

Crowdsensing: Socio-Technical Challenges and Opportunities

Javeria Noureen

COMSATS Institute of Information Technology,
Sahiwal, Pakistan

Muhammad Asif

University of Lahore,
Pakpattan Campus, Pakistan

Abstract—With the advancement in mobile technology, the sensing and computational capability of mobile devices is increasing. The sensors in mobile devices are being used in a variety of ways to sense and actuate. Mobile crowdsensing is a paradigm that involves ordinary people to participate in a sensing task. This sensing model has the capability to provide a new vision of people centric sensing as a service. This research work reviewed different domains utilizing mobile crowdsensing for solving different domain specific problems. Mobile crowd sensing model is also posing different socio-technical challenges which needs to be addressed. The research work reviewed and analyzed a variety of socio-technical challenges of mobile crowdsensing and possible solutions presented by different studies. There are different socio-technical challenges but the challenge of privacy in crowdsensing requires extra measures to realize the vision of mobile crowdsensing.

Keywords—Crowdsensing; sensing devices; privacy; smart phones

I. INTRODUCTION

The sensing capability of mobile devices is increasing day by day. The use of sensor enabled mobile devices is becoming ubiquitous. Researchers and engineers are seeking a variety of ways where sensing capabilities of mobile devices can be utilized. Mobile Crowdsensing (MCS) is an emerging sensing model which primarily depends on the strength of the people's sensor enable mobile devices to sense the data for a particular sensing task. Crowdsensing permits a huge number of sensing devices that share the collected data by the purpose to enumerate a phenomena of mutual interest [1]. Mobile devices are equipped with different sensors such as camera, GPS, digital compass, microphone, light sensor, accelerometer, and bluetooth as proximity sensor [2]. Crowdsensing empowers a large amount of mobile phones to be utilized for trading data among their clients, as well as for activities which might have an enormous societal impact. Mobile crowdsensing permits a large amount of mobile phone clients to share native knowledge (e.g., local information, ambient context, noise level, and traffic conditions) collected by their sensor-enhanced devices[3]. Mobile Crowdsensing has two distinct feature are as: 1) Implicit and explicit participation; 2) user-participant data sources [4].

Mobile crowdsensing has various perspectives and defined in a variety of way as defined by Guo et al, "a new sensing paradigm that empowers ordinary citizens to contribute data sensed or generated from their mobile devices, aggregates and fuses the data in the cloud for crowd intelligence extraction and people-centric service delivery" [5, 6]. The

intrinsic nature of mobility in MCS allows a new and fast developing sensing model. It has the ability to acquire local knowledge through sensor-enhanced mobile devices – e.g., location, personal and surrounding context, noise level, traffic conditions, and in the future more specialized information such as pollution – and the possibility to share this knowledge within the social sphere, healthcare providers, and utility providers [5].

Mobile Crowdsensing (MCS) permits the large amount of cell phone clients share native knowledge such as (local information, ambient context, noise level, and traffic conditions) collected by their sensor-enhanced devices, and more information can be collects in the cloud for large scale sensing and community intelligence mining [7]. This model generally focus on the crowd powered data collection and processing [8][9].

Section II describes different application domains of crowdsensing and different socio-technical challenges are described in Section III. Privacy challenges and possible solutions are elaborated in Section IV and Section V concludes the paper.

II. CROWDSENSING APPLICATIONS DOMAINS

Crowdsensing have different applications which is divided into three categories like (a) Infrastructure monitoring, (b) Social networking monitoring and, (c) Environmental monitoring [1]. In the infrastructure monitoring (Road monitoring, Traffic control/congestion, Road condition, and Individual travel planning and public transport) are further discussed. In Social networking monitoring (cinemas and historical places) and Environmental monitoring (natural environment, air pollution, walking, driving, level of water, wildfire habitats, noise pollution) are discussed [6].

A. Environmental Monitoring

The crowdsensing paradigm is being utilized for environment monitoring, nature preservation, air pollution and many others. The Personal Environmental Impact Report (PEIR) project [10] utilize sensors in mobile phones to construct a framework which allows customized environmental effect reports, which follow how the activities of people's affect both their experience and their impact to troubles. The objective of the project was to evaluate the effect of individual user/public participation to observe the environment like contamination, climate and noise tracking and so on. Noise pollution creates problems in fitness and in quality of life, quoting high blood pressure, hearing damage,

frustration, and others [11]. The European Commission mandates the generation of noise to collect data and create noise maps. Yet, the government efforts are limited because the deployed sensing nodes cannot protect all regions of the city. A noise map is a graphic demonstration of the sound level distribution. To create a noise map, shared measurements were used. In their daily lives, NoiseTube [12] could measure personal exposure to environmental noise. EarPhone [13] was also a participatory noise mapping system. The END (European Noise Directive) [14] states environmental noise such as “*unwanted or harmful outdoor sound created by human activities, including noise emitted by means of transport, road traffic, rail traffic, air traffic, and from sites of industrial activity*”.

Mobile phones were also used to collect the information of on the road diesel trace to study community exposure to urban air pollution [15]. ExposureSense [16] explored the integration of Wireless Sensor Network and participatory sensing paradigms for personal air quality exposure measurement. The BikeNet application [17] could measure CO₂ level and also report the path of a cyclist activity.

B. Transportation and traffic planning

The traffic congestion remains a serious global problem; for example, congestion alone could impact both the environment and human productivity (e.g., wasted hours due to congestion) [3]. As GPS based vehicles which is equipped with computers travels, it periodically records the present time and location and use wireless network to send information to a server. GPS receiver on mobile phone can provide the location information. Wi-Fi can also be used to send data to a nearest wireless get to point. Traffic deferrals and congestion are a prime cause of disorganization, squandered fuel, and commuter frustration [18].

To report the road and traffic condition, mobile phones can be utilized. In Nericell [19], different embedded devices such as accelerometer, microphone, and positioning system being utilized to identify as well as focus on transportation and road situations, for example quality of road (potholes, bumps), and driving behavior (braking and honking or beeping) [20]. A potholes [21] application can find fleabags in streets using the crowdsourced shaking and position information collected from smart phones. VTrack [18] was a system that used mobile phones to correctly estimate the traffic time between different locations. WreckWatch [22] removing the interruption among accident occurrence and primary responder dispatcher and automatically detect the accidents and send the notifications to a server. T-Share [23] was a taxi ridesharing service that can produce optimized ridesharing schedules based on crowd-powered data.

C. Social Networking Monitoring

Social networks are popular way of communications with other who are members of the same social networking application and share information between the social groups [24]. Social media (i.e. Twitter, Facebook, MySpace, and LinkedIn) are used for communication. Millions of people take part frequently within online social networks and share their views, their ideas about any subject. Social sensing system used to get and share social information among

friends, social clusters and communities [25]. There are two kinds of social sensing like implicit sensing and explicit sensing. In implicit social sensing always concerns on e-business sites like Amazon [26] which evaluate the purchasing behavior of their customers. While explicit social sensing concerns the existing study concentrates on the very famous tools for example, Flickr, Twitter and Facebook [27]. The Dartmouth CenceMe [28] development is *examining the utilization of sensors in the mobile phone to mechanically categorize actions in individuals' existence, this known as sensing existence.*

D. Health Care and Public Safety

In health care, public health and personal health is monitored. Mobile crowdsensing can be used to monitor the different diseases. Personal sensing systems collects people's data to monitor their health, routine life and physical activities such as heart rate, blood pressure, sugar level etc. [25]. Sensor-enabled cell phones utilized for the observation of physiological condition and well-being of patients utilizing inserted or exterior sensors such as wearable accelerometers, or air contamination sensors [29]. The DietSense [30] support the people who wants to lose their weight. This system allows the people to report or share their food choices via pictures and sound sample to get suggestions from online experts for weight loss. HealthAware [31] is also a similar kind of system that persuade people to participate in improving health through people centric feedback.

Public safety is about detecting or protecting the citizens from the events (e.g., crimes, disasters) that could be danger for the safety of the citizens. By evaluating the large number of geo tagged Twitter messages posted from mobile devices, Lee [32] proposed a method to detect the curious crowded spaces such as (a terrorist activity). SAIS (Smartphone Augmented Infrastructure Sensing) [33], also confirm public security in smart cities utilizing maintainable design. SAIS collects data from citizens and authorities for the security actions, using this information a dashboard smart phone application is produced which it helps each other to make better situation-awareness. Participatory mobile phone sensing systems can also be used for helping disaster relief [34]. Large-scale mobile phone can analyze the user data before and after earthquake movement behaviors, they construct a model and this model could predict community responses to future disasters. Similarly, in [35] Twitter could give near real-time report of earthquakes region by observing geo tagged user posts.

III. CROWDSENSING CHALLENGES

Crowdsensing has many challenges in addition to privacy and security challenges [36]. We focus on the social and technical challenges and we also outline general solutions. Some are as follows:

- Local analytics is key challenge in discovering searching and designing algorithms is to accomplish the imaginary function. Data mediation is one of the class of functions, for example clarifying of outliers, noise exclusion, or covering data gaps. For instance, GPS sample cannot be able to obtain correct or missing

(because of absence of observable pathway), in which occasion outliers ought to be eliminating or omitted specimens extrapolated.

- MCS applications depend on the examining data from accumulation of mobile devices, distinguishing spatial temporal designs. When a physical or social phenomenon is being observed these designs could helpful for constructing patterns. The challenge in recognizing designs from huge amounts of information is normally application- specific. It also contains data mining algorithms.
- Data storage in database is one of the conventional techniques of data mining. For the patterns detection different mining algorithms can be used for implementation against database.
- If sum of consistent data participation is excessively for storage, or application needs fast detection of patterns, stream data mining algorithms might be essential. Such algorithms take continuous data streams as an input and detect patterns, without the requirement of the first store of the data.
- The 3-tier system architecture [37] also have some challenges are as follows: Virtualization Overhead is the main challenge in system architecture.
- Configuration and performance is another challenge of inter-VM communication. Inter-VM communication performance is comparatively low when it is compare to inter-process communication.
- Migration-induced Reconfiguration is likewise challenges. With constraints of Non IP-based results , the Host Identify Protocol [38] are intended to scrape mind, still such protocols are essential for the evaluation of real networks.
- Standardization of Sensing Interfaces is a challenge.
- Different crowdsensing applications can construct similar sensor data, but use diverse system or model rate.
- Another challenge is how to provide valuable incentive mechanisms that allows honest contributions in mobile crowdsensing and computing becomes a critical challenge [6]. Recently, numerous game theory approaches [39-41] have been proposed for mobile crowdsensing and computing to encourage and reward truthful contributions. These game theory techniques are usually based on auction mechanisms, however slightly complex to apply in a fully distributed and time evolving system. Therefore, for a highly dynamic mobile crowdsensing and computing system, there is still need for new incentive and pricing mechanisms to attract, inspire, and reward truthful and high-quality sensing data contributors.
- Data delivery in transient network is a challenge in mobile crowdsensing, how to dispatch the sensed data from distributed participants to the backend server is another challenge because of an assortment of mobile crowdsensing and computing characteristics, for example the low bandwidth of wireless communication, recurrent network apportioning due to human mobility, and huge number of energy-constrained devices. Whereas this is also a well-known research challenge in both wireless sensor networks and general mobile systems.
- We have to consider an essential issue to mobile phone sensing (still no need of great tended): provided a block of focuses key steps or a focuses area, a set about mobile phones and a time limit, we discover a sensing schedule (which identifies sensing for each mobile phone) so aggregate energy utilization will minimize to subject to a coverage restriction [42]. Scheduling algorithms can solve this trouble and used sensing servers to arrange sensing events of mobile phones (an incentive mechanism use recruited). Note that opportunistic sensing applications will only use the scheduling algorithms; later on, in participatory sensing applications; mobile phone users control sensing task by manually.
- Since a more specialized point of view, one of the important difficulties is discovering a decent harmony between framework versatility and detecting accuracy for far reaching sending situations. In such another socio-specialized framework, the sorts of assets are overall different, crossing from figuring ones (system transmission capacity, memory, CPU, and so on.) to people (numeral individuals included, human consideration, specific aptitudes to contribute, and so on.), with these lines, it is difficult to entirely control them.
- Finally, the trade-offs are similar to the trade-offs that occur when using an ad hoc network instead of a fixed infrastructure network: it is easier to install and could be used in areas where establishing a fixed infrastructure is difficult but introduces the other complexities and challenges.
- The effect of scaling sensing applications from individual to resident's scale is ambiguous. Numerous problems identified with majority of the information exchanging, privacy, mining of data, and closing loop by given the meaningful feedback to a person, clusters, society, and people stay open. For constructing scalable sensing systems we just limited experience [6].
- Different sensing scale types are used, which ranges users that are actively includes in sensing system [43]. Author focus on two facts such as configuration space: participatory sensing, where individuals efficiently involves in data gathering events (i.e., the individuals physically decides how, what, and where to model) and opportunistic sensing, where information gathering phase is completely automatic and user has no participation.

- Opportunistic sensing has one key challenge which is phone context problem. For example, an application needs to simply take a sound pattern for a city extensive noise map whereas cell phone has not available in pocket or bag. Context problems can be solve by using different mobile phone sensors. These sensors such as accelerometer or light sensors determine whether mobile phone has not available in pocket.
- Participatory sensing is acquisition interest in cell phone sensing society, puts an extreme load or cost on individual; such as, manually select information to gather (e.g., least prices of petrol) and then model it (e.g., getting an image). Participatory sensing has one drawback, in which data quality is totally based on applicant interest to consistently gather sensing information and the similarity of an individual's flexibility pattern to the expected objectives of the application (e.g., get smog patterns in the region of schools).

IV. CROWDSENSING PRIVACY

Privacy is very important for everyone. No one wants to reveal his /her privacy in front of anyone. We can use different techniques to provide privacy to mobile devices or nodes. Here some overheads and risks are discussed. We also discuss privacy techniques, how these methods used in current sensing applications that address these issues. We also describe some solution of these overhead and risks. Data collection infrastructure layer is use to collect information from the chose sensor nodes. It gives information to data contributors along with privacy preserving techniques. Some component such as task allocation, sensor gateways, data anonymization, incentive mechanism and big data storage are used in this layer, which collected data from the selected nodes [6]. Author in [1] describes different privacy methods to protect our privacy, these methods are Anonymization, Encryption, and Data Perturbation.

1) *Anonymization*: Anonymization approach removes the identification information, which is collected through Crowdsensing applications. The anonymization of data will increase the privacy safeguard but is reduce data utility. Anonymization approach has two further techniques to preserve the privacy such as pseudonyms and connection anonymization. *Pseudonyms*: it is the simple technique that makes participants anonymous by replacing their identification information with an alias [44]. *Connection Anonymization*: Using this technique, we can avoid the network based tracking attacks using IP addresses. One such technique which is used in Crowdsensing applications [45] is onion routing [46].

2) *Encryption*: Encryption is a technique in which the illegal third parties not allowed to utilize the private data of mobile users. In encryption large volume of data required significant resources for encryption.

3) *Data Perturbation*: To preserve the privacy of individuals' data perturbation, immediately increase noise to

the sensor data before distributing it with the group of people, that sensory data will be unidentifiable. However, such information empowers excellent process of Crowdsensing applications.

Providing privacy anonymous routing technique is used such as onion routing [47] in a decentralized mobile cloud. For example, exist in peer-to-peer domain [48-50]. However, there exist certain outflows and a risk of unreliable delivery connected with most anonymous peer-to-peer routing protocols [51]. As a solution, the degree of security and anonymity must be flexible and depend on the context. For example, the capability of malicious nodes is high and these nodes should have the high level of privacy but this would bring on higher transmission (i.e. longer path) and computation costs (i.e. cryptography processing overheads) [52]. Cryptography technique is used to transmute data to preserve the privacy. Another privacy preserving approach which is secure multiparty computation [53], in which cryptographic techniques are used to transfer data to preserve the security. Cryptographic approaches used for calculating intensively, not versatile. Cryptographic require maintenance and generation of numerous keys. Likewise prompts top vitality utilization which participant uploads their reports, k-anonymity technique can be used to provide location privacy. [54]. Basic idea behind the k-anonymity is to construct clusters of k applicants or reports. In this way they share common feature (e.g., k participants situated in the alike region), interpreting them indistinct to everyone. To build a group of k users we can use different methods to find the suitable and common attribute. So these methods categorized into two main sections such as generalization and perturbation [55].

V. PRIVACY AND SECURITY CHALLENGES/THREATS

A sensor device may be used by the user to report a false data. There may be chances of location and time bias when the data is sensed. Additionally, the readiness and accessibility of setup is very important for these applications to be use full. There are some privacy and privacy challenges or risk where campaign administrator breaks the trust among participants and reveals the sensitive data about participants [44].

- *Time and location*: HealthSense gather the information about time and place freely of their people environmental driven nature. So GPS receivers which is embedded in the smart phones provide vary accurate location of the user. So, within the absence of GPS, WiFi or cellular system depends mostly triangulation which utilized to get coarse-grained area data [57]. Through embedded sensors contextual information can be used to recognize a person location [58]. Moreover, the threats ensuing from time and location traces aren't confined to applications, wherever authentication is needed [59].
- *Sound samples*: Besides deriving personalities and preference form temporal and spatial data, the representation of participants clarified through completing this information by patterns of other detecting modalities. In a few of the previously stated applications, patterns if sound either recorded

purposefully by the users, or automatically caught through cell phones. However, participants simply secure their protection just recording non sensitive occasions in the previous instance; cell phones efficiently act as intelligent spies in situation of automatic recordings.

- *Picture and video:* The substance of distributed picture and recorded recordings is also probable to disclose personal information related to the members and their environments. While Diet- Sense [31] targets to take photos of consumed meal, no countermeasures are taken to cover the faces of person's share-out their meal with the participants. In entirely situations, in which the camera is arranged far from the participant, faces of other persons in the region are conceivably caught in the pictures, and consequences about the number and identity of the participant's social relations might be drawn. The publications of capturing images can lead to the alike conclusions as in online social networks, such as Facebook, where an instructor was suspended because of a photo demonstrating her holding glasses loaded with liquor [60], or a disheartened woman who lost benefits from her health insurance for images demonstrating her presence parties and relaxing on the beach [61]. Alike to sound recordings, the existing user context and their nearby environment could also be extracted from sensor data. For example, images displaying points of interest could easily found the participant's attendance at those locations.
- *Acceleration:* learning of raw accelerometer might show up fewer threatening in exposing personal data about the members. Yet this theory not every times correct also might regularly just help as an incorrect sense about safety. For example, if the mobile phone is carry on hip, data about the walk, in this way through conceivable indication about the user can inferred the identity of user [62]. Moreover, the study of action recognition also creates wide usage of accelerometer analyses [63]. The misuse of this data by pernicious clients might have undesirable outcomes. For instance, employers might need to confirm that their employees are really doing work throughout their working times. If employers discover any abnormalities. Could terminate the respective worker.
- *Environmental Data:* Recording gas and particles focuses or barometric burden might not be straightforwardly undermines protection of members without anyone else's input. Be that as it may, specific air pieces joined with optional data, for example, exact air temperature, may distinguish the area of the members at the phase of granularity as well as room levels inside structures, where area information can be wrong because of area administrations or non-availability of GPS.
- *Biometric Data:* Sensor data of biometric utilized for discovering the user's present physiological condition. Likewise, to medical staff, opponent may distinguish

health irregularities or diseases built on the caught sensor information. Revealed medical data later used for health insurance corporations or employers to repudiate agreements, if diagnosis any damage of physiological states of the participants.

Another approach which produces a privacy threat to reveal the location information, forgetting frequently visited locations of individual's anonymized GPS sensor measurements is still used. It also used to get personal information of participants. PEIR [10] utilizes sensitive private information, and its schemes should planned to reduce information release from the user's control to prevent different security threats [64-67]. In different cases, getting features might be very sensitive than crude data: researchers discovered crucial places like home and offices. It also gives extremely valuable context information and can learn by inference methods, but discharging this information unnecessarily and should be preventable.

Applications such as PEIR should help the participants in linking sensing information to their everyday practices and long term aims. To this end, investigation, collection, and alerting specifically absolutely should be configurable as well as information and high level of conclusions navigable from various points of view. Support (1) comprehension of specific samples, (2) personal progression of research and substitutes, (3) setting aim, (4) comparison, (5) comprehension of marvels relationship [68]. In participatory detecting, the detecting operations needs some method for human impedance [69] e. g the assignment could request that the client take a photo of the menu when she visits an eatery or to remark on her view about the sustenance at the cafeteria or to gauge the gas costs when she passes a recording station [70]. The human components incorporate extra security assignments. As for security, the client may undertake additional data about his or her character by the way of his or her response.

VI. CONCLUSIONS

Mobile crowdsensing is an emerging sensing model based on participatory sensing paradigm. This paper describes different concepts of crowdsensing and how it is applied in different domains so far. Crowdsensing has the potential to produce interesting business models such as sensing as a service. This participatory sensing paradigm has many socio-technical challenges and major is a privacy. However, it requires innovative approaches to solve the socio-technical challenges.

REFERENCES

- [1] Dimov, D., Crowdsensing: State of the Art and Privacy Aspects. InfoSec Institute, 2014. 29.
- [2] Mardenfeld, S., et al. Gdc: Group discovery using co-location traces. in Social computing (SocialCom), 2010 IEEE second international conference on. 2010. IEEE.
- [3] Lane, N.D., et al., A survey of mobile phone sensing. Communications Magazine, IEEE, 2010. 48(9): p. 140-150.
- [4] Talasila, M., R. Curtmola, and C. Borcea, Mobile Crowd Sensing.
- [5] Guo, B., et al. From participatory sensing to mobile crowd sensing, in Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on. 2014. IEEE.

- [6] Guo, B., et al., Mobile crowd sensing and computing: The review of an emerging human-powered sensing paradigm. *ACM Computing Surveys (CSUR)*, 2015. 48(1): p. 7.
- [7] Zhang, D., B. Guo, and Z. Yu, The emergence of social and community intelligence. *Computer*, 2011. 44(7): p. 21-28.
- [8] Pournajaf, L., et al., A survey on privacy in mobile crowd sensing task management. 2014, Technical Report TR-2014-002, Department of Mathematics and Computer Science, Emory University.
- [9] Sirsikar, S. and V. Powar, Mobile Crowd Sensing Using Voronoi Based Approach. *International Journal of Computer Science And Applications*, 2015. 8(1).
- [10] Mun, M., et al. PEIR, the personal environmental impact report, as a platform for participatory sensing systems research. in *Proceedings of the 7th international conference on Mobile systems, applications, and services*. 2009. ACM.
- [11] Stansfeld, S.A. and M.P. Matheson, Noise pollution: non-auditory effects on health. *British medical bulletin*, 2003. 68(1): p. 243-257.
- [12] Maisonneuve, N., M. Stevens, and B. Ochab, Participatory noise pollution monitoring using mobile phones. *Information Polity*, 2010. 15(1, 2): p. 51-71.
- [13] Rana, R.K., et al. Ear-phone: an end-to-end participatory urban noise mapping system. in *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*. 2010. ACM.
- [14] Directive, E., Directive 2002/49/EC of the European parliament and the Council of 25 June 2002 relating to the assessment and management of environmental noise. *Official Journal of the European Communities*, 2002. 189(12).
- [15] Goldman, J., et al., Participatory Sensing: A citizen-powered approach to illuminating the patterns that shape our world. *Foresight & Governance Project, White Paper*, 2009: p. 1-15.
- [16] Predic, B., et al. Exposuresense: Integrating daily activities with air quality using mobile participatory sensing. in *Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2013 IEEE International Conference on. 2013. IEEE.
- [17] Eisenman, S.B., et al., BikeNet: A mobile sensing system for cyclist experience mapping. *ACM Transactions on Sensor Networks (TOSN)*, 2009. 6(1): p. 6.
- [18] Thiagarajan, A., et al. VTrack: accurate, energy-aware road traffic delay estimation using mobile phones. in *Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*. 2009. ACM.
- [19] Mohan, P., V.N. Padmanabhan, and R. Ramjee. Nerice: rich monitoring of road and traffic conditions using mobile smartphones. in *Proceedings of the 6th ACM conference on Embedded network sensor systems*. 2008. ACM.
- [20] Higuchi, T., H. Yamaguchi, and T. Higashino, Mobile devices as an infrastructure: A survey of opportunistic sensing technology. *Journal of information processing*, 2015. 23(2): p. 94-104.
- [21] Eriksson, J., et al. The pothole patrol: using a mobile sensor network for road surface monitoring. in *Proceedings of the 6th international conference on Mobile systems, applications, and services*. 2008. ACM.
- [22] White, J., et al., Wreckwatch: Automatic traffic accident detection and notification with smartphones. *Mobile Networks and Applications*, 2011. 16(3): p. 285-303.
- [23] Ma, S., Y. Zheng, and O. Wolfson. T-share: A large-scale dynamic taxi ridesharing service. in *Data Engineering (ICDE)*, 2013 IEEE 29th International Conference on. 2013. IEEE.
- [24] Finucan, R., *Mobile Social Networking*. 2009, Google Patents.
- [25] Khan, W.Z., et al., Mobile phone sensing systems: A survey. *Communications Surveys & Tutorials, IEEE*, 2013. 15(1): p. 402-427.
- [26] Ziegler, C.-N., G. Lausen, and J.A. Konstan, On exploiting classification taxonomies in recommender systems. *AI Communications*, 2008. 21(2-3): p. 97-125.
- [27] Rosi, A., et al. Social sensors and pervasive services: Approaches and perspectives. in *Pervasive Computing and Communications Workshops (PERCOM Workshops)*, 2011 IEEE International Conference on. 2011. IEEE.
- [28] Miluzzo, E., et al. Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application. in *Proceedings of the 6th ACM conference on Embedded network sensor systems*. 2008. ACM.
- [29] Kanhere, S.S., Participatory sensing: Crowdsourcing data from mobile smartphones in urban spaces, in *Distributed computing and internet technology*. 2013, Springer. p. 19-26.
- [30] Reddy, S., et al. Image browsing, processing, and clustering for participatory sensing: lessons from a DietSense prototype. in *Proceedings of the 4th workshop on Embedded networked sensors*. 2007. ACM.
- [31] Gao, C., F. Kong, and J. Tan. Healthaware: Tackling obesity with health aware smart phone systems. in *Robotics and Biomimetics (ROBIO)*, 2009 IEEE International Conference on. 2009. Ieee.
- [32] Chen, W., et al., A survey and challenges in routing and data dissemination in vehicular ad hoc networks. *Wireless Communications and Mobile Computing*, 2011. 11(7): p. 787-795.
- [33] Liao, C.-C., et al. Sais: Smartphone augmented infrastructure sensing for public safety and sustainability in smart cities. in *Proceedings of the 1st International Workshop on Emerging Multimedia Applications and Services for Smart Cities*. 2014. ACM.
- [34] Consulting, V.W., *mHealth for development: the opportunity of mobile technology for healthcare in the developing world*. 2009.
- [35] Sakaki, T., M. Okazaki, and Y. Matsuo. Earthquake shakes Twitter users: real-time event detection by social sensors. in *Proceedings of the 19th international conference on World wide web*. 2010. ACM.
- [36] Ganti, R.K., F. Ye, and H. Lei, Mobile crowdsensing: current state and future challenges. *Communications Magazine, IEEE*, 2011. 49(11): p. 32-39.
- [37] Heggen, S., A. Adagale, and J. Payton, Lowering the barrier for crowdsensing application development, in *Mobile Computing, Applications, and Services*. 2013, Springer. p. 1-18.
- [38] Nikander, P., A. Gurtov, and T.R. Henderson, Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks. *Communications Surveys & Tutorials, IEEE*, 2010. 12(2): p. 186-204.
- [39] Huangfu, S., et al. Using the model of markets with intermediaries as an incentive scheme for opportunistic social networks. in *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*. 2013. IEEE.
- [40] Lee, J.-S. and B. Hoh. Sell your experiences: a market mechanism based incentive for participatory sensing. in *Pervasive Computing and Communications (PerCom)*, 2010 IEEE International Conference on. 2010. IEEE.
- [41] Yang, D., et al. Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing. in *Proceedings of the 18th annual international conference on Mobile computing and networking*. 2012. ACM.
- [42] Sheng, X., et al., Sensing as a service: Challenges, solutions and future directions. *Sensors Journal, IEEE*, 2013. 13(10): p. 3733-3741.
- [43] *Smartphone Sensing Group*. September 2013.
- [44] Christin, D., et al., A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 2011. 84(11): p. 1928-1946.
- [45] Shin, M., et al., AnonySense: A system for anonymous opportunistic sensing. *Pervasive and Mobile Computing*, 2011. 7(1): p. 16-30.
- [46] Dingedine, R., N. Mathewson, and P. Syverson, Tor: The second-generation onion router. 2004, DTIC Document.
- [47] Syverson, P.F., D.M. Goldschlag, and M.G. Reed. Anonymous connections and onion routing. in *Security and Privacy*, 1997. *Proceedings., 1997 IEEE Symposium on*. 1997. IEEE.
- [48] Han, J., et al. Provide privacy for mobile p2p systems. in *Distributed Computing Systems Workshops*, 2005. 25th IEEE International Conference on. 2005. IEEE.
- [49] Han, J. and Y. Liu. Rumor riding: Anonymizing unstructured peer-to-peer systems. in *Network Protocols*, 2006. *ICNP'06. Proceedings of the 2006 14th IEEE International Conference on*. 2006. IEEE.

- [50] Ghinita, G., P. Kalnis, and S. Skiadopoulos. PRIVE: anonymous location-based queries in distributed mobile systems. in Proceedings of the 16th international conference on World Wide Web. 2007. ACM.
- [51] Han, J. and Y. Liu, Mutual anonymity for mobile p2p systems. *Parallel and Distributed Systems*, IEEE Transactions on, 2008. 19(8): p. 1009-1019.
- [52] Fernando, N., S.W. Loke, and W. Rahayu, Mobile cloud computing: A survey. *Future Generation Computer Systems*, 2013. 29(1): p. 84-106.
- [53] Yao, A.C. Protocols for secure computations. in *Foundations of Computer Science, 1982. SFCS'08. 23rd Annual Symposium on*. 1982. IEEE.
- [54] Sweeney, L., k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2002. 10(05): p. 557-570.
- [55] Huang, K.L., S.S. Kanhere, and W. Hu, Preserving privacy in participatory sensing systems. *Computer Communications*, 2010. 33(11): p. 1266-1280.
- [56] Shi, J., et al. Prisense: privacy-preserving data aggregation in people-centric urban sensing systems. in *INFOCOM, 2010 Proceedings IEEE*. 2010. IEEE.
- [57] LaMarca, A., et al., Place lab: Device positioning using radio beacons in the wild, in *Pervasive computing*. 2005, Springer. p. 116-133.
- [58] Azizyan, M., I. Constandache, and R. Roy Choudhury. SurroundSense: mobile phone localization via ambience fingerprinting. in *Proceedings of the 15th annual international conference on Mobile computing and networking*. 2009. ACM.
- [59] Shilton, K., Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM*, 2009. 52(11): p. 48-53.
- [60] Did the Internet Kill Privacy? 2011.
- [61] Depressed woman loses benefits over Facebook photos. 2009.
- [62] Derawi, M.O., et al. Unobtrusive user-authentication on mobile phones using biometric gait recognition. in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*. 2010. IEEE.
- [63] Györfi, N., Á. Fábrián, and G. Hományi, An activity recognition system for mobile phones. *Mobile Networks and Applications*, 2009. 14(1): p. 82-91.
- [64] Gruteser, M. and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. in *Proceedings of the 1st international conference on Mobile systems, applications and services*. 2003. ACM.
- [65] Hoh, B., et al. Preserving privacy in gps traces via uncertainty-aware path cloaking. in *Proceedings of the 14th ACM conference on Computer and communications security*. 2007. ACM.
- [66] Krumm, J., Inference attacks on location tracks, in *Pervasive Computing*. 2007, Springer. p. 127-143.
- [67] Krumm, J., J. Letchner, and E. Horvitz. Map matching with travel time constraints. in *SAE world congress*. 2007.
- [68] Agapie, E., et al. Seeing Our Signals: Combining location traces and web-based models for personal discovery. in *Proceedings of the 9th workshop on Mobile computing systems and applications*. 2008. ACM.
- [69] Burke, J.A., et al., Participatory sensing. *Center for Embedded Network Sensing*, 2006.
- [70] Bulusu, N., et al. Participatory sensing in commerce: Using mobile camera phones to track market price dispersion. in *Proceedings of the International Workshop on Urban, Community, and Social Applications of Networked Sensing Systems (UrbanSense 2008)*. 2008.