Ad Hoc Networks 37 (2016) 122–132

Contents lists available at ScienceDirect

Ad Hoc Networks

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

PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks[☆]

David Förster[a,*], Frank Kargl[b,c], Hans Löhr[a]

[a] Robert Bosch GmbH, Germany
[b] Ulm University, Germany
[c] University of Twente, The Netherlands

ARTICLE INFO

Article history:
Received 28 February 2015
Revised 25 September 2015
Accepted 29 September 2015
Available online 8 October 2015

Keywords:
Intelligent transportation systems
Vehicular ad-hoc networks
Location privacy
Pseudonym schemes
Security
Anonymous credentials

ABSTRACT

Pseudonym certificates are the state-of-the-art approach for secure and privacy-friendly message authentication in vehicular ad-hoc networks. However, most of the proposed pseudonym schemes focus on privacy among participants. Privacy towards backend providers is usually (if at all) only protected by separation of responsibilities. The protection can be overridden, when the entities collaborate, e.g. when revocation of long-term credentials is required. This approach puts the users' privacy at risk, if the backend systems are not fully trusted.

We propose PUCA – a scheme that provides full anonymity for honest users, even against colluding backend providers. The scheme uses anonymous credentials for authentication with the backend, while leaving the communication among vehicles and with road side units unchanged and in compliance with existing standards. For removal of misbehaving vehicles from the system, we leverage a privacy-friendly revocation mechanism, that does not require resolution of pseudonyms. With our scheme, we demonstrate that strong and verifiable privacy protection in vehicular networks can be achieved, while fulfilling common security requirements, such as sybil-resistance and revocation.

1. Introduction

Inter-vehicular communication (*V2X communication*, comprising vehicle-to-vehicle and vehicle-to-infrastructure communication) is expected to improve road safety as well as to deliver a more pleasant driving experience. After extensive research [2,3] and standardization efforts [4,5], car makers have announced the first V2X-enabled models for 2017 [6]. In the U.S. there are ongoing efforts in legislation to require V2X-based safety functions for new vehicles [7]. Besides legislation, user acceptance is a crucial success factor for rapid deployment. Privacy concerns have been raised in the media repeatedly and need to be addressed.

Cooperative awareness messages, sent via short-range radio communication, are the foundation of many V2X based safety functions. Broadcasted several times a second, these messages contain information such as the vehicle's current GPS position, velocity, and direction. This information can be used by other vehicles for safety features, such as Co-operative Collision Avoidance, as well as by traffic control infrastructure to implement traffic efficiency applications. Message authentication is needed as forged messages could endanger travelers' physical safety, e.g. by faking an imminent collision and provoking an autonomous emergency braking. To ensure only authorized parties can participate in the network, all messages are signed cryptographically. This threatens the users' privacy as the signing keys are unique identifiers, that expose them to tracking attacks by anybody

[☆] This article is a revised and extended version of work that was presented at VNC 2014 [1].

[*] Corresponding author. Tel.: +4971181149827.
E-mail addresses: david.foerster@de.bosch.com (D. Förster), frank.kargl@uni-ulm.de (F. Kargl), hans.loehr@de.bosch.com (H. Löhr).

http://dx.doi.org/10.1016/j.adhoc.2015.09.011
1570-8705/© 2015 Elsevier B.V. All rights reserved.

who receives their messages (no matter if the receiver is a legitimate participant of the V2X network or not). Tracking users' movements by their messages an attacker could infer frequently visited locations such as their place of work or home, as well as personal preferences, or even their identity [8–10].

In order to protect the users' privacy, a scheme employing changing *pseudonym certificates* has been proposed [2,11] and is included in the recent standards of the ETSI Technical Committee on ITS [4] for Europe and the IEEE 1609 working group [5] for the U.S. Instead of using one fixed certificate per user, messages are signed using short-lived pseudonym certificates. These are changed periodically in order to prevent tracking across pseudonym changes. The users' privacy towards authorities can be protected by a separation of duties between the Pseudonym CA (PCA) and the Long-term CA (LTCA) as suggested by the CAR 2 CAR Communication Consortium [12]. If required, they can cooperate to resolve a user's identity from his pseudonyms (*pseudonym resolution*) and exclude him from the system. The privacy offered by this approach obviously depends on the authorities' correct behavior and can easily be subverted, e.g. by fraudulent operators. If regulations change, the user may be faced with unexpected use of his mobility data. In particular, the approach is insufficient in an environment where the government fails to adequately protect the rights of individuals. Beyond, car manufacturers in the US have expressed their favor of drivers' anonymity over liability in order to protect themselves from lawsuits by drivers who's identity has been resolved [13].

In order to provide optimal privacy protection and prevent the problems stated above, we should aim for a system where privacy of vehicle owners has priority even over interest of other stakeholders like law enforcement. Pseudonym resolution must not be possible, that means nobody else but the owner should be able to identify a vehicle just based on recorded message signatures and pseudonyms. Still, revocation is required to protect the V2X system from misbehaving vehicles, that are sending invalid messages, either unintentionally (e.g. due to a technical defect) or intentionally (e.g. by manipulation of sensor data). Of course, with the consent of the legitimate vehicle owner, it should always be possible to revoke a vehicle's credentials that authorize its participation in the network.

Our contribution

We present PUCA[1], a pseudonym scheme where the user's privacy is protected by cryptographic methods instead of separation of responsibilities. When obtaining and using pseudonyms he remains fully anonymous. PUCA is built on top of the CAR 2 CAR Communication Consortium's basic pseudonym scheme and only changes how pseudonyms are obtained, not how they are used. Therefore, it is fully compatible with the currently standardized approach and can be deployed alongside existing solutions.

Based on an earlier publication [1] we propose several extensions: first, we are integrating a privacy-friendly revocation mechanism based on secure hardware that was originally proposed in [14]. The extenden PUCA scheme with the REWIRE revocation mechanism integrated allows exclusion of misbehaving vehicles based on their messages, which is not possible in the original PUCA scheme, and which does not require resolution of pseudonyms. As a further extension, we propose two alternative implementation variants, that use different credential schemes and promise increased efficiency. One comes at the cost of slightly lower privacy guarantees for revoked users, while for the other one, efficient revocation mechanisms are still under development.

To the best of our knowledge, we are the first to propose a system that gives vehicle owner's privacy absolute priority while still enabling revocation of misbehaving participants.

We present the high-level system model of a V2X network in the Section 2 and lay out the requirements for our approach in Section 3. In Section 4 we describe other pseudonym schemes and related work. The building blocks for our scheme are introduced in Section 5. The PUCA scheme is presented in Section 6 where we also describe extensions and implementation variants. We close with an evaluation and discussion in Section 7 and provide a conclusion in Section 8.

2. System model and scenario

We use the following system model of an Intelligent Transport System (ITS). Participating vehicles are equipped with a V2X onboard unit (OBU), that contains a trusted component (TC) to store secret keys and perform security-sensitive operations. Prior to deployment, an IVS is registered with the Long-term CA (LTCA) that keeps track of all participants within the ITS. The Pseudonym CA (PCA) issues pseudonym certificates to the participants which they use to secure their communication. The Revocation Authority (RA) receives reports about misbehaving vehicles and may revoke their permission to participate in the system. The interactions within an ITS can be split into five different phases, which we will later refer to. Fig. 1 shows an overview over the entities' interactions.

1. *Initialization:* Global system setup; this phase is only executed once when the ITS is established.
2. *Setup-Vehicle:* Add a new IVS to the ITS and provide it with a long-term authentication token ⓐ.
3. *Obtain-Pseudonyms:* Is executed by the IVS to refresh its supply of pseudonyms. It obtains pseudonyms from the PCA, authenticating with its long-term credential ⓑ. The PCA may rely on the LTCA to validate the authentication ⓒ.
4. *Communication:* Vehicles communicate among each other using the pseudonym certificates to authenticate their messages ⓓ.
5. *Revocation:* Misbehavior reporting ⓔ and removal of misbehaving vehicles from the system ⓕ. Terminology: *Revocation* refers to the (forced) removal of a misbehaving participant from the system, whereas *invalidation* of a credential can be triggered either by misbehavior or by a user's request to leave the system.

3. Requirements and constraints

We base our requirements on the general requirements for V2X pseudonym schemes outlined by Schaub et al. [15].

[1] Pseudonyms with User Controlled Anonymity; pronounced *pooka*, Irish for spirit/ghost