Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 377 – 384

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

HPDM: A Hybrid Pseudonym Distribution Method for Vehicular Ad-hoc Networks

Abdelwahab Boualouache[a,*], Sidi-Mohammed Senouci[b], Samira Moussaoui[a]

[a]*Department of Computer Science, RIIMA laboratory, USTHB University BP 32 El Alia Bab Ezzouar, Algiers, Algeria*
[b]*DRIVE Laboratory, University of Burgundy, 58027 Nevers, France*

Abstract

Protecting the location privacy of drivers is still one of the main challenges in Vehicular Ad-hoc Networks (VANETs). The changing of pseudonym is commonly accepted as a solution to this problem. The pseudonyms represent fake vehicle identifiers. Roadside Units (RSUs) play a central role in the existing pseudonyms distribution solutions. Indeed, the VANET area should totally be covered by RSUs in order to satisfy the demand of vehicles in terms of pseudonyms. However, the total coverage is costly and hard to be achieved, especially in the first phase of VANETs deployment. In addition, RSUs could be overloaded due to the large number of pseudonyms requests that could be received from vehicles. In this paper, we propose a new hybrid pseudonyms distribution method, called HPDM that relies not only on RSUs but also on vehicles to perform the pseudonyms distribution. The analysis demonstrate that HPDM is privacy and accountability preserving. The performance evaluation of the proposed method is carried out using veins framework based on OMNet++ network simulator and SUMO mobility engine and shows its feasibility.

Peer-review under responsibility of the Conference Program Chairs
Keywords: VANETs; Security; Location privacy; Pseudonyms distribution.

1. Introduction

Vehicular Ad-hoc networks (VANETs) are considered as a subclass of Mobile Ad-hoc networks (MANETs)[1]. The mobile nodes represent the vehicles, which communicate to each other and to fixed infrastructure points, called Roadside Units (RSUs). Many interesting applications are enabled due to these communications. The existing applications allow not only to preserve road safety (e.g., emergence reporting and collision warning) but also to provide traffic efficiency and entertainment[2].

The VANETs are exposed to a variety of attacks that could cause serious damages both on VANET system and users. Location tracking is one of the attacks that can hinder the deployment of VANETs[3]. The problem is coming from the authenticated safety-related messages that are broadcasted with a high frequency and in clear text. Indeed, several studies demonstrated that a simple passive adversary could collect these messages and relate them according

* Corresponding author. Tel.: +213-21-24-76-07 ; fax: +213-21-24-76-07
E-mail address: aboualouache@usthb.dz

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.199

to vehicles' identifiers[4]. The adversary could then generate a movement trajectory of each vehicle to know the emplacements visited by the driver over time, which violates the driver's privacy[5].

The changing of pseudonym is accepted as solution to this problem. The pseudonyms represent fake vehicle identifiers. The vehicle is equipped by a set of pseudonyms, where each pseudonym is used for a limited period of time. An expiry pseudonym is changed by a new one and cannot generally be reused again. The current 1609.2 standard is based on a public key infrastructure (PKI)[6]. The pseudonyms are public keys certified by the trusted authority (TA) and generated using one of the following methods[7]. (i) They could be generated by vehicles themselves, sent to TA to be signed and sent back to vehicles through RSUs, (ii) They could be generated by RSUs instead of vehicles, sent to TA to be signed, and then distributed by RSUs to the vehicles, (iii) They could be generated by a third party, sent to TA to be signed, and distributed by RSUs, and finally (iv) They could generated and singed by TA, and distributed to vehicles by RSUs. In addition, due to the accountability (liability) issues only the TA can still know the link between the real identifier of a vehicle and the set of pseudonyms associated to it.

In[8], Raya and al. estimated the number of pseudonyms needed by a vehicle. They suggested to provide about 43,800 pseudonyms per year for a vehicle that is used 2 hours, in average, per day and changes its pseudonym every 1 minute. However, the number of needed pseudonyms mainly depends the frequency of pseudonym changing and the use of vehicle. Obviously, the more pseudonym changing frequency is, the more location privacy protection is achieved. This is on condition that pseudonym chaining frequency is not less then a certain threshold[9]. Therefore, a huge number of pseudonyms should be stored by vehicles, which can exceed vehicle storage capabilities. For this reason, the existing solutions suggested that pseudonyms should be requested according to the vehicle demand. Indeed, the RSUs play a central role in these solution because they are not only used to request the pseudonyms but also to distribute them. These solutions assume that the VANET area is already covered by RSUs. This assumption might generate a high deployment costs and it is hard to be achieved, especially in the first phase of the VANET deployment. In addition, the RSUs could be overloaded due to frequent pseudonyms requests and distributions operations.

To address these limitations, in this paper, we propose a new hybrid pseudonyms distribution method, called HPDM. HPDM is based not only on RSUs but also on vehicles to distribute the pseudonyms. It aims to involve vehicles in the pseudonyms distribution to ensure the availability of pseudonyms (e.g. in the case of luck in the number of deployed RSUs) and to reduce the overload on RSUs. The analysis demonstrated that proposed method is privacy and accountability preserving. The performance evaluation is carried out using veins framework based on OMNet++ network simulator and SUMO mobility engine. The simulation results show the feasibility of the proposed method.

Our contribution is then threefold:

- We propose a new pseudonym pseudonyms distribution method, called HPDM that is based both on vehicles and RSUs.
- We suggest to integrate HPDM with Urban Pseudonym Changing Strategy (UPCS)[10][11].
- We evaluate the performance of HPDM using veins framework based on OMNet++ network simulator and SUMO mobility engine.

The remainder of this paper is organized as follows. Section 2 describes some related work. The proposed method (HPDM) is presented in Section 3. HPDM analysis are given in Section 4 and performance evaluations are presented in Section 5. The conclusion is given in Section 6.

2. Related work

In[12], the authors investigated the optimal strategy for refilling pseudonyms. Two pseudonyms refill strategies were then identified : refilling a large number of pseudonyms at one time (strategy 1) or refilling a small number of pseudonyms several times (strategy 2). After citing the benefits and the drawbacks of each strategy, the authors concluded that the strategy 2 has more benefits than the strategy 1. For this reason, they proposed a new pseudonym refill solution called pseudonym-on-demand (POD). POD is based on the strategy 1, where vehicles send their requests to the pseudonym provider (PP) through RSUs when they need new pseudonyms. However, as mentioned by the authors themselves the strategy 1 has a high cost of deployment. In[7], the authors evaluated the amount of data that