Crowd Sensing

Subjects: Engineering, Electrical & Electronic
Contributor: Yuichi Sei

Crowd sensing (also known as participatory sensing, or mobile crowdsensing) is a means of collecting people's surrounding information via mobile sensing devices. Its highly expressive and powerful sensing capabilities can carry out a big sensing project by fragmenting tasks into small pieces. The key to success is to get more participants to collect higher quality data.

Keywords: Participatory sensing ; Incentive Mechanism ; Trustworthiness ; Differential privacy

1. Introduction

Today's smartphones are powerful minicomputers that contain an impressive array of sensing components such as cameras or accelerometers, with the ability to collect and analyze users' surrounding information [1] (Figure 1). Extensive research shows that as well as through mobile phones, data is collected through different means of transportation, such as trains, cars, or bicycles. Such information collection is referred to as participatory sensing or mobile crowdsensing. Many studies have been conducted on crowd sensing. For example, Bridgelall et al. proposed a system that detects anomaly locations of roadways using participatory vehicle sensors [2]. Kozu et al. developed a hazard map of bicycle accidents based on data from the accelerometers of participatory smartphones [3].

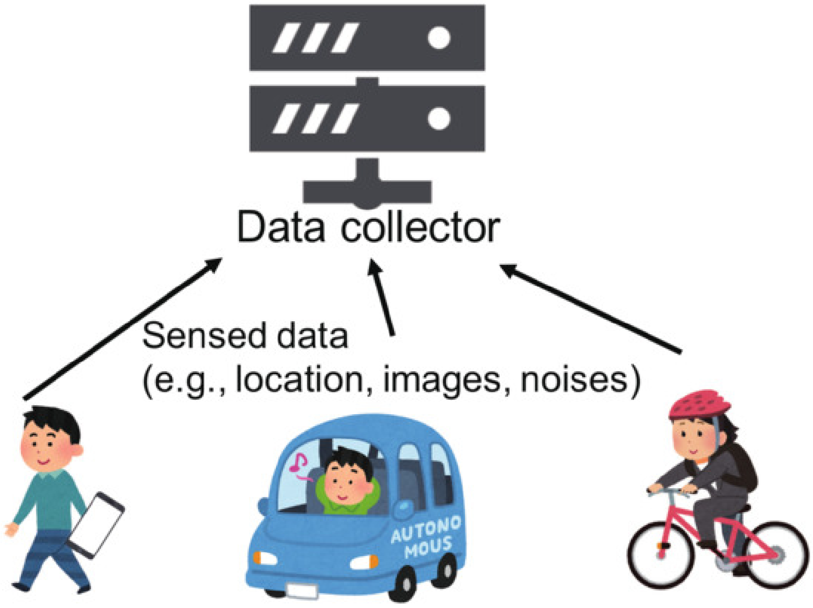

Figure 1. Participatory sensing.

Although high participation is necessary for crowd sensing to be successful, participants may be discouraged by privacy concerns or having to use extra battery power. As such, it is necessary to develop a participatory sensing method featuring both low battery power requirements and high privacy protection [4]. To avoid potential undesired side effects of this data analysis method, such as privacy violations, considerable research has been conducted over the last decade to develop participatory sensing that looks to preserve privacy while analyzing participants' surrounding information. To protect privacy, each participant perturbs the sensed data in his or her device, then the perturbed data is reported to the data collector. The data collector estimates the true data distribution from the reported data.

2. Datas

Several frameworks use geotagged posts of Twitter and/or Instagram [5][6]. Although Twitter and Instagram users disclose their locations intentionally, a privacy mechanism could motivate users to share more geotagged posts.

Several privacy-preserving techniques have been proposed for crowd sensing. By perturbing data based on ϵ-differential privacy [7], privacy leakage can be controlled [8].

An incentive mechanism is a very important issue for crowd sensing. If the incentive mechanism works well, it is expected that the crowd sensing system can gather many participants even if the privacy levels are relatively low. On the other hand, if there are no good incentive mechanisms, the privacy levels should be higher to recruit many participants.

Pouryazdan et al. proposed three new metrics to quantify the performance of mobile crowdsensing [9]: platform utility, user utility, and false payments. Using these metrics, they showed that data trustworthiness and data utility could be improved by collaborative reputation scores, which are calculated based on statistical reputation scores and vote-based reputation scores. Pouryazdan et al. also proposed a gamification incentive mechanism [10]. They formulated a game theory approach and showed that their mechanism could improve data trustworthiness greatly. Moreover, the proposed mechanism could prevent the data collector from paying rewards to malicious participants.

Suliman et al. proposed an incentive-compatible mechanism for group recruitment [11]. They considered the greediness of participants of in-group recruitment, and the proposed mechanism can increase the quality of the collected information by selecting participants who are expected to give high-quality data at a low cost.

There are several important mobile crowdsensing survey articles. Capponi et al. analyzed mobile crowdsensing studies and outlined future research directions [12]. Liu et al. [13] focused on privacy and security, resource optimization, and incentive mechanisms. They argued that ensuring privacy and trustworthiness is important.

Privacy-preserving mechanisms could be combined with such incentive mechanisms to increase participants while maintaining a low cost.

References

1. Emiliano Miluzzo; Nicholas D. Lane; Kristóf Fodor; Ronald Peterson; Hong Lu; Mirco Musolesi; Shane B. Eisenman; Xiao Zheng; Andrew T. Campbell; Sensing meets mobile social networks. *Proceedings of the 6th ACM Conference on Bioinformatics, Computational Biology and Health Informatics - BCB '15* **2008**, *1*, 337, 10.1145/1460412.1460445.
2. Raj Bridgelall; Denver Tolliver; Accuracy Enhancement of Anomaly Localization with Participatory Sensing Vehicles. *Sensors* **2020**, *20*, 409, 10.3390/s20020409.
3. Ryohei Kozu; Takahiro Kawamura; Shusaku Egami; Yuichi Sei; Yasuyuki Tahara; Akihiko Ohsuga; User Participatory Construction of Open Hazard Data for Preventing Bicycle Accidents. *Joint International Semantic Technology Conference (JIST)* **2017**, *10675*, 289-303, 10.1007/978-3-319-70682-5_20.
4. Ngo Manh Khoi; Sven Casteleyn; Mehdi Moradi; Edzer Pebesma; Do Monetary Incentives Influence Users' Behavior in Participatory Sensing?. *Sensors* **2018**, *18*, 1426, 10.3390/s18051426.
5. Daniel Rodríguez Domínguez; Rebeca P. Diaz Redondo; Ana Fernández Vilas; Mohamed Ben Khalifa; Sensing the city with Instagram: Clustering geolocated data for outlier detection. *Expert Systems with Applications* **2017**, *78*, 319-333, 10.1016/j.eswa.2017.02.018.
6. Monica Aguilar Igartua; Florina Almenares Mendoza; Rebeca P. Diaz Redondo; Manuela I. Martin Vicente; Jordi Forne; Celeste Campo; Ana Fernandez-Vilas; Luis J. De La Cruz Llopis; Carlos Garcia-Rubio; Andres Marin Lopez; et al. INRISCO: INcident monitoRing in Smart COmmunities. *IEEE Access* **2020**, *8*, 72435-72460, 10.1109/access.2020.2987483.
7. Cynthia Dwork; Frank McSherry; Kobbi Nissim; Adam Smith; Calibrating Noise to Sensitivity in Private Data Analysis. *Journal of Privacy and Confidentiality* **2017**, *7*, 17-51, 10.29012/jpc.v7i3.405.
8. Yuichi Sei; Akihiko Ohsuga; Differential Private Data Collection and Analysis Based on Randomized Multiple Dummies for Untrusted Mobile Crowdsensing. *IEEE Transactions on Information Forensics and Security* **2017**, *12*, 926-939, 10.1109/tifs.2016.2632069.
9. Maryam Pouryazdan; Burak Kantarci; Tolga Soyata; Luca Foschini; Houbing Song; Quantifying User Reputation Scores, Data Trustworthiness, and User Incentives in Mobile Crowd-Sensing. *IEEE Access* **2017**, *5*, 1382-1397, 10.1109/access.2017.2660461.
10. Maryam Pouryazdan; Claudio Fiandrino; Burak Kantarci; Tolga Soyata; Dzmitry Kliazovich; Pascal Bouvry; Intelligent Gaming for Mobile Crowd-Sensing Participants to Acquire Trustworthy Big Data in the Internet of Things. *IEEE Access* **2017**, *5*, 22209-22223, 10.1109/access.2017.2762238.

11. Ahmed Suliman; Hadi Otrok; Rabeb Mizouni; Shakti Singh; Anis Ouali; A greedy-proof incentive-compatible mechanism for group recruitment in mobile crowd sensing. *Future Generation Computer Systems* **2019**, *101*, 1158-1167, 10.1016/j.future.2019.07.060.
12. Andrea Capponi; Claudio Fiandrino; Burak Kantarci; Luca Foschini; Dzmitry Kliazovich; Pascal Bouvry; A Survey on Mobile Crowdsensing Systems: Challenges, Solutions, and Opportunities. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 2419-2465, 10.1109/comst.2019.2914030.
13. Yutong Liu; Linghe Kong; Guihai Chen; Data-Oriented Mobile Crowdsensing: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials* **2019**, *21*, 2849-2885, 10.1109/comst.2019.2910855.
