VANET Privacy

SVSU FACULTY RESEARCH GRANT FINAL REPORT

George Corser
May 10, 2017

Emerging networks which connect cars and other vehicles may violate drivers' privacy, exposing motorists to surveillance by eavesdroppers, from casual stalkers to Big Brother. Existing location privacy research has not thoroughly considered vehicular mobility patterns and unique architectures. This research specifically focused on vehicle network congestion and application overhead caused by privacy protocols. This research addressed two important vehicular network location privacy questions**.**

- To what extent can a vehicle protect itself against surveillance even while using a location based service (LBS), which may require frequent hyper-accurate location data?
- What are the cost/benefit tradeoffs?

PROGRESS MADE TOWARD GOALS

Formative evaluation:

This project had the following research goals, methods, and anticipated outcomes:

1. Evaluate and develop new vehicular ad-hoc network (VANET) location privacy models using realistic vehicle mobility patterns. Specifically, evaluate the effect of active decoy protocols[1] on location based service (LBS)[2] application performance and roadside unit (RSU)[3] performance.
2. Test new and existing vehicular privacy protocols using computer simulation tools.
3. Formalize and quantify the relationship between safety/security, network/application service quality/efficiency, and privacy.

It took longer than anticipated, however all objectives were achieved, at least to some measurable extent.

1. New VANET models developed and evaluated include privacy protocols called Stationary Mix Point Protocols—Regular (SMP-R), Stationary Mix Point Protocols—Irregular (SMP-I), On-the-fly Point—Regular (OTFP-R) and On-the-fly Point—Irregular OTFP-I). The mobility patterns did not include Intelligent Driver Model (IDM) but did use actual road layouts from a popular data source.
2. Models were tested using simulation tools I developed at Oakland University while completing my PhD, and further developed here at SVSU during the time of this project.
3. The research focused on only one aspect of network/application service quality/efficiency, specifically, congestion/overhead. Several relationships were confirmed, but no meaningful equation could be written to describe the effect of privacy on overhead or of privacy on congestion. This is a continuing research question.

[1] An active decoy protocol is a computer networking technique which enables a vehicle in-transit to pretend to be a different vehicle in-transit for the purpose of protecting location privacy of one or more vehicles.
[2] A location based service is a computer program or app that uses global positioning system (GPS) data of the user.
[3] A roadside unit is a computer router and antenna which enables cars and other vehicles using wireless communications equipment to communicate with the wired Internet.

Summative evaluation:

The research makes the following conclusions.

- First, there may be a price to be paid in network performance if active decoy location privacy protocols are to be utilized. SMP-R, SMP-I, OTFP-R and OTFP-I offered strong privacy protection but may took a toll in LBS overhead and network congestion.
- Second, in terms of overhead, that price is more or less costly depending on vehicle density and type of protocol, but generally speaking the overhead consequence are less pronounced in low density situations and when using OTFP-R rather than SMP-I. The overhead cost could be over 60%. If LBSs used these privacy protocols they would have to be built to accommodate the additional decoy queries.
- Third, in terms of congestion, the number of additional transmissions at specific RSU positions under the conditions tested did not result in any more than 10% dropped packets. In general it appeared that protocols anonymizing at regular time intervals create more overall congestion than irregular ones.
- Fourth, OTFP-R demonstrated the highest continuous average anonymity set size of the protocols tested. If the goal if a privacy protocol were to achieve the maximum anonymity set size during the duration of an anonymity trajectory, then OTFP-R might be a better choice than the other methods studied here.
- Fifth, in this study average distance anonymity decreased with vehicle density unless SMP-R was used. In other words, the more vehicles there were in the system the easier it was for an attacker to estimate the general location of a target. Average distances ranged from under 20 meters to about 225 meters. A great unanswered location privacy question must be: How can location privacy protocols achieve more sizeable average distances between vehicles during their anonymized trajectories?
- Sixth, time of anonymity exhibited a roughly inverse relationship with distance anonymity. Researchers must ask whether it is better to achieve a greater distance between members of an anonymity set, or to have those members anonymized for a longer period of time.

EXPENDITURES

Item:	**Budget**	**Actual**
Computer hardware:	$1,000.00	$872.01
Student worker (Aaron Hooper):	2,260.00	1,663.65

EXTERNAL FUNDING

None.