Pervasive and Mobile Computing 21 (2015) 75–91

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

EPA: An efficient and privacy-aware 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 13 August 2013
Received in revised form 24 December 2013
Accepted 14 January 2014
Available online 23 January 2014

Keywords:
Revocation
Privacy
Merkle Hash Tree
Crowds
VANET

ABSTRACT

Security is vital for the reliable operation of vehicular ad hoc networks (VANETs). One of the critical security issues is the revocation of misbehaving vehicles. While essential, revocation checking can leak private information. In particular, repositories receiving the certificate status queries could infer the identity of the vehicles posing the query and the target of the query. An important loss of privacy results from this ability to tie the checking vehicle with the query's target, due to their likely willingness to communicate. In this paper, we propose an Efficient and Privacy-Aware revocation Mechanism (EPA) based on the use of Merkle Hash Trees (MHT) and a Crowds-based anonymous protocol, which replaces the time-consuming certificate revocation lists checking process. EPA provides explicit, concise, authenticated and unforgeable information about the revocation status of each certificate while preserving the users' privacy. Moreover, EPA reduces the security overhead for certificate status checking, and enhances the availability and usability of the revocation data. By conducting a detailed performance evaluation, EPA is demonstrated to be reliable, efficient, and scalable.

1. Introduction

Vehicular ad hoc networks (VANETs) aim at enhancing safety and efficiency in 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). As any other wireless network, VANETs can be vulnerable to attacks and jeopardize users' privacy. For instance, an attacker could inject false information, or collect vehicles' messages, track their locations, and infer sensitive user data. To thwart such attacks, security and privacy enhancing mechanisms are necessary or, in fact, a prerequisite for deployment. According to the IEEE 1609.2 standard [1], 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 [1] 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.

Unfortunately, the CRL size in VANETs is expected to be large for the following reasons: (i) the scale of VANET will be significantly large; (ii) to preserve the privacy of the drivers (i.e., to prevent the leakage of the real identities and location information of the drivers from any external eavesdropper) each OBU should be preloaded with a set of anonymous digital

* Corresponding author. Tel.: +34 660590255.
E-mail addresses: carlos.ganan@entel.upc.edu, krlos.hdez@gmail.com (C. Gañán), jose.munoz@entel.upc.edu (J.L. Muñoz), oesparza@entel.upc.edu (O. Esparza), jorge.mata@entel.upc.edu (J. Mata-Díaz), juanjo@entel.upc.edu (J. Alins).

1574-1192/$ – see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2014.01.002

certificates, where the OBU has to periodically change its anonymous certificate to mislead attackers. Consequently, a revocation of an OBU results in revoking all the certificates carried by that OBU leading to a large increase in the CRL size [2–5]. Thus, distributing and updating CRLs raise a challenge. Several CRLs distribution protocols have been proposed to palliate this pitfall, e.g., compressed CRLs by using Bloom filters [6]. Other proposals suggest the use of regional CAs and short lived certificates to decrease the number of entries in the CRL [7]. However, these works overlooked the disruption nature of vehicular networks. Recently, some work has appeared dealing with the distribution of certificate status information (CSI) in environments prone to disruption [8–11]. These mechanisms take advantage of caching strategies combined with hashing techniques to enhance the availability of the revocation service. Nevertheless, none of these approaches take into account the loss of privacy due to the CSI checking process.

Regardless of their particulars, current revocation methods that differ from the traditional CRL approach have an unpleasant side-effect: they divulge too much information [12]. 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. 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 of the PKI such as who sends a message to whom, how often, etc. Recently, there have appeared some works that intend to provide privacy during the revocation process [13]. However, they mainly use CRLs to convey the revocation information. Though CRLs prevent the user's privacy, they consume too much bandwidth when transmitted.

In this article, we address the issue of checking the status of a certificate by exploiting the use of Merkle hash trees (MHT) [14]. MHT have already been suggested as means to provide an efficient revocation service [10,15]. However, they were used in such a way that each time a certificate had to be checked, users had to contact a local repository to verify its validity. We propose an Efficient and Privacy-Aware (EPA) revocation mechanism that uses MHT to provide certificate no-invalidity proofs (i.e., a proof that a given certificate is not revoked) that each vehicle stores locally. Thus, EPA allows vehicles proving the no-invalidity of their certificates to other entities. CAs will transmit an extended CRL to the RSUs that will act as repositories. RSUs will construct a MHT from the information contained in the CRL. Then, any vehicle will be able to download the corresponding certificates' no-invalidity proofs. For enforcing anonymity in multi-hop VANETs, vehicles using EPA do not contact directly the RSU when updating the CSI. In contrast, they follow a Crowds-like protocol [16] according to which each user probabilistically decides to send a message directly to a common receiver, or else to forward it to a peer, who is asked to repeat the process. Our protocol differs from the original Crowds in that, first, it does take into account transmission losses, and second, it is specifically conceived for multi-hop VANETs, rather than for wired networks.

EPA enjoys three main advantages over the traditional revocation mechanisms: (i) EPA saves dramatically on bit transmissions and costs, i.e., vehicles do not have to download the whole CRL, just positive proofs of their certificates' no-invalidity; (ii) EPA always provides a positive statement about the no-invalidity status of each not-yet-expired certificate; (iii) EPA always allows a complete answer to any possible query of a user to the RSU and without trusting the latter in any special way. Thus, EPA decreases the dependency on the infrastructure to provide the certificate status checking service at the same time that prevents RSUs to acquire any private information. Once the vehicles have obtained these short proofs asserting the no-invalidity of their certificates, they do not need to contact the infrastructure anymore. To obtain and update these proofs, vehicles contact RSUs without leaking the personal information. Therefore, EPA provides explicit, concise, authenticated and unforgeable information about the revocation status of each certificate while preserving the users' privacy.

The rest of this article is organized as follows. In Section 2 we summarize the related work regarding CSI management. Section 3 describes the Efficient and Privacy-Aware (EPA) revocation mechanism. In Section 4 we evaluate and compare our proposal to other revocation mechanisms. Finally, we conclude in Section 5.

2. Background

In this section, we describe the existing revocation proposals for VANET.

2.1. Privacy aware revocation approaches for VANET

The IEEE 1609.2 standard [1] 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. [17] 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