Location Privacy, Application Overhead and Congestion in VANET Location Based Services

George P. Corser, *Member, IEEE,* Abdelnasser Banihani, *Student Member, IEEE*, Johnathan Cox, Risalatul Hoque, Huirong Fu, *Member, IEEE,* Ye Zhu, *Member, IEEE*

***Abstract*—Vehicular ad hoc networks (VANETs) may one day improve vehicle safety and traffic management, but VANETs raise location privacy concerns because they would transmit data which could also be used for unwanted surveillance. Some location privacy researchers have proposed application-layer protocols that would require dummy event communications which may lead to network congestion and/or location based service overhead. This research investigates the degree of additional network congestion and overhead resulting from these protocols.**

***Index Terms*—dummy event, location based service, LBS, KDT, vehicular ad-hoc network, VANET, DSRC, location privacy**

I. Introduction

THIS research measures application-layer network congestion and overhead caused by proposed *active decoy* location privacy protocols [4] that would employ dummy events in vehicular ad-hoc networks (VANETs). Someday VANETs may help reduce the number of vehicle accidents, but they may also introduce location privacy risks. One particular location privacy problem may occur when vehicles access location based services (LBS) requiring continuous or frequent precise location (FPL) queries. Powerful but possibly costly methods of defending against location privacy attacks include dummy event location privacy protocols [1]. What is the tradeoff between network overhead, network congestion and location privacy in VANETs using LBSs that require FPL queries and vehicles using dummy event location privacy protocols? Let us call this the dummy event congestion-overhead (DEOC) problem.

The DEOC problem is important because if dummy event solutions can be found that are not too costly in terms of network performance then motorists may be able enjoy stronger privacy protection protocols than would be available using other methods, such as hiding, anonymizing and obfuscating, as described in [2]. Other traditional privacy techniques, like spatial cloaking, will not protect FPL queriers because eavesdroppers might compare successive queries to identify a specific entity. In fact, cloaking obfuscates location and so does not enable precise location queries.

Dummy-event, dummy-user (DE/DU) and *active decoy* [3] techniques may be useful to protect FPL query privacy while maintaining precision, but their costs must be understood before such techniques may be justified. DE/DU solutions have largely been rejected because dummies have been too easy to detect, but active decoy methods might be more effective. Because vehicles are naturally confined to a narrow set of mobility patterns, it may be possible to construct decoys which behave in a manner similar to genuine vehicles because signals are generated by real vehicles [3]. DE/DU solutions have also been rejected by some researchers because of anticipated costs, such as network congestion and overhead [1]. To determine the net benefits of active decoy methods we must measure their costs in terms of network congestion and overhead, which is the purpose of the present research.

The overhead/congestion problem is complex because it requires consideration of a wide range of factors, notably built-in VANET privacy capabilities such as temporary MAC addressing, roadside unit (RSU) capacity, wireless communications range, vehicle mobility, vehicle density, and privacy protocol. It also requires clear definitions and measurement criteria for overhead and congestion.

Prior solutions do not appear to exist in the literature perhaps because active decoy techniques represent a relatively new branch of location privacy research. The authors of this paper are not aware of any prior methods to measure VANET-LBS application-layer congestion and overhead of active decoy location privacy protocols.

The primary contributions of this paper are (1) definitions and metrics for VANET application-layer overhead and congestion, and (2) simulation and performance evaluation of four active decoy location privacy protocols.

The rest of this paper is organized as follows. Section II presents background for the VANET location privacy problem, and the network congestion/overhead at the application-layer. Section III proposes overhead and congestion metrics . Section IV presents simulation setup. Section V evaluates performance discusses of simulation results. Section VI concludes the paper.

G. P. Corser is with Saginaw Valley State University, University Center, MI 48710 USA (e-mail: gpcorser@svsu.edu).

A. Banihani is with Oakland University, Rochester, MI 48309, USA (e-mail: abanihani@oakland.edu).

J. R. Cox is with Park University, Parkville, MO USA 64152, (e-mail: 601383@park.edu).

R. Hoque is with Minnesota State University - Moorhead, Moorhead, MN 56563 USA (e-mail: hoquemd@mnstate.edu).

H. Fu is with Oakland University, Rochester, MI 48309 USA (e-mail: fu@oakland.edu).

Y. Zhu is with Cleveland State University, Cleveland, OH 44115 (e-mail: y.zhu61@csuohio.edu).

978-1-5090-6296-6/17 $31.00 © 2017 IEEE
DOI 10.1109/BigDataSecurity.2017.52

II. Background

VANETs depend on vehicles each having access to accurate Global Positioning System (GPS) data. Vehicles transmit their positions to each other using vehicle-to-vehicle (V2V) communications. Vehicles may communicate with application servers, such as Location Based Services (LBS) via wired roadside units (RSU) using vehicle-to-infrastructure (V2I) communications. See Fig. 1.

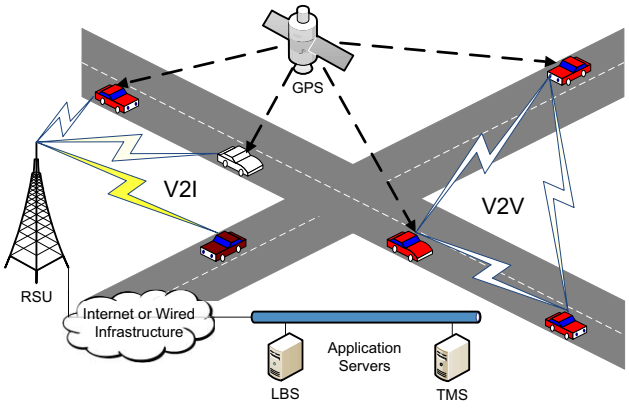

Fig. 1. System model: includes vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Roadside units (RSUs) relay queries to application servers such as transportation management systems (TMSs).

A. Threat Model

Intelligent Transportation Systems (ITSs) are expected to one day include air-traffic-control-like LBS systems called Traffic Management Systems (TMSs) which would enable traffic managers to guide drivers or driverless cars based on current vehicle traffic conditions. If US DOT decides to mandate the use of TMSs, and if vehicles access TMSs through WSMP, then a malicious insider or an outsider who has hacked a TMS might be able to track vehicles from the comfort and anonymity of her own home laptop.

This paper analyzes privacy protocols using the threat modeling framework proposed in [2], which defines the means, actions and goals of the potential attacker. This paper assumes a global passive adversary (GPA) with the following means: *access* to LBS application data, RSU data and perhaps to certain license plate reader (LPR) or other camera data; and *knowledge* of geography (road maps / road topology), traffic conditions (blocked / slow roads), home owner names and addresses and geographical coordinates, and the target's name, address, license plate number, and perhaps expected mobility profile. This paper considers DSRC communications only, not cell phone data or other information from other devices even though that might also be useful to an attacker.

B. Location Privacy Preserving Mechanisms

This paper applies the location privacy framework defined in [2], which enumerates location privacy preserving mechanisms which include four methods: hiding, obfuscating, anonymizing and dummifying. Previously proposed VANET privacy solutions have suggested silent periods (an example of *hiding*), pseudo identifiers or *pseudoIDs,* mix zones and group signatures (*anonymizing*), spatial and temporal cloaking (*obfuscating*) and transmitting false data, i.e. adding dummy events (*dummifying*). Recently, a new dummifying technique has been suggested, called active decoy [3]. The method has been analyzed for its impact on safety [5], and privacy performance [3], and dynamic measurement in terms of k-anonymity, distance-anonymity and time-of-anonymity [4]. This paper examines the cost in terms of network performance.

III. Proposed Network Performance Metrics

This research examines application layer network performance of location privacy protocols in terms of overhead and congestion. Overhead is defined as the ratio of fake-to-total queries passed over the network given the particular privacy protocol. For example, if there were 100,000 total LBS queries (assuming one packet per query) and 40,000 of them were fake, dummies or decoys, then the overhead ratio would be 40%. This measure could also be viewed as the congestion at the central LBS server.

Congestion is defined as the ratio of dropped-to-total queries (assuming one packet per query) passed over the network given the particular privacy protocol at a specific point, called the bottleneck. If many vehicles were close together and transmitting both genuine and dummy queries, then it may be possible that an unacceptable number of packets would be dropped. This phenomenon would occur at a localized position in the overall VANET system, perhaps at an RSU. The study in [6] reports that there may be an optimal number of messages for an RSU to maximize throughput. The authors of this paper assume this is the case and measure congestion as the proportion of dropped packets dropped y RSUs in the overall system. For example, if there were 100,000 total LBS queries and RSUs dropped 30,000 of them, then congestion would be 30%.

TABLE I
Simulation Parameters

Parameter	Setting
Size of region, R	3000 m x 3000 m
Communications Range	200m, 300 m, or 400m
Mobility Patterns	GMSF (City, Urban, Rural) [21]
Mix Points	50, 60, 70, …, 150, or continuous
Silent Period (Δt)	30 seconds
Simulation Time	2000 s (33.3 min)
Avg. Vehicle Speed	20 m/s

IV. Simulation Setup

This section describes simulations conducted to evaluate the effectiveness of various privacy protocols. The experimental set-up is described in Table I.

A. Simulation Overview

In each simulation, the goal was to achieve anonymous FPL LBS access. That is, vehicles attempted to anonymize with as many other vehicles as possible, remaining anonymous for as great a distance as possible, and for as long a time as possible.

Each vehicle did the following.

- Enter region, deanonymized.
- Execute privacy protocol and become anonymized.
- Exit region and become deanonymized again, or otherwise terminate anonymous LBS access.

The rationale behind the anonymization process outlined above was to create a controlled environment to compare protocols. One could imagine entering a large region where there are few means of ingress and egress, with each ingress/egress point monitored by license plate readers. If a motorist desired to move about the interior of region anonymously, she would have to anonymize after the point of ingress and would lose anonymity upon egress.

B. Mobility Patterns

This research employed Generic Mobility Simulation Framework, GMSF [7], which offers Multi-agent Microscopic Traffic Simulator, MMTS, trace files linked on the GMSF website [8] and provided at the Laboratory for Software Technology website [9], specifically *city*, *urban* and *rural*. All three trace files contain records of time-stamps, vehicle-ids, x-coordinates, y-coordinates within a 3000x3000 meter (9 million square meter) grid. Each mobility pattern starts with a different number of vehicles, v. City starts with v=897. Urban starts with v=488. Rural starts with v=110. Vehicles enter and leave the region at the same rate, but the number of vehicles in the pattern at any given time is not always precisely the same as the number at the start.

Sometimes road topologies, such as in the Freeway pattern (*a* straight road with perhaps several lanes) and the Manhattan pattern (a grid of horizontal and vertical roads), provide wide ranging linear density versus area density. That is, the vehicle density per linear meter can be out of sync with the vehicle density per square meter, especially when compared with more realistic road topologies. For example, for 900 vehicles in a 3000x3000 meter grid, the Freeway pattern might have a linear density of 0.3 v/m, 900 vehicles divided by 3000 meters, and a square density of 0.0001 v/m2, 900 vehicles divided by 9 million square meters. The Manhattan pattern would have a linear density of 0.004839 v/m, 900 vehicles divided by 186,000 meters, but the same square density as the Freeway pattern. In other words, the linear density of the Manhattan pattern is 1.6% that of Freeway pattern given the same square density.

The mobility patterns used in this simulation, however, have similar linear distances: city, 14,783 meters; urban, 13,955 meters; and rural, 10,175 meters. The areas covered are identical, 3000 m x 3000 m, so the mobility patterns provide relatively realistic traffic flows and comparable roadway linear distances and square areas.

C. Location Privacy Protocols and Mix Points

To create mix zones, as defined in [10], the simulation used the concept of a mix point, a position in space and time, with coordinates (x,y,t). The mix point was used to create a circular mix zone of radius, r. If a vehicle was positioned within r, i.e. within *comrange*, of (x,y) at time t, then that vehicle initiated whatever the privacy protocol required. If the vehicle never came within comrange of any mix point then it never became anonymized.

This paper evaluates four protocols: SMP-R, stationary mix points, occurring at regular time intervals; SMP-I, stationary mix points, occurring at irregular time intervals; OTFP-R, randomly chosen *on-the-fly* mix points, occurring at regular time intervals; OTFP-I, randomly chosen mix points, occurring at irregular time intervals.

1) Stationary Mix Point Protocols (SMP-R and SMP-I)

An SMP creates a region that does not move in which vehicles may switch pseudoIDs. A similar protocol is described in [11], but in SMP presented by this paper, a fixed point *(x, y)* was chosen. To maximize k, the busiest intersection in the mobility pattern was chosen as the "social spot" for mixing. In scenario SMP-R, regular time intervals were chosen. In scenario SMP-I, irregular time intervals were chosen. Vehicles that were within radius, r, of point *(x, y)* at time, t, were added to the anonymity set. Upon anonymizing, vehicles enter a silent period. They ceased all communications at both MAC and APP layers because, if they were to continue communications via one, under RSU LBS collusion they would be linkable to the other. All vehicles in the anonymity set changed pseudoIDs, but remained silent until the silent period expired, at which point all silent vehicles resumed communications, including anonymous LBS access, using new identifiers.

2) On-the-fly Point Protocols (OTFP-R and OTFP-I)

OTFP, similar to the protocol presented in [3], Privacy-by-Decoy (PBD), is similar to SMP except vehicles anonymize at random locations. Timing could be at regular intervals, as OTFP-R, or irregular ones, OTFP-I. If regular time intervals were instituted, then there would need to be some method of informing the vehicle as to what the timing would be. If irregular time intervals were instituted, the vehicle could beacon for anonymity at any opportune point along its trajectory. As in the other protocols, in OTFP, when vehicles willing to anonymize move within communications range of each other, they agree to anonymize, go silent for a time, then resume transmissions.

V. Simulation Results

Overhead and congestion were measured for three vehicle densities, low density (rural), medium density (urban) and high density (city). Four protocols were evaluated, SMP-R, SMP-I, OTFP-R and OTFP-I.

A. Effect of Vehicle Density on Overhead

SMP-R resulted in low overhead for low density, high overhead for medium density and low overhead for high density. This occurred because at low vehicle density there were few cars with which to anonymize at the stationary mix point, so there was no opportunity to incur overhead. At medium density overhead was maximized because the vehicles in comrange were more often eligible to anonymize, not already engaged in other anonymization commitments, as in high

density conditions, but more numerous than at low density conditions. At high vehicle density more vehicles were already committed to prior anonymization requests. See Fig 2.

SMP-I presented similar results as SMP-R except low density and medium density resulted in similar congestion levels. The introduction of irregular time intervals produced higher anonymization levels because of more *clumping*, variability in anonymization group size.

OTFP-R introduced the highest overhead at all density levels. This is because mixing at random locations rather than stationary ones ensures that a high number of vehicles will be involve in some sort of anonymization commitment.

OTFP-I displayed consistently high overhead, but not as high as overhead for OTFP-R. Overhead is increased the higher the number of vehicles are anonymized and the higher the number of vehicles per clump. For example, 10 vehicles in one clump all sending 10 messages per vehicle (1 genuine and 9 fakes) would result in 90 fake messages out of 100 total messages, or 90% overhead. But ten vehicles in two clumps of five vehicles would send 5 messages per vehicle (1 genuine and 4 fakes), for a total of 50 messages and 40 fakes, or 80% overhead. OTFP-I creates more clumps than OTFP-R so it produces less overhead. See Table II.

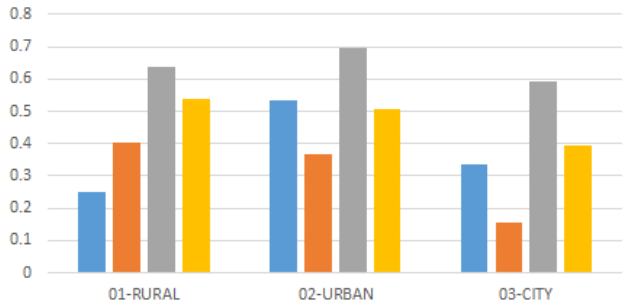

Fig. 2. Overhead. The chart above shows three clusters of four bars. The four bars are overhead ratios under simulated conditions for SMP-R, SMP-I, OTFP-R and OTFP-I, respectively.

TABLE II
OVERHEAD

DENSITY	SMP-R	SMP-I	OTFP-R	OTFP-I
RURAL	25%	40%	63%	54%
URBAN	53%	37%	70%	50%
CITY	34%	16%	59%	39%

B. *Effect of Vehicle Density on Congestion*

Congestion did not become a consideration until vehicle density reached a critical point. In all cases less than 10% of the packets were dropped due to congestion.

All privacy protocols evaluated under low density rural conditions resulted in zero congestion at the RSUs.

SMP-R resulted in higher congestion for urban than city again because more vehicles at a specific location were eligible to anonymize with the requesting vehicle so there were higher concentrations, larger clumps, of vehicles transmitting in comrange of the RSU positions. See Fig. 3.

SMP-I presented no congestion under the conditions evaluated in this study. Irregular time intervals spread out the clumps sufficiently broadly as to avoid hitting the packet-dropping threshold. It also resulted in fewer vehicles being anonymized at all so there were fewer communications overall.

OTFP-R introduced a more linear congestion result. While it produced too few communications in low density to have an effect on congestion, as vehicle density increased it produced more anonymized cars overall and these were clustered in clumps in such a way as to produce more congestion.

OTFP-I resulted in fewer vehicles being anonymized at all so there were fewer communications overall. Consequently, congestion was not a factor until vehicle density became very high. See Table III.

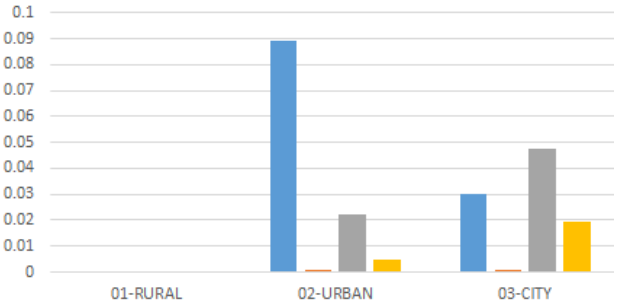

Fig. 3. Congestion. The chart above shows three clusters of four bars. The four bars are congestion ratios under simulated conditions for SMP-R, SMP-I, OTFP-R and OTFP-I, respectively.

TABLE III
CONGESTION

DENSITY	SMP-R	SMP-I	OTFP-R	OTFP-I
RURAL	0%	0%	0%	0%
URBAN	9%	0%	2%	0%
CITY	3%	0%	5%	2%

C. *Effect of Vehicle Density on K*

This paper measures continuous location privacy, or KDT-anonymity, as defined in [4]. The continuous anonymity set size, *K*, is the average number of vehicles with which a vehicle is anonymized over the course of an entire trajectory.

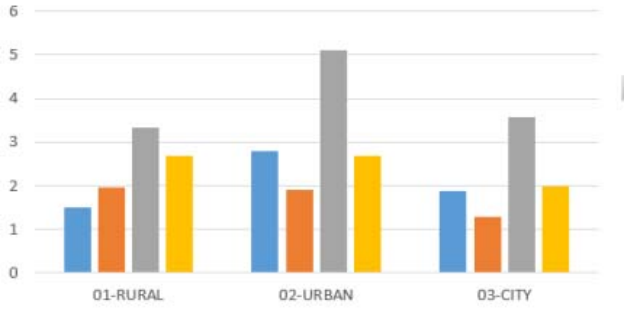

Fig. 4. K (Average Anonymity Set Size). The chart above shows three clusters of four bars. The four bars are average anonymity set sizes of vehicles over their trajectories under simulated conditions for SMP-R, SMP-I, OTFP-R and OTFP-I, respectively. Y-axis indicates number of vehicles in anonymity set.

In general, medium density resulted in maximum anonymity set size. This is due to clumpiness, as discussed in subsection V.A. Fewer, larger clumps increase average anonymity set size,

K. This effect was more pronounced in SMP-R than in SMP-I because in high density situations even though more vehicles are in comrange with SMP-I fewer have no prior anonymization commitments compared to SMP-R. The same was the case for OTFP-R and OTFP-I for the same reasons. See Fig. 4.

In general, OTFP privacy protocols outperformed SMP privacy protocols in terms of *K*. See Table IV.

TABLE IV
K (AVERAGE ANONYMITY SET SIZE IN NUMBER OF VEHICLES)

DENSITY	SMP-R	SMP-I	OTFP-R	OTFP-I
RURAL	1.51	1.97	3.34	2.68
URBAN	2.78	1.92	5.11	2.70
CITY	1.88	1.28	3.57	2.00

D. Effect of Vehicle Density on D

Continuous distance anonymity, *D*, is the average distance between a vehicle and other vehicles with which a vehicle is anonymized over the course of an entire trajectory. This is explained in detail in [4].

In general, the lower the density the greater the distance anonymity. But this was not the case for SMP-R. See Fig. 5. See also Table V.

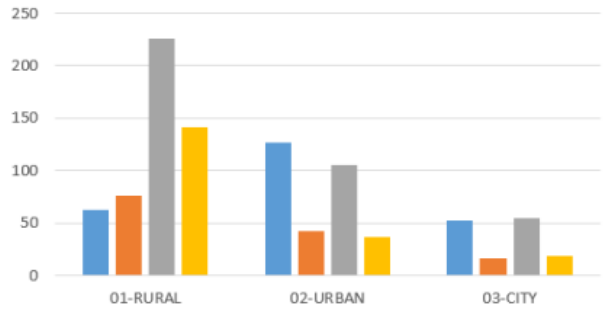

Fig. 5. D (Average Distance Anonymity). The chart above shows three clusters of four bars. The four bars are average distances between anonymized vehicles over their trajectories under simulated conditions for SMP-R, SMP-I, OTFP-R and OTFP-I, respectively. Y-axis indicates average distance in meters.

TABLE V
D (AVERAGE DISTANCE IN METERS)

DENSITY	SMP-R	SMP-I	OTFP-R	OTFP-I
RURAL	62.51	76.26	225.58	140.88
URBAN	127.18	42.63	105.03	36.18
CITY	52.54	16.98	54.20	18.98

In the simulation vehicles that anonymized either went in the same direction, or diverged at angles, or diverged in opposite directions. Since most roads in the simulation intersected at right angles, vehicles which diverged at angles were likely to have diverged at right angles. If a vehicle anonymized with a vehicle going the same direction then distance anonymity would be near zero for the entire trajectory, reducing *D*. The greater the number of vehicles anonymized, i.e. the greater the vehicle density, the greater the reduction in *D*.

In SMP-R and SMP-I protocols vehicles always anonymized near an intersection. Each vehicle had an equal chance of anonymizing with another vehicle going, say, north, south, east or west. The difference between SMP-R and SMP-I is that the irregular time intervals meant that in SMP-I a greater proportion of vehicles anonymized going in the same direction—enough to overwhelm the clumpiness effect.

In OTFP-R and OTFP-I vehicles usually anonymized at a point other than an intersection. They were much more likely to have anonymized with vehicles going in the same direction or in opposite directions. Vehicles going in the same direction reduce *D*. Vehicles going in opposite directions maximizes *D*, but minimizes *T*. (See next subsection.) Stated more plainly, OTFP protocols mixed with vehicles going in the same direction and opposite directions, but they were anonymized with vehicles going in the same direction for a much longer period of time. This explains why the pattern for OTFP-R and OTFP-I demonstrated the pattern: the lower the density the greater the distance anonymity.

E. Effect of Vehicle Density on T

Continuous time of anonymity, *T*, is the average duration of an entire trajectory during which a vehicle is anonymized with at least one other vehicle. This is described in detail in [4].

OTFP outperformed SMP protocols in terms of duration of anonymity, *T*. See Fig. 6. See also Table VI.

This is due to the fact that under OTFP more vehicles traveled in the same direction and thereby stayed in anonymity sets longer than in SMP circumstances. This effect was more pronounced in higher densities.

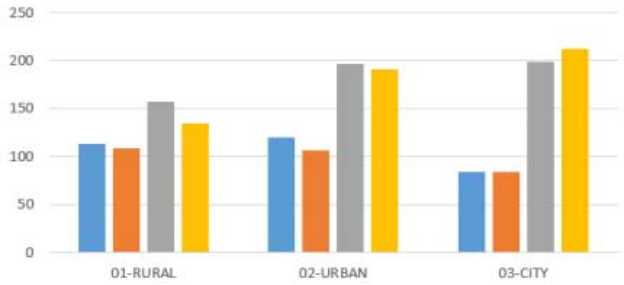

Fig. 6. T (Average Duration/Time of Anonymity). The chart above shows three clusters of four bars. The four bars are average trajectory times between anonymized vehicles over their trajectories under simulated conditions for SMP-R, SMP-I, OTFP-R and OTFP-I, respectively. Y-axis indicates time in seconds.

TABLE VI
T (AVERAGE TIME IN SECONDS)

DENSITY	SMP-R	SMP-I	OTFP-R	OTFP-I
RURAL	113.70	109.23	156.89	134.65
URBAN	119.95	106.87	197.03	190.42
CITY	83.65	83.94	198.58	212.44

VI. CONCLUSION AND FUTURE WORK

This paper offered methods of measuring network performance given different vehicle density conditions and four active decoy protocols. It also evaluated protocols using those metrics. This study did not test extremely high congestion situations, such as football stadiums or big-city traffic jams.

This paper has shown the following.

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.

ACKNOWLEDGEMENT

This paper is based in part upon work supported by Saginaw Valley State University (SVSU) Undergraduate Research Program as part of a research grant. Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of SVSU.

This research work is partially supported by the National Science Foundation under Grants CNS-1338105, CNS-1343141, CNS-1460897, DGE-1623713. Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing 2(1), 46–55 (2003).

[2] Shokri, R., Freudiger, J., & Hubaux, J. P. (2010). A unified framework for location privacy. 3rd Hot Topics in Privacy Enhancing Technologies (HotPETs).

[3] Corser, G., Fu, H., Shu, T. D'Errico, P., Ma, W., Leng, S., Zhu, Y. (2014, June). Privacy-by-Decoy: Protecting Location Privacy Against Collusion and Deanonymization in Vehicular Location Based Services. In 2014 IEEE Intelligent Vehicles Symposium. IEEE. Dearborn, MI.

[4] Corser, G. P., Fu, H., & Banihani, A. Evaluating Location Privacy in Vehicular Communications and Applications. IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 9, pp. 2658-2667, Sept. 2016.

[5] Corser, G. P., Arenas, A., & Fu, H. (2016, February). Effect on vehicle safety of nonexistent or silenced basic safety messages. In 2016 International Conference on Computing, Networking and Communications (ICNC) (pp. 1-5).

[6] Kenney, J. B., Bansal, G., & Rohrs, C. E. (2011, September). LIMERIC: a linear message rate control algorithm for vehicular DSRC systems. In Proceedings of the Eighth ACM international workshop on Vehicular inter-networking (pp. 21-30).

[7] Baumann, R., Legendre, F., & Sommer, P. (2008, May). Generic mobility simulation framework (GMSF). In Proceedings of the 1st ACM SIGMOBILE workshop on Mobility models (pp. 49-56). ACM.

[8] http://gmsf.sourceforge.net/

[9] http://www.lst.inf.ethz.ch/research/ad-hoc/car-traces

[10] Beresford, A.R., Stajano, F.: Mix zones: user privacy in location-aware services. In: Pervasive Computing and Communications Workshops, pp. 127–131 (2004)

[11] Lu, R., Li, X., Luan, T. H., Liang, X., & Shen, X. (2012). Pseudonym changing at social spots: An effective strategy for location privacy in vanets. Vehicular Technology, IEEE Transactions on, 61(1), 86-96.