International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.217-222
http://dx.doi.org/10.14257/ijsia.2015.9.12.21

Road Network-based Location Privacy Protection

Chen Wen

School of Mathematics and Computer Science, Tongling College, Tongling, P. R. China
tlxychenwen@163.com

Abstract

The traditional location privacy protection means mainly employs reliable central server framework, and it mainly applies the anonymous region meeting the k-anonymity at the anonymous server to replace the real location of users. However, the disadvantages of the central server, such as being attacked easily, high communication cost, etc. are disclosed accordingly. In addition, the anonymous method of most locations is oriented for the European style, and it is not applicable to the road network. In order to solve the above problem, virtual user group-based centerless server framework is proposed for solving the location privacy protection in road network. This algorithm mainly forms the virtual user group with several virtual users in several road segments of the road network, and replaces the real position of the user with a certain point in the section, so as to realize the k-anonymity of user position with the increment nearest neighbor query. Since the algorithm adopts the accurate increment nearest neighbor query method, it guarantees the service quality. The experiment proves that the algorithm can reduce the communication cost effectively and improve the application safety.

Keywords: *location privacy; road network; virtual user group; incremental query*

1. Introduction

With the development of wireless communication and mobile location technology, the location service-based business also develops gradually. However, when users apply the services, they may be confronted by the threat of privacy disclosure. Mobile users shall send their accurate location to the location service provider for achieving the search result. The vicious location service provider or attacker can trace the public information of users according to the location and inquiry of users, thus to gain the privacy information of users [1]. In order to protect the location privacy of users, researchers have proposed a number of solutions. But most suppose that mobile users move in European-style space. In real life, no matter the user takes the traffic mean or walks, he may follow fixed road network. Apparently, in the road network, the space region hiding method is not applicable. In addition, most solutions employ the central server framework, but it has certain disadvantages. In order to protect the location privacy of users, and guarantee the service quality, a kind of location privacy protection plan employing the centerless server framework of virtual user group in the road network is put forward.

2. Related Work

The location privacy protection problem has already won the attention from the industry. The main solutions include the hiding of space region, fake location, etc. The hiding space region technology mainly adopts the location k-anonymity model [1], which mainly take place of the real location of user who sends the request with the anonymous region covering *k* users. At present, study based on k-anonymity model [2-4] mainly employs the central server framework. However, there are certain disadvantages in the

ISSN: 1738-9976 IJSIA

central server framework, for instance, the central server may become the bottleneck of system performance, it may be attacked by hacker easily, and it may consumer extra computing resource and communication. In order to solve the problem of central server, the user cooperation-based centerless server framework is proposed [5-8]. These methods all assume that the cooperation is reliable, but actually, it may not be true. The method based on the fake location [8] employs the nearby point of the real location as the location of check inquiry. However, it cannot realize the *k*-anonymity of location. In addition, a kind of cooperative non-anonymity region location privacy protection algorithm is proposed in reference [9].

The above methods suppose that users move in a free space. In reference [10], the location privacy protection in the simple road network is considered for the first time, and section *1*-diversity is proposed, which guarantees the location *k*-anonymity. Reference [11] proposed a method of solving the location privacy protection in the simple and complex road network. However, the above methods are still based on the central server framework. At present, the solution to the road network-oriented centerless server framework has not been proposed.

3. Virtual User Group Location Privacy Protection Method

3.1. Definition and Description

Definition 1, Road network model. Undirected graph G=(V,E) is adopted to stand for a road network. The edge of the graph can be considered as a road, and any uncovered edge in the undirected graph is called "tree edge".

For instance, in Figure 1, edge n5n6, n5n7, etc. are the tree edges.

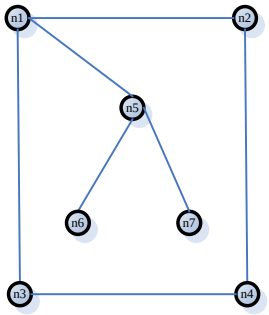

Figure 1. Road Network Model

The section *l*-diversity proposed in reference [10] points out that: if the information of a user satisfies location *k*-anonymity, and it contains at least *l* section (*l*>=*k*), the anonymous location may meet the *l*-diversity. The section *l*-diversity is a significant condition of the user location privacy in road network. On that basis, the definition of location privacy in road network is given.

Definition 2, Location privacy .(*k*, *1*) is employed to indicate the location privacy of a mobile user, in which, *k* means that the anonymous location shall include at least *k* users, while *l* means that the anonymous location shall include at least *l* section.

Definition 3, *k*-anonymous group. (*k*, anchor) is employed to indicate a *k*-anonymous group. *k* stands for the number of members in the anonymous group, while anchor stands for the anchor points in the anonymous group, namely the location where the user sends the inquiry.

Definition 4, Largest boundary tree .The free tree formed by tree edges in the undirected graph of road network is called the "boundary tree". As for a boundary tree, if another edge is added, it will not be the boundary tree, and such boundary tree is called the largest boundary tree.

For instance, in Figure 1. the tree edge n1n5, n5n6 and n5n7 form the largest boundary tree.

As for the tree edges forming the largest boundary tree, their boundary tree is unique. Therefore, attackers cannot figure out the possibility of users on each edge. Since attackers cannot learn about the number of users in each section. Suppose that there is a user on each edge of the largest boundary tree (namely section), the numbers of edge are equal or greater than *l* (*l*>=*k*), it may guarantee the section *l*-diversity. The process of looking for the largest boundary tree adopts the width-first search, and the algorithm description is shown as follows:

Algorithm 1: look for the largest boundary tree

Input: undirected graph G; the tree edge n_in_j of user *u*;

Output: all tree edges forming the largest boundary tree

for each u={ n_i,n_j }

for each adjacent vertex *w* of *u*

if vertex w is not accessed&&(*u*,*w*) is tree edge

output (*u*,*w*)

3.2. Virtual User Group and Location Anonymity

The basic steps of realizing the location privacy protection with virtual user group are shown as follows: the first user initiating the query, with algorithm 1, looking for the largest boundary tree in the undirected graph of road network. When the number of edges of the maximum boundary tree is equal or larger than *l* (*l*>=*k*), suppose there is a user in each edge. A certain point of the tree edge in the zone of largest boundary tree is selected at random as the anchor point. The user shall use the anchor point to replace his real position, and send the increment nearest neighbor query to the location server, while user of other tree edges shall launch the *l*-1 fake query. After the query, the anonymous group shall be dissolved. Since the tree edge (section) of the largest boundary tree is *l*, and supposing that there is at least one user in each tree edge (section). In this way, it can satisfy the section *l*-diversity proposed in reference [10], realizing the *k*-anonymity of user location, and guaranteeing the user location privacy. Next, the algorithm description of the increment nearest neighbor query is given.

Algorithm 2: increment nearest neighbor query

Input: query user r_0 and his current location *loc*, the anonymous zone radius appointed by the user *s*, $W_K \leftarrow$ max heap established according to the query result and rank of the user distance, supply space $\tau \leftarrow 0$, demand space $\gamma \leftarrow W_K$

Output: W_K

The anchor point $r_0.anchor$ is applied to launch the increment nearest neighbor query to the location service provider

while $\gamma + dist(r_0, r_0.anchor) > \tau$ and $\tau < r_0.s$

for each point *p* of the response packet *S* received from the location service supplier

$\tau \leftarrow dist(p, r_0.anchor)$

if $dist(p, r_0.loc) < \gamma$ then

In W_K, *p* and $dist(p, r_0.loc)$ shall be updated

$\gamma \leftarrow W_K$ distance from the top heap elements

In algorithm 2, the query user shall maintain the max heap W_K established according to the increment query return result and user distance $dist(p, r_0.loc)$, and it is applied for recording the l nearest neighbor in the road network, and he demand space γ is the distance from the top heap elements. The user may apply the anchor point $r_0.anchor$ to send the nearest neighbor query, and receive the result *p* constantly. The $dist(p, r_0.anchor)$ is applied for updating the supply space τ of the user, and then, it shall judge if the distance $dist(p, r_0.x)$ between the user and *p* is smaller than γ, if it is smaller than γ, *p* and $dist(p, r_0.loc)$ shall be applied to update the W_K. The distance of the top heap elements from W_K is used to update the γ, while $\gamma + dist(r_0, r_0.anchor) < \tau$, and $\tau > r_0.s$ stands for the complete coverage of supply space on the demand space and the minimum privacy region appointed by the user. At this moment, the user has already gained $r_0.l$ nearest neighbor query, and ended the increment nearest neighbor query.

In algorithm 2, location *k*-anonymity can guarantee that the risk of location disclosure is lower than 1/*k*. In this algorithm, since the number of appointed tree edge is *l* and *l*>=*k*, which guarantees that the risk is lower than 1/*l*; the minimum region s is set by the user freely, which improves the degree of participation. As for the service quality, the increment nearest neighbor query is a kind of accurate query method [8], which guarantees that the algorithm protects the location privacy of mobile user without at the cost of sacrificing the service quality.

4. Experiment and Result Analysis

4.1. Comparison Algorithm

The algorithm of this paper is realized with Java, recorded as algorithm a, and it runs in Windows XP with E5800 3.2GHz processor and 2G internal storage. The algorithm of this paper is compared to the algorithm proposed in reference [11] (recorded as algorithm b). The algorithm of reference [11] realizes the location privacy protection of the simple and complicated road according to the hiding ring and hiding forest, but it is based on the central server framework.

4.2. Experiment Data and Parameters

In this paper, the simulation data generated by the ThomasBrinkhoff road network data builder [12] is employed. The experiment default parameters are: anonymous parameter *k*=3, and the increment at each time is 3, the privacy protection zone radius *s*=1000m, and the anonymous location shall include at least *1*=3 sections, and the increment at each time is 3. Besides, other experimental parameters of the algorithm proposed in reference [11] adopt the default value.

4.3. Experiment Measuring Standard

The two algorithms are compared with the anonymous success rate, average query execution time, average candidate result size, etc. in which, the anonymous success rate reflects the percentage of the message of successful anonymity and quests sent by the user; the average query execution time refers to the time cost by the server for finishing the query of user, and it is used to measure the execution efficiency of algorithm; the average candidate result size reflects the average candidate result returned by the server to the location anonymity device after the query of the anonymous location, and it is applied for measuring the communication cost between the location server and location anonymity device.

4.4. Experimental Result Analysis

(1) Anonymous success rate. It can be seen from Fig. 2 (a) that with the increase of k and l, the difficulty of looking for the largest boundary tree with the two algorithms increases, and the anonymity success rate decline accordingly. When the k and l reaches the maximum, the anonymity success rate of the two algorithms is low. Since the two algorithms mainly carry out the location anonymity by finding out the largest boundary tree, the anonymity success rate is similar.

(2) Average query execution time. It can be seen from Fig. 2 (b) that with the increase of k and l, the average query time of the two algorithm increases gradually, suggesting that with the increase of anonymous section, the number of users also increases accordingly, and the query time also increases. In this paper, the centerless server framework of virtual user group is employed, and the computing cost and communication cost of the location server declines accordingly, reflecting the advantages of algorithm.

(3) Average candidate result size. It can be seen from Figure 2 (c) that with the increase of k and l, the average candidate result of the two algorithms increases, for the quantity of sections needing processing increases, which may result in the increase of communication cost. However, the communication cost of the algorithm in this paper is relatively small.

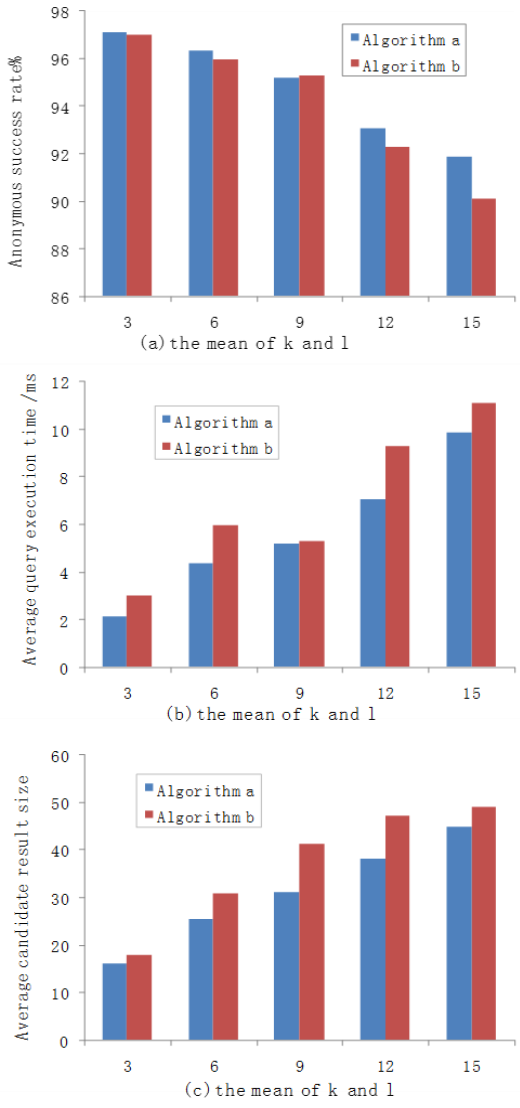

Figure 2. Experimental Result

5. Conclusion

In order to avoid the location service-based location privacy disclosure in the road network, virtual user group is adopted to realize the k-anonymity of user location and the *1*-diversity of sections proposed in reference [10]. Since the accurate increment nearest neighbor query is employed, it can guarantee the service quality. In addition, the virtual user group is a kind of non-central server framework, and it can reduce the communication cost effectively and avoid the disadvantages of the central server framework.

Acknowledgements

This work was supported by funds from Universities Key Fund of Anhui Province for Young Talents of China under Grant 2013SQRL082ZD, Natural Science Research Universities Key Project of Anhui Province of China under Grant KJ2014A256 and 2016 Anhui provincial colleges and universities outstanding young talent support program key projects.

References

[1] M. Gruteser, D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking[C]"//Proceedings of the 1st international conference on Mobile systems, applications and services. ACM, 2003: 31-42.
[2] B. Gedik , L. Liu, "A customizable k-anonymity model for protecting location privacy[J]." 2004.
[3] M F Mokbel , C Y Chow, W G Aref. The new Casper: query processing for location services without compromising privacy[C]//Proceedings of the 32nd international conference on Very large data bases. VLDB Endowment, 2006: 763-774.
[4] B. Gedik, L. Liu. "Protecting location privacy with personalized k-anonymity: Architecture and algorithms [J]". Mobile Computing, IEEE Transactions on, 2008, 7(1): 1-18.
[5] C Y Chow, M F Mokbel, X Liu. "A peer-to-peer spatial cloaking algorithm for anonymous location-based service[C]"//Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems. ACM, 2006: 171-178.
[6] G. Ghinita, P. Kalnis , S. Skiadopoulos . "PRIVE: anonymous location-based queries in distributed mobile systems[C]"//Proceedings of the 16th international conference on World Wide Web. ACM, 2007: 371-380.
[7] A. Solanas, A. Martínez-Ballesté A. "A TTP-free protocol for location privacy in location-based services [J]". Computer Communications, 2008, 31(6): 1181-1191.
[8] M L Yiu,C S Jensen, X Huang , et al. "Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services[C]"//Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on. IEEE, 2008: 366-375.
[9] Y Huang , Z Huo, X F. Meng . "Coprivacy: A collaborative location privacy-preserving method without cloaking region [J]". Jisuanji Xuebao(Chinese Journal of Computers), 2011, 34(10): 1976-1985.
[10] T Wang, L. Liu, "Privacy-aware mobile services over road networks [J]". Proceedings of the VLDB Endowment, 2009, 2(1): 1042-1053.
[11] J. Xue, X Y Liu, X C Yang , et al. "A location privacy preserving approach on road network[J]". Jisuanji Xuebao(Chinese Journal of Computers), 2011, 34(5): 865-878.

Author

Chen Wen, he is an Associate Professor in the School of Mathematics and Computer Science, Tongling College, Tongling, P.R.China. He holds a master degree in Computer Science and Technology from the Anhui University, Anhui, P.R.China. His previous research areas include privacy preserving.

