Endpoint Protection Zone (EPZ): Protecting LBS User Location Privacy Against Deanonymization and Collusion in Vehicular Networks

George Corser, Huirong Fu, Tao Shu
Computer Science and Engineering Department
Oakland University
Rochester, MI - USA

Patrick D'Errico[1], Warren Ma[2]
[1]The College of New Jersey
Ewing Township, NJ - USA
[2]Emory University, Atlanta, GA - USA

***Abstract*—In vehicular networks when map databases may be used to deanonymize user locations, we propose location based services, LBSs, be designed so that LBS users are grouped by spatial location, into endpoint protection zones, EPZs. Users in the same EPZ would share login credentials, and remain transmission-silent until outside of the EPZ, thus preventing an LBS administrator from knowing which particular user from the EPZ is active—even if the LBS administrator colludes with administrators of roadside units, RSUs. Simulations using realistic vehicle traffic mobility models measure improvements in privacy protection under varying EPZ sizes and vehicle densities.**

Keywords—location based service, LBS, k-anonymity, security, location privacy, VANET, DSRC/WAVE, SAE J2735, IEEE 1609.2

I. Introduction

Vehicular ad-hoc networks, VANETs, present distinctive location privacy challenges. VANETs are governed by standards called Dedicated Short Range Communications / Wireless Access in Vehicular Environments, DSRC/WAVE, which require vehicles to transmit precise locations several times per second. Location based services, LBSs, may also require continuous, precise location data. LBS administrators could *deanonymize* LBS users' origin/termination locations, *endpoints*, by cross-referencing home/work addresses using Google Maps or a similar map database, and thereby identify or track a driver. How can motorists protect their vehicle's location privacy under such conditions?

This problem is important because the solution will to some extent shape society. What is socially acceptable depends on what is technically possible. If no technical solution emerges to enable drivers to protect the privacy of their vehicles' locations, then, perhaps, surveillance may be unpreventable, therefore socially acceptable. Employers, for example, might monitor an employee's car parked at a competitor's office (revealing an employee's job interview) or at specialized medical facilities (revealing an employee's health condition). It is not difficult to construct scenarios for further privacy breaches arising from vehicle surveillance by spouses and ex-spouses, paparazzi and other stalkers.

The location privacy challenge from a technical standpoint is large-scale and complicated in VANETs. Equipment supporting wireless/wifi networks is already being installed in new vehicles. Industry representatives estimate that 90% of vehicles will be wifi-connected within the decade [1]. LBS usage continues to grow rapidly [2] and is expected to expand to VANET platforms [3]. Standards governing VANETs [4] have outlined sophisticated encryption schemes to enable privacy, but researchers continue to find privacy vulnerabilities inherent in VANET protocols and vehicle mobility patterns.

Spatial cloaking has been the standard solution to the LBS location tracking problem. The idea is, if k LBS users are operating in a spatial area, s, then k,s-privacy is achieved. The problem is, if LBS requests are repeated frequently over time, and only one of the k LBS users is consistent throughout the set of cloaked requests, then that user is exposed. Researchers have modified spatial cloaking to preserve k-anonymity even when LBSs receive continuous requests. However, no research has been performed which addresses the dual protocol stacks of vehicular networks and the distinctive mobility patterns of vehicular users.

We propose location based services, LBSs, be designed so that LBS users are grouped by spatial location into endpoint protection zones, EPZs. Users in the same EPZ would share login credentials, and remain transmission-silent until outside of the EPZ, thus preventing an LBS administrator from knowing which particular user from the EPZ is active—even if the LBS administrator colludes with administrators of roadside units, RSUs. Our contribution is the EPZ model, a solution to the continuous, precise vehicle location problem under deanonymization and collusion. We also measure the effectiveness of this solution.

The rest of this paper is organized as follows. Section II provides background and related work. Section III presents the EPZ model. Section IV discusses metrics and measurements. Section V presents simulation and performance analysis. Section VI concludes the paper and suggests implications and directions of future research.

II. Background and Related Work

It is difficult to protect location privacy in vehicle networks due to the need for continuous precise location information. To achieve faster-than-human reaction times, safety applications transmit precise positions every 300 ms or more [5]. Concealing vehicle coordinates would render safety applications useless. Spatially shifting coordinates would render them dangerous.

978-1-4799-2491-2/13/$31.00 ©2013 IEEE

DOI 10.1109/ICCVE.2013.92

A. Privacy Mechanisms, Link Layer (RSU)

PKI. Researchers have proposed encryption techniques which, while not concealing vehicles' precise locations, do conceal identities of vehicles. To ensure safety-related messages are valid, transmissions include public key certificates. DSRC standards enable *message authenticity* by providing standards for encryption through public key infrastructure, PKI. DSRC standards achieve *identity privacy* by using temporary identifiers, i.e., temporary media access control addresses, *temp-MAC*s, and temporary pseudo-identities, *pseudoIDs*, with their corresponding *digital certificates*. Permanent, real identifiers are not transmitted. Certificates are issued for pseudoIDs—thousands per vehicle—each valid for perhaps five or ten minutes during the course of a given year. [5]

Temporary identifiers provide only limited *location privacy*. On one hand, if a malicious system administrator, a *tracker*, were to *mark* a target using its temp-MAC or pseudoID, he would not be able to track a vehicle for very long because the identifier would periodically change, perhaps every five or ten minutes. On the other hand, if a single vehicle changed its identifier while all other nearby vehicles maintained their identifiers, then a tracker might determine a vehicle's current identifier is correlated to its prior one. Theoretically a tracker could track a vehicle for a period of time longer than the duration of the temporary identifier.

Group signatures. Researchers have proposed various solutions to the temporary identifier tracking problem. They have recommended groups of neighboring vehicles synchronize times (e.g., silent periods) and locations (e.g., mix zones) when and where they change pseudo-identities [6]. One subset of proposals describes a *group model* in which vehicles travel in clusters, all using the same group temporary identifier, and authenticating messages using the same *group signature* [7]. The group model has been shown to be effective in achieving anonymity in wireless/WSMP communications but it is less effective the lower the vehicle density, since anonymity level depends on the number of vehicles in each group. Some researchers suggest the group model is infeasible due to limitations of bandwidth and computation power, since pseudoID schemes create large *certificate revocation lists*, CRLs, and associated *checking costs*, network overhead necessary to verify that certificates have not been revoked [8].

These solutions do not protect against deanonymization.

B. Privacy Mechanisms, Higher Layers (LBS)

Motorists may be more vulnerable to location tracking when they access an LBS. The identity used to log in to the LBS may not be temporary, which may extend trackability time while logged in to the LBS. Further, transmissions and LBS queries may be correlated, deanonymized, using public databases, such as home address databases, which may diminish the identity privacy protection provided by temporary identifiers. Group signatures have been suggested as a solution to this problem, too [9], though we suggest *group logins* where the group is defined by an EPZ. Neither group signatures nor group login protect against deanonymization, and neither defends against LBS/RSU collusion.

Trusted server. Some privacy models require a proxy server which acts as a privacy-protecting intermediary between vehicles and applications. Spatial cloaking schemes usually require a trusted server. The two basic problems with this technique are cost and trust. There is additional overhead and hardware costs, and there is the need to trust a server which can itself become a target or vulnerability.

Spatial cloaking. Spatial cloaking is not always feasible in vehicular situations when LBSs require precise, continuous vehicle location information. While a single request can be obfuscated by a spatial cloak, a series of requests makes it ever more difficult to protect the link between the identity of a user and his location. If a user requests *k,s*-privacy in several snapshots, the snapshots might be assembled to identify which user is common to all requests. Of course, if one end of the trajectory could be deanonymized, the user's identity might be linked with his location.

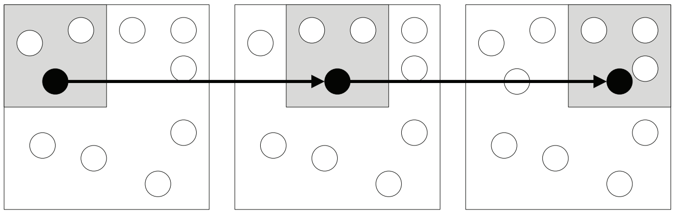

Fig. 1. Spatial cloaking in a series of three snapshots: A vehicle maintains *k,s*-privacy at each snapshot but the snapshots may be assembled to isolate the user, especially if the user is issuing the same query across snapshots.

Dummy events. A few studies have explored the use of dummy events, i.e., counterfeit transmissions, in continuous, precise location situations. Instead of transmitting a spatially cloaked region in a single LBS request, a user would transmit multiple LBS requests, each containing a specific location, perhaps real, perhaps fake. Users would achieve location privacy by *k*-anonymity since LBS administrators could not tell which of *k* precise locations is genuine. The problem with this solution is under LBS/RSU collusion the LBS administrator could determine which locations were fake if the request used a false location. Even if the LBS user used real locations from real vehicles in its transmission range, the spatial range of the fakes would be limited by the vehicle's wireless communications range; that is, the decoy might be undetectable but it might be so close to the real vehicle that the location privacy achieved would be minimal.

These solutions do not protect against deanonymization.

C. DSRC protocol stack

The FCC dedicates a 75 MHz spectrum in the 5.9 GHz band for wireless communication between vehicles. IEEE and SAE have established standards, DSRC/WAVE, to achieve interoperability between devices communicating in this spectrum. The protocol stack features two distinct protocol sets. See Fig. 2. IPv6/TCP/UDP typically would be used in communication vehicle-to-infrastructure, V2I, such as accessing Internet applications like infotainment or LBSs. WAVE short message protocol, WSMP, would typically be used in communications vehicle-to-vehicle, V2V, such as safety applications. For a discussion of WAVE, see [14].

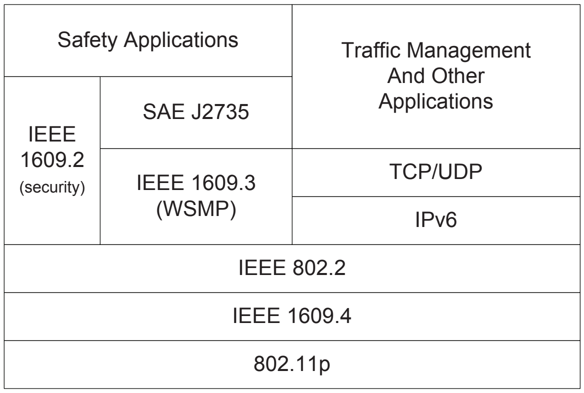

Fig. 2. DSRC protocol stack

Internet applications are assumed to include a wired network infrastructure component, while safety applications are assumed to be wireless-only. Internet applications such as LBSs present new location privacy vulnerabilities to motorists because LBS administrators may be able to monitor motorists anonymously from anywhere in the Internet from the comfort of their own cubicles. Safety applications present new location privacy vulnerabilities because the SAE J2735 standard would require vehicles to transmit their precise locations every 100ms over a 300m radius. This Basic Safety Message, BSM, or heartbeat message could be used to pinpoint a target vehicle.

III. EPZ Model

Imagine *www.HomeOwnerMobile.com*, a fictional LBS which displays on your car's dashboard the names of the owners of homes in view. It might also display the prices of the homes, if they are for sale, or the most recent price paid, if they are not for sale, assuming this is public information. Such a service would simplify the process of shopping for a home, but it would also require continuous precise location information from the vehicle making the request. What if the shopper does not want LBS administrators to know his identity?

Suppose the LBS is constructed in such a way that LBS users who live near each other use the same login credentials. Suppose those users remain completely transmission-silent while driving in their specially designated area near their own home or workplace, i.e. their endpoint protection zone, EPZ. Then, if there are k users in the EPZ, each user achieves k-anonymity. The LBS administrator cannot identify which member of the EPZ is requesting the information.

A. *EPZ Grids*

The EPZ model divides a region, R, of width, W, and height, H, into grids of rectangles of width, w, and height, h. Let V be the total number of vehicles in R. Let λ be the ratio of LBS users to V, so the number of LBS users in R is λV. Assuming a uniform distribution of random variable V in R, the expected anonymity set size for an LBS user is as follows.

$$E\{ AS_{EPZ} \} = k = \lambda V wh / WH \qquad (1)$$

In the EPZ model all LBS users in an EPZ protect each others' location privacy by using the same login credentials. See Fig. 3.

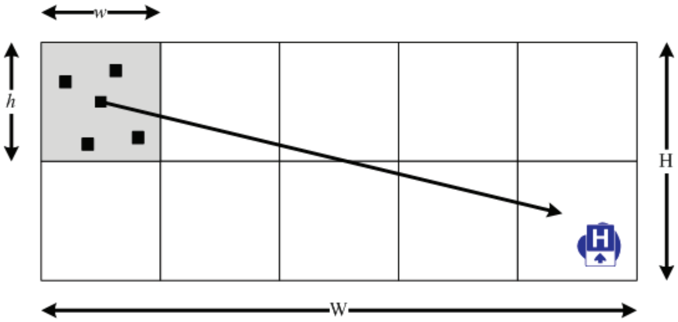

Fig. 3. The proposed model divides regions into square sections, called endpoint protection zones, EPZs.

B. *Threat Model*

Attackers can be categorized by the scope of their surveillance capabilities. If the attacker can observe the entire system of vehicles, we define him as a *global* attacker, even though the scope of the system may only include a single municipality. If the attacker has access only to a subset of the system, such as the communications range of an RSU, we refer to the attacker as *local*. Attackers can also be categorized by their intent, *passive* or *active*, i.e. whether they intend merely to monitor targets or whether they also intend to mislead or otherwise influence targets.

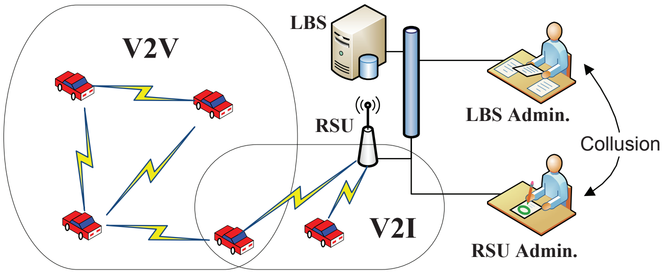

Fig. 4. VANET system model and threat model addressed in this paper

TABLE I. Location Privacy Attacks by LBS Administrator

LBS User Action	LBS Administrator Attack
Transmit precise home location	Identify user with deanonymization*
Obfuscate position with spatial cloaking	Isolate trajectory from snapshots, then identify user with deanonymization*
Do not transmit to LBS inside EPZ, but always transmit safety messages	Isolate trajectory from snapshots, then collude with RSU to correlate paths, then identify user with deanonymization*
Remain transmission silent within EPZ	Cannot deanonymize* (no identifiable endpoint)

* LBS administrator uses endpoint (origination or termination) to deanonymize

This paper assumes a global passive adversary at the LBS colluding with a local passive adversary at the RSU nearest the vehicle under surveillance. This global-local adversary may be an "insider" with legitimate authority to monitor these systems, or the attacker may have acquired/hacked such access illegally.

We assume the adversary wishes to determine the location of a target vehicle, and that the adversary may have already linked the target's LBS userID with a pseudo-identity of a vehicle within range of an RSU or another vehicle. Table 1 outlines potential LBS administrator attack scenarios.

C. Limitations of the Model

For each LBS user driving inside his EPZ, this model prevents *sending* safety and traffic management data, reducing some functionality of the system. The model also precludes infotainment while in one's own EPZ. For other vehicles, the model degrades safety and traffic management functionality to the extent vehicles are operating in their own EPZ. We envision EPZs to be as small as possible to mitigate these limitations. Also, not all LBS users will care about privacy. This model protects only those users who do.

The model does not defend against license plate readers, mobile phone monitoring, roadside cameras, and physical surveillance. These attacks are outside the scope of this paper.

IV. Metrics

In the VANET security literature, privacy is often equated to anonymity. Even the IEEE 1609.2 (2013) security standard [4] itself does so, saying, "Anonymity—meaning the ability of private drivers to maintain a certain amount of privacy—is a core goal of the system." A frequently used metric is *k*-anonymity, though others include *l*-diversity [10] *t*-closeness [11], and ε-differential privacy [12]. This paper confines itself to the concept of *k*-anonymity, or anonymity set size, defined below. In this paper we measure privacy by anonymity set size, entropy of the anonymity set size and tracking probability. For a discussion of this topic, see [13].

Anonymity set size. The anonymity set, AS_i, of target LBS user, *i*, is the collection of all LBS users, *j*, including *i*, within the set of all LBS userIDs, *ID*, whose trajectories, T_j , are indistinguishable from T_i .

$$AS_i = \{ j \mid j \in ID, \exists T_j \ \ s.t. \ \ p(i,j) \neq 0 \} \tag{2}$$

The anonymity set size, $|AS_i|$, equals *k*, by definition.

Entropy of the anonymity set size. Entropy represents the level of uncertainty in the correlations between trajectory T_i and trajectories T_j. The entropy H_i of the anonymity set AS_i is:

$$H_i = -\sum_{j \in AS_i} p(i,j) \times \log_2(p(i,j)) \tag{3}$$

Tracking probability. Tracking probability, Pt_i, is the probability that the size of the anonymity set of a vehicle under surveillance is equal to one, which can be written as follows.

$$Pt_i = P(|AS_i| = 1) \tag{4}$$

This metric is important because average *Pt* tells what percentage of vehicles have privacy, not just how much privacy exists in the overall system. If $AS_i = k = 1.0$, then a vehicle has no defense against tracking.

V. Simulation

A. Simulation Setup

Since no real-world VANET system was available, using real LBSs, real RSUs, and real vehicles to test our model was impossible. We used simulation to evaluate the model. To prepare the simulation we used realistic vehicle mobility models and estimated privacy levels using custom simulation software we wrote in the Python programming language.

1) Mobility Models

Computer simulations do not always represent vehicle traffic flows accurately. Harri, et al. [15] suggest that minimum requirements for realistic simulations include techniques for intersection management, lane changing and car following. Several systems offer these features, including Generic Mobility Simulation Framework, GMSF [16]. We used Multi-agent Microscopic Traffic Simulator, MMTS, trace files linked from the GMSF website [17] and provided at the Laboratory for Software Technology website [18], specifically City, Urban and Rural. All three models contain records of time-stamps, vehicle-ids, x-coordinates, y-coordinates within a 3000x3000 meters (9 million square meters) grid. Each model 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 system at roughly the same rate, so the number of vehicles in the model at any given time is not always precisely the same as the number at the start.

Road topologies in some mobility models, such as the Freeway model (a straight road with perhaps several lanes) and the Manhattan model (a grid of horizontal and vertical roads), 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 model might have a linear density of 0.3 v/m, 900 vehicles divided by 3000 meters, and a square density of 0.0001 v/m^2, 900 vehicles divided by 9 million square meters. The Manhattan model 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 model. In other words, the linear density of the Manhattan model is 1.6% that of Freeway model given the same square density.

Our simulation does not have this problem because the linear distances covered by the road topologies are similar: City, 14,783 meters; Urban, 13,955 meters; and Rural, 10,175 meters. The areas covered are identical, so the mobility models we used provide both realistic traffic flows and comparable coverage distances and areas.

2) Metrics Computations

We wrote a program which read MMTS mobility model files, city, urban and rural. Each mobility model has a different vehicle density in the same size region. The program divided each 3000m x 3000m region into square EPZs, ranging from 300m x 300m (100 EPZs) to 1500m x 1500m (4 EPZs). For each mobility model the program computed the metrics, |AS|, H(|AS|) and *Pt*. All simulations covered vehicle movements over a time period of 2000s, or 33.3 minutes.

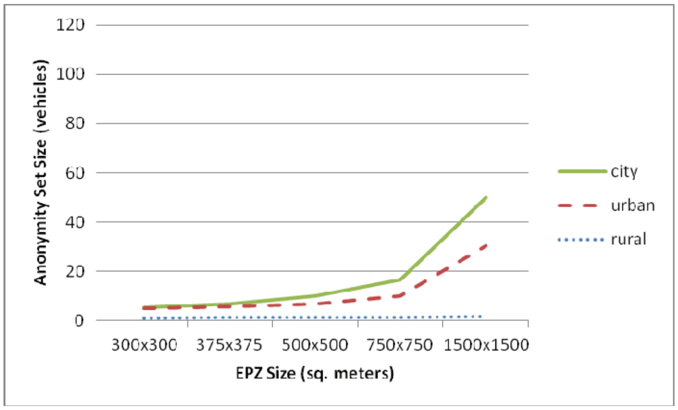

Fig. 5. Average anonymity set size by EPZ size, 10% LBS users.

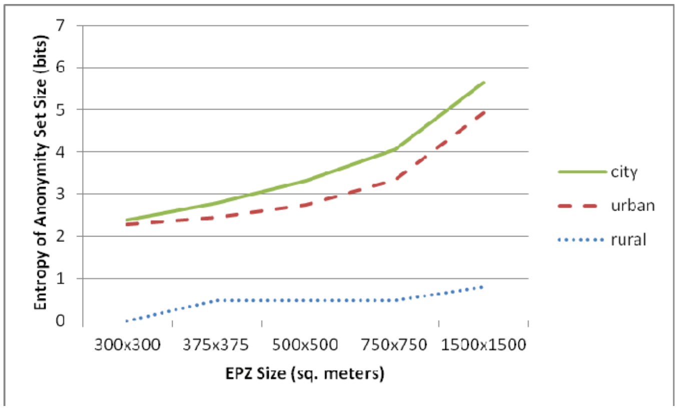

Fig. 6. Entropy of average anonymity set size by EPZ size, 10% LBS users.

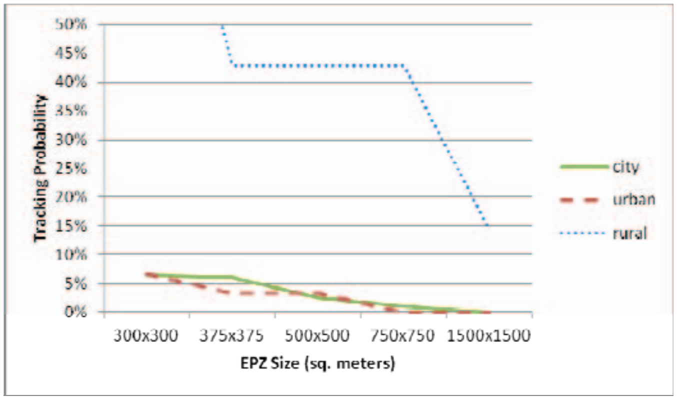

Fig. 7. Tracking probability by EPZ size, 10% LBS users.

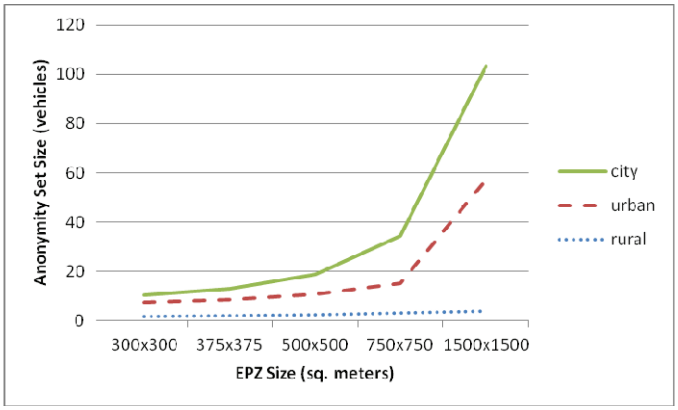

Fig. 8. Average anonymity set size by EPZ size, 20% LBS users.

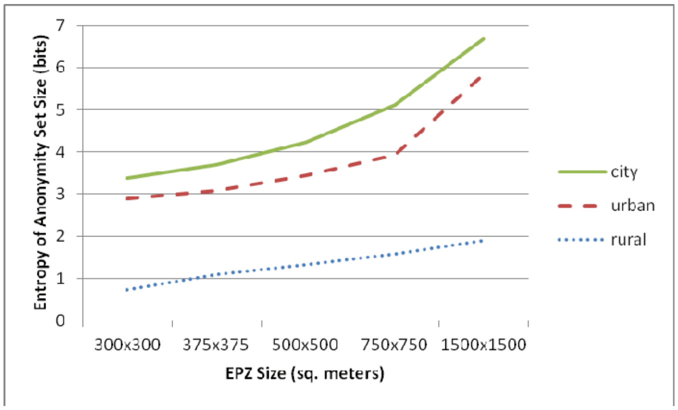

Fig. 9. Entropy of average anonymity set size by EPZ size, 20% LBS users.

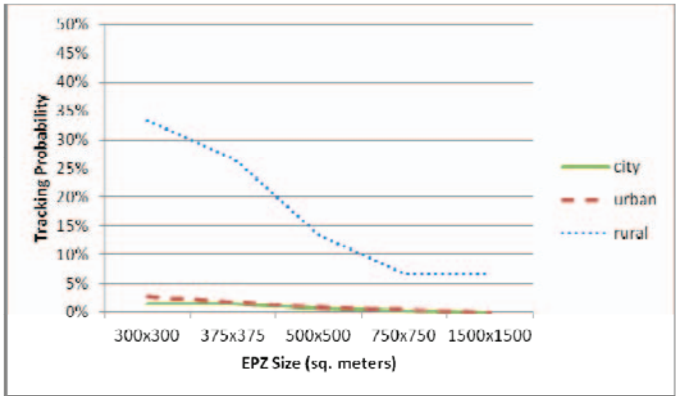

Fig. 10. Tracking probability by EPZ size, 20% LBS users.

B. Performance Evaluation

The EPZ model was effective only in sufficiently high density areas. When vehicle density, and therefore LBS user density, was low, and EPZ sizes were small, then anonymity set sizes approached 1.0 and tracking probabilities approached 100%, which represents the poorest possible privacy protection under our metrics.

Figs. 5, 6 and 7 show results when λ=10%. Figs. 8, 10 and 11 show results when λ=20%. Doubling λ doubled |AS| and H(|AS|), but at low densities it more than halved *Pt*.

Anonymity set size. Average anonymity set size for the high-density city model ranged from 5.26 (100 EPZs) to 50 (4 EPZs); for the medium-density urban model, from 4.84 to 30.25; for the low-density rural model, from 1.0 to 1.75. In other words, an attacker would have roughly a 1/5 to 1/50 chance of identifying the target vehicle in the city model; a 1/5 to 1/30 chance in the urban model; but a 1/1 to 1/2 chance in the rural model. Low density settings would require a different method, or EPZs larger in size than the sizes we tested.

Entropy of the anonymity set size. Average entropy ranged from 2.39 to 5.64 for city; 2.27 to 4.92 for urban; and 0 to 0.81

for rural. Again, low density settings would require a different method, or EPZs larger in size than the sizes we tested.

Tracking probability. Average tracking probability ranged from 7% to 0% for the city model; 7% to 0% for the urban model; and 100% to 14% for the rural model. The model is of little use in areas of low density given the EPZ sizes we tested.

In practice the model may need to be modified so that the density of LBS users determines EPZ size, not the other way around. Further experimentation may determine the optimal breakeven EPZ size given the tradeoff between privacy protection and service degradation.

In computing the total number of vehicles, V, we ignored vehicles whose trajectories originated at the edge of the region. Vehicles whose trajectories originated on the edge were assumed to belong to EPZs located outside of the region. More details and the program code for this simulation can be obtained from *www.vanetprivacy.com*.

VI. Conclusions and Future Work

Endpoint protection zones, EPZs, protect vehicle location privacy from deanonymization. If LBS administrators can correlate origin and destination points with home and work addresses, they can link identity and location of vehicle owners. This is not possible if vehicles remain transmission-silent in their respective EPZs.

EPZs protect vehicle location privacy from collusion between LBS administrators and RSU administrators. Even if LBS administrators can verify with RSUs the locations of transmissions at their points of origination, they cannot be certain which vehicle from the EPZ is making the request unless they have additional information beyond the scope of this study.

The effectiveness of EPZs depends upon density, multiple LBS users originating from each EPZ. In sparsely populated areas, the EPZ model may be ineffective. One workaround might be encouraging local friends and family to use LBS. Another workaround might be to increase EPZ sizes in sparsely populated areas. The practicality of this is a subject of future study. Perhaps the most important finding of this paper is that a small increase in LBS users in a sparsely populated area, which may yield only a proportional effect in anonymity set size, may have a much greater effect on tracking probability.

An interesting property of the EPZ model is that it provides protection even if only one LBS user from an EPZ is active outside that EPZ. The LBS administrator cannot know *which* LBS user is active. This implies that LBS users especially concerned about privacy could register under multiple false identities, or have friends and family who do not use the LBS register under real identities. In this way a single person could achieve *k*-anonymity > 1.0.

EPZs do not protect against many forms of surveillance, such as license plate readers, mobile phone monitors, roadside cameras or physical surveillance. However, against collusion and deanonymization attacks, EPZs may be a useful tool in high density areas to protect vehicular location privacy.

Acknowledgment

This work is partially based upon work supported by the National Science Foundation under Grant No. 1062960. 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] Bush, I. (2013, Feb 25). GM, AT&T readying in-vehicle wi-fi. http://philadelphia.cbslocal.com/2013/02/25/gm-att-readying-in-vehicle-wi-fi/

[2] Johnson, L. (2012, Oct 31). Location-based services to bring in $4b revenue in 2012: study. http://www.mobilemarketer.com/cms/news/research/14115.htmlhttp://www.mobilemarketer.com/cms/news/research/14115.html

[3] Koslowski, T. (2012, Jan 3). Your connected vehicle is arriving. http://www.technologyreview.com/news/426523/your-connected-vehicle-is-arriving/

[4] IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," IEEE Std 1609.2-2013 (Revision of IEEE Std 1609.2-2006) , vol., no., pp.1,289, April 26 2013, doi: 10.1109/IEEESTD.2013.6509896

[5] Kenney, John B. "Dedicated short-range communications (DSRC) standards in the United States." Proceedings of the IEEE 99.7 (2011): 1162-1182.

[6] Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K., & Sezaki, K. (2005). CARAVAN: Providing location privacy for VANET. Washington Univ Seattle Dept Of Electrical Engineering.

[7] Jinhua Guo; Baugh, J.P.; Shengquan Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," 2007 Mobile Networking for Vehicular Environments , vol., no., pp.103,108, 11-11 May 2007, doi: 10.1109/MOVE.2007.4300813

[8] Sun, Y., Lu, R., Lin, X., Shen, X., & Su, J. (2010). An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications. Vehicular Technology, IEEE Transactions on, 59(7), 3589-3603.

[9] Shokri, Reza, Julien Freudiger, and Jean-Pierre Hubaux. "A unified framework for location privacy." 3rd Hot Topics in Privacy Enhancing Technologies (HotPETs) (2010).

[10] Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1), 3.

[11] Li, Ninghui, Tiancheng Li, and Suresh Venkatasubramanian. "t-closeness: Privacy beyond k-anonymity and l-diversity." Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on. IEEE, 2007.

[12] Dwork, Cynthia. "Differential privacy." Automata, languages and programming. Springer Berlin Heidelberg, 2006. 1-12.

[13] Beresford, Alastair R., and Frank Stajano. "Location privacy in pervasive computing." Pervasive Computing, IEEE 2.1 (2003): 46-55.

[14] Uzcategui, R.; Acosta-Marum, G., "Wave: A tutorial," Communications Magazine, IEEE, vol.47, no.5, pp.126,133, May 2009, doi: 10.1109/MCOM.2009.4939288

[15] Harri, Jerome, Fethi Filali, and Christian Bonnet. "Mobility models for vehicular ad hoc networks: a survey and taxonomy." Communications Surveys & Tutorials, IEEE 11.4 (2009): 19-41.

[16] Baumann, Rainer, Franck Legendre, and Philipp Sommer. "Generic mobility simulation framework (GMSF)." Proceedings of the 1st ACM SIGMOBILE workshop on Mobility models. ACM, 2008.

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

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