Computer Standards & Interfaces xxx (2013) xxx–xxx

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks

Carlos Gañán *, Jose L. Muñoz, Oscar Esparza, Jorge Mata-Díaz, Juanjo Alins

Universitat Politècnica de Catalunya, Departament Enginyeria Telemàtica, 1–3 Jordi Girona, C3 08034 Barcelona, Spain

ARTICLE INFO

Article history:
Received 24 November 2012
Received in revised form 5 August 2013
Accepted 6 August 2013
Available online xxxx

Keywords:
Revocation
Privacy
One way accumulators
VANET

ABSTRACT

One of the critical security issues of Vehicular Ad Hoc Networks (VANETs) is the revocation of misbehaving vehicles. While essential, revocation checking can leak potentially sensitive information. Road Side Units (RSUs) receiving the certificate status queries could infer the identity of the vehicles posing the query. An important loss of privacy results from the RSUs ability to tie the checking vehicle with the query's target. We propose a Privacy Preserving Revocation mechanism (PPREM) based on a universal one-way accumulator. PPREM provides explicit, concise, authenticated and unforgeable information about the revocation status of each certificate while preserving the users' privacy.

1. Introduction

Vehicular ad-hoc networks (VANETs) have recently attracted extensive attentions as a promising technology for revolutionizing the transportation systems. VANETs consist of entities including On-Board Units (OBUs) and infrastructure Road-Side Units (RSUs). Mobile nodes are capable of communicating with each other (i.e. Vehicle to Vehicle Communication — V2V communication) and with the RSUs (i.e. Vehicle to Infrastructure Communication — V2I communication). Multi-hop communication facilitates information exchange among network nodes that are not in direct communication range [1,2], by means of short range wireless technology based on IEEE 802.11p.

Obviously, any malicious behaviors, such as injecting beacons with false information, modifying and replaying the previously disseminated messages, could be fatal to the other users. Thus, identifying the message issuer is mandatory to reduce the risk of such attacks. According to the IEEE 1609.2 standard [3], vehicular networks will rely on the public key infrastructure (PKI). In PKI, a certification authority issues an authentic digital certificate for each node in the network. Due to misbehavior, intentional or otherwise, certificates need to be revoked in order to limit the risk that potential misuse poses to the rest of the network. The IEEE 1609.2 standard [3] states that VANETs will depend on certificate revocation lists (CRLs) to achieve revocation. CRLs are black lists that enumerate revoked certificates along with the date of revocation and, optionally, the reasons for revocation.

As VANETs can have a great amount of nodes (i.e. vehicles), CRLs will be large. Moreover, each vehicle in the network will own many temporary certificates (also called pseudonyms) to protect the users' privacy. Consequently, these lists will require hundreds of Megabytes [4–6]. However, distributing and updating CRLs raise a challenge. If there are no more communication media than the own VANET, no trusted-third parties (like the corresponding CA) can be assumed to be permanently available. Thus, online certificate status protocol (OCSP) [7] or, in general, any online solution is not suitable for this context. Several CRLs distribution protocols have been proposed for this purpose. For instance, to distribute these lists efficiently, authors in [8] proposed revocation using compressed CRLs. They divided the CRL into several self-verifiable parts and strongly reduced its size by using Bloom filters. Authors in [5] also propose the use of Bloom filters to store the revoked certificates for increasing the search speed in the CRL. On the other hand, authors in [9] proposed to use regional CAs and short lived certificates to decrease the number of entries in the CRL. However, these works overlooked the authentication delay resulting from checking the CRL for each received certificate. Regarding this issue, in the literature there are some mechanisms for distributing certificate status information (CSI) in environments prone to disruption [10–13]. They mainly use caching strategies combined with hashing techniques to enhance the availability of the revocation service. Nevertheless, none of these approaches takes into account the loss of privacy due to the CSI checking process.

On the one hand, traditional CRLs satisfy both privacy of the target and authenticity of the membership. The CRL is free from the privacy issue because sending a list does not reveal information about the target. However, CRLs are bandwidth-inefficient due to their size, which grows linearly to the number of revoked users ($O(n)$). Other explicit revocation methods just exchange information about the target

* Corresponding author.
E-mail addresses: carlos.ganan@entel.upc.edu (C. Gañán), jose.munoz@entel.upc.edu (J.L. Muñoz), oesparza@entel.upc.edu (O. Esparza), jmata@entel.upc.edu (J. Mata-Díaz), juanjo@entel.upc.edu (J. Alins).

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.08.002

certificates. This makes them much more bandwidth-efficient than CRLs but then, they have privacy issues [14]. In particular, a non-trusted third party (e.g. a RSU) could gain knowledge about who is talking to whom, by just analyzing the CSI requests. In other words, a RSU could determine the identity of the party posing the query, as well as the target of the query. This is significant, because the revocation status check typically serves as a prelude to actual communication between the two parties. Hence, RSUs could acquire significant statistics such as who sends a message to whom, how often, etc. Recently, there appeared to be some works that intend to provide privacy during the revocation process [15,16]. However, they mainly use CRLs to convey the revocation information. Though CRLs provide a certain degree of privacy, they result bandwidth inefficient.

To provide privacy and, at the same time, a bandwidth-efficient revocation mechanism we propose PPREM, a Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks. PPREM is based on a universal one-way accumulator (OWA) to check the validity of the certificates. The CA accumulates all the revocation information in one single value that is transmitted to all the entities in the network. Then, any vehicle can convince any other entity that its certificate is still valid by providing the witness for the unique value contained in its certificate. To obtain and update this witness, vehicles contact RSUs without leaking personal information. The only data vehicles need to check the validity of any certificate are the accumulated value and the corresponding witness. This data can be downloaded from any mobile repository which is in charge of contacting the RSU in range and downloading an updated copy of the OWA and the auxiliary information necessary to update the witness. Thus, PPREM provides explicit, concise, authenticated and unforgeable information about the revocation status of each certificate while preserving the users' privacy. By conducting detailed performance evaluation, PPREM is demonstrated to be reliable, efficient, and scalable.

The rest of this article is organized as follows. In Section 2 we summarize the related work regarding CSI management. Section 3 describes the Privacy Preserving REvocation Mechanism. Next in Section 4 we perform a security analysis of the proposed mechanism. In Section 5 we evaluate and compare our proposal to the traditional method of periodical issuance. Finally, we conclude in Section 6.

2. Background

In this section, first we start describing existing revocation proposals for VANET. Then, we give a brief overview of the basics of one-way accumulators [17], which is one of the foundations of the proposed certificate validation mechanism.

2.1. Privacy aware revocation approaches for VANET

The IEEE 1609.2 standard [3] proposes an architecture based on the existence of a Trusted Third Party (TTP), which manages the revocation service. In this architecture each vehicle possesses several short-lived certificates (used as pseudonyms), to ensure users' privacy. However, short-lived certificates are not enough as compromised or faulty vehicles could still endanger other vehicles until the end of their certificate lifetimes. Thus, the IEEE 1609.2 promotes the use of CRLs to manage revocation while assuming pervasive roadside architecture. CRLs provide privacy, as all users ask for the same file and they check the certificate status locally.

Raya et al. [18] propose the use of a tamper-proof device (TPD) to store the certificates. They investigated the privacy issue by proposing a pseudonym based approach using anonymous public keys and the PKI, where the public key certificate is needed, giving rise to extra communication and storage overhead. Thus, when a vehicle is compromised/misbehaving, it can be removed from the network by just revoking the TPD. To ensure that messages from this OBU are not considered valid once the certificates have been revoked, revocation information must also be distributed via CRLs. The authors also proposed to use frequently updated anonymous public keys to fulfill users' requirement on identity and location privacy. To reduce the bandwidth consumed by the transmission of CRLs, these authors proposed to compress the CRLs by using Bloom filters. However, this method gives rise to false positives which degrades the reliability of the revocation service.

Other proposals are based on identity-based (ID-based) signatures and group signatures to provide the revocation service. Group signature-based schemes are proposed in [19,20], where signer privacy is conditional on the group manager. As a result, all these schemes have the problem of identity escrow, as a group manager who possesses the group master key can arbitrarily reveal the identity of any group member. In addition, due to the limitation of group formation in VANETs (e.g., too few cars in the vicinity to establish the group), the group-based schemes [19–21] may not be applied appropriately. The election of group leader will sometimes encounter difficulties since a trusted entity cannot be found among peer vehicles. In [19], group signatures for OBUs and identity-based signatures for RSUs have been proposed in order to maintain security and privacy. A message received from an OBU can be verified by its signature; so that receiver can determine whether that OBU is legitimate. However, coverage of multi-hop routing is lacking in that proposal.

On the other hand, the distributed certificate service is a promising approach to decrease revocation cost [22,23]. In these proposals vehicles can update their anonymous certificates set from the certificate issuer by vehicle-to-RSU communication on the road. As each certificate has a short-time period and is used in a specifically geographic region, the CRL size broadcast in a region can decrease. However, the CRL size still depends on how many anonymous certificates are held by the revoked vehicles. In [22], authors proposed an Efficient Conditional Privacy Preservation Protocol (ECPP) which aims overcoming the limitation of pre-storing a large number of anonymous certificates. Under the most ideal condition that one RSU is deployed for 600 m along each road, a vehicle takes only one certificate with a quiet short validity period so that it becomes unnecessary for the vehicles to have a copy of the CRL while preserving conditional privacy. Since a vehicle should change anonymous certificate quite often to avert tracing of messages, it should frequently interact with RSUs. This short-lived anonymous certificate needs to be sent and forwarded to verifiers for validating messages from anonymous originator. Wasef et al. [23] extend RSU-aided distribute certificate service into a hierarchical authority architecture and propose an efficient Distributed-Certificate-Service (DCS) scheme that supports batch signature verification. However, the performance of the aforementioned schemes [22,23] largely depends on the RSU density. The fewer the number of RSUs, the larger the revocation cost and the certificate-updating cost.

There are other proposals that use caching strategies to improve the revocation service. Authors in [10] proposed ADOPT (Ad-hoc Distributed OCSP for Trust) that provides a revocation service based on the Online Status Checking Protocol (OCSP) [24] in a decentralized manner. ADOPT uses cached OCSP responses that are distributed and stored on intermediate nodes in the VANET. Authors in [12] describe a COllaborative certificate stAtus CHecking mechanism (COACH) based on the use of Merkle hash trees [25] to store the revocation information. In COACH, CAs issue extended-CRLs in which some extra information is embedded allowing vehicles to respond to certificate status queries.

Regarding ID-based protocols, authors in [26] proposed an ID-based security framework for VANETs to provide authentication, nonrepudiation, and pseudonymity. However, their framework is limited by the strong dependence on the infrastructure for short-lived pseudonym generation, which renders the signaling overhead overwhelming. The proposed nonrepudiation scheme enables a single authority to retrieve the identity which may raise the concern on potential abuse. Authors in [27] adopted an identity-based (ID-based) ring signature scheme to achieve signer ambiguity and hence fulfill the privacy requirement in

VANET applications. The main drawback of the ring signature scheme in the VANET context, is the unconditional privacy, resulting in the traceability requirement unattainable.

2.2. Cryptographic accumulators

Accumulator schemes were first proposed by Benaloh and de Mare [17], and were defined as a family of one-way hash functions with an additional special property, called *quasicommutativeness*. Intuitively, an accumulator consists in hashing a large set of inputs in a single short value, i.e. the *accumulator*, and provides evidence (i.e., a witness) that a given value is indeed contained in the accumulator.

Since this first proposal, there have been proposals for a wide range of accumulator schemes [28–32]. They can be classified regarding their properties as [33,34]:

- *Static/Dynamic*: Dynamic accumulators allow to add and remove elements to the set, while static accumulators only allow adding elements.
- *Weak/Strong*: Weak accumulators depend on a trusted third party to manage the accumulator and strong do not.
- *Universal*: Universal accumulators allow to efficiently compute a non-membership witness of any value that has not been accumulated. Non universal accumulators only allow obtaining witness of membership.

2.3. Bilinear maps

PPREM is mainly based on the use of bilinear pairings on elliptic curves [35] Consider two groups and $\mathbb{G}_2$ of prime order q. For clarity, we denote $\mathbb{G}_1$ using additive notation and $\mathbb{G}_2$ using multiplicative notation, even though the group operations in $\mathbb{G}_1$ and $\mathbb{G}_2$ may well be very different from the well-known arithmetic addition and multiplication. We consider P and Q two generators of $\mathbb{G}_1$. Then, we consider the mapping $\widehat{e}$ as follows: $\widehat{e}:\mathbb{G}_1\times\mathbb{G}_1\rightarrow\mathbb{G}_2$. Useful bilinear maps have three properties:

1. Bilinear: $\widehat{e}(aP,bQ)=\widehat{e}(P,Q)^{ab},\ \ \forall P,Q\in\mathbb{G}_1$ and $a,b\in_R Z_q$,
2. Non-degeneracy: $\widehat{e}(aP,bQ)\neq 1_{\mathbb{G}_2}$,
3. Computability: $\widehat{e}$ is efficiently computable.

We can find $\mathbb{G}_1$ and $\mathbb{G}_2$ where these properties hold: the Weil [36] and Tate [37] pairings prove the existence of such constructions.

3. PPREM: Privacy Preserving REvocation Mechanism

In this section, first we explain the security architecture necessary to support PPREM and the scheme outline. Then, we present PPREM which mainly consists of four phases: system initialization, mobile repositories creation, certificate status checking and updating the revocation information. The notations used throughout this paper are given in Table 1.

Table 1
Notation used in PPREM's algorithms.

Symbol	Definition
CA	An arbitrary certification authority
RSU	An arbitrary Road Side Unit
sk_{CA}	Secret key for CA
pk_{CA}	Public key for CA
R	Set of revoked certificates
r_i	ID of an arbitrary revoked certificate
s	Trapdoor of the accumulator
$v(s)$	Auxiliary information
t_i	Time stamp
Z	Signed accumulated value
OBU_k	An arbitrary On-Board Unit
TPD_k	An tamper-proof device of an arbitrary OBU
$pseud_k$	An arbitrary pseudonym
$cert_i^k$	An arbitrary certificate of an arbitrary OBU
ID_i^k	An arbitrary identifier of an arbitrary OBU
PK_i^k	An arbitrary public key of an arbitrary OBU

3.1. Security architecture

The security architecture is an adaptation of a mesh PKI system to a vehicular scenario constructed of peer-to-peer CA relationships. CAs cross-certify each other preventing the compromise of a single CA from bringing down the entire PKI. Vehicles need to build a trusted path when changing to a new domain. Building a path is nothing but traversing a graph and PPREM could benefit of any of the current methods to build a trusted validation path such as [38–40]).

This architecture consists of 3 different types of entities (see Fig. 1):

1. *Certification Authorities*: CAs are responsible for holding and managing the credentials and identities of all the vehicles which are registered under its hood. CAs are responsible for generating the set of pseudonyms that are stored in each OBU. They are also responsible for managing the revocation information and making it accessible to the rest of the entities. By definition of TTP, the CA should be considered fully trusted by all the network entities, so it should be assumed that it cannot be compromised by any attacker. In fact, in our proposal CAs are the only trusted entities within the network.
2. *Road-Side Units*: RSUs are fixed entities that are fully controlled by the CA. They can access the CA anytime because they are located in the infrastructure-side, which does not suffer from disconnections. If the CA considers that an RSU has been compromised, the CA can revoke it. RSUs will act as repositories of the CSI.
3. *Vehicles*: They are the clients of the network. They have their cryptographic material stored in a tamper-proof device (TPD).

3.2. Scheme outline

PPREM uses a dynamic weak universal accumulator from bilinear pairings to provide a bandwidth efficient proof about the status of a given certificate. This accumulator scheme allows the CA to accumulate the set of revoked pseudonyms into a single value so that OBUs can compute witnesses that demonstrate that a pseudonym has not been accumulated, i.e., a proof that a certificate is still valid. CAs will be in charge of managing the accumulated value and trapdoor. By using the accumulated value, any network entity will be able to check the validity of a given certificate once they obtain the corresponding non-membership witness. To prevent RSUs from gaining knowledge about the statistics of the PKI (i.e., who sends a message to whom, how often, etc.), PPREM uses a clustering approach allowing vehicles to act as mobile repositories (MR). Vehicles contact the MR when they need to update their witnesses and/or the accumulated value. Hence, vehicles' privacy is preserved as they do not disclose any information when updating the revocation information. Once the revocation information is obtained, OBUs can update locally their non-membership witnesses.

Basically, PPREM consists in 4 different phases:

1. *Initialization*: The CA creates the certificates corresponding to the vehicles' pseudonyms. It also creates the signed accumulated value and some auxiliary information.[1] All these data are communicated to the RSUs via a secure wireline.
2. *Mobile repositories creation*: Depending on an affinity metric, some vehicles are selected to act as mobile repositories. To act as repositories, vehicles just download the most updated revocation information from any RSU (or from any other repository in range) and provide to other vehicles the signed accumulated value and the data necessary to calculate their witnesses. Thus, PPREM increases the persistence of

[1] The auxiliary information will allow repositories to compute the information necessary for the OBUs to update their nonmembership witnesses.

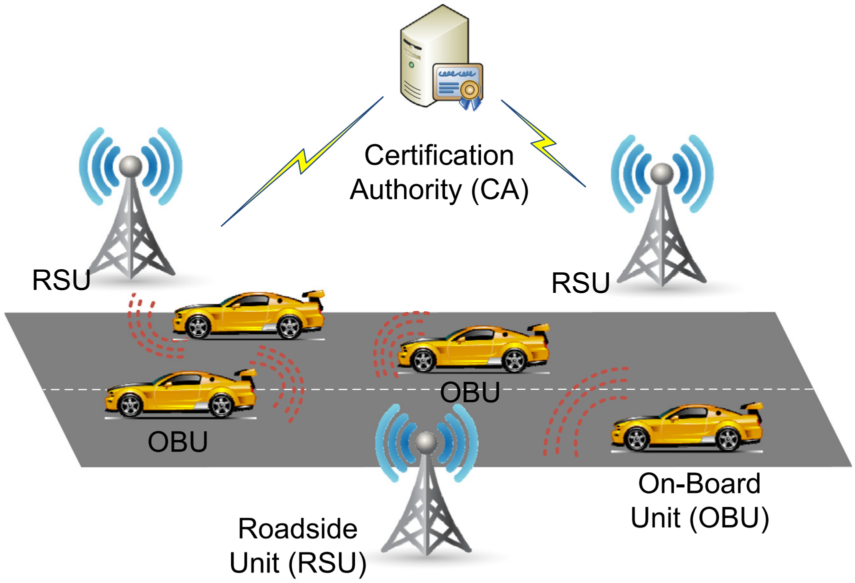

Fig. 1. System architecture.

the revocation information and avoids the dependence of the revocation service on the RSU availability.

3. *Certificate status testing*: Once a vehicle has obtained the signed accumulated value, it can check the validity of any certificate by performing the nonmembership test. To pass this test, they have to obtain the corresponding nonmembership witness from the other OBU and check that its value has not been accumulated in the signed accumulated value.
4. *Revocation data updating*: Each time a new set of new certificates is revoked, the CA has to issue a new accumulated value and the corresponding auxiliary information. These data will be transmitted to RSUs and mobile repositories, which in turn will transmit the new accumulated value and the information required to update their witnesses to the vehicles.

3.3. System initialization

During the initialization, the CA creates all the necessary cryptographic material to provide the authentication and revocation services. In particular it initializes PPREM by calculating the accumulated value and the auxiliary information, and signing both. These data can be used by non-TTP (e.g. RSUs and vehicles inside the VANET) to act as repositories and allow them updating the vehicles' witnesses. All the tasks of this system initialization are performed in the CA locally, so the computational delay is not suffered by the other network entities.

PPREM needs a *dynamic* accumulator as it should allow adding and removing revoked certificates from the accumulated value. Moreover, PPREM's accumulator must be *universal*, i.e., it must not only allow efficient generation of membership witness, but also non-membership proofs, i.e., proofs that a certificate is not revoked. As the accumulator is managed by the CA it does not need to be strong. There exist several accumulator schemes [17,28,30,41,31,42,32,43]. Accumulators proposed in [17,28] are not dynamic and, therefore, not suitable as a revocation mechanism. Proposals in [41,30,42,43] are not universal. Using non-universal accumulators as a revocation mechanism will lead to accumulate all valid certificates. In a VANET environment the number of valid certificates could exceed the billion (recall that each vehicle possesses a large number of certificates which act as pseudonyms) which makes it unfeasible to use this type of accumulators. Authors in [32] propose a strong accumulator which is also dynamic and universal. However, we do not require our accumulator to be strong as our architecture assumes the existence of a CA who issues the cryptographic material. Thus, we need to modify one of the non-universal accumulators. Based on the performance analysis in [44], we chose Nguyen's OWA as it achieves the best trade-off between initialization duration and verifying process. We modified Nguyen's OWA to allow the efficient generation of non-membership proofs (see Algorithm 5). The security of this new non-membership verification test is proved using the *q*-strong Diffie–Hellman assumption on general groups. Similar to the non-membership extension of the RSA accumulator (see, e.g., [17,28,30]) that was proposed in [31] this non-membership extension makes the OWA usable in real-life revocation mechanisms.

The CA initializes the system by executing Algorithm 1. Note that we assume that all vehicles are equipped with a tamper-proof device (TPD). In Algorithm 1, element *g* has to be chosen so that it can generate $\mathbb{G}_2$. Additionally, group $\mathbb{G}_2$ is chosen such that it supports a (non-degenerate) bilinear pairing to a target cyclic group $\mathbb{G}_T$ of prime order *p*. That is to say, if $\mathbb{G}_2$ is generated by element *g*, then there exists a bilinear, non-trivial, map $\hat{e}:\mathbb{G}_2\times\mathbb{G}_2\rightarrow\mathbb{G}_T$ from pairs of elements in $\mathbb{G}_2$ to elements of target

```
Algorithm 1: System initialization
Select two generators, $P \in \mathbb{G}_1$ and $g \in \mathbb{G}_2$ of prime order $p$
Select a master secret key $sk_{CA} \in \mathbb{Z}_p^*$
Set the corresponding public key $pk_{CA} = sk_{CA} \cdot P$
Given the set of $n$ elements $\mathcal{R} = \{r_1, r_2, \ldots, r_n\}$ of revoked certificates, create the CRL including all the elements
Select $s \in \mathbb{Z}_p^*$ (i.e. trapdoor of the accumulator)
Compute the polynomial $v(s) = \prod_{i=1}^{n}(r_i + s)$
Accumulate all the element of $\mathcal{R}$ in $Acc$ as: $Acc(\mathcal{R}) = g^{v(s)}$
Sign $Acc(\mathcal{R})$ and $v(s)$ and append a timestamp: $Z = (Acc(\mathcal{R})||v(s)||t_i)_{sig_{CA}}$
forall the $OBU_k$, $CA$ do
    Generate a set of anonymous certificates $pseud_k = \{cert_i^k(ID_i^k, PK_i^k), sig_{CA}(ID_i^k||PK_i^k))|1 \leq i \leq \alpha\}$
    Upload $pseud_k$ in $TPD_k$ of $OBU_k$
Convey $P, g, pk_{CA}$ and $(Acc(\mathcal{R})||v(s)||t_i)_{sig_{CA}}$ to the RSUs, and publicize them to all the OBUs
```

group $\mathbb{G}_2$, such that for any two integers a and b it holds that $\widehat{e}(g^a, g^b) = \widehat{e}(g, g)^{ab}$, and where, additionally, element $\widehat{e}(g, g) \in \mathbb{G}_T$ generates $\mathbb{G}_T$.

It should be noted that in step (1), PK_i denotes the i^{th} public key for OBU_k , where the corresponding secret key is SK_i; ID_i denotes the ith pseudonym for OBU_k, where the CA is the only entity that can relate ID_i to the real identity of OBU_k; and α is the number of pseudonyms loaded in each OBU.

3.4. Mobile repositories creation

After the initialization phase, vehicles possess a set of pseudonyms to protect their anonymity. A vehicle that needs to check the validity of a certificate must contact any RSU in range. However, using RSUs to obtain the revocation information presents two main drawbacks: (i) RSUs could collect statistics and acquire some knowledge about the communication parties, (ii) RSUs could become a bottleneck as they will be serving the revocation information to all the vehicles in their range. For instance, if a vehicle wants to communicate with another vehicle, both vehicles will need to check the revocation data (i.e. the accumulated value). If they do not have a valid OWA, they will contact a RSU in range (probably the same RSU) and ask for a valid OWA. At this point, the RSU will receive two requests and could infer that both users are about to establish a communication. Obviously, as the population grows it becomes more difficult to infer who is talking to whom. However, there exist several traffic-correlation techniques that could be used by the RSU to gain this knowledge [45,46]. Using a clustering algorithm and allowing the creation of mobile repositories, PPREM palliates the effectiveness of these traffic-correlation techniques.

To solve these issues, PPREM allows vehicles to act as mobile repositories (MR). MRs will be capable to provide revocation information and answer to witness update queries. Thus, both the users' privacy and the revocation service availability are enhanced. To choose which entities will act as MRs, we propose an algorithm based on a technique called Affinity Propagation (AP) [47]. AP allows identifying the most suitable entities to act as MRs head based on three different metrics: similarity, availability and responsibility. The priority of a vehicle to become a MR is determined by these metrics which are computed based on the mobility information of its neighborhood and the revocation information they possess.

We define a similarity function for the AP algorithm with the goal of maximizing the availability of the mobile repository, and tailored to the VANET environment. Our similarity function aims to select as MRs those entities in the VANET that have lower relative movement respect to their neighbors. Thus we define the similarity function s_{ij} as the addition of the negative Euclidean distance between node positions now to the negative Euclidean distance between vehicle positions in the future (after τ_f seconds). This is a simple way to consider both vehicle position and vehicle mobility when choosing the MRs.

$$s_{ij} = -\left(\left|\mathrm{x}_i^{ini} - \mathrm{x}_j^{ini}\right| + \left|\mathrm{x}_i^{fut} - \mathrm{x}_j^{fut}\right|\right), \tag{1}$$

with

$$\mathrm{x}_i^{ini} = \begin{bmatrix} x_i \\ y_i \end{bmatrix} \quad \mathrm{x}_i^{fin} = \begin{bmatrix} x_i + v_{xi}\tau_f \\ y_i + v_{yi}\tau_f \end{bmatrix}. \tag{2}$$

Given similarity matrix s_{ij}, AP attempts to find the entities that maximize the net similarity, i.e. the overall sum of similarities between all entities of the network. The AP process can be viewed as a message passing process with two kinds of messages exchanged among data points: responsibility and availability. Responsibility, r_{ij}, is a message from vehicle i to vehicle j that reflects the accumulated evidence for how well-suited vehicle j is to serve as the MR for vehicle i. Availability, a_{ij}, is a message from vehicle j to i that reflects the accumulated evidence for how appropriate it would be for vehicle i to choose vehicle j as its MR. All responsibilities and availabilities are set to 0 initially, and their values are iteratively updated as follows to compute convergence values:

$$r_{ij} = (1-\lambda)r_{ij}^{new} + \lambda r_{ij}^{old}, \tag{3}$$

$$a_{ij} = (1-\lambda)a_{ij}^{new} + \lambda a_{ij}^{old}. \tag{4}$$

where λ is a damping factor introduced to avoid numerical oscillations, and r_{ij}^{new} and a_{ij}^{new} are the propagating responsibility and propagating availability, respectively. r_{ij}^{new} and a_{ij}^{new} are computed by the following equations:

$$r_{ij}^{new} = \begin{cases} s_{ij} - max_{k:k\neq j}\{a_{ik} + s_{ik}\} & (i\neq j) \\ s_{ij} - max_{K:k\neq j}\{s_{ik}\} & (i = j) \end{cases} \tag{5}$$

$$a_{ij}^{new} = \begin{cases} min\left(0, r_{ij} + \sum_{k\neq i,j} max_{k:k\neq j}\{0, r_{ik}\}\right) & (i\neq j) \\ \sum_{k\neq i} max_{k\neq j}\{0, r_{ik}\} + \rho_i & (i = j) \end{cases} \tag{6}$$

where ρ_i is modeled as an exponential function:

$$\rho = e^{-(t_c - t_i)} \tag{7}$$

where t_c denotes the current time and t_i the instant when the cached accumulated value and auxiliary information (Z) were issued. Note that nodes that have been disconnected from the revocation infrastructure will have outdated cached information, i.e., $\rho \rightarrow 0$. The ρ factor is critical in the selection process, as vehicles that have cached a valid Z will be selected as MR with the highest probability even when their relative velocity is high.

It is worth noting that MR beacons could be used to track vehicles position. To avoid that, proposals dealing with *location privacy* [48–51] could be also in conjunction with PPREM. Actually, PPREM does not need the exact values of the vehicle's position/velocity and distortion-Based techniques [52,53] could also be used to provide location privacy. On the other hand, PPREM does not disclose any data aside from the usual information used by safety applications. The basic application of a VANET is to allow arbitrary vehicles to broadcast regularly safety messages (messages about vehicle speed, turning direction, road condition, traffic accident information) to other nearby vehicles and to RSUs. This allows other vehicles to adjust their traveling routes and allows RSUs to inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. Thus, velocity and position values are essential to make safety applications useful and they are broadcast periodically. The IEEE 1609.4 already acknowledges the potential leakage of personal information when broadcasting and states that "the messages should minimize data that uniquely identifies the vehicle or that would allow a recipient to link messages". This requirement must be consistent with also requiring messages to be authenticated. Therefore, one of the vehicle's pseudonyms must be included in each broadcast message.

The message passing that takes places during the selection of the MRs is described in Algorithm 2. Basically, every vehicle maintains a neighbor list, $\mathbf{N}$, containing the parameters shown in Table 2 for each neighbor. Each vehicle periodically broadcasts a MR beacon containing its ID, position, velocity and current MR. Upon the reception of the MR beacons, vehicles update the corresponding entries $\mathbf{N}_i^j$.

Table 2
Parameters of the clustering algorithm.

Symbol	Definition
s_{ij}	Similarity between vehicle *i* and *j*
r_{ij}	Responsibility between data point *i* and *j*
a_{ij}	Availability between data point *i* and *j*
$\mathbf{x}_i = (x_i, y_i)$	Position vector of node *i*
$\mathbf{v}_i = (v_{xi}, v_{yi})$	Velocity vector of node *i*
λ	Damping factor, 0 ≤ λ < 1
MR_{cnvg_j}	Mobile repository convergence flag for node *j*
MR_j	Index of *j*'s current mobile repository
ρ_i	Cached *Z* aging factor of node *i*

Once a vehicle *i* has received the MR beacons from its neighbors, it selects its MR from the neighbors that have their MR_{cnvg_j} flag activated as:

$$MR_i = arg\max_j \left\{a_{ij} + r_{ij}\right\}. \qquad (8)$$

It is worth noting several aspects about the MR selection procedure. Firstly, VANETs will operate under the DSRC standard [1], so that vehicles can use control channel (CCH) to exchange periodic messages and gather information about their neighborhood. Thus, MR beacons will be sent periodically during the CCH intervals. Secondly, as the AP algorithm takes around 10 iterations to converge [47], it will take around 1 s to select the MR during the initialization stage. This time is highly reduced once a vehicle is in possession of a recent *Z*, as the high value of the ρ parameter will make the algorithm converge faster. Thirdly, as the table **N** is not reset between iterations, it gives memory to the algorithm and provides preference to previous MR, i.e., less frequent MR changes. Finally, note that if a node cannot find another MR within range, it will become MR and will contact the RSU to download *Z*.

Algorithm 2: Message Passing to select MRs

```
foreach $OBU_i$ Broadcast do
    Calculate responsibility $r_{ij}$ for each neighbor $j$ as in Eq. (3)
    Calculate availability $a_{ij}$ for each neighbor $j$ as in Eq. (4)
    Store responsibility for neighbor $j$: $\mathbf{R}_i[n] = r_{ij}$
    Store availability for neighbor $j$: $\mathbf{A}_i[n] = a_{ij}$
    Store the $ID$ of $j$ in the index array: $\mathbf{I}[n] = j$
    if $r_{ii}(k) + a_{ii} > 0$ then
        $MR_{cnvg} = r_{ii}(k) + a_{ii}$
    Broadcast $MR_i$ beacon:
    $MR_i = \{j||(x,y)_j||(v_x,v_y)_j||MR_j||\mathbf{R}_i||\mathbf{A}_i||\mathbf{I}_i||MR_{cnvg}\}_{sign_{OBU_i}}$
foreach $OBU_i$ upon $MR_j$ reception do
    if $\mathbf{v}_i \cdot \mathbf{v}_j > 0$ then
        Calculate its similarity with $j$, $s_{ij}$
        if $ID_i \in \mathbf{I}_j$ then
            Get the corresponding responsibility and availability value at $\mathbf{R}_j[ID_i]$ and $\mathbf{A}_j[ID_i]$
        if $MR_{cnvg} > 0$ then
            Update $MR_{cnvg_j}$ field in $j$'s neighbor list entry, $\mathbf{N}_i^j$
    else
        Ignore beacon
```

Once a node is selected as MR, it has to contact the RSU in range to download the most recent *Z*.[2] The MR will check the authenticity of the *Z* by verifying that the signature is valid and correspond to the CA. It will also check the validity of these data by verifying that the timestamp has not expired. Then, the MR will be able to act as repository and convey the $Acc(R)$ value to any requesting vehicle.

Finally, it is worth noting that mobile repositories basically: i) improve the performance of the revocation service and ii) decrease the success probability of inference attacks. These benefits should encourage VANET entities to collaborate but additionally PPREM provides incentives to collaborate. Inside a cluster, MRs are able to access the RSU using the control channel and their traffic is sent with the highest priority (i.e. access category 3). Hence, those vehicles acting as MR will reduce their communication delay when communicating with the RSU. However, we must stress that if no vehicle is willing to act as MR, the revocation service will still work.

3.5. Certificate status testing

During the initialization phase, the CA codes a large set of all revoked certificate identities into the system accumulated value $Acc(R)$, so that there is a short proof that a given certificate is revoked. To test that a given certificate has not been revoked, OBUs have to provide a non-membership witness so that any other OBU can test that the certificate ID has not been included in the accumulated value. Note that as the $Acc(R)$ is signed by the CA, the test can be performed locally while assuring the authenticity. Moreover, forging a non-membership proof is not feasible as it will mean that an OBU can break the *q*-strong Diffie–Hellman assumption [54]. Thus, under the *q*-Strong Diffie–Hellman assumption, for any nonmember of set *R* there exists a unique non-membership witness with respect to the accumulated value $Acc(R)$.

Algorithm 3: Certificate Validity Test

```
Input: Certificate to test $(c_j)$
Output: Revocation status
1  if $Acc(\mathcal{R})$ not cached then
2      Download $Acc(\mathcal{R})$ from any repository in range.
3  else
4      if Timestamp in $Acc(\mathcal{R})$ is not expired then
5          Obtain non-membership witness $\hat{w}_j = (w_j, u_j)$ for certificate $c_j$
6          Check the validity of the non-membership witness, i.e., $u_j \neq 0$
7          /*Perform the non-membership test*/
8          if $(w_j^{(c_j+s)} == Acc(\mathcal{R}) \cdot g^{u_j})$ then
9              return Non-revoked certificate
10         else
11             return Revoked certificate
12     else
13         Update $Acc(\mathcal{R})$ and go to step 5.
```

Note that when testing the validity of a given certificate bilinear pairing is also used. For any $r_i \in R$, we define the membership witness $w_i \in G_2$ of r_i with respect to accumulation value $Acc(R)$ to be the value w_i satisfying the membership verification test $w_j^{(c_j+s)} = Acc(R)$, which, using the bilinear map $\widehat{e}(\cdot,\cdot)$ and the publicly known group element $h = g^s$, is realized in practice as $e(w_i, g^i \cdot h) = e(Acc(R), g)$. Given a certificate c_j to be verified, a vehicle performs the test protocol described in Algorithm 3. Contrary to traditional certificate status checking mechanism, the vehicles do not need neither to download the whole CRL nor to disclose the ID of the certificate they need to check. Once the vehicles have obtained the accumulated value, they just need to get the non-membership witness from the other entity and check its validity locally.[3] Thus, PPREM enhances both the privacy of the user and the performance of the network.

3.6. Updating the revocation information

Updating the revocation information is a critical point in any mechanism. Traditionally, new CRLs are issued periodically. For instance, authors in [55] analyzed the issuing policies of the main CAs which range

[2] Note that if no RSU is in range, the vehicle will continue acting as MR but any CSI query will be delayed until *Z* is obtained.

[3] Note that vehicles can store in their cache the witnesses of their neighbor vehicles to avoid additional communication costs.

from 1 day to 1 month. However, a policy that enforces frequent updates is highly inefficient for wireless networks, where the medium is shared and downloading a big-sized CRL is bandwidth-costly. Thus, cost-optimized strategies should be applied as authors pointed out in [56]. To this respect, the PPREM's updating process is much more efficient than the traditional CRL issuing approach. PPREM just requires the CA to compute again the accumulator and transmit it to all the repositories. Vehicles only need to download the new accumulated value and update their witnesses. Therefore, a CA could afford to update the OWA several times per day. This allows us to set the validity of the accumulated value, for instance, to several hours. In this case, it will only be necessary to update once the revocation information per journey since in average, people spend around less than 2 h driving per day. As updating PPREM only requires a few Kbytes, PPREM takes advantage of the control channel specified in the IEEE 1609.4 to issue these data to the requesting entities. This channel is not secure but this is not a problem because our accumulated value is signed by the CA and thus it cannot be forged.

Algorithm 4 describes the procedure the CA follows to update the accumulated value. Note that as our accumulator is dynamic the CA can efficiently update the accumulator value by adding new revoked certificate to and deleting the expired ones from the value. Furthermore, as it is universal when a value is updated, e.g., from $Acc(R)$ to $Acc(R)'$, the non-membership witness w_j for some certificate c_j w.r.t. $Acc(R)$ can also be efficiently updated to the witness w_j for the same certificate c_j w.r.t. the new value $Acc(R)'$. Thus, this algorithm is efficient in terms of time complexity, i.e., it is independent of the cardinality of the accumulated element set R.

```
Algorithm 4: Accumulator value update
  Input: $k$ certificates to be added, $c_a$ with $a = [1..k]$
         $z$ certificates to be deleted; $c_d$ with $d = [1..z]$
         Old Accumulated Value $Acc(\mathcal{R})$
  Output: New Accumulated Value, $Acc(\mathcal{R})'$
  $P = \prod_{\substack{a=1..k \\ d=1..z}} \frac{s+c_a}{s+c_d}$
  $Acc(\mathcal{R})' = (Acc(\mathcal{R}))^P$
  return $(Acc(\mathcal{R})'||v(s)||t_i)_{sig_{CA}}$
```

Once the CA updates the accumulated value, it is signed and sent to the RSUs. RSUs announce the existence of new Z through the control channel [1], so that the MR can update its cached version. Then, vehicles that need to check the validity of a certificate must update the accumulated value and their non-membership witnesses, as described in Algorithm 5. Note that the updating process is done locally, so that vehicles just need to download $v(s)$ and the new accumulated value $Acc'(R)$ from the MR. Thus, no statistical information can be inferred neither by the RSU nor the MR about the communications that are taking place.

```
Algorithm 5: Non-membership witness generation
  Input: Certificate $c_j$
  Output: Non-membership witness $\hat{w}_j$
  Download the polynomial $v(s)$ from the MR, where
    $v(s) = \prod_{i=1}^{n}(c_i + s)$
  Compute a polynomial division of $v(s)$ by $(s + c_j)$.
  Since $(s + c_j)$ is a degree one polynomial and
    $c_j \neq c_i \forall i$, there exists a degree $k - 1$ polynomial $r(s)$
    and a constant d such that $v(s) = r(s)(s + c_j) + u_j$.
  Expand $r(s)$ as $r(s) = \sum_{i=0}^{i=n-1}(\alpha_i s^i)$
  Compute $w_j = g^{r(s)} = \prod_{i=0}^{i=n-1} g_i^{\alpha_i}$
  The non-membership witness of $c_j$ is $\hat{w}_j = (w_j, u_j)$
  return $\hat{w}_j$
```

4. Security analysis

In this section, we analyze the security of the proposed protocol against some common attacks.

1 *Mis-authentication resistance*: Mis-authentication occurs when an OBU uses a revoked certificate to successfully authenticates herself to another OBU. Consider an adversary A whose pseudonym r'_i has been revoked. To mist-authenticate, A should be able to obtain a non-membership witness value for r_i, i.e., A is able to find another set $R' = \{r'_1, r'_2, \ldots, r'_n\} = \{r_1, r_2, \ldots, r_n\} = R$ such that

$$g^{\left(r'_1+s\right)\left(r'_2+s\right)\ldots\left(r'_n+s\right)} = g^{(r_1+s)(r_2+s)\ldots(r_n+s)}.$$

Since $r'_i \notin R$, we have $(r'_i + s)$ that does not divide $\prod_n = (r_1 + s)(r_2 + s) \ldots (r_n + s)$ and therefore A has to find c and P such that $\prod_n = c + P(r'_j + s)$. Therefore, A has to find $g^{\left(\frac{1}{r'_j+s}\right)}$, which is equivalent to break the q-strong Diffie–Hellman assumption.

2. *Replay attack resilience*: Consider an adversary A whose pseudonym r_i has been revoked. Since the accumulated value issued by the CA includes the current time stamp, A cannot use a non-membership witness valid at time T_i and replay it at a later time T_{i+1} to pass the revocation checking process as the receiving OBU compares the current time $T_i + 1$ with that included in the current accumulated value. Consequently, PPREM is secure against replay attacks.
3. *Non-repudiation*: Nonrepudiation is achieved by requiring all the messages exchanged in the network to be digitally signed by its issuer. Note that it is not possible to forge signature as it will mean that an OBU is able to solve the Elliptic-curve discrete-logarithm problem which is a hard computational problem [57], i.e., it cannot be solved in a subexponential time.
4. *Privacy*: In PPREM, privacy is preserved by the following techniques.
   (a) Anonymous authentication: Each OBU is equipped with a TDP where a set of pseudonyms are stored. Moreover, the OBU certificates have a short lifetime. As a result, each OBU has to periodically change its certificate from the pool of pseudonyms, which decreases the probability of being tracked by an external observer. Thus, it is not possible to link in anyway the real identity of the OBU with the pseudoidentity that is used to communicate with the other vehicles. Furthermore, by deploying anonymous authentication, PPREM can efficiently prevent an adversary from tracking the real identity of the vehicle.
   (b) Anonymous revocation updates: Since only the MR will contact the RSU to obtain the revocation information, the RSU cannot obtain any statistics of the communications that are taking place by analyzing the queries related to the revocation service. Similarly, vehicle will contact the MR to download the accumulated value and the necessary data to update their non-membership witnesses. Thus, MRs cannot obtain any knowledge about the vehicle by analyzing these queries.
   (c) Transparent roaming: Since any OBU can update its non-membership witness from any MR in the network, PPREM overcomes the need to reregister the OBU entering a new domain with the CA. Vehicles can locate the most akin MR by listening to the DSRC control channel. Consequently, the transparent roaming is guaranteed in PPREM.

5. Performance evaluation

In this section, we evaluate the efficiency of PPREM and we compare it with other certificates status management protocols designed for VANET. First, we compare the computational and communication costs of our mechanism. Then, we evaluate the proposed mechanism by simulation.

Please cite this article as: C. Gañán, et al., PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks, Computer Standards & Interfaces (2013), http://dx.doi.org/10.1016/j.csi.2013.08.002

Table 3
Complexity comparison.

Scheme	Certificate validation				
	Communication		Computation		
	Downlink	Uplink	OBU check	OBU prove	Repository
CRL (IEEE1609.2) [3]	$O(N)$	–	$O(\Delta_n)$	–	$O(\Delta_n)$
DCS [23]	$O(N)$	–	$O(\Delta_n)$	–	$O(\Delta_n)$
ECPP [22]	$O(N)$	–	$O(\Delta_n)$	–	$O(\Delta_n)$
ADOPT [10]	$O(\Delta_n)$	$O(1)$	$O(\Delta_n)$	–	$O(\Delta_n)$
COACH [12]	$O(log_2N)$	$O(1)$	$O(log_2\Delta_N)$	–	$O(log_2\Delta_n)$
PPREM	$O(1)$	$O(1)$	$O(\Delta_n)$	$O(N+\Delta_n)$	$O(1)$

Table 4
Comparison of the overhead introduced by PPREM and other certificate validation mechanisms.

Mechanism	Unit size	Item number	Total size (bytes)
CRL (IEEE1609.2) [3]	21 bytes	$\frac{L_w+1}{2}$	$10.5^* \frac{L_w+1}{2}$
DCS [23]	8 bytes	$\frac{L_w+1}{2}$	$4^* \frac{L_w+1}{2}$
ECPP [22]	21 bytes	$\frac{L_w+1}{2}$	$10.5^* \frac{L_w+1}{2}$
COACH [12]	710 bytes	1	710
ADOPT [10]	586 bytes	1	586
PPREM	406 bytes	1	406

5.1. Complexity analysis

The core component of PPREM, which has the most impact on performance, is the OBU's pseudonym status checking protocol. Table 3 summarizes the complexity of PPREM and shows comparisons with existing schemes. The analysis is based on the following variables: N is the total number of revoked certificates while Δ_n is the number of newly added revoked certificates with respect to the repository's local copy.

With traditional CRLs, OBUs have to download the whole blacklist so the communication cost of Downlink is of course $O(N)$. COACH is based on the use of a Merkle hash tree, i.e., if N certificates are revoked, the length of the proof is $O(log_2N)$. ADOPT is a modification of the traditional OCSP (Online certificate status protocol) [24], where to validate a certificate a vehicle sends a certificate status request to the mobile repository. The latter sends back a signed response indicating the status (revoked, valid or unknown) of the specified certificate. Therefore the communication cost is $O(\Delta_n)$ in the Downlink and $O(1)$ in the Uplink. On the other hand, in PPREM, the OBU only needs to download the accumulated value and the corresponding witness to check the validity of any certificate. Thus, the communication cost is $O(1)$ both in the Downlink and Uplink.

Using CRLs, the complexity of User Check is at least $O(\Delta_n)$, with a simple linear search. In PPREM, OBUs only need to update the witness, making computation cost grow linearly with Δ_n. In ADOPT, a valid signed response has to be located among the caching nodes so the complexity of User Check is at least $O(\Delta_n)$. In COACH, the validity of the root hash has to be checked which takes at least $O(log_2\Delta_n)$. The costs of producing, transferring and verifying such proofs at the repositories are $O(\Delta_n)$ per validity period in the case of CRL and ADOPT, $O(log_2\Delta_n)$ in the case of COACH as new leaves can be added to the hash tree without recomputing the whole tree, and $O(1)$ in the case of PPREM as all new revoked certificates can be added in a single operation. Finally, as PPREM is the only implicit revocation mechanism, there are computational costs associated to the witness update at the user side. This is the drawback of PPREM, mainly due to the complexity of the witness update algorithm. PPREM needs $N+\Delta_n$ exponentiations on a base in G_1 for every element accumulated (N) or newly revoked (Δ_n). However, the exponentiations only have to be performed once per validity period and can be done prior to any witness request.

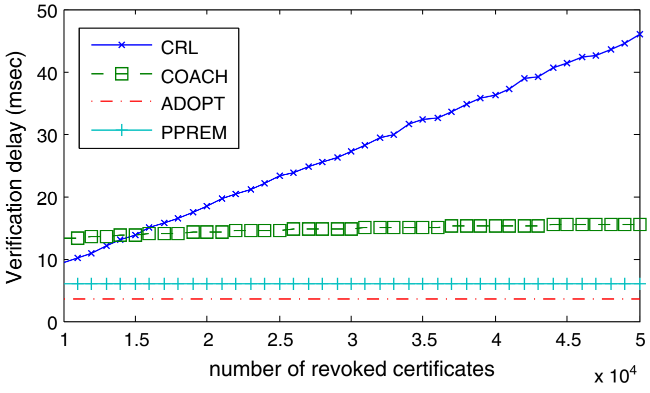

Fig. 2. Verification delay.

In other anonymous authentication schemes such as ECPP [22], and DCS [23] when a vehicle receives a message signed by an unknown certificate, it checks the certificate validity against the CRL. Thus, their communication costs are similar to the traditional CRL mechanism, and the revocation checking complexity depends on the string search algorithm.

5.1.1. Certificate status checking delay

We compare the message status validation delay employing the IEEE 1609.2, COACH and ADOPT with that employing PPREM to check the revocation status of an OBU. The IEEE 1609.2 trial use standard proposes the use of CRL to check the status of a certificate. To check the validity of certificate against the CRL, a progressive search of the revoked certificates is performed. Let T_{hash} and T_{mul} denote the time required to perform a pairing operation and a point multiplication, respectively. The elliptic curve digital signature algorithm is the digital signature method chosen by the VANET standard IEEE1609.2, where a signature generation takes T_{mul} and a signature verification takes $4T_{mul}$. In COACH, to verify a credential, a verifier must perform a hash operation to compute the current contents of the leaf node corresponding to the target serial number. Therefore, the total computation overhead when checking the status of a certificate is $T_{hash}(logN+1)+4T_{mul}$. In [58], T_{mul} are found for an MNT curve with embedding degree $k=6$ that is equal to 0.6 ms. In our simulation, we use an Intel Core i7 950 (at 3.07 GHz) which is able to perform 1015952 SHA-1 Hashes per second, i.e., $T_{hash}=0.98\ \mu s$. We choose a pairing over Type-D curves for the implementation of our PPREM. Such curves have the form $E{:}y^2=x^3+cx+d$ and have embedding degree 6. $\mathbb{G}_1$ is defined over $E(\mathbb{F}s)$ and has order p where s and p are 248-bits and 224-bits respectively. PPREM only requires two pairing operation and one exponentiation to verify the accumulator.

Fig. 2 shows a comparison between the verification delay per message using PPREM, CRL checking process, COACH and ADOPT vs. the number of the revoked certificates. It can be seen that the delay using the CRL checking process increases with the number of revoked certificates. With COACH the delay also increases but in a logarithmic manner. On the other hand, this delay remains almost constant when using ADOPT and PPREM. ADOPT performs slightly better than PPREM as it

Table 5
Parameter values for the reference scenario.

Parameter	Value
Simulation time	500 s
Number of vehicles	100
Self-similarity	−2000
τ_f	30 s
Number of RSUs	10
RSU Transmission power	28.8 dBm
MAC	IEEE 802.11p
Propagation model	Nakagami
Transport protocol	UDP

Please cite this article as: C. Gañán, et al., PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks, Computer Standards & Interfaces (2013), http://dx.doi.org/10.1016/j.csi.2013.08.002

only requires to check the correctness of a signature and the freshness of a timestamp, while PPREM also requires to check the accumulator. However, the main delay in ADOPT is not due to the verification process but to the location of a valid pre-signed response. It is worth noting that the delay in PPREM will be higher if the OBUs need to update their witnesses. However, this operation should be done offline, and just provide the updated witness when required.

5.1.2. Revocation overhead

The updated revocation information will be transmitted to all vehicles. While in PPREM, vehicles just need to download the accumulated value and the corresponding witness, current proposals such us COACH [12], DCS [23] and ECPP [22] need to download the whole CRL. Table 4 presents the CRL size to revoke one vehicle. In ECPP, and DCS, all the pseudonyms of unexpired certificates belonging to the revoked vehicle should be added into the CRL. Since the maximal size of the short-time anonymous certificate set in both ECPP and DCS is L_w, the average number of unexpired certificates is $(Lw + 1) / 2$. In PPREM, the new revoked pseudonym has to be added to the accumulated value. Thus, the size of the data to update the revocation information in PPREM is constant. Note that PPREM introduces the lowest overhead in the network when downloading the revocation information.

5.2. Simulation

In this section, we use the OMNeT++ network simulator [59] and its *INET Framework* [60] extension to evaluate the performance of PPREM. OMNeT++ is a well-known discrete event simulator based on C++ which offers excellent capabilities for protocol and network modeling. The *INET Framework* [60] is a collection of protocols for the use with OMNeT++ which, among others, contains implementations of IPv4, IPv6, TCP, UDP and several application models as well as link-layer models of PPP, Ethernet and 802.11. Especially its sophisticated implementation of 802.11 Medium Access Control (MAC) and MAC Layer Management makes the INET Framework a good choice for the simulation of 802.11p-based car-to-x communication.

We use the traffic simulator SUMO (Simulation of Urban MObility) [61] in order to generate our mobility models. We distinguish two scenarios: a highway scenario and an urban scenario. In the highway scenario, we consider a road segment of 10 km composed of 2 lanes where all vehicles move in the same direction. The highways moving in either direction were separated by more than the 500 m broadcast range, so that clustering could not occur across them. In the urban scenario, we consider a set of 4 adjacent intersections. Each road is composed of 2 lanes where vehicles move in opposite directions. The distance between any two intersections is set to 1000 m. Upon entering the network, each vehicle picks a random destination. In both scenarios, vehicles are distributed randomly in the network.

The main parameter settings used in the simulations are listed in Table 5. Note that we have configured the Future Prediction Period, τ_f, and the self-similarity to improve the stability of the clusters according to the scenario characteristics.

The transmitter and receiver powers of the OBUs were defined in the IEEE WAVE family of standards, so as receivers they have a sensitivity of −82.0 dBm (see Table 6). The MAC retransmission policies for unicast messages are the default. We use the 802.11 short retry limit of 7 retransmissions before it gives up on transmitting a given message. If the message is not transmitted after 7 retries it is dropped and it is the responsibility of the executing application to ensure that it resends the message if that is still needed. Since the revocation information is deemed to be very important for the robustness of the network, they are sent with the maximum priority, which corresponds to access category 3. The configuration parameters of the vehicles are shown in Table 6.

Table 6
Car profile.

Parameter	Value
Max. speed	{10,15,20,25,30,35,40} m/s
Max. acceleration	5 m/s
Max. deceleration	3 m/s
Channel bandwidth	10 MHz
OBU receiver sensitivity	−82.0dBm
OBU antenna height	1 m
Type of antenna	Omnidirectional

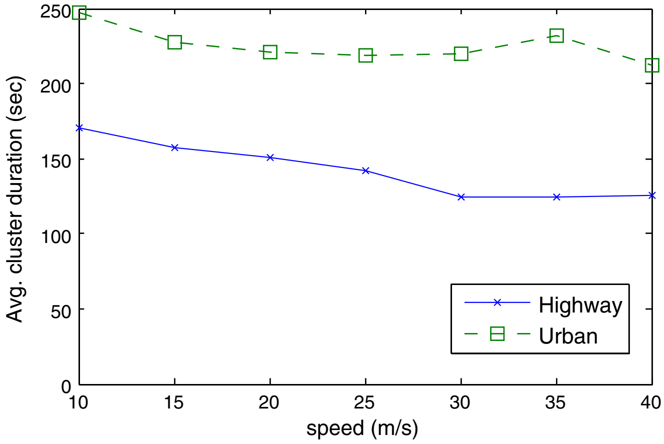

Fig. 3. Average cluster member duration vs vehicle's speed.

5.2.1. Cluster analysis

In this section, simulation results are presented for the PPREM clustering algorithm. Both cluster stability and the number of clusters formed are studied. The average cluster member duration is displayed in Fig. 3. As expected, PPREM algorithm obtains clusters with high stability as it considers cluster member suitability during both cluster formation and maintenance. As the vehicle's speed increased, the cluster becomes more unstable. However, even when vehicles are moving at 40 m/s, the cluster memberships remain unaltered for more than 100 s in average. It is worth noting that as the highway vehicle reach their maximum speed more frequently, the duration of the cluster is higher in the urban scenario than in the highway. This is also a side effect of the vehicle's speed and the junctions that are present in the highway scenario.

PPREM clustering algorithm also intends to reduce the number of clusters in order to reduce the number of queries to the RSUs. Fig. 4 shows the average number of clusters. It is evident that an increase in speed results in an increase in the number of clusters formed. Once again, as in the highway the maximum speed is achieved more often

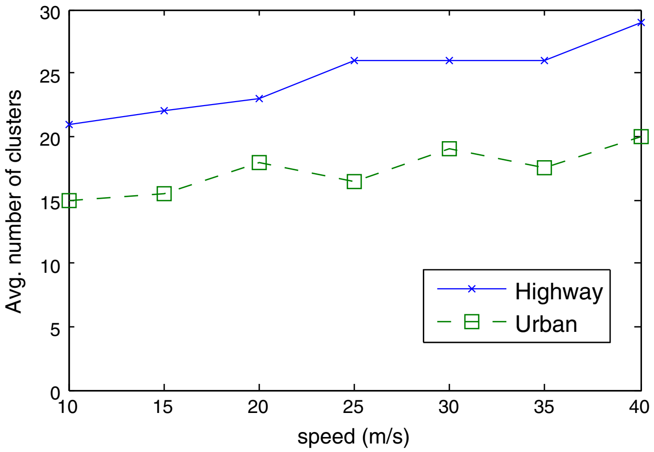

Fig. 4. Average number of clusters vs vehicle's speed.

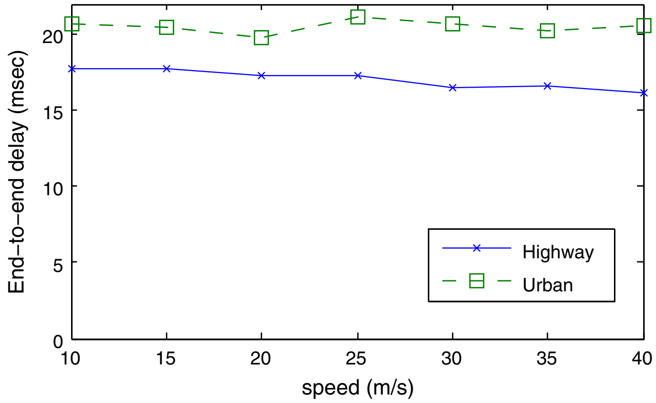

Fig. 5. PPREM end-to-end delay vs vehicle's speed.

than in the urban scenario, as the number of cluster in the highway is higher. It is worth noting that the mean number of member per cluster is between 65 and 40 vehicles.

5.2.2. End-to-end delay

To further evaluate PPREM, we analyze the end-to-end delay, which is defined as the time to transmit a message from the sender to the receiver. Fig. 5 shows the end-to-end delay in milliseconds vs. the vehicle's speed, by employing authentication using the proposed PPREM in the two scenarios. In the simulation, we consider 30,000 revoked certificates. It can be seen that the end-to-end delay decreases with the speed because the number of the received packets decreases (as well as the OBUs density) resulting in longer waiting time for the packets to be processed by the application layer in each OBU. In addition, the end-to-end delay tends to be constant in the urban scenario where there are higher OBU densities and the number of received packets reaches the maximum number of packets an OBU can verify within a specific duration. Note that in any case, the end-to-end delay is below the 25 ms, which allows to rapidly check the status of a given certificate, while downloading a CRL containing the IDs of 30,000 revoked certificates could take minutes.

5.2.3. Message loss ratio

According to DSRC, each vehicle should disseminate a traffic message every 300 ms. The average message loss ratio is defined as the average ratio between the number of messages dropped every 300 ms, due to the message certificate status checking delay, and the total number of messages received every 300 ms by an OBU. Fig. 6 shows the simulated message loss ratios every 300 ms for PPREM, COACH and CRL respectively. It can be seen that PPREM performs the best due to the lowest authentication overhead.

At the initial stage of simulation, vehicles using CRLs have no idea on which certificates are veritable and have to verify both of the certificate and the message signature for the received messages. They have to download the whole CRL but they cannot afford so much overhead, and some messages are dropped. Thus, the message loss ratio is large at the beginning and reduces during the running of the simulation. Similarly, with COACH, at first users do not know whether a certificate belongs to the Merkle Hash tree. However, after some iteration they have enough information to reconstruct the necessary parts of the hash tree to verify whether a certificate belongs to one of the leaves of the tree or not. PPREM does not present this transient state during the initialization phase as the accumulator can be downloaded in milliseconds.

6. Conclusions

We have proposed PPREM for VANETs, which enhances the certificate status checking process by replacing the time-consuming CRL with a fast revocation checking process employing a one-way accumulator. PPREM not only satisfies the security and privacy requirements of VANETs but can also significantly reduce the revocation cost. Moreover, PPREM enhances the driver's privacy so that the adversaries cannot trace the communication of legitimate vehicles, although they have compromised the RSUs.

Analytic results show that allocating a small bandwidth is enough to ensure that vehicles can download fresh revocation information within few milliseconds. The performance improvement is obtained at the expense of having an implicit revocation protocol, where vehicles have to obtain a witness of the certificate prior to validate its status. Therefore, PPREM significantly reduces the complexity of certificate management and achieves great efficiency and scalability, even when it is deployed in heterogeneous vehicular networks.

Acknowledgment

This work is funded by the Spanish Ministry of Science and Education under the projects CONSOLIDER-ARES (CSD2007-00004) and TEC2011-26452 “SERVET”, FPU grant AP2010-0244, and by the Government of Catalonia under grant 2009 SGR 1362.

References

[1] R. Bera, J. Bera, S. Sil, S. Dogra, N. Sinha, D. Mondal, Dedicated short range communications (DSRC) for intelligent transport system, Wireless and Optical Communications Networks, 2006 IFIP International Conference, 2006, pp. 1–5.
[2] IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments, , 2008.
[3] IEEE, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages, IEEE Std 1609.2-2006, 2006. 1–117.
[4] M. Nowatkowski, H. Owen, Certificate revocation list distribution in VANETs using most pieces broadcast, IEEE SoutheastCon 2010 (SoutheastCon), 2010, pp. 238–241.
[5] J. Haas, Y.C. Hu, K. Laberteaux, Efficient certificate revocation list organization and distribution, IEEE J. Sel. Areas Commun. 29 (2011) 595–604.
[6] A. Wasef, X. Shen, MAAC: Message Authentication Acceleration Protocol for vehicular ad hoc networks, Global Telecommunications Conference, 2009. GLOBECOM 2009, IEEE, 2009, pp. 1–6.

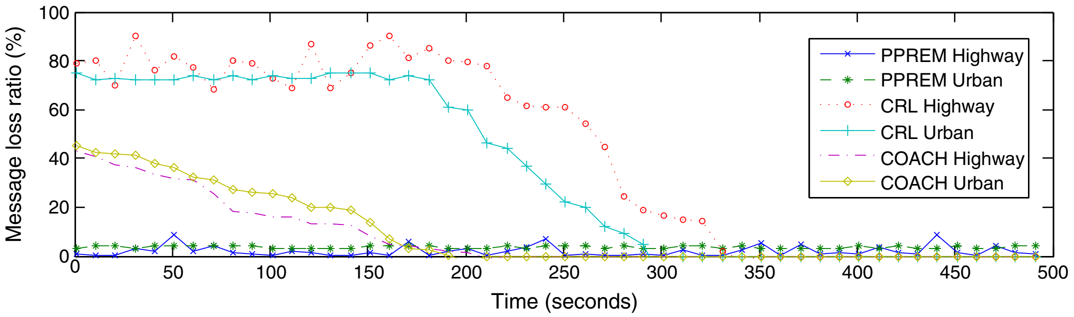

Fig. 6. Comparison between message loss ratios for different schemes.

Please cite this article as: C. Gañán, et al., PPREM: Privacy Preserving REvocation Mechanism for Vehicular Ad Hoc Networks, Computer Standards & Interfaces (2013), http://dx.doi.org/10.1016/j.csi.2013.08.002

[7] S. Santesson, P. Hallam-Baker, Online certificate status protocol algorithm agility, RFC 6277 (Proposed Standard), 2011.

[8] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, J.-P. Hubaux, Certificate revocation in vehicular networks, Technical Report, EPFL, 2006.

[9] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communication systems: design and architecture, IEEE Commun. Mag. 46 (2008) 100–109.

[10] G.F. Marias, K. Papapanagiotou, P. Georgiadis, ADOPT. A Distributed OCSP for Trust Establishment in MANETs, 11th European Wireless Conference 2005, 2005.

[11] A. Wasef, X. Shen, EDR: Efficient Decentralized Revocation Protocol for vehicular ad hoc networks, IEEE Trans. Veh. Technol. 58 (2009) 5214–5224.

[12] C. Gañán, J.L. Muñoz, O. Esparza, J. Mata-Díaz, J. Hernández-Serrano, J. Alins, COACH: COllaborative certificate stAtus CHecking mechanism for VANETs, J. Netw. Comput. Appl. 36 (5) (2013) 1337–1351, http://dx.doi.org/10.1016/j.jnca.2012.02.006, (ISSN 1084–8045).

[13] A. Wasef, X. Shen, EMAP: Expedite Message Authentication Protocol for vehicular ad hoc networks, IEEE Trans. Mob. Comput. (2011) 1.

[14] J. Solis, G. Tsudik, Simple and flexible revocation checking with privacy, Proceedings of the 6th International Conference on Privacy Enhancing Technologies, PET'06, Springer-Verlag, Berlin, Heidelberg, 2006, pp. 351–367.

[15] Y. Sun, R. Lu, X. Lin, X. Shen, J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications, IEEE Trans. Veh. Technol. 59 (2010) 3589–3603.

[16] K. Priya, K. Karuppanan, Secure privacy and distributed group authentication for VANET, 2011 International Conference on Recent Trends in Information Technology (ICRTIT), 2011, pp. 301–306.

[17] J.C. Benaloh, M. de Mare, One-way accumulators: a decentralized alternative to digital signatures (extended abstract), Advances in Cryptology — EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, May 23–27, 1993, Proceedings, Lect. Notes Comput. Sci., vol. 765, Springer, 1993, pp. 274–285.

[18] M. Raya, J.-P. Hubaux, The security of vehicular ad hoc networks, Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN '05, 2005, pp. 11–21.

[19] X. Lin, X. Sun, P.-H. Ho, X. Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications, IEEE Trans. Veh. Technol. 56 (2007) 3442–3456.

[20] A. Studer, E. Shi, F. Bai, A. Perrig, TACKing together efficient authentication, revocation, and privacy in VANETs, SECON '09. 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009., 2009, pp. 1–9.

[21] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, CARAVAN: providing location privacy for VANET, Embedded Security in Cars (ESCAR), 2005.

[22] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, ECPP: efficient conditional privacy preservation protocol for secure vehicular communications, INFOCOM 2008. The 27th Conference on Computer Communications, IEEE, 2008, pp. 1229–1237.

[23] A. Wasef, Y. Jiang, X. Shen, DCS: an efficient distributed-certificate-service scheme for vehicular networks, IEEE Trans. Veh. Technol. 59 (2010) 533–549.

[24] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, Xrd.509 internet public key infrastructure online certificate status protocol — OCSP, RFC 2560 (Proposed Standard), http://www.ietf.org/rfc/rfc2560.txt1999updated by RFC 6277.

[25] R. Merkle, A certified digital signature, Advances in Cryptology — CRYPTO'89 Proceedings, Lect. Notes Comput. Sci., vol. 435, Springer, Berlin / Heidelberg, 1990, pp. 218–238.

[26] P. Kamat, A. Baliga, W. Trappe, Secure, pseudonymous, and auditable communication in vehicular ad hoc networks, Secur. Commun. Netw. 1 (2008) 233–244.

[27] C. Gamage, B. Gras, B. Crispo, A.S. Tanenbaum, An identity-based ring signature scheme with enhanced privacy, Securecomm and Workshops, 2006, 2006, pp. 1–5.

[28] N. Baric, B. Pfitzmann, Collision-free accumulators and fail-stop signature schemes without trees, Proceedings of the 16th Annual International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT'97, Springer-Verlag, Berlin, Heidelberg, 1997, pp. 480–494.

[29] M.T. Goodrich, R. Tamassia, J. Hasic, An efficient dynamic and distributed cryptographic accumulator, Proceedings of the 5th International Conference on Information Security, ISC '02, Springer-Verlag, London, UK, 2002, pp. 372–388.

[30] J. Camenisch, A. Lysyanskaya, Dynamic accumulators and application to efficient revocation of anonymous credentials, Proceedings of the 22nd Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '02, Springer-Verlag, London, UK, 2002, pp. 61–76.

[31] J. Li, N. Li, R. Xue, Universal accumulators with efficient nonmembership proofs, Proceedings of the 5th International Conference on Applied Cryptography and Network Security, ACNS '07, Springer-Verlag, Berlin, Heidelberg, 2007, pp. 253–269.

[32] P. Camacho, A. Hevia, M. Kiwi, R. Opazo, Strong accumulators from collision-resistant hashing, Proceedings of the 11th International Conference on Information Security, ISC '08, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 471–486.

[33] P. Camacho, A. Hevia, M. Kiwi, R. Opazo, Strong accumulators from collision-resistant hashing, Int. J. Inf. Secur. 11 (2012) 349–363, http://dx.doi.org/10.1007/s10207-012-0169-2.

[34] S.S.C. YaTolga Acar, L. Nguyen, Accumulators and U-Prove revocation, Financial Cryptography and Data Security 2013, vol. 2, 2013, pp. 1–8.

[35] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, SIAM J. Comput. 32 (2003) 586–615.

[36] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, J. Cryptol. 17 (2004) 297–319.

[37] M. Scott, Computing the tate pairing, in: A. Menezes (Ed.), Topics in Cryptology — CT-RSA 2005, Lect. Notes Comput. Sci, vol. 3376, Springer, Berlin / Heidelberg, 2005, pp. 293–304.

[38] C. Satizábal, J. Hernández-Serrano, J. Forné, J. Pegueroles, Building a virtual hierarchy to simplify certification path discovery in mobile ad-hoc networks, Comput. Commun. 30 (2007) 1498–1512.

[39] G. Kambourakis, E. Konstantinou, A. Douma, M. Anagnostopoulos, G. Fotiadis, Efficient certification path discovery for MANET, EURASIP J. Wirel. Commun. Netw. 20 (1–20) (2010) 13.

[40] B. Muniyal, K.V. Prema, S. Nayak, Creating virtual hierarchy in peer-to-peer PKI to simplify certificate path discovery, Int. J. Comput. Appl. 41 (2012) 09–12.

[41] L. Nguyen, Accumulators from bilinear pairings and applications, Proceedings of the 2005 International Conference on Topics in Cryptology, CT-RSA'05, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 275–292.

[42] M.H. Au, Q. Wu, W. Susilo, Y. Mu, Compact e-cash from bounded accumulator, Proceedings of the 7th Cryptographers' track at the RSA conference on Topics in Cryptology, CT-RSA'07, Springer-Verlag, Berlin, Heidelberg, 2006, pp. 178–195.

[43] J. Camenisch, M. Kohlweiss, C. Soriente, An accumulator based on bilinear maps and efficient revocation for anonymous credentials, Irvine Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC '09, Springer-Verlag, Berlin, Heidelberg, 2009, pp. 481–500.

[44] J. Lapon, M. Kohlweiss, B. Decker, V. Naessens, Performance analysis of accumulator-based revocation mechanisms, Security and Privacy — Silver Linings in the Cloud, IFIP Adv. Inf. Commun. Technol., vol. 330, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 289–301.

[45] Y. Zhu, X. Fu, B. Graham, R. Bettati, W. Zhao, Correlation-based traffic analysis attacks on anonymity networks, IEEE Trans. Parallel Distrib. Syst. 21 (2010) 954–967.

[46] X. Fu, B. Graham, R. Bettati, W. Zhao, D. Xuan, Analytical and empirical analysis of countermeasures to traffic analysis attacks, Proceedings of International Conference on Parallel Processing, 2003, pp. 483–492.

[47] B.J. Frey, D. Dueck, Clustering by passing messages between data points, Science 315 (2007) 972–976.

[48] R.A. Popa, H. Balakrishnan, A.J. Blumberg, VPriv: protecting privacy in location-based vehicular services, Proceedings of the 18th Conference on USENIX Security Symposium, SSYM'09, 2009, pp. 335–350.

[49] M. Dahl, S. Delaune, G. Steel, Formal analysis of privacy for anonymous location based services, Proceedings of the 2011 international conference on Theory of Security and Applications, TOSCA'11, 2012, pp. 98–112.

[50] R.A. Popa, A.J. Blumberg, H. Balakrishnan, F.H. Li, Privacy and accountability for location-based aggregate statistics, Proceedings of the 18th ACM Conference on Computer and communications Security, CCS '11, 2011, pp. 653–666.

[51] Y.-C. Wei, Y.-M. Chen, Safe distance based location privacy in vehicular networks, 2010 IEEE 71st Vehicular Technology Conference (VTC 2010-Spring), 2010, pp. 1–5.

[52] R. Shokri, J. Freudiger, M. Jadliwala, J.P. Hubaux, A distortion-based metric for location privacy, Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society, WPES '09, 2009, pp. 21–30.

[53] G. Dini, P. Perazzo, Uniform obfuscation for location privacy, Proceedings of the 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, DBSec'12, 2012, pp. 90–105.

[54] D. Boneh, X. Boyen, H. Shacham, Short group signatures, in: M. Franklin (Ed.), Advances in Cryptology — CRYPTO 2004, Lec. Notes Comput. Sci., vol. 3152, Springer, Berlin Heidelberg, 2004, pp. 41–55.

[55] C. Gañán, J.L. Muñoz, O. Esparza, J. Mata-Díaz, J. Alins, Impact of the revocation service in PKI prices, Information and Communications Security, Lec. Notes Comput. Sci., vol. 7618, Springer, Berlin Heidelberg, Hong Kong, 2012, pp. 22–32.

[56] C. Ma, N. Hu, Y. Li, On the release of CRLs in public key infrastructure, Proceedings of the 15th Conference on USENIX Security Symposium — Volume 15, Berkeley, CA, USA, 2006.

[57] N. Koblitz, A. Menezes, S. Vanstone, The state of elliptic curve cryptography, Des. Codes Crypt. 19 (2000) 173–193.

[58] C. Zhang, R. Lu, X. Lin, P.-H. Ho, X. Shen, An efficient identity-based batch verification scheme for vehicular sensor networks, INFOCOM 2008. The 27th Conference on Computer Communications, IEEE, 2008, pp. 246–250.

[59] A. Vargas, Objective Modular Network Testbed in C++ (OMNET++), (Version 4.2. Available: www.omnetpp.org).

[60] A. Ariza, INEMANET framework for OMNeT++, http://github.com/inetmanet/inetmanet/tree/master.

[61] D. Krajzewicz, G. Hertkorn, C. Rössel, P. Wagner, SUMO (Simulation of Urban MObility); an open-source traffic simulation, 4th Middle East Symposium on Simulation and Modelling (MESM2002), MESM2002, 2002, pp. 183–187.