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

Yipin Sun, Rongxing Lu, Xiaodong Lin, Jinshu Su, Xuemin (Sherman) Shen
Date Submitted: 7 June 2009
Date Published: 11 June 2009

Updated information and services can be found at:
http://129.97.58.88/ojs-2.2/index.php/pptvt/article/view/496

These include:

Subject Classification Vehicular Technology > Wireless Networks

Keywords Vehicular communications; Privacy preservation; Certificate Management; Hash chain; Information security;

Comments You can respond to this article at:
http://129.97.58.88/ojs-2.2/index.php/pptvt/comment/add/496/0

Copyright ©2009 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.
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.of 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: {yipin, rxlu, xshen}@brcr.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, irrespective to the large number of revoked certificates in NEHCM. Furthermore, since NEHCM can strictly limit each vehicle’s certificate set, it decreases the risk of other attacks in vehicular communications, such as sybil attack. 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]–[5]: (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 on 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 [3]–[8]. Raya et al. [3] 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 [6], 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. [7] 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. [8] also propose a similar short-time certificate management scheme, named ECMV, which supports hierarchical architecture and batch signature verification. Furthermore, Zhang et al. [9] introduce an RSU-aided message authentication scheme, which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles.

The RSU-aided schemes [7]–[9] 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; (2) CRL increases in direct proportion to the number of certificates taken by each vehicle. More seriously, greedy vehicles may request certificates from RSUs repeatedly and obtain a large certificate set. 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 [3]. 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 with no 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. Moreover, NEHCM limits the size of certificate set in each vehicle, which can decrease the risk of other attacks such as sybil attack. Furthermore, the communication cost and computation cost of RSUs are immune to the level of privacy preservation. 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

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta T$</td>
<td>privacy requirements on the period one pseudonym is used</td>
</tr>
<tr>
<td>$TS_j$</td>
<td>the j-th time slot</td>
</tr>
<tr>
<td>$CA_k$</td>
<td>the k-th certificate authority</td>
</tr>
<tr>
<td>$RSU_g$</td>
<td>the g-th RSU</td>
</tr>
<tr>
<td>$V_i$</td>
<td>the i-th vehicle</td>
</tr>
<tr>
<td>$E$</td>
<td>an entity, which could be a vehicle, an RSU or a CA</td>
</tr>
<tr>
<td>$ID_E$</td>
<td>the long-term unique identity of $E$</td>
</tr>
<tr>
<td>$PuK_E$, $PrK_E$</td>
<td>public key and private key of $E$</td>
</tr>
<tr>
<td>$Sig_{PrK_E}(\cdot)$</td>
<td>a signature function with $PrK_E$, the correction of which can be verified by others with $PuK_E$</td>
</tr>
<tr>
<td>$Cert_{V_i}^j$</td>
<td>the j-th certificate of $V_i$</td>
</tr>
<tr>
<td>$SN_{Cert_{V_i}^j}$</td>
<td>the unique serial number of $Cert_{V_i}^j$</td>
</tr>
<tr>
<td>$VP_{Cert_{V_i}^j}$</td>
<td>the validity period of $Cert_{V_i}^j$</td>
</tr>
<tr>
<td>$Ssk_{V_i,E}$</td>
<td>the shared secret key between $V_i$ and $E$</td>
</tr>
<tr>
<td>$Frg_{Cert_{V_i}^j}$</td>
<td>the fragmentary $Cert_{V_i}^j$ lacking the serial number</td>
</tr>
<tr>
<td>$Key_{V_i}^j$</td>
<td>an activation keys, using for reverting the serial number of certificates and can be decrypted by RSUs.</td>
</tr>
<tr>
<td>$Enc_{SSK}(\cdot)$</td>
<td>a secure symmetric encryption algorithm with secret key $SSK$</td>
</tr>
<tr>
<td>$HL(\cdot)$</td>
<td>one-way hash function as SHA1</td>
</tr>
</tbody>
</table>

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](attachment:image.png)

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, and it is infeasible for any attacker to compromise. TA is in charge of the registration of CAs. TA can detect the abnormalities in VANETs. 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 trusted and in charge of the registration of RSUs and vehicles in its own coverage area. Moreover, CA can issue several 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**: RSU participates in certificate management. When a vehicle submits its identity and authentication credential to RSU for requesting a certificate service, RSU will deal with the request if the vehicle is legitimate and passes authentication. RSU then reverts the kernel part of pseudonym serial number for vehicle instead of generating pseudonyms in previously reported works [7], [8]. Note that TA can inspect all RSUs. Once an RSU is compromised, TA can detect and take action to recover it at once.

- **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 [3] takes a set of fragmentary pseudonyms issued by CAs and communicates with RSUs for recovering the serial numbers of pseudonyms.
Since the number of RSUs is limited, most vehicles cannot contact with CAs and RSUs anywhere. Let $P_{CA}$ denote the maximal period in which all vehicles can contact with any CA once, and $P_{RSU}$ denote the maximal period in which almost all vehicles can contact with RSUs. In an actual environment, e.g., a metropolis, $P_{CA}$ may be several months to one year, and $P_{RSU}$ is likely to be hours or days in the early deployment stage of VANETs. 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 [3]. Let $\text{Cert}^{0}_{i}$ denote the identity certificate, and $\text{Cert}^{j}_{i}$ (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. $\text{Cert}^{j}_{i} = \text{Info}^{j}_{i} \parallel \Sigma_{Pr\rightarrow CA_{i}}(\text{Info}^{j}_{i})$. "$\parallel"$ is the concatenation operator. $\text{Info}^{j}_{i}$ includes the serial number of certificate $SN^{j}_{i}$, the public key $Pu^{j}_{i}$, the validity period $VP^{j}_{i}$, and $CA_{i}$'s identity $ID_{CA_{i}}$. Moreover, for $\text{Cert}^{j}_{i}$, $\text{Info}^{j}_{i}$ should include the identity number $ID_{V_{i}}$. $CA_{i}$ maintains a map from $\{SN^{j}_{i}\}$ to $ID_{V_{i}}$, so 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 $\{SN^{j}_{i}\}$ of its unexpired pseudonyms to CRL.

When $V_i$ is ready to send some message payload (denoted as $m$), it first generates its signature $\Sigma_{Pr\rightarrow CA_{i}}(m)$. Then, the message format is $M = m || \Sigma_{Pr\rightarrow CA_{i}}(m) || \text{Cert}^{j}_{i}$. Other entities in VANETs can use the public key $Pu^{j}_{i}$ to verify the signature. If the verification passes and $SN^{j}_{i}$ (or $ID_{V_{i}}$) is not in CRL (VRL), the message is accepted. Moreover, when requesting services from CAs and RSUs, the communication process should be encrypted for privacy preservation. Therefore, $V_i$ first launches the key agreement process with the infrastructure node E for generating a shared secret key $Ssk_{V_{i}, E}$, then it encrypts the subsequent messages by a secure symmetric encryption algorithm $Enc_{Ssk_{V_{i}, E}}(.)$.

C. Research Objectives

Basic pseudonymous authentication can improve privacy in VANETs, but the revocation cost increases obviously as well. The revocation cost mainly contains two parts: (1) the transmission overhead of CRL. It costs the limited wireless bandwidth, and it's difficult to transmit a large CRL to all vehicles in timely fashion; (2) the checking overhead in vehicles. This overhead is proportion to the size of CRL and the cost of checking operation. Small checking overhead is favorite for submitting real-time data to driving assistant applications. 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.

Though the number of RSUs is small, with the assistance of RSUs, the validity period of certificates can be limited to the range of days or even hours, and thus it is good for decreasing the size of CRL. 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 [10]: 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 $H(x)=H(y)$. Furthermore, suppose $H^{0}(x)=x$ and $H^{i}(x)=H^{i-1}(x)$, 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 $S_{i-1}$ but infeasible to obtain $S_{i+1}$.

B. Initialization

TA publishes some public parameters for the whole system: (1) the time period $\Delta T$. For simplicity, suppose that the privacy requirements for most vehicles are satisfied if each pseudonym is used no more than $\Delta T$; (2) TA divides the time domain into a serial time slots by $\Delta T$. Let $T_{Sj}$ denote the j-th time slot that ends at $j*\Delta T$, 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 $N_{RSU}=[P_{RSU}/\Delta T]$; (4) the total number of pseudonyms which a vehicle should request from CAs each time, $N_{CA}$, where $N_{CA}=[P_{CA}(N_{RSU}/\Delta T)]*N_{RSU}$; (5) the maximal size of pseudonym set in vehicles, $N_{MAX}$, where $N_{MAX}=N_{CA}*2$. In this way, a vehicle can get enough pseudonyms just if it can contact with CAs once at any time during every $P_{CA}$; (6) the validity period length of pseudonym, $\Delta V P$, where $\Delta T < \Delta V P < 2*\Delta T$.

Each $CA_{k}$ has a sequence of secret keys $\{SK^{k}_{CA_{k}}\}$. When the time slot $T_{Sj}=T_{S(j-1)}+N_{RSU}$ begins, $CA_{k}$ submits $SK^{k}_{CA_{k}}$ to TA, then TA transmits $SK^{k}_{CA_{k}}$ to all legitimate RSUs in secure communication. $CA_{k}$ maintains a large set of hash seeds, $HS_{k}$, where $HS_{k}=\{<SD_{L}, SD_{R}> | Vi \in [1, N_{CA}], H(H^{i}(SD_{L}))=H^{i}(SD_{R})\}$ is unique as the serial number of a certificate.

Each $V_{i}$ has a unique identity certificate $\text{Cert}^{0}_{i}$ introduced in section II-B, while its pseudonyms are mapping to each time slot. In other words, suppose $\text{Cert}^{j}_{i}$ is the pseudonym corresponding to time slot $T_{Sj}$, then set $VP^{j}_{i}=j*\Delta T$. Each pseudonym $\text{Cert}^{j}_{i}$ is valid between the moment $VP^{j}_{i}$ - $\Delta V P$ to the moment $VP^{j}_{i}$.
two pseudonyms during $\Delta VP\cdot\Delta T$ time before every time slot ends, and changes pseudonyms on its own initiative at a flexible opportunity. However, $V_i$ needs two steps to obtain an intact pseudonym. First, it gets the fragmentary pseudonym lacking the serial number (denoted as $Frg\_Cert^i_{V_i}$) from any $CA_k$, where $Frg\_Cert^i_{V_i} = PuK^i_{V_i} || VP^i_{V_i} || ID_{CA_k} || \text{Sig}_{Pr\_KCA}\_k(SN^i_{V_i} || PuK^i_{V_i} || VP^i_{V_i} || ID_{CA_k})$. Secondly, $V_i$ recovers $SN^i_{V_i}$ by the assistance of RSUs. This process is called certificate activation. Notice that, if there is no RSUs in early system, $V_i$ obtains intact pseudonyms directly from CAs. Let $MV^i_{V_i}$ denote the maximal serial number of the time slot in which $V_i$ has a fragmental pseudonym, and $MV^{ac}_{V_i}$ denote the maximal serial number of the time slot in which $V_i$ has an intact pseudonym. TA maintains the record $<ID_{V_i}, MV^i_{V_i}, MV^{ac}_{V_i}>$, which should be updated as soon as $V_i$ requests and activates pseudonyms.

C. Certificate Generation

Legitimate $V_i$ can request $Frg\_Cert^i_{V_i}$ from any $CA_k$ if the total number of its unused pseudonyms is less than $N_{CA}$. There are four steps:

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

Step2: $V_i$ first checks its local $MV^i_{V_i}$. If $MV^i_{V_i} < n$, set $MV^i_{V_i} = (n-1)N_{RSU}\cdot N_{RSU}$. Then $V_i$ generates $N_{CA}$ pairs of public key and private key $<PuK^i_{V_i}, PrK^i_{V_i}> (j \in [MV^i_{V_i}+1, MV^i_{V_i}+N_{CA}])$. Let $T_{stamp}$ denote the current time stamp. Furthermore, $V_i$ composes a request message, where

$$m = T_{stamp} || MV^i_{V_i} || PuK^i_{V_i} || ... || PuK^{MV^i_{V_i}+N_{CA}}$$

Then $V_i$ sends $Enc_{SSk_{V_i,Ca}}(M)$ to $CA_k$.

Step3: Upon receiving the message request, $CA_k$ first decrypts it. Let $MV^{ac}_{V_i}$ denote the corresponding information in the request message. If $T_{stamp}$ is fresh, $MV^{ac}_{V_i}$ mod $N_{RSU} = 0$, $MV^{ac}_{V_i} - n < N_{CA}$, and $ID_{V_i}$ is not in VRL, $CA_k$ deals with this request. Firstly, it finds out $MV^i_{V_i}$ from TA. If $MV^i_{V_i} > MV^{ac}_{V_i}$, $CA_k$ stops this service, and reports this abnormality to TA. Otherwise, $CA_k$ sets $MV^i_{V_i} = MV^{ac}_{V_i}$ and 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 $TS_{MV^i_{V_i}+1}$ to $TS_{MV^i_{V_i}+N_{CA}}$, where

$$j \in [MV^i_{V_i}+1, MV^{ac}_{V_i}+N_{CA}]$$

At same time, $CA_k$ adds a 4-tuples $<ID_{V_i}, MV^i_{V_i}+1, SD_L, SD_R>$ into its local database. For reverting the real identity of a vehicle quickly, $CA_k$ also stores the identity mapping $<VP^i_{V_i}, SN^i_{V_i}, ID_{V_i}>$ for each pseudonym. $CA_k$ composes the first part of message response (denoted as $m1$),

$$m1 = MV^i_{V_i} || SD_L || \text{Sig}_{Pr\_KCA}\_k(Info^i_{V_i})$$

On the other hand, $CA_k$ encrypts these $RSN^q_{V_i,N_{RSU}}$, called activation keys, for recovering the serial numbers of intact pseudonyms. Fig. 2 illustrates the relationship between pseudonyms and activation keys. Let $Key^q_{V_i}$ denote $q$-th activation keys. For any $q \in [MV^i_{V_i}/N_{RSU} + 1, (MV^i_{V_i} + N_{CA})/N_{RSU}]$, set $Key^q_{V_i} = Enc_{SK_{CA}\_k}(ID_{V_i} || \text{q} || RSN^q_{V_i,N_{RSU}})$. Then, the other part of response message (denoted as $m2$) is composed , where $m2 = Key^q_{V_i} || MV^i_{V_i}/N_{RSU}+1 || ... || Key^{m2}_{V_i}$. Furthermore, $CA_k$ composes the response message $M$, where $M = m1 || m2 || \text{Sig}_{Pr\_KCA}\_k(m1 || m2)$, and sends $Enc_{SSk_{V_i,Ca}}(M)$ back to $V_i$. At the same time, $CA_k$ apprizes TA to update $MV^i_{V_i}$ with the new value $MV^i_{V_i}+N_{CA}$.

Step4: After decrypting the response message from $CA_k$, $V_i$ first verifies its signature. If it is successful, $V_i$ updates $MV^i_{V_i}$, set $MV^i_{V_i} = MV^i_{V_i}+N_{CA}$, and stores $<VP^i_{V_i}+1, ID_{CA_k}, M>$ (denoted $PS_{MV^i_{V_i}+1}$). Before activating the pseudonyms in $PS_{MV^i_{V_i}+1}$, $V_i$ transforms it into the format as $\{LSN^j_{V_i} || Frg\_Cert^j_{V_i}\} \cup \{Key^q_{V_i}\}$.

D. Certificate Activation

$V_i$ requests service for recovering the serial number of pseudonyms for following $N_{RSU}$ time slots when it passes by an RSU. There are four steps:

Step1: $V_i$ launches the key agreement process with the known $RSU_g$, and gets the shared secret key $SSk_{V_i,RSU_g}$.

Step2: Suppose $V_i$ wants to activate the pseudonyms in $PS_{g}$ issued by $ID_{CA_k}$, then $V_i$ selects $Key^q_{V_i}$, where $q = min(\lfloor n/N_{RSU}\rfloor + 1, (c-1+N_{CA})/N_{RSU})$. Furthermore, $V_i$ composes the request message $M$ as follows,

$$m = T_{stamp} || ID_{CA_k} || q || Key^q_{V_i}$$

Then $V_i$ sends $Enc_{SSk_{V_i,RSU_g}}(M)$ to $RSU_g$.

Step3: Upon receiving the request message, $RSU_g$ first decrypts it. If $T_{stamp}$ is fresh and $ID_{V_i}$ is not in VRL, $RSU_g$ deals with this request. If $q \leq \lfloor n/N_{RSU}\rfloor + 1$, $RSU_g$ has gotten the secret key $SK_{CA_k}^q$ from TA and can decrypt $Key^q_{V_i}$ for $ID_{V_i}$. Suppose the plain text is presented as $<ID_{V_i}, q', RSN^q_{V_i,N_{RSU}}>$. If $ID_{V_i} \neq ID^q_{V_i}$ or
RSU stops this service and reports abnormalities to TA. Otherwise, let \( N_{ac} \) denote the maximal number of pseudonyms which would be activated by RSU in this time, and set \( N_{ac} = \min(N_{RSU} + n, q * N_{RSU}) \). Computing that \( RSN_{F}^{N_{ac}} = H^{q * N_{RSU} - N_{ac}}(RSN_{F}^{N_{ac}}) \), then RSU composes the response message \( M \) as \( ID_{V_i} || N_{ac} || RSN_{F}^{N_{ac}} || Sig_{Pr_{RSU}}(ID_{V_i} || N_{ac} || RSN_{F}^{N_{ac}}) \). At last, RSU sends \( Enc_{sk_{V_i,RSU}}(M) \) back to \( V_i \), and apprizes TA to update \( MV_{act} \) with the new value \( N_{ac} \).

**Step 4:** After decrypting the response message from RSU, \( V_i \) first checks \( ID_{V_i} \) and verifies the message signature. If it is successful, \( V_i \) computes \( SN_{V_i} \) for \( Frg_{Cert_{V_i}} \), such that for \( j \in [\max(N_{ac} - N_{RSU}, n), N_{ac}] \), set \( RSN_{V_i} = H^{n+1}(RSN_{V_i}^{N_{ac}}) \), and \( SN_{V_i} = H(LSN_{V_i} || RSN_{V_i}^{ac}) \). Furthermore, \( V_i \) verifies these latest intact pseudonyms. If the verification doesn’t pass, \( V_i \) reports the abnormality 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 \( T_{Sn} \) to the time slot \( T_{FD_{V_i}} \) (\( F_{D_{V_i}}(x) = n \)), it adds \( <ID_{V_i}, F_{D_{V_i}}(x)> \) 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 \( T_{FD_{V_i}} \) ends. Furthermore, if each CA checks its database and finds out what it has issued the pseudonyms \( \{Cert_{V_i}^{ac}\} \) (\( j \in [n, min(MV_{V_i}^{ac}), F_{D_{V_i}}(x)) \)). If it is true, let \( MN_{CA_k,V_i} \) denote the maximal serial number of \( Cert_{V_i}^{ac} \) issued by \( CA_k \). Given \( x = \min(MN_{CA_k,V_i}, min(MV_{V_i}^{ac}), F_{D_{V_i}}(x)) \), then \( CA_k \) sends \( <x, LSN_{V_i}^{ac}, RSN_{V_i}^{ac}> \) to TA. TA adds \( <x, LSN_{V_i}^{ac}, RSN_{V_i}^{ac}> \) to CRL, and publishes CRL to all vehicles using [11], [12].

Let \( CRL_j \) denote the CRL used in time slot \( T_{S_j} \) by vehicles. Selecting one item in the original CRL from TA, denoted as \( <x, LSN_{V_i}^{ac}, RSN_{V_i}^{ac}> \), the vehicle computes \( SN_{V_i}^{ac} = H(LSN_{V_i}^{ac} || RSN_{V_i}^{ac}) \) (\( j \in [n, x] \)), and adds \( SN_{V_i}^{ac} \) in both \( CRL_{j-1} \) and \( CRL_j \). When \( n > x \), the item is deleted from the original CRL. Since vehicle can construct \( CRL_j \) using the idle time in the time slot \( T_{S_j-1} \), its 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, rigorous certificate management, and mitigation of sybil attack.

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.

4) **Rigorous certificate management.** In the proposed scheme, vehicles just can obtain \( N_{RSU} \) intact pseudonyms no matter how many times they request the RSU service repeatedly. Moreover, vehicles can’t activate pseudonyms for others. Thus, the certificate management is rigorous.

5) **Mitigation of sybil attack.** By limiting the range of validity period of certificate, each vehicle only has at most two legitimate pseudonyms in each time slot. Thus, it can mitigate a single malicious vehicle to launch sybil attack.

**IV. PERFORMANCE EVALUATION**

In this section, we evaluate the performance of the proposed NEHCM scheme in terms of the pseudonym storage of vehicles, and the revocation cost.

**A. 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 \( Stor_{pse} = N_{CA} * S_{cert} + [N_{CA}/N_{RSU}] * S_{act} \).

Since there is the annul inspection mechanism for vehicles in most country, \( P_{CA} = 1 \) Year. Moreover, set \( P_{RSU} = 1 \) day and \( \Delta T = 1 \) minute. Furthermore, we employ ECDSA as the basic signature algorithm [13], and set \( S_{cert} = S_{act} = 200 \) Bytes. Then, \( Stor_{pse} \approx 101 \) MBytes. The maximal storage overhead for vehicles is less than \( 2^4 * Stor_{pse} \), which is very small for the storage capacity nowadays.

**B. Revocation Cost**

Without loss of generality, consider in a city with \( \beta \) vehicles, each vehicle contacts with CAs once year, and changes certificates per minute for privacy preservation, i.e., \( P_{CA} = 1 \) Year, and \( \Delta T = 1 \) Minute. Moreover, suppose one percent of \( \beta \) vehicles may be revoked in a year, and the distribution of revoked vehicles is uniform. TA publishes the updated CRL every 30 minutes. Let \( F(\tau) \) denote the number of revoked vehicles presented in \( \tau \) minutes, where \( F(\tau) = 1% * \beta / (60*24*365) \).

In early deployment stage of RSUs, \( P_{RSU} \) is far larger than \( \Delta T \). In short-time certificate schemes [7], [8], given \( P_{RSU} = 1 \) Hour, it is impractical for RSUs to issue tens of certificates for each passing-by vehicle. Therefore, we just compare NEHCM with BP [3] and HS [6] as follows.

For simplicity, suppose every data unit is \( S_{unit} \) Bytes. Then, the size of one item of CRL in both BP and HS is \( S_{unit} \), while
the size of one CRL item in NEHCM equals $3 \times S_{\text{unit}}$. Let $NC_{BP}$ denote the size of pseudonym set in each vehicle in BP. According to the privacy requirement, $\Delta T = 1$ minute, set $NC_{BP} = 525600$. Let $SC$ denote the size of the updated CRL, then set $SC_{BP} = NC_{BP} \times F(30) \times S_{\text{unit}}$ Bytes, $SC_{NEHCM} = 3 \times F(30) \times S_{\text{unit}}$ Bytes, and $SC_{HS} = F(30) \times S_{\text{unit}}$ Bytes. Obviously, the size of the updated CRL in NEHCM and HS is linear in the number of revoked vehicles. Suppose $S_{\text{unit}} = 20$ Bytes, Fig. 3 shows the size of the updated CRL when the total number of vehicles $\beta$ varies from $10^5$ to $10^7$. According to [11], the updated CRLs which are no more than 350 Bytes in NEHCM and HS can be transmitted to all vehicles by vehicle-to-vehicle communication while the CRL in BP is too large, i.e. about 60 MB when $\beta = 5 \times 10^6$, to be transmitted.

Furthermore, let $CO$ denote the overhead for checking the CRL for a message at the end of the first year in our simulation, and $NC$ denote the number of CRL items in the vehicles that had gotten all updated CRLs successfully. $NC_{BP}$ and $NC_{HS}$ increase with the number of revoked vehicles in a year, set $NC_{BP} = NC_{BP} \times F(1 \text{ year})$ and $NC_{HS} = F(1 \text{ year})$. In NEHCM, each revoked vehicle has at most $N_{RSU}$ intact pseudonyms, and it would be deleted from the original CRL when these pseudonyms are expired. So the length of the original CRL is no more than $F(P_{\text{RSU}})$. Since each vehicle has two usable pseudonyms in a time slot, set $NC_{NEHCM} = 2 \times F(P_{\text{RSU}})$. The checking operation in BP and NEHCM consists of string comparisons, the cost of which is denoted as $C_{str}$. Suppose CRLs in BP and NEHCM are organized by tree-based data structure, and each checking operation needs $\log_2(NC)$ string comparisons. In addition, the checking operation in HS includes two pairing calculations, and the cost is denoted as $C_{pair}$. Therefore, $CO_{BP} = \log_2(NC_{BP}) \times C_{str}$, $CO_{NEHCM} = \log_2(NC_{NEHCM}) \times C_{str}$, $CO_{HS} = NC_{HS} \times C_{pair}$. Set $C_{str} = 1 \text{e-}6 \text{ sec}$ and $C_{pair} = 1 \text{e-}4 \text{ sec}$ as in [6], and consider tow scenarios in NEHCM, $P_{\text{RSU}} = 1$ day or there is no RSUs in the aiming city, i.e., $F_{\text{RSU}} = F_{CA}$. Fig. 4 shows the checking overhead when the total number of vehicles $\beta$ varies from $10^5$ to $10^7$. We observe that, the checking cost in NEHCM is always less than 0.018 msec while $CO_{HS}$ has increased to 1 sec just given $\beta = 10^6$.

Therefore, NEHCM indeed outperforms BP and HS in terms of the revocation cost including transmission overhead and checking overhead.

![Graph showing the size of the updated CRL in a city with $10^5$ to $10^7$ vehicles](image)

**Fig. 3.** The size of the updated CRL in a city with $10^5$ to $10^7$ vehicles

**Fig. 4.** The checking overhead of vehicles in a city with $10^5$ to $10^7$ vehicles

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, NEHCM can restrain the risk of other attacks such as sybil attack. For future work, we intend to investigate the diversity of privacy preservation for vehicles with different backgrounds in NEHCM.

REFERENCES


