MELANGE PUBLICATIONS
International Innovative Research Journal of Engineering and Technology
ISSN: 2456-1983 Vol: 5 Issue: 3 March 2020

Secure Mobile Crowdsensing Obfuscation for Patient Feedback Using Location Privacy Approach

P. Maragathavalli[1], R. Prabhakaran[2]

[1]Assistant Professor, [2]Master of Technology
Information Technology, Pondicherry Engineering College, Puducherry
[1]marapriya@pec.edu, [2]rprabhakaran824@pec.edu

Abstract: The broad of smart gadgets prompts the improvement of progressively complex distributed applications, attractive endeavours from both research and business networks. Recently, a new volunteer commitment worldview dependent on participatory and sharp detecting is equipping in the Internet of Things scenario: Mobile Crowdsensing, Sparse Mobile Crowdsensing (MCS) has become a compelling approach to urban- scale sensing information acquiring and making inferences. However, while recording data with their real sensing locations, participants threaten their location confidentiality. To address this issue, Sparse MCS embraces differential- security to give a hypothetical assurance to the area protection of patients or individuals regardless of prior knowledge of an adversary. It was designed to provide aggregated data to patients about their health variation over time. A mobile feedback form platform will help a patient to understand and get better control of their health. In addition, to decrease the quality of data induced by differential location obfuscation, a security protecting framework is proposed.

Keywords: Mobile Crowdsensing, urban sensing, Quality of service, Internet of Things, Data Recovery, Patient Feedback, Mobile Healthcare Services, Location Privacy, Internet of Things.

1. INTRODUCTION

Mobile crowdsensing (MCS) is a developing model that influences the recent emergence of sensor-equipped smartphones to gather information on an urban scale, such as noise and traffic. Internet of Things (IoT) is an interrelated set of computing devices, mechanical and virtual machines, artifacts, animals or individuals capable of transferring data over a network without needing human- to - human or computer - to - computer communication with unique identifiers (UIDs). Crowdsensing, sometimes referred to as mobile crowdsensing, is a technique in which a large group of people with mobile devices can collectively detect and compute data and extract information (such as smartphones, tablet computers, wearable computers) to measure, map, analyze, estimate or infer any common interest process. In short, this means that sensor data from mobile devices are crowd sourced. However due to budget or time constraints, the target sensing area may sometimes be so wide that it may be difficult to have adequate spatial coverage for mobile users. One approach is to use Sparse Mobile Crowdsensing by integrating historical records with available sensing data from nearby regions to impute information from uncovered regions. Through Sparse MCS, participants record sensing data with time stamps and geographic co-ordinates that may pose significant privacy risks. To attract participants, therefore, the privacy of the location is essential. Many existing work on location-based systems (LBS) concentrates on location privacy, and has introduced two general protective mechanisms shown in Fig.1.,

[1] Protecting users' identities through anonymity, so that their location traces cannot be linked to specific individuals,

[2] Using location obfuscation to change the specific locations of users that are accessible to the service provider.

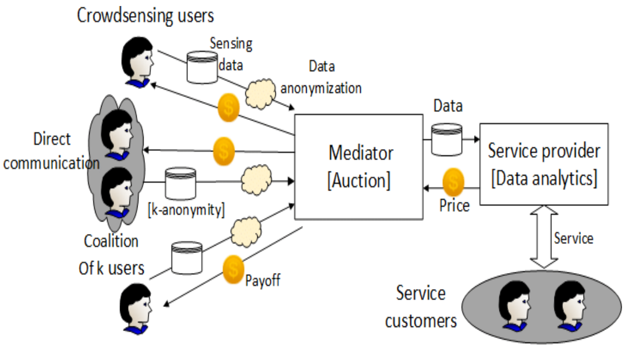


Figure 1. Mobile Crowdsensing

2. LITERATURE SURVEY

The following are the existing work done on mobile crowdsensing and location based approaches

2.1 Spatial Cloaking

Kazemi et. al. showed that spatial k- anonymity methods used in location-based services are not directly applicable to Participatory Sensing. Therefore, they proposed that a group of the representative participants ask for spatial tasks from an untrusted server, and share their results with the rest of participants. They would also adjust the spatial regions in queries to make queries independent from the location of other participants. While most traditional location cloaking methods rely on syntactic privacy models and are subjective to inference attacks, recent works applied more rigorous privacy notion based on differential privacy. A method of location disruption based on a rigorous notion of distinguishability, similar to the concept of differential privacy. Another recent work protects the exact locations with differential privacy in a proposed delta-location set, which is derived in Markov model to denote the possible locations where a user might appear at any time.

2.2 Temporally Constrained Sharing

Krause et al. use a spatial obfuscation approach. They divide the space into a series of regions in their solution, and then subsets of participants are chosen in each region to disclose their exact location with a certain distribution of probability. Such methods can be used in traffic monitoring applications. Another method assigns spatial tasks to participants in a way that the number of tasks for each participant is minimized. In such an approach, there will be longer intervals between each location disclosure, mitigating location-based inference attacks. This scheme can be further controlled by participants by setting explicit policies regarding the intervals in which they prefer to share their location.

2.3 Aggregated Location with Differential Privacy

Differential Privacy is a promising privacy preserving approach with a strong protection guarantee. This method is adopted in privacy-preserving publishing of statistical information about location based datasets guaranteeing that individual location information disclosure does not occur. It can also prevent the aggregated number of participants at a location from attacking privacy.

2.4 Private Information Retrieval

In autonomous pull-based tasking schemes, participants can retrieve the best suited tasks without providing their attributes using private information retrieval (PIR). PIR-based methods have been adopted for location-based services recently since they guarantee cryptographic privacy by allowing data retrieval from a database without revealing any information to the database server about the retrieved item. Such an anonymous tasking scheme suffers from overlapping task selection and bias since sharing entities do not learn which tasks are retrieved.

2.5 Policy-based Privacy Preferences

Shilton et. al. introduced the concept of participatory privacy regulation in MCS which promotes participants' involvement in developing their own privacy policies and setting their personal boundaries. Some methods provide a trusted cloud- based storage and processing entity for each participant to store and fully control sharing of her personal information with applications and end users. A recent incentive-based task assignment approach allows participants to set their preferred privacy levels, which are then incorporated into a tasking cost model to limit the frequency of location disclosures.

2.6 Differential Privacy Under Temporal Correlations

Due to the rapid proliferation of GPS- enabled devices and location-based applications, questions regarding location privacy frequently arise. Although comprehensive study has been carried out on techniques of spatial transformation such as position disruption or generalization, most techniques rely on models of syntactic privacy without robust privacy guarantee. Many of them consider only static scenarios or interact with the position at single timestamps without considering temporal comparisons of the positions of a moving client and are therefore vulnerable to various inference attacks. Although differential privacy has been recognized as a privacy standard, the implementation of differential privacy in location-based applications presents new challenges, as security needs to be applied on the fly for a single user and must incorporate transient differences between the locations of a user.

2.7 Algorithmic Privacy Preserving

The data analysis protection issue has a long history spanning multiple disciplines in privacy preserving.

When electronic data on individuals becomes more and more comprehensive and as software allows more and more efficient data collection and duration, the need for reliable, meaningful data increases, and a rigorous mathematical definition of privacy, along with a computationally rich class of algorithms that meet this criteria.

2.8 Community Sensing

There is a great opportunity to combine data from private-held sensor populations to create useful applications for sensing. For example, for traffic monitoring and routing, GPS devices embedded in cell phones and cars could one day be used as distributed networks of velocity sensors. Unfortunately, considerations of privacy and expense limit access to these sources of data. We define group sensing concepts that provide frameworks for data sharing from private sensors. Sensor availability, context-sensitive reliability of sensor information based on phenomena and demand models, and privacy and resource preferences of sensor owners are taken into account in the methods. A well-defined approximation of optimal sensing policies is provided. We provide details on key community sensing principles and emphasize their use in a case study for road traffic monitoring.

2.9 Privacy in Location-based Services

Since most service providers are reluctant to adopt privacy-friendly protocols because of their business model, we are researching the development and evaluation of security mechanisms focused on obfuscation. Such mechanisms for location-privacy preserving (LPPMs) enable users to protect their locations while participating in protocols that invade privacy. A system that allows the computation of the optimal LPPM for users who participate sporadically in LBSs and that is customized to a user's mobility profile and the user's constraints. For a first-order location privacy approximation of applications which often employ LPPMs. Finally we conclude this thesis 'study results and describe approaches for future study. Here we emphasize the analysis of quantification systems, which take the middle ground between complexity and simplicity [9].

3. SMCOPFLPA PROPOSED SYSTEM

Regular data collection requires participants to record their individual regions in Sparse MCS. Using obfuscation to incorporate location privacy protection may mitigate the worries of the participants, but it can lead to loss of data quality if the sensing data allocated to an obfuscated area is not reflective of the actual situation. This therefore combines two specific elements in the development of a position-preserving framework: location obfuscation and data modification.

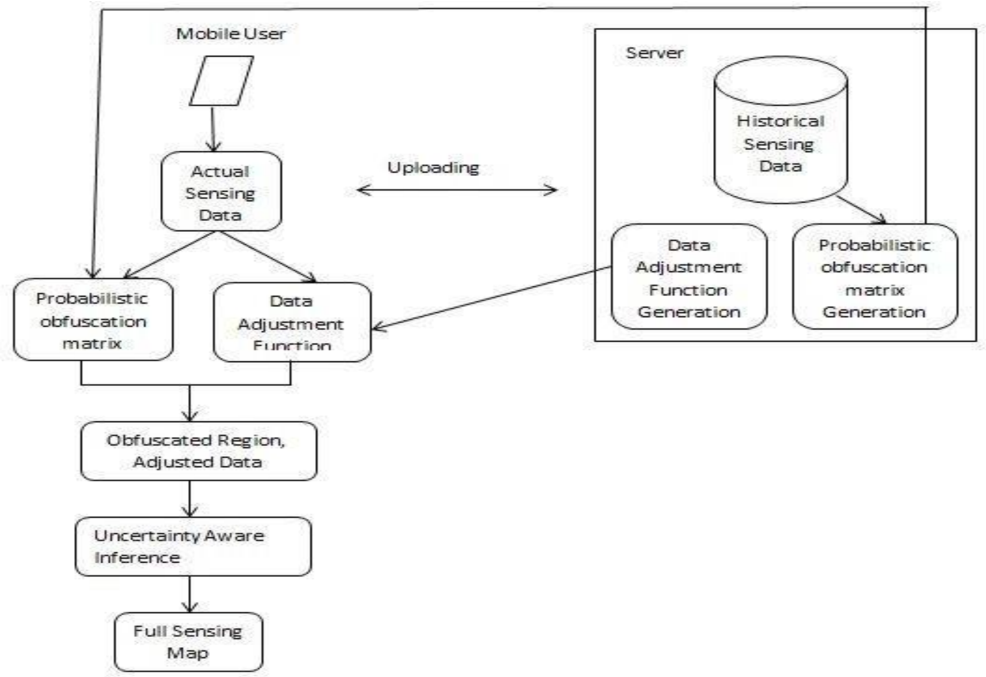

Mobile User
Server
Historical Sensing Data
Uploading
Actual Sensing Data
Data Adjustment Function Generation
Probabilistic obfuscation matrix Generation
Probabilistic obfuscation matrix
Data Adjustment Function
Obfuscated Region, Adjusted Data
Uncertainty Aware Inference
Full Sensing Map

Figure 2. SMCOPFLPA Proposed System

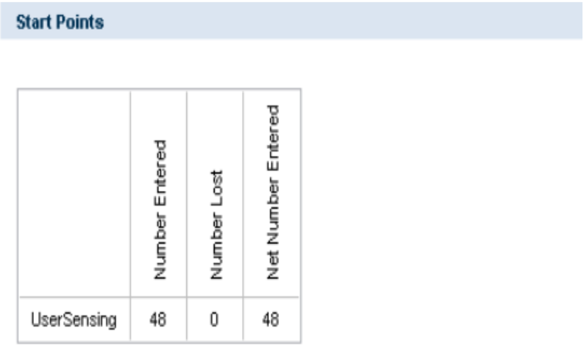
Fig.2. is an outline of our proposed Sparse MCS location privacy system. It consists of two levels — server side and mobile client side. Before a Sparse MCS task begins, the server side produces a probabilistic obfuscation matrix based on the historical sensing data.

- The matrix encodes the probability of obfuscating one region to another region. A data adjustment functions features are in an offline manner. Users can protect location privacy by carefully selecting the probabilities that may make it impossible to accurately infer from their obfuscated counterpart an actual region, even if the opponent knows the matrix of obfuscation. The data adjustment function is used because of region obfuscation to reduce data uncertainty. It is learned by analysing the correlation in the historical log between the sensing data of any two regions.
- After both the obfuscation matrix and the data adjustment feature have been pre-downloaded to their mobile phones, the user scans the mobile client's sensing task as follows. First, the exact location of each mobile phone is sensed. Then it maps the corresponding region to another region based on the probabilistic obfuscation matrix. The data adjustment function subsequently changes the original sensing data to fit the obfuscated region's properties. Then the mobile client uploads to the server the changed region and information. The database then collectively infers the full sensing map from all the obfuscated areas, which includes some degree of uncertainty compared to the actual data.

4. EXPERIMENTAL RESULTS AND ANALYSIS

The server utilisation is calculated by working and waiting time. From the server the average Queue time is calculated for each resource sensed. The average queue size and average queue times are calculated by minimum and maximum size of queue and time of queue.

i. User Sensing

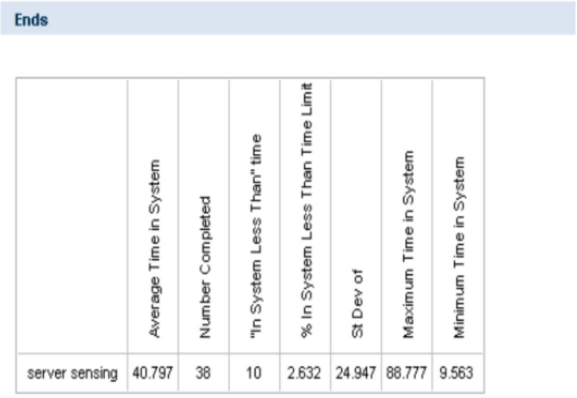


Start Points

	Number Entered	Number Lost	Net Number Entered
UserSensing	48	0	48

Figure 3. User Sensing

ii. Server Sensing



Ends

	Average Time in System	Number Completed	"In System Less Than" time	% In System Less Than Time Limit	St Dev of	Maximum Time in System	Minimum Time in System
server sensing	40.797	38	10	2.632	24.947	88.777	9.563

Figure 4. Server Sensing

iii. Resource Utilization and Execution Time

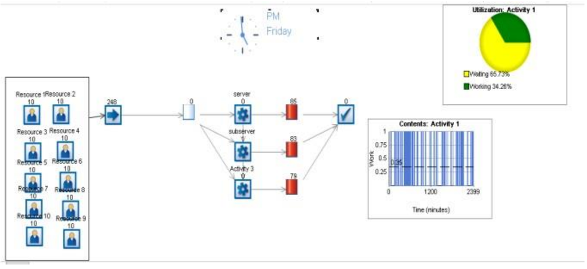


Figure 5. Resource Utilization and Execution Time

Table 1. Experimental Results

S. N O	PERFORMANCE FACTOR	EXISTING SYSTEM	PROPOSED SYSTEM
1	Ease of use	Sensor Networks	Mobile Devices
2	Security	Authentication is not initiated	The authentication is done by using Adversary Model
3	Time	The execution time was very High	. Less Execution time
4	Data Loss	Data Loss while transmitting the File	Data loss reduction is done by Differential Privacy Location

5. CONCLUSION

Mobile crowd sensing is a modern concept with a wide variety of possible applications. However, MCS's functionality depends on the participation of individuals who may be uncertain about their privacy. Task management, in particular, as a central part of the crowd sensing system, poses many risks to the privacy of participants which should be identified and addressed. This paper provides a differential location privacy system for Sparse MCS. This paper takes into account the desired level of privacy protection, previous information about the location distribution of participants and the lack of data quality due to location obfuscation. The next work is to incorporate the anonymous locations and trajectory resources into cartographic information and historical data in order to develop the distributed networks for the method of trajectory privacy protection.

REFERENCES

[1] Liu, X.; Ota, K.; Liu, A.; Chen, Z. An incentive game based evolutionary model for crowd sensing networks. Peer-to-Peer Netw. Appl. 2016, 9, 692–711.

[2] Zhang, X.; Yang, Z.; Sun, W.; Liu, Y.; Tang, S.; Xing, K.; Mao, X. Incentives for mobile crowd sensing: A survey. IEEE Commun. Surv. 2016, 18, 54–67.

[3] AlOrabi,W.A.; Rahman, S.A.; El Barachi, M.; Mourad, A. Towards on demand road condition monitoring using mobile phone sensing as a service. Procedia Comput. Sci. 2016, 83, 345–352.

[4] L. Kazemi and C. Shahabi. A privacy-aware framework for participatory sensing. ACM SIGKDD Explorations Newsletter, 13(1):43–51, 2011.

[5] M. E. Andr´es, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi. Geo-in distinguishability: Differential privacy for location-based systems. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pages 901–914. ACM, 2013.

[6] Y. Xiao and L. Xiong. Protecting locations with differential privacy under temporal correlations. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 1298–1309, 2015.

[7] C. Dwork. Differential privacy. In Automata, languages and programming, pages 1–12. Springer, 2006

[8] Krause, E. Horvitz, A. Kansal, and F. Zhao. Toward community sensing. In Proceedings of the 7th international conference on Information processing in sensor networks, pages 481–492. IEEE, 2008.

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

[10] K. Shilton, J. A. Burke, D. Estrin, M. Hansen, and M. Srivastava. Participatory privacy in urban sensing, 2008.

[11] Z. Feng, Y. Zhu, Q. Zhang, L. M. Ni, and A. V. Vasilakos, ―TRAC: Truthful auction for location-aware collaborative sensing in mobile crowdsourcing,‖ in INFOCOM, pp. 1231–1239, 2014.

[12] K. Han, Y. He, H. Tan, S. Tang, H. Huang, and J. Luo, ―Online pricing for mobile crowd sourcing with multi-minded users,‖ in MobiHoc, pp. 18:1–18:10, 2017

[13] K.Han, C.Zhang, J.Luo,M.Hu, and B. Veeravalli,―Truthful scheduling mechanisms for powering mobile crowdsensing,‖ IEEE Trans. Comput., vol. 65, no. 1, pp. 294– 307, 2016.

AUTHOR BIOGRAPHY

Dr. P. Maragathavalli

She received her B.E. degree in CSE from Bharathidasan University, M.Tech. and Ph.D. degree in CSE from Pondicherry University. She joined Pondicherry Engineering College in 2006 and currently working as Assistant Professor in the Department of Information Technology. She has published several research papers in various referred journals and international conferences. Her area of interest includes Security Testing, Optimization Techniques, Genetic Algorithm and Information Security. She is a Life member of ISTE.

R.Prabhakaran

He is pursuing M.Tech degree in the Department of Information Technology, Pondicherry Engineering College, Pondicherry.