Protecting Location Privacy with Clustering Anonymization in Vehicular Networks

Bidi Ying
School of Information & Electronic Engineering
Zhejiang Gongshang University
Hangzhou, China
yingbidi@mail.zjgsu.edu.cn

Dimitrios Makrakis
School of Electrical Engineering and Computer Science
University of Ottawa
Ottawa, Canada
dimitris@eecs.uottawa.ca

Abstract—Location privacy is an important issue in location-based services. A large number of location cloaking algorithms have been proposed for protecting location privacy of users. However, these algorithms cannot be used in vehicular networks due to constrained vehicular mobility. In this paper, we propose a new method named Protecting Location Privacy with Clustering Anonymization (PLPCA) for location-based services in vehicular networks. This PLPCA algorithm starts with a road network transforming to an edge-cluster graph in order to conceal road information and traffic information, and then provides a cloaking algorithm based on *k*-anonymity and *l*-diversity as privacy metrics to further enclose a target vehicle's location. Simulation analysis shows our PLPCA has good performances like the strength of hiding of road information & traffic information.

Keywords—vehicular networks; cluster; location privacy; location-based services

I. INTRODUCTION

Vehicular ad-hoc network (VANET) is a promising technology expected to play an important role in road safety, traffic management, and information dissemination to drivers and passengers [1]. The VANET enables useful functions like cooperative driving and probe vehicle data, and offers access to Location-Based Service (LBS) applications [2-3]. A LBS makes spatial data available to the drivers through one or more Location Providers (LPs) which index and answer drivers' queries. An example of spatial queries could be “where is the closest hotel to my current location” or “what is the traffic condition on highway 411”.

However, with semi-trust LPs which are revealing users' information like positions and identities, it is easier for an attacker to launch active attacks such as a forgery attack. For example, inquiring for pharmacies offers medicines for diseases associated with a social stigma. Such user privacy is really important and should be protected. To solve this problem, pseudonyms are generated in such (predefined) a way that an adversary cannot link the new pseudonym of a vehicle to the one used previously by this vehicle [4-5]. Unfortunately, using a pseudonym is not sufficient because the user's location itself may disclose his/her real-world identity.

Location cloaking [6-7, 9-12] is a commonly-used approach to protect user's location privacy in LBSs. Exact coordinates are replaced with a Cloaking Region (CR) which contains the user's location and satisfies privacy requirements. Privacy requirements are specified by user's attributes like its identity and location, and implemented with *k*-anonymity [9] as a privacy metric. *k*-anonymity is the most prominent location privacy metric, and aims to protect user's privacy. In such scenarios, the objective is to protect the exact location of the user who is issuing the LBS query, and the requirement is that each CR must contain at least *k* distinct users. This way, the probability of identifying the querying user's location is bounded above by 1/*k*.

However, due to the constraints vehicular mobility has (e.g. vehicles have to be moving on a transportation network), there have vehicle's location and movement scenarios that weaken the level of the privacy protection. For example, if all vehicles in the CR are located on the same single road segment, it is easier for an attacker to track down the target vehicle compared to when the vehicles are spreading over many different road segments. Besides, an attacker can know the transportation network and the number of vehicles moving on a road segment by setting monitoring devices, and use this information can guess which road segment the target vehicle is located on with a high probability. Therefore, *k*-anonymity is not applicable in vehicular networks.

To avoid the above problems, we propose a novel method named Protecting Location Privacy with Clustering Anonymization (PLPCA) for LBSs. This method firstly provides an edge-cluster graph concept and transforms a road map into the edge-cluster graph; thus, it can conceal road information & traffic information. We use the strength of hiding information to measure information associated with the road map and the edge-cluster graph. Then, we provide a cloaking algorithm whose CR has at least *k* vehicles (*k*-anonymity) and *l* road segments (*l*-diversity). This cloaking algorithm provides definitions of a cloaking cycle & a simple loop, and principles of how to determine the optimum cloaking cycle. Finally, we conduct a series of experiments to evaluate the performance of the proposed PLPCA using location data generated from a road map——Oldenburg Country. Experimental results show that our proposed PLPCA is efficient in terms of the strength of hiding of road information & traffic information, size of cloaking region.

The remainder of the paper is organized as follows. In section II, the related work is surveyed. Section III presents the preliminaries and attack model. Section IV describes our

978-1-4799-3088-3/14/$31.00 ©2014 IEEE

PLPCA in details. Section V provides performance analysis results. Finally, section VI concludes the paper.

II. Related Work

Location privacy is gaining increasing interests in vehicular networks. Multi-pseudonyms and mix-zones are used to prevent an attacker from linking the new pseudonym of a vehicle to the one used previously by this vehicle [4-5]. Unfortunately, using a pseudonym is not sufficient because the user's location itself may disclose his/her real-world identity.

Location cloaking has been extensively studied to protect vehicle's location privacy [6-8]. Gruteser and Grunwald first proposed to achieve identity anonymity in LBS by spatiotemporal cloaking based on a *k*-anonymity model. In this case, the cloaking region should include at least *k* users [9]. The extensions of cloaking based on the *k*-anonymity model have been studied [10-12] from various aspects like bandwidth usage of requested services, user's specific privacy requirement, location information accuracy. In addition, some cloaking algorithms are proposed to issue continuous LBS queries by a target user [19-22]. A location obfuscation method proposed by Xu is used to protect location privacy of continuous LBS queries by using a log of historical user locations rather than the real-time location information to generate cloaking regions [20]. However, the privacy metric for these techniques, is not feasible in the vehicular network because the cloaking region might contain a single road segment, which enables the attacker to track down the vehicle easily.

Liu et al. proposed ExapandCloak[13] which is based on the *l*-diversity model [14]. A cloaking region contains at least *k*-users and *l*-diversity query contents. As the use of entropy of *l*-diversity, it may be too restrictive when the users' points of interests distribution is non-uniform. This way can make an attacker link query contents with a specific user with a high probability. Bamba et al. proposed a *k*-anonymity and *l*-diversity method that the query issuer could not be identified from *l* different physical locations (such as buildings and postal addresses) [15]. J-H. Um et al. proposed a cloaking method. This method creates a minimum cloaking region by finding *l* number of buildings (*l*-diversity), and finds *k* number of users (*k*-anonymity) by using R*-tree based index [16]. Dewri et al. developed a cloaking region method based on *m*-invariance (query contents) in the continuous LBS queries [17]. However, these works are focusing on how to hide query contents, not dealing with cloaking regions. Besides, *l*-diversity in these schemes is different with our work. For our work, *l*-diversity means different road segments.

Wang firstly proposed an approach based on *k*-anonymity and *l*-diversity for the vehicular network [18]. The cloaking algorithm is to construct a star network from a road network, and to establish a cloaking region based on *k*-anonymity and *l*-diversity. In the star network, each vertex whose degree is ≥ 3 represents a star node, and two vertices are adjacent if their corresponding star nodes in the road network share a common segment. This approach can improve the privacy level of LBSs. However, if a star node does not satisfy the privacy requirements, it needs to be expanded super-star. This will increase the LBS query process cost. Besides, an attacker still can know the road network and traffic information from the star network, and then can guess vehicle's privacy with a high probability. Different from [18], our PLPCA transfers a road map into edge-cluster graph to conceal road information & traffic information, and uses a cloaking cycle to reduce the size of the final cloaking region. Therefore, our PLPCA has good performances.

III. Preliminaries and Attack Model

For the reader's convenience, we provide the definitions of notations appearing in the remaining of this work in Table I.

TABLE I. Notations

Parameter	Meanings
G_C	Edge-cluster graph $G_C = (V_C, E_C)$, where V_C is a set of vertices, and E_C is a set of edges.
$d_C(n)$	Degree if a vertex n in G_C
G	Road graph G=(V, E), where V is a set of vertices, and E is a set of roads.
C_t	A vertex in G_C
$\|C_t\|$	Total number of vehicles in C_t
d_t	Sum degree of C_t 's two corresponding point ends in G
D_V	The strength of hiding of traffic information(which is caused by removing vehicles' attributes)
D_E	The strength of hiding of road information(which is caused by transforming all edges of the graph G into the vertices of the graph G_C)
S_i	Simple loop i
$\|S_i\|$	Total number of vehicles in S_i
L_i	Length of the simple loop S_i
CC_i	Cloaking cycle i
$\|CC_i\|$	Total number of vehicles in cloaking cycle CC_i
l_i	Total number of road segments in cloaking cycle CC_i
Λ	Total number of simple loops in the cloaking cycle discovery phase
Υ	Total number of cloaking cycles in the cloaking cycle discovery phase

A. Preliminaries

In [18], a road model was proposed as an undirected graph G=(V, E) with the node set V and the edge set E representing road intersections and road segments, respectively. In addition, each edge has a set of vehicles with their attributes, such as vehicles' identities and locations. Combinations of such attributes together with LBS queries could be leaking vehicles' privacy by means of tracing attacks.

Assume that a vehicle is moving along a road segment, and sends its LBS query together with its current location. Upon receiving the LBS query, the third trusted Anonymizer (AZ) computes a cloaking region including the target vehicle, replaces the target vehicle's location with the cloaking region, and forwards it to location providers. If all vehicles from the cloaking region are on the same single road segment, it is easier for an attacker to track down the target vehicle. Therefore, we give the following definition of the location privacy model which the cloaking region should satisfy:

Definition 1: (*k*, *l*, $l_{\max}$, $A_{\max}$)-Location privacy model. The trusted anonymizer has to meet the following parameters for protection vehicles' location privacy when cloaking regions.

(1) *k*: It means *k*-anonymity, in other words, each cloaking region should cover at least *k* different vehicles. The larger the value of *k* is, the stronger the offered privacy is.

(2) *l*: It means *l*-diversity, in other words, each cloaking region should contain at least *l* different road segments. The larger the value of *l* is, the stronger the offered privacy is.

(3) $l_{\max}$: It represents the maximum number of road segments which a cloaking region has. The larger the value of $l_{\max}$ is, the worse of the query accuracy is as well.

(4) $A_{\max}$: It represents the maximum area that a cloaking region CR_i has, and is a QoS parameter. The larger the value of $A_{\max}$ is, the worse the given query accuracy is as well.

B. Attack Model

An attacker we consider in this paper is a malicious location provider which aims to associate a vehicle's identity with the location. Note that the attacker has known the road network and traffic information (e.g., the number of vehicles in each road segment). Assume that an attacker gains the cloaking region including *k*' vehicles and *l*' road segments ($k' \geq k, l_{\max} \geq l' \geq l$). The attacker firstly can remove these road segments without any vehicles, and then can guess which road segment the target vehicle is located on by knowing the number of vehicles in each road segment.

IV. THE PROTECTION PRIVACY PROTOCOL

A. Anonymization based on Edge-Cluster

Let $\{C_1,...,C_T\}$ be members of a set of *E*, $E=\bigcup_{t=1}^{T} C_t$, and $C_t \bigcap C_s = \phi$ for all $1 \leq t \neq s \leq T$, where *T* is the number of all roads in the road graph. The corresponding edge-cluster graph $G_C = (V_C, E_C)$ of the road graph *G*=(*V*, *E*) is defined as follows:

(1) V_C is a set of nodes in the graph G_C , and is defined the set of *E* in *G*. $V_C = \{C_1,...,C_T\}$.

(2) E_C is a set of edges in the graph G_C . An edge links C_t and C_s in E_C if C_t and C_s are connected in *G*.

(3) Each $C_t \in V_C$ is accompanied by two pieces of information——$|C_t|$ (the number of vehicles that C_t contains), and d_t (the sum degree of C_t 's two corresponding point ends in *G*).

An example of a road network of 6 road intersections and 8 road segments, and a corresponding edge-cluster network with 8 nodes, are given in Fig.1-a and Fig.1-b. C_1 in the edge-cluster graph is corresponding the edge $\overline{n_1 n_2}$ in the road network, and $|C_1|$=3, d_1=6. C_2 is corresponding to the edge $\overline{n_1 n_6}$, and $|C_2|$=3, d_2=5.

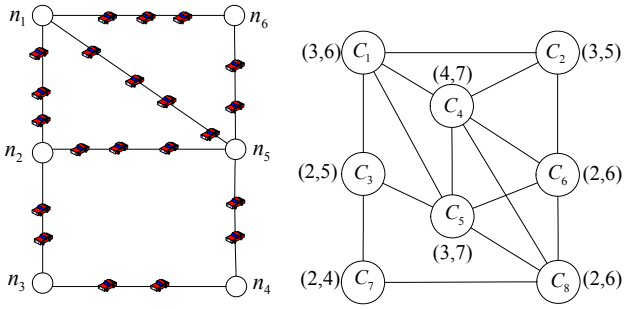

Fig.1-a A road network Fig.1-b Edge-cluster graph

Fig.1 A road network and the corresponding edge-cluster graph

By this definition, this edge-cluster graph possesses the desired properties: (i) it is easy to show the vehicle's local adjacent road segments; therefore, employing it as choosing the nearest segments is expected to lead to an anonymous cloaking region with highly compact structures. (ii) it is obvious to conceal information about the road network, and thus it is easy to enclose vehicles' attributes like identities and locations.

Since information about the road network can be known by an attacker, we replace the road network with an edge-cluster graph to avoid the leakage of this information. Thus, we use the strength of hiding of information to evaluate how much the graph information will be hidden. The higher value of the strength of hiding of information is, the less graph information is known by the attacker.

Given a road network graph *G*=(*V*, *E*) and an edge-cluster graph $G_C = (V_C, E_C)$, the strength of hiding of information associated with replacing the road network by the corresponding edge-cluster network is defined as a weighted sum of the two metrics

$$D = \omega \times D_V + (1-\omega) \times D_E \quad (1)$$

where, $\omega \in (0,1)$ is weighted parameter, D_V is the strength of hiding of traffic information caused by removing vehicles' attributes like identities and locations, D_E is the strength of hiding of road information caused by transforming all edges of the graph *G* into the vertices of the graph G_C .

Assume that each vehicle has *m* attributes, then, these attributes are hidden in a cluster C_t . Thus, the strength of hiding of traffic information in the cluster C_t

$$D_V(C_t) = \frac{|C_t|}{m} \quad (2)$$

The overall the strength of hiding of traffic information is $D_V = \sum_{t=1}^{T} D_V(C_t)$.

Let $d_C(n)$ be the degree of a vertex *n* in the graph G_C . Given two vertices C_t and C_s , the structure of these vertices connected to C_t and C_s is hidden. The strength of hiding of road information is quantified as the probability of wrongly identifying a segment in *G* as a node in G_C , and it equals

$$D_E(C_t, C_s) = (d_C(C_t) + d_C(C_s)) \times (1 - \frac{d_C(C_t) + d_C(C_s)}{d_t + d_s}) \quad (3)$$

The overall strength of hiding of road information for the $C = \{C_1, ..., C_T\}$ is $D_E = \sum_{1 \le t \ne s \le T} D_E(C_t, C_s)$.

B. Cloaking Algorithm based on Edge-Cluster

Definition 2: Cloaking cycle. In an undirected edge-cluster graph, a cloaking cycle should have: (i) there are at least three vertices; (ii) at least two vertices of them have vehicles; (iii) the number of vertices should be $\ge l$ and $\le l_{\max}$; (iv) the number of vehicles should be $\ge k$.

For example, given the parameters of k=12, l=3, $l_{\max}$ =4 and a target vehicle in C_1, (shown in Fig.1-b), the cloaking cycle might includes vertices $<C_1, C_5, C_8, C_4>$, or $<C_1, C_5, C_6, C_4>$, or $<C_1, C_3, C_5, C_4>$, or $<C_1, C_2, C_6, C_4>$.

To find the cloaking region satisfying the (k, l, $l_{\max}$, $A_{\max}$)-location privacy model, it has been turning that this problem is equivalent to the problem of finding the optimum cloaking cycle. Therefore, The cloaking algorithm includes: (1) Discover the cloaking cycle; (2) Determine the optimum cloaking cycle.

1) Discover the cloaking cycle

Definition 3: Simple loop. In an undirected edge-cluster graph $G_C = (V_C, E_C)$, a path of $C_1, C_2, ..., C_t$ becomes a simple loop if (i) $C_1 = C_t$, $1 \le t \le T$; (ii) all nodes of $C_2, ..., C_t$ being unequal.

In order to find the cloaking cycle, we firstly use breadth-first search to find simple loops with their lengths belonging to in the range of [l, $l_{\max}$]. The simple-loop-search algorithm of finding simple loops is bellow:

Input: an undirected edge-cluster graph
Output: simple loops S_i

(a) determine which vertex the target vehicle belongs to in the undirected edge-cluster graph; assume that this node is vertex C_t;
(b) set $i \leftarrow 0$;
(c) choose the vertex C_t and label it with i;
(d) mark all vertices unlabeled;
(e) search the set **J** of vertices that are unlabeled and are adjacent to some vertices labeled with i;
(f) if $\mathbf{J} \ne \phi$, then set $i \leftarrow i+1$. Label the vertices in **J** with i, and go to step #(d);
(g) if $i = l_{\max}$, stop.

After that, we can find Λ simple loops S_i ($1 \le i \le \Lambda$). We represent as L_i ($3 \le L_i \le L$) the length of the simple loop S_i and assume that the simple loop S_i includes vertices $C_t, C_{t+1}, ..., C_{t+L_i-1}$. Thus, the sum number of vehicles in the simple loop S_i is calculated as $|S_i| = |C_t| + |C_{t+1}| + ... + |C_{t+L_i-1}|$. According to the definition 2, we can get Υ ($0 \le \Upsilon \le \Lambda$) cloaking cycles CC_i ($1 \le i \le \Upsilon$) from those Λ simple loops by checking the following conditions —— (i) $l_{\max} \ge L_i \ge l$; (ii) $|S_i| \ge k$; (iii) at least two vertices in the simple loop have vehicles. If Υ equals zero, we have to execute the simple-loop-search algorithm by increasing the value of L in order to expand simple loops.

2) Determine the optimum cloaking cycle

If there exist some cloaking cycles, we have to choose the optimum cloaking cycle which satisfies the following condition —— maximum value of the strength of hiding of traffic information associated with a cloaking cycle. This is because the larger value of the strength of hiding of traffic information is, the higher level of privacy is.

From Eq. (2) & (3), we can achieve that the strength of hiding of traffic information in the cloaking cycle CC_i equals

$$D_{CC_i} = \omega \times \sum_{1 \le t \le l_i} D_V(C_t) + (1-\omega) \times \sum_{1 \le t \ne s \le l_i} D_E(C_t, C_s) \quad (4)$$

where $\omega \in (0,1)$ is weighted parameter, l_i is the total number of road segments in the cloaking cycle CC_i, $D_V(C_t) = \frac{|C_t|}{m}$ and $D_E(C_t, C_s) = (d_C(C_t) + d_C(C_s)) \times (1 - \frac{d_C(C_t) + d_C(C_s)}{d_t + d_s})$, m be the number of a vehicle' attributes.

According to the condition and the (k, l, $l_{\max}$, $A_{\max}$)-location privacy model location, the cloaking region should satisfy:

$$\eta = \max(D_{CC_i}) \quad (5)$$

$$s.t. \begin{cases} |CC_i| > k \\ l \le l_i \le l_{\max} \\ A(CC_i) \le A_{\max} \end{cases}$$

where $|CC_i|$ is the total number of vehicles in the cloaking cycle CC_i, l_i is the total number of road segments in the cloaking cycle CC_i, $A(CC_i)$ is the size of the cloaking cycle CC_i.

V. Performance Evaluations

All our simulation results were performed over a real road map corresponding to the roads in the city of Oldenburg, which contains 6105 nodes and 7035 edges. We simulated traffic conditions using the Network-based Generator of Moving Objects described in [23]. We compared our PLPCA and XStar method [18]. XStar method is included for

comparison because we are interested in finding out *what and how much* is improved by our proposed cloaking algorithms. All cloaking algorithms are implemented in C++ and run on a Lenovo X220 laptop having a dual Intel 2.2GHz processor and 2GB RAM.

A. Measure Strength of Hiding of Information

We provide the strength of hiding of road information versus the level of k in Fig.2. X axis represents the level of k required by the location privacy model. The value of "1/2/3/4/5/6" means the values of k are in the range of [1-8], [9-13], [14-18], [19-23], [24-28], [29-33], respectively. The conclusions are the following: the strength of hiding of road information caused by transforming all edges of the graph G into the vertices of the graph G_C in the case of l=4 & $l_{\max}$ =5 is larger than that in the case of l=3 & $l_{\max}$ =4. This is because more edges in graph G become vertices in graph G_C with the increase of the value of l. Besides, there has only a little impact on the strength of hiding of road information as the increase of the level of k required by the location privacy model.

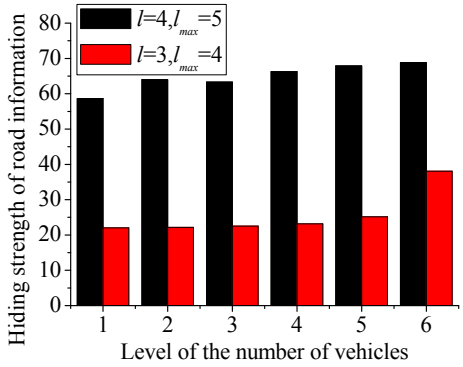

Fig.2 The strength of hiding of road information

Fig.3 shows the strength of hiding of information associated with replacing the road network by the corresponding edge-cluster network varies with the increase of the level of k required by the location privacy model. Y axis represents the strength of hiding of information such as road information and traffic information. As can be seen, in the case of l=4 & $l_{\max}$ =5, the value of the strength of hiding of information (when ω =0.3) is larger than that when ω =0.5. In other words, the strength of hiding of traffic information linked with all vehicles (like their identities, locations) has less impact than the strength of hiding of road information. The main reason is as follows: in PLPCA scheme, road information is completely removed in edge-cluster graph; thus, the strength of hiding of road information has more impact on the strength of hiding of information. From Eq. (4), we also can draw the same conclusion that the strength of hiding of road information has a high affect on the total strength of hiding of information.

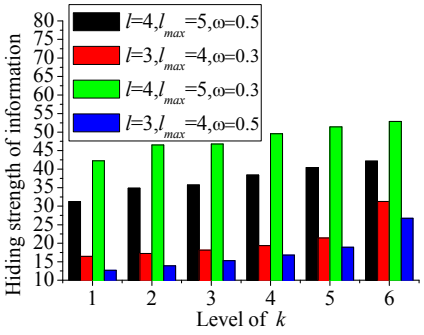

Fig.3 The strength of hiding of information VS level of k

Fig.4 illustrates the strength of hiding of information as the increase of l. This figure shows an uptrend of the strength of hiding of information when the value of l increases. In other words, the larger the value of l is, the stronger the offered privacy is. Another conclusion is that we have a higher the strength of hiding of information when the value of ω decreases. This phenomenon is also explained in Fig.3.

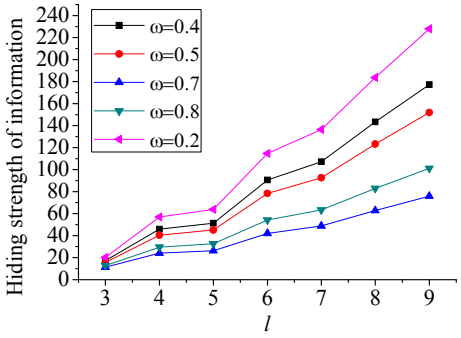

Fig.4 The strength of hiding of information VS l

B. Efficiency

In Fig. 5 displays the cumulative distribution function results of the cloaking area. In the case of l=3 & $l_{\max}$ =4, over 80% of the cloaking regions are less than 68km^2 , while in the case of l=4 & $l_{\max}$ =5, over 70% of the cloaking regions are less than 100km^2. If the shape of the cloaking is square, we can get the length of the cloaking region is about 260 meters in the case of l=3 & $l_{\max}$ =4. This value is acceptable in terms of server query processing overhead [18].

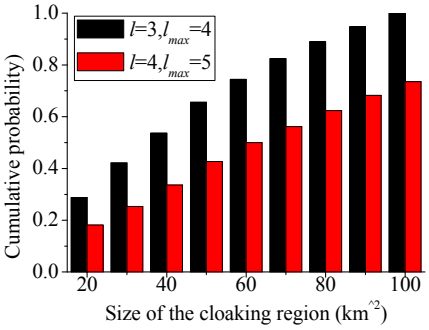

Fig. 5 cumulative distribution function

Fig. 6 & 7 displays the size of the cloaking region under the simulation condition of $l=l_{max}$ in our PLPCA scheme and the Xstar scheme. X axis defines values of l, and Y axis represents the total number of vehicles in the cloaking region. The perpendicular -to X and Y- plane axis displays the size of the cloaking region. From Fig.6, we can see the curve goes up slowly when $l \leq 5$, rises fast from l=5 to l=6, and then turns to a gentle incline from l=6 to l=7. This is because: in the Xstar scheme, the star nodes connects at least 3 road segments; if in the case of l=6, the cloaking region at least needs two star nodes, which leads to the increase of size of the cloaking region fast. In Fig.7, the trend of the curve goes up quickly with the increase of the value of l. Compared to Fig.6, we can see that our PLPCA has smaller size of the cloaking region. This is beneficial to save cost in LBS query processes since it needs less query processes due to small size of cloaking regions.

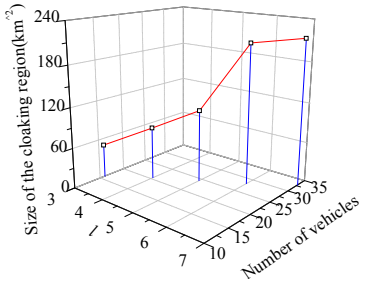

Fig. 6 Size of the cloaking region in Xstar scheme

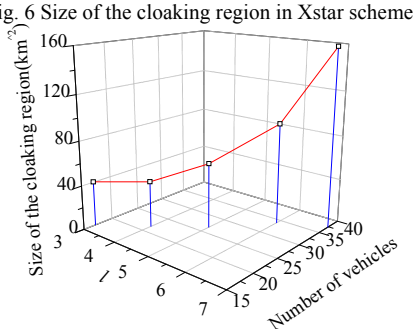

Fig. 7 Size of the cloaking region in our proposed PLPCA scheme

VI. CONCLUSIONS

Most of existing location cloaking algorithms cannot be used in vehicular networks due to constrained vehicular mobility. In this paper, we proposed a new method where it turns a road map into an edge-cluster graph, in order to hide road information & traffic information, and constructs a cloaking cycle based on k-anonymity and l-diversity. The experimental results show that our PLPCA has good performances in terms of the strength of hiding of information and efficiency.

ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of Zhejiang Province LQ13F010001, Y201328392, National Natural Science Foundation of China 61272306&61301142, and SRF for ROCS, SEM (2013[1792]).

REFERENCES

[1] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, 15(1):39-68, 2007.

[2] H. Baik, M. Gruteser, X. Hui, A. Alrabady, "Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking", IEEE Transactions on Mobile Computing, Vol. 9(8), pp. 1089-1107, 2010.

[3] Computer Science and Telecommunications Board. IT Roadmap to a geospatial Future. The National Academics Press, 2003.

[4] IEEE, IEEE 1609.2-Standard for wireless access in vehicular environments (WAVE)- security services for applications and mangement messages, available from ITS standards program.

[5] M. Garlach and F. Guttler, "Privacy in VANETs using changing pseudonyms - Ideal and real," in Proc. of IEEE VTC-Spring, Dublin, Ireland, Apr. 2007.

[6] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE Trans. Knowledge and Data Eng., Vol. 19(12), pp. 1719-1733, Dec. 2007.

[7] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The new casper: query processing for location services without compromising privacy," Proc. Int'l Conf. Very Large Data Bases (VLDB), pp. 763-774, 2006.

[8] A. Gkoulalas-Divanis, P. Kalnis, and V. S. Verykios, "Providing *k*-anonymity in location based services," SIGKDD Explorations Newsletter, Vol. 12(1), pp. 3-10, Jun. 2010.

[9] M. Gruteser and D. Grunwald, "Anonymous usage of location- based services through spatial and temporal cloaking," Proc. ACM MobiSys, pp. 31-42, 2003.

[10] H. Xu and J.L. Xu, "2PASS: bandwidth-optimized location cloaking for anonymous location-based services," IEEE. Trans. Parallel and Distributed Systems, Vol. 21(10), pp. 1458-1472, Oct. 2010.

[11] B. Gedik, L.Liu, "Protecting location privacy with personalized *k*-Anonymity: architecture and algorithms," IEEE Trans. Mob. Comput. Vol. 7(1), pp. 1-18, 2008.

[12] C. Ardagna, M. Cremonini, et al., "An obfuscation-based approach for protecting location privacy," IEEE Tran. Dependable and Secure Computing, Vol. 8(1), pp. 13-27, 2011.

[13] F. Liu, K. A. Hua, and Y. Cai, "Query l-diversity in location-based services, " in Proceedings of the 10th International Conference on Mobile Data Management: Systems, Services and Middleware, pp. 436-442, 2009.

[14] A.Machanavajjhala, J.Gehrke,D.Kifer,and M.Venkitasubramaniam, "*L*-diversity: privacy beyond k-anonymity," in ICDE,2006,p.24.

[15] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacy grid," in WWW '08 Proceedings of the 17th international conference on World Wide Web , pp. 237–246, 2008.

[16] J-H Um, M-Y Jang, et al., "A new cloaking method supporting both k-anonymity and l-diversity for privacy protection in location-based service," ISPA, pp. 79-85, 2009.

[17] R. Dewri, I. Ray, et al., "Query m-invariance: preventing query disclosures in continuous location-based services," 2010 Eleventh International Conference on Mobile Data Management, Kanas City, Missouri, USA, pp. 95-104, 2010.

[18] T. Wang, L. Liu, "Privacy-aware mobile services over road networks, " PVLDB, Vol. 2(1), pp. 1042-1053, 2009.

[19] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving User Location Privacy in Mobile Data Management Infrastructures," Proc. Privacy Enhancing Technology Workshop (PET '06), 2006.

[20] T. Xu and Y. Cai, "Exploring historical location data for anonymity preserving in location-based services," Proc. IEEE INFOCOM, 2008.

[21] J. Xu, X. Tang, H. Hu, and J. Du, "Privacy-conscious location-based queries in mobile environments," IEEE Trans. Parallel and Distributed Systems, Vol. 21(3), pp. 313-326, Mar. 2010.

[22] X. Pan, J.L. Xu, X.F. Meng, "Protecting location privacy against location-dependent attacks in mobile services," IEEE Trans. Knowledge and Data Engineering, Vol. 24(8), pp. 1507-1519, Aug. 2012.

[23] Thomas Brinkhoff Network-Based Generator of Moving Ojbects, http://iapg.jade-hs.de/personen/brinkhoff/generator/