Maximizing Mix Zone Effectiveness for the Mitigation of De-Anonymization Threats in the Traffic Probe Message Service

Jeremy J. Blum, Peter O. Okosun

777 W. Harrisburg Pike
Middletown, PA 17057 USA
{jjb24,poo102}@psu.edu

Abstract. The Traffic Probe Message Service uses vehicle-to-roadside wireless communication to collect kinematic and other state data from participating vehicles. The draft standard requires vehicles to use pseudonymous identifiers in order to hide their identity. Whenever vehicles transmit state data to base stations called roadside equipment, the vehicles change their identifier and halt the collection of state data for a random period. These changes are designed to prevent a de-anonymization attack from reconstructing a vehicle's path through the road network. Thus, the roadside equipment creates mix zones, which given enough vehicles within a zone and sufficient changes in vehicle mobility patterns, can reduce the success of de-anonymization attacks. In highway scenarios, optimal mixing is likely in the regions near highway interchanges. This paper hypothesizes that given the rules snapshot generation, the optimal place for pseudonym changes is upstream of the middle of an interchange. Simulations of various traffic conditions in a large highway scenario support this hypothesis, and suggest that roadside equipment be placed such that they create pseudonym changes at these locations in order to maximize the ability of mix zones to mitigate de-anonymization threats.

1 Introduction

The deployment of Digital Short-Range Communications equipment in vehicles and on the roadside will quickly be able to support a range of applications, known as Day-One applications. One of the applications, the Traffic Probe Message Service, will enable traffic managers to gather roadway state data via wireless communication with vehicles [1]. Whenever equipped vehicles pass by base stations called roadside equipment, the vehicles will transmit a series of recent snapshots containing their locations and kinematic information.

The willingness of consumers to accept limited privacy protection in other mobile service contexts has been a function of the direct benefits realized from the service [2]. While the Traffic Probe Message Service provides system-wide benefits, the benefits to participating drivers are indirect. Given these, privacy concerns have been acknowledged as a potential hurdle for consumer acceptance of this service.

QSHINE 2010, November 17-19, Houston, United States

DOI 10.4108/eai.17-11-2010.2245446

Consequently, the Probe Message Service includes mechanisms to protect the privacy of participating vehicles. The most important of these mechanisms is the use of short-lived pseudonymous identifiers, which change at specified intervals during a vehicle's journey, including whenever the vehicles communicate with a newly encountered roadside unit. These short-lived identifiers are designed to mitigate the threat of de-anonymization attacks, which would seek to reconstruct a vehicle's trip through a road network. Given these short lived pseudonyms, such an attack would need to link the different pseudonyms used by a vehicle during one trip.

This timing and location of pseudonymous identifier affects on the ability of these short-lived pseudonyms to provide privacy protection. Intuitively, the pseudonym changes should be coordinated in the mix zones that occur in roadway scenarios, for example, near highway interchanges. The lane changes, changes in speeds, and entering and exiting of vehicles from a roadway increase privacy protection that can be provided through coordinated changes of identifiers in these areas. Using a model of a highway interchange, this paper hypothesizes that in general the pseudonym changes should occur upstream of an interchange, rather than downstream of the interchange.

Simulations and analysis of vehicle movement on a section of highway of I-880 in California, USA, support this hypothesis. Against a simple, multi-target de-anonymization attack, areas just upstream of interchanges provide better privacy protection than areas downstream from interchanges. In these areas, the de-anonymization algorithm experienced a misclassification rate that was 15.2% higher on average. These results support guidelines that suggest roadside equipment should be placed such that it creates pseudonym changes upstream, rather than downstream, of interchanges.

2 Background and Related Work

After an overview of the Traffic Probe Message Service, this section describes common mechanisms used to provide privacy protection in mobile services, including short-lived pseudonymous identifiers and obfuscation. Then, the section describes the privacy preserving mechanisms for the probe message service that have been proposed in the draft standard and previous research.

2.1 The Traffic Probe Message Service

Vehicles participating in the Traffic Probe Message Service collect snapshots due to three distinct types of triggers. When a vehicle is within range of a roadside unit, it transmits messages to the roadside with these collected snapshots in groups of one to four snapshots per message.

Event-Triggered Snapshots are generated sporadically by one-time events, such as roadway hazards. For example, the activation of the traction control system, indicative of poor roadway conditions, could trigger this type of snapshot [1]. These snapshots are sent in messages completely anonymously without any pseudonymous

ID.

Start/Stop Snapshot Messages are triggered initially whenever a vehicle stops for more than a set period of time and then again when the vehicle exceeds a threshold velocity. By default, the stop snapshot is triggered whenever a vehicle stops for more than five seconds, and a start snapshot is triggered when a vehicle exceeds the speed of 4.5 m/s. Unlike the event-triggered snapshots, these snapshots are sent with a pseudonymous ID.

While participating vehicles are moving, they collect Periodic Snapshot Messages. These snapshots are generated at intervals specified by the roadside. By default, a vehicle travelling 20 miles per hour would generate a snapshot every 4 seconds, while a vehicle travelling 60 miles per hour would generate a snapshot every 20 seconds.

The Periodic Snapshots include data on the location and kinematics of the vehicle including latitude, longitude, heading, velocity, acceleration, and yaw rate. In addition, snapshots can contain a range of other data elements, including control systems state, e.g. brake applied pressure, steering wheel angle, and traction control state; vehicle type, tire pressure, wiper rate, rain sensors, sun sensors, ambient air pressure, and temperature.

2.2 Privacy for Mobile Users

A common approach to provide privacy protection for mobile users relies on pseudonymous identifiers and obfuscation of mobile users' paths and data. The effectiveness of these approaches can be measured by their ability to prevent de-anonymization attacks that can link an individual to the path of a mobile user.

Pseudonyms that last for an entire trip or longer provide limited protection for mobile users. For example, vehicle traces with an update period of one record per minute have been used in de-anonymization attacks in which researchers were able to identify 85% of the homes of the mobile users [3]. In another de-anonymization attack with a shorter update period of 6 seconds, researchers were able to determine the location of users' homes within 61 meters [2].

From a traffic manager's point of view, these long-term pseudonyms would provide valuable data, for example, for the reconstruction of origin-destination matrices. However, due to the limited protection provided by these pseudonyms, the Traffic Probe Message Service uses short-lived pseudonyms, in which a vehicle changes pseudonyms during a single trip.

However, inference attacks can reconstruct a user's path even if the user changes pseudonyms during a trip. In order to link together messages produced under different pseudonyms, these attacks can use trajectory-based linking, relying on the tendency of users to continue moving in the same direction; map-based linking, relying on constraints imposed by a road network to aid in the linking; and empirical linking, relying on previous mobility patterns to aid in linking [4].

In order to limit the effectiveness of these linking attacks, often a pseudonym change will be accompanied by a random period of silence [5]. If users are transmitting messages at precise time intervals, the timing of the first message with a new pseudonym may be sufficient to link to the old pseudonym. A random period of

silence can also increase the distance between transmissions with different pseudonyms increasing the difficulty in linking together the transmissions.

In addition, changes in pseudonyms can be synchronized by having users change identifiers in the same geographical area, called a mix zone. For mobile services offered by base stations, these mix zones fall naturally in areas outside of the range of application providers [6]. For other services, intersections can serve as attractive mix zones because of the difficulty in linking that arises due to the changes in paths that occur there [7]. In addition, pseudonym changes can be coordinated in an ad hoc fashion via direct user-to-user communication, e.g. with direct vehicle-to-vehicle communication in vehicular networks [8].

2.3 Privacy Protection in the Traffic Probe Message Service

The Traffic Probe Message Service includes two primary mechanisms to preserve participant privacy. The probe message service is designed to obfuscate the beginning and end of every trip. The first snapshot is generated only after a vehicle has travelled 500 meters in the beginning of a trip. In addition, the vehicle deletes the snapshots collected at the end of a trip between the last roadside equipment and the final destination.

Given typical travel patterns for many users, a vehicle's path in the middle portion of the trip may allow for an inference attack. In order to prevent this type of attack, the probe service also requires vehicles to periodically change their pseudonymous identifiers. After changing their identifier, the vehicles wait a random period of silence time before creating the next snapshot. Two random numbers are generated, one for a distance between 50 and 250 meters, and another for a time between 3 and 13 seconds. The next snapshot is generated when after the random distance is travelled or the random time elapses, whichever comes first.

After a vehicle transmits a message to new roadside equipment, it must change its pseudonym. Therefore, the roadside equipment creates a mix zone, in which the changing of pseudonymous ids is synchronized geographically.

In addition, vehicles are required to change their pseudonyms every 120 seconds or 1 km, whichever comes last. Therefore, a vehicle may use multiple pseudonyms in messages to a single RSE. The snapshots generated under different pseudonyms cannot appear in the same message. Otherwise, linking an old pseudonym and new pseudonym would be straightforward if both appeared in a single message.

Previous research has focused on changes in the Traffic Probe Message Service that can improve privacy protection for participating vehicles [9]. These key changes include promoting the geographic coordination of pseudonym changes. Pseudonym changes at roadside equipment are coordinated geographically. However, other changes occur every 120 seconds or 1 km, whichever comes first. The authors suggest that vehicles be forced to change their pseudonyms at fixed distances, so that all pseudonym changes occur in fixed geographic locations. In addition, the authors suggest that snapshots include limited additional data, for example, vehicle type, that could aid in de-anonymization attacks. This paper extends this work by investigating locations that maximize the effectiveness of mix zones occurring at roadside equipment.

3 A De-anonymization Attack on Traffic Probe Message Service in Highway Scenarios

A de-anonymization attack on vehicles travelling in highway scenarios must link together pseudonyms used by a particular vehicle. This section describes a linking attack that attempts to link the last snapshot transmitted by a vehicle with an old pseudonym with the first snapshot generated by a vehicle under a new pseudonym. In order to increase the complexity of a de-anonymization attack, the snapshot messages are assumed to contain a minimum of information, only a timestamp, position information and velocity.

The attack uses a multi-target tracking approach to link together an old pseudonym with a new pseudonym. It first determines the feasibility of a match between the last snapshot calculated under an old pseudonym and the first snapshot calculated under a new pseudonym. In order for a match to be feasible, three constraints must be satisfied.

3.1 Snapshot Time Difference Constraint

The *Snapshot Time Difference Constraint* ensures that the timing of snapshot *j* is such that it could have generated by the same vehicle that generated snapshot *i*. At the low end of this time difference, a vehicle could have generated its last snapshot immediately before changing its pseudonym. After changing its pseudonym, the vehicle could then have chosen the smallest delay (3 seconds) before generating its next snapshot. At the high end, a vehicle could have been just about to generate a snapshot when changing its pseudonym, i.e. it generated its last snapshot just less than 20 seconds prior to the pseudonym change. This vehicle could then choose the longest delay (13 seconds) before generating its next snapshot. Thus, the *Snapshot Time Difference Constraint* is defined as follows:

$$3 \leq \Delta t < 33 \tag{1}$$

Where:

Δt is the difference between the timestamp of snapshot *j*, generated under a new pseudonym, and the timestamp of snapshot *i*, the last snapshot generated under an old pseudonym (in seconds)

3.2 Maximum Distance Travelled Constraint

The maximum distance that could be travelled between two snapshots is determined by two different cases. In the first case, the vehicle, starting at a velocity of v_i at the time of snapshot *i* accelerates as fast and as long as possible and at the last possible moment decelerates at the fastest possible rate to achieve a velocity of v_j at the time of snapshot *j*. The maximum velocity during this case never exceeds a maximum possible velocity for this section of roadway.

In cases where the maximum velocity would be exceeded, the maximum distance is calculated as follows. It is assumed that the vehicle accelerates as fast as possible in order to raise its velocity from v_i at time of snapshot *i* until it reaches the maximum possible velocity. The vehicle than travels at this maximum velocity until the last possible moment at which point it brakes as hard as possible to lower its velocity to v_j at time of snapshot *j*. Thus, the *Maximum Distance Travelled Constraint* is specified as follows.

Upper Bound on $\|l_j - l_i\|$	**Condition**
$\frac{(v_i + a^+_{max} t_a)}{2} t_a + \frac{(v_i + a^+_{max} t_a + v_j)}{2} t_b,$ $t_a = \frac{v_j - v_i - a^-_{max} \Delta t}{a^+_{max} - a^-_{max}}$ $t_b = \frac{v_j - v_i - a^+_{max} \Delta t}{a^-_{max} - a^+_{max}}$	if $(v_i + a^+_{max} t_a) \leq v_{max}$
$\frac{(v_i + v_{max})}{2} t_a + v_{max} t_c + \frac{(v_{max} + v_j)}{2} t_b,$ $t_a = \frac{v_{max} - v_i}{a^+_{max}}$ $t_b = \frac{v_j - v_{max}}{a^-_{max}}$ $t_c = \Delta t - t_a - t_b$	Otherwise

(**2**)

Where:

$\|l_j - l_i\|$ is the distance travelled along the roadway between snapshot *i* and snapshot *j* (in meters)

v_i is the velocity reported in snapshot *i* (in meters/second)

v_j is the velocity reported in snapshot *j* (in meters/second)

v_{max} is the maximum possible velocity on this section of roadway (in meters/second)

a^+_{max} is the maximum possible positive acceleration possible on this section or roadway (in meters/second^2)

a^-_{max} is the maximum possible negative acceleration (deceleration) possible on this section or roadway (in meters/second^2)

Δt is the difference between the timestamp of snapshot *j* and the timestamp of snapshot *i* (in seconds).

t_a is a possible time spent accelerating in the interval between snapshots (in seconds).

t_b is a possible time spent braking in the interval between snapshots (in seconds).

t_c is a possible time spent travelling at a constant speed in the interval between snapshots (in seconds)

3.2 Minimum Distance Travelled Constraint

Like the maximum distance constraint, the *Minimum Distance Travelled Constraint* is determined by two different cases. In the first case, the vehicle, starting at a velocity of v_i at time of snapshot *i* brakes as fast and as long as possible and at the last possible moment accelerated at the fastest possible rate to achieve a velocity of v_j at the time of snapshot *j*. The minimum velocity during this case never goes below a minimum possible for the given section of roadway.

In cases where the minimum velocity would be reached, the distance is calculated as follows. It is assumed that the vehicle decelerates as fast as possible in order to lower its velocity from v_i at time of snapshot *i* until it reaches the minimum possible. The vehicle than travels at the minimum velocity (or stops) until the last possible moment at which point it accelerates as fast as possible to raise its velocity to v_j at time of snapshot *j*. Thus, the *Minimum Distance Travelled Constraint* is specified as follows.

Lower Bound on $\|l_j - l_i\|$	**Condition**
$\frac{(v_i + a_{max}^- t_b)}{2} t_b + \frac{(v_i + a_{max}^- t_b + v_j)}{2} t_b,$ $t_b = \frac{v_j - v_i - a_{max}^+ \Delta t}{a_{max}^- - a_{max}^+}$ $t_b = \frac{v_j - v_i - a_{max}^- \Delta t}{a_{max}^+ - a_{max}^-}$	if $(v_i - a_{max}^- t_b) \geq v_{min}$
$\frac{(v_i + v_{min})}{2} t_b + v_{min} t_c + \frac{(v_{min} + v_j)}{2} t_a,$ $t_b = \frac{v_{min} - v_i}{a_{max}^-}$ $t_b = \frac{v_j - v_{min}}{a_{max}^+}$ $t_c = \Delta t - t_a - t_b$	Otherwise

(**4**)

Where:

$\|l_j - l_i\|$ is the distance travelled along the roadway between snapshot *i* and snapshot *j* (in meters)

v_i is the velocity reported in snapshot *i* (in meters/second)

v_j is the velocity reported in snapshot *j* (in meters/second)

v_{min} is the minimum possible velocity on this section of roadway (in meters/second)
a^{+}_{max} is the maximum possible positive acceleration possible on this section or roadway (in meters/second^2)
a^{-}_{max} is the maximum possible negative acceleration (deceleration) possible on this section or roadway (in meters/second^2)
Δt is the difference between the timestamp of snapshot *j* and the timestamp of snapshot *i* (in seconds)
t_a is a possible time spent accelerating in the interval between snapshots (in seconds)
t_b is a possible time spent braking in the interval between snapshots (in seconds).
t_c is a possible time spent travelling at a constant speed in the interval between snapshots (in seconds)

3.4 Snapshot Pairing

Snapshot pairs that satisfy the three constraints are then ranked in ascending order according to the following score:

$$s_{i,j} = \left| \left\| l_j - l_i \right\| - \frac{v_i + v_j}{2} \Delta t \right| \quad (5)$$

Where:
$s_{i,j}$ is the score assigned to the snapshot pair (snapshot *i*, snapshot *j*)
$\left\| l_j - l_i \right\|$ is the distance that would be travelled along the roadway between the location reported in snapshot *i* and the location reported in snapshot *j* (in meters)
v_i is the velocity reported in snapshot *i* (in meters/second)
v_j is the velocity reported in snapshot *j* (in meters/second)
Δt is the difference between the timestamp of snapshot *j* and the timestamp of snapshot *i* (in seconds)

The de-anonymization attack then iterates through the list of sorted snapshot pairs. If neither the snapshot *i* nor the snapshot *j* in the next pair has been linked already then a link is established between these pairs. The algorithm then repeats this process until all snapshots have been linked.

By eliminating snapshots that have already been paired, the de-anonymization takes a multi-target tracking approach, which has been more effective than single-target tracking attacks in similar inference attacks on mobile users [4]. The approach could be further improved by expanding the information used. For example, the current attack uses only the first and last snapshot generated by a vehicle under a given pseudonym. A stronger attack could use all of the snapshots generated under a pseudonym to create a profile of a driver, and then use these profiles to aid in the linking. In addition, if the snapshots include attributes other than pseudonym,

timestamp, position, and velocity, these attributes could also be used in the linking attack.

4 Optimizing Mix Zone Location in the Traffic Probe Message Service

Roadside equipment, because of the pseudonym change that occurs after an exchange of messages with a vehicle, should be placed where they can create the most effective mix zones. Based on the mixing that occurs near highway interchanges and the rules of snapshot generation, the paper hypothesizes that causing pseudonym changes upstream of interchanges will be more effective than downstream changes. Simulation of the Traffic Probe Message Service in a large highway scenario is then used to test this hypothesis.

4.1 Mix Zones in Highway Scenarios

Highway scenarios offer ideal locations for mix zone locations promoting probe participation privacy. Intersections on arterial roadways also provide for opportunities to "create confusion at the crossroads," due to the possibility that a vehicle could turn [7]. However, in the probe message service, the periodic snapshots and start/stop snapshot messages can aid in the tracking of vehicles through an intersection.

In highway scenarios, one would intuitively expect mix zones to occur near highway entrances and exits. Upstream of off-ramps, there is mixing of traffic as exiting vehicles move from their chosen travel lane to the exit lane. These lane changes create and remove gaps between vehicles causing other vehicles to change their velocity. Highway on-ramps similarly create mixing downstream of the ramp as new vehicles enter the highway.

Figure 1 shows two potential locations for pseudonym changes near a simple highway interchange. As shown upper part of the figure, these changes could occur upstream of the interchange or the changes could occur after the interchange. In both scenarios, the change can take advantage of mixing that occurs upstream of off ramps and downstream of on ramps. Because snapshots are generated at highway speeds every 20 s, the last snapshot under the old pseudonym will be generated between 0 and 20 s prior to the pseudonym change. At highway speeds, this location will be between 0 and approximately 580 m. At these speeds, the vehicle then generates the first snapshot under the new pseudonym between 3 and 13 seconds after the pseudonym change, i.e. after travelling approximately 90 to 380 m.

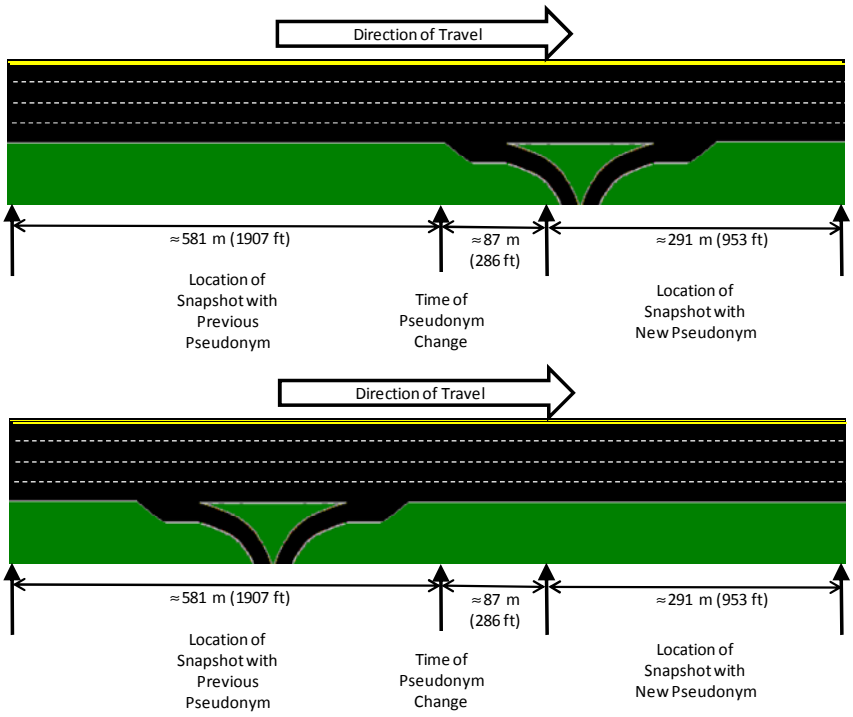

Fig. 1. Scenarios for Pseudonym Changes Near Interchanges.

There is, however, a significant difference between the mixing that occurs upstream of off ramps and downstream of on-ramps. Because of the uncertainty involved in when gaps in a target lane will occur, drivers, who need to exit a highway, will on average perform their lane changes well in advance of the off ramp. Drivers entering a highway, on the other hand, will tend to make their lane changes as soon as a suitable gap in the desired lane appears.

Therefore, the mixing upstream of an off-ramp will tend to occur at father distances from an interchange than the mixing that occurs after an on-ramp. The scenario at the top of Figure 1, therefore, should provide better privacy protection because it has a better chance of covering both the mixing that occurs at longer distances upstream of the off-ramp and the mixing that occurs at closer distances downstream from the on-ramp.

Interchanges in highway scenarios can be significantly more complex that the ones considered here. In a more complex scenario, though, there is likely to be more mixing throughout area covered by an interchange. Therefore, given this more significant mixing, the precise location of the pseudonym change is likely to be less important in this type of scenario from the point of view of privacy protection.

4.2 Simulation of De-anonymization Attacks on the Traffic Probe Message Service

The simulation of de-anonymization attacks on the probe message service has three distinct pieces. The first component is the highway environment, which is a simulated highway based on I-880 in Hayward, California, USA, with traffic demand for rush hour and also for off-peak times. The second component is the simulation of the traffic probe message service. The third component is the de-anonymization algorithm that attempts to link the snapshot with the old pseudonym and the snapshot with the new pseudonym. The attack is the one described in Section 3.

The simulation of vehicular mobility was done with the microscopic vehicle traffic simulator CORSIM, a validated and widely used simulation program [10]. This program tracks each individual vehicle as it travels through the road network. The vehicle's mobility patterns are a function of driver behavior, vehicle performance characteristics, and constraints imposed by the roadway geometry and surrounding vehicles.

CORSIM was used to model the roadway geometry of a 9.2 mile section of highway similar to I-880 in Hayward, California [11]. This section of highway contains ten off-ramps and ten on-ramps. The scenarios are based on traffic counts obtained by loop detectors and reported in the Freeway Service Patrol Evaluation Project, University of California. The highway contains between 8 and 10 lanes, and the scenarios model average traffic, without HOV lanes, during peak hours and off peak hours. In peak traffic scenario, the average density of vehicles was approximately 170 vehicles per mile. In the off-peak scenario, the average density was approximately 70 vehicles per mile.

The mobility of vehicles provided by the CORSIM simulation was used in the simulation of the traffic probe message service. The percentage of the vehicles participating in the service was varied from 5% and 15%. These vehicles begin participating in the service after passing roadside equipment placed either upstream from an off-ramp or downstream from an on-ramp. The vehicles create their first snapshot after a random interval chosen from between 3 and 13 seconds, the defaults defined in the standard. Thereafter, vehicles create new snapshots every 20 seconds until the vehicles pass another piece of roadside equipment. At this point, the vehicle changes its pseudonym, waits another randomly chosen interval between 3 and 13 seconds, and then begins to create snapshots with a new pseudonym.

4.2 Simulation Results

The simulation results show that the location of the most effective mix zones in highway environments is a function of the roadway geometry. Indeed, the results support the hypothesis that in simple interchanges, better privacy protection arises from having vehicles change their pseudonyms upstream of an interchange rather than downstream.

The error in the de-anonymization attack can be measured as the misclassification rate, i.e. the number of correctly linked snapshots generated under old and new pseudonyms divided by the total number of old snapshots. The pool of old snapshots

is drawn only from participating vehicles currently on the highway when passing roadside equipment. The pool of new snapshots, though, includes all participating vehicles. This larger pool is necessary because vehicles may not be generating snapshots prior to entering the highway when they may be close to the start of their trips.

Figure 2 shows the misclassification rate of the de-anonymization attack as a function of the traffic scenario, level of participation in the service, and location of pseudonym change. As shown in this figure, as the participation rates increase, the misclassification rate increases. Higher participation rates result in higher density of participating vehicles, which increase the likelihood of an incorrect pairing by the inference attack. Similarly, in these scenarios, both of which contain free flowing traffic, the higher traffic densities in the peak hour scenario resulted in a higher misclassification rate than in the off peak scenario.

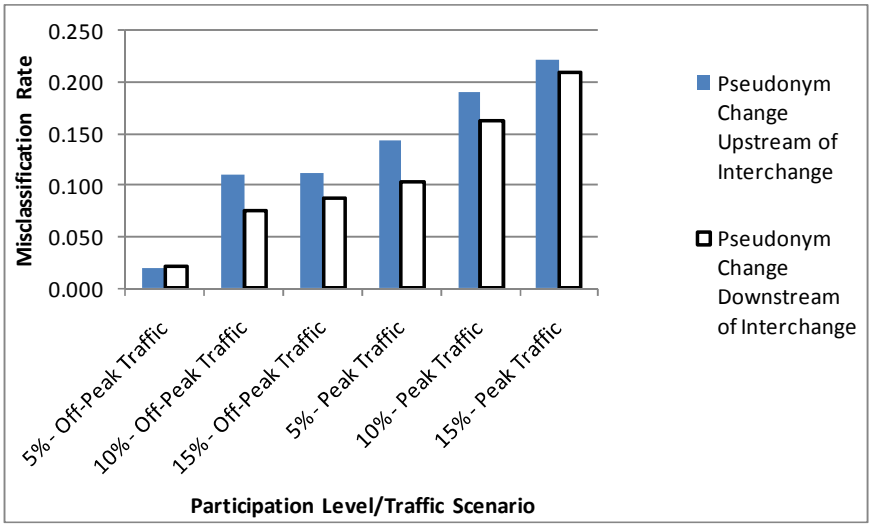

Fig. 2. De-anonymization Attack Misclassification Rate by Traffic Scenario, Participation Level (%), and Location of Pseudonym Change

More importantly, the results shown in Figure 2 suggest that the optimal mix zones are a function of roadway geometry. In all but the scenario with the lowest density of participating vehicles, the de-anonymization attack performs worse when pseudonym changes occur upstream of an interchange. The misclassification rate in these scenarios is 15.2% higher on average. Therefore, pseudonym changes in these locations provide better privacy protection.

Figure 3 shows the misclassification rate when pseudonyms are changed at different locations upstream from an off-ramp. As shown in this figure, the privacy protection provided by upstream changes in pseudonyms is not significantly affected by the precise location of the change. Particularly as vehicle density increases, the misclassification rates are fairly constant across all of these locations between 0 and 250 ft upstream of an off-ramp.

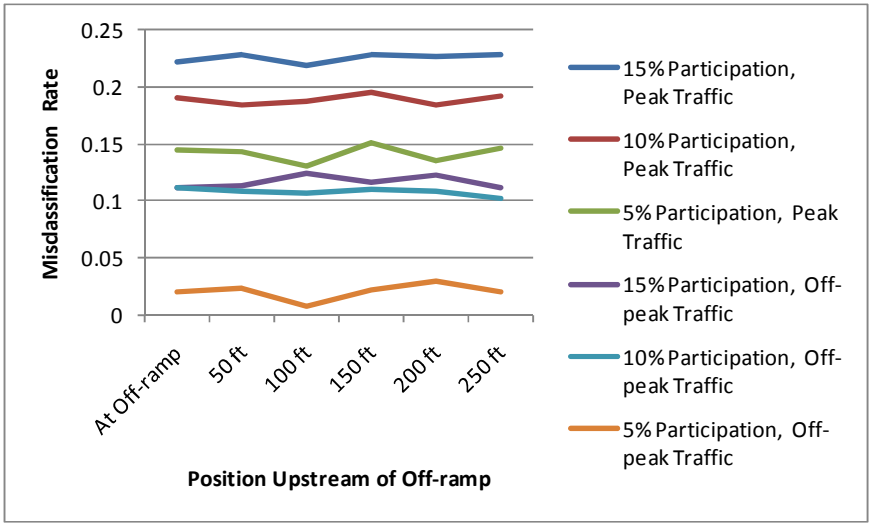

Fig. 3. Effect of Location of Pseudonym Change on the De-anonymization Attack Misclassification Rate at Various Locations Upstream of Off-ramps

These results provide guidance for the placement of roadside equipment to increase privacy protection for vehicles participating in the Traffic Probe Message Service. In order to obtain the most effective mix zones, this equipment should be placed such that vehicles change their pseudonyms upstream, rather than downstream, of interchanges. These locations appear to provide better mixing regardless in most traffic conditions. Moreover, as participation in the probe message service grows, the advantages provided by these locations will increase.

5 Conclusions and Future Work

The Traffic Probe Message Service promises a wealth of additional information to help traffic operators efficiently manage road networks. However, widespread participation in the service is needed in order to realize the full promise of the system. Privacy concerns have been identified as a potential obstacle to achieving this widespread participation.

This paper examined the effect of roadside equipment placement on the privacy protection for users of the service. The placement of this equipment affects privacy protection because vehicles change their pseudonymous identifiers every time they pass this equipment. Therefore, for privacy protection, the equipment should be placed in areas where maximum mixing can occur.

In highway environments, simulation of a large highway suggests that in order to capture the mixing that occurs both upstream and downstream from an interchange,

the pseudonym changes should happen upstream rather than downstream of the interchange.

This current study does have two significant limitations. First, the vehicle mobility patterns were generated from a microscopic vehicle simulator. Although this simulation program has been validated, it likely does not produce the same range of variable driver behavior as in the real world. Moreover, this study examined a limited set of scenarios, focusing on only one highway with a limited variety of interchanges.

The authors currently plan future work to extend this work and address these limitations. The authors intend to confirm the results of simulations with results from field observations of vehicle mobility patterns. In addition, the authors intend to study additional roadway scenarios.

References

1. DSRC Committee. DRAFT SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary: Annex B: Traffic Probe Message Use and Operation. Warrendale, PA: Society of Automotive Engineers (2007).
2. Krumm, J. A survey of computational location privacy, Personal and Ubiquitous Computing, 13(6), 391-99 (2009).
3. Hoh, B., Gruteser,,M., Xiong,, H., Alrabady, A. Enhancing security and privacy in traffic-monitoring systems, IEEE Pervasive Computing Magazine, 38-46 (2006).
4. Gruteser, M. Hoh, B. On the anonymity of periodic location samples, Conference on Security in Pervasive Computing, 179-92 (2005).
5. Huang, L., Matsuura, K., Yamane, H., Sezaki K. Towards modeling wireless location privacy. Proc. of Privacy Enhancing Technologies, 59–77 (2005).
6. Beresford, A.R., Stajano, F. Location privacy in pervasive computing, IEEE Pervasive Computing Magazine, 46-55 (2003).
7. Meyerowitz, T.J., Choudhury, R.R. Realtime location privacy via mobility prediction: creating confusion at crossroads. 10th Workshop on Mobile Computing Systems and Applications, 1-6 (2009).
8. Li, M., Sampigethaya, K., Huang, L., Poovendran, R. Swing & swap: user-centric approaches towards maximizing location privacy. ACM Workshop on Privacy in Electronic Society, 19-28 (2006).
9. Blum, J.J., Okusun, P.O., "Privacy Implications of the Traffic Probe Message Service," IEEE Intelligent Transportation Systems Conference, 342-347, (2010).
10. Owen, L.E., Zhang, Y., Rao, L., McHale, G. Traffic flow simulation using CORSIM. Winter Simulation Conference, 2:1143-7 (2000).
11. Petty, K. FSP 1.1: The Analysis Software for the FSP Project. Berkeley, CA: University of California, Berkeley (1994).