COMPUTERS & SECURITY 60 (2016) 193–205

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

# An autonomous privacy-preserving authentication scheme for intelligent transportation systems

*Victor Sucasas* *, *Georgios Mantas*, *Firooz B. Saghezchi*, *Ayman Radwan*, *Jonathan Rodriguez*

*Instituto de Telecomunicações, Aveiro, Portugal*

ARTICLE INFO

*Article history:*
Received 29 September 2015
Received in revised form 18 March 2016
Accepted 19 April 2016
Available online 3 May 2016

*Keywords:*
Privacy
Authentication
Pseudonyms
Vehicular
Intelligent transportation systems

ABSTRACT

Privacy-preservation is of paramount importance for the emerging Intelligent Transportation System (ITS) applications, such as traffic monitoring and road safety. These applications require regular transmission of messages among vehicles or between vehicles and back-end servers. The received messages should be authenticated so that messages from malicious or malfunctioning entities can be detected and discarded. However, this requirement poses a challenge in terms of location privacy, since the user's identity is sent in clear text in the transmitted messages, and thus it can be linked to the vehicle's position. Cryptographic pseudonyms are advocated as computationally efficient solutions for preserving the privacy of vehicles' location. However, pseudonym-based systems require permanent contact between vehicles and a trusted authority (TA) to periodically renew the pseudonyms. This might cause network congestion or be infeasible in some situations due to the lack or scarcity of deployed infrastructure. In this paper, we address this challenge by proposing an autonomous privacy-preserving authentication scheme, where vehicles only need to contact the TA once; afterward, they can renew their pseudonyms by themselves without communicating with the TA. To the best of our knowledge, this is the first authentication scheme providing vehicles with the capability to renew their pseudonym sets without requiring permanent contact with a TA.

© 2016 Elsevier Ltd. All rights reserved.

## 1. Introduction

Nowadays, vehicular communication technology is envisioned under the umbrella of the Internet of Everything (IoE) paradigm, which foresees vehicles as intelligent machines that are able to process and share information with other vehicles and the smart city infrastructure (Naufal et al., 2014). In the near future, vehicles will be equipped with on board communication units (OBUs), allowing on demand vehicle-to-vehicle (V2V) communications. Moreover, roadside units (RSUs) will also be deployed alongside roads to enable vehicle-to-infrastructure (V2I) communications. This new paradigm has opened the possibility for a wide range of Intelligent Transportation System (ITS) applications, such as roadway operations and maintenance, traveler information, traffic monitoring and road safety. Traffic monitoring and road safety have raised the interest of the research community due to its application potential (Olariu and Weigle, 2009). Traffic monitoring, where vehicles will send traffic reports to a back-end server, will be used to provide accurate and on-demand traffic information for smart navigation, which will enable intelligent transportation services directly

* *Corresponding author.*
*E-mail address:* vsucasas@av.it.pt (V. Sucasas).
http://dx.doi.org/10.1016/j.cose.2016.04.006
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

impacting the society's economy (Bekiaris and Nakanishi, 2004; Juan et al., 2006). On the other hand, road safety applications will enable on-demand message transmission, among vehicles and between vehicles and infrastructure, that will include information such as traffic light status, vehicle movements, and collision avoidance or priority vehicles notification, which will be a major advance toward safe driving. Hence, ITS applications have opened a new vision of vehicular communication technology, as a part of the IoE paradigm, that brings major benefits for the society.

However, vehicular communication technology faces new technical challenges, related with the security–privacy tradeoff, that hinders its practical implementation. Due to the nature of the information transmitted by vehicles, message authentication, which is also called data-origin authentication, is one of the most important security requirements that should be satisfied so that misbehaving entities (e.g. malicious OBUs) can be detected. Particularly, message authentication allows misuser detection by enabling verification of the message sender's identity and data transmission tracking. Misusers can be malfunctioning or malicious OBUs that spread false information, such as false traffic reports, which can affect navigation systems or trigger false emergency alarms. However, OBU's identification can threaten user's location privacy, since it allows eavesdroppers to track people's activities (travel routes, timetables, destinations, etc.) by linking the location information of transmitted messages to the transmitter's real identity. Therefore, it is to provide a mechanism to support conditional privacy. Namely, the vehicles (i.e. OBUs) should be allowed to transmit messages anonymously; the messages should be validated by receivers (RSUs or OBUs), and a trusted authority (TA), acting as a third party, should be able to retrieve the vehicle's real identity in case of misbehavior.

Violation of user's privacy can discourage users from adopting this new technology. Hence, privacy-preserving mechanisms are of paramount importance to foster a rapid penetration of vehicular communication technology in the market. The state-of-the-art includes a number of privacy-preserving mechanisms, based on anonymous credentials (Raya and Hubaux, 2005), Public Key Infrastructure (Liu et al., 2007), group signatures (Lin et al., 2007), cooperation (Sampigethaya et al., 2007) and pseudo-identities (Lu et al., 2013). Among existing solutions, it is the latter, pseudonym-based schemes, which provide the more efficient approach in terms of computational complexity and latency. However, existing pseudonym-based solutions have a common disadvantage; they require a permanent contact with the TA that is in charge of granting and renewing the cryptographic pseudonyms to vehicles. In this paper we extend our work in Sucasas et al. (2015) and propose an autonomous privacy-preserving authentication scheme that overcomes this constraint, since it only requires the vehicles to contact the TA once. Moreover, in this paper we propose efficient anonymity revocation mechanisms supported by our privacy-preserving authentication scheme.

To the best of the authors' knowledge, the proposed privacy-preserving authentication scheme is the first that achieves location privacy, conditional privacy, efficient revocation, unlinkability and forward unlinkability, and at the same time it is fully autonomous. The autonomous feature is of paramount importance since it allows the system to work even in scenarios where vehicles do not have a permanent contact with the TA. This scenario is likely to happen in situations of network congestion or lack of infrastructure.

Following the introduction, the paper is structured as follows: Section 2 details the related work; Section 3 provides the system model; Section 4 defines the security objectives; Section 5 caters for the mathematical preliminaries to understand the privacy-preserving authentication scheme proposed; Section 6 provides a thorough description of the proposed scheme; the anonymity revocation mechanisms are detailed in Section 7; the security analysis of the proposed scheme is included in Section 8; Section 9 describes the mechanism to address synchronization offsets; in Section 10 the autonomy of the proposed scheme is discussed; Section 11 provides a comparison between the proposed scheme and other anonymous credential systems with similar functionality; and finally, Section 12 concludes this paper.

## 2. Related work

Several research works have previously suggested mechanisms to authenticate data transmissions while ensuring conditional privacy in VANETs, such as the work in Raya and Hubaux (2005) where authors propose a system based on anonymous certificates. These certificates are distributed by a certification authority (CA) to the vehicles and the vehicles use the certificates to sign messages anonymously. The CA keeps track of the vehicles' real identities, serial number (SN), and the associated certificates in order to recover the user's real identity in case of misbehavior. The CA stores 43,800 certificates that are pulled randomly by users. The scalability problem is however evident in this system since vehicles are required to contact the CA every time they want to get a new certificate, which are short-lived and discarded after a short period of time. Moreover, in case of detecting misbehavior the CA must perform an exhaustive search on the certificate pool to find the pair (Certificate, SN), which reduces the efficiency of the revocation mechanism. However, this approach based on digital signatures is more efficient than any asymmetric counterpart, since there is no need for preliminary handshakes for key establishment between vehicles at the time of transmitting authenticated messages.

Similar approach was also suggested by the work in (Liu et al., 2007), which provided a Public Key Infrastructure (PKI) where the CA distributes public/secret key pairs to the users to sign messages. The vehicles can own a set of different key pairs to mislead eavesdroppers. The main disadvantage is as well the scalability since the vehicles must store a big set of key pairs, and the revocation mechanism is not efficient due to the exhaustive search required to recover the key pairs of each user.

A different approach based on group signatures was suggested in Calandriello et al. (2007), Lin et al. (2007), and Lu et al. (2008). Group signature schemes allow the association of several private keys to one public key, hence a receiver can verify the signature and associate such signature to a group of vehicles, but the receiver cannot distinguish the sender of the message inside the group. This approach also provides conditional privacy, since the CA can still track the real identity

Download English Version:

https://daneshyari.com/en/article/456389

Download Persian Version:

https://daneshyari.com/article/456389

Daneshyari.com