Improving Efficiency and Privacy of Moving Objects

[1]D. Anil Kumar, [2]M. RajaBabu
[1,2]Dept. of CSE, Aditya Engineering College, Aditya Nagar, Surampalem, AP, India

Abstract
Object databases have gained much interest due to the advances in mobile communications and positioning technologies. To provide security to moving object need monitoring . Monitoring moving objects have two fundamentals issues like efficiency and privacy. This paper proposes an efficient algorithm for finding good anonymization group for given objects (MOB) with respect to its Quasi-Identifier (QID) and dynamic query updation. To address the efficiency and privacy issues we are using a new technique which updates the query of the mOB in the base stations automatically. Furthermore , by using the location management method we are solving the issues of location updating.

Keywords
Privacy, Anonymity, Location Based Services, Safe Region

I. Introduction

Location awareness, the ability to determine geographical position, is an emerging technology with both significant benefits and important privacy implications for users of mobile devices. We are on the cusp of a new era in technology where the location of computing and communications devices can be determined accurately and inexpensively. Now-a-days almost all the people are using location aware devices, e.g., GPS-enabled cell phones and PDA's location sensors and active RFID tags. This enables monitoring of moving objects and real-time analysis of their motion patterns, as well as the collection of the traces left by these moving objects To provide secrecy to the moving object location we need to update the location information along with the query of that moving object. We can do the updation of the moving object with the help of the location management method. Time-based Location Management method forms two phases: Location Update (LU) and paging (P).

When we are working with moving objects location information we need to monitor moving objects time to time so that location information should be updated and can provide security to the moving object. Existing works has problem with dynamic query update, this paper overcomes that problem by using the dynamic query updation algorithm and location management method.

A mobile informs the Base Station (BS) of its location during a Location Update operation at the same time BS will get the query information from the MOB.

The system stores this information of a Mobile Terminal (MT) when the query is set and in exchange it sends the code of the query generated by the system with the MT call. There are very few studies on continuous query monitoring are focused on location updates. Two commonly used updating approaches are periodic update and deviation update. We are using the quasi-identifier for providing good anonymity to the moving objects. It is very likely that various moving objects have different quasi-identifiers and this should be taken into account in modeling adversarial knowledge.

Hence the concept of quasi-identifier must be modeled subjectively, on an individual basis. Fig. 1(a) shows a moving object database. Each row represents the trajectory of a Moving Object (MOB) and shows the position of the MOB at different times, in a rectangular grid. The original identities (say I1, I2, I3) of the individuals have been suppressed and have been replaced by MOB ids O1, O2, O3. For the three individuals I1, I2 and I3, a possible scenario is that an adversary knows the location of I1 at time point t1, and that of I2 and I3 at t2. In this paper, we study the problem of privacy-preserving publishing of a moving objects database. Our goal is to anonymize the trajectories so that no MOB can be re-identified by matching its quasi-identifier with the published dataset. The main issue in anonymizing MOB data is that, due to the fact that different objects may have different QIDs, anonymization groups associated with different objects may not be disjoint, as illustrated below.

Example 1: Consider the trajectories in Figure 1(a) and illustrated in Figure 1(c). Let k = 2 and QID(O1) = {t1}, QID(O2) = QID(O3) = {t2}. Intuitively the best (w.r.t. information loss) anonymization group for O1 w.r.t. its QID {t1} is AS(O1) = {O1,O2}. This is illustrated in Figure 1(c) with a dark rectangle. This means in the anonymized database we assign the region [(1, 2), (2, 3)] to O1 and O2 at time t1. The best anonymization group for O2 as well as for O3 w.r.t. their QID {t2} is {O2, O3}. Thus, in the anonymized database, O2 and O3 will both be assigned to the common region [(2, 6), (3, 7)] (the second dark rectangle) at time t2. Clearly, the anonymization groups of O1 and O2 overlap. Due to this fact providing a robust and sound definition of k-anonymity in the case of MOD is challenging. The most obvious way of defining k-anonymity is to say that a given object must be indistinguishable from all the objects in its own anonymization group for each timestamp in its own QID. According to this definition the database in Figure 1(b) is 2- anonymous and thus "safe". This obvious definition of k-anonymity still suffers privacy breaches. Indeed, due the fact that anonymization groups may not be disjoint, it is possible that by combining overlapping anonymization groups, some moving objects may be uniquely identified, as explained next. Recall the previous example. There, I1 and I2 are in the same anonymization group (i.e., have the same generalized location) at time point t1 (i.e., the QID of I1), while I2 and I3 are in the same anonymization group at time point t2 (i.e., the QID of I2 and I3). However, when the adversary tries to map the three MOBs O1, O2, O3 to the three individuals I1, I2, I3, with the adversary knowledge of QID values of these three MOBs, he can infer that I1 must be mapped to either O1 or O2, while I2 (and I3) should be mapped to either O2 or O3. If I1 is mapped to O2, we cannot find a consistent assignment for I2, I3. As a result, the adversary can conclude that O1 must map to I1.

Thus, we need a more sophisticated definition of k-anonymity to avoid privacy breaches in the case of moving object databases.

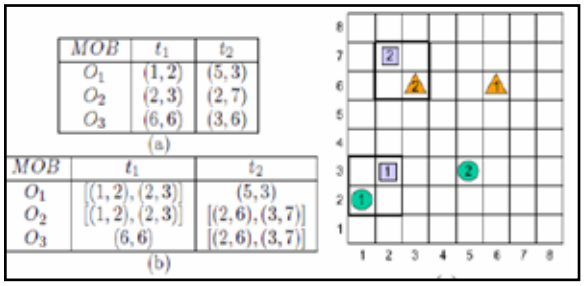

Fig 1: Example MOB Database (assuming QID(O1) = $\{t_1\}$, QID(O2) = QID(O3) = $\{t_2\}$): (a) original database; (b) a 2-nonymity scheme that is not safe, and (c) its graphical representation.

The theme of this paper is to update the query of MOB for preventing moving object from tracking to do so we have to monitor the moving object which needs to overcome the fundamental issues of monitoring [4].

II. Related Works

Existing work on preventing of patiotemporal moving objects location from tracking has been mainly conducted in the context of Location Based Services (LBS). In this context a trusted server is usually in charge of handling users' requests and passing them on the service providers, and the general goal is to provide the service on-the-fly without threatening the anonymity of the user requiring the service. The trusted server uses spatial-cloaking (i.e., space generalization) to make the request sent from a user indistinguishable from k−1 other requests [11]. Based on this idea a system that supports different queries and various anonymization requirements was developed in [9-10]. Early work assumed a static data set and focused on efficient access methods (e.g., R-tree [12]) and query evaluation algorithms (e.g., [13-14]). Recently, a lot of attention has been paid to moving-object databases, where data objects or queries or both of of them move.

Assuming that object movement trajectories are known a priori, Saltenis et al. [15] proposed the Time-Parameterized R-tree (TPR-tree) for indexing moving objects, where the location of a moving object is represented by a linear function of time. Benetis et al. [16] developed query evaluation algorithms for NN and reverse NN search based on the TPR-tree. Tao et al. [17] optimized the performance of the TPR-tree and extended it to the TPR_-tree. Chon et al. [18] studied range and kNN queries based on a grid model. Patel et al. [19] proposed a novel index structure called STRIPES using a dual transformation technique. The work on monitoring continuous spatial queries can be classified into two categories. The first category assumes that the movement rajectories are known. Continuous kNNmonitoring has been investigated for moving queries over stationary objects [20] and linearly moving objects [21-22]. Iwerks et al. [21] extended to monitor distance semijoins for two linearly moving data sets [23]. However, as pointed out in [24], the known-trajectory assumption does not hold for many application scenarios (e.g., the velocity of a car changes frequently on road). The second category does not make any assumption on object movement patterns. Xu et al. [25] and Zhang et al. [26] suggested returning to the client both the query result and its validity scope where the result remains the same. As such, the query is reevaluated only when the query exits the validity scope. However, their solutions work for stationary objects only. For continuous monitoring of moving objects, the prevailing approach is periodic reevaluation of queries [27-30]. Prabhakar et al. [29] proposed the Q-index, which indexes queries using an R-tree-like structure. At each evaluation step, only those objects that have moved since the previous evaluation step are evaluated on the Q-index. While this study is limited to range queries, Mokbel et al. [28] proposed a scalable incremental hash-based algorithm (SINA) for range and kNN queries. SINA indexes both queries and objects, and achieves scalability by employing shared execution and incremental evaluation of continuous queries [28, 31].

Kalashnikov et al. and Yu et al. suggested grid-based in memory structures for object and query indexes to speed up reevaluation process of range queries [32] and kNN queries [30]. Access methods to support frequent location updates of moving objects have also been investigated [27, 33]. Our study falls into this category but distinguishes itself from existing studies with a comprehensive framework focusing on location update. Uncertainty and privacy issues have been recently studied in moving object monitoring. To protect location privacy, various cloaking or anonymizing techniques have been proposed to hide the client's actual location. Among them are the spatiotemporal cloaking [34], the Clique-Cloak [35-36], the Casper anonymizer [37], hilbASR [38-39], and peer-to-peer cloaking [40-41].

In spatiotemporal cloaking, or each location update, the server divides the space recursively in a quad-tree-like format till a suitable subspace is found to cloak the updated location. The CliqueCloak algorithm constructs a clique graph to combine some clients who can share the same cloaked spatial area. The Casper anonymizer is associated with a query processor to ensure that the anonymized area returns the same query result as the actual location. In hilbASR, all user locations are sorted by Hilbert space-filling curve ordering, and then, every k users are grouped together in this order. Besides, location cloaking, pseudonym, dummy, and transformation were also proposed for privacy preservation. Pseudonym decouples the mapping between the user identity and the location so that an untrusted server only receives the location without the user identity [42-43]. Dummy generates fake user locations (called dummies) and mixes them together with the genuine user location into the request [44-46]. Transformation utilizes certain one-way spatial transformations (e.g., a space filling curve) to map the query space to another space and resolves query blindly in the transformed space [47].

As for location uncertainty, a common model for characterizing the uncertainty of an object is a closed region with a predefined probability distribution of this object in the region. Based on this probabilistic model, query processing and indexing algorithms have been proposed to evaluate probabilistic range queries [48], [37] and kNNqueries [49]. While in these studies, the objects are uncertain, the queries themselves are still certain. Chen and Cheng extended the probabilistic processing to more general cases where the queries are also uncertain [50]. Our study, on the other hand, addresses the continuous monitoring issue. By adopting the notion of "safe region," the frequency of query reevaluation on uncertain location information is reduced, and hence, the system efficiency and scalability are improved. Distributed approaches have been investigated to monitor continuous range queries [51-52] and continuous kNNqueries [53]. The main idea is to shift some load from the server to the mobile clients. Monitoring queries have also been studied for distributed Internet databases [54], data streams [55], and sensor databases [56]. However, these studies are not applicable to monitoring of moving objects, where a two-dimensional space is assumed.

A location update is used to inform the network of a mobile device's location. This requires the device to register its new location with the current base station, to allow the forwarding of incoming calls. Each location update is a costly exercise, involving the use of cellular network bandwidth and core network communication; including the modification of location databases [AMH+99]. A wide variety of schemes have hence been proposed to reduce the number of location update messages required by a device in a cellular network. Location update schemes are often partitioned into the categories of static and dynamic [BNIM95, AMH+99, WL00, ADM98]. Static schemes offer a lower level of cost reduction but reduced computational complexity. Dynamic schemes adjust location update frequency per user and are hence able to achieve better results, while requiring a higher degree of computational overhead. Dynamic location update schemes allow per-user parameterisation of the location update frequency.

These account for the dynamic behaviour of users and may result in lower location management costs than static schemes. Unlike static location management strategies, a location update may be performed from any cell in the network, taking into consideration the call arrival and mobility patterns of the user. Dynamic location update properties varies as per the schemes, the following are the schemes we have in:

- Threshold-based Scheme
- Time-based Scheme
- Movement-based Scheme
- Distance-based Scheme
- Profile based and adaptive

III. Methodology

A. Problem Definition

The existing system proposes that the server will not automatically update the Query of the Mobile Object (MO) as it is updating the location when the mobile is moving from one Base Station (BS) to the other. The Problem with the existing system is that the updation of MO query is not happening when the MO moves to the other BS's. In the proposed system we are introducing an algorithm along with the anonymity which will help the BS's to identify the query of the MO and provide security as per the query of MO.

B. Moving Object Concealment

A basic building block for devising any notion of anonymity is a notion of indistinguishability. Let D* be a distorted version of a MOD D. We say that two MOBs O, O′ are indistinguishable in D* at time t provided that D* (O, t) = D* (O′, t), i.e., both are assigned to the same region in D*. The most obvious way of defining k-anonymity is the following: a distorted version D* of a MOD D satisfies k-anonymity provided: for every MOB O

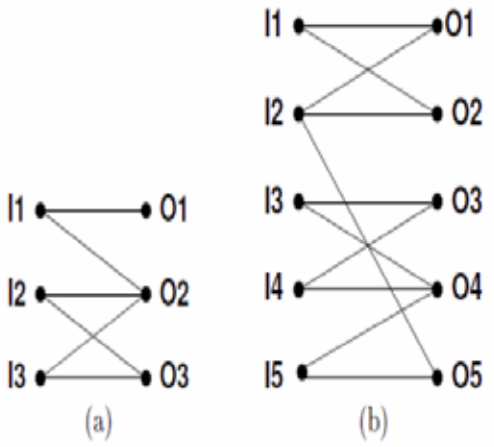

Fig 2: Attack graphs for different anonymization schemes: (a) for D* in Figure 1(b); (b) for a hypothetical database D* satisfying modified definition of k-anonymity.

everyI-node corresponding to an individual has at least k-neighbors, it does not have any restriction on the degree of the O-nodes. What if we required that in addition, every O-node must have degree at least k? Suppose we say that a distorted database is k-anonymous provided in the corresponding attack graph, every I-node as well as every O-node has degree ≥ k. Figure 2(b) shows a possible attack graph that satisfies this condition. In this graph, every I-node and every O-node has degree 2 or more. Yet, O5 can be successfully re-identified asI5 as follows. Suppose O5 is instead assigned to I2, to which it is adjacent as well.Then it is easy to see that no I-node can be assigned to one of O1,O2. Thus, the edge (I2,O5) cannot be a part of any perfect matching. Thus, this edge can be pruned, leaving I5 as the only I-node to which O5 can be assigned.

C. Definition 2(Attack Model)

The attacker first constructs an attack graph associated with the published distorted version of D and the known QIDs as described in

Definition1:

It repeats the following operation until there is no change to the graph:

- Identify an edge e that cannot be part of any perfect matching.
- Prune the edge e.

Next, we propose a notation of k-anonymity, which guarantees there exists a perfect matching for any arbitrary node in the attack graph.

D. Definition 2(K-Anonymity)

Let D be a MOD and D* its distorted version. Let G be the attack graph w.r.t.D, D*, given a set of QIDs for the MOBs in D. Then D* satisfies the k-anonymity condition provided: (i) every I- node in G has degree k or more; and (ii) G is symmetric, i.e., whenever G contains an edge (Ii,Oj), it also contains the edge (Ij ,Oi). An immediate observation is that in an attack graph that satisfies the above conditions, every O-node will have degree k or more as well. We call a distorted database D* k-anonymous if it satisfies Definition 3.

Dynamic Query updation algorithm

ALGORITHM

1. While receiving a request do
2. ifthe request is to register query q then
3. evaluate q;
4. generate unique query id;
5. compute its quarantine area and insert it into the query index;
6. return the result to application server;
7. return unique query id to the mobile terminal;
8. update the changed safe regions of objects and the Query updation through unique id;
9. else if the request is to deregister query q then
10. remove q from the query index;
11. else if the request is a location update from object then
12 determine the set of affected queries;
13. for each affected query q0 do
14. reevaluate q0;
15. update the results to the application server;
16. recomputed its quarantine area and update the query index;
17. update the safe region of p;

Algorithm for the automatic updation of Query and Location of MOB

The data i.e, request will be generated by the MT then the request will be carried to the server by the BS. In this scenario BS acts as an interface, query varies from user to user of the MT sometimes it may be about location, sometimes it may be about the privacy, the algorithm in Fig 3 explains that to process the query regarding privacy it processes two queries one is location and the another one is privacy, because to provide privacy to the MOB / MT the server should know its location or the BS it is connected to. The query processor in the server processes the query and generates query index, object index and unique id. Location update manages upadates the location every time when ever the object moves from one location to the other and sets the location safe region only

when the MOB moves out of the BS range. Unique id is send to the MOB/MT, whenever the object moves out of the range simultaneously along with the location updation the privacy will be provided to the MOB/MT.

IV. Conclusion

This paper proposes an algorithm for automatic privacy query updation along with the location updation process. This is the first technique which address about the issue of the autotmaticprivacy query updation. Furthermore, this algorithm is best in providing privacy automatically even when the mobile terminal moves to other BS. As for future work, we plan to work on multiple queries.

References

[1] Dr. RobertP.Minch,"Privacy Issues in Location – Aware Mobile Devices", Proceedings of the 37th Hawaii International Conference on System Sciences-2004.

[2] Toshihiko Sasama, Yasuto Nishii,"A location management mehtod for cellular networks", software, Telecommunications and Computer Networks, 2008.16th International Conference on 25-27 sept.

[3] Samir K.Shah, SirinTekinay, CemSaraydar,"Co-operative Location Update Algorithm For Mobiles In Next Generation Cellular Networks", High Performance Switching and Routing, 2004. IEEE 2004, Vol. 4.

[4] Haibo Hu, JianliangXu, Senior Member, IEEE, DikLun Lee,"PAM: An Efficient and Privacy – Aware Monitoring Framework for Continuously Moving Objects", IEEE Transaction on knowledge and Data Engineering, Vol. 22, No. 3, March 2010.

[5] C.S. Jensen, D. Lin, B.C. Ooi,"Query and Update Efficient B+-Tree Based Indexing of Moving Objects", Proc. Int'l Conf. Very Large Data Bases (VLDB), 2004.

[6] M.F. Mokbel, X. Xiong, W.G. Aref,"SINA: Scalable Incremental Processing of Continuous Queries in Spatio-Temporal Databases", Proc. ACM SIGMOD, 2004.

[7] S. Prabhakar, Y. Xia, D.V. Kalashnikov, W.G. Aref, S.E. Hambrusch,"Query Indexing and Velocity Constrained Indexing: Scalable Techniques for Continuous Queries on Moving Objects", IEEE Trans. Computers, Vol. 51, No. 10, pp. 1124-1140, Oct. 2002.

[8] X. Yu, K.Q. Pu, N. Koudas,"Monitoring k-Nearest Neighbor Queries over Moving Objects", Proc. IEEE Int'l Conf. Data Eng. (ICDE), 2005.

[9] A. Guttman,"R-Trees: A Dynamic Index Structure for Spatial Searching", Proc. ACM SIGMOD, 1984.

[10] Y. Tao, D. Papadias, J. Sun,"The TPR-Tree: An Optimized Spatio-Temporal Access Method for Predictive Queries", Proc. Int'l Conf. Very Large Data Bases (VLDB), 2003.

Mr. D.Anil Kumar is a student of Aditya Engineering College, Surampalem. Presently he is pursuing his M.Tech from this college and He received his graduation from JNTUK UNIVERSITY in the year 2009.

M. RajaBabu received the B.Tech degree from MVGR Engineering College,Vizianagaram in 2003. He completed M.Tech in Information Technology from JNT University,kakinada in 2010. He is having nearly 7 years of teaching experience. He is currently working as Associate Professor, Dept of C.S.E, Aditya Engineering College,Kakinada, Andhrapradesh, India. He is a member of SrinivasaRamanujan Research Forum (SRRF), Godavari Institute of Engineering and Technology (GIET), Rajahmundry. His research interest includes Image Processing and Pattern Recognition..He is a life member of Indian Science Congress Association.