NEHCM: A Novel and Efficient Hash-chain based Certificate Management Scheme for Vehicular Communications

Yipin Sun[†,‡], Rongxing Lu[‡], Xiaodong Lin[§], Jinshu Su[†] and Xuemin (Sherman) Shen[‡]
[†] School of Computer Science, National University of Defense Technology, Changsha, Hunan, P.R. China 410073
[‡] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
[§]Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, Canada
Email: {ypsun, rxlu, xshen}@bbcr.uwaterloo.ca, Xiaodong.Lin@uoit.ca, sjs@nudt.edu.cn

***Abstract*— In this paper, we propose a Novel and Efficient Hash-chain based Certificate Management (NEHCM) scheme for vehicular communications. In NEHCM, to protect driver privacy, each vehicle is equipped with a large set of short-time certificates, and most importantly, serial numbers of these certificates satisfy hash-chain relationship. As a result, the certificate revocation becomes an easy task by simply releasing two hash chain seeds. However, without knowing the seeds, it is infeasible to reveal the linkability among these certificates. Thus, not only vehicles can obtain enough certificates for privacy preservation, but also the size of Certificate Revocation List (CRL) remains linear to the number of revoked vehicles, irrelative to the large number of revoked certificates in NEHCM. Furthermore, NEHCM adopts Roadside Units (RSUs) aided certificate service architecture, but the service overhead for an RSU is very low and irrelated to the number of the updated certificates. Extensive simulations demonstrate that the proposed scheme outperforms previously reported works in terms of the revocation cost.**

***Keywords* – Vehicular communications; Privacy preservation; Certificate Management; Hash chain**

I. Introduction

Vehicular ad hoc networks (VANETs) are expected to improve road safety and optimize traffic management. By equipping wireless On-Board Units (OBUs), vehicles can exchange speed and location information which is useful for driving assistance and accident warning. Meanwhile, the authentication for such life-critical information is essential, which can guarantee that any received message is indeed sent by a legitimate user and has not been altered. Even though user and data authentication was extensively studied in wired and wireless networks, it faces more challenges in VANETs [1], [2]: (1) *privacy preservation*. The privacy of drivers is compromised if the messages including their speed and position information are linked with themselves; (2) *identity revocation*. The membership of malicious vehicles should be revoked in time, and legitimate vehicles can distinguish the messages signed by the revoked members in VANETs.

Pseudonymous authentication is suggested as one way of improving privacy in VANETs [1], [3]–[7]. Raya et al. [1] introduce a basic pseudonym scheme (denoted as BP in the following context), where each vehicle stores a large set of certificates without its real identity information, called pseudonyms, and randomly chooses one of the available pseudonyms for signing a message at one time. Before validating the sender's signature on the received message, vehicles first check the certificate serial numbers included in the messages with Certificate Revocation List (CRL) published by the trust authority (TA). A limitation of this work is that the size of CRL can increase rapidly so it is difficult to transmit a large CRL to each vehicle in a timely fashion. In [4], Calandriello et al. propose a hybrid scheme (denoted as HS in the following context), where each vehicle can generate public and private key pairs by itself based on a group signature scheme. When a malicious vehicle is detected, TA only needs to add one item in Revocation List (RL). This scheme can reduce the size of RL, but the cost of identity checking with each revoked item increases. Reducing the validity period of legitimate credentials is favorite for decreasing the size of CRL, Lu et al. [5] propose that vehicles obtain short-time anonymous keys from Roadside Units (RSUs) frequently. Given the validity period is short enough, it becomes unnecessary for vehicles to have a copy of CRL. Instead, RSUs receive CRL from TA, and issue short-time anonymous keys for legitimate vehicles that are not in CRL. Wasef et al. [6] also propose a similar short-time certificate management scheme, named ECMV, which supports hierarchical architecture and batch signature verification.

The RSU-aided certificate service schemes [5]–[7] could perform well when the presence of RSUs is pervasive. However, RSUs deployment may not be ready everywhere due to the huge cost, especially at the early deployment stage of VANETs. When there are a few RSUs existing in a large area, e.g., metropolis, most vehicles may contact with an RSU once in hours or days. In this way, the validity period of short-time certificate should increase as well, so it is better to publish CRL to all vehicles. Moreover, vehicles need to request multiple certificates from RSUs for privacy preservation, then two problems are drawn attention and become critical: (1) due to the limited wireless channel bandwidth and computation capacity, RSUs can not afford to issue multiple certificates for so many vehicles passing by RSUs quickly. More seriously,

CHINACOM 2010, August 25-27, Beijing, China

DOI 10.4108/chinacom.2010.88

the malicious vehicles may request certificates from RSUs repeatedly to obtain a large certificate set or launch Deny of Service (Dos) attack; (2) the CRL still increases very quickly that its size is in direct proportion to the number of certificates taken by each vehicle. Therefore, efficient and flexible pseudonymous certificate management scheme is required to solve the collisions between privacy preservation and identity revocation.

To solve these issues, we propose a Novel and Efficient one-way Hash-chain based Certificate Management scheme, named NEHCM, which can be applied in any public key based authentication schemes [1]. In NEHCM, a large set of certificates whose serial numbers satisfy some hash-chain based serial relationship can be revoked by only releasing two hash seeds. However, it is infeasible to reveal the linkability among these certificates without knowledge on the correct seeds. In this way, vehicles can get enough pseudonyms for privacy preservation while the size of the CRL is just linear in the number of revoked vehicles. Furthermore, the communication cost and computation cost of RSUs are immune to the level of privacy preservation. The greedy vehicles can not benefit more even though they request the RSU service repeatedly. Extensive simulations demonstrate that the proposed scheme indeed outperforms previously reported works. As many symbols are used in this paper, Table I summarizes important ones.

TABLE I
NOTATIONS

Symbol	Notation
ΔT	the privacy requirement on the validity period length of a pseudonym
TS_j	the j-th time slot
TW_q	the q-th time window which contains N_{RSU} time solts
CA_k	the k-th certificate authority
RSU_g	the g-th RSU
V_i	the i-th vehilce
E	an entity, which could be a vehicle, an RSU or a CA
ID_E	the long-term unique identity of E
PuK_E, PrK_E	public key and private key of E
$\mathsf{Sig}_{PrK_E}(.)$	a signature function with PrK_E, the correction of which can be verified by others with PuK_E
$\mathsf{Cert}^j_{V_i}$	the j-th certificate of V_i
$SN^j_{V_i}$	the unique serial number of $\mathsf{Cert}^j_{V_i}$
$VP^j_{V_i}$	the validity period of $\mathsf{Cert}^j_{V_i}$
$\mathsf{Frg\_Cert}^j_{V_i}$	the fragmentary $\mathsf{Cert}^j_{V_i}$ lacking the serial number
$\mathsf{Key}^q_{V_i}$	an activation keys, using for reverting the serial number of certificates and can be decrypted by RSUs.
$\mathsf{Enc}_{SSK}(.)$	a secure symmetric encryption algorithm with secret key SSK
H(.)	one-way hash function as SHA1

The remainder of the paper is organized as follows. In section II, we present the system model, the basic pseudonymous authentication scheme, and the research objectives. The NEHCM is proposed in section III. In section IV, we analyze the storage overhead of vehicles in NEHCM and compare NEHCM with previous works in terms of revocation cost. Section V concludes the paper.

II. PRELIMINARIES

In this section, we formalize the system model, basic pseudonymous authentication, and identify the research objectives.

A. System Model

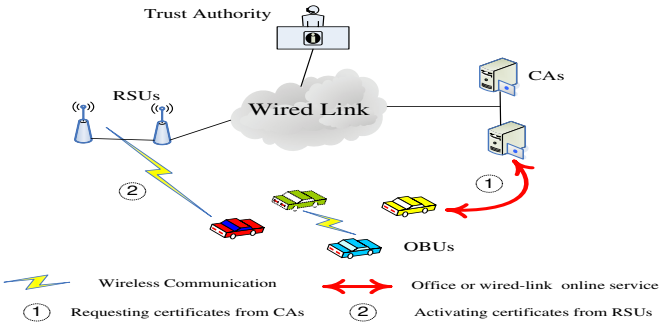

Fig. 1. System model

As shown in Fig. 2, a typical VANET consists of four entities in city scenarios: the top TA, the certificate authorities (CAs), the immobile RSUs at the road side, and vehicles equipping OBUs. Each entity has a long-term unique identity. TA, CAs and RSUs act as the infrastructure of VANETs, while CAs and RSUs are connected with the TA by wired links.

- *TA:* TA is fully trusted by all parties in the system. If any vehicle is comprised, TA adds its identity into Vehicle Revocation List (VRL), and the serial number of its pseudonyms to CRL respectively. TA publishes these VRL and CRL periodically.
- *CA:* Each CA is in charge of the registration of RSUs and vehicles in its own coverage area. Moreover, CA can issue serval fragmentary pseudonyms lacking serial number for any vehicle by wired-link online service or office service. The serial number of pseudonym can be recovered by $RSUs$ service.
- *RSU:* The RSU participates in certificate management. When a vehicle submits its identity and authentication credential to an RSU for requesting a certificate service, the RSU will deal with the request if the vehicle is legitimate and passes authentication.
- *Vehicle:* vehicles equipping OBUs mainly communicate with each other for sharing local traffic information to better the driving experiences. Each vehicle with large data storage capacity [1] can obtain a huge set of fragmentary pseudonyms issued by CAs during the vehicle investigation and communicates with RSUs for recovering the serial numbers of pseudonyms.

Since the number of RSUs is limited, most vehicles can not contact with an RSU anywhere. Let P_{RSU} denote the maximal period in which almost all vehicles can contact with an RSU, and P_{CA} denote the maximal period in which all vehicles can contact with any CA once. In an actual environment, e.g., a metropolis, P_{RSU} is likely to be hours or days in the early deployment of VANETs, P_{CA} may be years. Notice that if there is no RSUs in the aiming area, set P_{RSU}=P_{CA}.

B. Basic Pseudonymous Authentication

For basic pseudonymous authentication scheme, each vehicle has only one identity certificate and several pseudonyms [1]. Let $\mathsf{Cert}^0_{V_i}$ denote the identity certificate, and $\mathsf{Cert}^j_{V_i}$ (j≠0) denote the j-th pseudonym of V_i. Each certificate consists of two parts, the kernel property information and the signature signed by CAs, i.e. $\mathsf{Cert}^j_{V_i} = \mathsf{Info}^j_i \parallel \mathsf{Sig}_{PrK_{CA_k}}(\mathsf{Info}^j_i)$. "$\parallel$" is the concatenation operator. Info^j_i includes the serial number of certificate $SN^j_{V_i}$, the public key $PuK^j_{V_i}$, the validity period $VP^j_{V_i}$, and CA_k's identity ID_{CA_k}. Moreover, for $\mathsf{Cert}^0_{V_i}$, Info^j_i should include the identity number ID_{V_i}. CA_k maintains a map from $\{SN^j_{V_i}\}$ to ID_{V_i}, then it's easy for TA to revert the real identity of any message originator. If V_i is detected to be malicious, TA adds ID_{V_i} to VRL, and appends $\{SN^j_{V_i}\}$ of its unexpired pseudonyms to CRL.

C. Research Objectives

Basic pseudonymous authentication can improve privacy in VANETs, but the revocation cost increases obviously as well. Therefore, the kernel goal in this paper is to design an efficient pseudonymous certificate management scheme which can strengthen privacy preservation and restrain the revocation cost at the same time. Moreover, RSUs are expected to provide certificate service as well in the context of this paper. However, due to the limited wireless channel bandwidth and computation capacity, our scheme should not bring extra burden to RSUs even for high privacy preservation. Moreover, vehicles can't gain additional benefits by requesting RSUs service repeatedly.

III. The Proposed NEHCM Scheme

In this section, we describe the proposed NEHCM scheme and analyze its security. We first review the hash chains, which serves the basis of NEHCM.

A. Hash Chains

A one-way hash function $H(.)$ is said to be secure if the following properties are satisfied [8]: 1) $H(.)$ can take a message of arbitrary length as input and produce a message digest of a fixed-length output. 2) Given x, it is easy to compute $H(x) = y$. However, it is hard to compute $H^{-1}(y) = x$ given y. 3) Given x, it is computationally infeasible to find $x' \neq x$ such that $H(x') = H(x)$.

B. Initialization

TA publishes some public parameters for the whole system: (1) the time period ΔT. For simplicity, suppose that the privacy requirements for most vehicles are satisfied if each pseudonym is used no more than ΔT; (2) TA divides the time domain into a serial time slots by ΔT. let TS_j denote the j-th time slot that ends at j*ΔT, and n denote the serial number of current time slot; (3) the maximal total number of intact pseudonyms that each vehicle can take, N_{RSU}, where $N_{RSU} = \lceil P_{RSU}/\Delta T \rceil$; (4) TA divides the time domain into a serial time windows by $N_{RSU} * \Delta T$. let TW_q denote the q-th time slot that ends at q*$N_{RSU} * \Delta T$; (4) the total number of pseudonyms which a vehicle should require from CAs each time, N_{CA}, where $N_{CA} = \lceil P_{CA}/(N_{RSU} * \Delta T) \rceil * N_{RSU}$; (5) the validity period length of a pseudonym equals 2*ΔT.

Each CA_k has a sequence of secret keys $\{SK^q_{CA_k}\}$. When the time window TW_{q-1} begins, CA_k submits $SK^q_{CA_k}$ to TA, then TA transmits $SK^q_{CA_k}$ to all legitimate RSUs in secure communication. CA_k maintains a large set of hash seeds, HS_k, where $HS_k = \{<SD_L, SD_R> | \forall i \in [1, N_{CA}], H(H^i(SD_L) \| H^i(SD_R))$ is unique as the serial number of a certificate$\}$.

Each V_i has a unique identity certificate $\mathsf{Cert}^0_{V_i}$ as introduced in section II-B, while its pseudonyms are mapping to a time slot. Let $\mathsf{Cert}^j_{V_i}$ denote the j-th certificate of V_i, then set $VP^j_{V_i}$ = j*ΔT, which makes $\mathsf{Cert}^j_{V_i}$ is valid in time slots TS_j. Moreover, V_i needs two steps to obtain an intact pseudonym. First, it gets the fragmentary pseudonym lacking the serial number (denoted as $\mathsf{Frg\_Cert}^j_{V_i}$) from any CA_k, where $\mathsf{Frg\_Cert}^j_{V_i} = PuK^j_{V_i} \| VP^j_{V_i} \| ID_{CA_k} \| \mathsf{Sig}_{PrK_{CA_k}}(SN^j_{V_i} \| PuK^j_{V_i} \| VP^j_{V_i} \| ID_{CA_k})$. Secondly, V_i recovers $SN^j_{V_i}$ by the assistance of an RSU. This process is called *certificate activation*. Notice that, if there is no RSUs in early system, V_i obtains intact pseudonyms directly from CAs.

C. Certificate Generation

Legitimate V_i can request N_{CA} fragmentary pseudonyms $\{\mathsf{Frg\_Cert}^j_{V_i}\}$ from any CA_k during the vehicle investigation. There are four steps:

Step1: V_i launches the key agreement process with the known CA_k, and gets the shared secret key Ssk_{V_i,CA_k}.

Step2: V_i generates N_{CA} pairs of public key and private key $\{< PuK^j_{V_i}, PrK^j_{V_i} >\}$ (j∈[n+1,n+N_{CA}]). Let T_{stamp} denote the current time stamp. Furthermore, V_i composes a request message, where

$$\begin{cases} m = T_{stamp} \| PuK^{n+1}_{V_i} \| ... \| PuK^{n+N_{CA}}_{V_i} \\ M = m, \mathsf{Sig}_{PrK^0_{V_i}}(m), \mathsf{Cert}^0_{V_i}. \end{cases}$$

Then V_i sends $\mathsf{Enc}_{\mathsf{Ssk}_{V_i,CA_k}}$(M) to CA_k.

Step3: Upon receiving the request message, CA_k first decrypts it. If T_{stamp} is fresh and ID_{V_i} is not in VRL, CA_k deals with this request. CA_k selects one pair $<SD_L, SD_R>$ randomly from HS_k, and set $HS_k = HS_k - <SD_L, SD_R>$. Then CA_k generates pseudonyms for these time slots from TS_{n+1} to $TS_{n+N_{CA}}$, where

$$\begin{cases} j \in [n+1, n+N_{CA}], \\ f(j) = N_{CA} - j + n, \\ LSN^j = H^{j-n}(SD_L), \\ RSN^j = H^{f(j)}(SD_R), \\ SN^j_{V_i} = H(LSN^j \oplus RSN^j), \\ VP^j_{V_i} = j * \Delta T, \\ \mathsf{Info}^j_i = SN^j_{V_i} \| PuK^j_{V_i} \| VP^j_{V_i} \| ID_{CA_k} \end{cases}$$

At same time, CA_k adds a 4-tuples $<ID_{V_i}, n+1, SD_L, SD_R>$ into its local database. For reverting the real identity of a vehicle quickly, CA_k also stores the identity mapping $<VP^j_{V_i}, SN^j_{V_i}\ ID_{V_i}>$ for each

pseudonym. CA_k composes the first part of response message (denoted as $m1$), where $m1$=$SD_L \| \mathsf{Sig}_{PrK_{CA_k}}(\mathsf{Info}_i^{n+1}) \| ... \| \mathsf{Sig}_{PrK_{CA_k}}(\mathsf{Info}_i^{n+N_{CA}})$. Then, V_i can recompose $\mathsf{Frg\_Cert}_{V_i}^j$ from $m1$ and compute LSN^j using SD_L. However, V_i can not deduce the $SN_{V_i}^j$ without RSN^j.

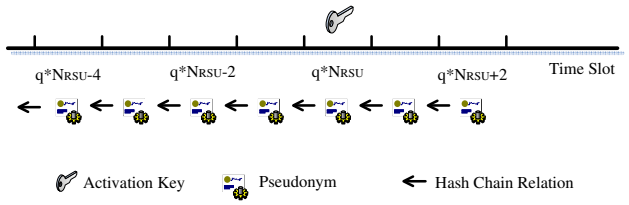

Fig. 2. Relationship between pseudonyms and activation keys

On the other hand, CA_k encrypts these $RSN_{V_i}^{q*N_{RSU}}$, named activation keys, for recovering the serial numbers of pseudonyms. Fig. 2 illustrates the relationship between pseudonyms and activation keys. Let $\mathsf{Key}_{V_i}^q$ denote q-th activation keys. For any q $\in [n/N_{RSU}+1, (n+N_{CA})/N_{RSU}]$, set $\mathsf{Key}_{V_i}^q$=$\mathsf{Enc}_{SK_{CA_k}^q}(ID_{V_i} \| q \| Enc_{LSN^{q*N_{RSU}}}(RSN^{q*N_{RSU}}))$. Then, the other part of response message (denoted as $m2$) is composed , where $m2$=$\{\mathsf{Key}_{V_i}^q\}$.

Furthermore, CA_k composes the response message M, where $M = m1 \| m2 \| \mathsf{Sig}_{PrK_{CA_k}}(m1 \| m2)$, and sends $\mathsf{Enc}_{\mathsf{Ssk}_{V_i,CA_k}}(M)$ back to V_i.

Step4: After decrypting the response message from CA_k, V_i first verifies its signature. If it is right, V_i stores these credentials $\{LSN^j \| \mathsf{Frg\_Cert}_{V_i}^j\} \cup \{\mathsf{Key}_{V_i}^q\}$.

D. Certificate Activation

V_i requests RSU service for recovering the serial number of pseudonyms for following time window when it passes by an RSU RSU_g. There are three steps:

Step1: Suppose the time window is TW_q, and V_i wants to activate the pseudonyms issued by ID_{CA_k}, then V_i selects $\mathsf{Key}_{V_i}^{q+1}$, and sends the request message M=$ID_{CA_k} \| q+1 \| \mathsf{Key}_{V_i}^{q+1}$.

Step2: Upon receiving the request message M=$ID_{CA_k} \| \mathsf{Key}_{V_i}^{q'}$, RSU_g decrypts $\mathsf{Key}_{V_i}^{q'}$ with the secret key $SK_{CA_k}^q$ published by TA. Suppose $\mathsf{Key}_{V_i}^{q'}$=$q' \| Enc_{LSN^{q'*N_{RSU}}}(RSN^{q'*N_{RSU}}$, if $q' = q+1$ and ID_{V_i} is unexpired, RSU_g sends $Enc_{LSN^{q'*N_{RSU}}}(RSN^{q'*N_{RSU}}$ back to V_i. At last, RSU_g sends the service record $<ID_{V_i}, ID_{CA_k}$,q+1$>$ to TA.

Step3: V_i decrypts the response message with $LSN^{(q+1)*N_{RSU}}$, and checks $RSN^{q*N_{RSU}} \stackrel{?}{=} H^q(RSN^{(q+1)*N_{RSU}})$. If it is successful, V_i computes $SN_{V_i}^j$ for $\mathsf{Frg\_Cert}_{V_i}^j$, such that for j $\in [q*N_{RSU}+1, (q+1)*N_{RSU}]$, set $RSN^j = H^{(q+1)*N_{RSU}-j}(RSN^{(q+1)*N_{RSU}})$, and $SN_{V_i}^j = H(LSN^j \oplus RSN^j)$. Furthermore, V_i verifies these latest intact pseudonyms. If the verification doesn't pass, V_i reports the abnormity to TA. Otherwise, the certificate activation process is completed.

E. Revocation

When abnormal behaviors are detected, TA can revert the real identity of malicious vehicles with the help of CAs. Suppose TA decides to forbid the vehicle ID_{V_i} using VANETs from the current time slot TS_n to the time slot $TS_{FD_{V_i}}$ ($FD_{V_i} \geq$n), it adds $<ID_{V_i}, FD_{V_i}>$ to VRL which is published to CAs and RSUs as soon as possible. CAs and RSUs won't provide service to ID_{V_i} until $TS_{FD_{V_i}}$ ends. Furthermore, Suppose the current time window is TW_q, TA search the service reports submitted by all RSUs, if V_i had obtained intact pseudonyms issued by CA_k before $TW_{q'}$ ends, where $q' = qorq+1$, then TA informs CA_k to release the serial numbers of unexpired pseudonyms held by V_i, i.e., $\{\ \mathsf{Cert}_{V_i}^j \| j \in [n, q'*N_{RSU}]\}$. Then, CA_k sends $< n, LSN_{V_i}^n, q'*N_{RSU}, RSN_{V_i}^{q'*N_{RSU}} >$ to TA, and TA adds it into revocation list which would be transmit to all vehicles by vehicle-to-vehicle communication [9].

Let CRL_j denote the local CRL of a vehicle used in time slot TS_j. After receiving the revocation list published by TA, i.e., $\{<x, LSN_U^x, y, RSN_U^y>\}$, any vehicle computes SN_U^j=$H(H^{j-x}(LSN_U^x) \oplus H^{y-j}(RSN_U^y))$ ($j \in [x,y]$), and adds SN_U^j in both CRL_{j-1} and CRL_j. Please notice that it is hard to compute LSN_U^{x-1} based on LSN_U^x, so public entities cannot reduce the serial numbers of the pseudonyms which are used by the vehicle U before it was revoked. Moreover, Since vehicle can construct CRL_j using the idle time in the time slot TS_{j-1}, the cost has small influence to system performance.

F. Security Analysis

In this subsection, we analyze the security of the proposed scheme in terms of message authentication and integrity, non-repudiation, privacy preserving, and mitigation of DoS attack against the RSUs.

1) *Message authentication and integrity.* In the proposed scheme, each entity should sign its signature before sending messages, and any receiver should check its validity of the message. Therefore, if the serial number of certificate in message lies in CRL, the message will be dropped. What's more, if the message has been modified by an attacker, the verification won't pass.
2) *Non-repudiation.* Based on the signature enclosed in message as well, TA can reveal the real identity of the originator, while the originator also can't deny that the message generated by itself.
3) *Privacy preserving.* Based on one-way hash function, anyone, without knowing two hash seeds, can not link those messages signed by same originator. Furthermore, even a vehicle was revoked, any public entity cannot reduce the serial numbers of the pseudonyms which are used by the revoked vehicle before revocation. Therefore, our scheme provides strong privacy preservation to the vehicles.
4) *Mitigation of DoS attack against the RSUs.* In the proposed scheme, a vehicle can obtain N_{RSU} intact

pseudonyms from an RSU service. However, the size of the exchanged messages between a vehicle and an RSU and is constant and irrelated to the number of revoked vehicles. Therefore, the service overhead for an RSU is very low. Moreover, the greedy drivers can not benefit more no matter how many times they request the RSU service repeatedly. It decreases the risk for an RSU to be compromised by the DoS attack.

IV. Performance Evaluation

In this section, we evaluate the performance of the proposed NEHCM scheme in terms of the revocation cost and the pseudonym storage of vehicles. Without loss of generality, suppose a vehicle contacts with CAs once a year, and changes certificates per minute for privacy preservation, i.e., P_{CA}=1 Year, and ΔT=1 Minute. In early deployment stage of VANETs, the RSU density is very small, and suppose P_{RSU}=1 Day. In short-time certificate schemes [5], [6], a vehicle has to obtain 1440 certificates from an RSU. It is impractical for the RSUs to issue so many certificates for each passing-by vehicle. Therefore, we just compare NEHCM with BP [1] and HS [4] here. Suppose he classical PKI digital signature approach, ECDSA, is adopted in NEHCM and BP. Moreover, all three schemes run the implementation of Tate pairing on a MiyajiCNakabayashiCTakano curve with embedding degree 6 and group order 160 bits.

A. Revocation Cost

TABLE II
CRL size for revoking one vehicle

method	unit size	item number	total (in bytes)
BP	20	PS_{BP}	20*PS_{BP}
HS	21	1	21
NEHCM	48	1	48

Table II presents the CRL size to revoke one vehicle. PS_{BP} is denoted the size of pseudonym set in each vehicle in BP, where PS_{BP}= $P_{CA}/\Delta T$=525600 in the simulation. Obviously, the size of the updated CRL in NEHCM and HS is constant to revoke a vehicle. Furthermore, suppose in a city with 5 million vehicles, and 10^{-6} of these vehicles may be revoked in half an hour. The size of the updated CRLs in NEHCM and HS are 240 Bytes and 105 Bytes respectively while the CRL in BP is too large, i.e. more 50 MB, to be transmitted by vehicle-to-vehicle communication [9].

Although HS performs the best in term of the CRL size, its checking operation against one item in CRL needs two pairing operations which could take about 10^4 times of computation cost than a string comparison, e.g., the computation overhead for a vehicle is 10^{-2} sec in [4]. Given that CRL usually contains 10 revoked identities and a vehicle receives 20 messages per second, the total checking cost is 2 sec. In BP and NEHCM, a vehicle just checks the serial number of pseudonym 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 [4][5], and the total overhead can be omitted.

B. Pseudonym Storage Overhead of Vehicles

In our scheme, pseudonym set costs the storage space in vehicles. Through a requesting process, vehicle gets N_{CA} pseudonyms and N_{CA}/N_{RSU} activation keys. Let S_{cert} denote the size of a certificate, and S_{act} denote the size of an activation key. The storage for pseudonym requesting each time is $Stor_{pse} = N_{CA} * S_{cert} + \lceil N_{CA}/N_{RSU} \rceil * S_{act}$.

In the simulation, it can be seen that S_{cert}= 87 Bytes and S_{act}= 28 Bytes. Then, $Stor_{pse}$≈46 MB, which is acceptable for the current storage capacity.

V. Conclusions

In this paper, we have proposed a novel efficient one-way hash-chain based certificate management (NEHCM) scheme, which strengthens privacy preservation without increasing revocation cost. Furthermore, the service overhead for an RSU is very low and irrelated to the number of the updated certificates. For our future work, we intent to investigate the diversity of privacy preservation for vehicles with different backgrounds in NEHCM.

Acknowledgements

The work described in this paper is partially supported by the grants from National Grand Fundamental Research 973 Program of China under Grant No. 2005CB321801 and No. 2009CB320503, by the National 863 Development Plan of China under Grant No. 2008AA01A325 and No. 2009AA01Z423, by the National Science Foundation of China under Grant No. 90604006, and by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

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

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, "Security in vehicular ad hoc networks", *IEEE Communications Magazine*, Vol. 46, No. 4, pp. 88-95, 2008

[3] 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.

[4] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET", in *Proc. the fourth ACM international workshop on Vehicular ad hoc networks 2007*, Montreal, Quebec, Canada Sep., 2007.

[5] R. Lu, X. Lin, H. Zhu, P.-H. Ho and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communicationss", in *Proc. INFOCOM 2008)*, Phoenix, Arizona.

[6] A. Wasef, Y. Jiang, and X. Shen, "ECMV: Efficient Certificate Management Scheme for Vehicular Networks", *Proc. IEEE Globecom'08*, New Orleans, LA, USA, Nov. 2008.

[7] C. Jung, C. Sur, Y. Park, and K. Rhee, "A robust conditional privacy-preserving authentication protocol in VANET", in *Proc. MobiSec 2009*, pp. 35-45, Turin, Italy, June 2009.

[8] W. Mao, "Modern cryptography: theory and practice", *Upper Saddle River, NJ: Prentice-Hall PTR*, 2003.

[9] K. Laberteaux, J. Haas and Y. Hu, "Security certificate revocation list distribution for vanet", in *Proc. the fifth ACM international workshop on VehiculAr Inter-NETworking 2008*, San Francisco, California, USA September 15, 2008.