Future Generation Computer Systems 64 (2016) 50–60

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

On-siteDriverID: A secure authentication scheme based on Spanish eID cards for vehicular ad hoc networks

J. Sánchez-García, J.M. García-Campos, D.G. Reina, S.L. Toral *, F. Barrero

University of Seville, Escuela Superior de Ingenieros, Avda. Camino de los Descubrimientos, s/n, 41092 Sevilla, Spain

HIGHLIGHTS

- On-SiteDriverID, a secure authentication scheme and its application for VANET road authorities, based on the already in use Spanish eID smart cards.
- The proposed security scheme is of high interest as improves security in VANETs, specifically in situations where a direct, on-site and on demand authentication mechanism is required by a road authority.
- The evaluation of the proposed On-SiteDriverID on simulated realistic VANET urban scenarios.
- In the 60–70% of cases the proposed On-SiteDriverID successfully obtains the identity of the drivers.

ARTICLE INFO

Article history:
Received 28 August 2015
Received in revised form
20 January 2016
Accepted 30 April 2016
Available online 13 May 2016

Keywords:
PKI
Vehicular ad hoc networks
Authentication
ID card

ABSTRACT

Security in Vehicle Ad Hoc Networks (VANETs) has been a topic of interest since the origins of vehicular communications. Different approaches have been followed as new security threats have emerged in the last few years. The approach of conditional privacy has been widely used as it guarantees authentication among vehicles but not revealing their real identities. Although the real identity of a vehicle can be traced by the authorities, the process to do that is time consuming and typically involves several entities (for instance road authorities that request the identification, license plate records bodies, a judge to allow revealing the identity associated to a license plate…). Moreover, this process is always subsequent to the detection of a road situation that requires knowing the real vehicle identities. However, in vehicular scenarios, authorities would beneficiate from knowing the real drivers' identity in advance. We propose in this paper On-SiteDriverID, a secure protocol and its application which allows authorities' vehicles to obtain drivers' real identities rapidly and on demand on VANET scenarios. Thus, authorities would be able to gather information about drivers and vehicles, allowing them to act in a safer and better manner in situations such as traffic control duties or emergencies. The obtained simulation results in real VANET scenarios based on real maps guarantee that in the 60%–70% of cases the proposed On-SiteDriverID successfully obtains the identity of the drivers.

1. Introduction

New security threats have emerged in the field of communication networks due to the recent growth of mobile computing and the intensive use of the Internet. The birth of new communication paradigms like the Internet of things (IoT) envision a world full of connected devices capable of exchanging information through the Internet [1]. The communications among such mobile devices must be carried out in a secure way so that the interlocutors taking part in it can trust each other by means of authentication mechanisms. It is also important to guarantee message integrity and confidentiality of the information exchanged.

In general computer networks, there are plenty off-the-shelf security resources that could be applied with affordable costs in order to provide authentication. Methods for authentication are often categorized as (i) something known, such as a password, (ii) something possessed, for instance an identity card or (iii) something a person is, i.e. a personal characteristic like a fingerprint. Smart cards bring less security vulnerabilities than only-password based authentication, and also their security deployment is cheaper than biometrics. Smart cards are considered a two-factor authentication mechanism, which is based in something possessed, that

* Corresponding author. Tel.: +34 954 48 12 93; fax: +34 954 48 73 73.
E-mail addresses: jsanchez73@us.es (J. Sánchez-García), josgarcam@etsi.us.es (J.M. García-Campos), dgutierrezreina@us.es (D.G. Reina), storal@us.es (S.L. Toral), fbarrero@us.es (F. Barrero).

http://dx.doi.org/10.1016/j.future.2016.04.024
0167-739X/

is the card, and something known, a password [2]. Also, smart cards' cryptographic capacity and portability are two features that make them one of the most widely adopted authentication methods [3].

National Governments have promoted the use of this authentication method during the last decade, improving the existing identity (ID) cards to include an information security infrastructure for citizens. This is the case of Spain, where the personal ID card has become a smart card, named after *electronic ID* or eID from now on. The Spanish eID contains personal information within a microchip that can be used for information security purposes. The Spanish government is constantly promoting the electronic use of ID cards and has been distributing the API for developing new services based on it [4]. In addition to these resources, it can also be found a complete public key infrastructure (PKI), which is based on the Spanish ID card. This infrastructure is enabled and managed by the General Directorate of Police, known in Spanish as *Dirección General de la Policía*, DGP from now on. A complete description of the PKI used in the Spanish eID can be found in [5]. This PKI makes use of X.509 certificates [6] and the Online Certificate Status Protocol (OCSP) [7]. Thus, the Spanish eID enables any Spanish citizen to authenticate him against any service that requires identification, making use of its digital signature and also other security mechanisms. It is worth pointing out that the digital or electronic advanced signature is considered like the handwritten signature by the Spanish law.

Ad hoc networks [8], and also the broader concept of Internet of Things paradigm [9], require novel security mechanisms. These networks are susceptible of both common and brand-new security threats [10]. The infrastructure-less nature of ad hoc networks, the fact of every node acting as a router, the mobility and the use of wireless communications links are the main reasons of such new security threats. As mentioned in [11], it is difficult to ensure authenticity and confidentiality in ad hoc networks, but one way to establish secure communications in ad hoc networks is the use of authentication and certification services.

As occurs with routing protocols for ad hoc networks, there is not a perfect security solution for ad hoc networks that guarantees secure communications in every situation, so the solution highly depends on the scenario characteristics.

In this paper, the Spanish eID is used to develop On-SiteDriverID, a secure authentication scheme and its application for urban VANET scenarios. In those scenarios, the road authorities, for instance the police, may find useful to know the real identity of the driver before taking any action. The proposed security scheme is of high interest as it improves security in VANETs, specifically in situations where a direct, on-site and on demand authentication mechanism is required by a road authority.[1] Our solution of using the eID to secure specific communications in V2V communications complements current approaches for securing VANETs.

The primary objective of On-SiteDriverID is the creation of secure VANET scenarios through a mechanism that allows authorities to easily and automatically obtain drivers' identities. This avoids involving other entities (such as a judge) in the driver identification process which would make it complex and time-consuming. Consequently, On-SiteDriverID has a user-centric design from the point of views of the authorities which get the drivers' identities easily, from the point of view of the drivers which identify themselves against the authorities smoothly. This is simply accomplished by running the application that implements On-SiteDriverID security scheme.

The main contributions of this paper are twofold:

- The design of On-SiteDriverID, a secure authentication scheme and its application for VANET road authorities, based on the already in use Spanish eID smart cards.
- The evaluation of the proposed On-SiteDriverID on simulated realistic VANET urban scenarios.

The paper is organized as follows. Section 2 describes the related work. Section 3 describes the Spanish eID card and its public key infrastructure implementation. Section 4 describes the On-SiteDriverID application, its application scenario and its implementation. The simulation results of an urban scenario are presented in Section 5. Finally, some conclusions are drawn in the Section 6.

2. Related work

Several works describe the challenges in the field of secure ad hoc networks and the requirements for adapting traditional security mechanisms to ad hoc networks [12–14]. In [13], it is stated that a combination of cryptographic mechanisms can prevent the majority of attacks in ad hoc networks. In [11,15–17], the authors propose cryptographic mechanisms based on Public Key Infrastructure, PKI from now on, for securing ad hoc networks.

Regarding security mechanisms for VANETs, it is clear that there is a need for the information to be secured [18], as the messages contain relevant information such as driving routes and timestamps. Revealing this information associated with drivers' identity could be used for malicious purposes.

In [19], it is stated that PKI is one of the most suitable options for securing VANETs. Both authentication and non-repudiation are essential for identifying vehicle drivers liable for certain actions such as car accidents or traffic infractions. Even so, the security hardware architecture in VANETs was conceived with two main in-vehicle devices: (i) the event data recorder or EDR, for recording vehicles' critical data in emergency situations; and (ii) a tamper-proof device or TPD, responsible for all the cryptographic operations and the storage of private keys and certificates.

In [19], the authors also propose a Vehicular Public Key Infrastructure or VPKI. In this approach, the Certificate Authorities (CAs) will issue public–private key pairs for each vehicle, and at the same time, each vehicle would have a list of anonymous, but certified, keys that change frequently and are like one-time keys. This will maintain the drivers' privacy in order to protect them from several threats, but at the same time has to allow the authorities to reveal the message's source, i.e. the vehicle, for driving liability purposes. This is known as conditional privacy or conditional anonymity in [18]. Usually the approval of a judge is required in order to reveal the real identity of the driver [19]; other approaches involve several entities in this process, such as [20], which defines a Tracing Manager for approving the search of real identities and the Membership Manager which performs the search of the real identity in a database.

As stated in [21], the authentication schemes using smart cards are one of the simplest and most convenient authentication methods for secure data communications in insecure network environments. In [22], a protocol called PAAVE is described. This protocol uses smart cards for securing VANETs communications. In PAAVE, the vehicle firstly authenticates itself against a Road Side Unit (RSU) through a public key cryptography procedure in which the RSU shares with the vehicle a session key; the session key is shared by all the vehicles authenticated against the same RSU so they can read other vehicles messages anonymously, i.e. the RSU is the only entity that could know the real identity of the driver. However, the vehicle's real identity is limited to knowing the driving license to identify the driver/owner. PAAVE does not clarify if a person driving a vehicle, and not being the owner of it, could be identified.

[1] We call "authority" in this paper to any public organization with authority in the domain of road traffic. Examples of these are the police, and other emergency bodies like firefighters and paramedics.