Location Privacy in Vehicular Networks

Karim Emara

Department of Informatics
TU Munich
Munich, Germany
emara@in.tum.de

Abstract—Location privacy is one of the main challenges in vehicular ad hoc networks (VANET), which aim to protect vehicles from being tracked. Most of research work concern changing pseudonyms effectively to avoid linking messages through them. However, the sensitive information the vehicles send periodically in beacon messages make them vulnerable to tracking even if beacons are totally anonymous. In this thesis, we consider how to protect vehicles from being tracked while they are sharing sensitive information in beacons. The high beacon rate, high precision of shared information and strict latency constraints of application are the main challenges to our objective. We propose two solutions for this issue. The first one is to send the precise information only every period of time while sending inaccurate beacons in between. The second solution is to use secure group communication to prevent attacker from overhearing broadcast information. Both choices will be implemented and evaluated against a state-of-the-art tracker.

Keywords—VANET; Location privacy; Vehicle tracking;

I. INTRODUCTION

Privacy in vehicular networks concerns user anonymity, unlinkability and protecting her location information from tracking. To protect the driver's identity, previous work suggested to provide each vehicle with a set of pseudonyms [1]. Vehicles should use a different pseudonym every period of time according to a change policy so that users cannot be identified through messages sent from their vehicles. However, due to the beacons sent frequently (up to 10 Hz) containing accurate position, speed, acceleration and heading [2] along with a pseudonym, vehicles are vulnerable to tracking. Wiedersheim et al. [3] claim that vehicles can be tracked with an accuracy of almost 100% in some cases. This means that even changing pseudonyms does not effectively protect the location privacy of vehicles due to the precise frequent information they send. Although revealed vehicles traces are anonymous, further correlation between real identities and those anonymous traces can be achieved as Golle and Partridge claimed in [4] which may lead users to reject VANET usage at all.

In this thesis, we study location privacy in vehicular networks and how to protect broadcast information from misuse. We concern beaconing communication pattern that is mostly used in safety applications. We assume a passive global observer who can eavesdrop every message sent in the wireless channel. Although, many research work used analytic metrics for privacy evaluation, we aim to evaluate it against an empirical state-of-the-art tracker to reflect the realistic capabilities of the adversary.

II. OBJECTIVES

We aim to protect vehicles from tracking which is possibly accomplished by exploiting information sent in beacon messages. This goal is divided into the following objectives:

1) Identify the kind of information in beacons which affects user and location privacy.
2) Develop a tracking module which is practically able to track vehicles effectively using beacons.
3) Evaluate typical pseudonym change policies against the developed tracking module to determine their effectiveness to provide location privacy.
4) Design and evaluate a scheme for preserving user privacy and preventing unauthorized vehicle tracking.
5) Propose solutions for tracking in low-density or low-penetration cases.

III. OPEN ISSUES AND METHODOLOGY

In the beginning, we will analyze information sent in beacons and other related factors that affect the vehicles privacy. Then we will survey tracking methods and develop a tracker that produces reasonable tracking results with anonymous vehicles traces generated by a traffic simulator. We consider these results as the tracking benchmark which will be used in evaluating the proposed privacy-preserving technique. This benchmark can be enhanced by using additional information gained from road maps, pseudonyms and fixed attributes in beacons to resolve confusing situations.

Then we propose a scheme to protect the vehicles privacy by either skipping precise location information or using group communication as explained next.

A. Skipping Precise Location Information

Based on results presented in [3], vehicles are vulnerable to tracking even if they are totally anonymous. Authors showed that a large beacon interval ($\geq 2$s) and noised location information (even only 1m) can effectively decrease the tracking vulnerability. However, infrequent and noised data may not be suitable to many safety applications. Thus,
we propose to broadcast the precise information only every $\epsilon$ beacons where $\epsilon$ can be fixed or adaptively selected based on the speed, amount of surrounding vehicles, application-specific situations and other factors. During $\epsilon$ intervals, beacons are still sent but with a random noise added to the location received from GPS. We hypothesize by doing that the tracking vulnerability is largely decreased. In evaluation, we concern lane change warning and forward collision warning safety applications. We choose these two applications as representative as they require the most precise location information (<1m) and the highest beacon rate (10 Hz) [2] which are two of the most effective factors in tracking accuracy [3].

**Challenges**

1) Many safety applications depend on precise periodic location information. By hiding or skipping such information will affect the effectiveness of these applications.

2) The random noise added to the location should be carefully calculated to be reasonable in the current context, minimize the effect on the application behavior and minimize the tracking vulnerability as well.

3) On the other hand, carefully selecting the $\epsilon$ is crucial. Is it effective to simply use a fixed value or adaptive based on the context?

4) The previous challenges are interdependent. For example, changing the random noise or the $\epsilon$ value will affect the application effectiveness and vice versa.

To tackle these challenges, vehicles trace files are modified to add suitable random noises to location information except $\epsilon$ intervals. Then we evaluate them using the developed tracker and identify how the tracking accuracy is decreased. The requirements of the selected applications are investigated to check if they are still capable with noised skipped information. Also the $\epsilon$ value and the noise amount are selected and tuned iteratively based on the achieved tracking accuracy and the impact on the application effectiveness.

**B. Secure Group Communication**

Due to the imprecise location information sent in less-frequent beacons, the previous scheme seems to have a negative impact on applications effectiveness. Also, advanced tracking techniques may even filter this imperfection and infrequency in beacons. It may be more effective to secure beacons using symmetric cryptography among vehicle neighbors forming local secure groups. Secure group communication is already used for authentication in several previous work, however the efficiency of its key management and group membership are challenging, especially for infrastructure-less schemes. Also, the latency constraint is the most challenging issue as vehicle has to decrypt and authenticate hundreds messages every second.

Thus, instead of securing communication along the whole road, we think to broaden the usage of mix zones to secure beacons in discrete areas on the road. Mix zones are already applied in intersections to prevent an attacker from observing the pseudonyms change in a mix area by providing a cryptographic zone [5]. We hypothesize that forming secure groups only in specific critical locations will be more efficient. Thus, we will study the effective placements of such zones from this new perspective. Also, we will study establishing mix zones without the dependency on RSUs which helps in situations of few intersections as in highways and low infrastructure support as in the initial deployment of VANET.

**Challenges**

1) Forming secure groups is challenging in VANET due to the high mobility of vehicles. Also, discovering neighbors, join/leave process and key management should be so efficient with minimum overhead.

2) If discrete cryptographic zones are applied, identifying their efficient and effective placements should handle the trade-off between the amount of preserved privacy and the gained efficiency in communication.

Despite the location privacy concerns, vehicle tracking can be useful for several applications such as traffic-state information and fleet management applications. Thus, it is desirable to design the privacy scheme so that it allows authorized tracking but prevents the illegal one whether by an external attacker or a compromised or corrupted authority.

**ACKNOWLEDGMENT**

The author would like to thank J. Schlichter and W. Woerndl for their review and support in this PhD Forum extended abstract.

**REFERENCES**


