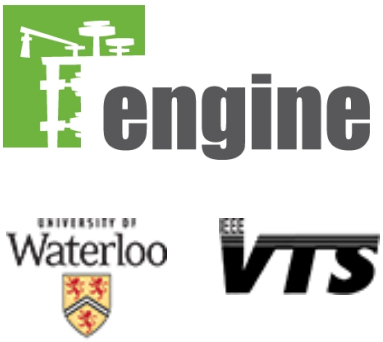


DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks

Albert Wasef, Yixin Jiang, Xuemin (Sherman) Shen

Date Submitted: 7 July 2009
Date Published: 9 July 2009

The final published version of this article is available at:
Wasef, *IEEE Transactions on Vehicular Technology*, vol. 59, no. 2, 2010, pp. 533.
DOI: 10.1109/TVT.2009.2028893

DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks

Albert Wasef, Yixin Jiang, and Xuemin (Sherman) Shen, Fellow, IEEE

Department of Electrical and Computer Engineering

University of Waterloo, Ontario, Canada

Email: {awasef, yixin, xshen}@bbcr.uwaterloo.ca

Abstract

In this paper, we propose an efficient Distributed Certificate Service (DCS) scheme for vehicular networks. The proposed scheme offers a flexible interoperability for certificate service in heterogeneous administrative authorities, and an efficient way for any On-Board Units (OBUs) to update its certificate from the available infrastructure Road-Side Units (RSUs) in a timely manner. In addition, the DCS scheme introduces an aggregate batch verification technique for authenticating certificate-based signatures, which significantly decreases the verification overhead. Security analysis and performance evaluation demonstrate that the DCS scheme can reduce the complexity of certificate management, and achieve excellent security and efficiency for vehicular communications.

Index Terms

Vehicular networks, Communication security, Certificate service, Batch verification, Revocation.

I. Introduction

Recently vehicular ad-hoc networks (VANETs) have attracted extensive attentions for their promises in revolutionizing the transportation systems. VANETs consist of network entities, mainly including vehicles and Road-Side Units (RSUs). Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are two basic vehicular communication modes, which respectively allow vehicles to communicate with each other or with the roadside infrastructure.

Due to the open medium nature of wireless communications and the high-speed mobility of a large number of vehicles in spontaneous vehicular communications, entity authentication, message integrity, non-repudiation, and privacy preservation are identified as primary security requirements [1],[2]. It is evident that any malicious behavior of a user, such as injecting false information, modifying and replaying the disseminated messages, could be fatal to other legal users. Furthermore, the privacy of users must be guaranteed in the sense that the privacy-related information of a vehicle should be protected to prevent an observer from revealing the real identities of the users, tracking their locations, and inferring sensitive data [3],[4]. Hence, to satisfy the security and privacy requirements, it is prerequisite to elaborately design a suite of protocols to achieve security and privacy for practical vehicular networks. A well-recognized solution is to deploy Public Key Infrastructure (PKI) [5], where each OBU has a set of authentic certificates. To protect the privacy of users, each OBU should use a certificate for a short duration and after that it has to replace this certificate, i.e., OBUs continuously consume their certificate sets. Eventually, each OBU will need to update its certificates. In classical PKI, any certificate update must be performed through a central Certification Authority (CA), which sends the updated certificate to the requesting OBU through the available RSUs on the roads. The centralized certificate update process in the classical PKI may be impractical in the large scale VANETs due to the following reasons: (1) Each CA encounters a large number of certificate update requests which can render the CA a bottle-neck; (2) The certificate update delay is long relative to the short V2I communication duration between the immobile RSUs and the highly mobile OBUs during which the new certificate should be delivered to the requesting OBU. The long certificate update delay is due to the fact that a request submitted by an OBU to an RSU must be forwarded to the CA, and CA has to send the new certificate to that RSU which in turn forwards the new certificate to the requesting OBU. Accordingly, the classical PKI

should be pruned or optimized to satisfy the certificate service requirement in volatile vehicular communication scenarios. To provide a practical certification service for VANETs, it is required for each OBU to efficiently update its certificate in a timely manner. The certification service should also be decentralized to enable VANET to efficiently process the expected large number of certificate update requests. Moreover, to protect the user privacy, the updated certificates should be anonymous and free from the key escrow issue.

Another important issue is the roaming between different domains [6],[7]. The OBUs should have the capabilities to roam between domains administered by different CAs. The Wireless Access in Vehicular Environments (WAVE) standard [8] did not consider the roaming between different domains, and the interopreability between different CAs is still an open problem that has not been previously tackled in the VANET literature.

According to the Dedicated Short Range Communication (DSRC) [9], which is part of the WAVE standard, each OBU in VANETs periodically broadcasts a message every 300 msec, where entity authentication and message integrity can be achieved by verifying the certificate and digital signature of the sender. In dense traffic areas, each OBU will receive a large number of messages in a short duration, and thus the ability to verify a large number of certificates and signatures in a specific period poses an inevitable challenge to the authentication technique.

To address the aforesaid security and performance issues, we introduce an efficient distributed certificate service (DCS) scheme for vehicular communications, which features the following properties.

1) **Scalability:** The DCS scheme is constructed in a hierarchical way, which enables any OBU to efficiently update its certificate from the available RSUs in a timely manner. Thus, the DCS scheme offers a distributed certification service. The DCS scheme also offers a flexible inter-operability between different administrative authorities, and it enables OBUs certificates to be free from the key escrow. All such policies efficiently enhance the system scalability, especially when it is deployed in a large-scale and heterogeneous vehicular networks.
2) **Efficiency:** Considering the requirement for each entity to verify a large number of messages in a timely manner, DCS introduces an efficient batch verification technique, which enables any entity to simultaneously verify a mass of signatures and certificates. Thus, the DCS scheme significantly decreases the verification overhead.

Therefore, the DCS scheme can meet the security and efficiency requirements for certificate service in vehicular communications.

The remainder of the paper is organized as follows. In section II, related works are surveyed. In section III, the preliminaries are discussed. The system design considerations in the proposed DCS scheme is investigated in section IV. The proposed DCS scheme is introduced in section V. Section VI introduces an efficient batch verification technique for authenticating certificate-based message signatures. Section VII and Section VIII respectively present the security analysis and performance evaluation for the proposed DCS scheme, followed by the conclusion in section IX.

II. Related Works

In spontaneous vehicular communications, the primary security requirements are identified as entity authentication, message integrity, non-repudiation, and privacy preservation. Deploying efficient Public Key Infrastructure (PKI) is a well-recognized solution to achieve security and privacy for practical vehicular networks [1],[5]. Although VANETs have recently gained extensive attention, very few works have addressed the design of a PKI suitable for the security requirements of VANETs.

In [5], Hubaux *et al.* identify the specific issues of security and privacy challenges in VANETs, and claim that a Public Key Infrastructure (PKI) should be well deployed to protect the transited messages and to mutually authenticate among network entities. In [1], Raya *et al.* use a classical PKI to provide secure and privacy preserving communications to VANETs. For this approach, each vehicle needs to pre-load a huge pool of anonymous certificates. The number of the loaded certificates in each vehicle should be large enough to provide security and privacy preservation for a long time, e.g., one year. Each vehicle can update its certificates from a central authority during the annual inspection of the vehicle. The requirement to load a large number of certificates in each vehicle incurs inefficiency for certificate management as revoking one vehicle implies revoking the huge number of certificates loaded in it.

Lin *et al.* [10] use the group signature in [11] to secure the communications between vehicles. For the group signature technique, any group member can sign messages on behalf of the group without revealing its real identity. Signatures can be verified using the group public key, thus, providing an excellent privacy for the users as the identities of the users are revealed in neither

signing nor verifying a message. However, the delay incurred in this technique for verifying a signature is linearly proportional to the number of revoked vehicles. Therefore, this technique may not achieve good performance in a large scale network such as VANETs, where the number of revoked vehicles may be large.

Based on anonymous group signature, Lu *et al.* [12] propose Efficient Conditional Privacy Preservation (ECPP) protocol for secure vehicular communications, which allows an OBU to get a short lifetime anonymous certificate from any RSU located in the domain in which the OBU was originally registered. In addition, the certificates of the OBU are free from the key escrow property. The performance of the ECPP protocol is also evaluated under a well-deployed VANET.

Jiang *et al.* [13] propose a verification scheme capable of detecting bogus signatures in batch signature verification schemes, based on a new data structure called binary authentication tree. In this scheme, a binary tree of the received signatures can be built as follows: (1) The leaf-nodes of the tree are the individual signatures; (2) The inner-nodes in the level above the leafs are the batch signatures of the leafs directly connected to it; (3) Upper levels is constructed in the same way as in step (2) until the root of the tree is reached. The verification process is performed in a top-to-bottom manner. At each level of the tree, the batch signature associated with each inner-node is verified. If the verification is successfully performed for an inner-node x at level $i-1$, this implies that all the signatures located at levels lower than $i-1$ and connected directly or indirectly to the inner-node x are correct. If the verification fails for the inner-node x, all the batch signatures of the inner-nodes connected to x and located one level below, i.e., at level $i-2$, must be individually verified. The process is continued until the leafs of the tree are reached, i.e., until all the bogus signatures are found.

Different from the above works, we propose an efficient Distributed Certificate Service (DCS) scheme which enables an OBU to update its certificate from any RSU no matter whether the RSU is located in the domain in which the OBU was originally registered or not. Consequently, an OBU is free to roam between domains administered by different authorities. Also, the DCS scheme considers batch verification of certificates and messages signatures. To the best of our knowledge, this is the first approach to address the roaming between different domains in VANETs. Also, the DCS scheme is the first to consider the integration between distributed certificate generation through RSUs and efficient message authentication using batch verification.

TABLE I

NOTATIONS

Symbol	Notation
CA_i, CA_w	two arbitrary CAs
RSU_j, RSU_l	two arbitrary $RSUs$
OBU_m, OBU_n	two arbitrary $OBUs$
s	master secret key of MA for secret key generation
α	partial secret signing-key for signing RSU certificates
γ	partial secret signing-key for signing OBU certificates
$P_\circ$	public key used to verify signatures on any message
$S_{\alpha i}$	CA_i secret key to sign RSU certificates
P_α	public key used to verify RSU certificates
$S_{\gamma j_i}$	RSU_j secret key, generated by CA_i, to sign OBU certificates
P_γ	public key used to verify OBU certificates
P_μ	public key used to verify any certificate
PK_i	public key for CA_i
SK_i	secret key for CA_i
PK_{j_i}	RSU_j public key generated by CA_i
SK_{j_i}	RSU_j secret key generated by CA_i
$cert_{RSU_{ji}}$	certificate for RSU_j generated by CA_i
$PK_{m_{ji}}$	OBU_m public key generated by RSU_j using PK_{j_i}
$SK_{m_{ji}}$	OBU_m secret key generated by RSU_j using SK_{j_i}
$vepriod$	OBU certificate validity period
$cert_{OBU_{mji}}$	OBU_m certificate generated by RSU_j using $S_{\gamma j_i}$
t_{stamp}	time stamp
H_1	hash function such that $\{0,1\}^* \in \mathbb{G}_1^*$
H_2	hash function such that $\{0,1\}^* \in \mathbb{Z}_q^*$

III. PRELIMINARIES

In this section, we introduce the bilinear pairings. The notations used throughout the paper are given in Table I.

A. Bilinear Pairing

The bilinear pairing [14] is the foundation of the proposed DCS scheme. Let $\mathbb{G}_1$ denote an additive group of prime order q, and $\mathbb{G}_2$ a multiplicative group of the same order. Let P be a generator of $\mathbb{G}_1$, and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear mapping with the following properties:

1) Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, for all $P, Q \in \mathbb{G}_1$ and $a, b \in_R \mathbb{Z}_q$.
2) Non-degeneracy: $\hat{e}(P, Q) \neq 1_{\mathbb{G}_2}$.
3) Symmetric: $\hat{e}(P, Q) = \hat{e}(Q, P)$, for all $P, Q \in \mathbb{G}_1$.
4) Admissible: the map $\hat{e}$ is efficiently computable.

The bilinear map e can be implemented using the Weil [15] and Tate [16] pairings on elliptic curves. We consider the implementation of Tate pairing on an MNT curve [17] with embedding degree 6, where $\mathbb{G}_1$ is represented by 161 bits, and the order q is represented by 160 bits. The group order of $\mathbb{G}_1$ is defined as the number of the points on the employed elliptic curve. For an MNT elliptic curve with embedding degree 6 and the order q is represented by 160 bits, the group order of $\mathbb{G}_1$ is 4.5×10^{30} [1], which qualifies the bilinear pairing as a practical choice for securing the large scale VANETs.

The security of the proposed scheme depends on solving the following hard computational problems:

- **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 [19] is to determine the integer l, $0 \leq l \leq q - 1$, such that $Q = lP$.
- **Computational Diffie-Hellman problem (CDH):** For two unknowns $a,\ b \in \mathbb{Z}_p^*$, the CDH problem [20] is given $aP,\ bP \in \mathbb{G}_1$, compute $abP \in \mathbb{G}_1$.

IV. SYSTEM DESIGN CONSIDERATIONS IN THE PROPOSED DCS SCHEME

In this section, we discuss the security objectives, system architecture, and network model of the proposed DCS scheme.

[1]This result is obtained using MIRACL library [18].

A. *Security Objectives*

In the DCS scheme, we aim to achieve the following security objectives.

1) Authentication: Entity authentication is required to prevent illegitimate users from injecting bogus messages into the network. Each vehicle in the network should possess an authentic identity. When a vehicle receives a message, it first checks the authenticity of the sender identity before performing further processing to the received message. Besides entity authentication, data authentication is a concern to ensure that the contents of the received data is neither altered nor replayed.
2) Non-repudiation: Non-repudiation is necessary to prevent legitimate users from denying the transmission or the content of their messages. Users anticipate the network to provide a high level of liability, where a vehicle involved in a crash should be efficiently identified. Liability can be achieved by investigating the messages saved in each vehicle involved in the crash. However, if non-repudiation cannot be guaranteed, this process will be trivial.
3) Privacy: Providing privacy is mainly related to preventing the disclosure of the real identity of the users and their locations information. Privacy can be provided by introducing identity anonymity such that any observer could neither identify the real identity nor correlate the real identity with the current location of any user. An observer is an attacker launching tracking attacks by installing receivers on the roads to eavesdrop the messages broadcasted by the OBUs. By trying to correlate some of the broadcasted certificates to an OBU, the observer may be able to track that OBU.
4) Transparent roaming: Users will not be satisfied if upon roaming between different network domains, they have to go to a central location to upload new security materials, e.g., keys, certificates, etc., to be able to use the VANET services. Transparent roaming is needed to ensure seamless operation of the OBUs in VANETs.
5) Access control: Access control is necessary to ensure reliable and secure operation of the system. Any misbehaving entity should be revoked from the network to protect the safety of other legitimate entities in the network. Moreover, any actions taken by that misbehaving entity should be canceled.

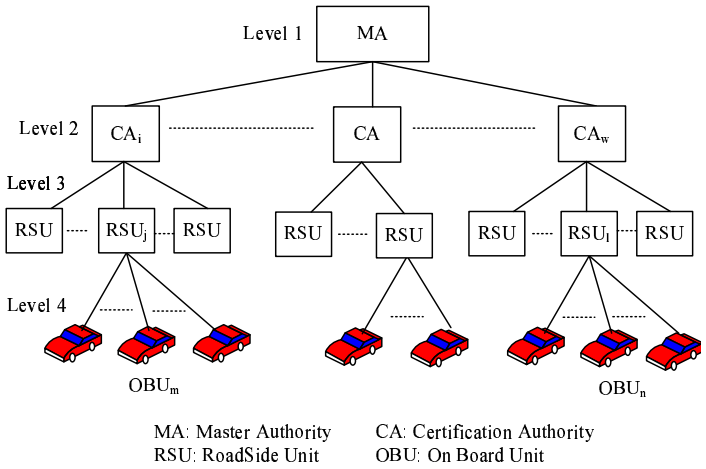


Fig. 1. The proposed DCS hierarchical architecture

B. Architecture

The DCS hierarchical architecture, shown in Fig. 1, consists of four levels: the Master Authority (MA), which is the root of the system, is located at level 1; the Certification Authorities (CAs) are located at level 2; the Road Side Units (RSUs) and the On-Board Units (OBUs) are located at level 3 and level 4, respectively. In this architecture, entity authentication for RSUs and OBUs is achieved using certificate-based authentication, while that for CAs is achieved using identity-based cryptography [14].

Basic Operation of the DCS Scheme: The basic operation of the DCS scheme is as follows.

- The MA is in charge of generating public verification keys for verifying any RSU/OBU certificate. It also generates a public/private key pair for each CA, for signing the outgoing messages and verifying the incoming messages. Moreover, it generates two secret certificate-signing keys for each CA;
- A CA uses the first certificate-signing keys, issued by the MA, to sign a certificate set for each RSU in its coverage area. Each certificate in the RSU certificate set is shared among a group of RSUs. The CA uses the second certificate-signing key as a partial signing key to generate secret OBU-certificate-signing keys for each RSU;
- An RSU uses the OBU-certificate-signing key to generate short lifetime anonymous certificates for any OBU. The public verification keys can be used by any entity to verify the

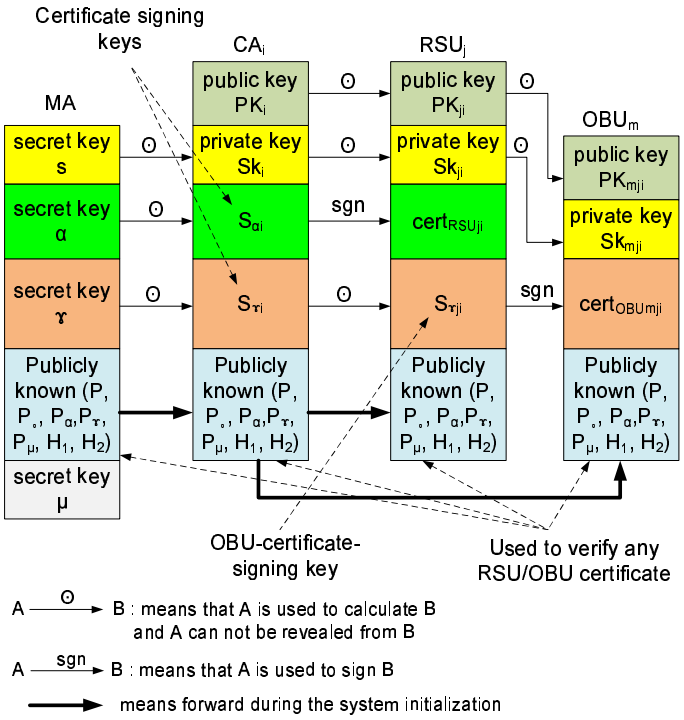


Fig. 2. The relations of different keys among the network entities in the DCS scheme

certificate of any OBU or RSU regardless of the issuer of that certificate. In this way, any OBU can roam transparently between the coverage areas of different CAs. The certificate generation in DCS is derived from the signature schemes proposed in [21], [22].

Fig. 2 shows the relations of different keys among the network entities in the DCS scheme.

C. Network Model

As shown in Fig. 3, the network model under consideration consists of the followings.

- A Master Authority (MA), which is the highest level in the system and is trustable by all the network entities. The MA has sufficient physical security measures such that it cannot be compromised irrespective of the capabilities of an attacker;
- Certification Authorities (CAs). Each CA is responsible for generating initial certificates for the RSUs and OBUs in its domain. The CAs are connected directly to the MA. Each CA is physically secure and cannot be compromised;
- Road-Side Units (RSUs), which are fixed units distributed in the network. RSUs in one

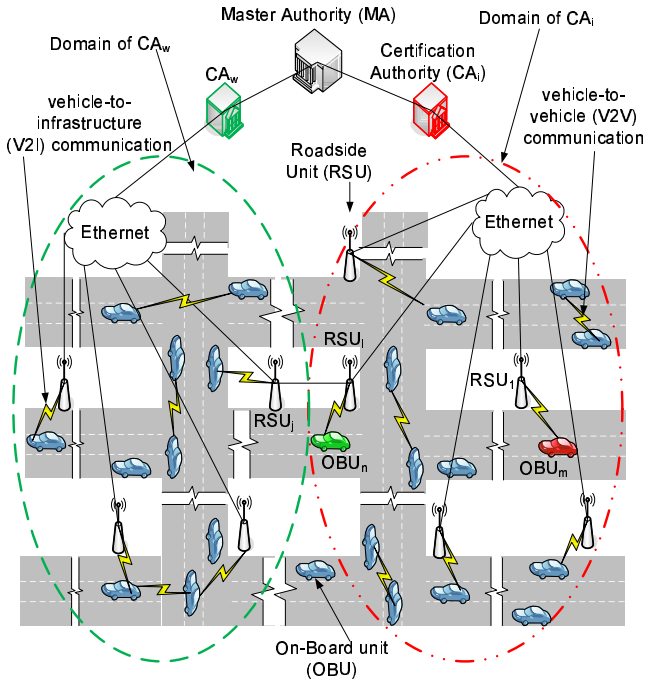


Fig. 3. The network model

domain are connected via Ethernet to the CA responsible for that domain. Also, an RSU_j at the border of one domain is connected to the nearest RSU_l in an adjacent domain. These connections are required to check the revocation status of an OBU roaming between two adjacent domains. Moreover, RSUs are responsible for updating the certificates of the OBUs;

- On-Board Units (OBUs), which can communicate either with other OBUs through Vehicle-to-Vehicle (V2V) communications or with the infrastructure RSUs through Vehicle-to-Infrastructure (V2I) communications. Each OBU is equipped with a Global Positioning Service (GPS) receiver which contains the geographical coordinates of the RSUs. It should be noted that a GPS receiver is necessary for the operation of an OBU in VANETs according to the WAVE standard [8];
- According to the WAVE standard, each network entity is equipped with a tamper-resistant Hardware Security Module (HSM) to store its security materials, e.g., secret keys, certificates, etc.

V. The Proposed DCS Scheme

In this section, the proposed DCS scheme is presented in detail including the system initialization, certificate issue, certificate update, and certificate revocation.

A. System Initialization

The initialization stage in the DCS scheme consists of two phases: (1) Phase I which is performed by the MA to generate the security keys necessary for the operation of the DCS scheme, and to upload the necessary security keys in the tamper-resistant HSM of each CA; (2) Phase II which is performed by each CA to upload the required security materials, e.g., keys, certificates, etc., in the tamper-resistant HSM of each OBU and RSU in its domain. It should be noted that both phases of the initialization stage are performed during the registration of CAs with MA in phase I, and RSUs and OBUs with a CA in phase II. In other words, both phases of the initialization stage are performed before triggering any of the VANET services or applications. The details of each phase are as follows.

Algorithm 1 Phase I

Require: ID_{CA_i}

1: Select a random number $s \in \mathbb{Z}_q^*$ as the *master* key, ▷ this is part of each entity secret key and set $P_\circ = sP$

2: Select random numbers $\alpha, \gamma \in \mathbb{Z}_q^*$, and set $P_\alpha = \alpha P, P_\gamma = \gamma P$ ▷ these are the *master signing* keys

3: Select a random number $\mu \in \mathbb{Z}_q^*$, and set $P_\mu = \mu P$; ▷ general verification public key

4: Select a hash function $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$

5: Select a hash function $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$

6: **for all** CA_i with identity ID_{CA_i} **do**

7: Set $PK_i = Q_i = H_1(ID_{CA_i}) \in \mathbb{G}_1^*$, ▷ this is CA_i public key

$SK_i = sQ_i$, ▷ this is CA_i secret key

$S_{\alpha i} = \alpha Q_i$, and ▷ this is CA_i certificate-signing key

$S_{\gamma i} = \gamma Q_i$ ▷ this is CA_i certificate-signing key

8: Upload $SK_i, S_{\alpha i}, S_{\gamma i}, P, P_\circ, P_\alpha, P_\gamma, P_\mu, H_1,$ and H_2 in CA_i

9: **end for**

1) Phase I: The MA executes Algorithm 1 to generate the necessary secret and public keys for the operation of the DCS scheme, and to upload the primary security materials in each CA.

It should be noted that the key s is the *master* secret key, and it will be part of the secret key of each entity. Also, the secret keys α and γ are *master signing* keys, and they will be parts of each signature on the certificates of the RSUs and OBUs, respectively. Moreover, $P_\circ, P_\alpha, P_\gamma,$ and P_μ are public verification keys, which can be used by any entity in the network to verify any RSU/OBU certificate. In addition, the public key of any CA_i is the hash of its identity ID_{CA_i}.

By the end of Algorithm 1, each CA will have the security materials required to execute phase II.

2) Phase II: In this phase, each CA_i runs Algorithm 2 and Algorithm 3 to respectively initialize each RSU_j and OBU_m in its domain by uploading them with the necessary security materials for their operation in VANETs as follows.

RSU initialization: Each CA_i executes Algorithm 2, to upload each RSU_j with a certificate $cert_{RSU_{ji}}$, secret OBU-certificate-signing key $S_{\gamma j_i}$ which will be used later by RSU_j to issue

Algorithm 2 Phase II: RSU initialization

Require: $PK_i = Q_i,\ SK_i = sQ_i,\ S_{\alpha i} = \alpha Q_i,$ and $S_{\gamma i} = \gamma Q_i$

1: **for all** RSU_j in the domain of CA_i **do**

2: select random numbers $x_j,\ a_j \in \mathbb{Z}_q^*$, and
a pseudo identity PID_j for RSU_j

3: set $SK_{j_i} = x_j SK_i = x_j s Q_i$, ▷ this is RSU_j secret key
$PK_{j_i} = x_j PK_i = x_j Q_i$, ▷ this is RSU_j public key
$S_{\gamma j_i} = x_j S_{\gamma i} = x_j \gamma Q_i$, ▷ this is the secret OBU-certificate-signing key
$U_j = a_j P$, $T_j = H_2(PK_{j_i}||PID_j||U_j||Q_i) \in \mathbb{Z}_q^*$,
$V_j = S_{\alpha i} + a_j T_j P_\mu$, and
$cert_{RSU_{ji}} = (PK_{j_i},\ U_j,\ V_j,\ PID_j,\ Q_i)$ ▷ this is RSU_j certificate

4: Select minimum and maximum value for the validity period $(vperiod)$ of any OBU certificate

5: Upload $cert_{RSU_{ji}}$, $S_{\gamma j_i}$, the minimum and maximum value of $vperiod$, $P, P_\circ, P_\alpha, P_\gamma, P_\mu, H_1,$ and H_2 in RSU_j

6: **end for**

certificates for OBUs, the minimum and maximum value of the validity period of OBUs certificates, and publicly known parameters $(P, P_\circ, P_\alpha,\ P_\gamma, P_\mu, H_1, \text{and } H_2)$.

Remarks on Algorithm 2

- It should be noted that U_j and V_j are the signature of CA_i on $cert_{RSU_{ji}}$.
- CA_i stores RSU_j real identity, PID_j, $cert_{RSU_{ji}}$, SK_{ji}, and $S_{\gamma ji}$, thus, CA_i can track the operations performed by RSU_j, in case it is compromised, by associating PID_j with its real identity.
- RSU_j or any other entity can verify the certificate $cert_{RSU_{ji}}$ by calculating $T_j = H_2(PK_{j_i}||PID_j||U_j||Q_i)$, and accepting if $\hat{e}(P, V_j) = \hat{e}(P_\alpha, Q_i)\hat{e}(T_jU_j, P_\mu)$. This verification follows since

$$\begin{aligned}\hat{e}(P, V_j) &= \hat{e}(P, S_{\alpha i} + a_jT_jP_\mu)\\ &= \hat{e}(P, \alpha Q_i + a_jT_jP_\mu)\\ &= \hat{e}(P, \alpha Q_i)\hat{e}(P, a_jT_jP_\mu)\\ &= \hat{e}(\alpha P, Q_i)\hat{e}(T_ja_jP, P_\mu)\\ &= \hat{e}(P_\alpha, Q_i)\hat{e}(T_jU_j, P_\mu).\end{aligned} \tag{1}$$

- The CA repeatedly runs Algorithm 2 to load each RSU with a set of certificates. Each certificate is shared with a different group of RSUs to enforce the anonymous group signature when generating OBUs certificates.

OBU initialization: Each CA_i executes Algorithm 3, to upload each OBU_m having identity ID_{OBU_m} in its domain with a number (N_{cert}) of short lifetime certificates. The identity ID_{OBU_m} is a unique identity loaded in OBU_m during the manufacturing process.

Remarks on Algorithm 3

- In Algorithm 3, CA_i selects an arbitrary RSU_j in its service area as the certificate issuer, and uses the security materials $\{cert_{RSU_{ji}} = (PK_{j_i},\ U_j,\ V_j,\ PID_j,\ Q_i),\ SK_{j_i} = x_jsQ_i,\ S_{\gamma j_i} = x_j\gamma Q_i\ \}$ of RSU_j. Note that CA_i is the entity which issued these security materials for RSU_j.
- CA_i stores the real identity (ID_{OBU_m}) and $\{PID_{m,r},\ cert_{m_{ji},r}, SK_{m_{ji},r} | 1 \leq r \leq N_{cert}\}$ of OBU_m, thus, CA_i can efficiently track OBU_m, in case it is compromised, by associating PID_m to ID_{OBU_m}.

Algorithm 3 Phase II: OBU initialization

Require: $\{cert_{RSU_{ji}} = (PK_{j_i},\ U_j,\ V_j,\ PID_j,\ Q_i),\ SK_{j_i} = x_j s Q_i,$ and $S_{\gamma j_i} = x_j \gamma Q_i\ \}$ of RSU_j and ID_{OBU_m} of OBU_m

1: **for all** OBU_m in the domain of CA_i **do**
2: Check the validity of ID_{OBU_m}
3: **if** ID_{OBU_m} is invalid **then**
4: **return** $\perp$
5: **else**
6: **for** r $\leftarrow$ 1 **to** N_{cert}, CA_i **do**
7: Select random numbers $y_{m,r},\ b_{m,r} \in \mathbb{Z}_q^*$
8: Set $y_{m,r}SK_{j_i} = y_{m,r}x_j s Q_i$, and ▷ partial secret key
$y_{m,r}PK_{j_i} = y_{m,r}x_j Q_i$ ▷ partial public key
9: **end for**
10: **return** $\{y_{m,r}SK_{j_i},\ y_{m,r}PK_{j_i} | 1 \leq r \leq N_{cert}\}$ to OBU_m
11: **for** r $\leftarrow$ 1 **to** N_{cert}, OBU_m **do**
12: Select a random number $z_{m,r} \in \mathbb{Z}_q^*$
13: Set $SK_{m_{ji},r} = z_{m,r}y_{m,r}SK_{j_i} = z_{m,r}y_{m,r}x_j s Q_i$, and ▷ final secret key
$PK_{m_{ji},r} = z_{m,r}y_{m,r}PK_{j_i} = z_{m,r}y_{m,r}x_j Q_i$ ▷ final public key
14: **end for**
15: **return** $\{PK_{m_{ji},r} | 1 \leq r \leq N_{cert}\}$ to CA_i
16: **for** r $\leftarrow$ 1 **to** N_{cert}, CA_i **do**
17: Select a validity period $vperiod_{m,r}$, and a pseudo identity $PID_{m,r}$
18: Set $U_{m,r}^{\backprime} = b_{m,r}P$,
$L_{m,r} = H_2(PK_{m_{ji},r}||vperiod_{m,r}||PID_{m,r}||U_{m,r}^{\backprime}) \in \mathbb{Z}_q^*$,
$V_{m,r}^{\backprime} = S_{\gamma j_i} + b_{m,r}L_{m,r}P_\mu$, and
$cert_{OBU_{mji,r}} = (PK_{m_{ji},r}, U_{m,r}^{\backprime}, V_{m,r}^{\backprime}, vperiod_{m,r}, PID_{m,r}, cert_{RSU_{ji}})$
19: **end for**
20: Upload $\{cert_{OBU_{mji,r}} | 1 \leq r \leq N_{cert}\} = \{PK_{m_{ji},r}, U_{m,r}^{\backprime}, V_{m,r}^{\backprime}, vperiod_{m,r},$
$PID_{m,r}, cert_{RSU_{ji}} | 1 \leq r \leq N_{cert}\}$, $P, P_\circ, P_\alpha, P_\gamma, P_\mu, H_1,$ and H_2 in OBU_m
21: CA_i stores ID_{OBU_m} and $\{PID_{m,r},\ cert_{m_{ji},r}, SK_{m_{ji},r} | 1 \leq r \leq N_{cert}\}$
22: **end if**
23: **end for**

- It should be noted that throughout the rest of the paper whenever the subscript r equals 1, it will be omitted for the ease of presentation.
- Any entity in the network can verify a single certificate $cert_{OBU_{mji}}$ by verifying $cert_{RSU_{ji}}$, then, verifying $cert_{OBU_{mji}}$. Alternatively, $cert_{RSU_{ji}}$ and $cert_{OBU_{mji}}$ can be aggregately verified as follows:
  1) Check $vperiod$ and proceed only if it is valid;
  2) Calculate $T_j = H_2(PK_{j_i}||PID_j||U_j||Q_i)$ and $L_m = H_2(PK_{m_{ji}}||vperiod||PID_m||U_m^{\backprime})$;
  3) Accept if $\hat{e}(P, V_j + V_m^{\backprime}) = \hat{e}(P_\alpha, Q_i)\hat{e}(P_\gamma, PK_{j_i})\ \hat{e}(T_jU_j + L_mU_m^{\backprime}, P_\mu)$. This verification follows since

$$\begin{aligned}\hat{e}(P, V_j + V_m^{\backprime}) &= \hat{e}(P, S_{\alpha i} + a_jT_jP_\mu + S_{\gamma j_i} + b_mL_mP_\mu)\\ &= \hat{e}(P, \alpha Q_i)\hat{e}(P, x_j\gamma Q_i)\hat{e}(P, a_jT_jP_\mu + b_mL_mP_\mu)\\ &= \hat{e}(\alpha P, Q_i)\hat{e}(\gamma P, x_jQ_i)\hat{e}(a_jT_jP + L_mb_mP, P_\mu)\\ &= \hat{e}(P_\alpha, Q_i)\hat{e}(P_\gamma, PK_{j_i})\hat{e}(T_jU_j + L_mU_m^{\backprime}, P_\mu).\end{aligned} \tag{2}$$

- Including $cert_{RSU_{ji}}$ in $cert_{OBU_{mji}}$ guarantees that $cert_{OBU_{mji}}$ is generated by a legitimate RSU_j with a valid public key PK_{j_i}. This inclusion also gives the CA the ability to revoke any operation performed by a compromised RSU during the period from the RSU compromising until the detection of the compromised RSU. In other words, consider an attacker compromises an RSU_l having a certificate $cert_{RSU_{li}}$, and the attacker generates some OBUs' certificates from the compromised RSU_l. When the CA detects that RSU_l is compromised, it revokes $cert_{RSU_{li}}$. The revocation of $cert_{RSU_{li}}$ automatically revokes all the OBUs certificates generated by RSU_j, as those certificates contain the revoked $cert_{RSU_{li}}$.

B. OBUs Certificates Update

The DCS scheme enables an OBU to update its certificate from an RSU. Thus, the scalability of the DCS scheme stems from the distributed certification service compared to the centralized certification service in the classical PKI where an OBU has to contact a CA to update its certificate. Since the DCS scheme depends on the RSUs to update the certificates of the OBUs, the density of RSUs is crucial to the operation of the DCS scheme. In this section, we discuss the adaptability of the DCS scheme to different densities of RSUs, and how an OBU can update its certificates dynamically even if it is roaming between different domains. In the certificate

update process, an RSU generates a number of short lifetime anonymous certificates for an OBU sufficient to secure the communications of the OBU until it meets another RSU. The number of generated certificates by an RSU depends on the RSUs density.

1) Adapting DCS to Different RSUs Densities: In this section, we discuss how the DCS scheme can adapt to different densities of RSUs. Let T_{RSU} denote the duration an OBU spent between meeting two different RSUs on its way. When the number of RSUs in a given area increases, it is intuitive that T_{RSU} will decrease and vice versa, i.e., T_{RSU} is inversely proportional to the RSUs density. It should be noted that an OBU has to periodically change its certificate during T_{RSU} to avoid being tracked. Since an OBU spends a time of $vperiod$, which is the validity period of the OBU certificate, using the same certificate, the number of certificates N_{cert} required to protect the privacy of that OBU in the duration it spent between meeting two different RSUs can be calculated as follows

$$N_{cert} = \left\lceil \frac{T_{RSU}}{vperiod} \right\rceil \tag{3}$$

An OBU_n moving on the road can calculate its T_{RSU} value based on its direction, speed, and the coordinates of the RSUs initially loaded in its GPS receiver. When OBU_n needs to update its certificates, it sends a request to update its certificate and the value of its T_{RSU} to an RSU_j. Then, using eq. (3) and the appropriate value for $vperiod$, RSU_j can calculate the required number of certificates (N_{cert}) that should be generated to the requesting OBU_n to protect its privacy until it meets the next RSU on its way. In this way, the DCS scheme can adapt to different RSUs densities.

2) OBUs Dynamic Certificates Update: The DCS offers a full interoperability for any OBU to update its certificate in a completely transparent way, even when it roams into a domain different from its home domain. Consider OBU_n, with certificate $cert_{OBU_{nlw}} = (PK_{n_{lw}}, U_n^{\backprime}, V_n^{\backprime}, vperiod, PID_n, cert_{RSU_{lw}})$ generated by RSU_l in the domain of CA_w, enters the domain of CA_i, and needs to update its certificate from RSU_j which has a certificate $cert_{RSU_{ji}} = (PK_{j_i},\ U_j,\ V_j, PID_j,\ Q_i)$, as shown in Fig. 3 where OBU_n is shown in green. The certificate update algorithm, shown in Fig. 4, has two phases: *phase I* for mutual authentication and generating a shared secret key in a non-interactive way, and *phase II* for issuing a bundle of N_{cert} short lifetime anonymous certificates for OBU_n. The *OBU-Certificate-Update* algorithm is as follows.

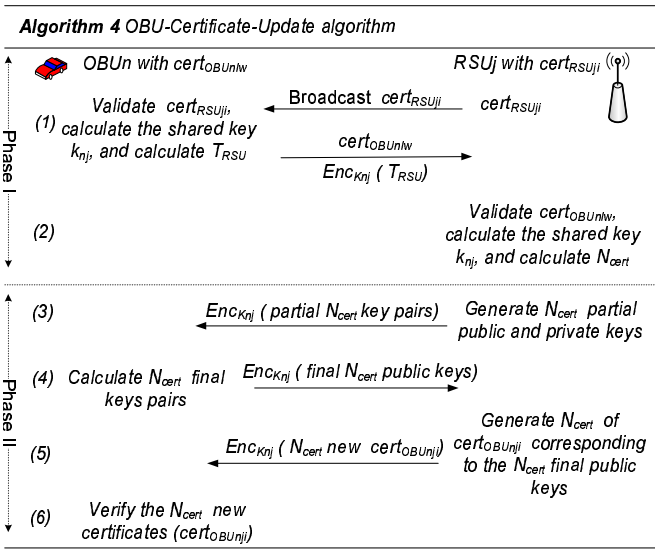


Fig. 4. OBU Certificate Update

Phase I

1) When OBU_n receives the periodically broadcasted certificate $cert_{RSU_{ji}}$ of RSU_j, it verifies $cert_{RSU_{ji}}$ by calculating $T_j = H_2(PK_{j_i}||PID_j||U_j||Q_i)$ and proceeds only if $\hat{e}(P, V_j) = \hat{e}(P_\alpha, Q_i)\hat{e}(T_jU_j, P_\mu)$. If valid, OBU_n calculates the shared secret key (k_{nj}) using its secret key $SK_{n_{lw}}$ and the public key PK_{j_i} of RSU_j included in $cert_{RSU_{ji}}$ as $k_{nj} = \hat{e}(SK_{n_{lw}}, PK_{j_i}) = \hat{e}(z_n y_n x_l s Q_w, x_j Q_i) = \hat{e}(Q_w, Q_i)^{z_n y_n x_l x_j s} = k_{jn}$. Then, OBU_n calculates T_{RSU} based on its speed, destination, and the loaded coordinates of the RSUs. After that, OBU_n encrypts T_{RSU} with k_{nj}, and sends its certificate $cert_{OBU_{nlw}}$ along with the encrypted T_{RSU} to RSU_j;
2) RSU_j verifies $cert_{OBU_{nlw}}$ by calculating $T_l = H_2(PK_{l_w}||PID_l||U_l||Q_w)$ and $L_n = H_2(PK_{n_{lw}} ||vperiod||PID_n||U_n^{'})$, and proceeds only if $\hat{e}(P, V_l + V_n^{'}) = \hat{e}(P_\alpha, Q_l)\hat{e}(P_\gamma, PK_{l_w})\hat{e}(T_lU_l + L_nU_n^{'}, P_\mu)$. If valid, RSU_j calculates the shared secret key as $k_{jn} = \hat{e}(PK_{n_{lw}}, SK_{j_i}) = \hat{e}(z_n y_n x_l Q_w, x_j s Q_i) = \hat{e}(Q_w, Q_i)^{z_n y_n x_l x_j s} = k_{nj}$ in a non-interactive key agreement way. Then, RSU_j decrypts T_{RSU} using k_{nj}, and calculates N_{cert} using eq. (3) based on the bounds of the certificate validity period $vperiod$ settled by CA_i.

Phase II

3) As shown in Fig. 4, RSU_j selects N_{cert} random numbers $\{y_{n,r}^{'} | 1 \leq r \leq N_{cert}\} \in \mathbb{Z}_q^*$, and

calculates N_{cert} partial secret keys as $\{y_{n,r}^{\backprime} x_j s Q_i | 1 \leq r \leq N_{cert}\}$ and the corresponding N_{cert} partial public keys $\{y_{n,r}^{\backprime} x_j Q_i | 1 \leq r \leq N_{cert}\}$. Then, it securely delivers the partial key pairs to OBU_n by encrypting them with the shared secret key k_{nj} established in *Phase I*;

4) OBU_n selects N_{cert} random numbers $\{z_{n,r}^{\backprime} \in \mathbb{Z}_q^* | 1 \leq r \leq N_{cert}\}$, and calculates its final secret keys $\{SK_{n_{ji},r} | 1 \leq r \leq N_{cert}\} = \{z_{n,r}^{\backprime} y_{n,r}^{\backprime} x_j s Q_i | 1 \leq r \leq N_{cert}\}$ and its final public key $\{PK_{n_{ji},r} | 1 \leq r \leq N_{cert}\} = \{z_{n,r}^{\backprime} y_{n,r}^{\backprime} x_j Q_i | 1 \leq r \leq N_{cert}\}$. After that, OBU_n sends its final public keys $\{PK_{n_{ji},r} | 1 \leq r \leq N_{cert}\}$ to RSU_j;

5) For each key in $\{PK_{n_{ji},r} | 1 \leq r \leq N_{cert}\}$, RSU_j chooses a validity period $vperiod_{n,r}$ and a pseudo identity $PID_{n,r}$. After that, RSU_j selects N_{cert} random numbers $\{b_{n,r}^{\backprime} | 1 \leq r \leq N_{cert}\} \in \mathbb{Z}_q^*$, and calculates $\{U_{n,r}^{\backprime} | 1 \leq r \leq N_{cert}\} = \{b_{n,r}^{\backprime} P | 1 \leq r \leq N_{cert}\}$, $\{L_{n,r}^{\backprime} | 1 \leq r \leq N_{cert}\} = \{H_2(PK_{n_{ji},r} || vperiod_{n,r} || PID_{n,r} || U_{n,r}^{\backprime}) | 1 \leq r \leq N_{cert}\} \in \mathbb{Z}_q^*$, and $\{V_{n,r}^{\backprime} | 1 \leq r \leq N_{cert}\} = \{S_{\gamma j_i} + b_{n,r}^{\backprime} L_{n,r}^{\backprime} P_\mu | 1 \leq r \leq N_{cert}\}$. Finally, RSU_j issues $\{cert_{OBU_{nji,r}} | 1 \leq r \leq N_{cert}\} = \{(PK_{n_{ji},r}, U_{n,r}^{\backprime}, V_{n,r}^{\backprime}, vperiod_{n,r}, PID_{n,r}, cert_{RSU_{ji}}) | 1 \leq r \leq N_{cert}\}$ and delivers them to OBU_n over a channel secured by the key k_{nj};

6) OBU_n verifies the received certificates $\{cert_{OBU_{nji,r}} | 1 \leq r \leq N_{cert}\}$ by calculating $\{L_{n,r}^{\backprime} | 1 \leq r \leq N_{cert}\} = \{H_2(PK_{n_{ji}} || vperiod_{n,r} || PID_{n,r} || U_{n,r}^{\backprime}) | 1 \leq r \leq N_{cert}\}$ and accepts only if

$$\hat{e}(P, \sum_{r=1}^{N_{cert}} V_{n,r}^{\backprime}) = \hat{e}(P_\gamma, \sum_{r=1}^{N_{cert}} PK_{j_i}) \hat{e}(\sum_{r=1}^{N_{cert}} L_{n,r}^{\backprime} U_n^{\backprime r}, P_\mu). \tag{4}$$

This verification holds since

$$\begin{aligned}
\hat{e}(P, \sum_{r=1}^{N_{cert}} V_{n,r}^{\backprime}) &= \hat{e}(P, V_{n,1}^{\backprime} + V_{n,2}^{\backprime} + \cdots + V_{n,N_{cert}}^{\backprime}) \\
&= \hat{e}(P, S_{\gamma j_i} + b_{n,1}^{\backprime} L_{n,1}^{\backprime} P_\mu + S_{\gamma j_i} + b_{n,2}^{\backprime} L_{n,2}^{\backprime} P_\mu + \cdots \\
&\quad + S_{\gamma j_i} + b_{n,N_{cert}}^{\backprime} L_{n,N_{cert}}^{\backprime} P_\mu) \\
&= \hat{e}(P, \sum_{r=1}^{N_{cert}} S_{\gamma j_i}) \hat{e}(P, b_{n,1}^{\backprime} L_{n,1}^{\backprime} P_\mu + b_{n,2}^{\backprime} L_{n,2}^{\backprime} P_\mu + \cdots + b_{n,N_{cert}}^{\backprime} L_{n,N_{cert}}^{\backprime} P_\mu) \\
&= \hat{e}(P, \sum_{r=1}^{N_{cert}} x_j \gamma Q_i) \hat{e}(L_{n,1}^{\backprime} b_{n,1}^{\backprime} P + L_{n,2}^{\backprime} b_{n,2}^{\backprime} P + \cdots + L_{n,N_{cert}}^{\backprime} b_{n,N_{cert}}^{\backprime} P, P_\mu) \\
&= \hat{e}(\gamma P, \sum_{r=1}^{N_{cert}} x_j Q_i) \hat{e}(L_{n,1}^{\backprime} U_{n,1}^{\backprime} + L_{n,2}^{\backprime} U_{n,2}^{\backprime} + \cdots + L_{n,N_{cert}}^{\backprime} U_{n,N_{cert}}^{\backprime}, P_\mu)
\end{aligned} \tag{5}$$

$$= \hat{e}(P_\gamma, \sum_{r=1}^{N_{cert}} PK_{j_i})\hat{e}(\sum_{r=1}^{N_{cert}} L_{n,r}^{\backprime} U_{n,r}^{\backprime}, P_\mu).$$

By the end of *phase II*, OBU_n gets N_{cert} short lifetime anonymous certificates which are sufficient to protect its privacy until it meets another RSU on its way.

Remarks

- The preceding algorithm enables an OBU_m from one domain (CA_w) to securely update its certificate in another domain (CA_i). Especially, if $i = w$, OBU_m updates its certification in its local domain.
- By increasing the number of the short lifetime certificates an OBU can get from an RSU, the distance an OBU can move without the need to contact another RSU to update its certificates increases. In other words, by changing the number of certificates N_{cert}, the DCS scheme can adapt to different densities of RSUs. Consider a constant $vperiod = 1min$ [1] for all the certificates of an OBU, and the OBU average speed in a domain is $60\ Km/h$. When an OBU updates its certificates from an RSU for values of N_{cert} equal 5 and 10 certificates, these values are sufficient to protect the privacy of that OBU over distances of $5\ km$ and $10\ km$, respectively, without the need to contact another RSU.
- When an RSU_j uses one of its certificates $(cert_{RSU_{ji}})$ and signing keys $(S_{\gamma j_i})$ to issue a certificate for an OBU, this is corresponding to using anonymous group signature since $S_{\gamma j_i}$ and $cert_{RSU_{ji}}$ are shared among multiple RSUs. Also, the generated certificate for OBU contains a pseudo identity (PID) which cannot be related to the real identity of the OBU. Since an observer can link an OBU certificate to neither the real identity of the OBU nor the location of the RSU which issued that certificate, the issued certificate $cert_{OBU_{nji}}$ is anonymous.
- The non-interactive key agreement in *Phase I* (Step 1 and Step 2) is very attractive to vehicular networks, since it enables any entity $\mathcal{A}$ to establish a shared secret key with another entity $\mathcal{B}$ by calculating the bilinear pairing of its secret key and the public key of $\mathcal{B}$. The non-interactive key agreement is of significant importance for updating certificates and establishing secure channels in VANETs.

C. Certificate Revocation

Revocation is required to prevent compromised entities from accessing the network. In the DCS scheme, we adopt the Certificate Revocation List (CRL) method, which is the revocation

method employed in the WAVE standard [8]. A CRL is a list containing all the identities and the validity periods of the revoked certificates. It should be noted that the short lifetime certificates of OBUs will be self revoked after their lifetime expires. The certificates of an entity (OBU or RSU) are added to a CRL only if the entity is compromised. When an entity (OBU or RSU) is compromised in one domain, the CA responsible for that domain adds all the certificates of the compromised entity to the current CRL, and broadcasts the new CRL in its domain. Each entity continuously maintains the recently received CRL by removing the certificates with expired validity periods.

According to the distribution of the CRLs in the DCS scheme, each CA distributes the CRL to the RSUs in its domain through its local Ethernet. Then, the RSUs receiving the new CRL broadcasts it to all the OBUs in that domain. Also, the CRL is delivered from the border RSUs in one domain (i) to the border RSUs in the adjacent domain (w) to enable the RSUs in domain (w) to check the revocation status of the OBUs coming from domain (i). However, the CRL corresponding to domain (i) will be kept in the border RSUs in domain w, and it will not be further broadcasted in domain w. For example, a CRL is broadcasted by CA_i in its domain (see Fig. 3). This CRL is broadcasted in domain i until it reaches RSU_l. Then, RSU_l broadcasts this CRL in its coverage area, and it delivers this CRL to RSU_j in domain w. RSU_j stores this CRL to check the revocation status of the OBUs moving from domain i to domain w. In case RSUs do not completely cover the domain of a CA, Laberteaux *et al.* [23] show that V2V communication can be used to efficiently distribute a CRL to all the OBUs. More results about the efficiency of the CRL distribution using V2V communications can be found in [23].

VI. Certificate-Based Message Signature and Verification

To satisfy the data authentication and non-repudiation security requirements of VANETs, each entity in the system should be capable of signing and verifying a given message with the corresponding certificate. In this section, we present the basic message signature and verification, followed by the proposed batch verification for message signature and certificate.

A. OBU/RSU/CA Message Signature and Verification

An OBU_m with $cert_{OBU_{mji}}$ can generate a valid signature $(U_m^{\backslash\backslash\backslash}, V_m^{\backslash\backslash\backslash})$ for a given message M as follows.

1) Select a random number $c_m \in \mathbb{Z}_q^*$;

2) Calculate $U_m^{\backprime\backprime\backprime}$, R_m, and $V_m^{\backprime\backprime\backprime}$, where $U_m^{\backprime\backprime\backprime} = c_m P$, $R_m = H_2(M||PK_{m_{ji}}||U_m^{\backprime\backprime\backprime}||PID_m||t_{stamp}) \in \mathbb{Z}_q^*$, and $V_m^{\backprime\backprime\backprime} = SK_{m_{ji}} + c_m R_m P_\mu$;
3) $(U_m^{\backprime\backprime\backprime}, V_m^{\backprime\backprime\backprime})$ is a valid signature on M.

Any entity in the network can verify the signature $(U_m^{\backprime\backprime\backprime}, V_m^{\backprime\backprime\backprime})$ on the message M as follows.

1) Verify that the sender of the message is a valid user and check the time stamp t_{stamp};
2) Calculate

$$R_m = H_2(M||PK_{m_{ji}}||U_m^{\backprime\backprime\backprime}||PID_m||t_{stamp}); \tag{6}$$

3) Accept if

$$\begin{aligned} \hat{e}(P, V_m^{\backprime\backprime\backprime}) &= \hat{e}(P, SK_{m_{ji}} + c_m R_m P_\mu) \\ &= \hat{e}(P, SK_{m_{ji}})\hat{e}(P, c_m R_m P_\mu) \\ &= \hat{e}(P, z_m y_m x_j s Q_i)\hat{e}(P, c_m R_m P_\mu) \\ &= \hat{e}(sP, z_m y_m x_j Q_i)\hat{e}(R_m c_m P, P_\mu) \\ &= \hat{e}(PK_{m_{ji}}, P_\circ)\hat{e}(R_m U_m^{\backprime\backprime\backprime}, P_\mu). \end{aligned} \tag{7}$$

Similarly, any CA or RSU can sign an arbitrary message using the aforementioned procedures.

B. Batch Verification for Messages Signatures

Consider an OBU $\mathcal{A}$ receives $(U_1^{\backprime\backprime\backprime}, V_1^{\backprime\backprime\backprime})$, $(U_2^{\backprime\backprime\backprime}, V_2^{\backprime\backprime\backprime})$, $\cdots$, $(U_K^{\backprime\backprime\backprime}, V_K^{\backprime\backprime\backprime})$, which are the signatures on the messages M_1, M_2, $\cdots$, M_K, respectively. Then, those signatures can be aggregately verified as follows.

1) Calculate $\overline{V}^{\backprime\backprime\backprime} = \sum_{k=1}^{K} V_k^{\backprime\backprime\backprime}$, and R_1, R_2, $\cdots$, R_K as in eq. (6);
2) Calculate $\overline{U}^{\backprime\backprime\backprime} = \sum_{k=1}^{K} R_k U_k^{\backprime\backprime\backprime}$;
3) Accept if

$$\hat{e}(P, \overline{V}^{\backprime\backprime\backprime}) = \hat{e}(P_\circ, \sum_{k=1}^{K} PK_{OBU,k})\hat{e}(\overline{U}^{\backprime\backprime\backprime}, P_\mu) \tag{8}$$

where $PK_{OBU,k}$ is the public key in certificate k.

PROOF: Firstly, we consider an OBU $\mathcal{A}$ receives two messages from OBU_m and OBU_n, where OBU_m generates a signature $(U_m^{\backprime\backprime\backprime}, V_m^{\backprime\backprime\backprime})$ on the message M_1, where $U_m^{\backprime\backprime\backprime} = c_m P$ and $V_m^{\backprime\backprime\backprime} = SK_m + c_m R_m P_\mu = z_m y_m x_j s Q_i + c_m R_m P_\mu$. In addition, OBU_n generates a signature $(U_n^{\backprime\backprime\backprime}, V_n^{\backprime\backprime\backprime})$ on the message M_2, where $U_n^{\backprime\backprime\backprime} = c_n P$ and $V_n^{\backprime\backprime\backprime} = SK_m + c_n R_n P_\mu = z_n y_n x_j s Q_i + c_n R_n P_\mu$. OBU

$\mathcal{A}$ calculates $\overline{V}'' = V_m'' + V_n'' = z_m y_m x_j s Q_i + c_m R_m P_\mu + z_n y_n x_j s Q_i + c_n R_n P_\mu$. The received signatures can be aggregately verified by calculating $R_m,\ R_n$ and checking that

$$\begin{aligned}\hat{e}(P, \overline{V}'') &= \hat{e}(P, z_m y_m x_j s Q_i + c_m R_m P_\mu + z_n y_n x_j s Q_i + c_n R_n P_\mu) \\ &= \hat{e}(P, z_m y_m x_j s Q_i + z_n y_n x_j s Q_i)\hat{e}(P, c_m R_m P_\mu + c_n R_n P_\mu) \\ &= \hat{e}(sP, z_m y_m x_j Q_i + z_n y_n x_j Q_i)\hat{e}(R_m c_m + P R_n c_n P, P_\mu) \\ &= \hat{e}(P_\circ, PK_{m_{ji}} + PK_{n_{ji}})\hat{e}(R_m U_m'' + R_n U_n'', P_\mu) \\ &= \hat{e}(P_\circ, \sum_{k=1}^{2} PK_{OBU,k})\hat{e}(\overline{U}'', P_\mu)\end{aligned} \tag{9}$$

As for the multiple-message, they can be verified in a similar way.

C. Batch Verification for Certificates

Consider an OBU_m with certificate $cert_{OBU_{mji}} = (PK_{m_{ji}}, U_m', V_m', vperiod_m, PID_m, cert_{RSU_{ji}})$, and OBU_n with certificate $cert_{OBU_{nlw}} = (PK_{n_{lw}}, U_n', V_n', vperiod_n, PID_n, cert_{RSU_{lw}})$, where $cert_{RSU_{ji}} = (PK_{j_i},\ U_j,\ V_j,\ PID_j,\ Q_i)$ and $cert_{RSU_{l_w}} = (PK_{l_w},\ U_l,\ V_l,\ PID_l,\ Q_w)$. An independent third party can aggregately verify the OBUs certificates and the RSUs certificates included in them as follows.

1) Check $vperiod$ of each certificate and proceed only if valid;
2) Calculate $T_j = H_2(PK_{j_i}||PID_j||U_j||Q_i)$ and $T_l = H_2(PK_{l_i}||PID_l||U_l||Q_i)$;
3) Calculate $L_m = H_2(PK_{m_{ji}}||vperiod_m||PID_m||U_m')$ and $L_n = H_2(PK_{n_{lw}}||vperiod_n||PID_n ||U_n')$;
4) Calculate $\overline{V} = V_j + V_l$, $\overline{V}' = V_m' + V_n'$, $\overline{U} = T_j U_j + T_l U_l$, and $\overline{U}' = L_m U' + L_n U'$;
5) Accept if $\hat{e}(P, \overline{V}+\overline{V}') = (P_\alpha, Q_i+Q_w)\hat{e}(P_\gamma, PK_{ji}+PK_{lw})\hat{e}(\overline{U}+\overline{U}', P_\mu)$. This verification holds since

$$\begin{aligned}\hat{e}(P, \overline{V} + \overline{V}') &= \hat{e}(P, S_{\alpha i} + a_j T_j P_\mu + S_{\alpha w} + a_l T_l P_\mu + S_{\gamma j i} + b_m L_m P_\mu + S_{\gamma l w} + b_n L_n P_\mu) \\ &= \hat{e}(P, \alpha Q_i + a_j T_j P_\mu + \alpha Q_w + a_l T_l P_\mu + x_j \gamma Q_i + b_m L_m P_\mu + x_l \gamma Q_w + b_n L_n P_\mu) \\ &= \hat{e}(P, \alpha Q_i + \alpha Q_w)(P, x_j \gamma Q_i + x_l \gamma Q_w)\hat{e}(P, a_j T_j P_\mu + a_l T_l P_\mu + b_m L_m P_\mu + b_n L_n P_\mu) \\ &= \hat{e}(\alpha P, Q_i + Q_w)\hat{e}(\gamma P, x_j Q_i + x_l Q_w)\hat{e}(T_j U_j + T_l U_l + L_m U' + L_n U', P_\mu) \\ &= \hat{e}(P_\alpha, Q_i + Q_w)\hat{e}(P_\gamma, PK_{ji} + PK_{lw})\hat{e}(\overline{U} + \overline{U}', P_\mu)\end{aligned} \tag{10}$$

For K OBUs, their certificates can be aggregately verified as follows:

$$\hat{e}(P, \overline{V} + \overline{V}^{\backprime}) = \hat{e}(P_{\alpha}, \sum_{k=1}^{K} Q_k)\hat{e}(P_{\gamma}, \sum_{k=1}^{K} PK_{RSU,k})\hat{e}(\overline{U} + \overline{U}^{\backprime}, P_{\mu}) \tag{11}$$

where $\overline{V} = \sum_{k=1}^{K} V_k$, $\overline{V}^{\backprime} = \sum_{k=1}^{K} V_k^{\backprime}$, $PK_{RSU,k} = PK_{ji} + PK_{lw} + \cdots$, $\overline{U} = \sum_{k=1}^{K} T_k U_k$, and $\overline{U}^{\backprime} = \sum_{k=1}^{K} L_k U_k^{\backprime}$

D. Batch Verification for Messages Signatures and Certificates

Consider K OBUs with K certificates generating different K signatures on K different messages. An independent third party can aggregately verify the K signatures and certificates by combining eq. (8) and eq. (11) as follows.

$$\hat{e}(P, \overline{V} + \overline{V}^{\backprime} + \overline{V}^{\backprime\backprime}) = \hat{e}(P_{\circ}, \sum_{k=1}^{K} PK_{OBU,k})\hat{e}(P_{\alpha}, \sum_{k=1}^{K} Q_k)\hat{e}(P_{\gamma}, \sum_{k=1}^{K} PK_{RSU,k})\hat{e}(\overline{U} + \overline{U}^{\backprime} + \overline{U}^{\backprime\backprime}, P_{\mu}) \tag{12}$$

The proof of eq. (12) follows directly from eq. (9) and eq. (10). Eq. (12) shows that the DCS scheme overcomes the need to separately verify signatures and certificates of the senders, which is common to most of the existing batch verification schemes. The DCS scheme amplifies the capabilities of any entity in the network to simultaneously verify a relatively large number of signatures and certificates compared to the conventional verification method which verifies signatures and certificates one by one, thus, decreasing the verification overhead.

It should be noted that eq. (12) can be used by any OBU or RSU to verify the signatures and the certificates included in the K different messages sent by K OBUs. Consequently, eq. (12) represents how authentication can be achieved in V2V and V2I communications.

When there are invalid signatures in the received messages, the data cross checking technique employed in the WAVE standard can alleviate the effect of the invalid signatures. In specific, each OBU_n compares the data included in the received message from an OBU_m with those received from other OBUs. If there is a mismatch, OBU_n rejects the message. It should be noted that the data cross checking technique is useful only when the data contents of the message are malicious. However, if either the data contents of the message are correct and the signature is invalid or the message and signature are correct and the certificate is invalid, this technique is not useful. In such case, a search approach based on the binary authentication tree [13] can be employed to avoid individually verifying every signature. The basic concept of the binary

authentication tree is introduced in section II. The performance evaluation under such scenario is not trivial [13].

VII. Security Analysis

In this section, we evaluate the proposed DCS scheme according to the security objectives presented in section IV-A.

1) Authentication: It can be seen that finding the secret keys $s,\ \alpha,\ \gamma,\ \mu$ from the corresponding public keys $P_\circ,\ P_\alpha,\ P_\gamma,\ P_\mu$ are instances of the ECDLP problem. For example, to find s, we have the following ECDLP problem: given P and $P_\circ = sP$, find s. In DCS, the authentication of RSUs and OBUs is achieved using digital certificates. For example, the signature of any CA_i on the certificate of any RSU_j is $(U_j,\ V_j)$, where $U_j = a_jP$, $T_j = H_2(PK_{j_i}||PID_j||U_j||Q_i) \in \mathbb{Z}_q^*$, and $V_j = S_{\alpha i} + a_jT_jP_\mu$. It can be seen that to forge the certificate of any RSU_j, an attacker should know either $S_{\alpha i} = \alpha Q_i$ or $a_jT_jP_\mu$. Since Q_i is publicly known, finding $S_{\alpha i}$ reduces to finding α which is ECDLP problem as indicated above. Also, since T_j can be easily obtained from the certificate of RSU_j, finding $a_jT_jP_\mu$ reduces to finding a_jP_μ, which can be formulated as a CDH problem, i.e., given $U_j = a_jP$ and $P_\mu = \mu P$, find $a_jP_\mu = a_j\mu P$. The hardness of the CDH problem is closely related to solving the Discrete Logarithm (DL) problem [20]. Similar analogy applies to the OBUs certificates. Since ECDLP and CDH are hard computational problems [19][20], i.e., they cannot be solved in a sub-exponential time, the certificates of RSUs and OBUs are unforgeable. Since in each communication, an authentication of the sender is performed first, an illegitimate entity cannot communicate with the authentic network users. Also, data authentication is achieved by employing digital signatures, where any message transmitted by any CA, RSU, or OBU has to be signed first. Consequently, any message alteration during the transmission will be detected by the recipient. In clogging attacks, an attacker tries to impersonate a legitimate user, and overwhelms legitimate entities in the network by involving them in a large volume of key exchange or by sending bogus messages [24]. In the DCS scheme, each OBU/RSU authenticates the received messages before being involved in any key exchange or responding to the received message. According to [24], since authentication is done first before taking any action, the clogging attacks is hard to launch in the proposed DCS scheme.

2) Non-repudiation: Non-repudiation is achieved by requiring all the messages exchanged in the network to be digitally signed by its issuer. For example, the signature of any OBU_m on an arbitrary message M is (U'', V''), where $U'' = cP$, and $V'' = SK_{m_{ji}} + cRP_{\mu}$. Similar to the above discussion of the security of RSUs certificates, to forge the signature of OBU_m on M, the attacker has to find either $SK_{m_{ji}}$, which is ECDLP problem, or cRP_{μ}, which is CDH problem. Consequently, the signature of any entity cannot be forged. In addition, since non-repudiation is guaranteed, the liability requirement is also achieved since users cannot deny the transmission or the content of their messages.
3) Privacy: In DCS, privacy is preserved by the following techniques:
   - *Anonymous authentication:* Anonymous authentication is employed in DCS in the sense that each OBU has a certificate containing only a pseudo identity, which cannot lead in any way to the real identity of the OBU. Furthermore, by deploying anonymous authentication, the DCS scheme can efficiently prevent an adversary from tracking the real identity of the users.
   - *Frequent certificate update:* OBUs certificates have a short-lifetime. As a result, each OBU has to periodically change its certificate, which decreases the probability of being tracked by an external observer.
   - *Anonymous certificate issuer:* Since each RSU certificate is shared among multiple RSUs, the RSU certificate included in each OBU certificate cannot lead to the location where the OBU issued its certificate.
   - *Avoiding key escrow:* When an OBU_m updates its certificate from an RSU_j, RSU_j sends a partial secret key $y_m x_j s Q_i$ to OBU_m. After that, OBU_m calculates its final secret key as $SK_{m_{ji}} = z_m y_m x_j s Q_i$. It can be seen that finding $SK_{m_{ji}}$ from the partial secret key is ECDLP problem. Since the secret key of any OBU cannot be forged, the DCS is free from the key screw which is common to any PKI. As a result, the messages signed by the secret key of any OBU can only be verified by the public key of that OBU, and this signature cannot be generated by any other entity in the network, hence, achieving high privacy level.

   Although the DCS offers a collation of privacy preserving mechanisms, an observer can still launch a tracking attack on an OBU. However, this tracking attack requires an observer

to launch a large number of receivers along the path of the targeted OBU, and the targeted OBU has to move with the same velocity and in the same lane between any pair of adjacent receivers launched by the observer [1]. To protect the OBUs against this tracking of attack, the DCS can be efficiently integrated with Random Encryption Periods (REPs) proposed in [25]. In REPs, using group communications, an OBU surrounds itself with an encrypted communication zone to violate the conditions of being tracked by an observer.

4) Transparent roaming: Since any OBU can update its certificate from any RSU in the network, the DCS scheme overcomes the need to re-register the OBU entering a new domain with the new CA. Consequently, the transparent roaming is guaranteed in the DCS scheme.
5) Access control: Any illegal network access by a compromised RSU can be efficiently thwarted, since a CA can broadcast a revocation message including the certificates of that RSU. Once receiving that revocation message, all the OBUs can de-associate with that compromised RSU. Also, all the OBUs certificates issued by that RSU are revoked, as the revoked RSU certificates are contained in those certificates. In addition, a CA can revoke any misbehaving OBU by broadcasting a CRL containing the certificate of the misbehaving OBU. Consequently, all the network RSUs and OBUs terminate the communications with that OBU.

VIII. Performance Evaluation

In this section, we evaluate the performance of the DCS scheme from different aspects.

A. OBU Certificate Update Delay

In this subsection, we compare between the OBU certificate update delay in the DCS scheme, the ECPP protocol, and the classical PKI where an OBU has to contact a CA to update its certificates.

Let $T_{cert-DCS}, T_{cert-ECPP}$, and $T_{cert-CA}$ denote the time from the moment an OBU requests N_{cert} new certificates from an RSU to the moment it receives the required certificates in the DCS scheme, ECPP protocol, and the classical PKI, respectively. We consider the cryptography delay only due to the pairing and point multiplication operations on an elliptic curve as they are the most time consuming operations in the schemes under consideration. Let T_{pair} and T_{mul} denote the time required to perform a pairing operation and a point multiplication, respectively.

TABLE II

DCS CERTIFICATE UPDATE CRYPTOGRAPHY DELAY

certificate update step	operation	entity involved	cryptography delay
step(2)	OBU_n certificate verification	RSU_j	$4T_{pair} + 2T_{mul}$
	calculation of the shared key k_{jn}	RSU_j	T_{pair}
step(3)	calculation of N_{cert} partial public keys	RSU_j	$N_{cert}T_{mul}$
	calculation of N_{cert} partial secret keys	RSU_j	$N_{cert}T_{mul}$
step(4)	generation of N_{cert} final public keys	OBU_n	$N_{cert}T_{mul}$
step(5)	calculation of $\{U^{\backprime}_{n,r} \vert 1 \leq r \leq N_{cert}\}$	RSU_j	$N_{cert}T_{mul}$
	calculation of $\{L^{\backprime}_{n,r} \vert 1 \leq r \leq N_{cert}\}$	RSU_j	$N_{cert}T_{mul}$

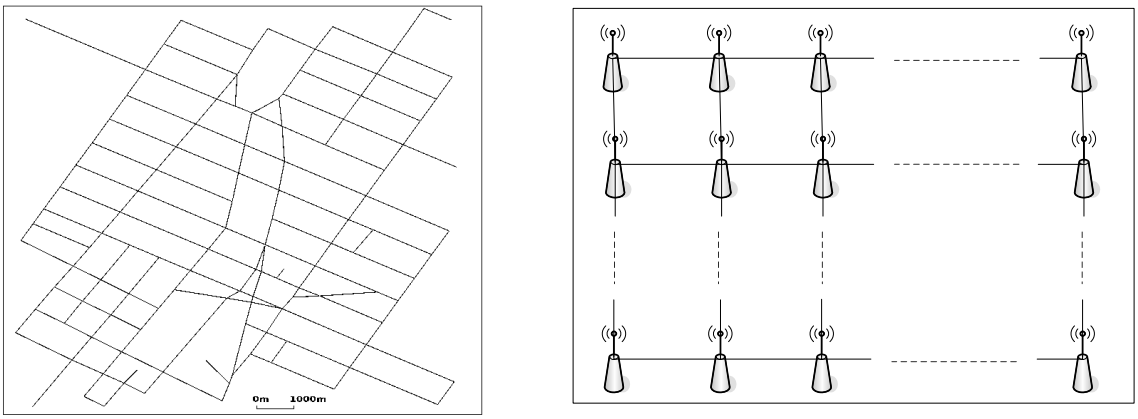
In [26], T_{pair} and T_{mul} are found for an MNT curve with embedding degree $k = 6$ to be equal to $4.5\ msec$, and $0.6\ msec$, respectively. Let $T_{crypt-DCS}$ and $T_{crypt-ECPP}$ denote the total incurred cryptography delay from the moment an OBU requests N_{cert} new certificates from an RSU to the moment it receives the required certificates in the DCS scheme, and ECPP protocol, respectively. It should be noted that the cryptography delay (T_{crypt}) is part of the certificate update delay (T_{cert}) in any of the schemes under consideration. Table II gives the cryptography delay incurred in each step of the DCS certificate update algorithm, shown in Fig. 4, from the moment an OBU requests N_{cert} new certificates from an RSU, i.e., step (2), until it receives the required certificates, i.e., by the end of step (5). According to Table II, we have

$$T_{crypt-DCS} = 5T_{pair} + (2 + 5N_{cert})T_{mul} \tag{13}$$

In the ECPP protocol [12], an RSU generates only one certificate for an OBU requesting certificate update. However, the ECPP protocol can be easily extended to enable an RSU to generate a bundle of N_{cert} certificates for the requesting OBU similar to the DCS scheme. In the case where ECPP protocol generates N_{cert} for the requesting protocol, we have

$$T_{crypt-ECPP} = (3 + 5N_{cert})T_{pair} + (4 + 9N_{cert})T_{mul} \tag{14}$$

We have conducted two ns-2 [27] simulations to respectively compare certificate update delay of the DCS scheme with that of the ECPP protocol and the classical PKI for the city street scenario shown in Fig. 5(a). The adopted simulation parameters are given in Table III. The mobility traces adopted in this simulation are generated using TraNS [28]. We use the IEEE



(a) City street map

(b) RSUs connection pattern

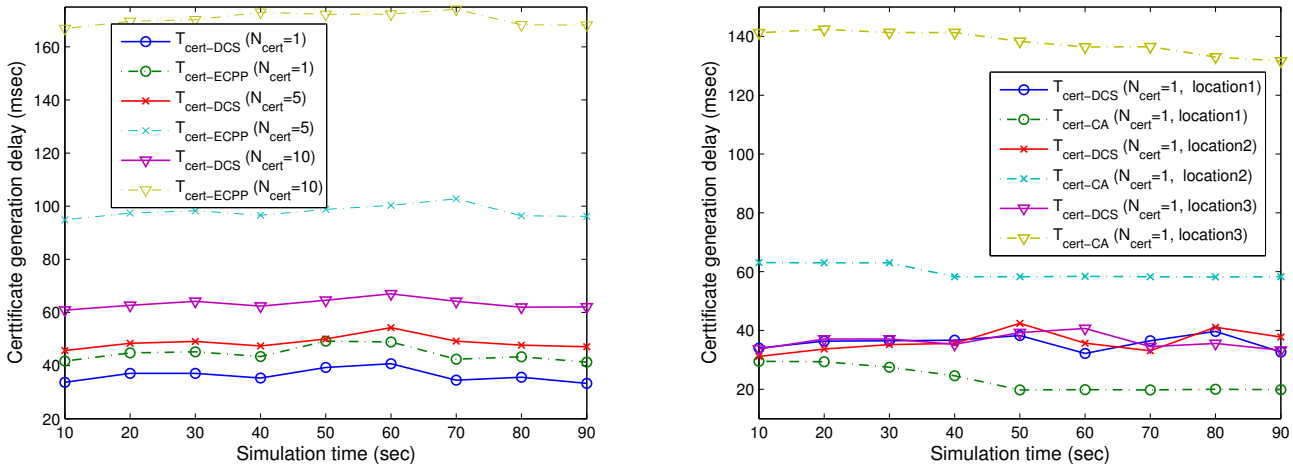
Fig. 5. Simulation scenario

TABLE III

NS-2 SIMULATION PARAMETERS

simulation area	13.4 $Km \times 12.3$ Km
simulation time	100 sec
max. vehicle speed	60 Km/h
OBU transmission range	300 m
MAC protocol	802.11a
OBU information dissemination interval	300 $msec$
wired channel capacity	100 Mbps
wireless channel capacity	6 Mbps
number of RSUs	576
distribution of RSUs	uniform

802.11a standard, which is the basis of DSRC, to simulate the Medium Access Control (MAC) protocol for VANETs [28][29]. VANETs have two types of links: wireless links connecting OBUs to each other and to the RSUs and wired links connecting the RSUs in one domain and the CA responsible for that domain as shown in Fig. 3 (we consider only the domain of CA_i in Fig. 3). According to the DSRC specifications, each wireless data channel in VANET has a bandwidth of 10 MHz corresponding to channel data rate in the range of 3 $Mbps - 27$ $Mbps$ [30]. We



(a) Certificate update delay for DCS and ECPP

(b) Certificate update delay for DCS and classical PKI

Fig. 6. Certificate update delay

select a data rate of 6 $Mbps$ for the wireless channels in VANET. We consider the links of the Ethernet connecting the RSUs and CA_i to have data rate of 100 $Mbps$. The RSUs connection pattern employed in our simulation is shown in Fig. 5(b). The adopted RSU connection considers a well deployed VANET, where the RSUs are uniformly distributed with the distance between any pair of adjacent RSUs is 500 m. CA_i is located at the top left corner of the city scenario shown in Fig. 5(a). To simulate real-life VANET scenarios, we conduct the certificate update scenarios imposed on VANET safety-related applications, where each OBU has to disseminate information about the road condition every 300 $msec$ according to DSRC.

The first simulation is conducted to compare the certificate update delay in the DCS scheme with that in the ECPP protocol. Fig. 6(a) shows the certificate update delay in $msec$ for the DCS scheme and the ECPP protocol vs. the simulation time in sec. In the conducted simulation, we consider N_{cert} to be constant for all the OBUs, where we consider values of N_{cert} equal 1, 5, and 10 certificates. In addition, an OBU sends a certificate update request every 10 sec during the simulation, and the corresponding certificate update delay is measured. The variations in $T_{cert-DCS}$ and $T_{cert-ECPP}$ are due to the variations of the distance separating the OBU requesting the certificate update and the RSU issuing the certificate. Table IV shows the average values of the certificate update delay shown in Fig. 6(a). It can be seen from Table IV that the DCS

TABLE IV

AVERAGE CERTIFICATE UPDATE DELAY

N_{cert}	avg. $T_{cert-DCS}$ (msec)	avg. $T_{cert-ECPP}$ (msec)	delay-saving
1	36.2	44.4	18.5%
5	48.8	98	50.2%
10	63.3	170.5	62.9%

scheme outperforms the ECPP protocol and the percentage of the delay-saving obtained by DCS compared to ECPP increases with N_{cert}. It should be noted that the average values for $T_{cert-DCS}$ and $T_{cert-ECPP}$ in Table IV are independent on the density of the RSUs as only one RSU is involved in each certificate update process. Therefore, the RSUs density has no effect on the certificate update delay.

The second simulation is conducted to compare the certificate update delay of the DCS scheme with that of the classical PKI [8] under a well-deployed VANET. The classical PKI certificate update requires each OBU requesting certificate update to contact the CA through the RSUs as the CA is the only entity responsible for generating the certificates. ECDSA [31] is the classical PKI digital signature method chosen by the WAVE standard, where a certificate and signature verification takes $4T_{mul}$, and a signature generation takes T_{mul}.

We consider two certificate update scenarios shown in Fig. 3 as follows. The first scenario is the classical PKI certificate update, where OBU_m (shown in red) needs to update its certificates. Hence, it should send a certificate update request to CA_i via the nearest RSU, which in this case is RSU_1. After the request reaches RSU_1, it will be forwarded through the RSUs' Ethernet to CA_i, where the request message experiences a delay of $4T_{mul}$ at each intermediate RSU, as each RSU has to verify the certificate and the signature of the sender before forwarding the request, otherwise, a denial of service attack can be easily launched by sending faked requests, which can overwhelm CA_i. When the certificate update request reaches CA_i, it has to verify the request which takes $4T_{mul}$, and generate new N_{cert} certificates for OBU_m which takes $N_{cert}T_{mul}$. Then, CA_i forwards the new certificates to RSU_l which in turn forwards them to OBU_m. In the second scenario, OBU_m updates its certificates directly from RSU_1 as proposed by the DCS scheme.

Fig. 6(b) shows the classical PKI certificate update delay $T_{cert-CA}$ and the DCS certificate

update delay $T_{cert-DCS}$ in $msec$ vs. the simulation time. We conducted simulation for the two certificate update scenarios triggered by OBU_m for N_{cert} equal 1 at three different locations: location1, location2, and location3 corresponding to initial distances of $2.7Km$, $4.7Km$, and $10.3Km$, respectively, from CA_i at the beginning of the simulation. The certificate update process is triggered every $10\ sec$ during the simulation and the corresponding certificate update delay is measured. The variations in $T_{cert-CA}$ are due to the number of the intermediate RSUs existing in the connection between CA_i and OBU_m. It can be seen that $T_{cert-DCS}$ is almost the same for the three locations, and is confined within the range $31msec - 43msec$. This is due to the fact that the DCS scheme is independent on CA_i. On the other hand, it can be seen that $T_{cert-CA}$ increases with the distance from CA_i. Consequently, the delay-saving of the proposed DCS scheme compared to the classical PKI certificate update increases with distance from the CA. For example, the average certificate update delay is $59.87\ msec$ for location2, while that for the DCS scheme is $36.2\ msec$. Consequently, the DCS scheme decreases the certificate update delay by 39.54% compared to the classical PKI in that case. From the aforesaid discussion, it can be seen that even under a well-deployed VANET the DCS scheme outperforms the classical PKI in terms of certificate update delay, which directly translates into a better certification service. In addition, since in the classical PKI, all certificates updates are handled by the CA, it is expected that the certificate update delay from the CA increases in real-life large scale VANETs.

B. Successful Certification Ratio

When an OBU_m requests N_{cert} certificates from an RSU_l, RSU_l should process the request, generate the required certificates, and deliver them to OBU_m before OBU_m moves out of the communication range of RSU_l, otherwise, the certificate update process fails. Therefore, if the number of certificate update requests is large, the RSU will not be able to process all the requests and some requests may be dropped. To calculate the maximum number of certificates that an RSU can generate within its coverage range, we adopt the following formula [12]

$$NC_{max} = \frac{R}{\overline{S} \cdot T_{cert}} \tag{15}$$

where NC_{max} is the maximum number of certificates an RSU can generate within its coverage range R, $\overline{S}$ is the average speed of the OBUs within R, and T_{cert} is the average certificate update delay of the scheme under consideration.

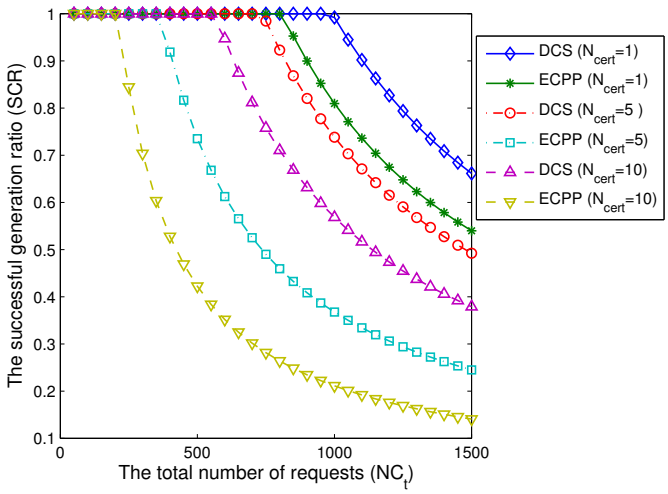


Fig. 7. Successful certification ratio

Successful Certification Ratio (SCR) is the metric usually used to evaluate the efficiency of authentication algorithms [32]. SCR is defined as the ratio of the number of successful certificate generations (NC_s) to the number of total certificate requests (NC_t). Hence, we have

$$SCR = \begin{cases} 1 & \text{if } NC_s \leq NC_{max} \\ \frac{NC_s}{NC_t} & \text{if } NC_s > NC_{max} \end{cases} \tag{16}$$

We consider an RSU with $R = 600m$ (corresponding to omnidirectional communication range with radius $300\ m$ according to DSRC), and the average speed of OBUs is $\overline{S} = 60\ Km/h$. Fig. 7 shows the successful certification ratio for the DCS scheme and the ECPP protocol [12] for values of N_{cert} equal $1,\ 5$, and 10 certificates vs. the total number of certificate requests, where we used the values of T_{cert} in Table IV. It should be noted that in the cases where $N_{cert} > 1$, each request in Fig. 7 is corresponding to generating N_{cert} certificates. It can be seen that DCS gives a higher SCR than the ECPP protocol. Also, the SCR for DCS with $N_{cert} = 10$ is even higher than that of the ECPP with $N_{cert} = 5$. Since DCS can handle a larger number of certificates requests than ECPP for the same duration, the DCS is more suitable for the requirement of vehicular networks.

C. The Required RSUs Density in DCS

In this section, we give a rough estimate of the required RSUs density in the DCS scheme. It is more meaningful to express the RSUs density $(density_{RSU})$ as the number of RSUs per

TABLE V

EXAMPLE OF THE REQUIRED $density_{RSU}$ IN DCS FOR $\overline{vperiod} = 1min$ AND $\overline{S} = 60Km/h$

state	New York	Hawaii
rural roads length (km)	106014	3285
urban roads length (km)	77033	3701
$\overline{N}_{cert}$ (rural)	20	20
$\overline{N}_{cert}$ (urban)	10	10
$density_{RSU}$ (rural)	0.05	0.05
$density_{RSU}$ (urban)	0.1	0.1
number of required RSUs (rural)	5301	165
number of required RSUs (urban)	7074	371
total number of RSUs	13005	536

road unit length (Km) instead of per unit area (Km^2) as RSUs are implemented only on the roads, and a road width is generally much smaller than its length. The average distance D_{RSU} the OBUs can move without the need to contact an RSU is

$$D_{RSU} = \frac{1}{60}\overline{N}_{cert}\ \overline{vperiod}\ \overline{S}\ \ (Km), \tag{17}$$

where $\overline{N}_{cert}$ is the average number of the generated certificates per OBU from the RSUs , $\overline{vperiod}$ is the average validity period of the OBUs certificates in min, and $\overline{S}$ is the average speed of the OBUs in Km/h. It should be noted that the parameters in eq. (17) are corresponding to only one domain. Since D_{RSU} can be interpreted as the road distance between two adjacent RSUs. Consequently, the required RSU density $(density_{RSU})$ for the DCS scheme can be calculated as

$$density_{RSU} = \frac{1}{D_{RSU}} = \frac{60}{\overline{N}_{cert}\ \overline{vperiod}\ \overline{S}}\ \ (/Km) \tag{18}$$

Eq. (18) can be used in the design phase of the DCS scheme to calculate the number of RSUs needed for the operation of the DCS scheme.

Table V gives an example of the required densities and numbers of RSUs for New York and Hawaii states for $\overline{vperiod} = 1min$ and $\overline{S} = 60Km/h$. New York has an area of $141299Km^2$ while that for Hawaii is $28311Km^2$ [33]. The total length of the urban and rural roads is obtained from [34]. Since the density of the OBUs in an urban road is higher than that in a rural road, it will not be cost-effective to implement RSUs in rural roads with a density equal to that in urban roads. Therefore, we select $\overline{N}_{cert}$ for rural and urban roads to be 20 and 10, respectively. The

TABLE VI

RSU_j CERTIFICATE SIZE IN DCS

parameter	PK_{j_i}	U_j	V_j	PID_j	Q_i	$cert_{RSU_{ji}}$
size in bytes	21	21	21	8	21	92

TABLE VII

OBU_m CERTIFICATE SIZE IN DCS

parameter	$PK_{m_{ji}}$	$U_m^{\backprime}$	$V_m^{\backprime}$	$vperiod$	PID_m	$cert_{RSU_{ji}}$	$cert_{OBU_{mji}}$
size in bytes	21	21	21	4	8	92	167

total number of the required RSUs can be decreased by increasing the validity period ($\overline{vperiod}$) of the certificates of the OBUs or increasing N_{cert}. However, increasing $\overline{vperiod}$ increases the probability of being tracked, i.e., lowering the privacy protection level. Also, increasing the number of certificates (N_{cert}) generated from RSUs decreases the SCR as shown in Fig. 7. A compromise between the privacy protection level and the SCR of RSUs should be made according to the required RSUs density. It should be noted that each CA can change the minimum and maximum bound to the value of the certificate validity period according to the required level of privacy protection, and broadcast these bounds to the RSUs in its domain through its local Ethernet.

D. Communication Overhead

We consider the Tate pairing implementation on an MNT curve with embedding degree 6, where $\mathbb{G}_1$ is represented by 161 bits. Accordingly, each point on this MNT curve is represented by 21 bytes. Table VI and Table VII give each parameter and the corresponding size in bytes for an RSU and OBU certificate, respectively. The last column in each table gives the total size of the certificate under consideration. It can be seen that an RSU has a certificate size of 92 bytes, while that for an OBU is 167 bytes.

It is indicated in section VI-A that an OBU_m with $cert_{OBU_{mji}}$ can generate a valid signature $(U^{\backprime\backprime}, V^{\backprime\backprime})$ for an arbitrary message M. Since $U^{\backprime\backprime}$ and $V^{\backprime\backprime}$ are points on the elliptic curve, the signature size in DCS is 42 bytes. Consequently, the communication overhead incurred in a signed message transmitted by an OBU is 209 bytes, which is the certificate size plus the signature

size, compared to an overhead of 189 bytes in the ECPP protocol. According to WAVE [8], the maximum payload data size in a signed message is 65.6 Kbytes. Consequently, the ratio of the communication overhead incurred by the DCS scheme to the payload data size is 0.3%, which means that the DCS scheme is feasible with respect to the incurred communication overhead.

E. OBU Message Signing Delay

In DCS, the signature of an OBU_m with $cert_{OBU_{mji}}$ on an arbitrary message M is (U'', V''). The cryptography operation involved in calculating either U'' or V'' is point multiplication. Therefore, the total delay for signing a message in DCS is $2T_{mul}$. The second column in Table VIII gives the message signing delay for ECDSA, BLS, CAS, ECPP, and DCS. BLS is a pairing-based aggregate signature [35]. CAS is a certificateless aggregate signature scheme [36], which is the basis of the DCS batch verification scheme.

It can be seen that ECDSA and ECPP give the lowest message signing delay, and DCS gives the second lowest delay. The effect of the message signing delay is alleviated by the fact that an OBU has to disseminate only one signed message every 300 $msec$, which means that an OBU has a time window of 300 $msec$ to prepare a signature on a message. The DCS scheme has a message signing delay of 1.2 $msec$, which can be neglected compared to the time window an OBU has to sign a message.

F. Batch Verification Delay

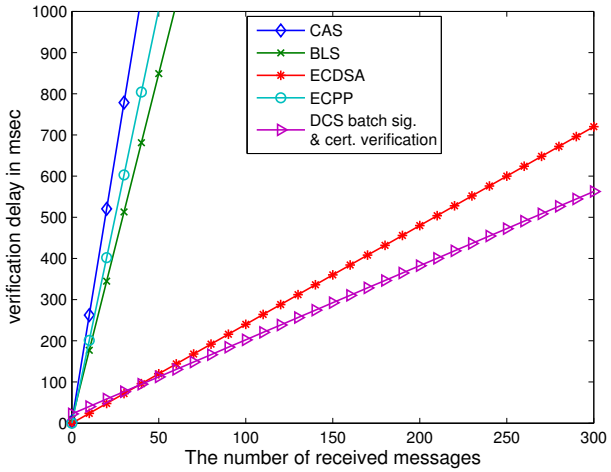
We compare the verification delay of the DCS batch signature and certificate verification scheme with ECDSA, BLS, CAS, and ECPP.

The time needed to verify one ECDSA signature is $2T_{mul}$, and that for BLS is $2T_{pair} + T_{mtp}$, where T_{mtp} is a map to point hash function. T_{mtp} is found for an MNT curve to be 3.9 $msec$ [37]. We consider the verification delay for a certificate sent with a message signature for ECDSA and BLS to be equal to that of a signature verification. The time needed to verify one CAS signature is $3T_{pair} + 2T_{mtp}$. For CAS, there is no certificate; however, to verify the sender, a check process must be performed which takes $2T_{pair}$. For ECPP, the total verification delay of a certificate and signature is $3T_{pair} + 11T_{mul}$. For the DCS scheme, the verification delay of a certificate and message signature requires $5T_{pair} + 3T_{mul}$, where $5T_{pair}$ corresponds to the pairing operations in the left and right hand sides of eq. (12), and $3T_{mul}$ corresponds to the point multiplication

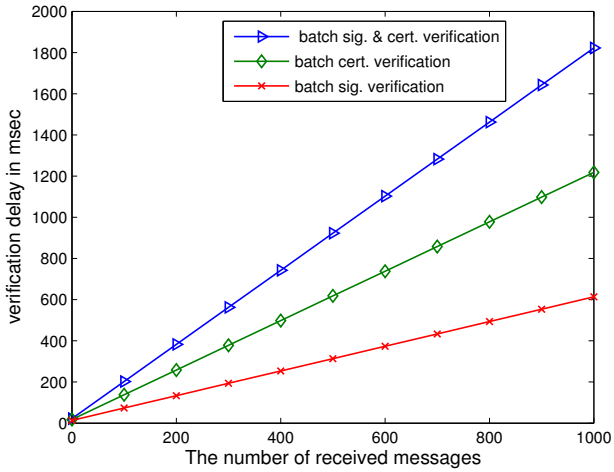
TABLE VIII

SIGNING AND VERIFICATION DELAY

Method	message signing	one signature and certificate verification	K signatures and certificates verifications
ECDSA	T_{mul}	$4T_{mul}$	$4KT_{mul}$
BLS	$T_{mul}+T_{mtp}$	$4T_{pair}+2T_{mtp}$	$(2K+2)T_{pair}+2KT_{mtp}$
CAS	$2T_{mul}+T_{mtp}$	$5T_{pair}+2T_{mtp}$	$(4K+1)T_{pair}+2KT_{mtp}$
ECPP	T_{mul}	$3T_{pair}+11T_{mul}$	$3KT_{pair}+11KT_{mul}$
DCS	$2T_{mul}$	$5T_{pair}+3T_{mul}$	$5T_{pair}+3KT_{mul}$



(a) Verification delay comparison between different schemes



(b) Verification delay of the different batch schemes of DCS

Fig. 8. Verification delay

operations in $\overline{U}$, $\overline{U}^{\backprime}$, and $\overline{U}^{\backprime\backprime}$. Table VIII shows a summary of the verification delays for ECDSA, BLS, CAS, ECPP, and the DCS schemes.

Fig. 8(a) shows the verification delay in $msec$ vs. the number of the received messages. It can be seen that the DCS scheme has the lowest verification delay. Also, from Table VIII and the values of T_{pair}, T_{mtp}, and T_{mul}, the most time-consuming operation in the signature verification process of the schemes under consideration is the pairing operation. Hence, the reason for the superiority of the DCS is that the number of the pairing operations required

for signatures verification is independent on the number of the signatures to be verified. The maximum number of signatures and certificates that can be verified simultaneously in $300\ msec$ is $11,\ 14,\ 17,\ 124,$ and 154 messages for CAS, ECPP, BLS, ECDSA, and the DCS schemes, respectively. The number of signatures and certificates that the DCS scheme can verify is greater than that of the ECDSA by 24.2%. Fig. 8(b) shows the delay for batch signature verification, batch certificate verification, and simultaneous batch signature and certificate verification. The maximum number of certificates that can be verified aggregately within $300\ ms$ is 234 certificates, while that for signatures is 477 signatures.

To further evaluate the DCS batch verification scheme, we conduct ns-2 [27] simulation using the same parameters in Table III except for simulation area and time, which become $7.4\ Km \times 7.4\ Km$ and $30\ sec$, respectively. In this simulation, we are interested in the message loss incurred by OBUs due to V2V communications only, i.e., we do not consider the implementation of RSUs. The average message loss ratio is defined as the average ratio between the number of messages dropped every $300\ msec$, due to signatures and certificates verification delay, and the total number of messages received every $300\ msec$. According to DSRC, each OBU has to disseminate information about the road condition every $300\ msec$. In order to react properly and instantly to the varying road conditions, each OBU should verify the messages received during the last $300\ msec$ before disseminating a new message about the road condition. Therefore, we chose to measure the message loss ratio every $300\ msec$. Fig. 9 shows the analytical and simulated average message loss ratio vs. the average number of OBUs within the communication range of each OBU for DCS, ECPP, ECDSA, BLS, and CAS, respectively. It can be seen that the simulated average message loss ratio closely follows the analytical message loss ratio which is calculated based on the maximum number of messages that can be verified within $300\ msec$ in the schemes under consideration. The difference between the analytical and simulations results stems from observing that some zones in the simulated area become more congested than other zones, thus, some OBUs experience higher message loss than other OBUs, which on the average leads to that difference between the analytical and simulation results. Also, the proposed DCS batch verification provides the lowest message loss ratio, and the message loss ratio increases as the number of OBUs within communication range increases. The reason of the superiority of the DCS scheme is that it can aggregately verify a number of signatures higher than that of ECPP, ECDSA, BLS, or CAS.

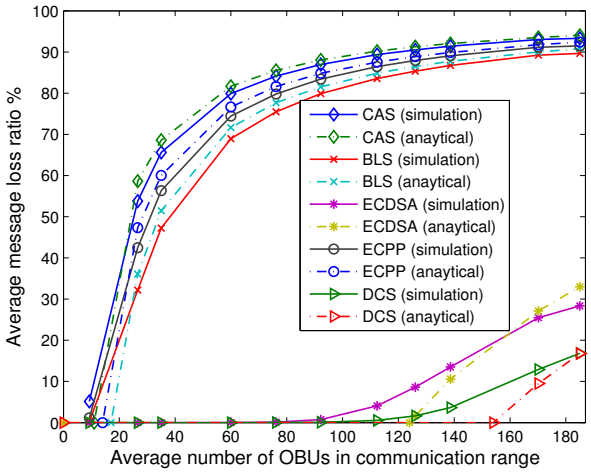


Fig. 9. Comparison between message loss ratio for different schemes

G. Additional GPS Memory Requirements

In the DCS scheme, the GPS receiver in each OBU is required to be loaded with the geographic coordinates of the RSUs, which incurs additional memory requirements. According to [8], each latitude or longitude coordinate of the geographic location of an RSU is represented by 4 bytes. With the results obtained in section VIII-C, the number of RSUs in a CA domain is in the order of 10^4. Consequently, the memory size required to save the coordinates of the RSUs in a domain requires 0.08 Mbytes. Most of the currently available GPS receivers have sufficient memory storage to meet this requirement.

IX. Conclusion

In this paper, we have proposed an efficient distributed certificate service (DCS) scheme for vehicular communications, which offers a flexible interoperability to avoid the key escrow issue in different administrative authorities and an efficient distributed algorithm for any OBUs to update or revoke its certificate from the available RSUs in a timely manner. In addition, with the batch verification, the entities in the DCS scheme can rapidly verify a mass of message signatures and certificates simultaneously. Therefore, the proposed DCS scheme can significantly reduce the complexity of certificate management, and achieve excellent efficiency and scalability, especially when it is deployed in heterogeneous vehicular networks. For our future work, we will investigate the revocation issue under the context of the proposed DCS scheme.

REFERENCES

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

[2] F. Dötzer, "Privacy issues in vehicular ad hoc networks," *Proc. 2nd ACM Workshop on Vehicular Ad Hoc Networks*, September 2006.

[3] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and identity management for vehicular communication systems: a position paper," *Proc. Workshop on Standards for Privacy in User-Centric Identity Management, Zurich, Switzerland*, July 2006.

[4] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET," *Proc. Embedded Security in Cars (ESCAR)*, November 2005.

[5] J. P. Hubaux, "The security and privacy of smart vehicles," *IEEE Security and Privacy*, vol. 2, pp. 49–55, 2004.

[6] M. Shi, X. Shen, and J. Mark, "IEEE 802.11 roaming and authentication in wireless LAN/cellular mobile networks," *IEEE Wireless Communications*, vol. 11, no. 4, pp. 66–75, 2004.

[7] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 9, pp. 2569–2577, 2006.

[8] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Std 1609.2-2006*, 2006.

[9] "5.9 GHz DSRC." [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[10] 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, pp. 3442–3456, 2007.

[11] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Proc. Crypto, LNCS*, vol. vol. 3152, pp. 41–55, 2004.

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

[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] D. Boneh and M. K. Franklin, "Identity-based encryption from the Weil pairing," *Proc. 21st Annual Inter. Cryptology Conf. on Advances in Cryptology*, pp. 213–229, 2001.

[15] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," *J. of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[16] M. Scott, "Computing the Tate pairing," *Topics in Cryptology, Springer*, pp. 293–304, 2005.

[17] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-Reductions." *IEIC Technical Report*, vol. 100, no. 323(ISEC2000 58-67), pp. 99–108, 2000.

[18] "Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL)." [Online]. Available: http://www.shamus.ie/

[19] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes and Cryptography*, vol. 19, no. 2, pp. 173–193, Mar. 2000.

[20] D. Boneh and R. Lipton, "Algorithms for black-box fields and their application to cryptography," *Proc. Advances in Cryptology - CRYPTO '96*, pp. 283–297, 1996.

[21] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," *Proc. Advances in Cryptology - ASIACRYPT 2003*, pp. 452–473, 2003.

[22] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," *Proc. 4th Inter. Conf. on CANS, LNCS*, vol. 3810, Springer Verlag, pp. 13–25, 2005.

[23] K. P. Laberteaux, J. J. Haas, and Y. Hu, "Security certificate revocation list distribution for VANET," *Proc. 5th ACM inter. workshop on VehiculAr Inter-NETworking*, pp. 88–89, 2008.

[24] R. Oppliger, "Protecting key exchange and management protocols against resource clogging attacks," *Proc. Joint Working Conf. on Secure Information Networks*, pp. 163–175, 1999.

[25] A. Wasef and X. Shen, "REP: location privacy for VANETs using random encryption periods," *ACM Mobile Networks and Applications (MONET)*, to appear.

[26] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," *Proc. IEEE INFOCOM 2008*, pp. 246–250, 2008.

[27] "The network simulator - ns-2." [Online]. Available: http://nsnam.isi.edu/nsnam/index.php/User Information

[28] "Traffic and network simulation environment - TraNS." [Online]. Available: http://trans.epfl.ch/

[29] D. Cottingham, I. Wassell, and R. Harle, "Performance of IEEE 802.11a in vehicular contexts," *IEEE 65th Vehicular Technology Conf.*, pp. 854–858, 2007.

[30] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty, "Performance evaluation of safety applications over DSRC vehicular ad hoc networks," *Proc. 1st ACM inter. workshop on Vehicular ad hoc networks*, pp. 1–9, 2004.

[31] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Inter. J. of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[32] K. Sadasivam and T. Yang, "Evaluation of certificate-based authentication in mobile ad hoc networks," *Proc. IASTED NCS 2005*, April 2005.

[33] "List of U. S. states by area." [Online]. Available: http://www.knowledgerush.com/kr/encyclopedia/List_of_U.S._states_by_area/

[34] "United states department of transportation - federal highway administration." [Online]. Available: http://www.fhwa.dot.gov/policyinformation/statistics/2007/hm20m.cfm

[35] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," *Proc. Advances in Cryptology. EUROCRYPT 2003*, pp. 416–432, 2003.

[36] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," *Proc. 8th ACIS Inter. Conf. on SNPD 2007*, vol. 3, pp. 188–193, 2007.

[37] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-ayer location privacy," *IEEE Transactions on Vehicular Technology,*, vol. 58, no. 3, pp. 1454–1466, 2009.