Journal of Network and Computer Applications 36 (2013) 1337–1351

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

COACH: COllaborative certificate stAtus CHecking mechanism for VANETs

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

Universitat Politècnica de Catalunya (UPC), Spain

ARTICLE INFO

Article history:
Received 14 July 2011
Received in revised form
27 December 2011
Accepted 20 February 2012
Available online 2 March 2012

Keywords:
VANET
Authentication
Certificate validation
PKI
CRL
Merkle hash tree

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) require mechanisms to authenticate messages, identify valid vehicles, and remove misbehaving vehicles. A public key infrastructure (PKI) can be used to provide these functionalities using digital certificates. However, if a vehicle is no longer trusted, its certificates have to be revoked and this status information has to be made available to other vehicles as soon as possible. In this paper, we propose a collaborative certificate status checking mechanism called COACH to efficiently distribute certificate revocation information in VANETs. In COACH, we embed a hash tree in each standard Certificate Revocation List (CRL). This dual structure is called *extended-CRL*. A node possessing an *extended-CRL* can respond to certificate status requests without having to send the complete CRL. Instead, the node can send a short response (less than 1 kB) that fits in a single UDP message. Obviously, the substructures included in the short responses are authenticated. This means that any node possessing an *extended-CRL* can produce short responses that can be authenticated (including Road Side Units or intermediate vehicles). We also propose an extension to the COACH mechanism called EvCOACH that is more efficient than COACH in scenarios with relatively low revocation rates per CRL validity period. To build EvCOACH, we embed an additional hash chain in the *extended-CRL*. Finally, by conducting a detailed performance evaluation, COACH and EvCOACH are proved to be reliable, efficient, and scalable.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

In the last years, wireless communications between vehicles have attracted extensive attention for their promise to contribute to a safer, more efficient, and more comfortable driving experience in the foreseeable future. This type of communications has induced the emergence of Vehicular Ad Hoc Networks (VANETs), which consist of mobile nodes capable of communicating with each other (i.e. Vehicle to Vehicle Communication—V2V communication) and with infrastructure (i.e. Vehicle to Infrastructure Communication—V2I communication). To make these communications feasible, vehicles are equipped with *On-Board Units* (OBUs), and fixed communication units called *Road Side Units* (RSUs) are placed along the road. Finally, multi-hop communication based on IEEE 802.11 is used to facilitate information exchange among network elements that are not in direct communication range (Bera et al., 2006; Jiang and Delgrossi, 2008).

The open-medium nature of these networks makes it necessary to integrate in VANET security mechanisms such as authentication, message integrity, non-repudiation, confidentiality and privacy (Raya and Hubaux, 2005). The solution envisioned to achieve these functionalities is to use digital certificates provided by a centralized certification authority (CA) (Hubaux et al., 2004; Papadimitratos et al., 2007).

In this context, according to the IEEE 1609.2 standard (IEEE, 2006), certificates will be used for digitally signing messages and also for encryption (using the ECIES algorithm). Finally, vehicular networks will rely on a public key infrastructure (PKI) to manage certificates. A critical part of the PKI is how to manage certificate revocation. In general, revocation systems for VANETs can be roughly classified as global or local depending on the extent of the revocation mechanism.

- *Local revocation approaches* enable a group of neighboring vehicles to revoke a nearby misbehaving node. In such approaches, revocation is possible without the intervention of external infrastructure at the expense of trusting other vehicles criteria.
- *Global revocation approaches* are based on the existence of centralized infrastructure such as the PKI, which is in charge of managing revocation.

According to the IEEE 1609.2 standard (IEEE, 2006), vehicular networks will rely on PKI and Certificate Revocation Lists (CRLs)

* Corresponding author. Tel.: +34 934017041.
E-mail addresses: carlos.ganan@entel.upc.edu (C. Gañán), jose.munoz@entel.upc.edu (J.L. Muñoz), oscar.esparza@entel.upc.edu (O. Esparza), jmata@entel.upc.edu (J. Mata-Díaz), jserrano@entel.upc.edu (J. Hernández-Serrano), juanjo@entel.upc.edu (J. Alins).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2012.02.006

will be used to distribute the status (revoked or valid) of certificates. CRLs are black lists that enumerate revoked certificates along with the date of revocation and, optionally, the reasons for revocation. CRLs in VANET are expected to be quite large because this type of network is expected to have many nodes (vehicles) and also because each vehicle will probably have many temporary certificates (also called pseudonyms) to protect the users' privacy. As a result, a VANET CRL might have a size of hundreds of MB (Nowatkowski et al., 2010; Haas et al., 2011; Wasef and Shen, 2009). The distribution of such a huge structure within a VANET is a challenging issue and it has attracted the attention of many researchers (Papadimitratos et al., 2008a; Laberteaux et al., 2008; Raya and Hubaux, 2005; Haas et al., 2011). A general conclusion about these works is that most of the research efforts have been put into trying to reduce the size of the CRL, either trying to split it or trying to compress it (see Section 2).

In this paper, we take a novel approach because our primary goal is not reducing the CRL size[1] but we aim to design a more efficient way of using the CRL information to distribute certificate status information (CSI) inside the VANET. Our proposal is called COACH (COllaborative certificate stAtus CHecking). COACH is an application-layer mechanism for distributing revocation data. The main idea behind COACH is to embed some little extra information into the CRL such that allows us to create an efficient and secure request/response protocol. For those nodes that just want to obtain status data of some certificates, our protocol replaces downloading a complete CRL. In more detail, we propose a way of efficiently embedding a Merkle hash tree (MHT) (Merkle, 1990) within the structure of the standard CRL to generate a so-called *extended-CRL*. To create the *extended-CRL*, we use an extension, which is a standard way of adding extra information to the CRL. Our extension contains all the necessary information to allow any vehicle or VANET infrastructure element that possesses the *extended-CRL* to build the COACH tree, i.e. a hash tree with the CSI of the CRL. Using this COACH tree, any entity possessing the *extended-CRL* can act as repository and efficiently answer to certificate status checking requests of other vehicles or VANET elements. COACH responses are short since in general, their size is less than 1 kB. This allows a COACH response to perfectly fit within a single UDP message. As we will demonstrate by simulation, this makes the distribution of CSI more efficient than distributing complete CRLs (even though they are compressed), reducing the data that have to be transmitted over the VANET. We must stress that a node possessing an *extended-CRL* can act as COACH repository but that a COACH repository is not a TTP. In other words, COACH is offline, which means that no online trusted entity (like a CA) is needed for authenticating the responses produced by COACH repositories.

Finally, we also propose an enhancement of our basic mechanism called EvCOACH (Evergreen-COACH) to improve the performance of COACH in scenarios with relatively few revocations per CRL validity period. Notice that low revocation rates or small CRL validity periods give rise to such scenarios. In these scenarios, it is plausible to have the same revocation information in several consecutive CRLs. In this case, EvCOACH prevents end-entities from downloading a new CRL whose information is already known. To build EvCOACH, we additionally embed a hash chain in the *extended-CRL*. With this structure, now we can extend the validity of a previous CRL by periodically disclosing successive values of the hash chain. As we will show by simulation, EvCOACH overcomes COACH in terms of bandwidth efficiency in scenarios with relatively few revocations per CRL validity period.

The rest of this paper is organized as follows. In Section 2, we present the background related to our mechanism. In Section 3 we describe in depth COACH. Section 4 depicts EvCOACH, the variant of our proposed mechanism. Section 5 provides a security analysis of the proposals. In Section 6, we evaluate the proposed mechanisms. Finally, Section 7 concludes this paper.

2. Background

In this section, first we start describing the existing global revocation proposals for VANET. Then, we provide a brief overview of Merkle hash trees (MHTs) (Merkle, 1989), which is one of the foundations of the proposed certificate validation mechanism.

2.1. Global VANET revocation mechanisms

Global revocation approaches assume the existence of a Trusted Third Party (TTP), which manages the revocation service. The IEEE P1609.2 standard (IEEE, 2006) proposes an architecture based on CAs. In this architecture, each vehicle possesses several pseudonyms, which are made publicly available by means of short-lived certificates. However, the revocation mechanism for VANET cannot rely uniquely on the use of short-lived certificates (e.g. as proposed in Lu et al., 2008) because compromised or faulty certificates could still cause damage until the end of their lifetimes.

Raya and Hubaux (2005) have proposed the use of short-lived certificates that are preloaded in a tamper-proof device (TPD). The TPD is a trusted component that forms part of the OBU. The TPD stores the valid certificates for a vehicle, signs messages, and performs encryption and decryption functions. Raya et al. introduced two centralized revocation protocols. The first one is based on the revocation of the TPD, which is necessary when all the certificates of a vehicle are to be revoked. This method assumes the presence of the (on-line) infrastructure to send these messages to the trusted component. 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 second protocol proposed in Raya and Hubaux (2005) is based on the use of compressed CRLs. To compress the CRL, they propose to use Bloom filters. Their method reduces the size of a CRL by using about half the number of bytes to specify the certificate serial number for revocation. Storing CRL information in this manner compresses the size of the CRL considerably since a fixed-length Bloom filter is distributed instead of distributing 8–14 B for every certificate that is revoked.

The distribution of CRLs to all vehicles is not trivial. Some authors Papadimitratos et al. (2007, 2008a) have proposed the use of regional certification authorities instead of using a single central authority. Papadimitratos et al. (2008b) suggest restricting the scope of the CRL within a region. The authors also propose breaking the Certificate Revocation List (CRL) into different pieces and transmitting these pieces using Fountain or Erasure codes. In this way, a vehicle can reconstruct the CRL after receiving a certain number of pieces. Similarly, in Wasef et al. (2010), each CA distributes the CRL to the RSUs in its domain through Ethernet. Then, the RSUs broadcast the new CRL to all the vehicles in that domain. In the case RSUs do not completely cover the domain of a CA, V2V communications are used to distribute the CRL to all the vehicles (Laberteaux et al., 2008). This mechanism is also used in Fan et al. (2008), where it is detailed a public key infrastructure mechanism based on bilinear mapping. Revocation is accomplished through the distribution of CRL that is stored by each user.

Another adaptation of classic public key infrastructure to VANETs is proposed in Armknecht et al. (2007). This architecture

[1] Indeed, our proposal can work together with these other approaches that try to reduce the size of the CRL.

Download English Version:

https://daneshyari.com/en/article/459341

Download Persian Version:

https://daneshyari.com/article/459341

Daneshyari.com