International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 2 – FEBRUARY 2016.

LOCATION BASED SERVICES BY USING RSASSOL ALGORITHM FOR TIME CONSUMPTION IN MOBILE COMPUTING

Mrs. K. Manohari, M.C.A, M.Phil[1] , Miss. S. Roobiya [2]

[1] *Assistant Professor, Department of Computer Science, Theivanai Ammal College for Women (Autonomous), Villupuram-645 401, India. Email Id:* ***manohema@gmail.com***

[2] *M.Phil Scholar, Department of Computer Science, Theivanai Ammal College for Women (Autonomous), Villupuram-645 401, India. Email Id:* ***rubisathik @gmail.com***

***Abstract*- This paper deals with the efficient approximation string search in large databases. In particular, we study range queries improved with a string similarity search in both Euclidean space and road networks. In Euclidean space, we propose an approximate solution, the Filter tree, which embeds user query and query server. The min-wise signature for an index node u maintains a brief representation of the union of filter tree from strings under the sub-tree of u. It is also discussed that how to estimate the selectivity of range query in large database in Euclidean space. For queries on road networks, we propose a novel exact method, RSASSOL, which is significantly, outperforms the baseline algorithm in practice. The RSASSOL combines the spatial queries and candidate points that prune away the unwanted candidate points. And thus, the privacy is experimented and controlled the system.**

Keywords: RSASSOL Algorithm, Road Networks, Euclidean distance, Filter Tree.

I. INTRODUCTION

Location-based services provide convenient information access for mobile users who can issue location-based snapshot or continuous queries to a database server at anytime and anywhere. Examples of snapshot queries include “where my nearest gas station is” and “what are the restaurants within one mile of my location”, while examples of continuous queries include “continuously report my nearest police car” and “continuously report the taxis within one mile of my car”. Although location-based services promise safety and convenience, they threaten the security and privacy of their customers. The use of LBS, however, can reveal much more about a person to potentially untrustworthy service providers than many people would be willing to disclose [1]. By tracking the requests of a person it is possible to build a movement profile which can reveal information about a user’s work (office location), medical records (visit to specialist clinics), political views (attending political events), etc.

To tackle the privacy threats in location-based services, several spatial cloaking algorithms have been proposed for preserving user location privacy The key idea of spatial cloaking algorithms is to blur the exact user location information into a spatial region that satisfies certain privacy requirements. Privacy requirements can be represented in terms of k-anonymity (i.e., a user location is indistinguishable among k users) and/or minimum spatial area (i.e., a user location is blurred into a region with a minimum size threshold). On the other hand, our proposed technique hides query contents from the LBS [2], and leaves no useful clues for determining the user’s current location. When a typical mobile phone accesses a third-party LBS provider through a wireless 3G data connection, we assume that it reveals only its identity and the query itself to the provider. Unavoidably, a mobile communications carrier is always aware of the user’s location based on the cell towers in contact, and so it must not collude with the LBS provider. Our assumption relies on the LBS provider not being integrated into the carrier’s infrastructure, such as a traffic reporting service using cell tower data that discovers a user’s location passively.

Our assumption is valid for the vast majority of LBS applications, which are unaffiliated with the carrier [3]; these include search portals, social applications, travel guides, and many other types. When communicating with such an application, the mobile user’s IP address is of no help in determining the user’s physical location, as it is dynamically assigned independent of location. Only a central gateway that is administered by the telecommunications carrier will be identified. We assume that no other information will be gleaned by the LBS provider. In the case where a mobile user utilizes Wi-Fi instead, the user will be assigned an address that points to the nearby access point, however, and may need to employ other techniques, such as Tor, to mask the address.

II. RELATED WORK

There are many researchers concentrating on the how to obtain the privacy and accuracy in LBSs One of the researchers was Dewri, who has a long history in the field of privacy in location-based services. He has various publications relating to achieving the privacy in LBSs His last paper [1] proposed a user-controlled privacy experience “a user-centric location based service architecture”, where the user determines the desired level of privacy based on his accuracy requirements. A provider “privacy-supportive LBS” provides supplemental information to the user for making “informed” privacy decisions. The system will inform the user of the accuracy (or lack thereof) based on the privacy specifications input into the system, depending on “a service-similarity profile” which the user gets.

If the user is satisfied with the result set (even if it has errors or the privacy is under the required level), they can choose to proceed with the query. If they are not satisfied, they can change the privacy level into the balance of accuracy/privacy that is acceptable to them. The main purpose of previous papers [2] is to understand (LBS) technology and identified the key components behind the service. Some papers present a concise survey of location based services, the technologies deployed to track the mobile user’s location, the accuracy and reliability associate with such measurements, and the network infrastructure elements deployed by the wireless network operators to enable these kinds of services [3]. Other papers define the user requirements in terms of mobile device features and LBS applications. In addition to the general idea of the LBS, the researchers discussed the impact on consumer, and utility computing offer attractive financial and technological advantages. As an example, Zhang and Mao studied the effects of three individual level factors; consumption values, privacy concerns, and subjective norms on consumers' intention to adopt location-based services on their mobile phones and to spread positive word-of-mouth (WOM) about LBS. Such knowledge helps business create effective communications to attract more potential adopters. In light of the current findings, marketing communications need to heighten perceived consumption values about using LBS [4-10].

All these scientific papers give the attracted people a general idea about LBSs, and how this service was important [12]. Researchers have long been aware of the potential privacy risks associated with LBSs, because they know while the user used one of these application services to retrieve the accuracy information, this new functionality comes with significantly increased risks to personal privacy. They have proposed a number of promising schemes that can help users protect their privacy. Some of these papers present an overview of different protection goals and fundamental location privacy approaches, as well as a classification of different types of attacks according to the applied attacker knowledge. They clarified different protection goals and fundamental location privacy.

III. PROPOSED RSASSOL ALGORITHM

For RSAS queries, the spatial solution is based on the Dijkstra’s algorithm. Given a query point q, the query range radius r, and a string predicate, we expand from q on the road network using the Dijkstra’s algorithm until the destined points are obtained. The distance r away from q and verify the string predicate either in a post-processing step or on the intermediate results of the expansion. The performance degrades quickly when the query range enlarges and/or the data on the network increases.

This motivates us to find a novel method to avoid the unnecessary road network expansions, by combining the pruning’s from both the spatial and the string predicates simultaneously. For ESAS queries, our experimental evaluation covers both synthetic and real data sets of up to 10 million points and 6 dimensions. We partition a road network G = {V,E} into m edge disjoint sub-graphs G1,G2, . . . ,Gm, where m is a user parameter, and build one string index (Filter Tree) for strings in each sub-graph. We also select a small subset VR of nodes from V as reference nodes: they are used to prune candidate points/nodes whose distances to the query point q are out of the query range r. The proposed architecture is given below:

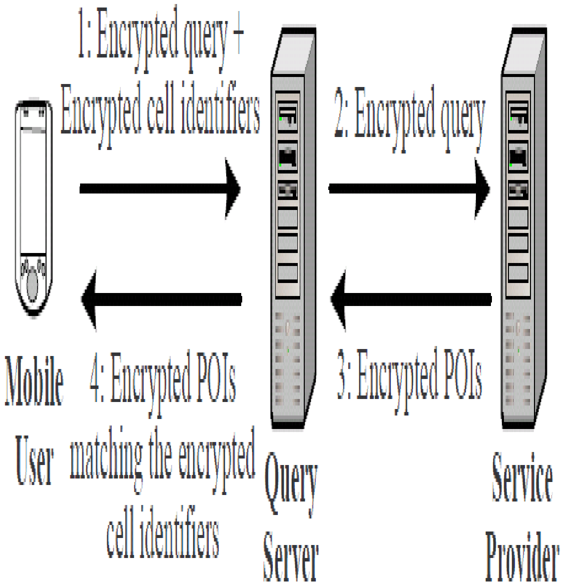

Fig.1. System architecture of User-Defined Privacy

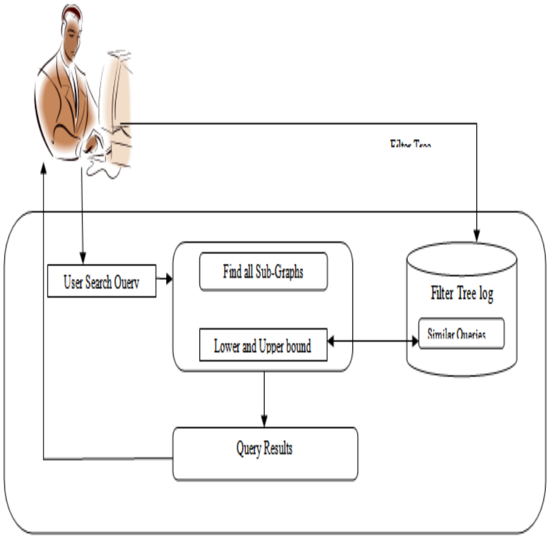

Fig.2. Working of RSASSOL algorithm

The RSASSOL algorithm is presented as follows:

1. Get the queries for string search.
2. Discovering the subgraphs for the given queries.
3. Filter tree approach is used as sub-graphs that display and output the similarity points of the actual queries string.
4. Lower and upper bound of candidate points is calculated and it is pruned from the distance of the candidates.
5. The above step 4 is repeated until the string predicate is estimated.
6. The accurate distance for every candidate points to the query points that returns the optimal distances for the specified query string.

IV. EXPERIMENTAL RESULTS

For RSAS queries, our evaluation is based on two large, real road network datasets that contain up to 175,813 nodes, 179,179 edges, and 2 millions points on the road network. In both cases, our methods have significantly outperformed the respective baseline methods. This is very helpful for Exact Result from Non Exact keywords.

And after that we examine the viability of the RSASSOL calculation for RSAS questions in this area. Firstly, we research the impact of determination and the quantity of reference hubs, and the quantity of subgraphs worked by the RPar calculation, in the preprocessing step, to the RSASSOL calculation. The effects of reference hubs determination on the queries execution come in two folds. To start with, various determination methodologies will wind up in selecting diverse reference hubs. Furthermore, our own particular perceptions, the streamlined planar calculation is dependably the best methodology, given the same number of reference hubs. Second, the quantity of reference hubs is additionally basic. After that, we think about the impact of number of subgraphs, on the running time of RSASSOL. Be that as it may, having more subgraphs likewise implies more access to smaller FilterTrees, which presents inquiry overhead when looking for surmised strings. The similarity matrix drawn between two queries is shown in Fig.3.

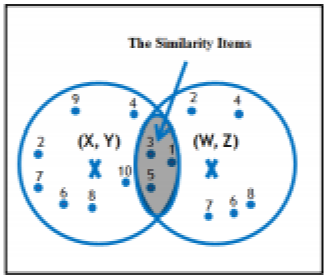

Fig. 3. Similarity matrix between two queries

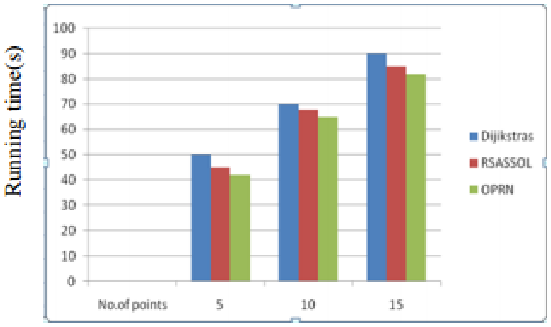

Fig.4. Time consumption chart

Overhead of RSASSOL calculation increases to a specific degree gradually in light of shared spatial and in addition string-based pruning power. RSASSOL has propelled space utilization as in addition it use Filter Trees to accelerate the estimated string coordination and in addition amass separations from hubs to reference hubs for third step pruning. In any case, these transparencies are still straight towards the information sets in assuming the worst possible scenario. Having extra reference hubs, lower and in addition upper separation limits have a penchant to be more tightly, prompting upgraded the pruning. More reference hubs in addition lead to unrivaled working out expenses to work out second rate and also higher separation limits all through query processing.

V. CONCLUSION

In this paper, we proposed a supplemental architecture to successfully address some of the inherent limitations of previous works. Improving the granularity of the previous similarity matrix was one of the great upgrades that improved the system. The system achieved better performance by not threatening the accuracy of the system without the requirements of providing results at such as sparse level. This paper presents a comprehensive study for spatial approximate string queries in both the Euclidean space and road networks. We use the edit distance as the similarity measurement for the string predicate and focus on the range queries as the spatial predicate. We also address the problem of query selectivity estimation for queries in the Euclidean space. The improvements now give the user true and complete flexible control over their privacy and the system.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T.Wang, "Supporting anonymous location queries in mobile environments with Privacy Grid," in WWW, 2008.

[2] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations," in SSTD, 2007.

[3] B. Gedik and L. Liu, "Protecting location privacy with personalized k anonymity: Architecture and algorithms," IEEE TMC, vol. 7, no. 1, pp. 1–18, 2008.

[4] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in ACM MobiSys, 2003.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," IEEE TKDE, vol. 19, no. 12, pp. 1719–1733, 2007.

[6] M. F. Mokbel, C.-Y. Chow, and W. G. Aref, "The new casper: Query processing for location services without compromising privacy," in VLDB, 2006.

[7] T. Xu and Y. Cai, "Location anonymity in continuous location-based services," in ACM GIS, 2007.

[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: Anonymizers are not necessary," in ACM SIGMOD, 2008.

[9] M. Kohlweiss, S. Faust, L. Fritsch, B. Gedrojc, and B. Preneel, "Efficient oblivious augmented maps: Location-based services with a payment broker," in PET, 2007.

[10] R. Vishwanathan and Y. Huang, "A two-level protocol to answer private location-based queries," in ISI, 2009.

[11] J.M. Kang, M. F .Mokbel, S. Shekhar, T. Xia, and D. Zhang, "Continuous evaluation of monochromatic and bichromatic reverse nearest neighbors," in IEEE ICDE, 2007.

[12] C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries of continuously moving objects," in IEEE ICDE, 2006.

[13] S. Wang and X. S. Wang, "AnonTwist: Nearest neighbor querying with both location privacy and k-anonymity for mobile users," in MDM, 2009.

[14] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in Pervasive Computing, 2009.

[15] Roman Schlegel, Member, IEEE, Chi-Yin Chow, Member, IEEE, Qiong Huang, Member, IEEE, and Duncan S. Wong, Member, IEEE, "User-Defined Privacy Grid System for Continuous Location-Based Services", IEEE Transactions on Mobile Computing, 2015.