Robust Query Processing For Privacy Deficient Location Based Service Provider

Manas Kumar Yogi
Asst. Prof. Dept. of CSE,Pragati Engineering College,Surampalem, India.

Darapu Uma
Asst. Prof. Dept. of CSE,Pragati Engineering College,Surampalem, India.

Abstract – Our proposed presents a distributed system which provides robustness up to a certain degree for privacy deficient location based service providers(LBSP's).The LBSP's facilitate spatial top-k query processing considering the point of interests(POI's) from a region with respect to highest ratings corresponding to specific POI attribute.

Index Terms – LBSP, POI, Query Processing, Freshness Value, Data Collector.

1. INTRODUCTION

In modern society all smart phones have internet access there by acquiring exact location with help of positioning software. For users who are new to a region it is convenient to access and share information regarding POI's like restaurants, hotels, grocery stores, coffee shops. Most of the LBSP's provide a location based query processing which have a drawbacks like limited datasets, POI reviews and multiple ratings for single POI by different LBSP's .sometimes even if the LBSP's are not malicious they may return query results under the effect of various type of attacks like submission of fake reviews for the same POI by the same attacker. This leads to unwise decisions made from the query results.

2. QUERY PROCESSING IN PROPOSED MECHANISM

Algorithm

Step 1: for an attribute 'A' calculate point of interest (POI_m) and freshness value λ_i in a $zone_a$ region.

Step2: for the same attribute 'A' calculate point of interest (POI_n) and freshness value λ_j in a $zone_b$ region.

Step 3: if (POI_m! =POI_n and λ_i>λ_j) for displacement in zone region then rating is verified to be correct. Otherwise go to step 4

Step 4: then the rating is leads to be malicious.

3. EXISTING SYSTEM ARCHITECTURE

In existing system data collector is assumed to be trusted while LBSP is untrusted.In our scheme we start with the notion data collector is untrusted and to make it authentic a suitable licensing measures are to be introduced. A simple licensing measure can be establishing the market value of the data collector.

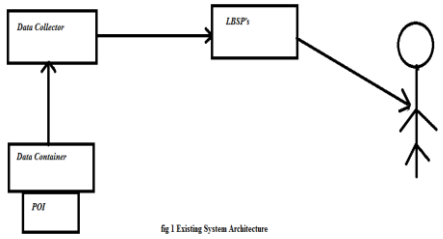

Figure 1 Existing System Architecture

In situation where the LBSP must return some query results even if it has no top-k POI satisfying the query significant communication overhead for a large query region occurs. To reduce the amount of information displayed to the user. Our scheme considers virtual zone which is aggregation of $zone_a$ and $zone_b$ .This scheme returns the largest attribute A's rating with respect to $zone_a$ $zone_b$

Advantages of proposed system

1. Privacy deficiency of LBSP's is reduced to a great extent by considering the freshness value λ.
2. The scheme we propose considers the creditability of reviewers and data collector.
3. Our scheme considers the reduction in computational cost as well as communicational costs.

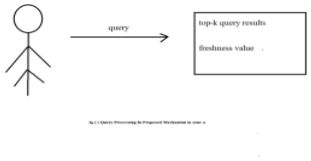

Figure 2.1.query processing in proposed mechanism in zone b

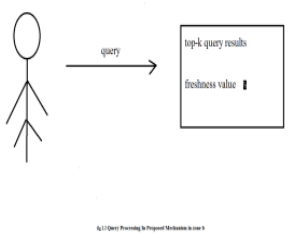

Fig 2.2.query processing in proposed mechanism in zone b

4. FUTURE WORK

In previous systems top-k queries are moved with the help of independent snapshots in a circular region of radius 5km.this causes computational overhead as well as LBSP's user overhead. We are extensively studying procedures to reduce this overhead using a hybrid scheme. The main consideration while reducing this overhead is deducting updated results from top-k POI's.

5. CONCLUSION

In this paper we have proposed robust top-k query processing for privacy deficient LBSP's using mechanisms which are less costly and effective. We have proposed a robust architecture which considers a metric called freshness value and creditability of reviewers, data collectors.

REFERENCES

[1] Beresford, F. Stajano, Mix Zones: User Privacy in Location-aware Services. In Proc. IEEE Workshop on Pervasive Computing and Communication Security (PerSec), pp. 127-131, IEEE, 2004.
[2] A. Beresford, F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46-55, 2003.
[3] C. Bettini, S. Jajodia, X.S. Wang, Time Granularities in Databases, Data Mining and Temporal Reasoning, Springer, 2000.
[4] C. Bettini, X. Wang, and S. Jajodia. Testing complex temporal relationships involving multiple granularities and its application to data mining, in Proc. Of ACM Symposium in Principles of Database Systems (PODS), ACM press, 1996.
[5] D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1(1): 65-75, 1988.
[6] D. Chaum, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24(2): 84-88, 1981.
[7] J. Cuellar, J. Morris, and D. Mulligan. Internet Engineering task force geopriv requirements. http://www.ietf.org/html.charters/geopriv-charter.html, 2002.