


Location-Privacy Evaluation Within the Extreme Points Privacy (EPP) Scheme for VANET Users

Messaoud Babaghayou, University of Tlemcen, Tlemcen, Algeria

Nabila Labraoui, University of Tlemcen, Tlemcen, Algeria

Ado Adamou Abba Ari, University of Maroua, Maroua, Cameroon, & LI-PaRAD Lab, Université Paris Saclay, University of Versailles Saint-Quentin-en-Yvelines, Versailles, France

 <https://orcid.org/0000-0001-5660-0660>

ABSTRACT

The main purpose of designing vehicular ad-hoc networks (VANETs) is to achieve safety by periodically broadcasting the vehicle's coordinates with a high precision. This advantage brings a threat represented in the possible tracking and identification of the vehicles. A possible solution is to use and change pseudonyms. However, even by changing pseudonyms, the vehicle could still be tracked if the adversary has a prior knowledge about the potential start and end points of a particular driver who has social interactions (e.g., with neighbors) which introduces the concept of vehicular social networks (VSNs). This article extends the authors previous work, namely: "EPP Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks," which exploits the nature of the end points that are common between VSN users in order to create shared zones to anonymize them. The extension is represented by (a) the evaluation of the enjoyed location privacy of VSN users after quitting the district in addition to (b) detailing the used environment during the evaluation.

KEYWORDS

Anonymity, Home Identification, Location Privacy, VSN

INTRODUCTION

Background

The emerging of wireless technologies had big impact on different fields which led to the birth of vehicular social networks (VSNs), one of the wireless technology applications in the field of vehicles; or the so-called vehicular ad-hoc networks (VANETs). The evolution and enhancement of VANET capabilities has significant influence on the successfulness of the Intelligent Transportation Systems (ITSs) (Lu et al., 2012; Mfenjou et al., 2018; Ngossaha et al., 2018). In VANETs there exist two kinds of communications and they are self-describing: Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). In order to be able to communicate, vehicles are equipped with onboard units (OBUs); specific devices that allow vehicles to: communicate, process data, receive GPS signal and use variant sensors. For a better system, vehicles may often communicate with central infrastructures. Such infrastructures may be roadside units (RSUs) (Al-Kahtani, 2012). VANET applications may be diverse; however, the number one reason for what it was proposed is to reduce the number of crashes

DOI: 10.4018/IJSITA.2019040103

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

and fatalities (Sampigethaya et al., 2005). The vehicle will succeed to do so by enabling periodic broadcasts (also called beacons or heartbeat messages) so that the vehicle includes its status in kind of location, speed, velocity and other information that can lead the neighborhood for better environment knowledge and that is the Basic Safety Messages (BSMs). According to the standard SAE J2735, the frequency of BSMs is set to be each 100ms with a 300 meter transmission range (Corser et al., 2013).

Problem Definition

The frequent and precise location provided by BSMs helps enormously the safety-related applications but, at the same time, reduces dramatically the privacy of VSN users since the BSMs' location is not encrypted for fast reaction and less delay (it is the requirements of safety-applications). Thus, any adversary willing to monitor and track the VSN users can do that in real time with just the possession of eavesdropping station(s) which does not cost him a lot and is not easily detectable. Among the solutions to defend against such privacy threats we find the use of pseudo-identifiers (pseudonyms) instead of the unchangeable real identifiers. This last solution increases the anonymity of drivers, but the adversary can match the real identity with the pseudonym by observing the trips of the vehicle. Making the pseudonyms changeable over time can be seen as an acceptable solution since the adversary can no longer see just one pseudonym. However, even so, if the vehicle changes its identifier in inappropriate situation (e.g., alone inside a set of vehicles), the adversary here can easily link the old (vanished) pseudonym with the new (emerging) one. For this last problem, the cooperation between vehicles by making a synchronous pseudonym change was the best countermeasure since the adversary will be confused on the new pseudonym of a vehicle inside the set of potential targets. Unfortunately, because of the exact and frequent periodic location, the adversary can predict the moves of the monitored vehicles inside the region of interest which helps him to link each new pseudonym with the old one for all those vehicles even though the changes were done simultaneously. For this advanced challenge, the concept of silent period was proposed in (Huang et al., 2005) for wireless networks and it is explained as a transition period of time between the newly changed pseudonym and the old one. By this definition, the vehicles will keep silent and during this silence time, they do change their pseudonyms and not sending BSMs until the time is ended. When the time is ended, the vehicle is allowed to use the new changed pseudonym. This technique was integrated in the field of VANETs in works done in (Sampigethaya et al., 2005; Butty'an et al., 2009). Silent periods highly enhance the privacy of VSN users but with the cost of safety, that is the sacrificing of privacy or the trade-off between safety and privacy. For this reason, such trade-off was widely debated.

Authors' Contributions and Organization of the Paper

In this paper, which is an extension of our previous work presented in (Babaghayou et al., 2019), (a) we evaluated the achieved location privacy after the targeted user leaves his district. The evaluation is done by using the well-known privacy-metric, the Anonymity Set Size (ASS) in a mix-zones system. (b) In addition, we contribute by detailing the environment used and the exact day time-period (which is the rush hours period) in where and when the evaluation took place. EPP takes into account the number of gates and the possible headings from each gate, the definition of these concepts will be further explained. This analytical study is accompanied by simulations in order to evaluate the effectiveness of EPP scheme. The remainder of this paper is organized as follows: next in section 2, we present some related work. Then, we describe the proposed EPP strategy in section 3. The experimental results in addition to giving more details about the evaluation are presented later in section 4. Finally, we conclude the paper in Section 5.

Related Works

It is important to mention that there are other potential solutions to defend against location privacy and identification (Corser et al., 2016). However, they may not be able to be used in the field of VANET due to the special features of the last one, we mention the four of them briefly as:

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/location-privacy-evaluation-within-the-extreme-points-privacy-epp-scheme-for-vanet-users/241867

Related Content

Citizen Journalism: How Technology Transforms Journalism Business through Citizen-Reporters in Nigeria

Olubunmi P. Aborisade, Caroline Howard, Debra Beasley and Richard Livingood (2011). *International Journal of Strategic Information Technology and Applications* (pp. 1-11).

www.irma-international.org/article/citizen-journalism-technology-transforms-journalism/54706

A CASE Tool Evaluation and Selection Methodology

Aniruddha Guha Biswas, Raveesh Tandon and Anurika Vaish (2013). *International Journal of Strategic Information Technology and Applications* (pp. 48-60).

www.irma-international.org/article/a-case-tool-evaluation-and-selection-methodology/89357

Enterprise Resource Planning Systems in a Global Environment

Paul Hawking (2010). *Strategic Information Systems: Concepts, Methodologies, Tools, and Applications* (pp. 382-396).

www.irma-international.org/chapter/enterprise-resource-planning-systems-global/36701

An Integrated RFOS Model for Risk Assessment on Real Time Operating System

Prashant Kumar Patra and Padma Lochan Pradhan (2014). *International Journal of Strategic Information Technology and Applications* (pp. 27-43).

www.irma-international.org/article/an-integrated-rfos-model-for-risk-assessment-on-real-time-operating-system/122827

Introduction to Strategic Alignment

Ratmond Papp (2001). *Strategic Information Technology: Opportunities for Competitive Advantage* (pp. 1-24).

www.irma-international.org/chapter/introduction-strategic-alignment/29758