International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume. 1, Issue 3, July 2014, PP 8-14
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Privacy Preserving for Participatory Sensing using Trajectory Mix-Zone Model

[1]MA.MUMTAJ MUTHU GADHIZA, [2]SD.SD.AKTHAR BASHA, [3]P.BABU

PG Schalor, CSE, Quba College of Engineering and Technology,
[2,3]Associate Professor, QCET, Nellore

Abstract: *The ubiquity of the various cheap embedded sensors on mobile devices, for example cameras, microphones, accelerometers, and so on, is enabling the emergence of participatory sensing applications. While participatory sensing can benefit the individuals and communities greatly, the collection and analysis of the participators' location and trajectory data may jeopardize their privacy. However, the existing proposals mostly focus on participators' location privacy, and few are done on participators' trajectory privacy. The effective analysis on trajectories that contain spatial-temporal history information will reveal participators' whereabouts and the relevant personal privacy. In this paper, we propose a trajectory privacy-preserving framework, named TRPF, for participatory sensing. Based on the framework, we improve the theoretical mix-zones model with considering the time factor from the perspective of graph theory. Finally, we analyze the threat models with different background knowledge and evaluate the effectiveness of our proposal on the basis of information entropy, and then compare the performance of our proposal with previous trajectory privacy protections. The analysis and simulation results prove that our proposal can protect participators' trajectories privacy effectively with lower information loss and costs than what is afforded by the other proposals.*

1. INTRODUCTION

With the development of wireless communication technologies, such as WLAN, 3G/LTE, WiMax, Bluetooth, Zigbee, and so on, mobile devices are equipped with a variety of embedded sensors surveyed in as well as powerful sensing, storage and processing capabilities. Participatory sensing (urban sensing), which is the process that enables individuals to collect, analyze and share local knowledge with their own mobile devices, emerges as required under these well conditions. Compared with WSNs, participatory sensing offers a number of advantages on deployment costs, availability, spatial- temporal coverage, energy consumption and so forth. It has attracted many researchers in different areas such as Intelligent Transportation System, healthcare and so on. There are lots of existing prototype systems that include *CarlTel*, *BikeNet*, *DietSense*, *PEIR* and so on.

Nowadays, participatory sensing applications mainly depend on the collection of data across wide geographic areas. The sensor data uploaded by participators are invariably tagged with the spatial-temporal information when the readings were recorded. According to the analysis in, the possible threats to a participator's privacy information that include monitoring data collection locations, tracing his/her trajectory, taking photographs of private scenes and recording the intimate chat logs. Once participators realize the serious consequences with the disclosure of their sensitive information, they are unwilling to participate in the campaign and use the services. Since the success of participatory sensing campaign strongly depends on the altruistic process of data collection, if the participators are reluctant to contribute their collected data, it would weaken the popularity and impact of this campaigns deployed at large scale while also reducing the benefits to the users. Therefore, the privacy problems are the significant barriers to data collection and sharing. How to ensure the participators' privacy is the most urgent task.

In typical participatory sensing applications, the uploaded data reports may reveal participators' spatial-temporal information. Analysts could obtain some valuable results from the published trajectories for decision making, for example, merchants may decide where to build a supermarket that can produce maximum profit by analyzing trajectories of customers in a certain area and the

Department of Transportation can make an optimized vehicle scheduling strategy by monitoring trajectories of vehicles. However, it may introduce serious threats to participators' privacy. Adversary may possibly analyze the trajectories which contain rich spatial-temporal history information to link multiple reports from the same participators and determine certain private information such as the places where the data reports are collected. Thus, it is necessary to unlink the participators' identities from sensitive data collection locations. To best of our knowledge, existing work on privacy in participatory sensing mainly concentrate on data contribution and reporting process. If an adversary has *a priori* knowledge of a participator's trajectory, it is effortless to deanonymize his/her reports.

In this paper, we propose a trajectory privacy-preserving framework, named TrPF, for participatory sensing. We observe that the locations on or nearby participators' trajectories may not all be sensitive, and with this thought, our proposal only deals with the sensitive trajectory segments that will be discussed in the following. Moreover, mix-zones are regions where no applications can track participators' movements. Some works focused on road network mix-zones, which are not applicable in participatory sensing. For one thing, they all build mix-zones at road intersection, which may restrict the random data collection time and the number of ingress/egress locations; for another thing, the trajectory segments at the road intersection may not be sensitive, while the others would be. Therefore, we improve the theoretical mix-zones model to construct trajectory mix-zones model for protecting sensitive trajectory segments from the perspective of graph theory. Compared with existing trajectory privacy-preserving proposals, our proposal has advantages of lower costs and information loss while the privacy level would not decrease.

In this paper, the main contributions of our work are summarized as follows:

- We propose a framework TrPF of participatory sensing for trajectory privacy protection;
- We improve the theoretical mix-zones model with considering time factor from the perspective of graph theory to construct trajectory mix-zones model for protecting participators' sensitive trajectory segments;
- We formalize privacy level metric, privacy loss metric and information lossmetric, and then analyze the attack models with different background knowledge;
- Compared with previous trajectory privacy protections, we run a set of simulation experiments to evaluate the effectiveness of our proposals and then make a comparison of the performance.

2. EXISTING SYSTEM

In typical participatory sensing applications, the uploaded data reports may reveal participators' spatial-temporal information. Analysts could obtain some valuable results from the published trajectories for decision making, for example, merchants may decide where to build a supermarket that can produce maximum profit by analyzing trajectories of customers in a certain area and the Department of Transportation can make an optimized vehicle scheduling strategy by monitoring trajectories of vehicles. However, it may introduce serious threats to participators' privacy. Adversary may possibly analyze the trajectories which contain rich spatial-temporal history information to link multiple reports from the same participators and determine certain private information such as the places where the data reports are collected. Thus, it is necessary to unlink the participators' identities from sensitive data collection locations. To best of our knowledge, existing work on privacy in participatory sensing mainly concentrate on data contribution and reporting process

3. DISADVANTAGES

1. If an adversary has *a priori* knowledge of a participator's trajectory, it is effortless to deanonymize his/her reports.
2. Adversary could infer the first exit might correspond to the first enter.

4. PROPOSED SYSTEM

We propose a trajectory privacy-preserving framework, named TrPF, for participatory sensing. We observe that the locations on or nearby participators' trajectories may not all be sensitive, and

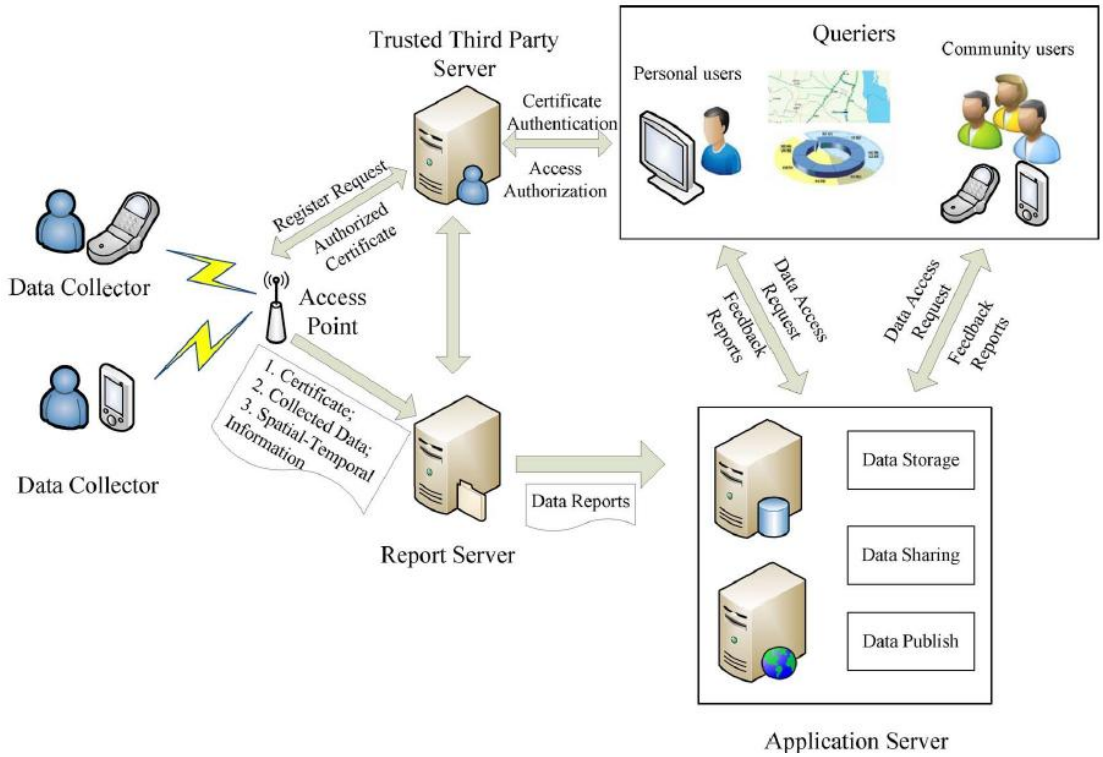
with this thought, our proposal only deals with the sensitive trajectory segments that will be discussed in the following. Moreover, mix-zones are regions where no applications can track participators' movements. Some works focused on road network mix-zones, which are not applicable in participatory sensing. For one thing, they all build mix-zones at road intersection, which may restrict the random data collection time and the number of ingress/egress locations; for another thing, the trajectory segments at the road intersection may not be sensitive, while the others would be. Therefore, we improve the theoretical mix-zones model to construct trajectory mix-zones model for protecting sensitive trajectory segments from the perspective of graph theory.

5. ADVANTAGES

1. Feasible to measure the trajectory privacy level

No ability in distinguishing related participators to specific trajectories, so that adversary knowledge is bounded.

6. ARCHITECTURE



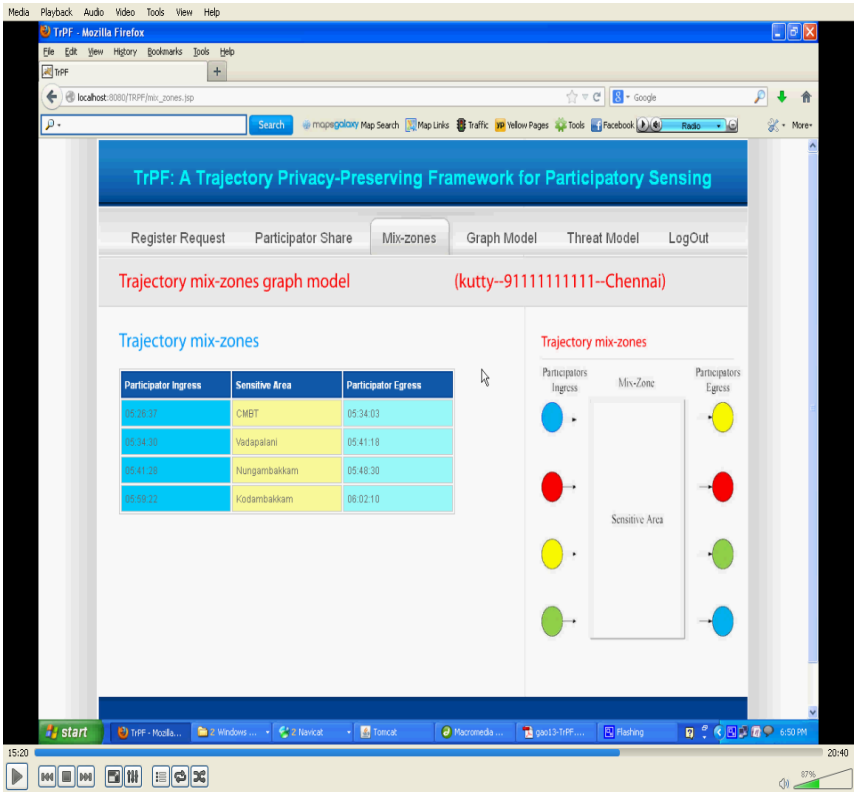
7. ALGORITHM

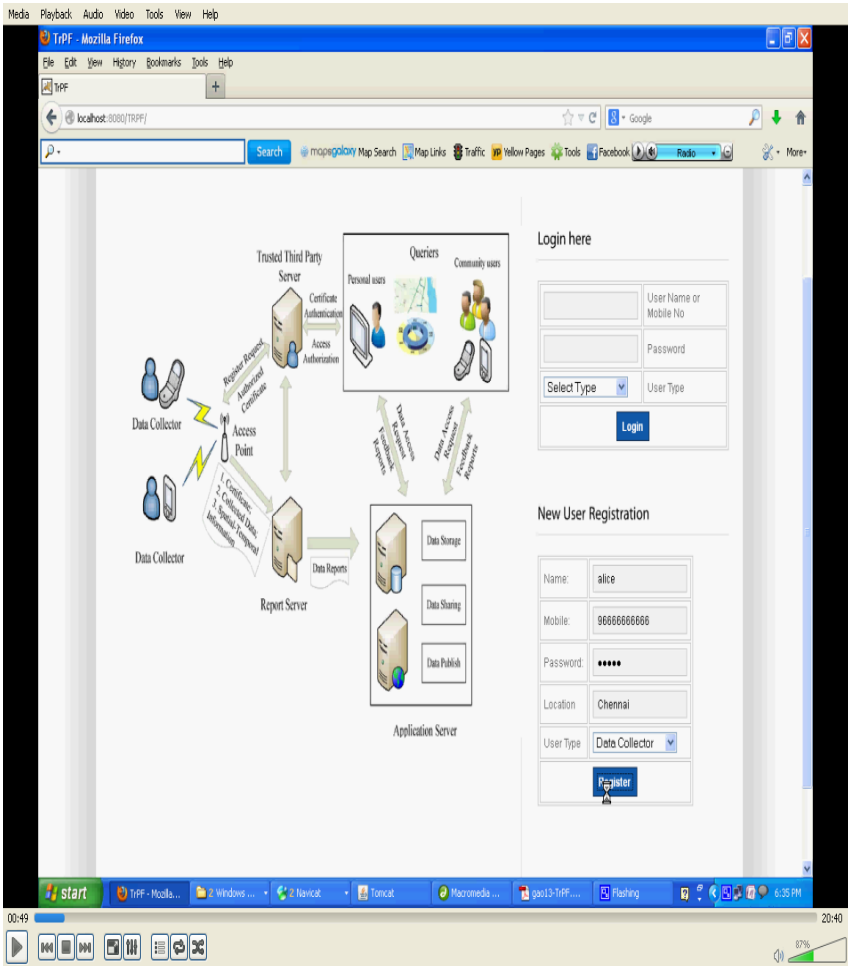
7.1. Trajectory Graph Construction

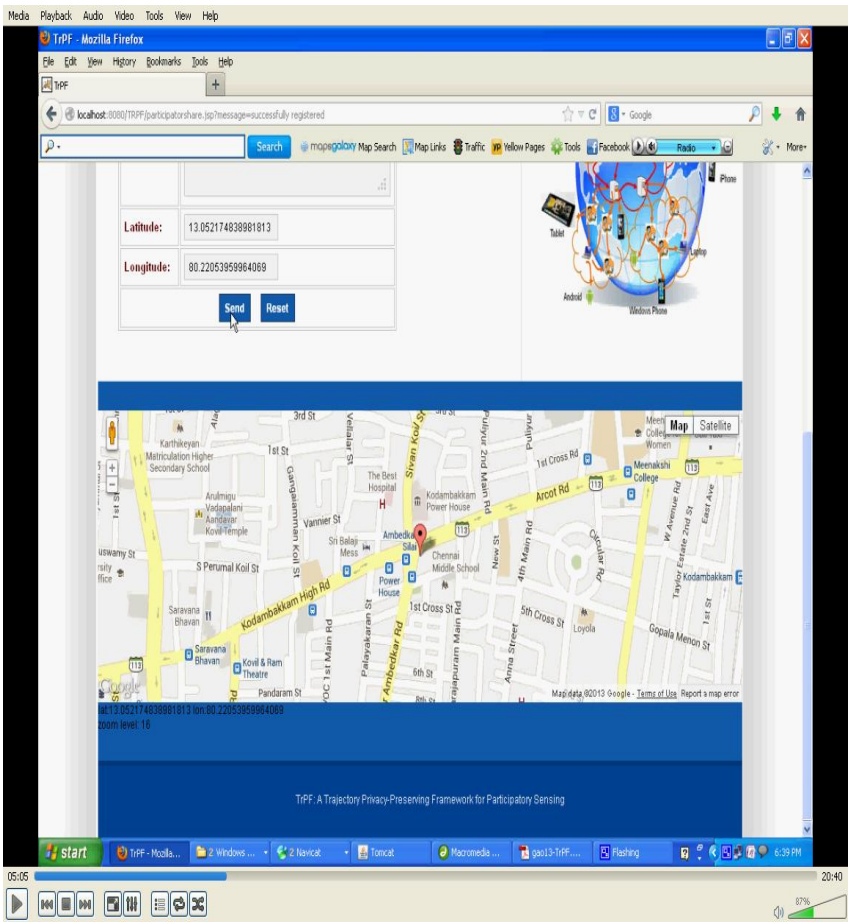
We propose to model the Trajectory Mix-zones as *Directed Weighted Graph (DWG),*which is formalized as G=(V,E) . V is the set of vertexes which are constructed by the pseudonyms provided by TTPs. A participator enters the sensitive area with a pseudonym and leaves it with another pseudonym. It can be depicted as V= {(V11,V12,…V1n),(V21,V22… V2n)} . E is the set of edges that represent the participators' trajectory mapping from the ingress to the egress in the sensitive area. As a result of pseudonym technique, there may be some difficulties for adversary to link the ingress and egress participator with the same identity..

7.2. Weight Construction Algorithm

A participator enters vi the mix-zones at time tingress(vi) and exits the mix-zones in a time interval from tj to tj+1 . Let P(vi,t) present the probability of participator vi exits the mix-zones in above-mentioned time interval [tj, tj+1]. P(vi,t) numerically equals to the probability that participator takes data collection time in mix-zones from tj- tingress(vi) to tj+1- tingress(vi).


TrPF: A Trajectory Privacy-Preserving Framework for Participatory Sensing
Register Request
Participator Share
Mix-zones
Graph Model
Threat Model
LogOut
Trajectory mix-zones graph model
(kutty--91111111111--Chennai)
Trajectory mix-zones
Participator Ingress
Sensitive Area
Sensitive Area
Participator Egress
CMBT
Vadapalani
Nungambakkam
Kodambakkam


Trusted Third Party Server
Queriers
Personal users
Community users
Data Collector
Access Point
Data Collector
Report Server
Application Server
Data Storage
Data Sharing
Data Publish
Login here
User Name or Mobile No
Password
Select Type
User Type
Login
New User Registration
Name:
alice
Mobile:
96666666666
Password:
Location
Chennai
User Type
Data Collector
Register



8. CONCLUSION

The disclosure of data collectors' trajectories poses serious threats to participators' personal privacy. It may prevent participators from data sharing. In this paper, we first propose a trajectory privacy-preserving framework TrPF for participatory sensing. Then, we propose a trajectory mix-zones graph model to protect participators' trajectories from the perspective of graph theory. We take the time factor into consideration to improve the mix-zones model. It may be more realistic in practice. Thirdly, we define the privacy metric in terms of the privacy level and privacy loss and information loss metric, and then analyze the threat models with different background knowledge. Finally, we evaluate the effectiveness and performance of our trajectory mix-zones graph model using the metric above with different parameter sets. The simulation results prove that the trajectory mix-zones graph model can protect participators' trajectories privacy effectively and reduce the information loss and costs in contrast to the other proposals. In the future, we will work on the semantic trajectory privacy problems of multiple mix-zones in detail.

REFERENCES

[1] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," IEEE Commun. Mag., vol. 48, no. 9, pp. 140–150, Sep. 2010.

[2] J. A. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, and M. B. Srivastava, "Participatory sensing," in Proc. Workshop on World-Sensor-Web (WSW'06): Mobile Device Centric Sensor Networks and Applications, 2006, pp. 117–134, ACM.

[3] A. T. Campbell, S. B. Eisenman, N. D. Lane, E. Miluzzo, and R. A. Peterson, "People-centric urban sensing," in Proc. 2nd Ann. Int. Workshop on Wireless Internet, 2006, p. 18, ACM.

[4] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, "Cartel: A distributed mobile sensor computing system," in Proc. 4th Int. Conf. Embedded Networked Sensor Systems, 2006, pp. 125–138, ACM.

[5] S. B. Eisenman, E. Miluzzo, N. D. Lane, R. A. Peterson, G. S. Ahn, and A. T. Campbell, "Bikenet: A mobile sensing system for cyclist experience mapping," ACM Trans. Sensor Netw. (TOSN), vol. 6, no. 1, p. 6, 2009.

[6] S. Reddy, A. Parker, J. Hyman, J. Burke, D. Estrin, and M. Hansen, "Image browsing, processing, and clustering for participatory sensing: Lessons from a dietsense prototype," in Proc. 4th Workshop on Embedded Networked Sensors, 2007, pp. 13–17, ACM.

[7] M. Mun, S. Reddy, K. Shilton, N. Yau, J. Burke, D. Estrin,M. Hansen, E.Howard, R.West, andP. Boda, "Peir, the personal environmental impact report, as a platform for participatory sensing systems research," in Proc. 7th Int. Conf. Mobile Systems, Applications, and Services, 2009, pp. 55–68, ACM.

[8] D. Christin, A. Reinhardt, S. Kanhere, and M. Hollick, "A survey onprivacy in mobile participatory sensing applications," J. Syst. Softw., vol. 84, no. 11, pp. 1928–1946, 2011.

[9] K. L. Huang, S. S. Kanhere, and W. Hu, "Preserving privacy in participatory sensing systems," Comput. Commun., vol. 33, no. 11, pp. 1266–1280, 2010.

[10] L.Hu and C. Shahabi, "Privacy assurance in mobile sensing networks: Go beyond trusted servers," in Proc. IEEE 8th Int. Conf. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010, pp. 613–619.

[11] L. Kazemi and C. Shahabi, "Towards preserving privacy in participatory sensing," in Proc. 9th Int. Conf. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011, pp. 328–331.

[12] R. K. Ganti, N. Pham, Y. E. Tsai, and T. F. Abdelzaher, "Poolview: Stream privacy for grassroots participatory sensing," in Proc. 6th ACM Conf. Embedded Network Sensor Systems, 2008, pp. 281–294, ACM.

[13] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, 2003.

[14] A. R. Beresford and F. Stajano, "Mix zones: User privacy in locationaware services," in Proc. 2nd IEEE Ann. Conf. Pervasive Computing and Communications Workshops, 2004, pp. 127–131, IEEE.

[15] J. Freudiger, M. Raya, M. Flegyhzi, P. Papadimitratos, and J. P. Hubaux, "Mix-zones for location privacy in vehicular networks," in Proc. 1st Int. Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 07), Vancouver, BC, Canada, 2007.

[16] B. Palanisamy and L. Liu, "Mobimix: Protecting location privacy with mix-zones over road networks," in Proc. IEEE 27th Int. Conf. Data Engineering (ICDE), 2011, pp. 494–505.

[17] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "Anonysense: Opportunistic and privacy-preserving context collection," Pervasive Comput., vol. 5013, pp. 280–297, 2008.

[18] E. De Cristofaro and C. Soriente, "Pepsi: Privacy-enhanced participatory sensing infrastructure," in Proc. ACM 4th Conf. Wireless Network Security (WiSec'11), 2011, pp. 23–28.

[19] D. Christin, M. Hollick, and M. Manulis, "Security and privacy objectives for sensing applications in wireless community networks," in Proc. IEEE 19th Int. Conf. Computer Communications and Networks (ICCCN), 2010, pp. 1–6.

[20] A. Kapadia, D. Kotz, and N. Triandopoulos, "Opportunistic sensing: Security challenges for the new paradigm," in Proc. IEEE 1st Int. Communication Systems and Networks and Workshops, 2009, pp. 1–10.

[21] C. Y. Chow and M. F. Mokbel, "Trajectory privacy in location- based services and data publication," ACM SIGKDD Explorations Newsletter, vol. 13, no. 1, pp. 19–29, 2011.

[22] L. Liu, "From data privacy to location privacy: Models and algorithms," in Proc. 33rd Int. Conf. Very Large Data Bases (VLDB2007), 2007, pp. 1429–1430, VLDB Endowment.

[23] J.Krumm, "A survey of computational location privacy," Personal and Ubiquitous Comput., vol. 13, no. 6, pp. 391–399, 2009.

[24] M. Decker, "Location privacy-an overview," in Proc. IEEE 7th Int. Conf. Mobile Business (ICMB'08), 2008, pp. 221–230.

[25] R. Shokri, J. Freudiger, and J. P. Hubaux, "A unified framework for location privacy," in Proc. 9th Int. Symp. Privacy Enhancing Technologies (PETS'10), 2010, pp. 203–214.

[26] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," in Proc. Int. Conf. Pervasive Services, 2005, pp. 88–97.

[27] H. Lu, C. S. Jensen, andM. L. Yiu, "Pad: Privacy-area aware, dummybased location privacy in mobile services," in Proc. 7th ACM Int.Workshop on Data Engineering for Wireless and Mobile Access, 2008, pp. 16–23, ACM.

[28] S. Gao, J. Ma, W. Shi, and G. Zhan, "Towards location and trajectory privacy protection in participatory sensing," in Proc.Mobile Computing, Applications and Services, Los Angles, CA, USA, 2011, pp. 381–386.

[29] L. Sweeney, "k-anonymity: Amodel for protecting privacy," Int. J. Uncertainty Fuzziness and Knowl. Based Syst., vol. 10, no. 5, pp. 557–570, 2002.

[30] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in Proc. ACM 1st Int. Conf. Mobile Systems, Applications and Services, 2003, pp. 31–42.