2014 IEEE Intelligent Vehicles Symposium (IV)
June 8-11, 2014. Dearborn, Michigan, USA

Privacy-by-Decoy: Protecting Location Privacy Against Collusion and Deanonymization in Vehicular Location Based Services*

George Corser, Huirong Fu, Tao Shu, Patrick D'Errico, Warren Ma, Supeng Leng, Ye Zhu

Abstract— **Wireless networks which would connect vehicles via the Internet to a location based service, LBS, also would expose vehicles to online surveillance. In circumstances when spatial cloaking is not effective, such as when continuous precise location is required, LBSs may be designed so that users relay dummy queries through other vehicles to camouflage true locations. This paper introduces PARROTS, Position Altered Requests Relayed Over Time and Space, a privacy protocol which protects LBS users' location information from LBS administrators even (1) when the LBS requires continuous precise location data in a vehicular ad hoc network, (2) when LBS administrators collude with administrators of vehicular wireless access points (a.k.a. roadside units, or RSUs), and (3) when precise location data might be deanonymized using map databases linking vehicle positions with vehicle owners' home/work addresses and geographic coordinates. Defense against deanonymization requires concealment of endpoints, the effectiveness of which depends on the density of LBS users and the endpoint protection zone size. Simulations using realistic vehicle traffic mobility models varying endpoint protection zone sizes measure improvements in privacy protection.**

I. Introduction

This paper considers the continuous precise location vehicle tracking problem. How can a vehicle protect itself against surveillance even while using a location based service, LBS, which may require frequent hyper-accurate location data?

Vehicular ad-hoc networks, VANETs, present distinctive location privacy challenges. In the United States standards are specified by Dedicated Short Range Communications / Wireless Access in Vehicular Environments, DSRC/WAVE. These standards call for MAC-layer transmissions of precise vehicle locations several times per second. DSRC can be used to access the Internet, including LBS applications which may also require frequent precise location data. Without privacy protections in place, system administrators could track specific vehicles, or cross-reference vehicles' precise origin and termination location data with home and work addresses, using Google Maps or some similar map database, perhaps revealing ("deanonymizing") the identity of a driver present at a given location at a given time. This could occur at either the MAC layer or higher layers.

This problem is important because driver location data can be misused. Employers 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 further privacy breaches arising from vehicle surveillance by spouses and ex spouses, or 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 a 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 (a derivative form of k-anonymity [26] is achieved [14]. But 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 deanonymization possible under DSRC protocol stacks and mobility patterns of vehicular users.

A prior paper [6] suggested that location based services, LBSs, be designed with LBS users grouped by spatial location into endpoint protection zones, EPZs. Users in the same EPZ would share login credentials (or log in anonymously), 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. This paper further proposes LBSs be designed so that users relay dummy/false queries through non-LBS-user vehicles to camouflage true locations.

Our main contributions are (1) a new way of looking at vehicular location privacy, called privacy-by-decoy, PBD, (2) a PBD model, and (3) a comparison of EPZ alone with EPZ and PBD. The representative PBD model is called Position

*Research supported by National Science Foundation (NSF).

G. C., H. F., and T.S. Authors are with Oakland University, Rochester, MI 48309 USA (gpcorser@oakland.edu).

P. D. Author is with The College of New Jersey, Ewing Township, NJ 08618 USA.

W. M. Author is with Emory University, Atlanta, GA 30322 USA.

S. L. Author is with University of Electronic Science & Technology, Chengdu CHINA.

Y. Z. Author is with Cleveland State University, Cleveland, OH 44115 USA.

Altered Requests Relayed Over Time and Space, or PARROTS.

The rest of this paper is organized as follows. Section II provides background and related work. Section III presents the PARROTS 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 at the MAC layer. To achieve faster-than-human reaction times, safety applications transmit precise positions every 100 ms. Concealing vehicle coordinates would render safety applications useless. Spatially shifting coordinates would make them dangerous.

A. Privacy Definitions and 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." The most frequently mentioned metric is *k*-anonymity [26], though others include *l*-diversity [17] *t*-closeness [18], and ε-differential privacy [19]. This paper confines itself to the concept of *k*-anonymity, or a closely related concept, anonymity set size.

This paper measures privacy in three ways: anonymity set size, entropy of the anonymity set size and tracking probability. All three are based on the anonymity set size of a vehicle under surveillance. For a deeper discussion of this topic, see [20].

B. Location Privacy Preserving Mechanisms

Shokri [10] identifies four location privacy preserving mechanisms: hiding events, adding dummy events, obfuscation and anonymization. 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 [26] 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 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.

At least six previous works have studied the use of dummy events in protecting location privacy. Chow and Golle [11] suggest dummy vehicle locations be generated by adding noise to traces from a trip planner. Researchers in [12] propose generating dummy locations in the same neighborhood as the genuine current location. Krumm [13] recommends generating dummy locations entire trajectories, full trips, using algorithms which offer realistic vehicular mobility modeling and derive positions from databases of previously-recorded real driver locations. Researchers in [14] advocate dummy location generation using either a local grid called a virtual grid, similar to [12], or a virtual circle, which ensures *k,s*-privacy. Researchers in [15] advise a scheme which randomly generates dummy locations rotating with movement patterns that consistent with observed human movement, though not vehicle movement. Researchers in [16] study packet routing issues.

None of these studies except Krumm generate dummies from realistic vehicular mobility models, let alone from actual vehicle positions. None consider the threat model in which LBS administrators collude with RSU administrators. None use *active decoys*, i.e. false locations (dummy events) of real vehicle locations transmitted by vehicles other than the target vehicle. Besides the EPZ model we are aware of no study to date which has examined the deanonymization of endpoints in VANETs under LBS/RSU collusion.

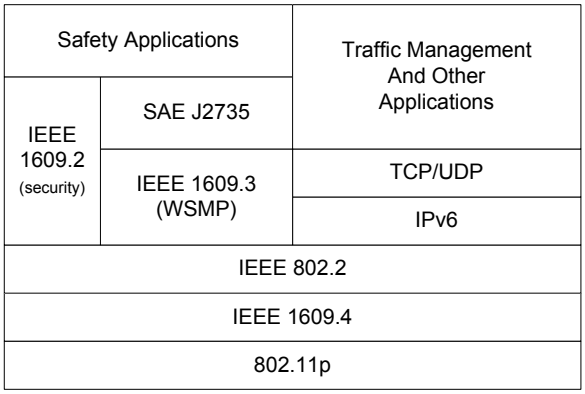


Fig. 1. Two DSRC protocol stacks, WSMP (left) and TCP/IPv6 (right)

The FCC dedicates a 75 MHz spectrum in the 5.9 GHz band for DSRC. Wireless communication between vehicles is better known as vehicle-to-vehicle (V2V) communication. Wireless vehicle-to-infrastructure (V2I) communication occurs between vehicles and roadside units (RSUs).

C. DSRC Protocol Stacks

DSRC features two distinct network/transport layer protocols. See Fig. 1. IPv6/TCP/UDP typically would be used in V2I, such as accessing Internet applications like infotainment or LBSs. WSMP, WAVE short message protocol, would typically be used in V2V communications, especially safety applications, though WSMP is not limited to V2V. For a more thorough discussion of WAVE, see [21].

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 accurately pinpoint a target vehicle.

III. PARROTS MODEL

A. Threat Model

Attackers can be categorized by the scope of their surveillance capabilities. If the attacker can observe the entire system of vehicles, this is a *global* attacker, even though the scope of the system may only include a single region or municipality. If the attacker has access only to a subset of the system, such as the communications range of an RSU, this attacker is *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 in some way.

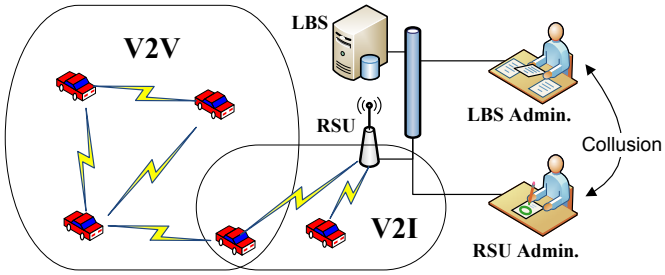


Fig. 2. Threat model under study in this paper

This paper assumes a global passive adversary, with access to LBS and RSU. In practice this may be two local adversaries colluding, one with access to LBS the other with access to RSU nearest the vehicle(s) under surveillance. See Fig. 2. This global adversary may be an "insider" with legitimate authority to monitor these systems, or the attacker may have acquired/hacked such access illegally. This paper assumes the adversary wishes to determine the location of a target vehicle, and that the adversary may have already linked the target with a certain pseudo-identity of a vehicle.

B. EPZ Equation

The EPZ model [6] divides regions into grids of rectangles of width, w, and height, h. Let V be the total number of vehicles in a region, R, of area, A. Let λ be the ratio of LBS users in the same region, so the number of LBS users in R is λV. The expected anonymity set size for LBS is then described by equation (1).

$$E\{ AS_{EPZ} \} = \lambda V w h / A \quad (1)$$

In the EPZ model all LBS users in an EPZ protect each others' location privacy by using the same group login credentials. This is enforced by the LBS when the user registers with the service; the EPZ is calculated at the point of registration after which the location information is discarded.

C. PARROTS Description

The EPZ Model can be enhanced by adding decoys. Consider a regime in which helper vehicles, called *parrots*, relay LBS requests on behalf of an LBS user in a vehicle desiring privacy, called a *pirate*. The pirate would transmit LBS requests normally. Parrots would transmit LBS requests on behalf of the pirate, using the pirate's login credentials but the parrots' locations. Parrots' locations could not be identified as fakes because they are real locations in real current traffic conditions. Parrots could mimic pirates over great temporal and spatial range.

In order for this scheme to work LBS systems must permit login credentials to be sent encrypted, but vehicle locations unencrypted. After all, if the LBS user's credentials are not encrypted a malicious parrot could misuse the pirate's credentials. And if the location is encrypted the parrot would not be able to perform the encryption since the parrot would not possess the pirate's private key.

Under this system there is no leakage of any information from the pirate to the parrot save the destination address of the LBS. Encryption prevents parrots from reading pirates' login information, query information or responses from LBSs since LBSs encrypt replies with the pirates' public keys.

Under this system the LBS cannot determine which vehicles are pirates and which are parrots. The login credentials are authentic, and the locations are real. Location privacy is achieved by k anonymity if a pirate has k-1 parrots. If LBSs permit group logins then even greater anonymity is accomplished.

By relaying each others' dummy queries, vehicles can protect each other from surveillance by LBS administrators – even if those administrators collude with administrators of other system infrastructure components such as RSUs. This protection can be accomplished if LBS software accepts authorizations using encrypted group userIDs, passwords and service requests, along with unencrypted locations.

In a traditional online system, such as Foursquare, used at a desktop or laptop computer or on a smart phone, a user may log in manually with a userID and password. Then, either the user may manually enter a location query, or the application may infer the location from contextual information such as the IP address or GPS information of the client computer. Using group signatures, authorization could be accomplished on a group basis. A traditional service permits users to log in from any computer. A secure session, such as occurs under HTTPS, would be authenticated using SSL certificates of the computers, not of the LBS userIDs, to allow multiple secure logins of LBS users.

The PARROTS model proposes that LBSs operate like traditional services, except the login information is enclosed in an encrypted message, and the location information is unencrypted. A vehicle which wishes to be parroted, a "pirate," sends an encrypted LBS authentication message to a vehicle which is willing to relay the decoy messages, a "parrot." The parrot relays to the LBS the pirate's encrypted message appended with the parrot's location. The pirate sends to the LBS the pirate's encrypted message appended with the pirate's location. The result is that the LBS administrator does not know which location is the location of the pirate – even if he can verify through IP traceback which vehicle is the source of each message.

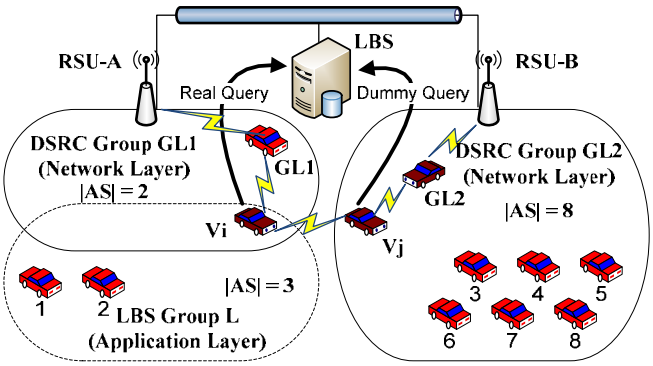
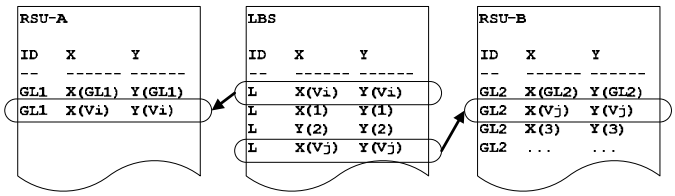


Fig. 3. LBS users form groups to protect themselves from potentially snooping LBS administrators. Individual LBS users may communicate with other vehicles which agree to relay the LBS user's dummy queries, increasing the anonymity set size, |AS|, of the entire LBS group.



RSU-A

ID	X	Y
GL1	X(GL1)	Y(GL1)
GL1	X(Vi)	Y(Vi)

LBS

ID	X	Y
L	X(Vi)	Y(Vi)
L	X(1)	Y(1)
L	Y(2)	Y(2)
L	X(Vj)	Y(Vj)

RSU-B

ID	X	Y
GL2	X(GL2)	Y(GL2)
GL2	X(Vj)	Y(Vj)
GL2	X(3)	Y(3)
GL2	...	...

Fig. 4. The reports above provide the information available to administrators of RSU-A, LBS and RSU-B, respectively, as modeled in Fig. 2. Notice that the |AS| of group L rises from 3 to 4 because of Vj, even though Vj is not part of LBS. If LBS administrator performs IP traceback he finds query originated from the location queried.

Fig. 3 shows how vehicle Vj could be contacted by vehicle Vi while in communication range. Vj would send no genuine queries of its own to the LBS, but rather it would send fake queries on behalf of Vi. Normally, the LBS would think Vi's request was from one of the members of LBS Group L, but in reality one query is coming from Vj, posing as a member of LBS Group L. If the LBS administrator performs an IP traceback to RSU-B, he will confirm the vehicle sending the transmission is in fact at the location queried, [X(Vj), Y(Vj)]. So, with parroting, the anonymity set size increases by 1 for every member of Group L. This is shown by the increase in LBS ID group L in Fig. 4.

D. Definitions and Assumptions

PARROTS depends on PKI. Each party in a secure communication has a public and private key. Define CA as the certificate authority which issues identities and certificates, including pseudo identities, or pseudoIDs, for vehicles. Let Vi indicate a vehicle with pseudoID *i*. Let Vj indicate a vehicle with pseudoID *j*. Assume pseudoIDs are valid for short periods of time, say 5-10 minutes, as in [5].

Let RSU refer to a roadside unit, a wireless access point for vehicles to connect to the wired infrastructure. Let LBS indicate a location based service. Let POI mean "point of interest," such as a restaurant or gas station. Let "request" be defined as a message asking for information, such that an LBS request would be a message asking for information from the LBS. Let Ui indicate the identity of LBS user in Vehicle i. Assume Ui is an email address, so it can have an associated public key, indicated by a trailing plus sign, Ui+. Define Cert(Ui) as the digital certificate binding Ui's email address and public key such that Cert(Ui) = CA-(Ui, Ui+).

Let "pirate" be defined as the vehicle of an LBS user who wishes to be mimicked. Let "parrot" be defined as a vehicle, not necessarily linked to any LBS user, willing to mimic the pirate. If Vi wishes to be mimicked, then Vi would be a pirate. If Vj is willing to mimic Vi, then Vj would be a parrot.

Assume LBS users have userID/password combinations which do not expire as quickly as vehicular pseudoIDs and temporary MAC addresses. Further assume LBS users may log in to the LBS from any computer/vehicle.

E. PARROTS Equations

The PARROTS model depends on EPZs. Recall equation (1). Now let ρ be the ratio of potential parrots, so the number of potential parrots in R is ρV. Note that the set of LBS users and the set of potential parrots are disjoint sets. Now let φ be the ratio of LBS users who desire privacy. Note if all LBS users desired privacy, φ=1. The expected anonymity set size for an LBS user under the EPZ model with PARROTS if the LBS enforces single-user login is as follows.

$$E\{ AS_{EPZpi} \} = 1 + \rho / \varphi \lambda \qquad (2)$$

The expected anonymity set size for an LBS user under the EPZ model with PARROTS, if the LBS uses group logins, is as follows.

$$E\{ AS_{EPZpg} \} = (\lambda + \rho)\, wh/A \qquad (3)$$

IV. Performance Metrics

Anonymity set size. In equation (2), AS_i is the anonymity set of vehicle *i*. ID is the pool of all possible pseudo-identifiers for all vehicles in the system. T_i and T_j are trajectories associated with pseudo-identifiers *i* and *j* and $p(i,j)$ is the a-posteriori probability that T_i correlates with T_j. AS_i contains all vehicles indistinguishable from the target vehicle. The anonymity set size, $| AS_i |$, is the number of elements in AS_i, which is a measure of location privacy for pseudonym identifier *i*. AS_i includes all pseudoIDs whose trajectories cannot be distinguished from *i*. In the case of the group model, this is the set of all current pseudoIDs belonging to the group.

$$AS_i = \{ j \mid j \in ID, \exists T_j \ s.t. \ p(i,j) \neq 0 \} \qquad (4)$$

The privacy measure supported by the anonymity set size is that if two vehicles change their pseudoIDs at the same time, the stalker has only a 50% chance of continuing to track the correct vehicle. The more vehicles in the anonymity set, the lower the odds of the stalker tracking the right vehicle.

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

$$H_i = -\sum_{j \in AS_i} p(i,j) \times \log_2(p(i,j)) \qquad (5)$$

The privacy measure supported by the entropy of the anonymity set size is that more disorderly and unpredictable the system, the more difficult it is for the stalker to track vehicles.

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.

$$Pt_i = P(|AS_i| = 1) \quad (6)$$

The privacy measure supported by the tracking probability is that the more vehicles that have $|AS_i| > 1$ the less chance that a stalker can track any particular car. This measure says if Pt_i=100% then all vehicles in the system can be tracked using their pseudoIDs. If Pt_i = 50% then only half of the vehicles can be tracked precisely because the other half have $|AS_i| > 1$.

V. Simulation

A. Simulation Setup

A simulation system was written using realistic vehicle mobility models. The system estimated privacy levels by calculating the metrics above under various EPZ sizes and parroting parameters.

1) Mobility Models

Computer simulations do not always represent vehicle traffic flows accurately. Researchers in [22] 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 [23], the website for which offers Multi-agent Microscopic Traffic Simulator, MMTS, trace files linked from the GMSF website [24] and provided at the Laboratory for Software Technology website [25], 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.

A problem with using 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), is that 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 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. The simulation upon which this paper is based does not suffer from 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 mobility models provide both realistic traffic flows and comparable coverage distances and areas.

2) Metrics Computations

The simulation software read the mobility model file and for each mobility model and computed the traditional metrics, AS_i, H_i and Pt_i,. All simulations covered a time of 2000s, or 33.3 minutes. The software divided a 3000m x 3000m region into square EPZs, ranging from 1500m x 1500m (4 EPZs) to 300m x 300m (100 EPZs).

B. Performance Evaluation

Fig. 5 summarizes the results of the simulation. It compares AS_i, H_i and Pt_i for two models: EPZ alone and EPZ with PARROTS, group login. The software simulated using 10% LBS users (λ=0.10) and 10% potential parrots (ρ=0.10 and φ=1.00). In computing V, the software 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.

1) EPZ Alone

Simulation showed that the EPZ model is effective to the extent that multiple LBS users have endpoints in EPZs. When vehicle density, and therefore LBS user density, is low, and EPZ sizes are small, then anonymity set sizes approach 1 and tracking probabilities approach 100%, which represents the poorest possible privacy protection under the privacy metrics. EPZ works, but only with sufficient vehicle and LBS user densities.

2) EPZ with PARROTS, Group Login

The PARROTS model with group login performed better than any other scenario tested. The effect of EPZ with group login, combined with PARROTS, produced anonymity set sizes close to the theoretical value, and showed visible improvement in tracking probabilities. Compare Figs. 5(e) and 5(f).

3) EPZ with PARROTS, Individual Login

The PARROTS model with individual login performed worse than the EPZ model alone, except in low density situations PARROTS demonstrated equivalent results. The reason for this is because PARROTS' performance depends not on the density of LBS users but on the ratio of potential parrots to pirates. In all cases, regardless of vehicle density, anonymity set size was near 2, the theoretical value.

VI. Conclusion and Future Work

This is the first paper to present active decoys as a privacy defense in continuous, precise LBS query conditions in a VANET system. EPZ requires no additional network transmissions to establish privacy levels, so there is no bandwidth tradeoff for implementation, though there are service quality and safety tradeoffs during silent periods. PARROTS requires a recruitment phase and multiple duplicate transmissions by parroting vehicles, which would add some network congestion overhead, as would the

parroting of false messages. However, if only relatively few vehicles desire privacy, parroting could be useful, especially under special conditions. The EPZ and PARROTS protocols address conditions, (1) when the LBS requires continuous precise location data in a vehicular ad hoc network, (2) when the LBS administrator colludes with administrators of vehicular wireless access points (a.k.a. roadside units, or RSUs), and (3) when precise location data can be deanonymized using map databases linking vehicle positions with vehicle owners' home/work addresses. Simulation under realistic mobility models showed PARROTS increased average privacy levels in high vehicle density conditions when deployed in combination with EPZs, and increased them even more effectively in low vehicle density.

Neither PARROTS nor EPZs 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 to protect vehicular location privacy. PARROTS enhances the effectiveness of EPZs. Other vehicle location privacy methods which use decoys for

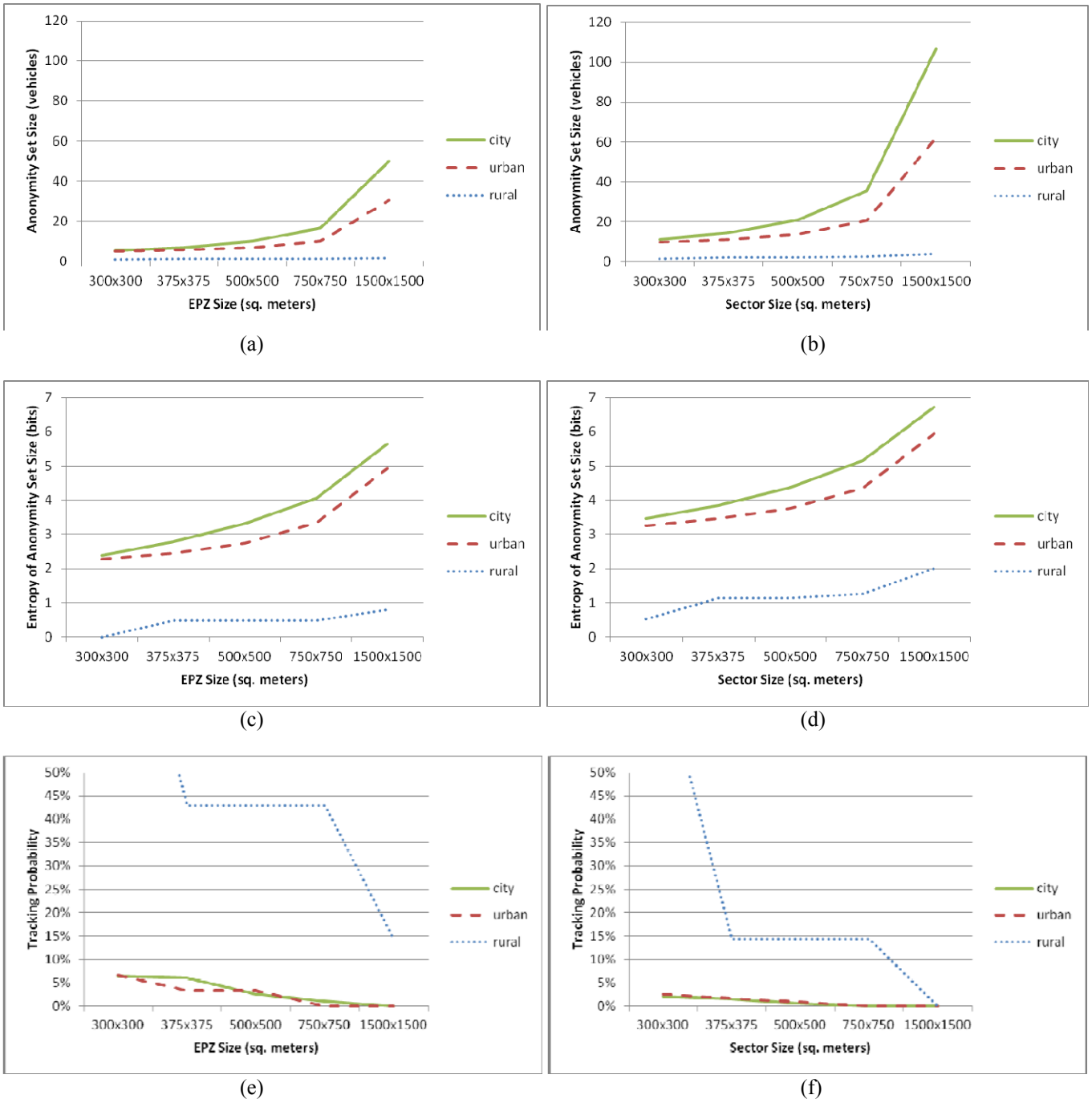


Fig. 5. (a) EPZ alone, anonymity set size, (b) EPZ with PARROTS, group login, anonymity set size, (c) EPZ alone, entropy of anonymity set size, (d) EPZ with PARROTS, group login, entropy of anonymity set size, (e) EPZ alone, tracking probability, (f) EPZ with PARROTS, group login, tracking probability.

protection would transmit dummy events while the real LBS querier is active. The PARROTS model is unusual in that parrots can make requests of an LBS on behalf of pirates even when pirates are inactive. Under the specific conditions presented in this paper, it has the further benefit of enabling undetectable decoys over a spatial range broader than the communications range of the LBS querier.

This study compared the privacy performances, not the network efficiencies, of the models. In future work we hope to run simulations to determine tradeoffs and optimal balances between a broader set of factors: safety (silent period), network performance (efficiency) and privacy (anonymity).

ACKNOWLEDGMENT

This work is 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.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] Corser, G., Fu, H., Shu, T., D'Errico, P., Ma, W. (2013). "Endpoint Protection Zone (EPZ): Protecting LBS User Location Privacy Against Deanonymization and Collusion in Vehicular Networks." The 2nd International Conference on Connected Vehicles & Expo (ICCVE 2013).

[7] 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.

[8] Guo, J., Baugh, J. P., & Wang, S. (2007, May). A group signature based secure and privacy-preserving vehicular communication framework. In 2007 Mobile Networking for Vehicular Environments (pp. 103-108). IEEE.

[9] 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.

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

[11] Chow, R., & Golle, P. (2009, November). Faking contextual data for fun, profit, and privacy. In Proceedings of the 8th ACM workshop on Privacy in the electronic society (pp. 105-108). ACM.

[12] Kido, H., Yanagisawa, Y., & Satoh, T. (2005, July). An anonymous communication technique using dummies for location-based services. In Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on (pp. 88-97). IEEE.

[13] Krumm, J. (2009). Realistic driving trips for location privacy. In Pervasive Computing (pp. 25-41). Springer Berlin Heidelberg.

[14] Lu, H., Jensen, C. S., & Yiu, M. L. (2008, June). Pad: Privacy-area aware, dummy-based location privacy in mobile services. In Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access (pp. 16-23). ACM.

[15] You, T. H., Peng, W. C., & Lee, W. C. (2007, May). Protecting moving trajectories with dummies. In Mobile Data Management, 2007 International Conference on (pp. 278-282). IEEE.

[16] Yang, Q., Lim, A., Ruan, X., & Qin, X. (2010, December). Location privacy protection in contention based forwarding for VANETs. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE (pp. 1-5). IEEE.

[17] 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.

[18] Li, N., Li, T., & Venkatasubramanian, S. (2007, April). t-closeness: Privacy beyond k-anonymity and l-diversity. In Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on (pp. 106-115). IEEE.

[19] Dwork, C. (2006). Differential privacy. In Automata, languages and programming (pp. 1-12). Springer Berlin Heidelberg.

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

[21] 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

[22] Harri, J., Filali, F., & Bonnet, C. (2009). Mobility models for vehicular ad hoc networks: a survey and taxonomy. Communications Surveys & Tutorials, IEEE, 11(4), 19-41.

[23] 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.

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

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

[26] Sweeney, Latanya. "k-anonymity: A model for protecting privacy." International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10.05 (2002): 557-570.

[27] Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. In Proceedings of the 1st international conference on Mobile systems, applications and services (pp. 31-42). ACM.