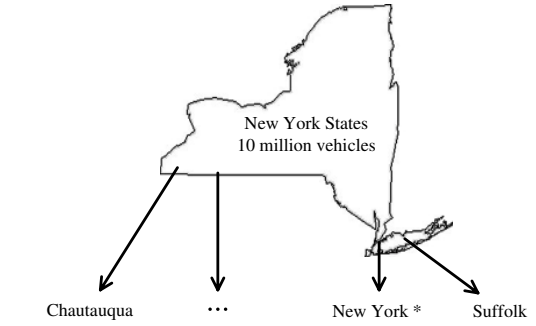
The number of revoked vehicles is another important factor for the updated CRL size. The revocation ratio (denoted as α) is defined as the ratio between the number of revoked vehicles every minute and the total number of vehicles. Suppose the TA is in charge of New York State where there are about 10 million vehicles with active registrations according to the statics of the New York State Department of Motor Vehicles [26], and the revocation ratio is uniform among the vehicles. So $\alpha * 10^7$ vehicles would be revoked every minute in the whole precinct. In BP and Hybrid, the TA should publish a CRL of all these revoked vehicles. In ECPP, DCS and PASS, the TA can divide the whole area to serval domains with the deployment of RSUs, as shown in Fig. 5. The CRL in each domain just contains the revoked membership in its own region. For example, New York city consists of Bronx, Kings, New York, Queens, and Richmond, and has 2 million registered vehicles. Suppose the real traffic in this region is about $2*(1+20\%)$ million vehicles, $\alpha * 2.4 * 10^6$ vehicles may be revoked in one minute in this domain. Fig. 6 shows the size of the updated CRL in 30 min in New York city when the revocation ratio α varies from 0 to 10^{-7}. Through the comparison between BP, ECPP, DCS and PASS and the comparison between Hybrid and PASS, it can be seen that distribute certificate service is really nice to reduce the CRL size. Furthermore, the CRL size in ECPP and DCS depends on the RSUs density, and three conditions such as L_w=1, L_w=60, and L_w=120 are presented. Obviously, if the RSUs are widely deployed, i.e., L_w=1, DCS has the smallest CRL. Otherwise, PASS performs better.

TABLE VII
REVOCATION CHECKING OVERHEAD FOR ONE MESSAGE

method	unit operation	iterations	total
BP, ECPP, DCS, and PASS	T_{hash}+T_{str}	O(1)	0
Hybrid	$2T_{par}$	N_{crl}	$2N_{crl}T_{par}$

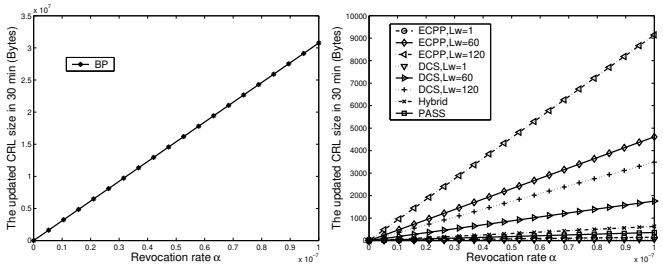
2) The overhead for revocation checking: Revocation checking should run before certificate verification and is a part of entity authentication. The summary of the checking cost is given in Table VII.

In pseudonymous authentication schemes such as BP, ECPP, DCS and PASS, when a vehicle receives a message signed by an unknown certificate, it checks the certificate pseudo identity



* This region consists of Bronx, Kings, New York, Queens, and Richmond, and has 2 million registered vehicles.

Fig. 5. Domain distribution in New York State



(a) (b)

Fig. 6. The size of the updated CRL in 30 min in New York Region

against the CRL. The efficiency of revocation checking depends on string search algorithm. Suppose they all use a hash map, the search algorithm takes $O(1)$ iterations [8]. Since the unit operation consists of a hash mapping (denoted as T_{hash}) and a string comparison (denoted as T_{str}), the total overhead can be omitted for the message authentication. In the group signature based scheme Hybrid, the checking operation against one item in CRL needs two pairing operations. Given the CRL with the size of N_{crl}, the whole cost is $2N_{crl}T_{par}$. It can be seen that the revocation checking cost for 20 received message per second can easily overcome 1 sec if N_{crl} is larger than 6.

B. The Certificate Updating Overhead

TABLE VIII
THE OVERHEAD FOR HANDLING ONE REQUEST

Method	Communication Overhead	Computation Overhead
ECPP	105+147L_w	(3+2L_w)T_{par}+ (4+9L_w)T_{mul}
DCS	270+84L_w	5T_{par}+(2+4L_w)T_{mul}
PASS	175	4T_{mul}

In this section, we compare the V2R communication overhead and the computation overhead for an RSU to handle a certificate updating request in ECPP, DCS and PASS.

In PASS, the information exchanged between a vehicle and an RSU includes the RSU certificate, the encrypted signing certificate, the hint of secret key, and the re-signature key. So the total communication overhead is 175 bytes. To serve a request, the RSU should compute the shared secret key and the re-signature key, and verify the signing certificate. So, the computation cost is $4T_{mul}$. In ECPP and DCS, a vehicle should require L_w pseudonymous certificates from an RSU. The overhead summary is given in Table VIII. It can be seen that PASS has the smallest communication overhead which is independent from L_w, while the larger the certificate number L_w, the more service burden an RSU in ECPP and DCS has.

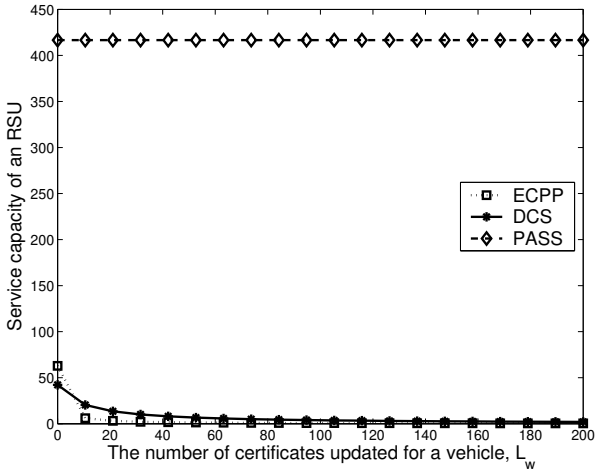


Fig. 7. The maximum number of requests that an RSU can serve per second

Furthermore, according to the computation overhead for handling a request as shown in table VIII, Fig. 7 shows the maximum number of requests that an RSU can serve per second vs. L_w, where the RSU is assumed to be equipped with an Intel Pentium IV 3.0 GHZ machine. It can be seen that PASS has the largest service capacity and performs much better than ECPP and DCS. Given L_w=60, an RSU in ECPP can handle only one request, while it can solve less than six requests in DCS. In other words, when L_w increases, the RSUs can be inclined to be overloaded or be compromised by DoS attack in ECPP and DCS.

C. Authentication Overhead

In this subsection, we analyze the overhead of authentication in three aspects: communication overhead, message signing cost, and message verification cost.

TABLE IX
COMMUNICATION OVERHEAD OF MESSAGE AUTHENTICATION

method	original format	one certificate for K messages ($K > 1$)
BP	105	$63/K + 63$
ECPP	189	$147/K + 63$
DCS	209	$167/K + 63$
Hybrid	189	$147/K + 63$
PASS	217	$175/K + 63$

1) Communication overhead: Compared with the original traffic message, the attached certificate and signature can be recognized as extra communication overhead. In PASS, since the pseudonymous certificate issued by an RSU is 175 bytes and the Schnorr signature is 42 bytes, the communication overhead for a signed message is 217 bytes. The overhead summary for BP, ECPP, DCS and Hybrid can be found in the second column in Table IX. BP achieves the smallest overhead because the vehicle certificates are issued by the TA directly. In the other schemes, a pseudonymous certificate has to embody

a credential of the certificate's issuer so that the certificate size increases.

As discussed in section V-F, it is efficient to broadcast a pseudonymous certificate once for K messages. In this way, the average overhead for a signed message in PASS decreases to $175/K + 63$ bytes. Similarly, the overheads of the other schemes are given in last column of Table IX. When K increases, the overhead is closer to 63 bytes, which is the total size of a public key and a signature.

2) Message signing cost: In PASS, a vehicle adopts Schnorr signature algorithm to sign the messages. The cryptography operation involves a point multiplication, so the signing overhead is T_{mul}. The delay is so small that there is no losing of the information accuracy of a routine traffic message. For example, suppose the speed of a vehicle is $15m/s$, its location may change less than 1 millimeter after the message have been signed. The second column in Table X gives the signing cost for BP, ECPP, DCS, Hybrid and PASS. It can be seen that all these schemes are feasible.

TABLE X
COST FOR SIGNING AND VERIFICATION

method	signing	certificate verification	signature verification
BP	T_{mul}	$2T_{mul}$	$2T_{mul}$
ECPP	T_{mul}	$3T_{par}$+$9T_{mul}$	$2T_{mul}$
DCS	$2T_{mul}$	$3T_{par}$+$2T_{mul}$	$3T_{par}$+T_{mul}
Hybrid	T_{mul}	$2N_{crl}T_{par}$+$3T_{par}$+$9T_{mul}$	$2T_{mul}$
PASS	T_{mul}	$3T_{par}$+$2T_{mul}$	$2T_{mul}$

3) Message verification cost: Message verification cost consists of certificate verification and signature verification. Before verifying a vehicle certificate, revocation checking must run if the local CRL is not empty. As discussed in section V-E, the checking cost can be omitted in the pseudonymous authentication schemes while it must be accounted in group signature based schemes such as Hybrid. Therefore, the certificate verification overhead in PASS depends on the cost for verifying an RSU certificate and the RSU's signature in the vehicle certificate, which takes three pairing operations and two point multiplications. Therefore, the certificate verification cost is $3T_{par}$ + $2T_{mul}$. In addition, verifying a message signature needs two point multiplications, so the cost is $2T_{mul}$. The overhead summary for the other schemes can be found in Table X. Notice that the certificate verification overhead of Hybrid involves the revocation checking cost $2N_{crl}T_{par}$.

It can be seen that BP has the lowest certificate verification cost because its pseudonymous certificate is signed by the TA directly, and DCS and PASS have the second lowest overhead. Moreover, PASS gives the lowest signature overhead as BP does. Using the public key buffer, a vehicle just needs to verify a valid certificate once while signature verification is necessary for every received message. Therefore, signature verification dominates the message authentication efficiency after most of the certificates of the neighboring vehicles have been verified. Then, PASS can perform the best as BP does.

To further evaluate the authentication efficiency, we conduct ns-2 simulation [27] using the real vehicle trajectory data on southbound US 101 (Hollywood Freeway) in Los Angeles, California on June 15th, 2005, which was provided by Next Generation Simulation (NGSIM) project [28]. As shown in Fig. 8, the study area is approximately 640 meters in length and consists of five lanes and an auxiliary lane. The adopted simulation parameters are given in Table XI. We use the vehicle trajectory data of the period from 7:51 am to 7:51:15 am when the most part of the communication range of the selected vehicle in the second lane is in the study area. According to DSRC, each vehicle has to disseminate traffic routine message every 300 msec. Without loss of generality, suppose 5% vehicles act as misbehaving members and broadcast two fake messages every 300 msec. One fake message attaches a bogus certificate, and the other one attaches a bad signature. Considering that the traffic information varies rapidly, the vehicles would drop the messages that can not be verified every 300 msec. The message loss ratio is defined as the ratio between the number of messages dropped every 300 msec and the total number of messages received every 300 msec. Notice that DCS supports batch verification for certificates and signatures, which is more efficient than verifying them separately when there is no fake messages. To evaluate the DCS when it adopts the batch verification strategy (denoted as DCS_batch), we use the average overhead of message verification based on binary authentication tree [13]

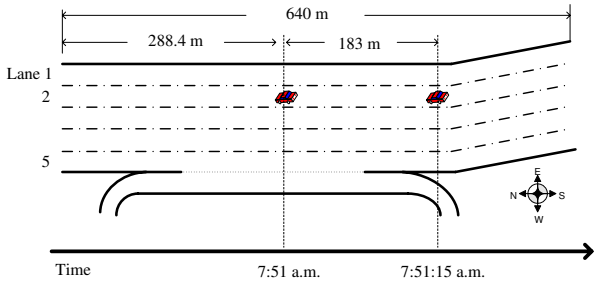


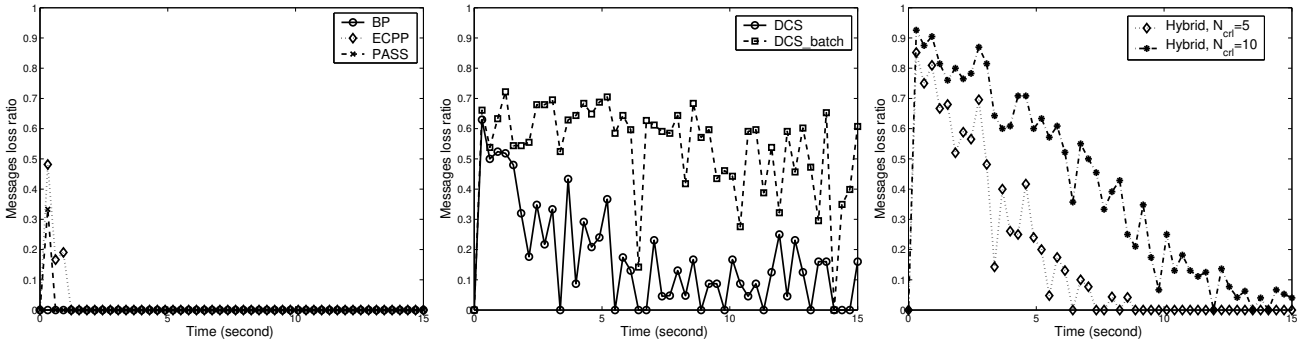
Fig. 8. The southbound direction of U.S Highway 101 in Los Angeles, California

TABLE XI
NS-2 SIMULATION PARAMETERS

parameter	value
simulation area length	640m
simulation time	15 sec
vehicle density	18 vehicles/100m
average vehicle speed	12.54 m/sec
transmission range	300 m
MAC protocol	802.11
channel bandwidth	6 Mbps

$$5(\frac{(N_f+1)}{N_m}\lg(\frac{N_m}{N_f})+\frac{4N_f-2}{N_m})T_{par}+3T_{mul},$$

where N_f is the number of fake messages ($N_f \geq 1$) every 300 msec, and N_m is the total number of received messages every 300 msec. Moreover, two conditions that $N_{crl} = 0$ and $N_{crl} = 50$ in Hybrid are observed. Fig. 9 shows the simulated message loss ratios at each 300 msec for BP, ECPP, DCS, DCS_batch, Hybrid and PASS, respectively. It can be seen that BP performs the best due to the lowest authentication overhead, and the performance of PASS is almost close to BP. At the initial stage of simulation, the vehicles in PASS have no idea on which certificates are veritable, and have to



(a) (b) (c)

Fig. 9. Comparison between message loss ratio for different schemes

verify both of the certificate and message signature for the received messages. They cannot afford so much overhead, and some messages will be dropped. As the number of verified certificates increases in the following stages of simulation, the message verification overhead is only contingent upon the signature verification, so PASS performs as efficiently as BP. With the same reasons, the message loss ratios in ECPP, DCS and Hybrid are also large at the beginning, and reduce as the running of the simulation. Because the certificate verification cost is high in DCS and Hybrid, and the number of received bogus certificates varies every 300 msec, the message lost ratios in them do not decrease monotonously. Moreover, we can observe the DCS_batch also doesn't work well, the reason is that the batch verification is not efficient once the fake messages exist.

D. Storage Overhead for A Vehicle

In PASS, a vehicle obtains $C * L_w$ secret keys, $C * L_w$ pseudonymous certificates and C signing certificates from TA, which dominate the storage overhead. According to the certificate size given in Tables IV and V, we can obtain the storage overhead

$$Stor = C * L_w * 21 + C * L_w * 66 + C * 66$$

Suppose all vehicles can pass through an RSU within 60 min, so L_w = 60 and C = $24 * 365$ = 8760. Therefore, the storage overhead $Stor$= 4605360 bytes $\approx$ 45Mbytes, which is acceptable for the current storage capacity.

VIII. CONCLUSIONS

In this paper, we have proposed an efficient pseudonymous authentication scheme with strong privacy preservation (PASS) for secure vehicular communications. PASS can not only satisfy the security and privacy requirements of VANET but also significantly reduce the revocation cost and the certificate updating overhead. Furthermore, PASS provides strong privacy preservation to the vehicles so that the adversaries can not trace the legitimate vehicles even though they have compromised all RSUs. For our future work, we will investigate the location privacy issue under the context of the proposed PASS scheme.

ACKNOWLEDGEMENTS

We would like to thank Xiaohui Liang, Qiaolin Hu, Baokang Zhao, and the anonymous reviewers for their helpful comments. This work is partially supported by the grants from National Grand Fundamental Research 973 Program of China under Grant No. 2005CB321801 and No. 2009CB320503, the National 863 Development Plan of China under Grant No. 2008AA01A325 and No. 2009AA01Z423, the National Science Foundation of China under Grant No. 90604006, and the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

[1] "Dsrc its standards advisory," [online] Available at: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[2] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. 4th Workshop on Hot Topics in Networks (HotNets-IV)*, November 2005.

[3] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: a new vanet-based smart parking scheme for large parking lots," in *Proceedings of INFOCOM 2009*, Rio de Janeiro, Brazil, April 2009, pp. 1413–1421.

[4] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proceedings of INFOCOM 2010*, San Diego, California, USA, March 2010, pp. 1–9.

[5] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[7] J. Guo, J. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. 2007 Mobile Networking for Vehicular Environments*, Anchorage, AK, May 2007, pp. 103–108.

[8] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proc. 4th ACM international workshop on Vehicular ad hoc networks (VANET '07)*, Quebec, Canada, 2007, pp. 19–28.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. INFOCOM 2008*, Phoenix, Arizona, USA, April 2008, pp. 1229–1237.

[10] B. Bellur, "Certificate assignment strategies for a pki-based security architecture in a vehicular network," in *Proc. IEEE GLOBECOM 2008*, New Orleans, LO, November 2008, pp. 1–6.

[11] C. Jung, C. Sur, Y. Park, and K. Rhee, "A robust conditional privacy-preserving authentication protocol in vanet," in *Proc. MobiSec 2009*, Turin, Italy, June 2009.

[12] A. Wasef, Y. Jiang, and X. Shen, "DCS: An efficient distributed certificate service scheme for vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, pp. 533–549, 2010.

[13] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: A robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, 2009.
[14] K. Laberteaux, J. Haas, and Y. Hu, "Security certificate revocation list distribution for vanet," in *Proc. 5th ACM international workshop on VehiculAr Inter-NETworking (VANET '08)*, California, USA, 2008, pp. 88–89.
[15] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proc. 5th ACM international workshop on VehiculAr Inter-NETworking (VANET '08)*, California, USA, 2008, pp. 86–87.
[16] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in *Proc. ACM CCS 2008*, Virginia, USA, October 2008, pp. 511–520.
[17] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. ACM CCS 2004*, 2004, pp. 168–177.
[18] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Proc. IEEE WCNC 2005*, no. 1187-1192, March 2005.
[19] J. Freudiger, M. Raya, M. Feleghhazi, P. Papadimitratos, and J.-P. Hubaux, "Mix zones for location privacy in vehicular networks," in *Proc. WiN-ITS 2007*, August 2007.
[20] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for vanet," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 25, no. 8, pp. 1569–1589, 2007.
[21] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology - CRYPTO 2001*, vol. LNCS 2139. Springer-Verlag, 2001, pp. 213–229.
[22] C.-P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.
[23] W. Mao, *Modern Cryptography: Theory and Practice*. Prentice Hall PTR, 2003.
[24] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.
[25] M. Scott, "Efficient implementation of cryptographic pairings," [online] Available at: http://ecrypt-ss07.rhul.ac.uk/Slides/Thursday/mscottsamos07.pdf.
[26] The New York State Department of Motor Vehicles, "NYS DMV - statistics - vehicle registrations in force - 2008," [online] Available at: http://www.nysdmv.com/Statistics/regin08.htm.
[27] "The network simulator - ns-2," [online] Available at: http://nsnam.isi.edu/nsnam/index.php/.
[28] "The next generation simulation (ngsim) program," [online] Available at: http://www.ngsim.fhwa.dot.gov/.

Yipin Sun (S'09) is currently working toward a Ph.D. degree with the School of Computer at National University of Defense Technology. Between Sep, 2008 to Sep, 2009, he was working with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include intrusion detection, network security, and applied cryptography.

Rongxing Lu (S'09) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xiaodong Lin (S'07-M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the IEEE International Conference on Computer Communications and Networks (ICCCN 2009) and the IEEE International Conference on Communications (ICC 2007) - Computer and Communications Security Symposium.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen has served as the Technical Program Committee Chair for IEEE VTC'10, the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He has also served as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; Computer Networks; and ACM/Wireless Networks, Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of IEEE Communications Society.

Jinshu Su (M'05) received his B.S degree of mathematics from Nankai University in 1985, and his M.S and Ph.D degrees from National University of Defense Technology in 1988 and 2000 respectively, both in Computer Science. He is a professor with the School of Computer at National University of Defense Technology. His research interests include Internet architecture, Internet routing, security, and wireless networks. Currently, he leads the Distributed Computing and High performance Router (DCHR) Lab and the Computer Networks and Information Security (CNIS) Lab, both are key Labs of National 211 and 985 projects, CHINA. He also leads the High performance computer networks (HPCN) Lab, which is a key Lab of Hunan Province, CHINA.