Exploiting Mobile Crowdsourcing for Pervasive Cloud Services: Challenges and Solutions

Ju Ren, Yaoxue Zhang, Kuan Zhang, and Xuemin (Sherman) Shen

ABSTRACT

With the proliferation of increasingly powerful mobile devices, mobile users can collaboratively form a mobile cloud to provide pervasive services, such as data collecting, processing, and computing. With this mobile cloud, mobile crowdsourcing, as an emerging service paradigm, can enable mobile users to take over the outsourced tasks. By leveraging the sensing capabilities of mobile devices and integrating human-intelligence and machine-computation, mobile crowdsourcing has the potential to revolutionize the approach of data collecting and processing. In this article we investigate the mobile crowdsourcing architecture and applications, then discuss some research challenges and countermeasures for developing mobile crowdsourcing. Some research orientations are finally envisioned for further studies.

INTRODUCTION

According to the report of *eMarketer* in June 2014, the number of global smartphone users surpassed the one billion mark in 2012, and is estimated to be 1.75 billion in 2014. With the explosion of mobile devices, mobile computing has become an overwhelming trend in the development of IT technology as well as the fields of commerce and industry. However, mobile devices are facing some limitations on various resources, e.g., computation, memory, and energy. To overcome these limitations, mobile cloud computing has become a promising solution to enable mobile devices to consume varied cloud resources via wireless networks. Such a cloud computing service model, i.e. mobile as a service consumer (MaaSC), can improve the computation capability and energy efficiency of mobile devices by offloading computation tasks onto cloud servers [1].

New mobile devices are embedded with a set of versatile sensors, providing a novel paradigm to collect a vast amount of data about individuals, human society, and environments. Meanwhile, since mobile devices are usually associated with human users, human-intelligence can be leveraged for the tasks that are intractable for machine-computation, e.g., entity resolution and image annotation. Empowered by these capabilities, mobile devices shift from service consumers to service providers, offering a new service model for mobile cloud computing, i.e. mobile as a service provider (MaaSP). In this emerging service model, a large number of mobile devices connect with each other via wireless networks, forming an unprecedentedly powerful mobile cloud to provide pervasive data collecting, processing, and computing services. With this powerful mobile cloud, mobile crowdsourcing has been gaining momentum as a feasible solution for solving very large-scale problems. By outsourcing tasks to the mobile cloud, cost-effective and pervasive cloud services can be achieved, using a possibly huge number of mobile users and devices to work together in a distributed way. The ideas behind mobile crowdsourcing involve a wide range of applications and are utilized in different business models [2]. For example, OpenStreetMap [2] is a crowdsourced map of the world, created by worldwide voluntary mobile users using their local knowledge, GPS trajectories, and donated sources. The rapid development of OpenStreetMap indicates that mobile crowdsourcing has the potential to revolutionize traditional data processing and collecting approaches, and in fact already has.

Despite the promising computing paradigm and tremendous advantages, mobile crowdsourcing is still in its infancy and facing many challenges. As mobile users become service providers, social relationships and interactions play a significant role in mobile crowdsourcing. It poses a particular challenge on exploiting the underlying social impacts, such as personal social attributes, preference, selfishness, etc. Meanwhile, in the presence of malicious users, mobile crowdsourcing is vulnerable to various kinds of attacks, e.g., denial-of-service attacks and Sybil attacks. In addition, the private information of both service consumers and mobile users may also be disclosed without sophisticated privacy preservation techniques. Having these security and privacy concerns, mobile users would lose their passion for mobile crowdsourcing. Therefore, it is extremely critical to address these challenges to facilitate the development of mobile crowdsourcing.

Ju Ren and Yaoxue Zhang are with Central South University.

Ju Ren is also a visiting scholar at the University of Waterloo.

Kuan Zhang and Xuemin (Sherman) Shen are with the University of Waterloo.

0163-6804/15/$25.00 © 2015 IEEE

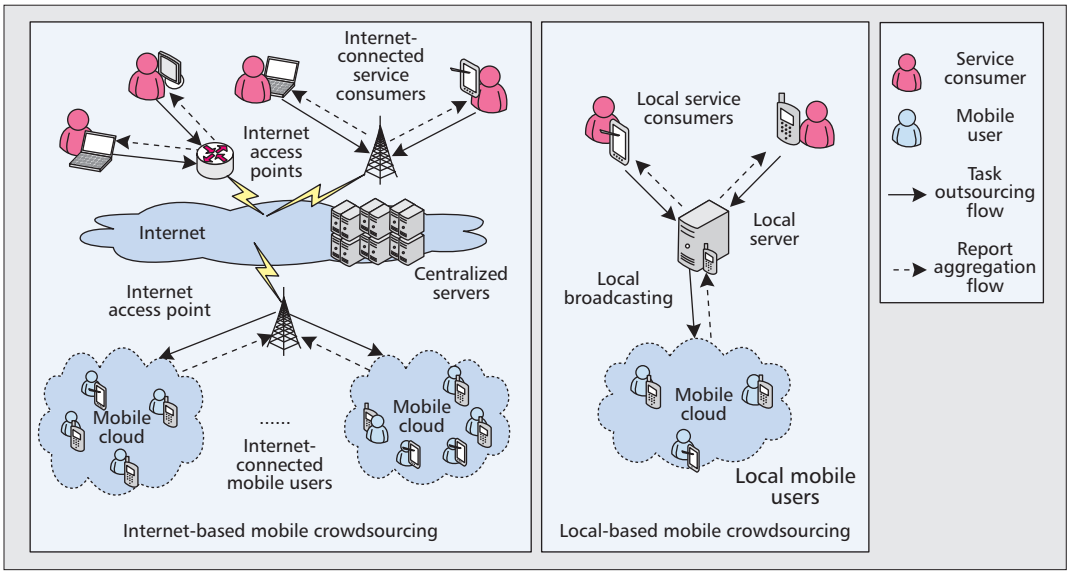

Figure 1. Network architectures of mobile crowdsourcing.

Mobile crowdsourcing is a type of electronic commerce service, where mobile users form a mobile cloud to sell cloud resources and services (e.g., data collecting, computing, and processing) for service consumers.

In this article we investigate the mobile crowdsourcing architecture and existing applications to achieve pervasive cloud services. In addition, we identify some key challenges that impede the implementation of mobile crowdsourcing. Two countermeasures are then presented to address these challenges. Finally, we envision some future research directions and open challenges, and conclude this article.

Mobile Crowdsourcing: Architecture and Applications

Mobile Crowdsourcing Architecture

Mobile crowdsourcing is a type of electronic commerce service, where mobile users form a mobile cloud to sell cloud resources and services (e.g., data collecting, computing, and processing) for service consumers. Different from the traditional cloud computing that depends on Internet connection, mobile crowdsourcing can provide pervasive cloud services for both online and local terminals. Figure 1 shows the architectures of mobile crowdsourcing in an Internet-based scenario and a local-based scenario, respectively. The main difference between the two kinds of mobile crowdsourcing models is that all the Internet-connected mobile users can potentially be a service provider in the Internet-based mobile crowdsourcing, while only the mobile users in the vicinity can provide cloud services in local-based mobile crowdsourcing. We describe the key components of mobile crowdsourcing as follows.

Service Consumers: Service consumers refer to the online and local users that require cloud services through the mobile crowdsourcing system. They utilize the cloud services by outsourcing tasks to mobile users.

Mobile Users: Mobile users with mobile devices can autonomously form a mobile cloud to provide cloud services, for online service consumers via cellular/WiFi networks, or for local service consumers by communicating with local servers or neighboring users using Bluetooth/NFC techniques. When a mobile user participates in an outsourced task, it can adopt local computing or require mobile cloud computing to execute this task.

Centralized Servers: Centralized servers can be seen as a mobile crowdsourcing platform for Internet-based service consumers. They store all the crowdsourcing information (e.g., users' profiles, historical service records) that can be used for task outsourcing and service evaluation. Generally, centralized servers can provide trusted services for task publishing, allocating, report collecting, and feedback processing for the Internet-connected service consumers and mobile users.

Local Servers: Local servers can provide local crowdsourcing services, such as outsourced task broadcasting and task result aggregation, for service consumers and mobile users in the vicinity. Local servers are generally equipped with dedicated mobile local gateways to disseminate the task information to neighboring mobile users and collect user report results. In addition, they can also query or update necessary information from centralized servers to support mobile crowdsourcing. However, local servers are usually deployed for commercial purposes and not trusted by mobile users.

Mobile Crowdsourcing Applications

In the last five years mobile devices have become sensor and information hubs in our daily life. By integrating mobile computing and crowdsourcing, some emerging applications have shown the potential to achieve highly efficient and cost-effective data computation, collection, and processing services. In this section we present two representative mobile crowdsourcing applications, as shown in Fig. 2: mobile crowdcomputing and mobile crowdsensing. Some related works on the two types of mobile crowdsourcing applications are and compared in Table 1.

Mobile Crowdcomputing: Mobile crowdcomputing is used to outsource data computation tasks to mobile users. The mobile users who participate in the outsourced tasks can locally exe-

Generally, mobile users have various capabilities for the outsourced tasks (e.g., personal knowledge, available resources for data collecting and computing), thus, incentive mechanism should stimulate more well-suited mobile users for a specific outsourced task, instead of indiscriminate stimulation.

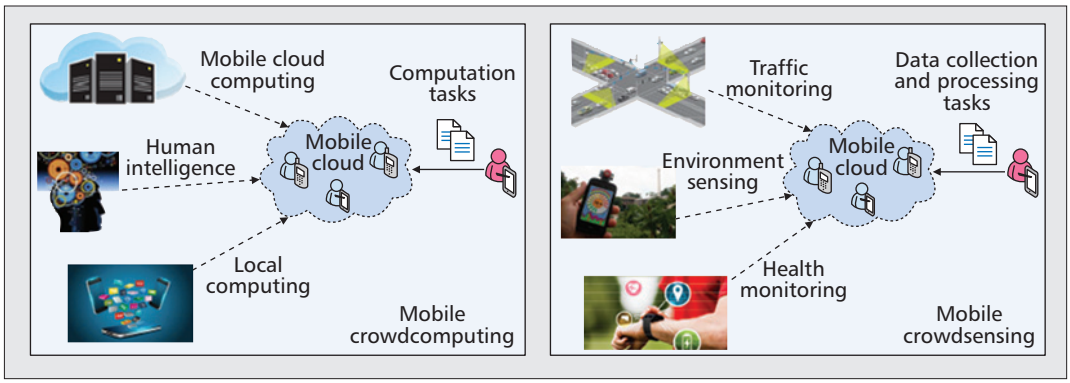

Figure 2. Mobile crowdcomputing and mobile crowdsensing.

cute these tasks or offload them to the cloud severs based on their own data and computation resources. Due to human intervention, mobile crowdcomputing can leverage human-intelligence to deal with the tasks that are more suitable for human evaluation than machine computation (e.g., entity resolution, image annotation, and sentiment analysis). Honeybee [4] is a local-based mobile crowdcomputing application, in which face detection and photography tasks are outsourced to local mobile users. The mobile users use their mobile devices to run face detection algorithms and take specific photos, together with their personal evaluation. CrowdDB [3] crowdsources the computing tasks in the form of querying and answering, based on the Amazon Mechanical Turk platform.

Mobile Crowdsensing: Data collection and processing, such as environment sensing and monitoring, generally require enormous technical efforts and significant economical resources. Mobile crowdsensing is used to outsource data collection and processing tasks to mobile users, who can perform data sensing with sensor-equipped mobile devices, and execute data processing by local computing or mobile cloud computing. By motivating mobile users' participation, mobile crowdsensing can provide cost-efficient mobile cloud services for data collection and processing. SignalGuru [5] is a local-based mobile crowdsensing application, utilizing smartphones to opportunistically detect current traffic signals and collaboratively exchange their detection information via an ad-hoc network. The smartphones can predict the future schedule of traffic signals based on the collection of exchanged information to guide the driving decision-making. Medusa [6] is a mobile crowdsensing application that collects specific sensing data by outsourcing sensing tasks, including video documentation, auditioning, and road monitoring, to Internet-connected mobile users via secure-HTTP based wireless communication.

Key Challenges in Mobile Crowdsourcing

Selfishness and Incentive

Motivating mobile users to participate in mobile crowdsourcing is critical for forming a powerful mobile cloud. The incentives to motivate mobile users could be varied, including financial rewards, personal contribution, social gains, etc. Experiences with micro-task markets, such as Amazon Mechanical Turk, provide positive indications on monetary incentives, while Wikipedia is a good example of human contribution for non-financial gain. However, since both service consumers and mobile users are selfish and aim to benefit from crowdsourcing, incentive mechanisms should economically balance the requirements of the two parties, and create mutual benefits and a win-win situation. Yang *et al.* [7] propose two incentive mechanisms, including reward-sharing and auction-based, to simulate mobile users to participate in mobile crowdsourcing. In reward-sharing incentives, service consumers offer fixed rewards for their outsourced tasks, and each reward is shared by the task participants according to the time they worked on the corresponding task. They also design a truthful auction-based incentive mechanism, where mobile users make offers for different outsourced tasks and service consumers choose appropriate participants to maximize their own utilities. Both the reward-sharing and auction-based incentive mechanisms can economically stimulate the formation of a mobile cloud and also can achieve mutual benefits. However, neither of them shows discrimination for different mobile users. Generally, mobile users have various capabilities for the outsourced tasks (e.g., personal knowledge, available resources for data collecting and computing), thus incentive mechanisms should stimulate more well-suited mobile users for a specific outsourced task, instead of offering incentives indiscriminately.

Task Allocation

In cloud computing it is essential to apply a type of server instance (e.g., high-memory instance, high-CPU instance) for the computation tasks from a larger number of networked cloud servers, according to the task characteristics and requirements. Similarly, in mobile crowdsourcing, task allocation aims to allocate a specific set of outsourced tasks to a set of mobile users who can potentially finish these tasks more accurately and efficiently. Some factors that may impact task allocation have been investigated in existing works. Reddy *et al.* [8] claim geographic and temporal availabilities of mobile users would highly impact the task delay, which should be considered in participant selection. He *et al.* [9]

Application	Service type	Working platform	Task type	Computation resources	Internet-based or local-based
CrowdDB [3]	Mobile crowdcomputing	Based on Amazon Mechanical Turk	Querying and answering	Human intelligence	Internet-based
Honeybee [4]	Mobile crowdcomputing	Android	Face detection	Human intelligence and machine computation	Local-based
SignalGuru [5]	Mobile crowdsensing	iOS	Traffic signal detection	Machine computation	Local-based
Medusa [6]	Mobile crowdsensing	Android	Environment sensing and data processing	Machine computation	Internet-based

Table 1. Representative existing mobile crowdsourcing applications/systems.

design a recruitment algorithm for a mobile crowdsensing application taking the mobility paths of mobile users into consideration. Despite the existing considered factors, the underlying social impacts between the outsourced task and mobile users should be considered in task allocation. For instance, if the outsourced task is "Find an unoccupied basketball court at the University of Waterloo," the mobile users who are interested in "Sport" and study at this university might be preferred to be recruited in the task. Therefore, investigating the social impacts and determining a matching degree for each pair of task and mobile user, and to describe the potential utility of a mobile user participating in an outsourced task, is necessary and crucial for mobile crowdsroucing. Furthermore, based on the determined matching degrees, an efficient task allocation scheme should be developed to maximize the potential utility for both service consumers and mobile users.

Security Threats

Security is one of the primary concerns for cloud service consumers, while the mobile crowdsourcing philosophy originates from the assumption that mobile users would honestly provide accurate results. This is a contradiction and also a persistent problem for mobile crowdsourcing, since there may be malicious mobile users attempting to misbehave in or undermine the mobile crowdsourcing. The malicious users can fabricate computation or sensing results, or maliciously suspend the ongoing tasks, or launch other types of attacks that can directly or indirectly cause negative impacts on the outsourced tasks and service consumers. Some related work has been proposed to mitigate the impacts of malicious task reports and identify the misbehaving users. Zhang *et al.* [10] develop a robust trajectory estimation strategy, to alleviate the negative influence of abnormal crowdsourced user trajectories and identify the normal and abnormal users. Huang *et al.* [11] employ the Gompertz function to compute the device reputation score and evaluate the trustworthiness of the contributed data. Although trust evaluation is an effective solution to measure the credibility of task reports and assist malicious user detection, the users' privacy may be disclosed by linking the trust values associated with multiple task reports [12]. In summary, a major challenge is to design sophisticated security countermeasures to resist malicious attacks and guarantee a reliable mobile crowdsourcing system.

Privacy Leakage

Another obstacle to the widespread deployment and acceptance of mobile crowdsourcing is the privacy concerns of both mobile users and service consumers. The outsourced tasks could reveal the personal interests and objectives of service consumers. Meanwhile, task reports generally tagged with spatio-temporal information disclose abundant personal information of mobile users, such as location, personal activities, and social relationships. Therefore, privacy preservation is of paramount importance in mobile crowdsourcing. For instance, mobile user's location privacy could be exposed when participating in environment sensing of a small space. Generally, we can use cryptography to provide protection for mobile users and service consumers from being eavesdropped by outside attackers when data transmitting and processing. To preserve data privacy from service consumers, Liu *et al.* [13] propose a collaborative learning scheme for classification tasks, e.g., activity or context recognition, in mobile sensing, which can ensure the classification accuracy without disclosing mobile users' privacy, by utilizing the feature perturbation and regression techniques. Anonymity, as an effective solution for privacy preservation, has also been adopted to preserve mobile users' privacy in mobile crowdsensing [12]. In particular, privacy leakage concerns should be given more attention for local-based mobile crowdsourcing, since local servers are generally deployed for commercial purposes and not trusted by mobile users. Therefore, anonymous techniques should be well developed for information transfer between mobile users and local servers.

Solutions for Mobile Crowdsourcing Applications

In this section we discuss two promising solutions for mobile crowdsourcing. Specifically, we present a social-aware task allocation scheme to address the incentive and task allocation challenges for Internet-based mobile crowdcomputing

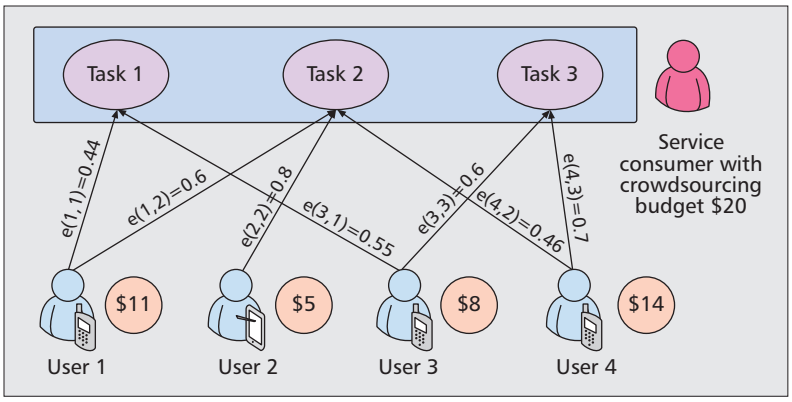

Figure 3. An example of task allocation by SATA.[1]

applications, and an anonymous reputation system to mitigate the security and privacy concerns for local-based mobile crowdsensing applications.

Social-Aware Task Allocation for Internet-based Mobile Crowdcomputing

In Internet-based mobile crowdcomputing, all the Internet-connected mobile users have the potential to provide cloud services for outsourced computation tasks. With such a huge service pool, incentives and task allocation are particularly important for this type of applications to achieve targeted computing services. In addition, since crowdcomputing generally depends on human-intelligence, the social attributes of mobile users (e.g., specialties, social activities) may highly impact the quality of computation tasks. In this section we present a social-aware task allocation (SATA) scheme for a typical Internet-based mobile crowdcomputing application [14], where the crowdsourcing procedures can be detailed as follows. A service consumer first publishes a set of tasks to outsource, which generally contain specific requirements (e.g., interested specialties, delay, and task budget). The mobile users, interested in these tasks, then estimate the task execution information (e.g., processing cost, delay), and apply for participation. Afterward, the service consumer allocates these tasks to a subset of applicants based on their application information. After task allocation, the selected participants execute the outsourced tasks with their own data and computation resources. After the tasks are finished, the task reports will be submitted to the service consumers. Finally, the service consumer evaluates the task reports and gives feedback (e.g., report evaluation, rewards), to the participants.

To motivate mobile users' participation and achieve mutual benefits, SATA adopts an auction-based incentive mechanism, where mobile users announce their bid prices for the interested outsourced tasks, according to their costs and capabilities. Service consumers then choose a subset of mobile users to take the outsourced computation tasks under a fixed budget. In order to identify the well-suited mobile users for a specific computation task, SATA introduces a matching degree, determined by three social factors, for each pair of mobile user and task. Social attribute overlap degree is the primary factor considered in the matching degree calculation. Each mobile user can be characterized by a set of social attributes based on their specialties, social interactions, and personal features, to identify the advantages in addressing some specific types of tasks. If we can specify the interested social attributes for an outsourced task, a higher social attribute overlap degree generally indicates a potential matching between a mobile user and this task. Moreover, each user can estimate a task delay to finish the task based on his available data resources and capabilities, which directly impacts the matching degree, especially for the delay-sensitive tasks. In addition, the reputation of the mobile user is a crucial factor in task allocation, since it indicates the trustworthiness of the mobile user according to his historical task evaluation. For each pair of mobile user and task, if we use three functions f, g, and h, to denote the impacts of social attribute overlap, estimated task delay, and reputation, respectively, the total matching degree can be calculated as a function $e(f, g, h)$ related to f, g, and h.

After the determination of matching degree, task allocation changes to a knapsack problem to maximize the potential utility of the service consumer. More specifically, if a service consumer has a set of tasks to crowdsource under a fixed budget, and there are a set of interested mobile users announcing their bid prices for participating in a subset of tasks, task allocation can be formulated as choosing a subset of interested mobile users to maximize the total matching degree $\Sigma\{e(f, g, h)\}$, subject to the constraint that the sum of the bid prices of chosen mobile users should not be larger than the task budget. It is known that a knapsack problem is NP-hard, but a fully polynomial time approximation solution can be achieved to address this problem [14]. Figure 3 shows an example of task allocation by SATA.

By employing SATA, service consumers can recruit the well-suited participants that can potentially optimize the quality of outsourced computing tasks. Meanwhile, SATA can lead mobile users to participate in the tasks with higher matching degrees, for which they can flexibly adjust their bidding strategies to maximize their own profits. Figures 4a and 4b show the task quality and average user profit comparison, respectively, between SATA and greedy allocation scheme (GAS). Here, GAS refers to allocating tasks to mobile users only according to their bidding prices, without considering the underlying matching degrees [7]. The experiment results show that SATA can notably improve the outsourced task quality and the benefits of mobile users.

Anonymous Reputation Management for Local-based Mobile Crowdsensing

Mobile crowdsensing has been widely adopted as an efficient and economical solution for environment sensing. However, since sensing reports generally contain abundant sensitive personal information, privacy leakage is a significant challenge for mobile crowdsensing applications. Moreover, due to the untrusted local servers, privacy preservation becomes particularly important in local crowdsensing scenarios [15]. In addition, in the presence of malicious users, the

[1] The matching degree of each pair of task and mobile user is denoted by the weight of edge. By employing SATA, User 1 and User 3 will be chosen to potentially optimize the quality of outsourced tasks.

sensing reports are easily fabricated or tampered with to pollute the final sensing results. Therefore, sophisticated security and privacy preservation techniques should be elaborately developed to mitigate these severe challenges for local-based mobile crowdsensing.

In [12], Wang *et al.* propose an anonymous reputation system based on blind signatures to simultaneously achieve trust evaluation and privacy preservation. By adopting trust evaluation and reputation management, malicious users can be detected accurately after repeated misbehaviors [15]. The reputation values of mobile users can also be used for determining the trustworthiness of sensing reports and generating the final sensing results. Meanwhile, blind signatures ensure the authenticity of signed messages without disclosing their content to the signing entity, and also can prevent the signing entity from linking the message with the identity of its generator. Therefore, mobile users' privacy can be preserved from both local servers and service consumers. The anonymous reputation system is illustrated in Fig. 5, which consists of a mobile user, a service consumer, local servers, and a reputation and pseudonym manager (RPM). We describe the procedures of mobile crowdsensing with anonymous reputation management as follows.

First, a mobile user should register with RPM for participating in the task t. RPM obtains the reputation level based on his actual reputation, and creates two certificates, C_u and C_0, for u, where C_0 is the anonymous certificate provided for the service consumer, while C_u contains the actual user ID u and is used by RPM to update u's reputation. Both the certificates are signed by RPM and contain the reputation level of u and task ID. If the mobile user wants to participate in a new task, it has to require two refreshed certificates with a different task ID, which can also partly prevent Sybil attacks [15]. After receiving certificates, the mobile user generates his blind ID as B_u based on the certificate C_u. Every time the user submits a sensing report, it should generate a different blind ID. The service consumer will assess the quality of the submitted sensing reports with the user's reputation level, and create a reputation feedback (RF) as $RF = B_u \mid \{f_{SR}\}_{K_{sp}} \mid C_0$, where f_{SR} is the reputation feedback encrypted by RPM's public key. Therefore, both mobile users and local server cannot decrypt this feedback. After receiving the RF, the mobile user can obtain an unblinded RF (URF) by retrieving C_u from B_u as $URF = C_u \mid \{f_{SR}\}_{K_{sp}} \mid C_0$. Note that both RF and URF are signed by the service consumer and hence cannot be forged by the user. When RPM receives a URF, it processes a security check to validate the URF. Only if the validation is passed will RPM extract the user's ID and reputation feedback to update his current reputation value.

Throughout the whole process, neither service consumers nor local servers can link the sensing reports and reputation values to the real identities of mobile users. Furthermore, by changing the blinded ID for each report submission, it becomes impossible to de-anonymize mobile users by multiple sensing reports.

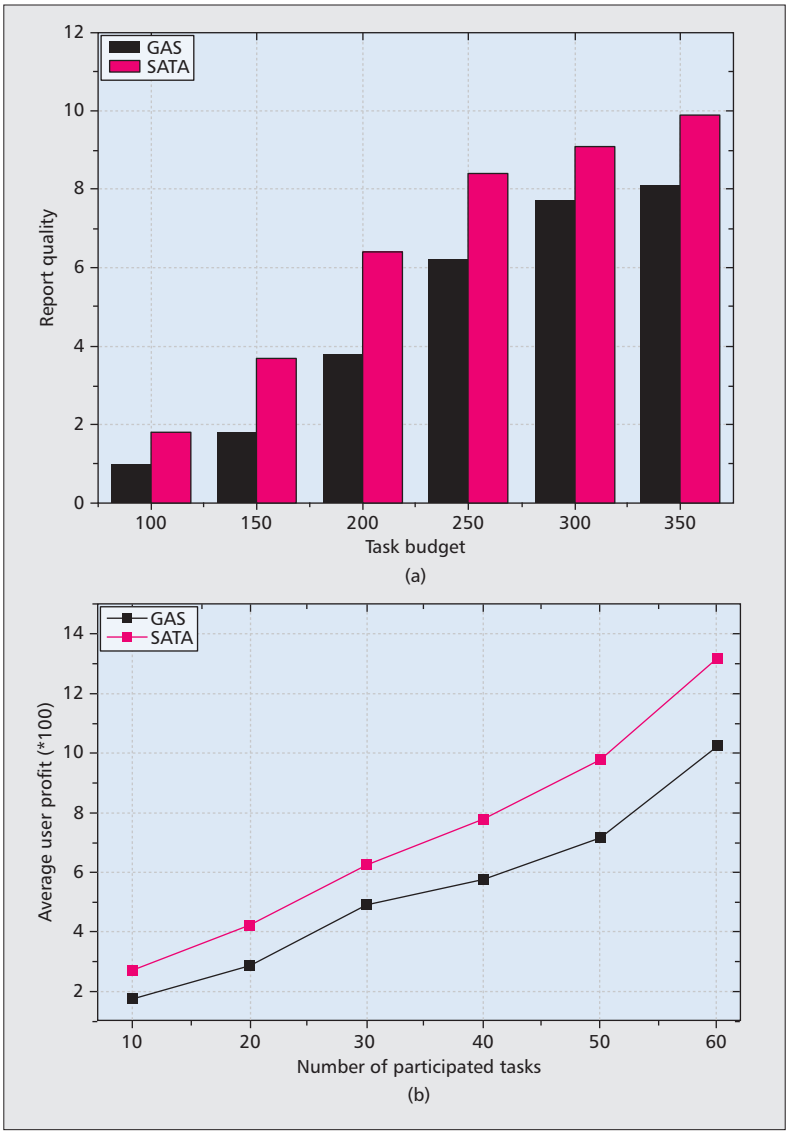

Figure 4. Performance comparison between SATA and GAS[2]: a) task report quality comparison; b) average user profit comparison.

Future Research Directions and Challenges

Recent research has provided some feasible solutions for the key challenges in mobile crowdsourcing, triggering an explosion of mobile crowdsourcing applications. However, there is still a long way to go before researchers will witness the flourishing of mobile crowdsourcing. In this section we present future research directions and challenges to foster continued advancement in this emerging and evolving field of study.

Community Oriented Mobile Crowdsourcing

In mobile crowdsourcing, mobile users themselves form a social network, where the underlying social relationships and interactions cause a significant impact on task crowdsourcing. Social community, as a social structure consisting of individuals with common social interests or attributes, can be introduced into mobile crowdsourcing to improve

[2] The task report quality is determined by the accuracy and actual delay of task reports, while the user's profit is calculated by received task rewards minus task costs.

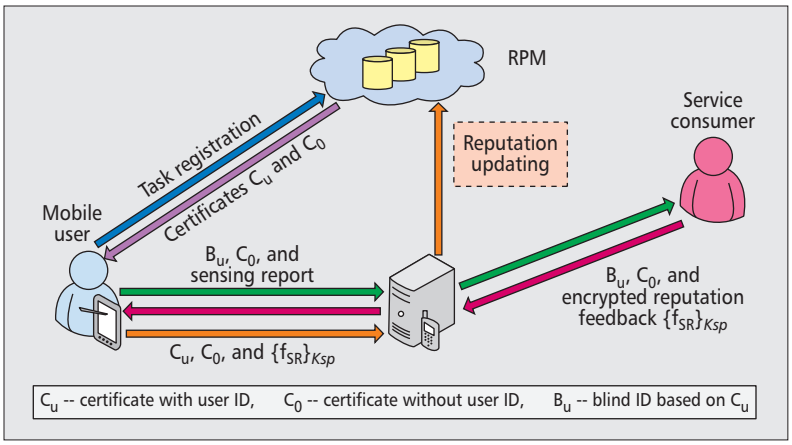

Figure 5. Illustration of anonymous reputation system for local-based mobile crowdsensing (K_{sp} is the public key of RPM).

the social aware task crowdsourcing. By introducing social community, service consumers can focus on outsourcing tasks to different social communities without considering which mobile user should be involved. Meanwhile, communities can recruit well-suited mobile users with required specialties and capabilities for service consumers to accomplish the specific tasks. By leveraging the hierarchical crowdsourcing, service consumers can enjoy more reliable services and achieve targeted task crowdsourcing, especially for tasks requiring specific data resources and processing background. However, exploring community oriented mobile crowdsourcing still faces some challenging issues. Mobile users of a community may contribute their efforts to maximize the profit or reputation of the community, rather than always being selfish. Therefore, task crowdsourcing would be impacted by stimulating users' contribution, and meet new challenges in balancing the benefits of mobile users and their community. In addition, since mobile users can simultaneously belong to different communities, task allocation of a community should consider many social factors (e.g., benefits for mobile users and communities, strength of the social ties between mobile users and different communities) to address the potential conflict of parallel task crowdsourcing in different social communities.

Exploring Big Data Applications by Mobile Crowdsourcing

Digging from previously inaccessible data sets is allowing companies and governments to improve operations and to discover some hidden regularities and new solutions to problems, making big data a hot topic in recent years. However, sorting and analyzing the mountains of information is a challenge even for the largest enterprises and institutions. This embarrassment could be eliminated by mobile crowdsourcing, which is able to exploit the spare processing power of millions of mobile devices and human brains via wireless communication networks. Furthermore, mobile crowdsourcing also provides a faster and more efficient way to access and collect a huge amount of data information from mobile users. The rapid evolution of wearable mobile devices and healthcare applications has proved that the vast potential market for personalized services is attracting industry attention based on mobile crowdsourcing assisted big data applications.

We can foresee the future of integrating mobile crowdsourcing and big data analytics from a successful example in Paris: Tranquilien. This is a smartphone app to help commuters pick a train where they are able to find a seat, based on urban mobility pattern modeling and mobile users' data contribution. By combining user contribution with search queries and location signals, it can accurately observe and predict origin-destination patterns, as well as where people change trains. The unpredicted success of Tranquilien indicates that mobile crowdsourcing and big data are converging, and providing unprecedented opportunities for this big data era. Unfortunately, the integration of mobile crowdsourcing and big data analytics brings not only opportunities but also challenges from both techniques. Since data collection is crowdsourced to a huge amount of various "always-on" mobile devices, the original challenges of data volume, velocity, and variety in big data analytics are amplified by mobile crowdsourcing. Furthermore, both big data and mobile crowdsourcing are still facing the challenge of privacy disclosure. Due to increasingly powerful data mining, personal privacy can be fully exposed even with advanced anonymity techniques. If we aim to outsource data collection to personal mobile devices, privacy concerns would be the biggest obstacle impeding the development of mobile crowdsourcing based big data applications.

Robust Evaluation of Multimedia Reports

In mobile crowdsourcing, fabricated or inaccurate task reports generally lead to useless and even misleading task results and cause significantly negative impacts on users' experiences. Therefore, report evaluation is critical for mobile crowdsourcing to evaluate the quality of aggregated task reports and identify false task reports, which is also the foundation of malicious attack detection. Existing works dealt with this challenge by recruiting multiple participants for a single outsourced task, and detected the false task reports by similarity analysis of these participants' reports [9, 12]. However, since task reports usually contain multimedia content, such as voice, pictures, and videos, especially in mobile crowdsensing, similarity analysis cannot apply to the evaluation of multimedia reports. For instance, if Bob outsources a real-time traffic-monitoring task for a specific area, the task reports could be in the form of pictures or videos. Regardless of which form the report is in, Bob will face the challenge of multimedia report evaluation. Although human evaluation can partially mitigate this challenge, it is not an efficient or even feasible solution for scalable report evaluation. Moreover, report evaluation is also vulnerable to collusion attacks and Sybil attacks, wherein malicious users collaboratively submit false task reports to subvert report evaluation. Therefore, future research can include exploiting an intelligent and robust evaluation scheme for multimedia reports to guarantee the quality and credibility of aggregated task reports, as well as malicious attack detection.

Conclusion

In this article we have investigated the mobile crowdsourcing architecture, and presented technical challenges with possible solutions to facilitate the implementation and development of mobile crowdsourcing. By outsourcing tasks to mobile users, mobile crowdsourcing can provide a highly efficient and cost-effective way to achieve pervasive cloud services. We have also discussed future research directions and challenges to nurture continuous improvements for mobile crowdsourcing. It is envisioned that mobile crowdsourcing will accelerate the pervasiveness and evolution of data collecting, processing, and computing.

Acknowledgment

This research work is supported by the International Science & Technology Cooperation Program of China under Grant No. 2013DFB10070, the China Hunan Provincial Science & Technology Program under Grant No. 2012GK4106, the National Natural Science Foundation of China under Grant No. 61272149, the Mittal Innovation Project of Central South University under Grant No. 12MX15, the Hunan Provincial Innovation Foundation for Postgraduate, and NSERC, Canada. Ju Ren is also financially supported by the China Scholarship Council.

References

[1] D. Huang, T. Xing, and H. Wu, "Mobile Cloud Computing Service Models: A User-Centric Approach." *IEEE Network*, vol. 27, no. 5, 2013, pp. 6–11.
[2] A. Faggiani *et al.*, "Smartphone-Based Crowdsourcing for Network Monitoring: Opportunities, Challenges, and a Case Study," *IEEE Commun. Mag.*, vol. 52, no. 1, 2014, pp. 106–13.
[3] J. Franklin *et al.*, "Crowddb: Answering Queries with Crowdsourcing," *Proc. ACM SIGMOD*, 2011, pp. 61–72.
[4] N. Fernando, W. Loke, and W. Rahayu, "Honeybee: A Programming Framework for Mobile Crowd Computing," *Mobile and Ubiq. Syst.: Comp., Net., and Services*, 2013, pp. 224–36.
[5] E. Koukoumidis, S. Peh, and M. R. Martonosi, "Signalguru: Leveraging Mobile Phones for Collaborative Traffic Signal Schedule Advisory," *Proc. ACM MobiSys*, 2011, pp. 127–40.
[6] M. Ra *et al.*, "Medusa: A Programming Framework for Crowd-Sensing Applications," *Proc. ACM MobiSys*, 2012, pp. 337–50.
[7] D. Yang, G. Xue, X. Fang, and J. Tang, "Crowdsourcing to Smartphones: Incentive Mechanism Design for Mobile Phone Sensing," *Proc. ACM Mobicom*, 2012, pp. 173–84.
[8] S. Reddy, D. Estrin, and M. Srivastava, "Recruitment Framework for Participatory Sensing Data Collections," *Pervasive Comp.*, 2010, pp. 138–55.
[9] S. He *et al.*, "Toward Optimal Allocation of Location Dependent Tasks in Crowdsensing," *Proc. IEEE INFOCOM*, 2014, to appear.
[10] X. Zhang *et al.*, "Robust Trajectory Estimation for Crowdsourcing-based Mobile Applications," *IEEE Trans. Parallel Distr. Sys.*, vol. 25, no. 7, 2013, pp. 1876–55.
[11] K. Huang, S. Kanhere, and W. Hu, "Are You Contributing Trustworthy Data?: The Case for a Reputation System in Participatory Sensing," *Proc. ACM MSWiM*, 2010, pp. 14–22.
[12] X. Wang *et al.*, "Enabling Reputation and Trust in Privacy-Preserving Mobile Sensing," *IEEE Trans. Mobile Comp.*, 2014, to appear.
[13] B. Liu *et al.*, "Cloud-Enabled Privacy-Preserving Collaborative Learning for Mobile Sensing," *Proc. ACM SenSys*, 2012, pp. 57–70.
[14] J. Ren *et al.*, "SACRM: Social Aware Crowdsourcing with Reputation Management in Mobile Sensing," *Computer Commun.*, 2015, http://dx.doi.org/10.1016/j.comcom.2015.01.022.
[15] K. Zhang *et al.*, "Exploiting Multimedia Services in Mobile Social Networks from Security and Privacy Perspectives," *IEEE Commun. Mag.*, vol. 52, no. 3, 2014, pp. 58–65.

Biographies

Ju Ren [S'13] (ren_ju@csu.edu.cn) received his B.Sc. and M.Sc. degrees in computer science from Central South University, China, in 2009 and 2012, respectively. He is currently a Ph.D. candidate in the Department of Computer Science at Central South University, China. Since August 2013 he has also been a visiting Ph.D. student in the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include wireless sensor network, mobile sensing/computing, and cloud computing.

Yaoxue Zhang (zyx@csu.edu.cn) received the B.S. degree from Northwest Institute of Telecommunication Engineering, China, and received the Ph.D. degree in computer networking from Tohoku University, Japan, in 1989. Currently he is a professor in the Department of Computer Science at Central South University, China, and also a professor in the Department of Computer Science and Technology at Tsinghua University, China. His current research interests include computer networking, operating systems, ubiquitous/pervasive computing, transparent computing, and active services. He has published over 200 technical papers in international journals and conferences, as well as nine monographs and textbooks. He is a fellow of the Chinese Academy of Engineering and the President of the Central South University, China.

Kuan Zhang [S'13] (k52zhang@bbcr.uwaterloo.ca) received his B.Sc. degree in electrical and computer engineering and M.Sc. degree in computer science from Northeastern University, China, in 2009 and 2011, respectively. He is currently working toward a Ph.D. degree in the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include packet forwarding, and security and privacy for mobile social networks.

Xuemin Shen [M'97, SM'02, F'09] (xshen@bbcr.uwaterloo.ca) received his B.Sc.(1982) degree from Dalian Maritime University, China, and his M.Sc. (1987) and Ph.D. (1990) degrees from Rutgers University, New Jersey, all in electrical engineering. He is a professor and university research chair, Department of Electrical and Computer Engineering, University of Waterloo. He was the associate chair for graduate studies from 2004 to 2008. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control and filtering. He has served as the Technical Program Committee Chair for IEEE VTC '10 Fall, Symposia Chair for IEEE ICC '10, Tutorial Chair for IEEE VTC '11 Spring and IEEE ICC '08, Technical Program Committee Chair for IEEE GLOBECOM '07, IEEE INFOCOM '14, General Co-Chair for Chinacom '07, QShine '06 and ACM MobiHoc '15, Chair for IEEE Communications Society's Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as editor-in-chief for *IEEE Network*, *Peer-to-Peer Networking and Applications*, and *IET Communications*. He is a founding area editor for *IEEE Transactions on Wireless Communications*; an associate editor for *IEEE Transactions on Vehicular Technology*, *Computer Networks*, and *ACM/Wireless Networks*. He has served as a guest editor for *IEEE JSAC*, *IEEE Wireless Communications*, *IEEE Communications Magazine*, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology and Communications Societies. He has been a guest professor of Tsinghua University, Shanghai Jiao Tong University, Zhejiang University, Beijing Jiao Tong University, Northeast University, and others.

Report evaluation is also vulnerable to collusion attacks and Sybil attacks. Therefore, future research can include exploiting an intelligent and robust evaluation scheme for multimedia reports to guarantee the quality and credibility of aggregated task reports, as well as malicious attack detection.