n-CD: A Geometric Approach to Preserving Location Privacy in Location-Based Services

Ming Li, Sergio Salinas, Arun Thapa, Pan Li
Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS 39762
Email: ml845@msstate.edu, sergio.salinas@ieee.org, at449@msstate.edu, li@ece.msstate.edu

Abstract*—With great advances in mobile devices, e.g., smart phones and tablets, location-based services (LBSs) have recently emerged as a very popular application in mobile networks. However, since LBS service providers require users to report their location information, how to preserve users' location privacy is one of the most challenging problems in LBSs. Most existing approaches either cannot fully protect users' location privacy, or cannot provide accurate LBSs. Many of them also need the help of a trusted third-party, which may not always be available. In this paper, we propose a geometric approach, called n-CD, to provide realtime accurate LBSs while preserving users' location privacy without involving any third-party. Specifically, we first divide a user's region of interest (ROI), which is a disk centered at the user's location, into n equal sectors. Then, we generate n concealing disks (CDs), one for each sector, one by one to collaboratively and fully cover each of the n sectors. We call the area covered by the n CDs the concealing space, which fully contains the user's ROI. After rotating the concealing space with respect to the user's location, we send the rotated centers of the n CDs along with their radii to the service provider, instead of the user's real location and his/her ROI. To investigate the performance of n-CD, we theoretically analyze its privacy level and concealing cost. Extensive simulations are finally conducted to evaluate the efficacy and efficiency of the proposed schemes.

I. Introduction

Location-based services (LBSs) provide mobile users with points of interest (POIs) close to their locations, such as restaurants, gas stations, shopping malls, and social events. With great advances in mobile devices, e.g., smart phones and tablets, LBSs have recently emerged as a very popular application in mobile networks. According to ABI Research [1], LBS revenue is forecasted to reach an annual global total of \$13.3 billion by 2013. However, since LBS service providers require users to report their location information, one major concern in LBSs is users' location privacy. For example, the LBS providers can be compromised by attackers to track some users, or they themselves may use users' location information for mobile advertising. Thus, how to provide LBSs while protecting users' location privacy is an important and challenging problem.

In the literature, there are generally two kinds of approaches addressing location privacy in LBSs: k-anonymity cloaking [2]–[10] and location obfuscation [11]–[15]. k-anonymity cloaking is firstly proposed by Gruteser and Grunwald [2]. Instead of sending one single user's LBS request to the server, including his/her exact location, k-anonymity cloaking employs a trusted third-party who collects k neighboring users' requests and sends them all together to the LBS service provider. However, an adversary can know that the user of interest must be located in one of the k locations. Besides, this scheme may lead to large service delay if there are not enough users requesting LBSs. Following [2], Gedik and Liu [3] design a joint spatial and temporal cloaking algorithm, which collects k LBS requests, each from a different user, in a specified cloaking area within a specified time period and then sends them to the service provider. In this scheme, however, users' requests will be blocked if there are only less than k requests within the predefined time period. Moreover, in the above two works, when user density is high, the k users' locations may be very close to each other, and hence these approaches will still reveal user's location privacy to some extent. Later on, Mokbel et al. [4] set a minimum size for the cloaking area, and require all mobile users to report their position frequently to an anonymizer (i.e., a third party) in order to provide LBSs with low delay. Unfortunately, frequent position update can incur overwhelming communication overhead for mobile users. Besides, [8], [9], [16] propose to let users exchange their pseudonyms when they meet in *mix zones*, which need the participation of other users. Note that [9] may not provide real-time services. In addition, Meyerowitz and Choudhury [10] predict users' paths and LBS queries, and send the results to users' before they submit queries. This approach may incur significant communication overhead in order to achieve good service accuracy, and also take up large storage spaces.

Different from k-anonymity cloaking, location obfuscation aims to protect users' location privacy either by inserting some fake LBS requests (i.e., fake users' locations) or by deviating a user's location from the real one in his/her LBS request. Specifically, Kido et al. [11] propose to send a user's location together with several generated false position data (dummies) to the LBS service provider. The server finds all the POIs regarding all these positions and send them back to the user. After that, Lu et al. [12] design circle-based and grid-based dummy generation methods, which take privacy area requirements into account. Duckham and Kulik [13] also propose an interactive negotiation protocol based on dummy generation. However, since in all these schemes adversaries know the user must be located at one of the submitted positions, the user's location privacy is still not well

This work was partially supported by the U.S. National Science Foundation under grants CNS-1149786 (CAREER), ECCS-1128768, and CNS-1147851.

protected and may be compromised [17]. Besides, Ardagna et al. [14], Pingley et al. [15] and Damiani et al. [18] develop location obfuscation schemes to hide users' real locations, e.g., by submitting shifted locations. Such schemes trade service accuracy for location privacy.

In other words, there is currently a lack of efficacious and efficient solutions to protecting location privacy in LBSs. Moreover, notice that most of the existing works deal with k nearest neighbor (kNN) query [19], [20], in which users retrieve the closest k POIs to their current locations. Nevertheless, distance may not always be the only criterion for a user to choose POIs. For example, when a user wants to find a restaurant, he/she may intend to go to the one with the highest rating within a certain range. When a user wants to find a gas station, he/she may wish to find the one with the lowest price within some area. Thus, we contend that finding all the POIs within a region specified by a user is more reasonable and practical. After receiving all the results, a user can rank them based on some criteria, e.g., rating, price, distance, and finally determine which one to go to. We call such kind of query "*ROI (region of interest) query*", which includes kNN query as a special case and is commonly used in many systems.

In this paper, we first propose a location privacy preserving algorithm, called n-CD, for realtime ROI query in LBSs which can guarantee service accuracy. In particular, we first divide a user's ROI, which is a disk centered at the user's location, into n equal sectors. Then, we generate n concealing disks (CDs), one for each sector, one by one to collaboratively and fully cover each of the n sectors. We call the area covered by the n CDs the "*concealing space*", which fully contains the user's ROI. After rotating the concealing space with respect to the user's location, we send the rotated centers of the n CDs along with their radii to the service provider, instead of the user's real location and his/her ROI. In so doing, the adversaries would not be able to know the exact location of each user, and can only know a user is within a certain region, which we call the "*anonymity zone*". Besides, we define the expected area of a user's minimum anonymity zone and that of a user's concealing space as his/her privacy level and concealing cost, respectively. We theoretically analyze the privacy level and concealing cost of the proposed n-CD algorithm, based on which users can choose their own control parameters such as n and the radius of the user's ROI. We also conduct extensive simulations to evaluate the performance of n-CD, which reveal a trade-off between privacy level and concealing cost. In addition, notice that many previous location privacy protection schemes [2]–[7], [13] rely on a trusted third-party to run those algorithms, which, however, may not always be available and can incur additional cost. The proposed n-CD does not need any trusted third-party.

Moreover, note that the proposed geometric approach does not rely on any security schemes. The main reason is that if we employ a security scheme, then probably either the location-based service providers or some central authorities managing security keys can know users' exact locations. Thus, users' location privacy may still be compromised. In contrast, in the proposed approach, no one else can know any user's exact locations even though they obtain all the information users send to location-based service providers.

II. System Model

A. System Architecture

We consider a system consisting of many mobile users and a location-based service provider. In particular, a mobile user first generates an original ROI query q in the form of $q := \langle u_{id}, \{(x, y), R\}, \mathcal{P}\rangle$, where u_{id} and (x, y) are the user's identity and location coordinates, respectively, R is the radius of the user's ROI, and $\mathcal{P}$ stands for the kind of POIs the user is interested in, e.g., restaurants, gas stations. Note that $\{(x, y), R\}$ denotes the user's ROI. Since any attacker will be able to know exactly where a user is after obtaining his/her ROI query q, before transmitting this request to the service provider, the user passes it through a local concealing engine, which aims to prevent the ROI query from revealing his/her location privacy. Specifically, upon receiving the original ROI query q, the concealing engine employs the proposed n-CD algorithm to transform the original ROI to a concealing space $\mathbb{C}$ that fully covers ROI. The concealing space is formed by multiple, say n, concealing disks (CDs), centered at $(x'_1, y'_1), ..., (x'_n, y'_n)$ and with radius of $r_1, ..., r_n$, respectively. The concealing engine thus can transform the original query q to a new one q_t as follows:

$$q_t := \langle u_{id}, \underbrace{\{[(x'_1, y'_1), r_1], ..., [(x'_n, y'_n), r_n]\}}_{\mathbb{C}:\ \text{concealing space}}, \mathcal{P}\rangle.$$

On the service provider's side, upon receiving a query from a user of the form $< u_{id}, \mathbb{C}, \mathcal{P} >$, it will search for and return all the POIs inside $\mathbb{C}$, including their locations. After receiving the POIs, the user adopts a "Results Filter" to rank the POIs in his/her ROI based on a chosen criterion, such as price for gas stations, and distance or reviewers' ratings for restaurants, and finally find the POIs he/she is interested in.

B. Attack Model

We consider that the service provider can be compromised by attackers, or itself can be an attacker because of being interested in users' locations, e.g., in order to benefit from advertising. Thus, attackers are aware of the queries submitted by users, i.e., $q_t := \langle u_{id}, \mathbb{C}, \mathcal{P}\rangle$. We also assume that attackers know how the location concealing algorithm n-CD works but do not know the private control parameters of each user, which will be introduced later. Note that although the users might mostly communicate with LBS service providers through cellular networks, we aim to protect users' location privacy from LBS service providers instead of cellular service providers, the former of which could be unreliable or compromised by attackers.

C. Definitions

Definition 1: **Lossless Query Transformation**: The transformation from a ROI query q to another query q_t is called a lossless query transformation if and only if $q_t.\mathbb{C} \supseteq q.\{[x,y],R\}$ and $q_t.\mathcal{P} = q.\mathcal{P}$.

Besides, although attackers cannot know the exact location of a user due to the use of a local concealing engine, they may still be able to infer that the user must be located inside a certain area with the knowledge of q_t. We call such an area the user's *anonymity zone*, based on which we define a user's privacy level as follows.

Definition 2: **Privacy Level**: A user's privacy level employing n-CD is the expected area of his/her anonymity zone.

Definition 3: **Concealing Cost**: A user's concealing cost employing n-CD is the expected area of the whole concealing space $\mathbb{C}$.

Note that in n-CD, each user can set his/her own control parameters based on his/her requirements on privacy level and concealing cost, which can both be computed locally.

III. Preserving Location Privacy by Concealing Disks

In this section, we detail the proposed algorithm n-CD, which generates n ($n \geq 3$) concealing disks to cover a user's ROI and preserve his/her location privacy in location-based services. Without loss of generality, we illustrate n-CD in the case of $n = 4$ in what follows.

A. Description of Basic n-CD

We first divide the original ROI into four equal sectors, or four quadrants. Then, we generate four CDs one by one, each of which is centered at a randomly chosen location in the uncovered region of a quadrant with a carefully chosen radius, to collaboratively and fully cover each of the four quadrants and hence the whole ROI. Briefly speaking, the first CD, denoted by CD_1, is generated to cover a randomly chosen quadrant, which we call the first quadrant and denote by q_1. After that, the other three CDs, denoted by CD_2, CD_3, and CD_4, respectively, will be generated to cover the uncovered areas in the other three quadrants one by one in counterclockwise order, which are denoted by q_2, q_3, and q_4, respectively.

1) Generating CD_1: We denote the radius and the center of CD_i ($1 \leq i \leq 4$) by r_i and S_i, respectively. In order to fully cover q_1 with CD_1, the radius r_1 and the center S_1 of CD_1 are chosen as follows.

Lemma 1: As shown in Fig. 1, with the center S_1 being a randomly chosen point in q_1 and $r_1 = \max\left\{|l_1^1|, |l_1^2|, |l_1^3|\right\}$, CD_1 can fully cover q_1, where l_1^1, l_1^2, and l_1^3 denote line segments S_1O, S_1Q_2, and S_1Q_1, respectively.

Proof: As shown in Fig. 1, S_1 is a randomly chosen point in q_1. Thus, q_1 can be divided into three parts[1]: ΔOS_1Q_2, ΔOS_1Q_1, and the region enclosed by l_1^2, l_1^3, and arc $\widehat{Q_1Q_2}$. To simplify the notation, we use $\langle Q_1S_1Q_2\rangle$ to denote the third region mentioned above. If CD_1 can cover all these three parts, then it can cover the whole quadrant q_1.

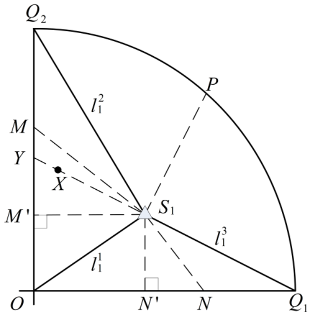


Fig. 1. Generating CD_1 to fully cover q_1.

In ΔOS_1Q_2, suppose that a point M' is on OQ_2 and S_1M' is perpendicular to OQ_2, i.e., $S_1M' \perp OQ_2$. For an arbitrary point M on OQ_2, if $M \in M'Q_2$, then $\angle S_1Q_2M < \pi/2 \leq \angle Q_2MS_1$ and hence $|S_1M| \leq \left|l_1^2\right|$, and if $M \in M'O$, then $\angle MOS_1 < \pi/2 \leq \angle S_1MO$ and hence $|S_1M| \leq \left|l_1^1\right|$. Therefore, given the radius $r_1 = \max\left\{|l_1^1|, |l_1^2|, |l_1^3|\right\}$, we have $|S_1M| \leq \max\{\left|l_1^2\right|, \left|l_1^1\right|\} \leq r_1$. Notice that for any point X in the triangular area ΔOS_1Q_2, i.e., $X \in \Delta OS_1Q_2$, we can always find a point Y on OQ_2 such that $X \in S_1Y$. Since $|S_1X| \leq |S_1Y| \leq r_1$, we can know that the whole triangular area ΔOS_1Q_2 can be covered by the concealing disk CD_1.

Similarly, we can also find that an arbitrary point N on OQ_1 satisfies $|S_1N| \leq \max\{\left|l_1^1\right|, \left|l_1^3\right|\} \leq r_1$. Consequently, the concealing disk CD_1 can cover ΔOS_1Q_1 as well.

As for $\langle Q_1S_1Q_2\rangle$, according to the above analysis, the region can be fully covered by the concealing disk CD_1 if an arbitrary point P on arc $\widehat{Q_1Q_2}$ satisfies $|S_1P| \leq \max\{|l_1^2|, |l_1^3|\}$. In what follows, we prove it by contradiction in two different scenarios, depending on the location of S_1.

- *Case I: $S_1 \in \Delta OQ_1Q_2$ (Fig. 2(a))*

Assume $|S_1P| > \max\{|l_1^2|, |l_1^3|\}$, i.e., $|S_1P| > \left|l_1^2\right|$ and $|S_1P| > \left|l_1^3\right|$. Then, we have $\angle\gamma_2 > \angle\gamma_1$ and $\angle\beta_2 > \angle\beta_1$ according to the Sine Theorem. Consequently, we get $\angle\gamma_2 + \angle\beta_2 > \angle\gamma_1 + \angle\beta_1$. Besides, since $\gamma_2^2 < \angle Q_1Q_2O$ and $\beta_2^2 < \angle Q_2Q_1O$, we have $\gamma_3 + \beta_3 > 180^\circ - (\angle Q_1Q_2O + \angle Q_2Q_1O) = 90^\circ$. Since the sum of all inner-angles of quadrilateral $\Diamond PQ_2S_1Q_1$ is 360°, we have $\sum_{j=1}^{3} \angle\gamma_j + \angle\beta_j = 360^\circ$, and hence

$$2\angle\gamma_1 + 2\angle\beta_1 < \angle\gamma_2 + \angle\gamma_1 + \angle\beta_2 + \angle\beta_1 < 270^\circ.$$

So we can obtain

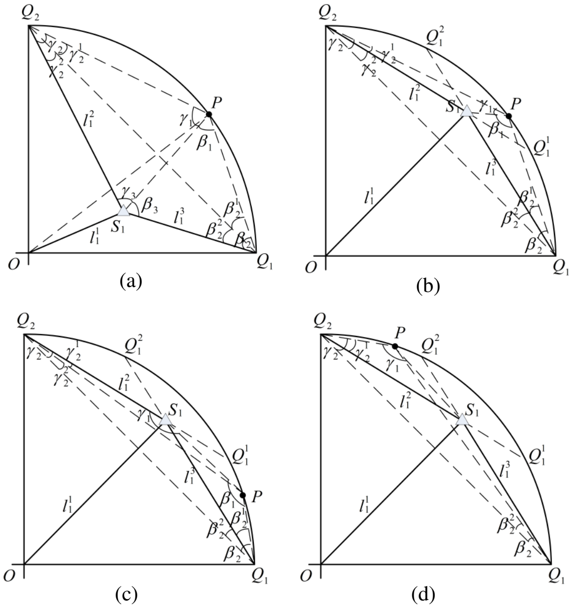
$$\angle\gamma_1 + \angle\beta_1 < 135^\circ. \tag{1}$$

On the other hand, notice that $\gamma_2^1 = \frac{1}{2}\angle POQ_1$ and $\beta_2^1 = \frac{1}{2}\angle POQ_2$, which result in $\angle\gamma_2^1 + \angle\beta_2^1 = \frac{1}{2}(\angle POQ_1 + \angle POQ_2) = 45^\circ$. Then, in ΔPQ_2Q_1, we get $\angle\gamma_1 + \angle\beta_1 = 180^\circ - (\angle\gamma_2^1 + \angle\beta_2^1) = 135^\circ$, which contradicts with (1). Therefore, the assumption that $|S_1P| > \max\{|l_1^2|, |l_1^3|\}$ does not hold, which in turn indicates that $|S_1P| \leq \max\{\left|l_1^2\right|, \left|l_1^3\right|\}$ in this case.

- *Case II: $S_1 \notin \Delta OQ_1Q_2$*

Similarly, we assume $|S_1P| > \left|l_1^2\right|$ and $|S_1P| > \left|l_1^3\right|$.

[1] We use Δabc to denote a triangular area enclosed by line segments ab, bc, and ca.



(a) (b)

(c) (d)

Fig. 2. Different locations of S_1 in q_1. (a) Case I. (b) Case II (when $P \in \widehat{Q_1^1Q_1^2}$). (c) Case II (when $P \in \widehat{Q_1Q_1^1}$). (d) Case II (when $P \in \widehat{Q_2Q_1^2}$.)

For an arbitrary point $P \in \widehat{Q_1^1Q_1^2}$ (as shown Fig. 2(b)), we can get $\angle\gamma_2^1 > \angle\gamma_1$, and $\angle\beta_2^1 > \angle\beta_1$. Consequently, $\angle\gamma_2 + \angle\beta_2 > \angle\gamma_2^1 + \angle\beta_2^1 > \angle\gamma_1 + \angle\beta_1$. Note that in ΔQ_1PQ_2, the sum of inner angles is equal to $180°$, i.e., $\angle\gamma_2 + \angle\beta_2 + \angle\gamma_1 + \angle\beta_1 = 180°$. Therefore, we have

$$\angle\gamma_1 + \angle\beta_1 < 90°. \qquad (2)$$

But, the same as proved in Case I, we can find that $\angle\gamma_1 + \angle\beta_1 = 135°$, which contradicts with (2). Thus, we also have that $|S_1P| \leq \max\{|l_1^2|, |l_1^3|\}$.

For an arbitrary point $P \in \widehat{Q_1Q_1^1}$ (as shown Fig. 2(c)), we can have that $\beta_2^1 < \beta_2 + \gamma_2^2 = 45°$. Since $|S_1P| > |l_1^3|$, we have $\beta_2^1 > \beta_1$ and hence $\beta_1 < 45°$. However, on the other hand, we have $\beta_1 > \angle Q_2PQ_1 = 180° - (\beta_2 + \gamma_2^2) = 135°$. Therefore, the assumption does not hold, i.e., $|S_1P| \leq \max\{|l_1^2|, |l_1^3|\}$.

For an arbitrary point $P \in \widehat{Q_1^2Q_2}$ (as shown Fig. 2(d)), we can also find that the assumption is not valid and hence $|S_1P| \leq \max\{|l_1^2|, |l_1^3|\}$. The details are omitted due to the similarity to the analysis when $P \in \widehat{Q_1Q_1^1}$.

Therefore, Lemma 1 simply follows. ■

Notice that although the first quadrant q_1 can be fully covered by CD_1 following Lemma 1, the user's location privacy may be compromised in some scenarios. For example, when $r_1 = \max\{|l_1^1|, |l_1^2|, |l_1^3|\} = |l_1^1|$, $r_2 = \max\{|l_2^1|, |l_2^2|, |l_2^3|\} = |l_2^1|$, the user will be located at one of the two intersections of the perimeter of CD_1 and that of CD_2. Besides, when $r_1 = |l_1^1|$, $r_2 = |l_2^1|$ and $r_3 = |l_3^1|$, the intersection point of the perimeters of the three concealing disks is where the user is located. In order to address this problem, we set r_1 to $\max\{|l_1^1|, |l_1^2|, |l_1^3|\} \cdot (1 + \Delta)$ where $\Delta \in (0, 1)$. Thus, none of the intersection points would be the user's real location.

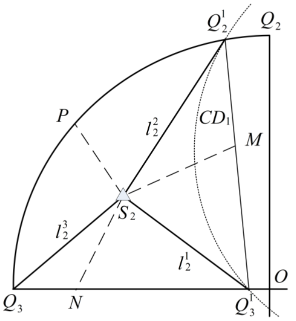


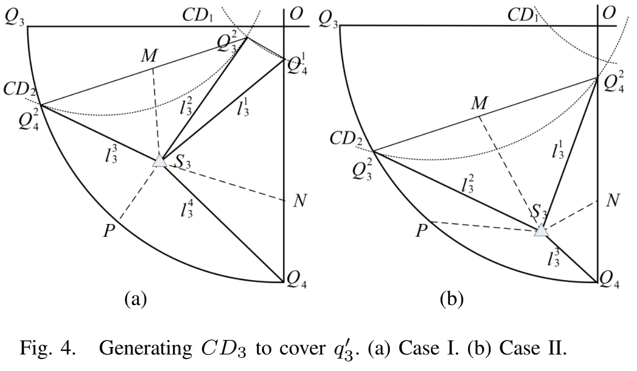
Fig. 3. Generating CD_2 to cover q_2'.

2) Generating CD_2: Next, we generate a concealing disk CD_2 to cover q_2. Since $r_1 > |l_1^1|$ and $r_1 > |l_1^2|$ according to the previous analysis, part of q_2 must have been covered by CD_1. Then, CD_2 only needs to cover $q_2' \subset q_2$, a region enclosed by $\widehat{Q_2^1Q_3^1}$, $Q_3^1Q_3$ and $\widehat{Q_3Q_2^1}$, as depicted in Fig. 3. Similar to Lemma 1, we have the following lemma.

Lemma 2: As shown in Fig. 3, with the center S_2 being a randomly chosen point in q_2' and $r_2 = \max\{|l_2^1|, |l_2^2|, |l_2^3|\}$, the second concealing disk CD_2 can fully cover q_2'.

Proof: We first extend the uncovered area in the second quadrant, i.e., q_2', to q_2'', a region enclosed by $Q_2^1Q_3^1$, $Q_3^1Q_3$, and $\widehat{Q_3Q_2^1}$. Obviously, if CD_2 can fully cover q_2'', then it can cover q_2' as well. Similar to the proof of Lemma 1, we can show that for three arbitrary points, M, N and P, on $Q_2^1Q_3^1$, $Q_3Q_3^1$, and $\widehat{Q_3Q_2^1}$, respectively, we have $|S_2M| \leq \max\{|l_2^1|, |l_2^2|\}$, $|S_2N| \leq \max\{|l_2^1|, |l_2^3|\}$, and $|S_2P| \leq \max\{|l_2^2|, |l_2^3|\}$. Thus, when $r_2 = \max\{|l_2^1|, |l_2^2|, |l_2^3|\}$, CD_2 can cover $\Delta Q_2^1S_2Q_3^1$, $\Delta Q_3^1S_2Q_3$, and $\langle Q_3S_2Q_2^1\rangle$, i.e., q_2'', and hence q_2'. ■

3) Generating CD_3: According to Lemma 1 and Lemma 2, both CD_1 and CD_2 will cover part of the third quadrant q_3. We then generate the third concealing disk CD_3 to cover the uncovered region of q_3, denoted by q_3'. As illustrated in Fig. 4(a) and Fig. 4(b), there are two cases, depending on whether one of the intersections of CD_1's and CD_2's perimeters lies inside q_3 or not. We have the following results. The proofs are similar to those shown above and are omitted due to space limit.



(a) (b)

Fig. 4. Generating CD_3 to cover q_3'. (a) Case I. (b) Case II.

Lemma 3: As shown in Fig. 4(a), if one of the intersections of CD_1's and CD_2's perimeters lies inside q_3, with the center S_3 being a randomly chosen point in q_3' and the radius $r_3 =$

$\max\left\{|l_3^1|, |l_3^2|, |l_3^3|, |l_3^4|\right\}$, the third concealing disk CD_3 can fully cover q_3'.

Lemma 4: As shown in Fig. 4(b), if CD_1's and CD_2's parameters do not intersect within q_3, with the center S_3 being a randomly chosen point in q_3' and the radius $r_3 = \max\left\{|l_3^1|, |l_3^2|, |l_3^3|\right\}$, the third concealing disk CD_3 can fully cover q_3'.

4) Generating CD_4: Finally, we find the fourth concealing disk CD_4 to cover the uncovered region in the fourth quadrant q_4, i.e., q_4'. Again, as shown in Fig. 5(a) and Fig. 5(b), there are two cases, depending on whether one of the intersections of CD_1's and CD_2's parameters lies inside CD_3 or not. If none of the intersections falls inside CD_3, as shown in Fig. 5(a), q_4' is enclosed by $\widehat{Q_4^2Q_4^3}$, $\widehat{Q_4^3Q_1^1}$, $\widehat{Q_1^1Q_1^2}$, and $\widehat{Q_1^2Q_4^2}$. Otherwise, as shown in Fig. 5(b), q_4' is enclosed by $\widehat{Q_4^2Q_4^3}$, $\widehat{Q_4^3Q_1^1}$, and $\widehat{Q_1^1Q_4^2}$. So we can generate the following concealing disk to cover q_4'.

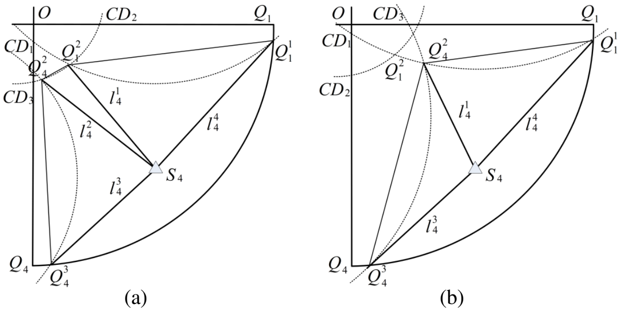


Fig. 5. Generating CD_4 to cover q_4'. (a) Case I. (b) Case II

Lemma 5: As shown in Fig. 5, with the center S_4 being a randomly chosen point in q_4', and the radius r_4 equal to $\max\left\{|l_4^1|, |l_4^2|, |l_4^3|, |l_4^4|\right\}$ if none of the intersections of CD_1's and CD_2's perimeters falls inside CD_3 and equal to $\max\left\{|l_4^1|, |l_4^3|, |l_4^4|\right\}$ otherwise, the fourth concealing disk CD_4 can fully cover q_4'.

B. Extension of Basic n-CD: Concealing Space Rotation

After generating the four concealing disks, the user will send the centers and the radii of these disks to the server, which then searches for all the POIs in $\bigcup_{i=1}^4 CD_i$ and returns the results to the user. With the information reported by the user, the server is able to infer that the user is located within a certain area, which we call the "*anonymity zone*". Obviously, larger anonymity zone results in higher location privacy for the user. In the following, we first analyze the anonymity zone that the above proposed algorithm results in and then try to prevent attackers from shrinking the anonymity zone.

In particular, since the four concealing disks are centered in four quadrants with respect to the user, respectively, the server can infer that the user must be located inside the quadrilateral $S_1S_2S_3S_4$. Moreover, as illustrated in Fig. 6, the server can know that the user cannot be in the light-shaded areas. For instance, if the user is inside ΔS_2S_3T, then S_1, S_2, and S_4 would all reside in the two quadrants q_1 and q_4, which is impossible. Thus, finally the server is able to narrow the anonymity zone down to the medium-shaded rectangle as illustrated in Fig. 6, the length and width of which, denoted by l_z and w_z, respectively, are as follows:

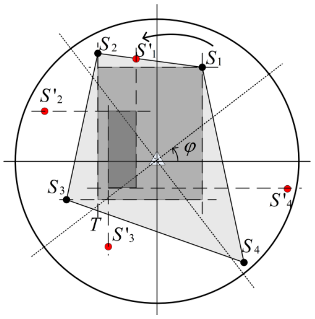


Fig. 6. Concealing space rotation.

$$w_z = \min\left\{|x_{S_1} - x_{S_2}|, |x_{S_1} - x_{S_3}|, |x_{S_4} - x_{S_2}|, |x_{S_4} - x_{S_3}|\right\}$$
$$l_z = \min\left\{|y_{S_1} - y_{S_3}|, |y_{S_1} - y_{S_4}|, |y_{S_2} - y_{S_3}|, |y_{S_2} - y_{S_4}|\right\}$$

where $(x_{S_i}, y_{S_i}), i = 1, ..., 4$, are the coordinates of S_i.

In order to address the above problem and prevent the server from narrowing the anonymity zone down to a largely shrinked rectangle, we rotate the generated concealing space, i.e., the four generated concealing disks, with respect to the user's location by a random angle $\varphi \in (0°, 360°)$. Suppose the concealing disk centers, i.e., S_1–S_4, are rotated to S_1'–S_4', respectively. Note that the concealing disk radii, i.e., r_i's, will not change after rotation. Then, we have the following result.

Lemma 6: If we rotate the original concealing space with respect to the user's location by a random angle $\varphi \in (0°, 360°)$, the server will not be able to narrow down the anonymity zone to a rectangle of area $l_z w_z$.

Proof: The proof of this lemma is briefly illustrated in Fig. 6. After rotating the whole concealing space by a random angle φ, the user will report new concealing disk centers, i.e., S_i''s, instead of S_i's to the server. As shown in Fig. 6, it is possible that the user is not inside the aforementioned rectangle, i.e., the heavy-shaded area. Since the value of φ is the user's private information and will not be reported to the server, the server cannot know whether the user is inside the constructed rectangle or not. Moreover, referring to Fig. 3 to Fig. 5, the user may not be located in the intersection area of the four concealing disks, either. ■

The above are all the procedures in our location privacy preserving algorithm n-CD when n is equal to 4. The other cases when $n \geq 3$ follow similar processes. In a nutshell, in order to preserve his/her own location privacy, a user conduct the ROI query procedure in two steps. First, the user generates n concealing disks to collaboratively and fully cover the user's ROI. The transformation from the ROI to the concealing space $\mathbb{C}$ is a *lossless query transformation*, which guarantees that the user can find all the POIs that he/she is interested in. Then, the user rotates the generated concealing space and sends the new concealing disks' centers and radii to the server. The orders of the concealing disks are scrambled so that attackers would not know which concealing disk is the first one[2]. We leave the

[2] Note that the first disk is not necessarily the largest one.

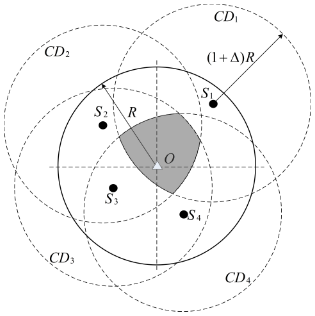


Fig. 7. A user's anonymity zone.

analysis of privacy level and concealing cost of the developed location privacy protection scheme to the next section.

IV. Analysis of Privacy Level and Concealing Cost

In the proposed n-CD, users are allowed to adapt his/her parameters n and to satisfy their own requirements on privacy level Γ and concealing cost Ψ. In this section, we analyze the privacy level and the concealing cost of n-CD.

A. Privacy Level

According to the proposed n-CD algorithm, a user need send the centers (S_i''s) and radii (r_i's) of the rotated concealing disks to the server. Based on such information, attackers will be able to reduce the anonymity zone from the whole concealing space $\mathbb{C}$ to a smaller area. In particular, in n-CD, the distance between S_i' and the user's real position must be no larger than R, i.e., the radius of the use's ROI. Therefore, attackers can know that the user must be located inside the intersection area of n disks centered at S_i''s ($1 \leq i \leq n$), respectively, with radius of R, as shown in Fig. 7, which is considered as the user's anonymity zone. Although the coordinates of S_i''s are known to the attacker, R is a private parameter which the attacker does not know. Thus, in order to make sure that the user is inside the anonymity zone, the attacker needs to estimate the maximum of R given S_i''s and r_i's.

As presented in Section III, r_1, the radius of the first concealing disk, is a function of R depending on the location of S_1, which we denote by

$$r_1 = f(x_{S_1}, y_{S_1})R. \tag{3}$$

Since the orders of the reported concealing disks are scrambled and the attackers do not know which one is the first concealing disk, the maximum of R, which we denote by R_{max}, can be found as follows:

$$R_{max} = \max_{i \in [1,n]} \{r_i\} / \min\{f(x_{S_1}, y_{S_1})\}. \tag{4}$$

We can firstly obtain the following result.

***Lemma** 7:* Denote by $r_{1,min}$ the minimum value of r_1. Then, we have

$$r_{1,min} = \begin{cases} \frac{\sqrt{3}}{2}(1+\Delta)R, & \text{when } n = 3, \\ (1+\Delta)\frac{R}{2\cos\frac{\pi}{n}}, & \text{when } n \geq 4. \end{cases}$$

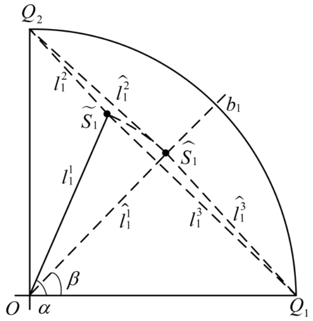


Fig. 8. Finding $r_{1,min}$ ($n \geq 3$).

Proof: As shown in Fig. 8, if S_1 is not on the angular bisector b_1, say at point $\widetilde{S}_1$, then we can always find a point $\widehat{S}_1$ on b_1 such that $|O\widehat{S}_1| = |O\widetilde{S}_1|$. Denote the radius of the first concealing disk when S_1 is at $\widetilde{S}_1$ and at $\widehat{S}_1$, by $\widetilde{r}_1$ and $\widehat{r}_1$, respectively. Then, we have

$$\begin{aligned} \widetilde{r}_1 &= \max\{|l_1^1|, |l_1^2|, |l_1^3|\} \geq \max\{|l_1^1|, |l_1^3|\}, \\ \widehat{r}_1 &= \max\{|\widehat{l}_1^1|, |\widehat{l}_1^2|, |\widehat{l}_1^3|\} = \max\{|l_1^1|, |\widehat{l}_1^3|\} \end{aligned}$$

since $|l_1^1| = |\widehat{l}_1^1|$ and $|\widehat{l}_1^2| = |\widehat{l}_1^3|$. Moreover, since

$$\begin{aligned} |l_1^3| &= |l_1^1|^2 + R^2 - 2|l_1^1|R\cos\alpha, \\ |\widehat{l}_1^3| &= |l_1^1|^2 + R^2 - 2|l_1^1|R\cos\beta, \end{aligned}$$

and $\alpha > \beta$, we can obtain that $|\widehat{l}_1^3| < |l_1^3|$ and hence $\widehat{r}_1 < \widetilde{r}_1$. This indicates that $r_{1,min}$ is achieved when S_1 is located on the angular bisector Ob_1, and

$$r_{1,min} = \min\big\{\max\{|l_1^1|, |\widehat{l}_1^3|\}\big\} \cdot (1+\Delta). \tag{5}$$

We then define two functions $G_1(x)$ and $G_2(x)$, where $x \in [0, R]$, as follows:

$$\begin{aligned} G_1(x) &= |l_1^1| = x, \\ G_2(x) &= |\widehat{l}_1^3| = \sqrt{\Big(R\cos\frac{\pi}{n} - x\Big)^2 + \Big(R\sin\frac{\pi}{n}\Big)^2}. \end{aligned}$$

When $n = 3$, we have $G_2(x) \geq G_1(x)$ for any $x \in [0, R]$. Thus, from (5), we can get

$$r_{1,min} = \min_{x \in [0,R]} \{G_2(x)\} = \frac{\sqrt{3}}{2}(1+\Delta)R,$$

which is achieved when $|l_1^1| = R/2$.

In the case of $n \geq 4$, we can obtain that

$$G_2(x) = \sqrt{x^2 - \big(2R\cos\frac{\pi}{n}\big)x + R^2}.$$

Letting $G_1(x) = G_2(x)$, we get that $G_1(x)$ and $G_2(x)$ only intersect at $x = \frac{R}{2\cos\frac{\pi}{n}}$ when $0 \leq x \leq R$. Therefore, from (5), we can have that $r_{1,min}$ is achieved at $x = \frac{R}{2\cos\frac{\pi}{n}}$, which is $r_{1,min} = (1+\Delta)\frac{R}{2\cos\frac{\pi}{n}}$. ■

Notice that we can have $\min\{f(x_{S_1}, y_{S_1})\} = r_{1,min}/R$ according to (3). Thus, from (4), we can have the following result.

Lemma 8: The anonymity zone is the overlapping region of n disks with centers at S_i''s ($1 \leq i \leq n$), respectively, and the same radius of

$$\overline{R}_{max} = \begin{cases} \frac{2}{\sqrt{3}} \cdot \max\limits_{i \in [1,n]} \{r_i\}, & \text{when } n = 3, \\ 2\cos\frac{\pi}{n} \cdot \max\limits_{i \in [1,n]} \{r_i\}, & \text{when } n \geq 4. \end{cases}$$

Proof: From (4), we can have

$$R_{max} = \frac{\max_{i \in [1,n]}\{r_i\}}{\min\{f(x_{S_1}, y_{S_1})\}} = \frac{\max_{i \in [1,n]}\{r_i\}}{r_{1,min}/R}.$$

When $n = 3$, we have $R_{max} = \max_{i \in [1,n]}\{r_i\}/[\frac{\sqrt{3}}{2}(1+\Delta)] < \frac{2}{\sqrt{3}} \max_{i \in [1,n]}\{r_i\}$, which we denote by $\overline{R}_{max}$, since attackers do not know the value of Δ. In other words, the attackers can only be sure that the user is not farther than $\overline{R}_{max}$ from the reported concealing disk centers, i.e., S_i''s. The results when $n \geq 4$ can be derived similarly. ■

Thus, from Lemma 8, the user's privacy level Γ is equal to the expected area of the overlapping region of n disks with centers at S_i''s ($1 \leq i \leq n$), respectively, and the same radius of $\overline{R}_{max}$.

B. Concealing Cost

Recall that concealing cost Ψ is defined as the expected area of the concealing space $\mathbb{C}$. Since the concealing space has an irregular shape, it is very difficult to obtain the exact Ψ. As a result, in what follows we find an upper bound on the area of concealing space $\mathbb{C}$, which can also serve as an upper bound on the expected area of $\mathbb{C}$, i.e., the concealing cost Ψ.

We denote the upper bound on Ψ by $\overline{\Psi}$. We can find $\overline{\Psi}$ by calculating the area of a disk $\overline{\mathbb{C}}$, which is centered at the user's location O covering the whole concealing space $\mathbb{C}$. Let d_{max}^i ($1 \leq i \leq n$) denote the maximum distance between O and an arbitrary point in the ith concealing disk CD_i. Then, the radius of $\overline{\mathbb{C}}$ is equal to $\max_{i \in [1,n]}\{d_{max}^i\}$.

We first find d_{max}^1 in the following.

Lemma 9: As shown in Fig. 9, the maximum distance between O and an arbitrary point in the first concealing disk CD_1, i.e., d_{max}^1, is

$$d_{max}^1 = \max_{l_1^1 \in [0,R], \alpha \in [0, \frac{2\pi}{n}]} \{|l_1^1| + r_1\}$$

where r_1 is the radius of CD_1.

Proof: Obviously, d_{max}^1 is achieved when an arbitrary point, say A, is on the perimeter of CD_1. As shown in Fig. 9, point B is the intersection of line OS_1 and the perimeter of CD_1. Then, we have

$$|OB| = |OS_1| + |S_1B| = |OS_1| + |S_1A| \geq |OA|.$$

Since $|OS_1| = |l_1^1|$ and $|S_1A| = r_1$, the final result for d_{max}^1 directly follows. ■

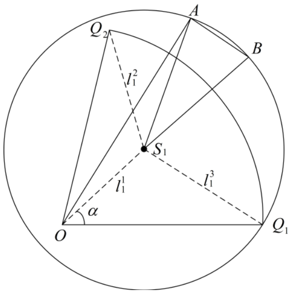


Fig. 9. Illustration of d_{max}^1.

From Lemma 9, we can see that d_{max}^1 is determined by l_1^1 and r_1. As shown in Fig. 10, we can divide the first sector into three areas, i.e., T_{Q_1}, T_{Q_2}, and T_O, with the help of three lines d_1, d_2, and d_3. Note that d_1 and d_2 are the perpendicular bisectors of line segments OQ_2 and OQ_1, respectively, while d_1 is the bisector of angle $\angle Q_2OQ_1$ which is also the perpendicular bisectors of line segment Q_1Q_2. We can easily prove that d_1, d_2 and d_3 intersect at the same point. Thus, we can have the following result.

Lemma 10: If $S_1 \in T_{Q_1}$, then $r_1 = (1+\Delta)|l_1^3|$; if $S_1 \in T_{Q_2}$, then $r_1 = (1+\Delta)|l_1^2|$; if $S_1 \in T_O$, then $r_1 = (1+\Delta)|l_1^1|$.

Proof: If $S_1 \in T_{Q_1}$, we can have $|l_1^3| \geq |l_1^1|$ since S_1 is to the left of d_2, and $|l_1^3| \geq |l_1^2|$ since S_1 is to the left of d_3. Thus, based on Lemma 1, we get $r_1 = (1+\Delta)\max\{|l_1^1|, |l_1^2|, |l_1^3|\} = (1+\Delta)|l_1^3|$. The results for the other two cases can be derived similarly. ■

Consequently, based on Lemma 9 and Lemma 10, letting $x = |l_1^1|$, we can obtain the following.

1) When $S_1 \in T_{Q_1}$, we get

$$\begin{aligned} d_{max}^1 =& \max\left\{x + (1+\Delta)\sqrt{(R\sin\alpha)^2 + (R\cos\alpha - x)^2}\right\} \\ =& \max\{x + (1+\Delta)\sqrt{x^2 - 2Rx\cos\alpha + R^2}\}. \end{aligned}$$

2) When $S_1 \in T_{Q_2}$, we have

$$\begin{aligned} d_{max}^1 =& \max\Bigg\{x + (1+\Delta) \cdot \\ & \sqrt{[R\sin(\frac{2\pi}{n} - \alpha)]^2 + [R\cos(\frac{2\pi}{n} - \alpha) - x]^2}\Bigg\} \\ =& \max\left\{x + (1+\Delta)\sqrt{x^2 - 2Rx\cos(\frac{2\pi}{n} - \alpha) + R^2}\right\}. \end{aligned}$$

3) When $S_1 \in T_O$, we get

$$d_{max}^1 = \max\{x + (1+\Delta)x\}.$$

As shown in Fig. 10, the shapes of T_{Q_1}, T_{Q_2}, and T_O are various depending on n. In particular, when $3 \leq n \leq 6$, both the perpendicular bisectors d_1 and d_2 intersect with the perimeter of the first sector q_1 on arc $\widehat{Q_1Q_2}$ (Fig.10(a)). When $n > 6$, d_1 and d_2 intersect with the perimeter of q_1 on OQ_1 and OQ_2 (Fig.10(b)), respectively. Next, we find d_{max}^1 in these two different cases, respectively.

- *Case I:* $3 \leq n \leq 6$. When $S_1 \in T_{Q_1}$, we find that d_{max}^1 can be obtained when $\alpha = \frac{2\pi}{n}$ and $x = R$. Therefore,

$$d_{max}^1 = \left(1 + 2(1+\Delta)\sin\frac{\pi}{n}\right)R.$$

When $S_1 \in T_{Q_2}$, d_{max}^1 is achieved when $\alpha = 0$ and $x = R$, which is the same as above. When $S_1 \in T_O$, d_{max}^1 is obtained

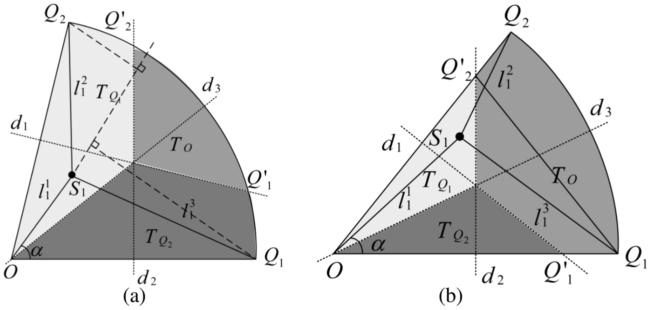


Fig. 10. Finding d^1_{max}. (a) $3 \le n \le 6$. (b) $n > 6$.

when $x = R$. So, we have

$$d^1_{max} = (2 + \Delta)R.$$

Since $n \le 6$, we have $\sin\frac{\pi}{n} \ge \frac{1}{2}$, and hence

$$d^1_{max} = \left(1 + 2(1 + \Delta)\sin\frac{\pi}{n}\right)R.$$

- *Case II:* $n > 6$. When $S_1 \in T_{Q_1}$, we can get

$$d^{1,Q_1}_{max} = \max\{x + (1 + \Delta)|l^3_1|\}$$

where $x \le R$ and $|l^3_1| \le \max\{|Q_1O|, |Q_1Q_2|\} = |Q_1O| = R$. And when $S_1 \in T_O$, we can have $d^{1,O}_{max} = R + (1 + \Delta)R$. Therefore, we can know that $d^{1,Q_1}_{max} \le d^{1,O}_{max}$.

Similarly, when $S_1 \in T_{Q_2}$, we can get $d^{1,Q_2}_{max} = \max\{x + (1 + \Delta)|l^2_1|\} \le d^{1,O}_{max}$. Consequently, we can have d^1_{max} is equal to $(2 + \Delta)R$ when $n > 6$.

Notice that in the other sectors, the uncovered area is no larger than the area of the first sector. So we can have $d^i_{max} \le d^1_{max}$ for $i > 1$[3]. As a result, an upper bound on the concealing cost Ψ is as follows

$$\overline{\Psi} = \begin{cases} \pi\left(1 + 2(1 + \Delta)\sin\frac{\pi}{n}\right)^2 R^2, & \text{when } 3 \le n \le 6 \\ \pi(2 + \Delta)^2 R^2, & \text{when } n \ge 6 \end{cases}$$

Obviously, $\overline{\Psi}$ is a non-increasing function of n.

V. Performance Evaluation

In this section, we evaluate the performance of the proposed *n-CD* algorithm by simulations in Matlab 2010a. Specifically, we consider a network area of $10^4m \times 10^4m$, in which there are 1000 points of interests (POIs) randomly and uniformly distributed. We employ the Monte Carlo method to obtain the area of anonymity zone and that of concealing space, and take the averages over 100 runs to get the expected values, i.e., the privacy level and the concealing cost.

A. Privacy Level

In this subsection, we evaluate the privacy level Γ of *n-CD* and compare it with that of PAD [12]. To study the impact of n on Γ, we show the privacy level Γ with $R = 1000m$ and $\Delta = 0.1$ while n ranges from 3 to 10 in Fig. 11(a). We can observe that Γ decreases as the number of concealing disks n increases. This indicates that a user can improve his/her location privacy by choosing a smaller n. We can also find that the privacy level remains relatively stable when $n \ge 6$. Besides, Fig. 11(b) shows the privacy level Γ of n-CD with different R's when $n = 3$, 6, and 9, respectively, compared with that of PAD. Note that in PAD, a user's privacy level is equal to k, which accounts for the user's real locations plus $k - 1$ dummy nodes' locations. We directly apply the settings specified in [12] in our simulations, where $k = 25$. On the other hand, in n-CD, a user's privacy level gets higher as R increases. We can see that n-CD achieves a much higher privacy level Γ than PAD.

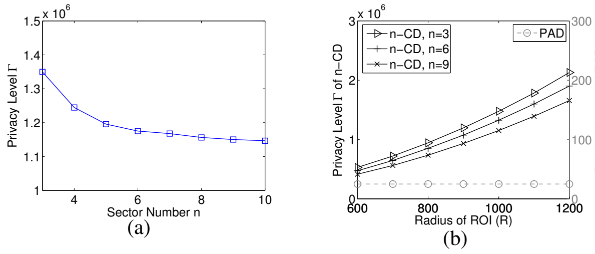


Fig. 11. Privacy level Γ of n-CD. (a) $R = 1000m$ and $\Delta = 0.1$. (b) $n = 3, 6, 9$ and $\Delta = 0.1$.

B. Concealing Cost and Communication Cost

Next, we study the concealing cost Ψ of the proposed n-CD algorithm. Recall that Ψ is defined as the expected area of the concealing space. In addition to Ψ, we also study the communication cost of n-CD, including both downstream and upstream traffic. In particular, the downstream traffic is calculated as $40 + 8 \times N$ bytes[4], where N is the number of POIs returned by the server, and the upstream traffic is calculated as $48 + 12 \times n$ bytes[5].

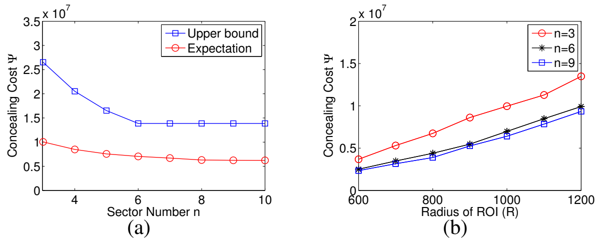


Fig. 12. Concealing cost Ψ of n-CD. (a) $R = 1000m$ and $\Delta = 0.1$. (b) $n = 3, 6, 9$ and $\Delta = 0.1$.

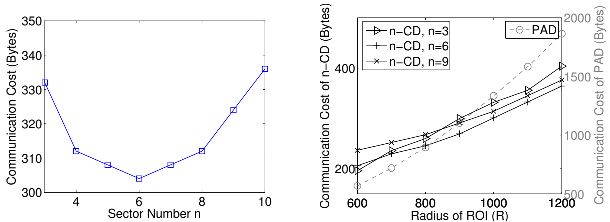
Fig. 12(a) shows the concealing cost Ψ of n-CD along with the derived theoretical upper bound $\overline{\Psi}$, when $R = 1000m$ and $\Delta = 0.1$. As mentioned in our analysis, $\overline{\Psi}$ is a non-increasing function with respect to n. We can also see that Ψ decreases as n increases. Fig.12(b) presents the concealing cost of n-CD when $\Delta = 0.1$ and $n = 3$, 6, and 9, respectively. We find that Ψ increases as R increases. Besides, the total incurred traffic (in bytes), including both downstream and upstream traffic, is shown in Fig. 13. In particular, Fig. 13(a) gives

[3] Note that although $d^i_{max} \le d^1_{max}$ for $i > 1$, the size of the first disk is not necessarily the largest.

[4] The header of a packet has 40 bytes. Besides, it takes 8 bytes to represent the coordinates of each POI.

[5] It takes 8 bytes and 4 bytes to represent the coordinates of the center and the radius of each concealing disk, respectively. In addition, a user's ID u_{id} and preference $\mathcal{P}$ take 4 bytes each.

the communication cost as n varies, when $R = 1000m$ and $\Delta = 0.1$. We find that the total traffic first decreases and then increases as n increases. This is because the downstream traffic decreases but the upstream traffic increases as n grows. The minimum total traffic amount is achieved when $n = 6$. Note that the optimal n for minimum total traffic amount is dependent on the network settings, and hence cannot be predicted by users. We then compare the communication cost of n-CD and that of PAD in Fig. 13(b). We can find that n-CD achieves lower communication cost than PAD since the LBS service provider needs to send back all the ROIs for all the k queries in PAD. From Fig. 11(b) and Fig. 13(b), we can observe that the proposed n-CD algorithm outperforms PAD by achieving much higher privacy levels at much lower communication costs.



(a) (b)

Fig. 13. Total communication cost (bytes). (a) $R = 1000m$ and $\Delta = 0.1$. (b) $n = 3, 6, 9$ and $\Delta = 0.1$.

On the other hand, users can estimate an optimal n by finding $\max_n \Gamma/\Psi$. The results when $R = 1000m$ and $\Delta = 0.1$, 0.2, and 0.3 can be found in Fig. 14. We can see that Γ/Ψ first increases as n increases and then roughly remains stable when n exceeds a certain threshold, i.e., the estimated optimal value, which is equal to 8 when $\Delta = 0.1$, 7 when $\Delta = 0.2$, and 6 when $\Delta = 0.3$. In general, users can set R, n, and Δ based on their requirements on privacy level and concealing or communication cost.

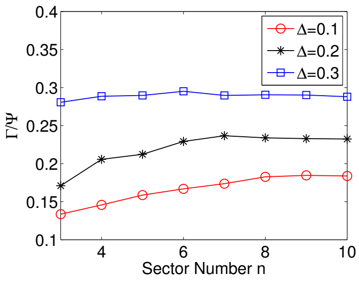


Fig. 14. Γ/Ψ with different n's and Δ's.

VI. Conclusion

In this paper, we have developed a novel location privacy preserving algorithm for LBSs, called n-CD. The basic idea is to generate n concealing disks (CDs) to collaboratively and fully cover a user's ROI and rotate the whole concealing space afterwards. Then, instead of simply sending users' locations to the service providers, we submit the positions of the rotated n CDs' centers and the n CDs' radii. In so doing, the users' location privacy can be protected since adversaries are only able to know that the users are within certain regions, i.e., anonymity zones. We have analyzed the privacy level and the concealing cost of this algorithm as well, and found there is a trade-off between them. Thus, each user can set the control parameters in the n-CD algorithm according to their own privacy and cost requirements.

References

[1] ABI, "http://www.abiresearch.com/press/1097-mobile+location+based+services+revenue+to+reach+$13.3+billion +worldwide+by+2013," 2008.

[2] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *ACM Mobisys'03*, May 2003.

[3] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, January 2008.

[4] M. F. Mokbel, C. Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proceedings of VLDB*, 2006.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719 – 1733, December 2007.

[6] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Proceedings of IEEE ICDCS*, Columbus, Ohio, June 2005.

[7] ——, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *Proceedings of ACM GIS*, Arlington, Virginia, November 2006.

[8] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, 2003.

[9] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Preserving privacy in gps traces via uncertainty-aware path cloaking," in *Proceedings of ACM CCS 2007*, Alexandria, VA, US, January 2007.

[10] J. Meyerowitz and R. R. Choudhury, "Hiding stars with fireworks: Location privacy through camouflage," in *Proceedings of ACM MobiCom*, Beijing, China, September 2009.

[11] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in *Proceedings of IEEE ICPS*, Santorini, Greece, July 2006.

[12] H. Lu, C. S. Jensen, and M. L. Yiu, "Pad: privacy-area aware, dummy-based location privacy in mobile services," in *Proceedings of ACM MobiDE*, Vancouver, Canada, June 2008.

[13] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proceedings of International Conference on Pervasive Computing*, Munich, Germany, May 2005.

[14] C. A. Ardagna, M. Cremonini, S. D. C. di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 1, pp. 13–27, January 2011.

[15] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "Cap: A context-aware privacy protection system for location-based services," in *Proceedings of IEEE ICDCS*, Montreal, Canada, June 2009.

[16] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, "Traffic-aware multiple mix zone placement for protecting location privacy," in *Proceeding of the IEEE International Conference on Computer Communications (INFOCOM'12)*, Orlando, FL, USA, March 2012.

[17] M. L. Yiu, C. S. Jensen, J. Moller, and H. Lu, "Design and analysis of a ranking approach to private location-based services," *ACM Transactions on Database Systems*, vol. 36, no. 2, May 2011.

[18] M. Damiani, E. Bertino, and C. Silvestri, "Probe: An obfuscation system for the protection of sensitive location information in lbs," *Technical Report 2001-145, CERIAS*, 2008.

[19] G. R. Hjaltason and H. Samet, "Distance browsing in spatial databases," *ACM Transactions on Database Systems*, vol. 24, no. 2, June 1999.

[20] N. Roussopoulos, S. Kelley, and F. Vincent, "Nearest neighbor queries," in *Proceedings of ACM SIGMOD*, San Jose, California, May 1995.