Privacy-Area Aware Dummy Generation Algorithms for Location-Based Services

Ben Niu*, Zhengyan Zhang†, Xiaoqing Li* and Hui Li*
*National Key Laboratory of Integrated Networks Services, Xidian University, China
Email: xd.niuben@gmail.com, {xqli, lihui}@mail.xidian.edu.cn
†School of Logistics Engineering, Wuhan University of Technology, Wuhan, China
Email: zhengyanzhang09@gmail.com

***Abstract*—Location-Based Services (LBSs) have been one of the most popular activities in our daily life. Users can send queries to the LBS server easily to learn their surroundings. However, these location-related queries may result in serious privacy concerns since the un-trusted LBS server has all the information about users and may track them in various ways. In this paper, we propose two dummy-based solutions to achieve k-anonymity for privacy-area aware users in LBSs with considering that side information may be exploited by adversaries. We first choose some candidates based on a virtual circle or grid method, then blur these candidates into the final positions of dummy locations based on the entropy-based privacy metric. Security analysis and evaluation results indicate that the V-circle solution can significantly improve the privacy anonymity level. The V-grid solution can further enlarge the cloaking region while keeping similar privacy level.**

I. Introduction

The widespread utilization of mobile devices and the social network have fostered the development of Location-Based Services (LBSs). Mobile users can easily download location-based applications from Apple Store or Google Play Store with their smartphones or tablets. With the help of these applications, users can send queries to the LBS server and enjoy the corresponding service data. Typical examples include the navigation, finding the nearby services or receiving location-based advertisements or traffic alerts.

Normally, the LBS server provides users with location-based service data by exploiting the knowledge about their geographic locations. This situation conflicts with the increasing privacy concerns of mobile users since the un-trusted LBS server knows all the information of users, such as their current and history locations. He may track users directly or just release these sensitive data to other parties. We thus need to pay more attention to user's privacy.

Besides the policy-based [1] and cryptography primitive-based approaches [2], existing works on this topic mainly focus on location perturbation and obfuscation [3]. It always protects user's privacy through pseudomyzation [4], perturbation [5], [6] and adding dummies [7], [8]. Gruteser *et al.* [9] first introduced *k-anonymity* into location privacy, which is a trusted anonymization server-based scheme and protects user's location privacy by hiding the real location from the LBS server. They design an adaptive interval cloaking algorithm which generates spatio-temporal cloaking boxes containing at least k_{min} users and use the boxes as the location sent to the LBS server. However, this kind of approaches always rely on a *location anonymizer* [10], [11] to enlarge the cloaking region, and hence the anonymization server becomes the central point of failure and the performance bottleneck. Additionally, the service quality is degraded by the enlarged cloaking region. Encountered-based solutions [12], [6] can avoid the *location anonymizer* by exchanging information in a Peer-to-Peer (P2P) mode. However, the drawbacks are obvious. Firstly, since these solutions always prefer to use the users' information nearby to participate in cloaking, this may cause serious privacy problem that all the submitted locations within the cloaking region may be very close to each other, for example, they may located at a same building, then the adversary can directly confirm that the real user is in this particular building. Secondly, there is no enough motivation for resource-restricted mobile users to exchange own information with others. To address these aforementioned problems, Kido *et al.* [13] propose the dummy locations-based solution to achieve anonymity without employing the *location anonymizer*. Lu *et al.* [7] propose two dummy location generating schemes called *CirDummy* and *GridDummy*, which achieve *k-anonymity* for mobile users considering the *privacy-area*. However, they generate dummy locations based on either a random walk model or virtual circle/grid, which cannot guarantee the desired privacy level when the adversary (e.g., the LBS server) has some *side information* [14], [15], [16], such as the user's query probability. For example, some randomly generated dummy locations may fall at some unlikely locations such as lakes, oceans, swamps, and rugged mountains, and can be easily filtered out by the adversary. The desired *k-anonymity* thus is failed to achieve.

In this paper, we propose two dummy location generation schemes: Virtual Circle-based (*V-circle*) and Virtual Grid-based schemes (*V-grid*), which are developed from the methods mentioned in [7] to achieve desired *k-anonymity* against the adversaries with *side information*. We first use the information of user's query probability on the local map to construct an entropy-based privacy metric to measure the privacy level. To achieve the desired *k-anonymity*, our *V-circle* scheme first generates several temporary locations, which makes up a virtual circle to guarantee bigger privacy area. Then we blue them into the proper positions for the final dummy locations based on our privacy metric. To further enlarge the privacy

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

area, our *V-grid* scheme first generates temporary locations based on a virtual grid in terms of k, then blurs them into the proper positions to achieve desired *k-anonymity*.

The rest of this paper is organized as follows. In Section II, we introduce some preliminaries of our work. Following in Section III, we describe the details of our proposed schemes. Then, the security analysis and evaluation results are provided in Section IV and V, respectively. Finally, we draw the conclusions in Section VI.

II. Preliminaries

A. Basic Concepts

Side information in this paper is limited to user's query probability in the local map. It indicates the probability to send a LBS-related query at a particular location.

Privacy-aware cloaking region (*PCR*) means the minimum cloaking region that covers all the possible location, and each location is hard to be distinguished from the others for the adversary with *side information*.

B. Entropy-based Privacy Metric

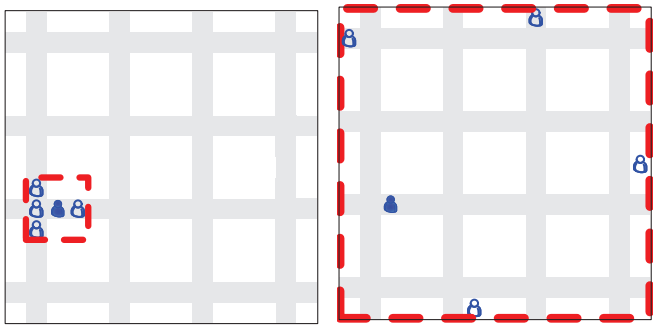
Entropy is well used to measure the degree of anonymity in LBSs. It indicates the uncertainty to determine the real location of an individual [17] from all the candidates. In our work, we consider the query probability of each possible location as the *side information* to construct the entropy-based privacy metric. We thus assign each possible location a probability of being queried in the past, denoted by p_i, and the sum of all probabilities p_i is 1. As the result, the entropy H of identifying an individual in the candidate set can be denoted as $H = -\sum_{i=1}^{k} p_i \cdot \log_2 p_i$. In *k-anonymity*, the maximum entropy $H_{max} = \log_2 k$ is achieved when all the k possible locations have the same probability $1/k$.

C. Adversary Model

We consider two types of adversaries in this work: *passive adversary* and *active adversary*. Any entity can be a passive adversary if he can monitor and eavesdrop on the wireless channels between entities or compromise users to obtain other users' sensitive information. A *passive adversary* can perform *eavesdropping attack* to learn extra information about a particular user. An *active adversary* can compromise the LBS server and obtain all the information the server knows. In this work, we directly consider the LBS server as the *active adversary*. Then, he is able to obtain all the information and monitor the current queries sending from the users. He can also obtain the historic data of a particular user as well as the current situation. Additionally, he knows exactly about the location privacy protection mechanism used in the system.

D. Motivation and Our Basic Ideas

To achieve *k-anonymity* [18], many existing approaches allow users to collect the nearby users' information through either P2P mode [10] or central server-based method. Intuitively, they are not good from the *PCR* point of view. We use a simple example shown in Fig. 1 to illustrate our concerns. Similar



(a) Smaller Privacy Area (b) Bigger Privacy Area

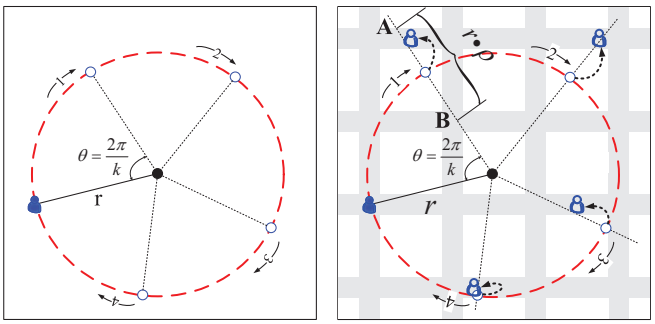
Fig. 1. Motivation

with experimental scenario in scheme [12], the cells in gray mean roads or some places where users can send queries. The solid user means the real user, and the hollows represent the collected users within the privacy area. The dashed rectangle indicates the cloaking region. For P2P-based solutions, since the natural feature of the communication restriction, it is hard to obtain the information of users far away, which means that, the collected users' locations may be very close to the real user. For example, in Fig. 1(a), the adversary may not need to guess the real location exactly, he can directly locate the real user into a very small area such as a bar or a clinic, which is also a kind of privacy leakage. Obviously, we prefer the case shown in Fig. 1(b) since it can provide bigger privacy area for the real user. Although the central server-based method can provide a bigger privacy area as that shown in Fig. 1(b), the server itself becomes the bottleneck of the whole system from both the privacy and system performance points of view. Dummy locations can solve the aforementioned problems with respect to either the privacy area issue or central server concerns, but leads to other problem. For example, in Fig. 1(b), the provided privacy area looks bigger, but we can see that two of the dummy locations are located in the unlikely place. As the result, the adversary can filter out these two locations easily and the privacy area then becomes smaller than desired.

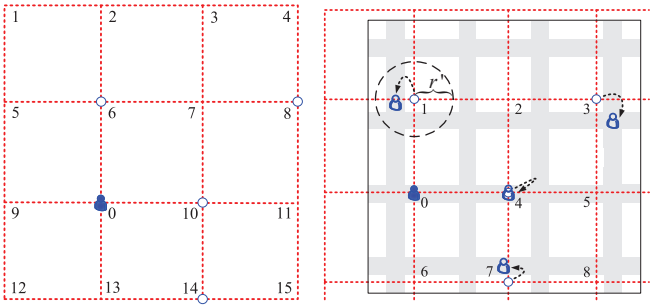
We solve this problem based on two phases: constructing phase and location blurring phase. The basic ideas are shown in Fig. 2, we first construct a virtual circle (in Fig. 2(a)) or a virtual grid (in Fig. 2(c)), which can guarantee a desired privacy-area requirement for mobile user. Next, we blur the chosen candidates into final positions to construct the cloaking region, which then be submitted to the un-trusted LBS server. The location blurring phase (shown in Fig. 2(b) or Fig. 2(d)) is needed since the query probability may be compromised by the adversary. It guarantees the effectiveness of our privacy-area aware dummy generation algorithms against the adversaries with *side information*.

III. Our Proposed Schemes

In this section, we present our V-circle-based dummy generation algorithm and V-grid-based dummy generation algorithm in turn. Followed with some implement issues.



(a) Constructing the Virtual Circle (b) Blurring into Final Positions



(c) Constructing the Virtual Grid (d) Grid Shifting and Location Blurring

Fig. 2. Our Basic Ideas

A. V-circle-Based Dummy Generation Algorithm

We use an example shown in Fig. 2(a) and 2(b)to illustrate our V-circle-based dummy generation algorithm. Firstly, we need to construct the virtual circle. The user-defined *PCR* A_{min} provides us a way to determine the radius r_{min} of the virtual circle, it should satisfy

$$\pi \cdot r_{min}^2 \geq A_{min}, \tag{1}$$

and for simplicity, we choose

$$r_{min} = \sqrt{\frac{A_{min}}{\pi}}. \tag{2}$$

The center c of our virtual circle is chosen randomly from the local map, it satisfies

$$r_{min} < r = d(l_r, c) \leq a/2, \tag{3}$$

where a is the length of the local map and $d(l_r, c)$ denotes the Euclidean distance between the real location l_r and c. Based on these information, we determine the first candidate's location l_1, which guarantees an angle satisfying $\theta = \angle l_c c l_1 = \frac{2\pi}{k}$. Through this way, the other candidates can be located around the center c with clock-wise rotation one by one. We denote the chosen k-1 locations as $\langle l'_1, \cdots, l'_{k-1} \rangle$.

Next, we perform the location blurring phase to blur the aforementioned k-1 locations $\langle l'_1, \cdots, l'_{k-1} \rangle$ into the final positions $\langle l_1, \cdots, l_{k-1} \rangle$, which can address the privacy concerns brought by the *side information*. Let's look at an example in Fig. 2(b), three of the generated candidates are located in the unlikely places, which may be easily filtered out by the adversary with *side information* and significantly decrease the size of the privacy area for mobile users. We thus blur them into the carefully selected locations to achieve *k-anonymity* effectively. Specifically, to guarantee the virtual circle, we use k radials to separate the circle with center c and radius $r = d(l_r, c)$ into k parts. Then, for each radial, it goes through several cells with different query probabilities, our aim is to blur each candidate chosen in the first step into a new position, which has similar query probabilities as the candidate's. Simultaneously, we define a parameter ρ, where $0 < \rho \leq 1$. It is used to define the range of distances between the possible positions to the candidate on the radial, the final position of this dummy location in our example then can be blurred within the range $AB = r \cdot \rho$. Based on these information, we prefer to choose a cell with the smallest difference on the query probability to assign the dummy location. Then we obtain the blurred locations $\langle l_1, \cdots, l_{k-1} \rangle$ to construct the cloaking region $\mathcal{C}$. The formal description of our V-circle-based scheme can be found in Algorithm 1.

Algorithm 1: V-circle-Based Dummy Generation Algorithm

Input : l_r, A_{min}, k
Output: $\mathcal{C}$
$\theta = \frac{2\pi}{k}$;
$r_{min} = \sqrt{\frac{A_{min}}{\pi}}$;
chooses c randomly which satisfies $r_{min} < r = d(l_r, c) \leq a/2$;
determines the k-1 locations $\langle l'_1, \cdots, l'_{k-1} \rangle$ based on the clock-wise rotation;
constructs the virtual circle;
for $(i = 1; i < k; i++)$ **do**
  while *(c_{ij} is on the radial i) $\cap$ (c_{ij} is within $r \cdot \rho$)* **do**
    chooses c_{ij} based on the smallest difference on query probability with the real location;
  end
  blurs the location l'_i into c_{ij};
end
constructs the cloaking region $\mathcal{C}$;
outputs $\mathcal{C}$.

B. V-grid-Based Dummy Generation Algorithm

The *V-circle* algorithm may not perform well all the time in terms of the privacy area, due to the real user's location may be close to the center of the local map. We thus propose the V-grid-based dummy generation algorithm (*V-grid*) (see 2(c) and 2(d)), it can provide a bigger privacy area no matter where the real location is located.

We first construct a virtual grid based on the user defined minimum privacy area A_{min}, which satisfies

$$a_{min}^2 \geq A_{min}. \tag{4}$$

Similar with *V-circle* algorithm, we compute

$$a = \sqrt{A_{min}}, \tag{5}$$

where a is the side length of the cloaking region. Then we divide the area with side length a into N cells, where

$$N = \lceil \sqrt{k} \rceil^2. \quad (6)$$

Based on these information, we can construct a virtual grid with N cells easily as shown in an example in Fig. 2(c). In this particular case, k is set to 5, we get $(\lceil \sqrt{k} \rceil + 1)^2 = 16$ positions totally, and we can see that, about $n = \lceil \sqrt{k} \rceil^2 = 9$ positions are located within the local map, we randomly select $k = 5$ locations from the n positions.

Algorithm 2: V-grid-Based Dummy Generation Algorithm

Input : l_r, A_{min}, k
Output: $\langle l_1, \cdots, l_{k-1} \rangle$
computes $a = \sqrt{A_{min}}$;
computes $N = \lceil \sqrt{k} \rceil^2$;
constructs the virtual grid;
selects k-1 locations $\langle l'_1, \cdots, l'_{k-1} \rangle$ randomly from n locations;
for $(i = 1; i < k; i++)$ **do**
  while *(c_{ij} is within the range r')* **do**
    chooses c_{ij} based on the smallest difference on query probability with the real location;
  end
  blurs the location l'_i into c_{ij};
end
outputs $\langle l_1, \cdots, l_{k-1} \rangle$.

The location blurring phase is similar to the *V-circle*'s, its aim is to blur the roughly selected k-1 locations $\langle l'_1, \cdots, l'_{k-1} \rangle$ into the final positions $\langle l_1, \cdots, l_{k-1} \rangle$ to resist from adversary with *side information*. The only difference is that we need to limit the blurring radius $r' < a/2$ to avoid the shorter distance between two blurred locations. Algorithm 2 gives the formal description.

C. Implementation Issues

In both of our proposed *V-circle* and the *V-grid* algorithms, to effectively achieve *k-anonymity*, *side information* such as the user's query probability in the local map should be obtained before generating the dummy locations. One simple solution is to let a well-known place such as an service provider (e.g., Google Latitude or Yelp!) to disseminate the users' query probabilities, users can obtain this information easily. Since the users' query probabilities do not change too much, the dissemination interval will be long, therefore, the dissemination overhead should not be high. In our work, we simply use the user density to represent the query probability since we believe a fact that the bigger user density always brings higher user query probability.

IV. Security Analysis

In our security analysis, since the cryptography techniques such as the public key infrastructure (PKI) can be easily applied to our schemes, we ignore the attacks such as *eavesdropping attacks* on the wireless channel between users and other entities. Instead, we pay much attention on the attacks such as *colluding attacks* and *inference attacks* from the *passive adversary* and *active adversary*, respectively.

A. Resistance to Colluding Attacks

Passive adversaries may collude with some users to learn extra information of other users, or collude with LBS server to predict private information of legitimate users.

Definition 1: A scheme is colluding attack resistant if the successful guessing probability of obtaining the others' privacy cannot be increased with the size of colluding group.
This definition can be formalized as

$$p_G^{U_i+U_j}(e) = p_G^U(e) = \frac{1}{k}, \quad (7)$$

where e is an event from a particular user U outside the colluding group and $p_G^U()$ is the successful guessing possibility with knowledge of user U on the adversary side. U_i and U_j are users in the colluding group.

Theorem 1: Our schemes are inference attack resistant if $p_G^{U_i+U_j}(l \in U) = \frac{1}{k}$, where l is an observed location of a particular user U.

Proof: The colluding always happens between a set of users. In our schemes, each user knows nothing about other users, and protects her location privacy by hiding her real location into a cloaking region covering other k-1 dummy locations. At the beginning, the adversary knows nothing about the users' information, the successful guessing possibility is $\frac{1}{k}$. When the first user U_i is compromised, the obtained information includes U_i's real locations in history and the generated dummy locations. Suppose the adversary then intercepts a query sending from user U to the LBS server, the successful guessing possibility is still $\frac{1}{k}$ based on two reasons: 1) there is no relationship between user U_i and user U on the dummy locations selection phase; 2) the location blurring phases in both of our proposed *V-circle* and the *V-grid* algorithms guarantee the privacy level for user U_i since all the chosen dummy locations have similar query probabilities to be targeted as the real location. Next, the adversary compromises another user U_j. Similar to user U_i, he obtains the user U_j's query history, including the real locations and the generated dummy locations. The adversary has no useful information to exactly locate the real user even he knows the *V-circle* and the *V-grid* algorithms. Therefore, the adversary can only guess the real location randomly from the k locations within the cloaking region with the knowledge from all the member of the colluding group, which means the successful guessing probability is no bigger than $1/k$, and we complete our proof. ■

The best case to *passive adversary* is that he can compromise LBS server as well as all the users, then he becomes an *active adversary* to perform *inference attack*.

B. Resistance to Inference Attack

We consider the LBS server as the *active adversary* directly since he knows the users' query probabilities of the whole map, and the history queries and the current queries (usually denoted as a cloaking region covering k locations $l_1, l_2, \cdots, l_r, \cdots, l_k$) which include the exact locations l_r and some dummy locations. With such information, the adversary's goal is to gain other sensitive information about the user by performing *inference attack*.

Definition 2: A scheme is inference attack resistant if $p_G(e_i) = p_G(e_j),\ \forall(i \neq j)$, where e_i, e_j are two different events from all the possibilities and $p_G(e)$ is the possibility that the adversary can successful guess if e is true.

Theorem 2: Our schemes are inference attack resistant.

Proof: On the *active adversary* side, he knows the history data of a particular user as well as the proposed algorithms. However, it is still helpless for him to increase the successful guessing probability with two reasons. Firstly, for all the generated dummy locations within the cloaking regions of our proposed *V-circle* and the *V-grid* algorithms, our proposed location blurring phases guarantee the smallest differences on their query probabilities with the real location. As the result, all the potential dummy locations have the same probability, which means that $p_G(l_i) = p_G(l_j),\ \forall(i \neq j)$, where l_i, l_j are two different locations from all the submitted locations with in the cloaking region. Then the uncertainty provided in Section II-B guarantees that our schemes can achieve the maximum entropy with a higher probability. With the similar uncertainties provided, our *V-grid* further enlarges the *PCR*, which protects user's location privacy within a larger privacy area. Secondly, the radius of the location blurring phase can be changed in either the *V-circle* (r in Fig. 2(b) and the *V-grid* (r' in Fig. 2(d)) algorithms. The bigger r or r', the higher chances to obtain the blurred locations which guarantee the similar query probabilities with the real location. ■

V. Performance Evaluations

A. Simulation Setup

To simulate the effectiveness of our proposed scheme, we implement them on a Windows 8 laptop. We use the central part ($5km \times 5km$) of the Borlange Data Set[1] (see [19] for more details) to generate the events between users in the local map since it covers more users than the edge areas of the map. To simplify our work, we believe the fact that more users always lead to higher query probability. This chosen map is divided into a grid of 50×50 cells. We can compute the users density on each cell as the query probabilities.

There are several parameters used in our evaluation. k is related to *k-anonymity*, and is commonly set from 2 to 30. A_{min} represents the user-defined *PCR*. We compare our proposed *V-circle* and *V-grid* algorithms with other four schemes. The random scheme represents the dummy selection algorithm in [13], which randomly chooses dummy locations to protect privacy. The *CirDummy* and *GridDummy* schemes are the dummy selection schemes designed in [7], which achieve *k-anonymity* for mobile users. The optimal scheme shows the optimal results of *k-anonymity* in theory.

[1]The data set is available at http://icapeople.epfl.ch/freudiger/borlange.zip in Jan. 2012.

B. Evaluation Results

1) Entropy vs. k: We first evaluate the relationship between k and the privacy level in terms of entropy. Fig. 3 shows the experimental results in details. Generally, the entropy of all the schemes increase with the varying k. It is obviously that the random based scheme performs worse than others, the reason is the ignorance on the *side information*. The performance of the *CirDummy* and *GridDummy* schemes are quite similar with the random scheme since they ignore the *side information* on the attacker's hand either. Our two proposed schemes outperform than the existing schemes, they indicate the ideal results ($H = log_2 k$) of k-anonymity on each tested k, by blurring the chosen locations into final positions which have similar query probabilities with the real user's. For example, when $k = 20$, the entropy of our *V-circle* and *V-grid* algorithms are 3.92 and 4.02, respectively. They are very close to the ideal privacy level provided by *k-anonymity*. While in the *CirDummy* and *GridDummy* schemes, the entropy are 2.68 and 2.09, respectively. It means that, about $2^{4.32} - 2^{2.68} \approx 14$ and $2^{4.32} - 2^{2.09} \approx 16$ submitted locations may be filtered out from the cloaking regions of the *CirDummy* and *GridDummy* schemes, respectively. Finally, the cloaking region may thus becomes smaller.

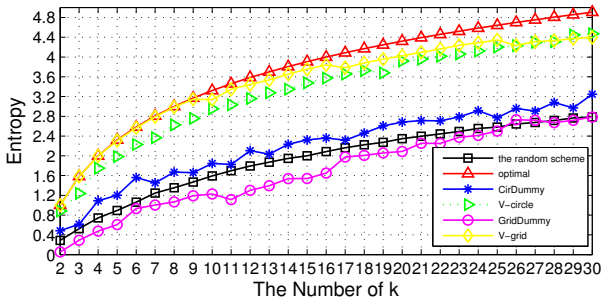


Fig. 3. Entropy vs. k

2) Privacy area vs. k: Since user's privacy is closely related with the cloaking region, we next evaluate the privacy area provided by different schemes with increasing k. Fig. 4 shows the evaluation results in details. In this figure, the random scheme performs worse than most of the other schemes, since it just generates dummy locations randomly and without considering any issues related to privacy area. In the *CirDummy* and *GridDummy* schemes proposed in [7], they can cover bigger area of local map with higher probability. Comparing these two schemes, the latter is better, the reason is that it always generates dummy locations in a virtual grid covering the map as much as possible. While in our proposed *V-circle* and *V-grid* algorithms, they outperform than the *CirDummy* and *GridDummy* schemes by the reason of the considerations on the *side information*. In our experiments, the privacy area is measured by computing region covered by the locations of

the submitted ones except that with low query probabilities (e.g., the location is located at the unlikely regions). For instance, when $k = 20$, the privacy area are 25 km^2 and 6.62 km^2 of the optimal and random schemes. The values of the *CirDummy* and *GridDummy* schemes are 6.65 km^2 and 14.96 km^2, respectively. While in our schemes, the privacy areas can achieve 9.90 km^2 and 16.31 km^2, respectively.

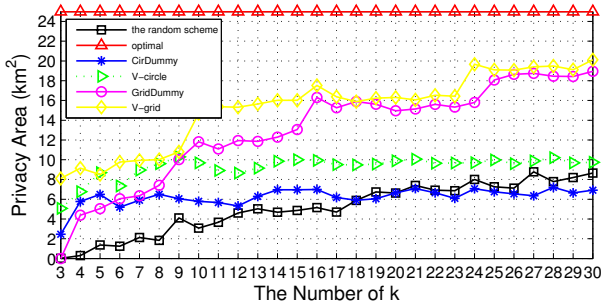


Fig. 4. Privacy area vs. k

3) The effect of the A_{min}: Based on different location privacy requirements, mobile users may define different levels of cloaking region to save the communication and computation cost while improving the service quality. We evaluate the effect of the minimum cloaking requirement A_{min} on the privacy level in terms of entropy. In Fig. 5, we can clearly see the different privacy levels provided by schemes under a fixed minimum privacy region. Not surprisingly, with the help of the location blurring phases, each chosen location is hard to distinguish from other k-1 locations, our schemes thus outperform than any other existing schemes. We illustrate this effect by a case $A_{min} = 4\ km^2$ and $k = 20$, which indicates that the mobile user prefers to protect her location privacy under *20-anonymity* and wishes to hide her real location into a cloaking region with 4 km^2. The entropy of the optimal scheme is $\log_2 20$. The performance of the random scheme is the worst, which is only 0.17. The entropy of the *CirDummy* and *GridDummy* schemes are a little bigger than the random scheme, they are 2.38 and 2.35, respectively. Finally, by utilizing our proposed *V-circle* and *V-grid* algorithms, the entropy can achieve 3.59 and 3.52, which are quite similar with the ideal value.

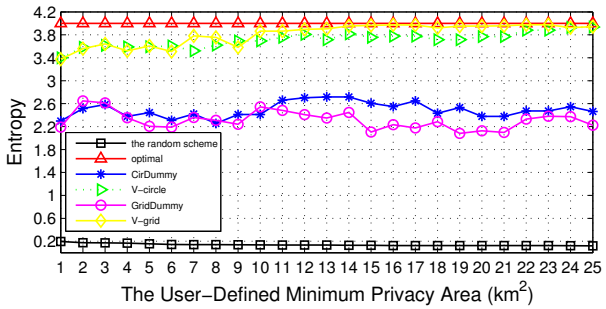


Fig. 5. The effect of the A_{min}

VI. Conclusion

To achieve *k-anonymity* effectively for privacy-area aware mobile users in LBSs, we proposed two cloaking algorithms based on the carefully selecting dummy locations with considering the *side information* may be compromised by the adversaries. In the *V-circle* algorithm, we first construct a virtual circle to guarantee a bigger privacy area, then blur the chosen locations into the final position based on the similar query probabilities, which can achieve higher privacy level in terms of entropy on all the submitted locations within the cloaking region. To further enlarge the privacy area, we also design a virtual grid based scheme, *V-grid*. The followed security analysis and performance evaluation show the effectiveness of our proposed algorithms.

Acknowledgment

This work was supported by National Natural Science Foundation of China under Grant 61272457, National Project 2012ZX03002003-002, 863 Project 2012AA013102, 111 Project B08038, IRT1078, FRF K50511010001 and National Natural Science Foundation of China under Grant 61170251.

References

[1] W3C. (2011, Apr.) Platform for privacy preferences (p3p) project. [Online]. Available: http://www.w3.org/P3P/
[2] I. Bilogrevic, M. Jadliwala, K. Kalkan, J.-P. Hubaux, and I. Aad, "Privacy in mobile computing for location-sharing-based services," in *ACM PETS 2011*.
[3] K. G. Shin, X. Ju, Z. Chen, and X. Hu, "Privacy protection for users of location-based services," *IEEE Wireless Communications*, vol. 19, no. 1, pp. 30–39, Feb. 2012.
[4] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46 – 55, jan-mar 2003.
[5] S. T. Peddinti, A. Dsouza, and N. Saxena, "Cover locations: availing location-based services without revealing the location," in *ACM WPES 2011*.
[6] B. Niu, X. Zhu, X. Lei, W. Zhang, and H. Li, "Eps: Encounter-based privacy-preserving scheme for location-based services," in *IEEE GLOBECOM 2013*.
[7] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: privacy-area aware, dummy-based location privacy in mobile services," in *ACM MobiDE 2008*.
[8] X. Zhu, H. Chi, B. Niu, W. Zhang, Z. Li, and H. Li, "Mobicache: When k-anonymity meets cache," in *IEEE GLOBECOM 2013*.
[9] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *ACM MobiSys 2003*.
[10] C.-Y. Chow, M. F. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *ACM GIS 2006*.
[11] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing for location services without compromising privacy," *ACM Trans. Database Syst.*, vol. 34, no. 4, 2009.
[12] B. Niu, X. Zhu, H. Chi, and H. Li, "3plus: Privacy-preserving pseudo-location updating system in location-based services," in *IEEE WCNC 2013*.
[13] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *IEEE ICPS 2005*.
[14] C. Y. Ma, D. K. Yau, N. K. Yip, and N. S. Rao, "Privacy vulnerability of published anonymous mobility traces," in *ACM MobiCom 2010*.
[15] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in *IEEE INFOCOM 2013*.
[16] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *IEEE INFOCOM 2014*.
[17] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *ACM PETS 2003*.
[18] L. Sweeney, "k-anonymity: a model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 557–570, Oct. 2002.
[19] E. Frejinger, "Route choice analysis: data, models, algorithms and applications," Ph.D. dissertation, Lausanne, 2008.