Computer Standards & Interfaces 36 (2014) 513–523

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 16 August 2013

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