ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Network Security using a Mobility-Aware location Cloaking Technique

C.Anuradha

Assistant Professor, Department of Computer Science, Bharath University, Chennai,TamilNadu, India

ABSTRACT: In location-based services, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. To protect location privacy, one typical approach is to cloak user locations into spatial regions based on user-specified privacy requirements, and to transform location-based queries into region-based queries. We shall focus on the privacy aspects of using location information in pervasive computing applications. In this paper, we identify and address three new issues concerning this location cloaking approach. First, we study the representation of cloaking regions and show that a circular region generally leads to a small result size for region-based queries. Second, we develop a mobility-aware location cloaking technique to resist trace analysis attacks. Finally, we develop an efficient polynomial algorithm for evaluating circular-region-based kNN queries.

KEYWORDS: Location-based services, location privacy, query processing, mobile computing.

I. INTRODUCTION

LOCATION-BASED services (LBS) are emerging as a major application of mobile geospatial technologies. In LBS, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. Spatial range queries and k-nearest-neighbor (kNN) queries are two types of the most commonly used queries in LBS. The Global Internet Liberty Campaign[3] has produced an extensive report that discusses personal privacy at length and identifies four broad categories: information privacy, bodily privacy, privacy of communications, and territorial privacy.

This article concentrates on location privacy, a particular type of information privacy that we define as the ability to prevent other parties from learning one's current or past location. Until recently, the very concept of location privacy was unknown: people did not usually have access to reliable and timely information about the exact location of others, and therefore most people could see no privacy implications in revealing their location, except in special circumstances. When location systems track users automatically on an ongoing basis, they generate an enormous amount of potentially sensitive information. Privacy of location information is about controlling access to this information. We do not necessarily want to stop all access—because some applications can use this information to provide useful services—but we want to be in control. In this paper, we identify and address three new issues concerning the location cloaking approach. We first show that the representation of a cloaking region has an impact on the result superset size of the region-based query. In general, a small result superset is preferred for saving the cost of data transmission and reducing the workload of the result refinement process (especially if this process is implemented on the mobile client). Our findings indicate that, given a privacy requirement, representing the cloaking region with a circle generally leads to a smaller result superset than using other shapes.

Second, we consider the location-cloaking problem for continuous LBS queries. In such scenarios, trace analysis attacks are possible by linking historical cloaking regions with user mobility patterns. If the LBS server somehow learns the user's maximum possible moving speed v_m, the server can draw a region R^e (the shaded area in Fig. 1b) expanded from the

DOI: 10.15680/IJIRSET.2014.0311088

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

last cloaking region R based on vm and the interval t between the two queries. The server is then able to infer that the user must be located in the intersection area of R^e and R^0, which degrades the quality of location cloaking and may fail to meet the expected privacy requirement. The cloaking quality will further deteriorate with the analysis of more successive queries and cloaking regions.

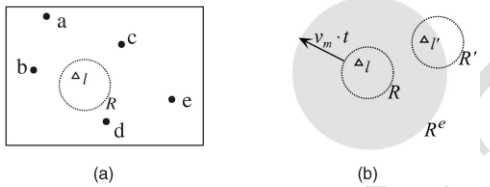


Figure1.Dynamic location cloaking. (a) Location cloaking. (b) Isolated cloaking.

To address this issue, we develop a mobility-aware location cloaking technique that resists trace analysis attacks. Given that the server observes a cloaking region together with any series of historical cloaking regions, our proposed technique makes equal the derivable probability that the user will be located at any one point within the cloaking region. To achieve this, we leverage the probability theory to control the generation of cloaking regions and design two cloaking algorithms, namely MaxAccu_Cloak and MinComm_Cloak, based on different performance objectives. MaxAccu_Cloak is designed to maximize the accuracy of query results, while MinComm_Cloak, attempts to reduce the network communication cost. Finally, we investigate how to evaluate efficiently circular-region-based spatial queries on the LBS server. While the evaluation of circular-region-based range queries is straightforward, we develop an efficient $O(kM^3)$ algorithm for evaluating circular-region-based kNN queries, where M is the cardinality of the spatial object set. In addition, we present two query-processing modes, namely bulk and progressive, which return query results either all at once or in an incremental manner.

II. RELATED WORK

Most existing approaches utilize a centralized anonymizer, a trusted server that acts as an intermediate tier between the issuers and LBS server. Gruteser and Grunwald[2] introduced location privacy based on k-anonymity that a trusted "location anonymizer" clocks a user's location by subdividing space into quadrant becomes the cloaked area. Bamba[1] described the privacy grid, which adds the l-diversity property to an already considered k-anonymity one. Location privacy protection. There are two main approaches to protecting location privacy in LBS. The first approach relies on a trusted LBS server to restrict access to location data based on rule-based policies [3], [4]. The second approach runs a trustworthy agent between the client and the LBS server. Every time the user makes a location-based query, the agent anonymizes the user identity and/or location before forwarding the query to the LBS server [5], [2].

Our study is under the framework of the second approach. Early studies on location privacy protection considered object tracking applications, where a proxy server is employed to collect exact locations from moving clients and to anonymize location data through depersonalization before release. In [4], once a client enters a predefined zone, its identity is mixed with all other clients in the same zone. It appears that this idea can be extended to deal with trace analysis attacks by associating each LBS request with a different pseudonym. Unfortunately, this approach may not be effective because historical user locations are highly correlative and, hence, they could be relinked using trajectory tracking methods (e.g., multitarget tracking [6]) even without knowing any identity [7]. In this paper, we investigate the location cloaking problem for continuous LBS queries. In particular, we focus on trace analysis attacks and propose a new mobility-aware cloaking

DOI: 10.15680/IJIRSET.2014.0311088

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

technique to resist them.Spatial query processing - A large body of research has investigated spatial query processing, in particular kNN queries. Most kNN query algorithms have focused on disk access methods based on R-tree-like index structures [8]. The branch-and-bound approach is often employed in query evaluation to traverse the index and prune search space. Various query evaluation algorithms differ in terms of the visiting order of index nodes and the metric used to prune search space [9]. Whereas the previous studies investigated the kNN problem for a location point or a line segment only, our recent work has developed an evaluation strategy for rectangular-region-based kNN queries that retrieve the k-nearest neighbors of all possible location points in a rectangular region [10]. We remark that the strategy developed in [10] is based on the fact that the perimeter of a rectangle can be decomposed into a set of straight-line segments. But because such decomposition is infeasible for a circle, the strategy of [10] cannot be extended to evaluate circular-region-based kNN queries. In another related work [11], Cheng et al. developed algorithms for evaluating probabilistic queries over imprecise object locations. In contrast, we are interested in using imprecise locations to retrieve result supersets through region-based spatial queries. Parallel to our work, Mokbel et al. [12] and Kalnis et al. [13] have investigated both the location cloaking and query processing problems.

But our work differs from theirs in several respects. First, like other previous studies [2], the location cloaking algorithms in [12] and [13] account for snapshot user locations only. Neither of them considers continuous queries and trace analysis attacks. In contrast, we focus on location cloaking for protecting against trace analysis attacks for continuous queries. Second, Kalnis et al. [13] and Mokbel et al. [14][15] did not study the issue of how to represent a cloaking region. In this paper, we show that a circular cloaking region generally leads to a small result superset size and, thus, we focus on query processing algorithms for circular regions. Finally, Mokbel et al. [16] investigated bulk query processing for rectangular regions only. Though Kalnis et al. [17] developed a bulk processing algorithm for circular-region-basedkNN queries, the algorithm has an exponential time complexity of $O(M^k)$, where M is the cardinality of the spatial object set. In this paper, we propose a polynomial $O(kM^3)$ algorithm for circular-region-based kNN queries. Furthermore, we develop a novel progressive query-processing algorithm, which is favorable to slow mobile networks.[18-20]

III. SYSTEM MODEL AND PRIVACY METRICS

A. System Model

The model for spatial cloaking can be defined in-terms of its main actors a depicted in figure.

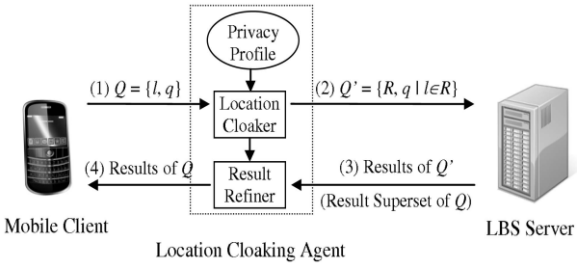


Figure. 2. System architecture.

1) Collaborative peers: It is assumed that a large number of LBS users (i.e. peers) who carry mobile devices with embedded positioning capabilities, and can establish communication network with any other device in the system through a base station, thus it is possible for a LBS initiator collaborating on a cloak area with k-1 peers for location privacy. In addition, any peer refuses to expose its location to others.

2) Ad-hoc network: it is assumed that a peer is able to build an ad-hoc network with other peers or to join an existing one. An ad-hoc network is created on the fly when peers have to exchange information with other peers in order to perform a

DOI: 10.15680/IJIRSET.2014.0311088

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

variety of tasks, so that, peers can enter the network at any time and leave quickly. In some developed countries (eg. Japan) there have already promoted mobile phones which equipped with positioning system and ad-hoc networking capability.

3) LBS Server: A LBS server plays the role of spatial data maintainers and spatial query processors, it is required to support the Nearest Neighbor (NN) queries of regions as opposed to points. Intuitively, the nearest neighbor of a region is the entire data object inside the region and plus the NN of every point in perimeter of the region. However the provider may not be trusted, users do not want to share their location with it.

As the architecture shown above, first of all, a mobile user initiates the LBS, searching k-1 companions and collaborating to form a cloak area, which covers k peers according to a certain degree of k anonymity, and these peers exchange information through an ad-hoc network. Furthermore, the initiator randomly selects a peer in the group as an agent, who sends a query message with location information on behalf of the initiator to LBS server. Upon this request, the LBS server seeks the desired information in its database and returns appropriate answers to initiator through the agent, finally the initiator selects a satisfied answer. Limited to the length, this paper mainly discusses the process of forming cloak area for location privacy.

B. The Process Of Spatial Cloaking

Our spatial cloaking protocol is based on the computation of the left-up and right-bottom of a minimum rectangle area that covers LBS initiator and its k-1 companions, moreover, without direct transmission of user's location. The security required by users can be mainly defined in terms of the number of companions k amongst which they want to be hidden, and the minimum desired area A_{min} that covers them. The larger the value of k and A_{min}, the more strict privacy requirement a user need, consequently the QoS reduction of LBS.

Definition 1 LU ($long_{min}$,lat_{min}): the coordinate of the left-up point of the cloaked area, $long_{min}$ and lat_{min} stand for the minimum longitude and latitude of the LBS initiator and its companions coordinate respectively, this paper used LU for brevity.

Definition 2 RB(longmax, latmax): the coordinate of the right-bottom point of the cloaked area, $long_{max}$ and lat_{max} stand for the maximum longitude and latitude of the LBS initiator and its campanions coordinate respectively, this paper used RB for brevity.

Definition 3 A_{min}: the minimum accepted area A_{min} that covers k peers, which was specified by initiator.
Definition 4 Tuple (LU, RB): the data structure that described the cloak area, this paper used Tuple for brevity.

IV. PROPOSED APPROACH

Ours is an approach to provide location privacy solution satisfying k-anonymity along with s-proximity using a location anonymizer. A thorough survey of literature reveals that lots of works have been done to deal with location privacy but none has proposed the inclusion of parameter like s-proximity.

Most of the location-privacy preservation frameworks use Location Anonymizer (LA) to meet the requester's k-anonymity requirement by providing a spatial region namely the Cloaked Region (CR) where the requester is indistinguishable from k-1 other request issuers.

DOI: 10.15680/IJIRSET.2014.0311088

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

(a) User selects her preferred services

V. EVALUATION

We have implemented a prototype version of our proposed system. The modules of context aware location anonymizer were developed on a machine with hardware configuration Intel Processor 1.7 Ghz, 1.5 GB Memory and Windows Vista as OS. The spatial data used in the evaluation were taken from North American data set [1] consisted of 15K points which were used by clients and the LA as user points in 2D space. Figure 4 depicts how the client module works. The initialization step consisting of the user registration tasks are shown in Figure 4 (a) (b)

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

(c) User submits query

(d) Reply from LA with POI list

. The next three figures display how a registered user submits location based query to the LA and gets reply subsequently. We have evaluated performance of our system and the findings are summarized in Figure 5. Performance of the system was measured in terms of the metrics: Query Success Rate, CR Construction Time and CR Size (absolute /relative).

The percentage of time a user was provided with her required service was denoted by Query Success Rate. Other

DOI: 10.15680/IJIRSET.2014.0311088

ISSN: 2319-8753

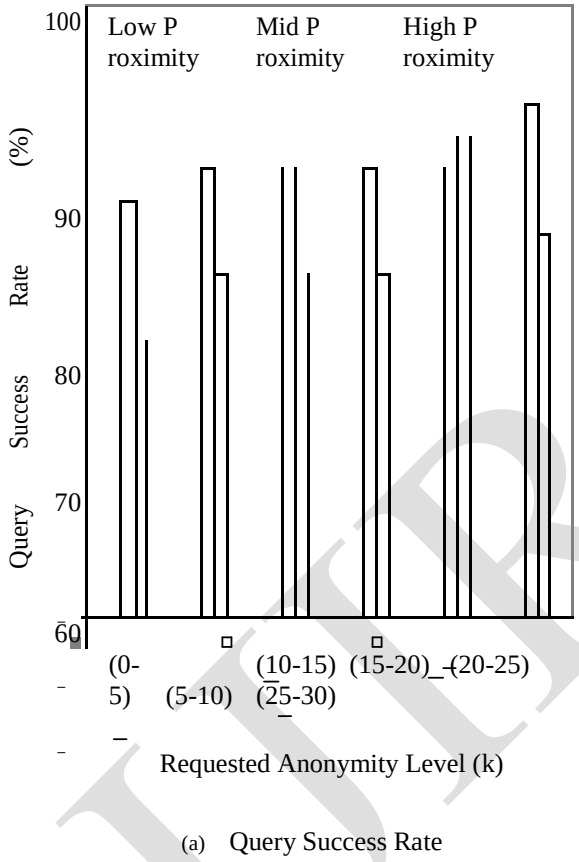
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

two metrics measured the time required for constructing a cloaked region and the size of the constructed CR. As Figure 5 (a) depicts, we achieved overall high success rate though it reduced a bit with higher proximity requirement.

The graphs in Figure 5 (b) demonstrates that the construction time and size of a cloaked region increases with higher proximity level. These parameters also show higher values for increased number of subscribers.Performance of our prototype implementation was compared with couple of other existing systems (NNC [13], IC [2], Casper [12], HC [14]) and it is found that our approach yields cloaked region with a bit large size (shown in Figure 5 (c)) which is quite acceptable considering the enhanced level of privacy it offers compared to the existing frameworks.



(a) Query Success Rate

Performance of the system is acceptable as compared to existing systems. The system implements both s-proximity and k-anonymity, which is a novel approach capable of safeguarding the attacks presented in this paper.

(b)Variations of CR construction Time according to requested anonymity level

From the experimental facts it is evident that our proposed framework with a context aware location anonymizer is really feasible to be implemented in real world LBS system. proposed framework with a context aware location anonymizer is really feasible to be implemented in real world LBS system.

ISSN: 2319-8753

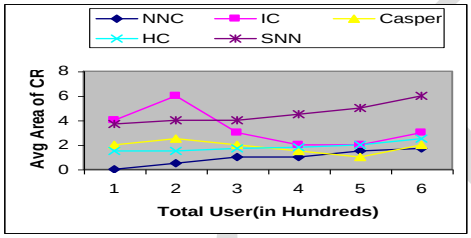
International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

VI.CONCLUSION AND FUTURE WORK

This paper has presented a complete study on processing privacy-conscious location-based queries in mobile environments. We have studied the representation of cloaking regions and showed that a circular region generally leads to a small result superset. We have developed a mobility-aware location cloaking technique to resist trace analysis attacks. Two cloaking algorithms, namely MaxAccu_Cloak and Min- Comm_Cloak, have been designed to favor different performance objectives. Experimental results show that the mobility-aware cloaking algorithms are robust against trace analysis attacks without compromising much on query latency or communication cost. MaxAccu_Cloak gets a 100 percent query accuracy while MinComm_Cloak achieves a good balance between communication cost and query accuracy. It is also shown that the progressive query-processing algorithm generally achieves a shorter user perceived response time than the bulk algorithm.



As for future work, we are going to extend the mobility aware location cloaking technique to other privacy metrics (e.g., the k-anonymity model and the l-diversity model) and road networks. We are also interested in investigating mobility-aware peer-to-peer cloaking techniques. We can also include the study of different attack scenarios (e.g. some noise introduced through the computation in chain), technique improvement in searching k-1 companions and effective method of representing the cloak area.

REFERENCES

1. B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting Anonymous Location Queries in Mobile Environments with Privacygrid," Proc. Int'l World Wide Web Conf. (WWW), 2008.
2. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "High data rate for coherent optical wired communication using DSP", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) 4772-4776.
3. M. Gruteser and D. Grunwald, "Anonymous Usage of Location- Based Services through Spatial and Temporal Cloaking," Proc. ACM MobiSys, 2003
4. Selva Kumar S., Ram Krishna Rao M., Deepak Kumar R., Panwar S., Prasad C.S., "Biocontrol by plant growth promoting rhizobacteria against black scurf and stem canker disease of potato caused by Rhizoctonia solani", Archives of Phytopathology and Plant Protection, ISSN : 0323-5408, 46(4) (2013) pp.487-502.
5. G. Myles, A. Friday, and N. Davies, "Preserving Privacy in Environments with Location-Based Applications," IEEE Pervasive Computing, vol. 2, no. 1, pp. 56-64, Jan.-Mar. 2003.
6. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Optical ring architecture performance evaluation using ordinary receiver", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4742-4747.
7. M. Youssef, V. Atluri, and N.R. Adam, "Preserving Mobile Customer Privacy: An Access Control System for Moving Objects and Custom Profiles," Proc. Sixth Int'l Conf. Mobile Data Management (MDM), 2005.
8. Subha Palaneeswari M., Abraham Sam Rajan P.M., Silambanan S., Jothimalar, "Blood lead in end-stage renal disease (ESRD) patients who were on maintainence haemodialysis", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(10) (2012) pp.1633-1635.
9. B.Vamsi Krishna, A New Technique for Elimination of Harmonics Using Three Phase Shunt Active Filter, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 5596-5602, Vol. 2, Issue 11, November 2013
10. A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing," IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, Jan.-Mar. 2003.

DOI: 10.15680/IJIRSET.2014.0311088

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

11. Udayakumar R., Khanaa V., Kaliyamurthie K.P., "Performance analysis of resilient ftth architecture with protection mechanism", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4737-4741
12. D. Reid, "An Algorithm for Tracking Multiple Targets," IEEE Trans. Automatic Control, vol. 24, no. 6, pp. 843-854, Dec. 1979.
13. A.Geetha, Universal Asynchronous Receiver / Transmitter (UART) Design for Hand Held Mobile Devices, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN: 2231-5381, pp 25-26, Volume 3 Issue 1 No1 – January 2012.
14. T. Xu and Y. Cai, "Exploring Historical Location Data for Anonymity Preservation in Location-Based Services," Proc. IEEE INFOCOM, 2008.
15. A. Guttman, "R-Trees: A Dynamic Index Structure for Spatial Searching," Proc. ACM SIGMOD, 1984.
16. G.R. Hjaltason and H. Samet, "Distance Browsing in Spatial Databases," ACM Trans. Database Systems, vol. 24, no. 2, pp. 265- 318, 1999.
17. H. Hu and D. Lee, "Range Nearest Neighbor Queries," IEEE Trans. Knowledge and Data Eng., vol. 18, no. 1, pp. 78-91, Jan. 2006.
18. A.Geetha, Face Recognition Using OPENCL, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering , ISSN (Print) : 2320 – 3765, pp- 7148-7151, Vol. 3, Issue 2, Febuary 2014.
19. B.Mehala, Mrs.Anitha Sampath Kumar, Design and Implementation of Resonant Circuit Based On Half-Bridge Boost Rectifier with Output Voltage Balance Control, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 9370-9378, Vol. 3, Issue 5, May 2014
20. B.Vamsi Krishna, Starting Inrush Current Control of Three-Phase Induction Motors for Dispersed Generating Systems, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Online): 2278 – 8875,pp 6411-6422, Vol. 2, Issue 12, December 2013