A Survey Paper on Crowdsensing and Privacy Techniques

Sangeeta
(sonisangam942gmail.com)
Dept. of Computer Science & Engg
Chandigarh University

Abstract- with the advancement in mobile users across the world mobile crowdsensing (MCS) is becoming popular as gathering data with less cost, less effort and quickly has become possible. In MCS you don't need to deploy different sensors to gather data from different location, participants do that for you. The openness of such system and collection of huge raw data demands paying attention to security, privacy of participants who are providing data. The main key components in MCS are its participants and the whole process of gathering data depend on participants. Without providing appropriate privacy mechanism many participants may not show interest in crow-sensing process. This paper gives a brief introduction of MCS, its applications, architecture and different privacy preserving mechanisms. Along with that incentives of participants has also discussed.

Keywords—Anonymization, crowdsensing (CS), encryption, obfuscation, participatory sensing, privacy, incentives.

1. Introduction

Internet of things (IoT) represent a concept for the way of network devices to sense and collect data from surrounding environment and share this information which can be further processed and use in different applications . [2][4]

Difinition: "The Internet of Things allows people and things to be connected Anytime, Anyplace with Anything and Anyone, ideally using Any path/network and Any service."[7] Crowdsensing uses this approach to collect information from surrounding environment without paying any extra cost on sensors. It involves ordinary people to provide raw data to them and make use of this information with further processing.

Crowdsensing serve as a building block of IoT. MCS creates a new way of extend services of IoT and provide new way exploring intelligent networks [1]. MCS requires a large number of participants to provide data. It relies on the willingness of people to participate in collecting raw data from different locations using their sensing devices sensors (i.e. camera, microphone, accelerometer, GPS, gyroscope etc.) which may me their mobile phone, laptop and IoT devices like wearable. Main advantage of MCS application is that given huge numbers of cell phone users, different kind of data can be collected in a fast, easy and cost effective manner. As there is no need of using additional sensors it aromatically decrease cost of deploying sensors at different location to collect data. After deploying static sensors there is constant need of their maintenance, repair. This requires more people as manual work is more here. Where in crowdsensing people are proving raw data using their own cell phones. There is no need for providing internet connectivity (i.e. every participant using their own mobile data) to collect and submit data. For example, if any CS application requires traffic information from an area, they have the potential to collect real time data from different roads. This task can be done in an economical feasible way without spending any extra cost on deploying sensors across roads. CS based traffic congestion applications are capable of doing this. Similarly measuring pollution data from different city, state via a CS application will allow the detection of abnormal level which is difficult with current static environmental sensing stations.

MCS use existing sensors of participant’s mobile phones to collect data based on the involvement of participants; crowdsensing can be categorized in two ways: *participatory sensing* and *opportunistic sensing* [2]. Participatory sensing is where user willingly participates in contributing information. And opportunistic sensing is, where data is automatically sensed and collected by CS applications. CS application can be classified into two categories, (i)the applications used in personal daily life, and (ii) the applications used in public infrastructure construction as shown in Figure.1. There are different existing CS applications which gather data to use for special purpose.

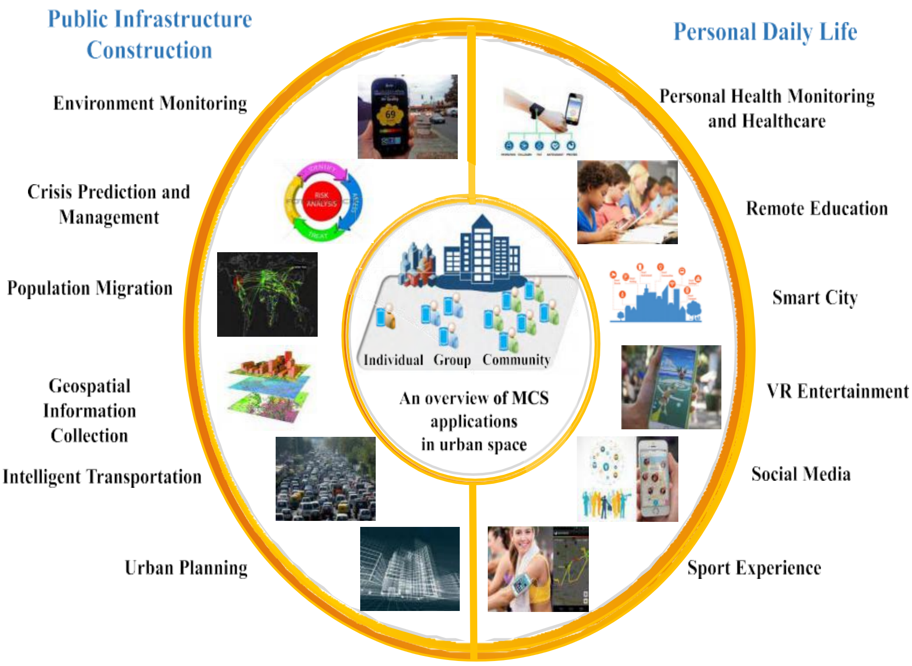
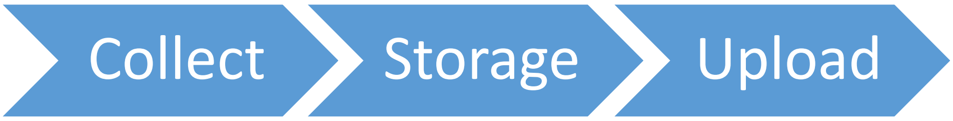

Public Infrastructure Construction
Personal Daily Life
Environment Monitoring
Crisis Prediction and Management
Population Migration
Geospatial Information Collection
Intelligent Transportation
Urban Planning
Personal Health Monitoring and Healthcare
Remote Education
Smart City
VR Entertainment
Social Media
Sport Experience
Individual Group Community
An overview of MCS applications in urban space

Figure 1. Applications of MCS[5]

For example, NoiseTube, Ear-Phone and NoiseMap, in these apps mobile phone microphones are used to measure the surrounding noise level [6]. Noise samples are used to make noise pollution map to understand the relationship between noise level and listening problems.

1.1 Procedure of data collection

We can divide procedure of collecting data into three phases:



Three models used in this procedure: (1) end user, who contribute into collecting raw data as required, (2) service provider who process this collected information further to generate service from this , (3) data requester who request this service[8].

Participants involvement can be classified into two processes: (i) tasking process and, (ii) reporting process [1][9]. In tasking process, tasks are informed to mobile user for any CS application campaign. Before collecting data all participants are informed about their requirements (location, sensors required, special skills required, sensing time window, and reporting time window). All this information is priory send to participants so they know what requirements, sensors are needed and if they interested can participate. This also helps in figuring out the numbers of participants interested. Tasking process can be repeated several times according to user and system. In reporting process participants send collected sensed data to processing infrastructure. Reported data may contain measurements, location, time, and physiological signals.

1.2 Challenges

Involvement of people in the process of CS application leads to a new challenge. Contributing to any CS Application campaign requires participants to put efforts and devote time. And collection and updating process of data use mobile data, its battery and communication bandwidth. To insure that people participate in gathering data their security, privacy should be insured. There can be applications which require special skills which make recruitment of participants more difficult. For example a CS application required sample of a specific plant species to fulfil this requirement requester wants to recruit those participants who have some knowledge of botany. In MCS to obtain accurate results there should be participants who are (i) sufficient in amount and (ii) as per required for the task [6]. Other than participants recruitment, their privacy and security there are more challenges [9]:

1. Privacy Protection
2. Anonymous tasking
3. Anonymous data reporting
4. Data authenticity
5. System integrity
6. Preventing data suppression
7. Participation
8. Limited recourse

1.3 Security Requirement

Crowdsensing security requirement includes participant's privacy, incentives, communication, task server, access control, data verification [17].

Participant's Privacy: to encourage user participation in Crowdsensing their privacy should be preserved. Many techniques (anonymization, obfuscation, cloaking, encryption techniques etc.) have been introduced to insure user privacy. Some techniques works on internal level and some on external level as explained in table 1 also.

Incentive mechanism: contribution in any CS application requires user's time, effort, mobile data and others factors. In return of these efforts user should provide appropriate incentives which encourage them to take participation in any CS campaign.

Communication security: system entities (task initiator, group manager, identity provider) should be protected from any modification. Their confidentiality, authentication and integrity should be preserved.

Verification of data**:** As people are providing all the data, data truth value should be checked so that any faulty data can be recognized.

Access control: Actions of end users as per the policies

2. Literature Review

Security of participants in CS is very important as they are providing data for application campaign to run. Security and privacy of users is discussed in [1][9][10][11][12][13][14][15][16][17]. Use of obfuscation and anonymization techniques has been discussed in [1][9][16][17]. Cloaking has been discussed in [16].

Anonymization, encryption and obfuscation are discussed in [1], where their use and drawbacks are explained. Anonymization in task and reporting process is discussed, how anonymization is useful in user privacy concern and anonymization techniques like anonymous authentication, direct tasking and attribute modification are explained. These techniques insure user privacy to a certain point but quality of data has been compromised. Group signature and double encryption can limit the rate of user authentication. Both techniques can prevent user privacy from external attacks.

A general framework AnonySense [11][12] is used for user protection. This can use for both process tasking and reporting to provide secure tasking in MCS. Using AnonySense nodes receive task anonymously. In opportunistic sensing user has no control over how much information they are sharing so AnonySense helps in keeping their identity anonymous. Nodes are not linked to each other with nodes which are sending data. And a multi-layered protection approach is used. For this tessellation technique is used in [1]. Blurring technique based tessellation is also described.

Whole work of CS depends on its user's participation. When data required for any CS application campaign is started and people are tasked through system. And id participants are interested they contribute in data collection. To make people contribute in data collection proper incentive mechanisms [18] should apply I.e. rewards and payment. Participants should have control over their payment for different tasks. A Stackelberg game as mechanism is used in which user ask for payment they want for task.

Recruiting participants [6] for different task in tough as different task require different skills in users which make recruitment task difficult. Different techniques on recruiting users are proposed. Online recruitment of user can be based on qualification, expertise based, budget based, reputation based and coverage based.

3. Privacy Preserving Mechanism

A good technique which insures participant's privacy is required to encourage more people to take participation in CS application campaigns. While sending data or getting informed about data any diversity can have access to sensitive information of participants. So having a good preserving technique is important to add more people to contribute into campaign. Different mechanisms are:

A. Anonymization Techniques

In this approach participant identity is not revealed. They authenticate themself anonymously. In this approach users don't need to reveal their location, name or other information. Authorization is done anonymously. There are different ways of anonymization technique using which user privacy can be protected.

Anonymous Authentication

As described in [1][11][12] AnonySense Architecture used to maintain privacy of end users. Different tasks to user are post repeatably and they can download these tasks from these tasking services. Tasks are not sending to each user so their sensitive information are not required at that time. Architecture for anonymization is AAV (Anonymous Authentication of User), in this information submit by user is authenticating without knowing their sensitive information. In anonymous authentication, no extra information is required which makes it less complex.

Direct Tasking

in this approach, main focus is on not revealing user location. To task user their identification are used but without using their location. Anonymization network is used name Tor [13]. This

network is used to anonymize TCS based application. Direct location is distributed approach

as there is no central node. This scheme selects only those participants who meets requirement of task. This approach is for tasking process of CS applications.

Attribute Based

In this approach some attribute of end users are used to authenticate with system without giving away any personal information. These attributes may be user's sensor, their group. Crystallographic techniques are used to are used to show that they belong to a certain group instead of using any sensitive information. For example a group certificate can be used to confirm that any user belong to that group or not, here it is irrelevant to use any personal information.[1][15]

Technique	**System Type**	**Protection provided**	**Complexity**	**Energy requirement**
Anonymous Authentication	Distributive	External/Internal	Low	Low
Direct tasking	Distributive	External/Internal	Low	Low
Attribute Based	Centralized	External only	High	High

Table. 1 Anonymization Techniques

B. Attribute Modification: obfuscation

Main focus of this approach is to modify user information in a way that any third person cannot know the actual values [1]. This approach helps in protecting the association of end users and their sensitive information. This is mainly used to modify user location [14]. A double encryption technique is used to modify actual location of end user and also enhance quality of data. Unlike anonymization technique it is least interested in knowing other users data. So these can applied to mobile phones to without contacting other nodes in system.

C. Encryption Based Mechanisms

Using photographic techniques in MCS is useful because these techniques can run on mobile phones. But they require high energy on mobile phones. Different types of encryption techniques are: group signature and double encryption. [1][11]

Group Signature: Main aim of this approach is to prevent user sensed data from any adversary. In this, authentication team sends *certificates* to already registered users. When end users have data to send they use this certificate for encryption. Server accepts only those reports which are signed by an appropriate certificate generated earlier. This ensures user privacy and don't demand any personal information to register user into system. Group signature is a distributive approach. Main drawback of this approach is any internal node can have access to user data. So it only provides protection from external attacks.

Double Encryption: Two servers are required for this approach. First, identification proxy and other is application server. Application server used to encrypt the sensed data and public key of identification proxy is used to encrypt its identification data. Validation of end user signature is done by identification proxy. Only application server can decrypt the data. This mechanism is distributive approach as there is no central entity. This approach provides protection from external attacks as administrators have knowledge of end user's data.

D. Cloaking

This approach is helpful where sensing task is assigned based on the location of the user. Cloaking is used to obfuscate location of users. In this approach, tasking server handle user locations, and cloaked locations are used instead of their actual locations. In [16] cloaking is used for spatial task assignment. A two stage approached is used where in first stage end users tasked by task assignment server using cloaked locations. For this different cloaked methods are used. In second stage, end users use their own location not obfuscation. At different stages greedy algorithms are used for optimization.

4. Conclusion

This paper gives a brief introduction of mobile crowdsensing, its applications, and user's recruitment. Different application and examples are provided which clears the use of MCS in different areas. And show how it is a fast and feasible solution to gather information without the hassle of deploying sensors. Participants here are key element and for safety of these different mechanisms of user privacy are briefly explained. To provide safety to participants different anonymous technique, encryption based technique and attribute modification technique are defined.

5. Reference

1. Vergara-Laurens, I. J., Jaimes, L. G., & Labrador, M. A. (2017). Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. *IEEE Internet of Things Journal*, *4*(4), 855-869.

2. Liu, J., Shen, H., & Zhang, X. (2016, August). A survey of mobile crowdsensing techniques: A critical component for the internet of things. In *Computer Communication and Networks (ICCCN), 2016 25th International Conference on* (pp. 1-6). IEEE.

3. Datta, S. K., Da Costa, R. P. F., Bonnet, C., & Härri, J. (2016, June). oneM2M architecture based IoT framework for mobile crowd sensing in smart cities. In *Networks and Communications (EuCNC), 2016 European Conference on*(pp. 168-173). IEEE.

4. Sharma, V., & Tiwari, R. (2016). A review paper on IOT & It's Smart Applications. *International Journal of Science, Engineering and Technology Research (IJSETR)*, *5*(2).

5. Shu, L., Chen, Y., Huo, Z., Bergmann, N., & Wang, L. (2017). When mobile crowd sensing meets traditional industry. *IEEE Access*. (pic)

6. Davari, M., & Amintoosi, H. (2016, October). A survey on participant recruitment in crowdsensing systems. In *Computer and Knowledge Engineering (ICCKE), 2016 6th International Conference on* (pp. 286-291). IEEE.

7. P. Guillemin and P. Friess. Internet of things strategic research roadmap. The Cluster of European Research Projects, Tech. Rep., Sept. 2009.
8. Liu, J., Bic, L., Gong, H., & Zhan, S. (2016). Data collection for mobile crowdsensing in the presence of selfishness. *EURASIP journal on wireless communications and networking*, *2016*(1), 82.
9. Kapadia, A., Kotz, D., & Triandopoulos, N. (2009, January). Opportunistic sensing: Security challenges for the new paradigm. In *Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International* (pp. 1-10). IEEE.
10. D. M. Konidala, R. H. Deng, Y. Li, H. C. Lau, and S. E. Fienberg, “Anonymous authentication of visitors for mobile crowd sensing at amusement parks,” in Information Security Practice and Experience. Heidelberg, Germany: Springer, 2013, pp. 174–188.
11. A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, “Anonysense: Opportunistic and privacy-preserving context collection,” in Proc. 6th Int. Conf. Mobile Syst. Appl. Services (MobiSys), Sydney, NSW, Australia, 2008, pp. 280–297
12. C. Cornelius et al., “Anonysense: Privacy-aware people-centric sensing,” in Proc. 6th Int. Conf. Mobile Syst. Appl. Services (MobiSys), Breckenridge, CO, USA, Jun. 2008, pp. 211–224.
13. R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The secondgeneration onion router,” in Proc. 13th Conf. USENIX Security Symp., Berkeley, CA, USA, 2004, p. 21.
14. Vergara, I. (2014). A hybrid privacy-preserving mechanism for participatory sensing systems (Doctoral dissertation, University of South Florida).
15. B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Achieving guaranteed anonymity in GPS traces via uncertainty-aware path cloaking,” IEEE Trans. Mobile Comput., vol. 9, no. 8, pp. 1089–1107, Aug. 2010.
16. Pournajaf, L., Xiong, L., Sunderam, V., & Goryczka, S. (2014, July). Spatial task assignment for crowd sensing with cloaked locations. In *Mobile Data Management (MDM), 2014 IEEE 15th International Conference on* (Vol. 1, pp. 73-82). IEEE.
17. Gisdakis, S., Giannetsos, T., & Papadimitratos, P. (2016). Security, privacy, and incentive provision for mobile crowd sensing systems. *IEEE Internet of Things Journal*, *3*(5), 839-853.
18. Yang, D., Xue, G., Fang, X., & Tang, J. (2016). Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones. *IEEE/ACM Transactions on Networking (TON)*, *24*(3), 1732-1744.