International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 2, Mar-Apr-2020, ISSN (Online): 2395-566X

Survey on Location Privacy in Participatory Sensing Applications

Vaishnavi K, Vaishnavi D R, Srujana S K, Vaibhav Talreja, Asst.Prof. Nikshepa T, Asst. Prof.Surabhi K R, Asst.Prof. Lavanya D
Department of Information Science and Engineering
Dayananda Sagar Academy of Technology and Management, Bangalore, Karnataka, India
vaishnavikyalnoor@gmail.com,vaishnavidr123@gmail.com,sk.srujana13@gmail.com,Vaibhav7talreja@gmail.com,
nikshepa.t@gmail.com,k.r.surabhi@gmail.com, Lavanya.ash86@gmail.com

Abstract – **Location Privacy is a major apprehension in participatory sensing applications. Here user can both give as well as retrieve valuable information. The major drawback in LBSs (Location Based Services) is the leakage of user's locality. These applications collect detailed sensor data which compromise user privacy. To solve this problem existing solutions bring in trusted third party (Anonymizer) connecting the user and the Location Service Provider (LSP). In some situations the Anonymizer may compromise which leads to leakage of user information. To deal with this issue, in this paper we adopt an enhanced location privacy preserving system for the LBS atmosphere. The main advantages of our method includes: 1) user can raise queries with secured locations, 2) no need of fully trusted third parties.**

Keywords– **K anonymity, Location Based Services (LBSs), Location Privacy, Voronoi diagram (VD).**

I. INTRODUCTION

Modern years have experienced the growing concerns regarding the security and confidentiality of user information in many participatory sensing applications. Users desire to protect their personal data such as identity, location etc. from revelation to unauthorized parties throughindirect inferences or straightdisclosure. Releasing of a bit of data withoutidentity informationmay still expose personaldata or information about users with high possibility.

With the advanced wireless technology and persistentprogress in participatory sensing applications (e.g., mobiles, GPS, activity trackers etc), follows an incredibledevelopment of LBSs. Real time examples consist of location based gas station finders ("gas stations near me"), tracking traffic condition ("The traffic condition near Silk Board"), spatial alarms. The mobile user can get such services by raising queries and providing theirlocalitydata to the service provider.

As providing ahuge convenience and other commercial opportunities, Location Based Servers (LBS)creates the way for mishandling of user's sensitivelocality information. Consider a situation, where the collected detailed location data of the user can be utilized to send spam to userswith surplus messages; User's health conditions, lifestyle, ostracized religiousor else political views are able to be hacked through observing users' visit to some explicit locations. GPS devices canbe used in substantial stalking. Aiming on offering safety against Confidentiality attacks at the same time preserving the information truthfulness, in this paper we suggest aproficientmethod based on Locality Sensitive Hashing (LSH).The mechanism conserves both K- anonymity and locality. After that we adopt an algorithm to solve kNN requests at any point in the spatial cloaks of polygonal shape.

II. METHODOLOGY

1. Anonymizer

Here Locality Sensitive Hashing is proposed to divide user localitiesinto groupsholding at least K users (termed as spatial cloaks). Thismethod is made known to protect both k-anonymity and locality. Later an Voronoi diagram is designed to solve kNN requests from any partinside the spatial cloaks of random polygonal outline. K-anonymity is a mechanism used toevade the exposure of user data. Spatial cloaking regions satisfy k- anonymity if each user data inside the region is impossible to differentiate from at least K-1 users' data.

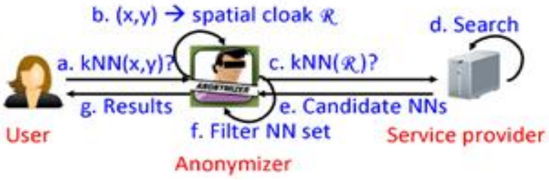


Fig.1. Structure for K anonymous location privacy. NN refers to nearest neighbour. kNN refers to k nearest neighbor query.[3].

2. Trusted Third Party (Ttp) And Function Generator

In this mechanism, Anonymizer which is a trusted entity is brought into the system. It works as an intermediate connecting LSP and the user. When Anonymizer is hacked by opponent, it may create a risk to the user privacy. Hence Function Generator is introduced to get avoid need of trusted entities. Hilbert curve is used to convert a real location into pseudo location through which the Anonymizer be able to construct the Anonymizing Spatial Region(ASR) along with filter Points of Interest(POIs).

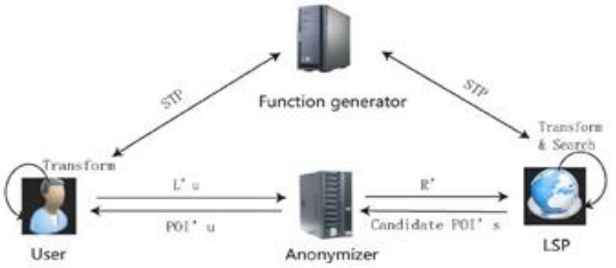


Fig.2. Enhanced location privacy preserving system (ELPP) meant for user privacy. R' refers to transformed ASR. POI'u is pseudo location of result to the user, L'u is pseudo location of user, and POI' is pseudo location of POI.[2]

3. Privacy Preserving Identification Mechanism

Here two layer neural network models is projectedwith the use of datathat is processed through differential privacy which is used to distinguish, classify and relatethis to a driver identification system and verify the viability.

- An algorithm is designed to separate data privacy sensitivity and placeparticular levels to measure the sensitivity of privacy and access the amount of privacy revelation.
- An adoptive confidentiality preserving schemethrough differential privacy is introduced to guardparticipants' data with high sensitivity of privacy.
- A driver identification system with the data protected by means of differential party is employed to recognize the drivers.

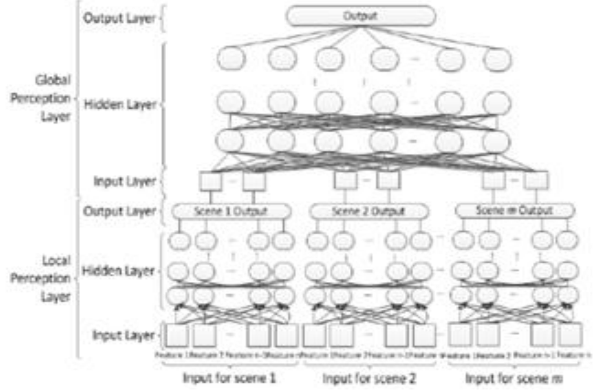
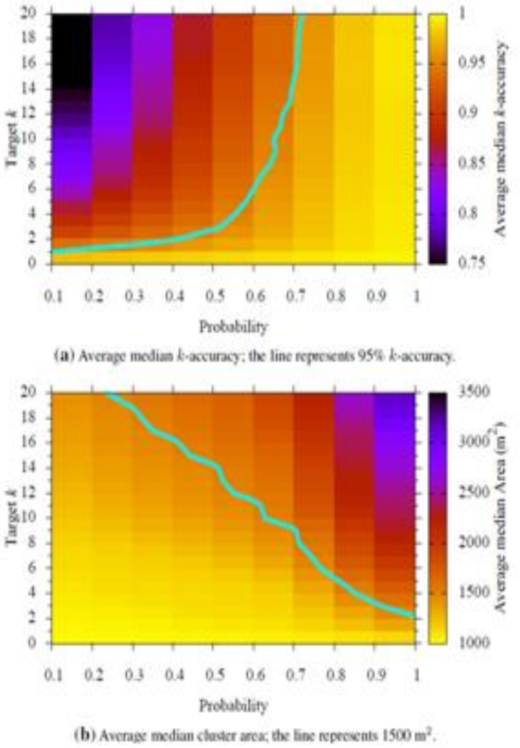


Fig.3. The structural design of Two Layer ANN model. [1]

4. Spatiotemporal Blurring

Aninnovative spatiotemporal blurring method which is based on clusteringalong with tessellationis used to guard the userinformation against the system while exposing thecondition. This technique uses probabilistic privacy termed as (k, p) anonymity. Itpermits users to carry out local blurring of information efficiently with no use of an online anonymization server prior to the information sent to the system. This scheme be able tomanage the quality of reports and degree of certainty in location privacyall the way through a system factor.



(a) Average median k-accuracy; the line represents 95% k-accuracy.

(b) Average median cluster area; the line represents 1500 m^2.

Fig.4.Target k vs. probability p. [8]

5. Anonymousdatareporting Protocol

An anonymous data reporting protocol is devisedin support of participatory sensing. This protocol offers data accuracy, generality and strong privacy protection. It contains two stages to be precise; they are slot reservation and message submission. During the first stage slot reservation, clusters containing N users collaborate to allocateevery user a message slot in a vector. It is basically message submission schedule; hereeach user slot is unaware to other users also to the application server. During second stage message submission, every user sends encoded information to the application server with the slot information well-knownmerely to herself/himself, in thismanner the application server could not link the data to theparticular user. By means of this type of data reporting protocol the connectionbetween the data and the users is broken down and as anoutcome, users' privacy is confined.

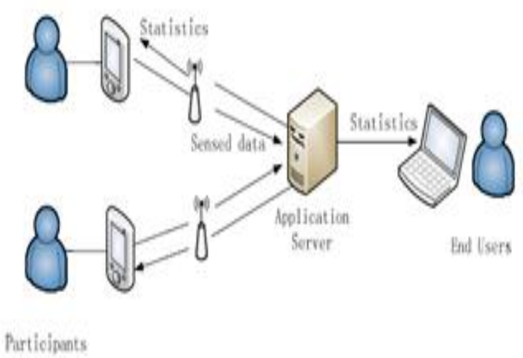


Fig.5. System architecture.[9]

III. RESULT COMPARISION

S.N.	Mechanism Used	Drawbacks	Efficiency
1	Anonymous Data Reporting Protocol	Applicable only for a limited extent of participants	60%
2	K-anonymity and Voronoi diagram	Fully dependent on Anonymizer	70%
3	Spatiotemporal blurring	Complete privacy is not assured	77%
4	Privary preserving identification	Complex to implement	80%
5	TTPand Function Generator	Restricted accessamong the user and the anonymizer	85%

IV. CONCLUSION

In our paper, we suggest aninclusive Enhanced Location Privacy Preserving (ELPP) method for the fortification of users' location privacy within LBS. The mainpoint is to avoid the use ofcompletely trusted entities to offer betterprotection. There is no acceptance that the mighty privacy assurance will leads to high cost. General evaluations imply that our proposed mechanismconserve location privacy at littlecommunication and computational cost. In our upcoming work, we strengthen our methodthroughimplementing multiple anonymizers to keep away from the restricted accessamong the anonymizer and the users and guarantee the elevatedsafety of the system.

REFERENCES

[1]. Ni, L., Tian, F., Ni, Q., Yan, Y., & Zhang, J. (2019). An anonymous entropy-based location privacy protection scheme in mobile social networks. EURASIP Journal on Wireless Communications and Networking, 2019(1), 93.

[2]. Peng, T., Liu, Q., & Wang, G. (2014). Enhanced location privacy preserving scheme in location-based services. IEEE Systems Journal, 11(1), 219-230.

[3]. Vu, K., Zheng, R., & Gao, J. (2012, March). Efficient algorithms for k-anonymous location privacy in participatory sensing. In 2012 Proceedings IEEE INFOCOM (pp. 2399-2407). IEEE.

[4]. Connolly, M., Dusparic, I., Iosifidis, G., & Bouroche, M. (2019). Privacy Aware Incentivization for Participatory Sensing. Sensors, 19(18), 4049.

[5]. Zhang, S., Li, X., Tan, Z., Peng, T., & Wang, G. (2019). A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services. Future Generation Computer Systems, 94, 40-50.

[6]. Liu, J., Li, X., Sun, R., Du, X., & Ratazzi, P. (2018, May). An Efficient Privacy-Preserving Incentive Scheme without TTP in Participatory Sensing Network. In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[7]. Wang, Y., Cai, Z., Tong, X., Gao, Y., & Yin, G. (2018). Truthful incentive mechanism with location privacy-preserving for mobile crowd sourcing systems. Computer Networks, 135, 32-43.

[8]. Shin, M., Cornelius, C., Kapadia, A., Triandopoulos, N., & Kotz, D. (2015). Location privacy for mobile crowd sensing through population mapping. Sensors, 15(7), 15285-15310.

[9]. Yao, Y., Yang, L. T., & Xiong, N. N. (2015). Anonymity-based privacy-preserving data reporting for participatory sensing. IEEE Internet of Things Journal, 2(5), 381-390.

[10]. Niu, X., Ye, Q., Zhang, Y., & Ye, D. (2018). A privacy-preserving identification mechanism for mobile sensing systems. IEEE Access, 6, 15457-15467.

[11]. Gao, S., Ma, J., Shi, W., & Zhan, G. (2015). LTPPM: a location and trajectory privacy protection mechanism in participatory sensing. Wireless Communications and Mobile Computing, 15(1), 155-169.

[12]. Tsolovos, D., Anciaux, N., & Issarny, V. (2018, October). A Privacy Aware Approach for Participatory Sensing Systems.

[13]. Tsolovos, D. (2018, December). Enforcing Privacy in Participatory Sensing Systems.