Chapter 13
Privacy Protection in Vehicular Ad-Hoc Networks

Gongjun Yan
University of Southern Indiana, USA

Bhed Bahadur Bista
Iwate Prefectural University, Japan

Danda B. Rawat
Georgia Southern University, USA

Wu He
Old Dominion University, USA

Awny Alnusair
Indiana University – Kokomo, USA

ABSTRACT

The first main contribution of this chapter is to take a non-trivial step towards providing a robust and scalable solution to privacy protection in vehicular networks. To promote scalability and robustness the authors employ two strategies. First, they view vehicular networks as consisting of non-overlapping subnetworks, each local to a geographic area referred to as a cell. Each cell has a server that maintains a list of pseudonyms that are valid for use in the cell. Each pseudonym has two components: the cell's ID and a random number as host ID. Instead of issuing pseudonyms to vehicles proactively (as virtually all existing schemes do) the authors issue pseudonyms only to those vehicles that request them. This strategy is suggested by the fact that, in a typical scenario, only a fraction of the vehicles in an area will engage in communication with other vehicles and/or with the infrastructure and, therefore, do not need pseudonyms. The second main contribution is to model analytically the time-varying request for pseudonyms in a given cell. This is important for capacity planning purposes since it allows system managers to predict, by taking into account the time-varying attributes of the traffic, the probability that a given number of pseudonyms will be required at a certain time as well as the expected number of pseudonyms in use in a cell at a certain time. Empirical results obtained by detailed simulation confirm the accuracy of the authors' analytical predictions.

DOI: 10.4018/978-1-4666-4691-9.ch013

1. INTRODUCTION AND MOTIVATION

Recent statistics show that in 2008 there were over 238 million passenger cars and trucks in the US, a vehicular fleet that increases yearly by almost seven million new cars (US Department of Transporation, Research and Innovative Technology Association, 2011). In an effort to help their vehicles compete in the marketplace, car and truck manufacturers are offering more and more potent on-board devices, including powerful computers, a large array of sensors, radar devices, cameras, and wireless transceivers. These devices cater to a set of customers that expect their vehicles to provide a seamless extension of their home environment populated by sophisticated entertainment centers, access to Internet and other similar wants and needs (Arif et al., 2012; Wang, 2010). The powerful on-board devices support new applications, including location-specific services, on-line gaming, delivering multimedia content and various forms of mobile infotainment made possible by the emergence of vehicular networks (Li et al., 2005). In the near future, a vehicle will be capable of intelligent data-mining based on its owner's preferences (Wen et al., 2011), identifying favorite hotels, shopping malls, restaurants (e.g. Chinese restaurants featuring Szechuan-style cuisine) and, perhaps, a convenient parking lot (Yan et al., 2011). Knowing the driver's preferences, around lunchtime the vehicle will automatically send queries to the roadside infrastructure and other vehicles to find a list of Chinese restaurants nearby (Li et al., 2005; Wen et al., 2011).

The increased Internet presence that enables the above applications invites various forms of privacy attacks mounted by unscrupulous characters in order to identify the location of various parties that might be exploited for financial gains. One well-known such attack has for goal to establish that a family is away from their home so that a burglary can be perpetrated; yet another one has for goal to obtain compromising information that can later be used to blackmail the driver. Invariably, these privacy attacks are mounted by exploiting the various forms of correlation that exist between the identity of a vehicle and that of its driver.

While a great deal of research has been devoted to information security in vehicular networks (Choi et al., 2006; Hubaux et al., 2004; Raya et al., 2006; Sun et al., 2010a, Yan et al., 2008; Yan et al., 2009a), far less attention has been given to privacy issues (Xie et al., 2010; Yan and Olariu, 2011). One of the reasons for this state of affairs is the mistaken idea that the privacy issues encountered in vehicular networks are similar to the ones experienced in cellular telephony and WiFi communications and, therefore, the same solutions can be applied. For example, it has been suggested that instead of radio communications, drivers use their cell phones to access the Internet. However, using a cell-phone while driving may not only be illegal, as it is currently in some states, it has also been identified as one of the principal causes of traffic accidents.

A more careful analysis reveals that many of the privacy challenges experienced in vehicular networks are either brought about or exacerbated by the increased on-line presence of drivers, the high mobility of the vehicular fleet as well as the short transmission requirements of the Dedicated Short Range Communications (DSRC) limiting transmission to between 300m and 1,000m (Yan and Olariu, 2011).

In summary, there are unique challenges to privacy protection in vehicular networks including (Yan et al., 2013; Arif et al., 2012):

- **High Vehicular Mobility:** This challenge renders the network connection inherently unstable and make pseudonyms difficult to manage and update (Yan and Olariu, 2011; Rawat et al., 2011). Therefore, the communication is not reliable;
- **Large and Fluctuating Population of Vehicles:** This challenge will make the scalability requirement of privacy solutions difficult to meet (Yan et al., 2012);