International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

An RSU Aided Distributed Certificate Update Scheme In Vehicular Networking Environment.

Sunil Solanki*
* PG Scholar,
Department of Computer Engineering, L D College of Engg., (Gujarat Technological University), Ahmedabad, India

Abstract- The Vehicular Ad-hoc Networks have been becoming promising technology towards developing applications like Intelligent Transport Systems (ITS) that aim to streamline the operation of vehicles, manage vehicle traffic, assist drivers with safety and other information, along with provisioning of convenience applications for passengers. As the open medium wireless communication leads to unreliable communication and brief (short-lived) connection and another important issue is the roaming between different domains due to high-speed mobility of vehicles and leads to the explicit cross-certificate agreement to provide interoperability for these vehicles. This paper presents a Robust Distributed Certificate approach for Authentication in vehicular networks which enables efficient certificate update from available Road-Side Unit in timely manner, to address the these security and performance issues,.

Index Terms- VANET, ITS, RSU, CA, OBU, WAVE, DSRC.

I. INTRODUCTION

VANETs consist of network entities, mainly including OBU (On Board Unit within Vehicle) 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. Prime applications of VANET services include automated toll collection systems, driver assist systems and other information provisioning systems. This grassroots movement has also been backed up by coordinated efforts for standardization and formation of consortia and other governmental and industrial bodies that aim to set the guiding principles, requirements, and first takes on solutions for communication systems that primarily involve vehicles and users within vehicles.

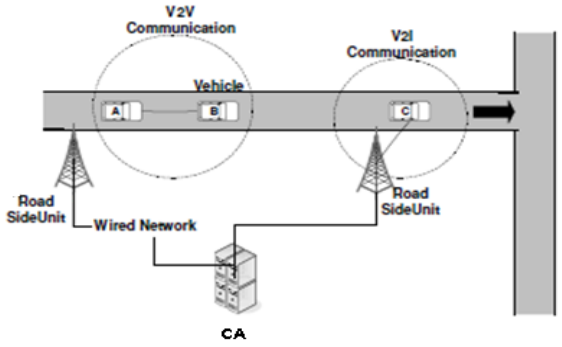


Figure. 1 Vehicular Networking Environment.

By the next decade it is expected that 70% of all vehicular components will be electronic and with this integration VANET vehicles will be capable of storing and processing great amounts of information, including a driver's personal data and geo-location information. A VANET vehicle (Figure.2) is equipped with processing, recording and positioning mechanisms with a potentially infinite power supply.

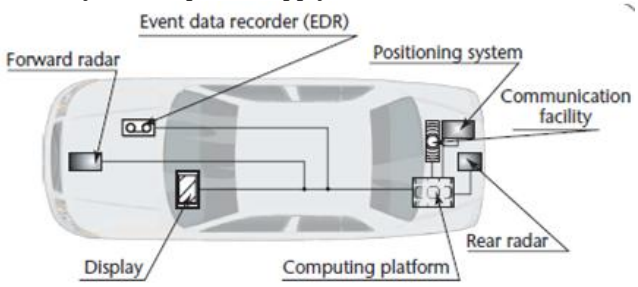


Fig. 2. A smart vehicles with central computing platform.

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. 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. 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), 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.

According to the Dedicated Short Range Communication (DSRC)[5], 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.

Security Challenges & Requirements.

As vehicle-to-vehicle(V2V), vehicle-to-roadside units and vehicle-to-infrastructure(V2I) communication involves variety of applications, ranging from infotainment applications, such as media downloading, to traffic safety applications, such as driving assistance co-operative awareness, impose diverse requirements on the supporting vehicular networking technologies. These diverse requirements lead us to a number of research challenges. This section describes these research challenges.

A. Addressing and Geographical addressing
B. Risk analysis and management
C. Data-centric Trust and Verification
D. Anonymity, Privacy and Liability
E. Secure Localization
F. Forwarding algorithms
G. Delay constraints
H. Prioritization of data packets and congestion control
I. Reliability and cross-layering between transport and network layers

WAVE/ DSRC Standards.[4][5]

DSRC-based ITS radio spectrum is a 75 MHz bandwidth in the 5.85 - 5.925 GHz for the DSRC frequency band. These standards are: IEEE 1609.1-resource manager, IEEE 1609.2-security, IEEE 1609.3-networking, IEEE 1609.4-multichannel operation. The combination of IEEE 802.11p and the IEEE 1609 protocol suite is denoted as WAVE (Wireless Access in Vehicular Environments).

Architecture for Secure Communication. [3]

The SeVeCOM architecture used in VANET addresses the following fundamental issues:

- Identity, credential, and key management
- Secure communication

The main elements of the architecture are.

AUTHORITIES
NODE IDENTIFICATION
HARDWARE SECURITY MODULE
SECURE COMMUNICATION

Digital signatures are the basic tools to secure communications and are used for all messages. To satisfy both the security and anonymity requirements, it relies on a *pseudonymous authentication* approach. Rather than utilizing the same long-term public and private key for securing communications, each vehicle utilizes multiple short-term private-public key pairs and certificates. A mapping between the short-term credentials and the long-term identity of each node is maintained by the CA.

The basic idea is that:

• Each vehicle is equipped with multiple certified public keys (pseudonyms) that do not reveal the node identity.
• The vehicle uses each of them for a short period of time, and then switches to another, not previously used pseudonym.

This way, messages signed under different pseudonyms cannot be linked. Signatures, calculated over the

message payload, a timestamp, and the coordinates of the sender, can be generated by the originator of a message, as well as relaying nodes, depending on the protocol functionality.

Security for frequently broadcast *safety beacon* messages, *restricted flooding* of messages within a geographical region or a hop-distance from the sender, and *position-based routing* used to transmit messages through a single route of relay nodes, where the nodes select as the next hop their neighbor with minimum remaining geographical distance to the destination position.

II. RELATED WORKS

Entity authentication, message integrity, non-repudiation, and privacy preservation in spontaneous vehicular communications are the primary security requirements and deploying efficient Public Key Infrastructure (PKI) is a well-recognized solution to achieve security & privacy for practical vehicular networks [1],[2].

In [2], 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 and efficiency for certificate management as revoking one vehicle implies revoking the huge number of certificates loaded in it, proves to trade-offs.

Panagiotis Papadimitratos, et. al[3] within the SeVeCom project, developed a security architecture that provides a comprehensive and practical solution to provide a solution that can be quickly adopted and deployed.

Lin *et al.*[6] use the group signature in [7] 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 signature verification delay is linearly proportional to the number of revoked vehicles, causes poor 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.*[8] propose Efficient Conditional Privacy Preservation (ECPP) protocol for secure vehicular communications, which allows an OBU to get a short lifetime anonymous certificate (free from the key escrow property) from any RSU located in the domain in which the OBU was originally registered. The performance of the ECPP protocol is also evaluated under a well-deployed VANET.

Jiang *et al.*[9] propose a verification scheme capable of detecting bogus signatures in batch signature verification schemes, based on a new data structure called BAT - binary authentication tree.

Albert Wasef, Yixin *et al.* [16] proposed a scheme which 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 with Master Authority at the topmost level raises single point failure possibility.

G. Calandriello *et al.* proposes a way to achieve efficient and robust *pseudonym*-based authentication, to enhance the availability and usability of privacy-enhancing VANET mechanisms: that enables vehicle on-board units to generate their own pseudonyms, without affecting the system security.

Brijesh Kumar Chaurasia *et al.*[P-9], proposed a mutual authentication technique for RSU and vehicle The technique has only one request reply message exchange.

V. Casola, *et al.*[17]presented a framework and its corresponding architecture to cope with security and interoperability problems appearing in VANET environments requiring the use of multiple regional Certification Authorities. The concept requires the Interoperability System (IS) & Reference Evaluation Methodology (REM).

In connection with [16] & [17], we propose a Robust Distributed Certificate based certificate update scheme which enables an OBU to update its certificate from any RSU. Consequently, certificate delay can be significantly decreased. Also, the scheme addresses the "Communication Silent" periods resulting in short-lived connections occurring due to natural characteristic of VANET, with the help of OBU Object (OO)- a software module.

III. PROPOSED SYSTEM

Now it is the time to articulate the research work with ideas gathered in above steps by adopting any of below suitable approaches:

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 $G1$ denote an additive group of prime order q, and $G2$ a multiplicative group of the same order. Let P be a generator of $G1$, and $e\hat{}: G1 \times G1 \rightarrow G2$ be a bilinear mapping with the following properties:

1) Bilinear: $e\hat{}(aP, bQ) = e\hat{}(P, Q)^{ab}$, for all $P, Q \in G1$ and $a, b \in R\ Z_q$.
2) Non-degeneracy: $\hat{}(P, Q) \neq 1_{G2}$.
3) Symmetric: $e\hat{}(P, Q) = e\hat{}(Q, P)$, for all $P, Q \in G1$.
4) Admissible: the map $e\hat{}$ is efficiently computable.

The bilinear map e can be implemented using the Weil and Tate pairings on elliptic curves. We consider the implementation of Tate pairing on a curve with embedding degree 6, where $G1$ is represented by 161 bits, and the order q is represented by 160 bits. The group order of $G1$ 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 $G1$ is 4.5×10^{30}, which qualifies the bilinear pairing as a practical choice for securing the large scale VANETs.

TABLE-I: NOTATIONS

SYMBOL	NOTATION
CA	Certifying Authoreity
RSU_i	ith Road Side Unit
OBU_m	mth OBU
S	Master secret key of CA for secret key generation
α	CA Secret signing-key for signing RSU certificat
γ	Partial secret signing-key for signing OBU certifi
P_0	Public key used to verify signatures on any messa
P_α	Public key used to verify RSU certificates
$P\gamma$	Public key used to verify OBU certificates
γ_i	RSU_i secret key, generated by CA, to sign OBU
P_K	Public key for CA
S_K	Secret key for CA
P_{Ki}	RSUi public key generated by CA
S_{Ki}	RSU_i secret key generated by CA
$CERT_{RSUi}$	Certificate for RSUi generated by CA
PKm_i	OBU_m public key generated by RSU_i using PK_i
SKm_i	OBU_m secret key generated by RSU_i using SK_i
vepriod	OBU certificate validity period
$CERT_{OBUmi}$	OBU_m certificate generated by RSU using γ_i
tstamp	Time stamp
H_1	Hash function such that $\{0,1\}^* \in G_1^*$.
H_2	Hash function such that $\{0,1\}^* \in Z_q^*$.

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 is to determine the integer l, $0 \leq l \leq q - 1$, such that $Q = lP$.
- Computational Diffie-Hellman problem (CDH): For two unknowns $a, b \in Z_q^*$, the CDH problem is given $aP, bP \in G1$, compute $abP \in G1$.

SYSTEM DESIGN CONSIDERATIONS

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

A. Security Objectives

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

1) Authentication:
2) Non-repudiation:
3) Privacy:

B. Architecture

The hierarchical architecture of the scheme, shown in Figure. 6, consists of three levels: The Certification Authority (CA) which is the root of the system, is located at level 1; the Road Side Units (RSUs) and the On-Board Units (OBUs) are located at level 2 and level 3, respectively. In this architecture, entity authentication for RSUs and OBUs is achieved using certificate-based authentication [10].

Basic Operation of the Scheme: The basic operation of the scheme (Figure.7) is as follows.

- The Certification Authorities (CAs) is responsible for generating initial certificates for the RSUs and OBUs in its domain. It also generates a public/private key pair for itself, for signing the outgoing messages and verifying the incoming messages. Moreover, it generates two secret certificate-signing keys; The CAs administering different domains are connected directly to the Repository. Each CA is physically secure and cannot be compromised;
- A CA uses the first certificate-signing keys, generated by itself, 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;
- Road-Side Units (RSUs), which are fixed units distributed in the network. RSUs in one domain are connected via Ethernet to the CA responsible for that domain. 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 [4];

• At first time registration, a OBU Object (O-O), a software module, is created on CA which stores both static (long term identity etc.) and dynamic (short term identity, credentials etc.) information about a vehicle (OBU), and then after runs on CA on behalf of vehicle, and refreshed periodically[17].

• 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.

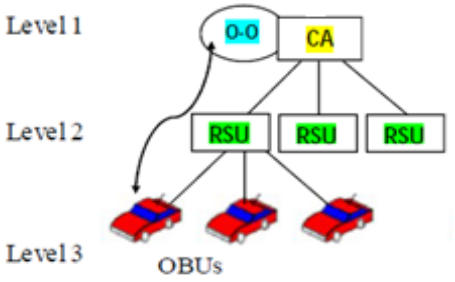


Figure. 6: The hierarchical structure of Proposed Scheme

• 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 certificate of any OBU or RSU regardless of the issuer of that certificate. The certificate generation derived from the signature schemes proposed in [14], [15].

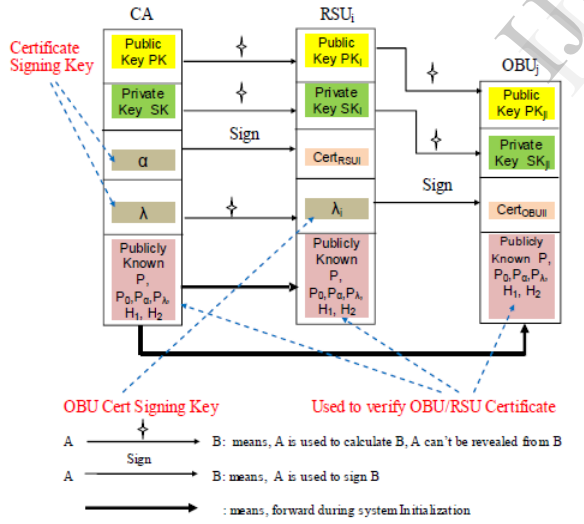


Figure. 7: shows the relations of different keys among the network entities.

THE PROPOSED SCHEME

In this section, the proposed scheme is presented in detail.

A. System Initialization

The initialization stage is performed by the CA to generate the security keys necessary for the operation of the scheme, and to upload the necessary security keys and the required security materials, e.g., keys, certificates, etc., in the tamper-resistant HSM of each OBU and RSU. It should be noted that the initialization stage is performed during the registration of RSUs and OBUs with a CA where in a OBU Object (O-O), a software module, is created on CA. In other words, the initialization stage is performed before triggering any of the VANET services or applications.

B. OBUs Certificates Update

The scheme enables an OBU to update its certificate from an RSU. Thus, the scalability of the 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 scheme depends on the RSUs to update the certificates of the OBUs, the density of RSUs is crucial to the operation of the scheme. 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 [16].

C. Certificate Revocation

To prevent compromised entities from accessing the network the Certificate Revocation List (CRL) method employed in the WAVE standard is adopted [4]. 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.

D. 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.

3.5. ALGORITHM

A) System Initialization.(By CA)

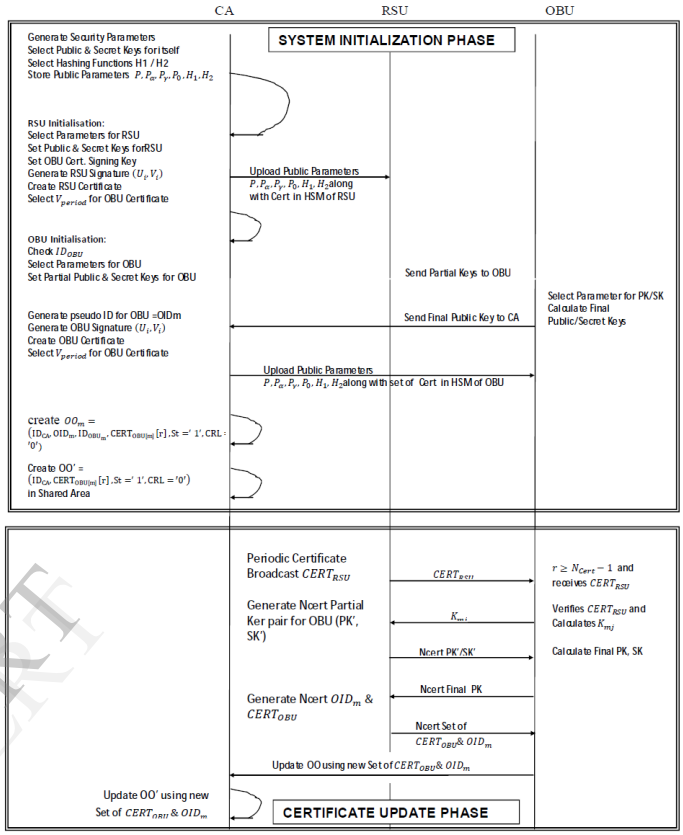
1. Generate security material: (Require : ID_{CA} - Long-Term Identity of CA, N; Number of Certificates initially loaded into HSM of OBU)
   Select random Parameters;
   Set Public and Private keys for CA;
   Set Master Signing Keys.
   Select a Hash Function $H_1 : \{0,1\}^* \rightarrow G_1^*$; $\{SHA-1\}$

Select a Hash Function $H_2 : \{0,1\}^* \rightarrow Z_q^*$; $\{SHA-1\}$
Store Security Material in CA.

2. RSU Initialization: (Require Public and Private keys of CA)
for all $RSUs$ in the Domain of CA do
Select a random Parameters;
Set a pseudo identity;
Set Public and Private keys for CA;
Set OBU Certificate Signing Key;
Generate Signature (Ui, Vi)
Generate Certificate;
Select validity period of any OBU Certificate.
Upload Cert., Vperiod & other Security material in HSM.
end for

3. OBU Initialization:
(Require Certificate and Public/Private keys of RSU;
ID_{OBU} : Original ID of OBU_m loaded at Manufacture Time; known to CA)
for all $OBUs$ in the Domain of CA do
Check the validity of ID_{OBU}
if ID_{OBU} is invalid then
Return $\emptyset$
else
for r← 1 to N , CA do
Select random parameters
Set Partial Secret Key and Partial Public Key;
end for
return set of Partial Secret and Public Keys to $OBUm$
for r← 1 to N , $OBU[m]$ do
Select random parameters
Set Final Secret Key and Final Public Key;
end for
return set of Final Public Keys to CA
for r← 1 to N , CA do
Select a validity period and a pseudo Id for OBU
Generate Signature of OBU (U',V')
Generate Certificate of OBU
end for
Upload Cert.,Vperiod &other Security material in HSM.
CA creates OBU Object OO containing
ID of CA;
ID of OBU;
Pseudo ID of OBU;
Certificate Set;
Status and CRL flags with default values '1' and '0'.
end if
end for

B) OBU Certificate Update:
Mutual Key Agreement and Calculate
$N_{CERT} = T_{RSU} / Vperiod$
T_{RSU} = Avg Dist between RSU / Avg. Speed of OBU
When (r>= N_{CERT} -1) &&
Receives Periodic Broadcast $CERT_{RSUj}$ from RSUj.
OBUm verifies $CERT_{RSUj}$ and
If valid
Calculates Kmj using its Skmi & RSUj's Pkj
Sends N_{CERT} and $CERT_{OBUmi}$ to RSUj.
RSUj verifies $CERT_{OBUmi}$
Calculates Kmj using its Skj & OBUm's Pkmi
RSUj generates Ncert partial key pairs (Skm' and Pkm')
Encrypts (Sk',Pk') using Kmj and sends to OBUm
OBUm decrypts (Sk',Pk') using Kmj
Calculates Ncert final key pairs (Skm & corresp Pkm).
Encrypts Pkm with Kmj and sends to RSUj
RSUj generates Pseudo Identities using Pkm, and
Generates a set of Ncert Certificates;
Delivers encry set of certificates using Kmj to OBUm
OBUm decryptes set of cert using Kmj and verifies & accepts if valid.
Update OO in CA
OBUm send its Set of new certificates to CA.
CA Refreshes OO'



Algorithm for Message Signing & Verifying.

An OBUm with $CERT_{OBUmi}$ can generate a valid Signature (Um" , Vm") for a given Message M, as:

Select a random number $c_m \in Z_q^*$;
Calculate $U_m'' = c_m P$
$R_m = H_2(M||P_{kmi}||OID_m[r]||U''_m||t_{stamp})$
$V_m'' = S_{kmi} + c_{m R_m}$

Any Entity can verify the Signature as:

Verify the sender of the message M is valid user and check the time stamp t_{stamp} .
Calculate $R_m = H_2(M||P_{kmi}||OID_m[r]||U''_m||t_{stamp})$;
Accept if ,
$\hat{e}(P, V_m'') = \hat{e}(P, S_{kmi} + c_m R_m)$

Similarly any CA/RSU can sign any Message using same process.

Algorithm for Certificate Revocation.

For RSU:
CRL (Certificate Revocation List) method of WAVE standard is used.
For OBU:
Automatic Revoke when validity period is over
Signature is not verified.
Update O-O in CA (Set CRL Flag in O-O).

IV. SECURITY ANALYSIS

In this section, we evaluate the proposed DCS scheme

according to the security objectives presented earlier.

1) *Authentication*: It can be seen that finding the secret keys s, α, γ from the corresponding public keys $P_0 \circ$, P_α , P_γ are instances of the ECDLP problem. For example, to find s, we have the following ECDLP problem: given P and $P_0 \circ = sP$, find s. In DCS, the authentication of RSUs and OBUs is achieved using digital certificates. For example, the signature of any CA on the certificate of any $RSU_{[i]}$ is (U_i, V_i), where $U_i = a_i P$, $T_i = H_2(P_{ki} || RID_i || U_i || Q) \in Z_q^*$, and $V_i = \alpha + a_i T_i$. It can be seen that to forge the certificate of any $RSU_{[i]}$, an attacker should know either α or $a_i T_i$. Since Q is publicly known, finding α reduces to finding only α which is ECDLP problem as indicated above. Also, since T_i can be easily obtained from the certificate of $RSU_{[i]}$, finding $a_i T_i$ reduces to finding only $a_i T_i$, which can be formulated as a CDH problem, i.e., given $U_i = a_i P$. The hardness of the CDH problem is closely related to solving the Discrete Logarithm (DL) problem. Similar analogy applies to the OBUs certificates. Since ECDLP and CDH are hard computational problems, 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. In this scheme, each OBU/RSU authenticates the received messages before being involved in any key exchange or responding to the received message. Since authentication is done first before taking any action, the clogging attacks is hard to launch in the proposed scheme.

2) *Non-repudiation*: Non-repudiation is achieved by requiring all the messages exchanged in the network to be digitally signed by its issuer. Similar to the above discussion of the security of RSU's certificates, to forge the signature of OBU_m on M , the attacker has to find either S_{kmi} , which is ECDLP problem, or c_{mR_m}, 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 proposed Scheme, privacy is preserved by the following techniques:

Anonymous authentication: Anonymous authentication is employed 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.

Although the scheme 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 scheme can be efficiently integrated with Random Encryption Periods (REPs) in which, using group communications, an OBU surrounds itself with an encrypted communication zone to violate the conditions of being tracked by an observer.

V. PERFORMANCE EVALUATION

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

A. OBU Certificate Update Delay

Let T_{CERT} denote the time from the moment an OBU requests N_{CERT} new certificates from an RSU to the moment it receives the required certificates. 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. Which are for an MNT curve with embedding degree $k = 6$ to be equal to 4.5 $msec$, and 0.6 $msec$, respectively. It should be noted that the cryptography delay (T_{crypt}) is part of the certificate update delay (T_{crypt}) in any of the scheme under consideration.

B. Successful Certification Ratio

When an OBU_m requests N_{cert} certificates from an RSU_i, RSU_i 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_i, 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 $N_{C_{max}} = {}^{R}/_{\bar{S}\,\overline{T_{cert}}}$ where $N_{C_{max}}$ is the maximum number of certificates an RSU can generate within its coverage range $R, \bar{S}$ is the average speed of the OBUs within R, and $\overline{T_{cert}}$ is the average certificate update delay of the scheme under consideration.

Successful Certification Ratio (SCR) is the metric usually used to evaluate the efficiency of authentication algorithms. 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,

$SCR = 1\ if\ NC_s \leq N_{C_{max}}\ and\ SCR = NC_s/NC_t\ if\ NC_s > N_{C_{max}}$

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 $S = 60\,Km/h$.

C. Communication Overhead

We consider the Tate pairing implementation on an MNT curve with embedding degree 6, where G_1 is represented by 161 bits. Accordingly, each point on this MNT curve is represented by $21\,bytes$. Following tables give each parameter and the corresponding size in bytes for an RSU and OBU certificate. The last column in each table gives the total size of the certificate under consideration.

RSU Certificate Size :

Parameter	P_{ki}	U_i	V_i	PID_i	Q	$CERT_{RSU_i}$
Size in Bytes	21	21	21	8	21	92

OBU Certificate Size :

Parameter	P_{ki}	U_i	V_i	$Vperiod$	PID_i	$CERT_{RSU_i}$	$CERT_{OBU_m}$
Size in Bytes	21	21	21	4	8	92	167

According to WAVE, the maximum payload data size in a signed message is $65.6\,Kbytes$. Consequently, the ratio of the communication overhead incurred by the proposed scheme to the payload data size is 0.3%, which means that this scheme is feasible with respect to the incurred communication overhead.

E. OBU Message Signing 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 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. Additional Memory Requirements

In the proposed scheme, the memory requirements for OO' and periodic update of OO' can be an overhead, but the same can be trade–off with the explicit re-registration of OBU with the foreign CA where the whole process of regeneration of security material for the OBU and corresponding RSU materials which goes to be very high

VI. CONCLUSION & FUTURE WORK

In this paper, a robust distributed certificate scheme for vehicular communications proposed, which offers an efficient distributed algorithm for any OBUs to update or revoke its certificate from the available RSUs in a timely manner. In addition, an OBU Object (O-O) is introduced to tackle with short-lived connections. Therefore, the proposed scheme can significantly reduce the complexity of certificate management, and achieve robustness and scalability, especially when it is deployed in heterogeneous vehicular networks.

As future work, the proposed scheme is to be implemented using ns-3 or OMNet++ simulator and compare the performance with ECPP and RAISE schemes and the proposed scheme is to be further extended for cross-domain authentication.

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

[3] Panagiotis Papadimitratos, Levente Buttyan and Tamás Holczer, Elmar Schoch, Julien Freudiger and Maxim Raya, Zhendong Ma and Frank Kargl, Antonio Kung, Jean-Pierre Hubaux, “Secure Vehicular Communication Systems: Design and Architecture” IEEE Communications Magazine • November 2008

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

[5] “5.9 GHz DSRC.” [Online]. Available: http://grouper.ieee.org/groups/scc32/dsrc/index.html.

[6] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A secure and privacy-preserving protocol for vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 56, pp. 3442–3456, 2007.

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

[8] 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.

[9] 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.

[10] 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.

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

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

[13] 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.
[14] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," *Proc. Advances in Cryptology - ASIACRYPT 2003*, pp. 452–473, 2003.
[15] 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.
[16] Albert Wasef, Yixin Jiang, Xuemin (Sherman) Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks**",** Wasef, IEEE Transactions on Vehicular Technology, vol. 59, no. 2, 2010, pp. 533.
[17] V. Casola, J. Luna, A. Mazzeo, M. Medina, M. Rak, and J. Serna, "An Interoperability System for Authentication and Authorization in VANETs." In International Journal of Autonomous and Adaptive Communications Systems , vol. 3, no. 2, 2010, pp. 115 – 135.