ChinaRxiv

AI translation · View original & related papers at
chinarxiv.org/items/chinaxiv-202204.00066

Postprint: Achieving Location Privacy Protection through Local Differential Privacy under K-Anonymity

Authors: Liu Zhenpeng, Miao Dewei, Liu Qiannan, Li Ruilin, Li Xiaofei

Date: 2022-04-07T15:01:57+00:00

Abstract

To address the issue of attackers exploiting background knowledge and other information to launch attacks during user location privacy protection, this paper proposes a location privacy protection method for mobile terminals. The scheme leverages k-anonymity and local differential privacy techniques to protect user locations, ensuring a trade-off between privacy and utility. It constructs anonymous sets by incorporating background knowledge, partitions the k-anonymous set via an improved Hilbert curve, perturbs the partitioned location set using the local differential privacy algorithm RAPPOR, and finally transmits the generated location set to the location service provider to obtain services. Experiments on real datasets compare the proposed approach with existing schemes in terms of user location protection, location availability, and time overhead. The results demonstrate that the proposed scheme enhances the degree of location privacy protection while ensuring the quality of LBS services.

Full Text

Preamble

Vol. 39 No. 8
Application Research of Computers

Location Privacy Protection Through Local Differential Privacy Under k-Anonymity

Liu Zhenpeng[1]†, Miao Dewei[1], Liu Qiannan[1], Li Ruilin[1], Li Xiaofei[2]
[1]School of Cyber Security & Computer, [2]Information Technology Center, Hebei University, Baoding, Hebei 071002, China

Abstract: To address the problem of attackers exploiting background knowledge to launch attacks during user location privacy protection, this paper proposes a location privacy protection method for mobile terminals. This solution leverages k-anonymity and local differential privacy technologies to safeguard user locations while ensuring a trade-off between privacy and utility. The scheme constructs anonymous sets by incorporating background knowledge, segments the k-anonymous set using an improved Hilbert curve, perturbs the divided location sets with the local differential privacy algorithm RAPPOR, and finally transmits the generated location sets to location service providers to obtain services. Experiments on real datasets compare the proposed scheme with existing approaches in terms of user location protection, location availability, and time overhead. Results demonstrate that the proposed scheme enhances location privacy protection while ensuring LBS service quality.

Keywords: RAPPOR; k-anonymity; Hilbert curve; location protection

0 Introduction

The rapid development of Internet technology, satellite positioning technology, and mobile devices has led to widespread adoption of location-based services (LBS) [1,2]. While users enjoy the convenience of location services, the resulting location privacy leakage from LBS poses significant concerns. Malicious location service providers (LSP) can extract sensitive user information from location data, severely compromising user privacy. Consequently, location privacy protection has become a critical research focus in user privacy preservation [3].

In location privacy protection research, k-anonymity technology has been widely applied. Originally proposed by Sweeney [4], its core idea uses attribute generalization to make individual data indistinguishable from k-1 other data points. Gruteser and Grunwald [5] first applied k-anonymity to location privacy protection, constructing k-anonymous location models through quadtree search to ensure anonymous regions met minimum size requirements. However, this method increases time overhead, tends to generate excessive anonymous locations, uses uniform k values, and cannot accommodate personalized user preferences. To address excessive anonymous location generation, Kido et al. [6] employed random strategies to generate k-anonymous sets, reducing communication costs, but failed to consider unreasonable dummy locations, thereby degrading security and service quality. Zhu et al. [7] added a location caching mechanism to Kido' s approach, designing the MobileCache system that reduced query frequency and resource overhead while improving utilization. Ye et al. [8] considered service similarity when generating anonymous regions to enhance service quality, but neither approach accounted for background knowledge attacks. Yin et al. [9] combined k-anonymity with pseudonym methods, selecting appropriate anonymization approaches based on k' s maximum and minimum values to improve location protection. Jin et al. [10] designed a trust-based location hiding

mechanism that added k-1 trusted users to anonymous regions, ensuring each user achieved their desired anonymity level, but this mechanism relied on centralized anonymous servers. Ling et al. [11] addressed untrusted anonymous servers by constructing a distributed location privacy protection mechanism based on offset grids, dividing location regions into grids using historical query probabilities and selecting k-1 grid coordinates to form anonymous sets, preventing untrusted servers from obtaining real user information. Zhang et al. [12] combined k-anonymity with irregular polygon generation algorithms to create polygonal anonymous regions, achieving spatial anonymity through density parameters and constructing dummy locations. Yan et al. [13] constructed similarity maps through service similarity, selected points of interest with query results similar to the user' s real location from these maps, and combined background knowledge to generate anonymous sets with maximum entropy, randomly selecting one location from the set to complete query services, thereby ensuring privacy while maximizing service quality. Yang et al. [14] designed a k-anonymous dummy selection algorithm based on historical query probabilities, improving location privacy security from geographical distribution and zero-query perspectives, but required discretization during anonymous set construction, increasing generation time.

Differential privacy (DP), first proposed by Dwork [15] in 2006, provides rigorous mathematical guarantees that user privacy remains protected against background knowledge attacks and individual data changes. Yuan et al. [16] designed an LBS trajectory protection algorithm combining Laplace mechanisms with anonymous groups, generating anonymous groups through multiple rounds of noise addition to real LBS user locations for service acquisition, addressing excessive privacy budget dependency in DP-based trajectory protection and enhancing effectiveness. Wang Jie et al. [17] proposed a location protection method based on differential privacy perturbation, using Hilbert curves to map locations into one-dimensional space and Laplace noise to perturb location information before sending it to service providers. Zhang et al. [18] employed a max-min distance-based multi-center clustering algorithm to generate multiple candidate dummy sets, selecting optimal virtual candidate sets to achieve k-anonymity. Zhang et al. [19] proposed a differential privacy-based location privacy protection scheme including mean and anonymous algorithms, using Laplace mechanisms to protect location privacy and exponential mechanisms to protect query privacy.

DP protection of sensitive information requires a fully-trusted third party (TTP) data collector, but third-party security cannot be guaranteed in real environments. Consequently, researchers proposed the concept of local differential privacy (LDP) [20-22], enabling users to process sensitive data locally and avoid untrusted third-party leakage issues. Wang et al. [23] proposed an LDP-based continuous location upload protection scheme, using Hilbert curves to dynamically subdivide regions based on user location counts, perturbing locations through LDP before uploading to servers, though this reduced data availability. Wang et al. [24] allowed participants to select between two LDP perturbation methods—

RAPPOR and k-RR—based on personal privacy requirements at their current location, segmenting participant locations and perturbing location regions before sending them to data collection servers for analysis.

Addressing these issues, this paper combines k-anonymity and LDP technologies to propose a local differential privacy perturbation scheme that requires no TTP and can resist background knowledge attacks, reducing the probability of attackers obtaining user information while ensuring performance and further improving location privacy security.

1.2 Location Entropy

Without considering background knowledge, the probability of identifying a user' s real location under k-anonymity protection is 1/k. Let qi denote the probability that loci is the real location, where i = 1, 2, ···, k, and Σqi = 1. Location entropy can estimate the privacy protection strength of an anonymous location set. The entropy value increases as the location set becomes more disordered, indicating higher privacy protection. The formula is as follows:

$H = -\Sigma(qi \times \ln(qi))$

When all qi values are equal, location entropy H reaches its maximum, representing the strongest privacy protection.

1.3 Hilbert Curve

The Hilbert curve maps s-dimensional space Rs to one-dimensional space R, denoted as H: Rs→R. If point p Rs, then H(p) R, meaning H(p) is the H-value corresponding to p. For a point set {p1, p2, ···, pn}, H{p1, p2, ···, pn} = {H(p1), H(p2), ···, H(pn)}. The Hilbert curve encoding rules are shown in Figure 1.

1.4 Location Local Differential Privacy

Given n locations where each corresponds to a record, and a privacy algorithm N with domain Def(N) and range Ran(N), algorithm N satisfies -local differential privacy if for any two location records t and t' (t, t' Def(N)) and any output result t* (t* Ran(N)), the following inequality holds:

$Pr[N(t) = t^*] \leq e^{\wedge} \times Pr[N(t') = t^*]$

This demonstrates that LDP controls algorithm N to produce similar outputs, preventing attackers from distinguishing which data represents the user' s real location.

2.1 System Architecture

In trusted third-party models, the TTP easily becomes a system efficiency bottleneck when users initiate multiple requests. Moreover, TTPs themselves are vulnerable; once compromised, all user privacy information leaks. Therefore, this

paper' s solution eliminates TTPs, consisting primarily of local users and LSPs, as shown in Figure 2. Local users obtain their location information through wireless devices and run privacy protection schemes locally, avoiding security risks from untrusted third parties. They send perturbed location queries to LSPs, which return query results. Local users then process these results through location processing algorithms to display required data.

2.2 k-Anonymous Location Set Generation

The k-anonymous location set generation process first obtains user query request probabilities at urban points of interest from historical records, sorts these probabilities to generate probability table T, stores T locally for future queries, and updates T periodically to prevent data staleness. To counter background knowledge attacks, the anonymous set' s entropy should be maximized. Therefore, points with query probabilities closest to the user' s real location Z are added to anonymous candidate region Lc. Research [13] shows that entropy in Lc increases with location count, approaching maximum entropy at 2k-2 locations with no significant increase beyond this point. Location count directly affects computational overhead. To balance efficiency and privacy protection, Lc' s location count is set to 2k-2. To ensure selected locations maintain good utility, the nearest points of interest are chosen based on Euclidean distance from the user' s real location. The Lc generation algorithm is as follows:

Algorithm 1: Anonymous Candidate Region Lc Generation
Input: T, Z, k
Output: Lc

a) Obtain Z' s query probability Zp from T

b) Retrieve points of interest with probability difference from Zp not exceeding , store in temporary location set R

c) Calculate Euclidean distance Si from each location ri in R to Z

d) Use heap sort to select the top 2k-2 points with smallest Si, store in Lc

e) End

As shown in Figure 3, after querying table T to obtain point-of-interest probabilities and comparing them with Z, points L1, L2, L3, L4, L5 have probability differences from Z not exceeding =0.01. Their Euclidean distances to Z are Si={1,2,3,4,5}. For k=2, after comparing Si values, Lc={L2, L3}. If temporary set R contains n points, Algorithm 1' s space complexity is O(n). Using heap sort to order distances yields time complexity O(nlogn).

From generated Lc, k-1 locations are randomly selected with the user's real location to form k-anonymous set L. During L generation, selected locations should be maximally dispersed to ensure anonymous region scope, using the sum of

Euclidean distances between points as the dispersion metric. Through multiple random assignments, the most dispersed location set is selected, making the probability of attackers obtaining the real location from L approach 1/k. Since selection criteria include Euclidean distance from the real location, anonymous locations tend to cluster around the real location, which compromises protection. To further reduce attack success probability, an Improved Hilbert Curve (IHC) segments locations, and the segmented map is perturbed through RAPPOR.

The Hilbert curve maps geographical locations from two-dimensional to one-dimensional space while preserving spatial adjacency, reducing data processing time and improving efficiency. However, it cannot reflect point-of-interest density distributions, and densely populated regions should use finer granularity. IHC construction proceeds as follows: the farthest point from Z in L serves as boundary R, enclosing all locations in an N×N map space. When a region contains more than threshold σ=1 points of interest, it is recursively divided into four equal square subregions. Figure 4(a) shows the regional distribution after point segmentation, ensuring density-based distribution. The segmented IHC is stored in a quadtree, as shown in Figure 4(b). With k points of interest, storage overhead is O(k) and IHC value computation complexity is O(k). Compared to standard Hilbert curves, IHC segmentation saves storage space and improves computational efficiency.

2.4 RAPPOR Perturbation Based on Local Differential Privacy

RAPPOR [22] can anonymize end-user crowdsourced data, providing efficient privacy and utility without trusted third parties. For anonymous candidate locations mapped to Hilbert curves, RAPPOR enables random perturbation for strong privacy protection. Let A={a1, a2, ···, an} represent region IDs after map segmentation, where n is the total region count. For region i, ai is set to 1 if a selected point of interest exists, otherwise 0. Let R be an n-bit array where Rj denotes the j-th bit value. When aj=1, the corresponding bit in R is set to 1, otherwise 0, as shown in formula (5).

Next, R is perturbed. Each bit in R undergoes random response perturbation as shown in formula (6), where f (f [0,1]) is a probability parameter controlling privacy level. Values closer to 1 provide stronger privacy guarantees. The generated R' is called the permanent random response in RAPPOR.

Another perturbation is then applied to each bit of R'to obtain the instantaneous random response U, as shown in formula (7). The generated U is called the instantaneous random response in RAPPOR, where the probability of the k-th bit being set to 1 depends on parameters q (or p) and Rk. According to RAPPOR, this random encoding method satisfies -differential privacy.

The probability that an initially selected region remains selected after RAPPOR perturbation is:

$Pr[U\_k = 1 \mid R\_k = 1] = p$

The probability that an initially unselected region becomes selected after perturbation is:

$Pr[U\_k = 1 \mid R\_k = 0] = q$

After RAPPOR perturbation, the geographical location set R is obtained through IHC decoding. Using R for queries ensures user location privacy. Since the real location may be lost during perturbation, when it is absent from R, the query results for the n locations nearest to the real location are retrieved from the LBS server' s response for anonymous set R, and their union is taken as the user' s query information. The location union algorithm is presented as Algorithm 2.

Algorithm 2: Location Union Acquisition
Input: R={lt, t=1,2,⋯,r}
Output: Result set T

a) Initialize T as empty

b) For all locations in R, calculate Euclidean distance to user' s real location

c) Use heap sort to select the top n locations with smallest distances

d) Select one location, store its query result points of interest in T

e) Sequentially query results for n locations, store union with T

f) Return T

Figure 5 shows query results for points of interest in location set R. With R={L1, L2, L3, L4, L5} as five points selected after perturbation and n=3, the three nearest locations are L2, L4, L5 with query results L2={a,b,e,f}, L4={e,f,g}, L5={c,d}. The union yields user query information T={a,b,c,d,e,f,g}. For r locations in R, heap sort complexity is O(rlogr). With m query results per location, generating T has complexity O(nmlogn). Thus Algorithm 2' s time complexity is max(O(rlogr), O(nmlogn)).

3.1 Experimental Environment and Methods

The San Francisco dataset [25] validates the proposed scheme' s performance, containing 174,956 points of interest. As shown in Figure 6, x and y represent Cartesian coordinates converted from latitude and longitude. Implementation uses Python 3.6 on Windows 10 Home with an Intel i7 CPU and 64GB RAM.

LBS servers can obtain user historical query records. As shown in literature [26], when query records are unavailable, point-of-interest counts on maps can serve as substitutes. This experiment uses San Francisco dataset points as user

query records. The map is divided into 100$×$100 uniform location cells, with each cell' s historical query probability serving as prior probability. One point of interest is randomly selected per cell, with its query probability equal to the cell' s historical query probability. The point in the user' s location cell serves as the real location.

3.2 Security Analysis

Security analysis examines anonymous set entropy and attack algorithm recognition probability, comparing the proposed scheme with others. Each data point represents averages over 100 experiments with k ranging from 2 to 30.

3.2.1 Attack Method Analysis

For LBS services, primary attacks include background knowledge attacks, probability attacks, and semantic attacks. Background knowledge attacks are typically mitigated by eliminating links between background information and user locations.

Probability attacks involve attackers using known information to filter unreasonable locations (e.g., rivers, deserts), increasing the probability of discovering real locations. While not directly associated with real locations, filtering such dummy locations from k-anonymous sets reduces privacy protection levels, enabling auxiliary attacks. Typically, probability attacks can be countered by using high-query-probability locations as dummy points after obtaining user history. This scheme uses real points of interest as dummies, selecting locations with query probabilities matching the user's real location to construct candidate sets, effectively preventing probability attacks.

Semantic attacks take many forms, with location homogeneity attacks being common. These occur when anonymous locations are too close to the real location, allowing attackers to further narrow the anonymous region through clustering even when k-anonymity is satisfied. This scheme selects the most dispersed location set as the anonymous set, reducing the probability of successful location homogeneity attacks.

3.2.2 Location Entropy

Performance validation compares the proposed scheme with literature [13], [14], and optimal selection. From the entropy formula, when k is fixed, location entropy depends on query probability differences among points in the anonymous set—smaller differences yield higher entropy. Maximum entropy occurs when all query probabilities are equal, defined here as optimal selection. Results are shown in Figure 7.

Figure 7 demonstrates that location entropy increases with k, enhancing anonymous set security. Optimal selection achieves maximum entropy. Literature [13] and [14] consider query probabilities, selecting points with probabilities similar

to the user' s location, achieving entropy values close to optimal (0.5% and 3% lower on average, respectively). The proposed scheme accounts for attacker-known background information, ensuring query probabilities in k-anonymous sets are as identical as possible. By introducing difference parameter in Algorithm 1 to select nearest-probability points, the generated anonymous set' s entropy approaches optimal selection most closely (only 0.3% lower on average), demonstrating high privacy protection.

3.2.3 Attack Algorithm Recognition Probability

When attackers obtain anonymous set R and combine it with background information, they can infer real locations using the attack algorithm from [14]. Figure 8 shows the probability distribution of anonymous set locations inferred by this attack algorithm for literature [13], [14], [17] and the proposed scheme under different privacy levels k. In formula (6), parameter f determines initial perturbation degree (f=1: fully random response; f=0: no perturbation). For privacy-utility balance, f is set to 0.5. In formula (7), parameters q and p determine perturbation degree and point count in location sets. Larger p+q values yield more points, while p+q=1 maintains approximately constant point counts. Based on utility analysis, q and p are set to 0.75 and 0.25, respectively. Experiments show that when n=k/2 in Algorithm 2, generated query results best match real location queries with highest efficiency, so n=k/2 is used.

Figure 8 shows the proposed scheme yields lower real location recognition probability than the other three schemes. Compared to [13] and [14], RAPPOR perturbation is added, potentially removing the real location from the anonymous set and increasing randomness. Literature [17] does not consider background knowledge when selecting obfuscation locations, allowing attackers to narrow location ranges. The proposed scheme' s anonymous region expands with k, reducing the probability of successful semantic attacks and effectively enhancing location protection.

3.3 Performance Analysis

Privacy protection schemes must consider performance utility. Figure 9 compares location service availability among literature [13], [14], [17] and the proposed scheme. Availability decreases as k increases. The proposed scheme better maintains query result availability because the anonymous set may or may not contain the real location. When it does, availability is optimal; when not, Algorithm 2 retrieves nearby query results, preserving availability. Under identical conditions, the proposed scheme achieves 11.95%, 5.92%, and 29.51% higher availability than literature [13], [14], and [17], respectively.

Figure 10 shows time overhead for literature [13], [14], [17] and the proposed scheme. Execution time increases with k. Literature [14] requires discrete location selection during anonymous set construction, resulting in slightly longer

runtime. The proposed scheme' s time overhead is marginally higher than literature [13] due to added perturbation.

4 Conclusion

This paper studies existing location privacy protection methods and proposes an anonymous protection scheme based on local differential privacy. By perturbing candidate locations in k-anonymous sets, the probability of real location leakage is reduced. Security and availability analyses demonstrate that the scheme achieves an excellent privacy-utility trade-off with significantly improved performance.

A limitation is low query result utilization when using anonymous sets for queries. Future work will employ local caching to improve query resource utilization, reduce interactions between users and LBS servers, and enhance location privacy protection.

References

[1] Dilay P, Udai P R. Towards Privacy-Preserving Dummy Generation in Location-Based Services [J]. Procedia Computer Science, 2020, 2020 (171): 1323-1326.
[2] Seo Y D, Cho Y S. Point of interest recommendations based on the anchoring effect in location-based social network services [J]. Expert Systems with Applications, 2021, 2021 (164): Article ID 114018.
[3] Zhang Qingyun, Zhang Xing, Li Wanjie, et al. Overview of location trajectory privacy protection technology based on LBS system [J]. Application Research of Computers, 2020, 37 (12): 3534-3544.
[4] Sweeney L. k-Anonymity: A Model for Protecting Privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10 (05): 557-570.
[5] Gruteser M, Grunwald D. Anonymous usage of location-based services through spatial and temporal cloaking [C]// Proc of the 1st International Conference on Mobile Systems, Applications and Services. New York: ACM Press, 2003: 31-42.
[6] Kido H, Yanagisawa Y, Satoh T. An anonymous communication technique using dummies for location-based services [C]// ICPS' 05. Proceedings. International Conference on Pervasive Services, 2005. Piscataway, NJ: IEEE Press, 2005: 88-97.
[7] Zhu Xiaoyan, Chi Haotian, Niu Ben, et al. Mobicache: When k-anonymity meets cache [C]// 2013 IEEE Global Communications Conference (GLOBECOM). Piscataway, NJ: IEEE Press, 2013: 820-825.
[8] Ye Ayong, Li Yacheng, Ma Jianfeng, et al. K-anonymous location privacy protection method based on service similarity [J]. Journal on Communications, 2014, 35 (11): 162-169.
[9] Yin Chunyong, Xi Jinwen, Sun Ruxia. Location Privacy Protection Based

on Improved K-Value Method in Augmented Reality on Mobile Devices [J]. Mobile Information Systems, 2017, 2017 (12): 1-7.
[10] Jin Lei, Li Chao, Palanisamy B, et al. k-Trustee: Location injection attack-resilient anonymization for location privacy [J]. Computers & Security, 2018, 78 (2): 212-230.
[11] Ling Jie, Xu Junyi. Decentralized Location Privacy Protection Method of Offset Grid [C]// 3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019). Atlantis Press, 2019: 113-120.
[12] Zhang Yongbing, Zhang Qiuyu, Yan Yan, et al. A k-Anonymous Location Privacy Protection Method of Polygon Based on Density Distribution [J]. International Journal of Network Security, 2021, 23 (1): 57-66.
[13] Yan Guanghui, Liu Ting, Zhang Xuejun, et al. Service similarity location k anonymous privacy protection method resisting background knowledge reasoning attack [J]. Journal of Xi' an Jiaotong University, 2020, 54 (01): 8-18.
[14] Yang Yang, Hu Xiaohui, Du Yongwen. K-anonymous dummy selection algorithm based on historical query probability [J/OL]. Computer Engineering: 1-14. (2021-03-30) [2021-12-10] https://doi.org/10.19678/j.issn.1000-3428.0060417.
[15] DWORK C. Differential privacy [C]// International Colloquium on Automata, Languages, and Programming. Berlin: Springer, 2006: 1-12.
[16] Yuan Jian, Wang Di, Gao Xilong, et al. An anonymous group LBS trajectory privacy protection model based on differential privacy [J]. Journal of Chinese Computer Systems, 2019, 40 (02): 341-347.
[17] Wang Jie, Wang Feng, Li Hongtao. Differential Privacy Location Protection Scheme Based on Hilbert Curve [J]. Security and Communication Networks, 2021, 2021 (1): Article ID 5574415.
[18] Zhang Yongbing, Zhang Qiuyu, Li Zongyi, et al. A k-anonymous Location Privacy Protection Method of Dummy Based on Geographical Semantics [J]. International Journal of Network Security, 2019, 21 (6): 911-920.
[19] Zhang Qingyun, Zhang Xing, Wang Mingyue, et al. DPLQ: Location-based service privacy protection scheme based on differential privacy [J]. IET Information Security, 2021, 15 (6): 442-456.
[20] DUCHI J C, JORDAN M I, WAINWRIGHT M J. Local privacy and statistical minimax rates [C]// 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. Piscataway, NJ: IEEE Press, 2013: 431-440.
[21] FANTI G, PIHUR V, ERLINGSSON Ú. Building a RAPPOR with the unknown: Privacy-preserving learning of associations and data dictionaries [J]. Proc on Privacy Enhancing Technologies, 2016, 2016 (3): 41-61.
[22] ERLINGSSON Ú, PIHUR V, KOROLOVA A. Rappor: Randomize aggregatable privacy-preserving ordinal response [C]// Proc of the 2014 ACM SIGSAC conference on computer and communications security. New York: ACM Press, 2014: 1054-1067.
[23] Wang Xiongjian, Yang Weidong. Protection method of continuous location uploading based on local differential privacy [C]// 2020 International Conference on Networking and Network Applications (NaNA). Piscataway, NJ: IEEE Press, 2020: 157-161.
[24] Wang Jian, Wang Yanli, Zhao Guosheng, et al. Location protection method

for mobile crowd sensing based on local differential privacy preference [J]. Peer-to-Peer Networking and Applications, 2019, 12 (5): 1155-1168.
[25] BRINKHOFF T. A framework for generating network-based moving objects [J]. GeoInformatica, 2002, 6 (2): 153-180.
[26] PINGLEY A, Zhang Nan, Fu Xinwen, et al. Protection of query privacy for continuous location based services [C]// Proceedings of the Computer and Communications Societies. Piscataway, NJ: IEEE Press, 2011: 1710-1718.

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv —Machine translation. Verify with original.