Mobile Crowd Sensing Using Voronoi Based Approach

Sumedha Sirsikar
Dept of Information Technology
MIT, Pune, MH, India

Varsha Powar
Dept of Information Technology
MIT, Pune, MH, India

Preeti Chakurkar
Dept of Information Technology
MIT, Pune, MH, India

***Abstract*— Crowd Sensing is a new business model which allows large number of smart phones to be used not only for exchanging information but also for activities that may have a huge social impact including traffic or road monitoring, urban planning, social networking and environmental monitoring. Here, we present a novel approach for developing a sensing application to collect a specific dataset where real privacy is major challenge. This paper presents an approach of crowd sensing applications that utilizes Voronoi diagram for protecting the privacy of participated mobile users. We can apply stated methods to partition a particular city into Voronoi cell which helps in user's location perturbation.**

Keywords—crowd sensing, voronoi diagram, privacy;

I. INTRODUCTION

The sensing devices includes for examples smart phones, sensor embedded gaming system, music players and in-vehicle sensor devices carried by millions of people around the world. It has opened up new possibilities of collecting and gathering sensed information for common interest.

Individuals who contribute to the crowd sensing applications feel exposed to high privacy threats for their own data. Such data may include interest of particular user, location data etc. It was pointed out that an adequate privacy protection of crowd sensing application users can be ensured only by the use of data perturbation. This approach of perturbation, which adds an artificial noise to sensor data, is achieved with the method of Voronoi diagram.

Given a set of n location points, a Voronoi diagram divides the space into n partitions. Each partition is called a voronoi cell and it corresponds to one point. The cell is in such a shape that the nearest neighbor of any point in this cell is the corresponding point. Delaunay triangulation for a set P of points in a plane such that lines connect the objects whose voronoi cells are adjacent and divide the space into partitions of a special shape-triangles.

II. RELATED WORK

To protect location privacy of individuals in location based services, location obfuscation methods have been studied widely in the literature of recent surveys [1], [2]. One typical obfuscation method is spatial cloaking or perturbation which hides the user's location inside a cloaked region using spatial transformations [4] or a set of dummy locations [3]. Most recently, the work [6] proposed a location perturbation method based on a rigorous notion of in distinguishability, which is similar to the differential privacy concept [5].

III. PROPOSED MODEL

There have been remarkable developments in the field of Crowd Sensing which exclusively depends on user provided data and its location details, where high numbers of participants are required. Considering the scenario user's privacy might get compromised. Hence mechanism is required to address challenging issues of user privacy. We have proposed a method where focus has been given on not revealing users exact location, which is achieved by perturbation of user location by construction of computational geometry i.e. Voronoi cell.

The proposed model as shown in Figure 1 consists of 3 main components:

A. Application server
B. Participants
C. End users

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. Application Server

It is an entity which collects data from the various participants or group of participants, the collected data is further analyzed and made available in various forms such as graphical representation or maps showing the sensing results.

It is also responsible for generating the Voronoi diagram, Delaunay triangulation, and WAG tree for specified location points which later can be sent to the sensing device for the application need.

B. Participants

Participants are primarily focusing on collecting sensed data which will be transferred to the application server for further processing.

C. End User

Analysis generated by application server of Crowd Sensing applications helps end user to make proper decisions in various applications of social paradigms.

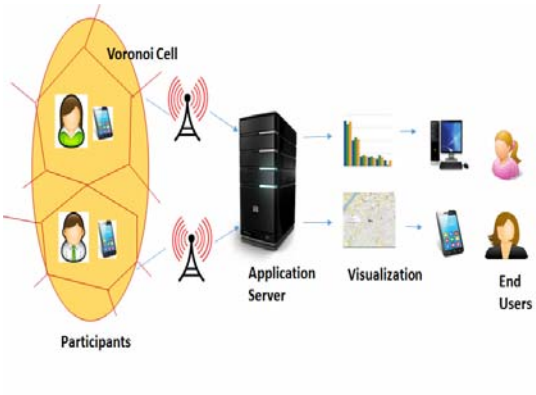

Fig. 1. Architectural diagram of Crowd Sensing applications

IV. Privacy Challenges in Crowd Sensing

Most Crowd Sensing applications collect data from individuals which can be used for the identification of those individuals. Such data may include, for example, different tastes and interests of a particular user, as well as location data. It should be noted that Crowd Sensing raises more privacy concerns. The creators of Crowd Sensing applications have to find a way to protect the data of individuals while at the same time enabling the operation of the applications. There are three main approaches on how to protect the privacy of the users of Crowd Sensing platforms. These approaches are anonymization, encryption, and data perturbation as follows:

a) Anonymization

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

b) Encryption

Encryption does not allow unauthorized third parties to use personal data of mobile users, but it encryption of large volume of data requires significant resources.

c) Data Perturbation

Data Perturbation hides the actual details of mobile user or sensor collected data. It can be done by adding noise or spatial transformation, which enables good operation for crowd sensing application.

A. Privacy challenges in Crowd Sensing

This approach is based on the concept of voronoi cell diagram where each cell contains mobile sensing devices. Figure 2 shows example of voronoi diagram with 6 points such as a, b, c, d, e and f. The blue solid lines show the borders of the voronoi cells, and the green lines connect the adjacent cells objects. The green lines are called Delaunay triangulation of the space because these lines divide the space into partitions of spatial shape-triangles. However, if the space is bounded, these green lines might not form a closed delaunay triangulation because two cells might share a border at somewhere beyond the bounded space. For example, in the rectangular space of Figure 2 (a). Their voronoi cells are not adjacent in this space, although they share a border outside the space. If the user knows the voronoi cells in advance, he or she can set the cloaked region to the voronoi cell of the nearest neighbor points [7].

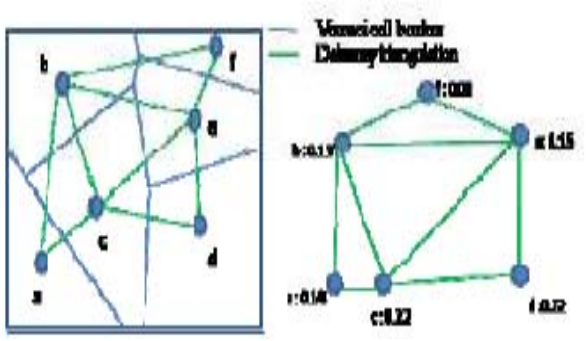

Fig. 2. Voronoi diagram and WAG

Data structure used to store the voronoi cell information is called as a weighted adjacency graph (WAG). WAG is a weighted undirected graph that stores the voronoi diagram and Delaunay triangulation. For example, in Figure 2(b), each vertex in this graph denotes an object, and each edge denotes a line in the Delaunay triangulation. Each vertex is also assigned a non-negative weight. The specialty of this graph is to notify that the WAG vertices are weighted based on voronoi cell area size.

To reduce computational overhead, partition the entire WAG into WAG snippets of reasonable size so that the user receives only the snippets surrounding the location. For example, in Figure 3(a), the four snippets are obtained by partitioning the space into four sub-spaces A, B, C and D of equal widths and heights and computing their WAG's, respectively. The weight of an object in a WAG snippet is set to its voronoi cell area that resides in this subspace. WAG snippets can be joined to become the WAG of the union of these subspaces. The join is done by merging the vertices corresponding to the same object and assigning its new weight as the sum of the weights of these vertices. WAG-tree follows a top down recursive fashion. For each node, the algorithm maintains points whose voronoi cells in the whole space overlap this sub-space. Since each such object is the nearest neighbor of some point in this sub-space, it is essentially the range nearest neighbor (RNN) of this sub-space.

The algorithm recursively computes range nearest neighbor of a child node until satisfying the certain criterion, e.g. the snippet area is larger than user defined threshold and Figure 3 shows a WAG-tree and snippet pointed by it. Proposed algorithm is able to save bandwidth usage compared with others by returning less number of non-result objects [7].

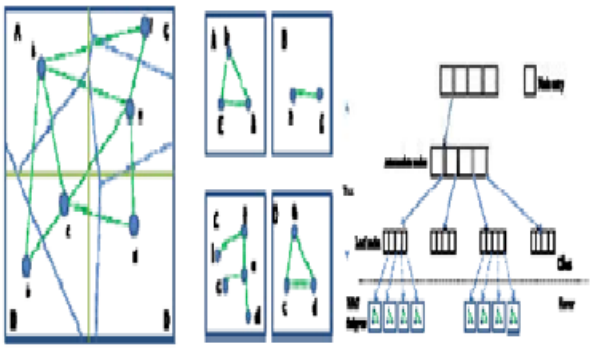

Fig 3. Wag snippet and WAG tree

B. Algorithm

Input: Dataset containing all location points of particular city S = {p1, p2, p3, …. pn}

Server side steps:

1. Construct a Voronoi diagram of V(s)
2. Compute Delaunay triangulation for a set of points P in a plane
3. Construct a WAG tree base on step 2
4. Group formation of participants

Client side steps:

5. Obtain WAG tree at the sensing device site
6. Acquisition of sensor data from location point q
7. S = {WAG snippets contains sensing location points q}

Data acquired in step 6 is transferred with location snippet S instead of q

Server side steps:

8. Data management and storage with location snippet S
9. Data analysis and visualization with location snippet S

VI CONCLUSION

In this paper, an approach of privacy in crowd sensing applications using Voronoi diagram has been proposed. In order to maintain location privacy of smartphone users, we have presented the efficient Voronoi algorithm for special transformation.

References

[1] G. Ghinita, Privacy for Location-Based Services, ser. Synthesis Lectures on Information Security, Privacy, and Tru. Morgan & Claypool, 2013. [Online].

[2] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, "Location privacy protection through obfuscation-based techniques," in Data and Applications Security XXI. Springer, 2007, pp. 47–60.

[3] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services." In Proceedings of the IEEE International Conference on Pervasive Services (ICPS), 2005.

[4] Priti Chakurkar, Vidya Deshpande; "Efficient Evaluation of MNN queries based on safe region"; 3rd International Conference on Recent Trends in Engineering and Technology, ICRTET' 2014, Nashik, India; March 28-30 2014; ELSEVIER, UK; pp. 22-28

[5] M. E. Andres, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems." ACM, 2013, pp. 901–914.

[6] M. E. Andr´es, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems."ACM, 2013, pp. 901–914.

[7] Haibo Hu, and Jianliang Xu. '2PASS: Bandwidth-Optimized Location Cloaking for Anonymous Location-Based Services,' IEEE Transactions On Parallel And Distributed Systems, 2010