A User Incentive-Based Scheme Against Dishonest Reporting in Privacy-Preserving Mobile Crowdsensing Systems

Xinyu Yang[1], Cong Zhao[1](✉), Wei Yu[2], Xianghua Yao[3], and Xinwen Fu[4]

[1] Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an, People's Republic of China
yxyphd@mail.xjtu.edu.cn, zhaocong@stu.xjtu.edu.cn

[2] Department of Computer and Information Sciences, Towson University, Towson, USA
wyu@towson.edu

[3] School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, People's Republic of China
txyao@mail.xjtu.edu.cn

[4] Department of Computer Science, University of Massachusetts Lowell, Lowell, USA
xinwenfu@cs.uml.edu

Abstract. Proliferating Mobile Crowdsensing Systems (MCSs) is a promising paradigm to realize large-scale sensing targets in an agile and economical manner. Privacy protection mechanisms, which alleviate mobile user's concern on participating MCS tasks, also introduce the issue of data quality to the MCS server. In privacy-preserving MCSs, dishonest reporting of mobile sensing data from task participants could severely affect the MCS sensing accuracy. In this paper, we develop a user incentive-based scheme against dishonest reporting in privacy-preserving MCSs. Our proposed scheme is capable of improving the MCS sensing accuracy by encouraging users to honestly upload obtained sensing information for a higher serving profit. The performance of our scheme is evaluated via extensive real-world trace-driven simulations. Our experimental results show that our scheme can effectively ensure MCS sensing accuracy while encouraging honest reporting.

Keywords: Mobile Crowdsensing System · Data quality · User incentive

1 Introduction

As a promising sensing paradigm in the big data era, Mobile Crowdsensing Systems (MCSs) [1,2] aim at realizing large-scale sensing targets, including environment monitoring [3], online urban sensing [4], mobile social networking [5,6], and other Internet of Things applications [7,8], by leveraging pervasively distributed personal mobile smart devices. Mobile smart devices with enriched sensing capabilities are capable of providing fine-grained and economically cheap sensing

L. Ma et al. (Eds.): WASA 2017, LNCS 10251, pp. 755–767, 2017.
DOI: 10.1007/978-3-319-60033-8_64

services [9,10]. Considering the proliferation of MCS applications with improving security intensities [11,12], the potential privacy leakage raised by the use of personal mobile devices has been hindering the development of MCSs [13,14]. Realizing the importance of user privacy protection in MCSs, considerable research efforts have been devoted to preserving mobile user's privacy, including real identity [15], geological location [16,17], contributed data [18], among others.

Nonetheless, in privacy-preserving MCSs, it is difficult to relate a mobile user to its MCS task reports if the identity of real user is obscured. Thus, the quality of sensing data reported by mobile users is difficult to achieve due to the lack of accountable information. In addition, self-interested mobile users are more likely to report non-objective information in MCS tasks, considering that the cost of such dishonest behavior is negligible, while the benefits may be substantial and monetary. How to ensure the sensing data quality in privacy-preserving MCSs is essential for MCS in real-world practice.

In this paper, we present a user incentive-based scheme against potential dishonest reporting in privacy-preserving MCSs, which guarantees the quality of sensing data by rewarding honest users who upload objective sensing reports. Our contributions are summarized as follows: First, we develop an online method for the MCS server to simultaneously compute the sensing truth and estimate the quality of user-reported data without the use of any historical information. Our method is feasible in privacy-preserving MCSs, since it only requires the sensing observations of all participants of the assigned MCS task. Second, based on the developed data quality estimation method and user profit model, we present a user incentive-based method to encourage MCS participants to report objective information for higher profit. Our method can autonomously adjust the actual profit of each participant according to its impact on the entire system. In doing so, our method can ensure that honest participants are rewarded while dishonest participants are reprimanded. Third, we carry out a thorough evaluation on the performance of our proposed scheme based on extensive real-world trace-driven simulations. Simulation results demonstrate that our scheme can realize effective user incentives to guarantee the sensing accuracy of MCSs against dishonest reporting in privacy-preserving MCSs.

The remainder of the paper is organized as follows: In Sect. 2, we present the system model and describe the user incentive problem in privacy-preserving MCSs. In Sect. 3, we present our scheme in detail. In Sect. 4, we present our experimental design and the results of our performance evaluation. Finally, we conclude the paper in Sect. 5.

2 System Model and Problem Formalization

In this section, we first introduce the system model. As shown in Fig. 1, a general MCS consists of a cloud server s and a set of registered mobile users $\mathcal{P}$, where $|\mathcal{P}| \geqslant 2$. All users in $\mathcal{P}$ can communicate with s via either WiFi access points, or cellular base stations. For the privacy-preserving requirement, each user in $\mathcal{P}$ has a pseudo-identity $i \in \{1, 2, \ldots, i, \ldots, N\}$ (where $N = |\mathcal{P}|$), which enables anonymous communications between i and s (will be explained later).

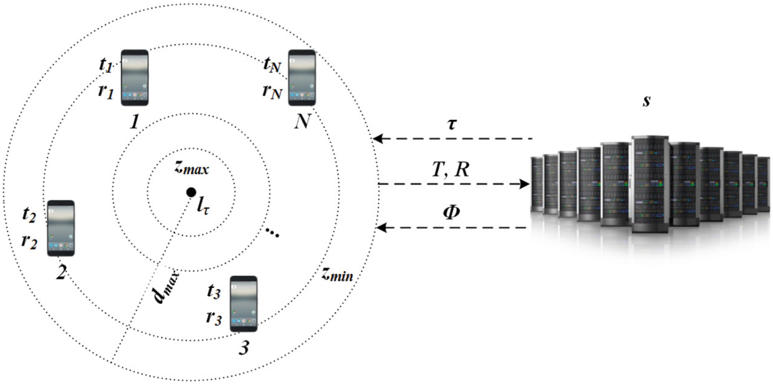


Fig. 1. A system model

For a specific MCS task τ, s publishes an announcement that clarifies the required sensing observation o_τ (e.g., what data is required), and the desired sensing location l_τ (e.g., where the data should be sensed). An user $i \in \mathcal{P}$ within the effective sensing area (e.g., the circular area with l_τ as the center, and d_{max} as the radius) can participate in τ according to their interests.

For each task participant $i \in \mathcal{E} = \{1, 2, \ldots, M\}$ ($\mathcal{E} \subseteq \mathcal{P}$), i determines its serving time t_i for τ based on its serving confidence c_i, and local status $\boldsymbol{x_i}$ (containing i's geological zone z_i and unit serving price p_i), which will be discussed later. Then, during the serving time t_i, a participant i conducts required sensing obligation and records corresponding observation o_i under s's instruction. When τ is finished, each $i \in \mathcal{E}$ uploads its sensing report $\boldsymbol{r}_i$, which contains o_i, c_i and $\boldsymbol{x_i}$, to s. According to $\mathcal{T} = \{t_1, t_2, \ldots, t_M\}$ and $\mathcal{R} = \{\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_M\}$, s pays corresponding monetary credits $\Phi = \{\phi_1, \phi_2, \ldots, \phi_M\}$ to $\mathcal{E}$.

We now explicitly define the user incentive problem in privacy-preserving MCSs. To begin with, we clarify the privacy-preserving settings in MCSs. We consider the protection of user privacy with respect to both real identities and precise geological locations. First, via anonymous communications based on pseudo-identities that are dynamically adjusted, the cloud server s will not maintain any derivative relation between sensing reports and their generators. For any user i, no information about its real identity will be disclosed because of participating in MCS tasks[1]. Second, instead of precise GPS coordinates, s is only interested in the rough geological locations of MCS task participants. As illustrated in Fig. 1, the effective sensing area is divided into several geological zones (i.e., from z_{min} to z_{max}, approaching the desired sensing location l_τ). As a user i only uploads its geological zone z_i as a part of its local status, the cloud server s cannot obtain the precise spatial-temporal tracks of MCS task participants.

[1] As this can be achieved according to anonymous communications described in [19–22], we provide no further discussion.

In order to provide incentives to users to participate in the sensing efforts in MCSs, it is reasonable for the cloud server s to pay the maximum credits to MCS task participants as a stimulation. Nonetheless, to guarantee MCS sensing accuracy, the actual profit that a participant can obtain by serving a certain task must be determined by the quality of its reported data and its serving costs. In privacy-preserving MCSs, the estimation of reported data quality is challenging for the reasons outlined as follows. First, the lack of relation between real identities and reported data of users obstructs the accountability of historical user behaviors. Second, it is highly possible that self-interested users report dishonestly for higher profits, especially in the non-accountable privacy-preserving scenario. Therefore, to achieve effective user incentives that encourage mobile users to upload quality reports in privacy-preserving MCS tasks, the cloud server s needs to address the following three problems: (i) How to estimate the quality of reported data without knowing user historical behaviors, (ii) How to maximize a participant's profit for stimulation according to the quality of its report, and (ii) How to realize effective user incentives against potential dishonest reporting.

3 Our Approach

In this section, we design our approach to address the aforementioned three problems.

3.1 Online Quality Estimation of User-Reported Data

In the following, we address the issue of how to estimate the quality of the sensing data reported, using only the information related to the current MCS task. Considering the fact that there is no available ground truth of an MCS task τ, meanwhile there is no referable historical information of task participants, s needs to compute τ's sensing truth o_τ according to all reported sensing observations $\mathcal{O} = \{o_1, o_2, \ldots, o_M\}$, which is treated as the criterion to estimate the quality of user-reported data.

To compute o_τ for the estimation of reported data quality, we construct Algorithm 1 based on the sensing truth discovery process in our prior work [23]. Here, it is worth noting the difference between Algorithm 1 and the truth discovery process in [23]: since the work of [23] did not focus on the privacy-preserving scenario, its weighted truth discovery process has access to the historical reputation of each participant, which reflects the prior credibility of its sensing observation. Nonetheless, our Algorithm 1 computes the sensing truth only based on observations of the current task. In addition, the primary purpose of truth discovery in [23] is to evaluate each participant's contribution to the MCS task, while the purpose of our Algorithm 1 is to estimate the quality of reported observations.

3.2 User Profit Definition and Maximization

In this subsection, we formally define the computation of user profits for serving MCS tasks. Meanwhile, we further demonstrate that any participant of an MCS task can obtain its maximum profit only when it behaves honestly and uploads an objective sensing report.

Intuitively, for each participant $i \in \mathcal{M}$ of task τ, its serving profit ϕ_i is determined by considering its serving time t_i ($t_i \geqslant 0$), serving confidence c_i ($0 < c_i \leqslant 1$), reported observation o_i, and local status $\boldsymbol{x_i} = (z_i, p_i)$ (i.e., geological zone z_i ($z_{min} \leqslant z_i \leqslant z_{max}$), and unit serving price p_i ($0 < p_i \leqslant 1$)). Here, c_i indicates the expected quality of i's observation o_i, and p_i indicates i's synthesized unit cost with respect to battery and network traffic for serving τ.

Algorithm 1. Data Quality Estimation based on Truth Discovery

```
Input:
$\mathcal{O}$: observations of $\forall i \in \mathcal{M}$;
$\epsilon$: convergence threshold of truth discovery;
Output:
$\mathcal{Q}$: data quality of $\forall i \in \mathcal{M}$.

Compute the standard deviation of $\mathcal{O}$: $std_{\mathcal{O}}$;
Initialize the discovered truth $o_\tau$ as a random value;
Initialize $\forall w_i \in \mathcal{W} = 0$ as the initial weight of $\forall o_i \in \mathcal{O}$;
Initialize $\forall q_i \in \mathcal{Q} = 0$ as the initial data quality of $\forall i \in \mathcal{M}$;
repeat
    for $\forall i \in \mathcal{M}$ do
        $w_i = \log(\frac{\sum_{j \in \mathcal{M}} \frac{(o_j - o_\tau)^2}{std_{\mathcal{O}}}}{\frac{(o_i - o_\tau)^2}{std_{\mathcal{O}}}})$;
    $o'_\tau = o_\tau$;
    $o_\tau = \frac{\sum_{j \in \mathcal{M}} w_j o_j}{\sum_{j \in \mathcal{M}} w_j}$;
until $|o_\tau - o'_\tau| < \epsilon$;
for $\forall q_i \in \mathcal{Q}$ do
    $q_i = 1 - \frac{|o_i - o_\tau|}{o_\tau}$;
return $\mathcal{Q}$;
```

Specifically, participant i can compute its expected serving profit $\hat{\phi}_i$ as:

$$\hat{\phi}_i = c_i t_i - p_i \frac{z_i}{z_{max}} t_i^2. \tag{1}$$

Similarly, the cloud server i can derive i's actual serving profit ϕ_i as:

$$\phi_i = q_i t_i - p_i \frac{z_i}{z_{max}} t_i^2. \tag{2}$$

where q_i can be estimated according to Algorithm 1 based on $\mathcal{O}$.

From a practical perspective, we assume that, for each MCS task τ, participant i can locally determine t_i, c_i, and o_i all by itself, whereas z_i and p_i are extracted by mobile device firmware as its local status $\boldsymbol{x}_i$. In this case, it is easy to obtain that $\hat{\phi}_{imax} = \frac{z_{max}c_i^2}{4p_iz_i}$ when participant i determines to serve τ for $\hat{t}_{imax} = \frac{z_{max}c_i}{2p_iz_i}$. Because $\boldsymbol{x}_i$ is always objectively reported, there is $\phi_{imax} = \hat{\phi}_{imax}$ only when $q_i = c_i$. Therefore, if participant i uploads a more objective c_i that was closer to q_i, and serves for $\hat{t}_{imax}$, he or she should obtain an actual profit ϕ_i, which is closer to $\hat{\phi}_{imax}$. According to Subsect. 3.1, for each MCS participant, an effective way to enhance the quality of reported data in privacy-preserving MCSs is to honestly report objective sensing observations.

3.3 User Incentive-Based Scheme Against Dishonest Reporting

Based on our data quality estimation mechanism and user serving profit model, we now design a user Incentive-based scheme Against Dishonest Reporting (IADR) for cloud servers of privacy-preserving MCSs.

According to Subsect. 3.2, each participant $i \in \mathcal{M}$ of task τ can determine t_i, c_i, and o_i in its sensing report r_i. In fact, participants may report dishonestly for potentially higher profits, considering their self-interested nature. To encourage participants to upload objective reports, the cloud server s is responsible for rewarding participants for quality data and reprimand those who are dishonest. Nonetheless, this is difficult to realize based solely on our data quality estimation method and user serving profit model.

From the perspective of the cloud server s, local report determinations of all participants can be formalized as a non-cooperative game, considering the fact that each $i \in \mathcal{M}$ does not know about the decisions of the other participants. Thus, inspired by the BMT algorithm in [24], we developed the IADR scheme for cloud server s to autonomously enhance/downgrade the serving profit of each participant according to its actual impact on the total profit of all participants. Specifically, IADR consists of two components: (i) *Zone-Distinguished Quality Estimation* and (ii) *Impact-Driven Profit Determination.*

Zone-Distinguished Quality Estimation. When receiving all $r_i \in \mathcal{R}$ of a single MCS task τ, it is reasonable for cloud server s to separately estimate the quality of the reported data of different geological zones, considering the fact that sensing observations at different distances from the desired sensing location are likely to be different. The quality of each observation is estimated considering all other observations from its same zone.

Impact-Driven Profit Determination. After obtaining all $q_i \in \mathcal{Q}$, s needs to determine the final serving profit ϕ_i for each $i \in \mathcal{M}$ based on $\mathcal{T}$, $\mathcal{R}$ and $\mathcal{Q}$. Specifically, our impact-driven profit determination process is shown in Algorithm 2: if a participant has a positive effect on τ, it deserves a bonus reward; otherwise it will be reprimanded.

Algorithm 2. Impact-Driven Profit Determination

```
Input:
$\mathcal{T}$: serving time of $\forall i \in \mathcal{M}$;
$\mathcal{R}$: sensing reports of $\forall i \in \mathcal{M}$, where $r_i = (o_i, c_i, z_i, p_i)$;
$\mathcal{Q}$: data qualities of $\forall i \in \mathcal{M}$;
Output:
$\Phi$: final profits of $\forall i \in \mathcal{M}$.

for $\forall i \in \mathcal{M}$ do
    calculate $\phi_i = q_i t_i - p_i \frac{z_i}{z_{max}} t_i^2$;
for $\forall i \in \mathcal{M}$ do
    for $\forall j \in \mathcal{M}/i$ do
        calculate $\phi'_j = \frac{z_{max} q_j^2}{4 p_j z_j}$;
    calculate $\delta_i = \sum_{j \in \mathcal{M}/i} \phi_j - \sum_{j \in \mathcal{M}/i} \phi'_j$;
    $\phi_i = \phi_i + \delta_i$;
return $\Phi$;
```

4 Performance Evaluation

In this section, we demonstrate the effectiveness of IADR in confronting dishonest reporting through extensive simulations. In the following, we first describe the evaluation methodology and then present evaluation results.

4.1 Evaluation Methodology

To evaluate the effectiveness of IADR, our evaluation adopted a real-world outdoor temperature dataset crowdsensed by taxis in Rome, Italy [25]. The used dataset contains 4485 entries, which are opportunistically uploaded by 366 taxis within 24 h. Each entry contains a temperature sensing observation, its generator, sensing time, and the GPS coordinates of the sensing location.

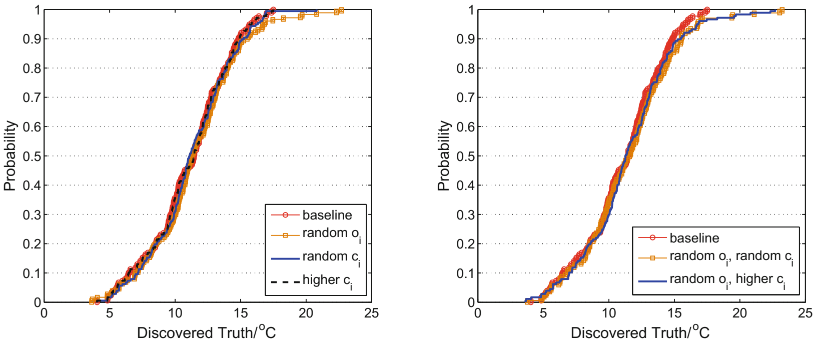
According to the dataset, we constructed an MCS with one cloud server and 366 mobile users on the OMNeT++4.6 simulator. A fixed effective sensing area was divided into 5 geological zones (i.e., $z_{min} = 1$, $z_{max} = 5$), and GPS coordinates in all data entries were mapped into corresponding geological zones. For each round of simulation, the cloud server spontaneously announced MCS tasks, and each user participated in the tasks and uploaded sensing reports according to corresponding data entries. Each round of simulation lasted for 86400 simulation seconds.

In terms of parameter settings, we set unit serving price p of all users as 0.5 for the sake of simplicity, and set the truth discovery convergence threshold $\epsilon = 0.1$ for controlling accuracy. For benign participants who follow the system regulations, the serving confidence c is set as the estimated data quality in the last MCS task q'. They serve each task for $\hat{t}_{max}$ before uploading objective sensing report r. Nonetheless, for potential dishonest participants, they may upload non-objective sensing observation o or/and serving confidence c.

In our simulations, we formulated two patterns of dishonest reporting from participants: (i) only a single factor in the report is non-objective (i.e., random o_i ($2\,^{\circ}\mathrm{C} \leqslant o_i \leqslant 24\,^{\circ}\mathrm{C}$), random c_i ($0 < c_i \leqslant 1$), or higher c_i ($c_i = 1$)), and (ii) there are multiple non-objective factors in the report (i.e., random o_i and random c_i, or random o_i and higher c_i). Without introducing any dishonest reporting into the system deliberately, we ran a round of simulation, in which all participants followed system regulations as our baseline scenario. Then, we designed two sets of experiments to analyze the impacts of dishonest reporting on MCS's sensing accuracy and participant's serving profit, respectively. We further discussed whether IADR can realize effective user incentive against dishonest reporting based on the results.

4.2 Impact of Dishonest Reporting on MCS's Sensing Accuracy

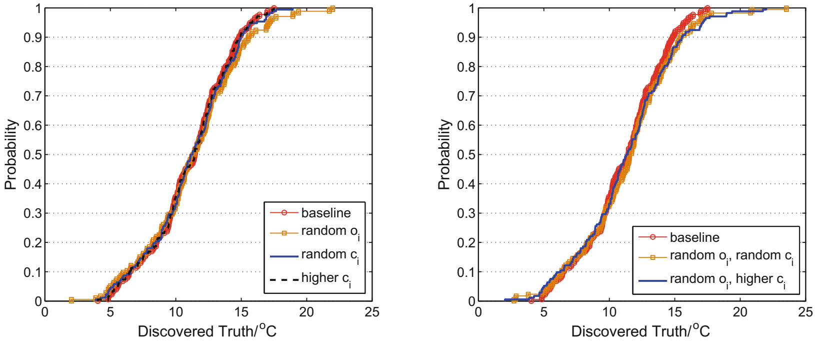
Considering the fact that the primary requirement of MCS is to achieve accurate sensing, we investigate the impacts of different ratios of dishonest reporting (i.e., the ratio of dishonest reporting to total reports) on MCS's sensing accuracy in this set of experiments. Specifically, we conducted two groups of simulations, where all participants were set to perform dishonest reporting at rates of 10% and 15% in all MCS tasks, respectively. One thing should be noted is that our settings should be reasonably considering the ratio of malicious behaviors in existing mechanisms (e.g., 10% in [26] and 4% in [27]). All discovered sensing truths during simulations were collected, and their cumulative distributions are shown in Figs. 2 and 3.



(a) Single Factor Impact (b) Multiple Factors Impact

Fig. 2. Impact of general dishonest reporting (10%) on discovered truth

According to Fig. 2, we can observe that: with a 10% general dishonest reporting ratio, neither the report with single non-objective factor, nor the report with multiple non-objective factors obviously affects the cumulative distribution of discovered sensing truth. In detail, the average discovered sensing truth of the 'baseline' scenario is 11.28 °C, and that of other scenarios are: (i) random o_i: 11.39 °C, (ii) random c_i: 11.26 °C, (iii) higher c_i: 11.28 °C, (iv) random o_i and random c_i: 11.54 °C, (v) random o_i and higher c_i: 11.39 °C. The maximum deviation of the average sensing truth is 2.30%, which is nearly negligible, especially considering that 10% of the total reporting are non-objective.



(a) Single Factor Impact (b) Multiple Factors Impact

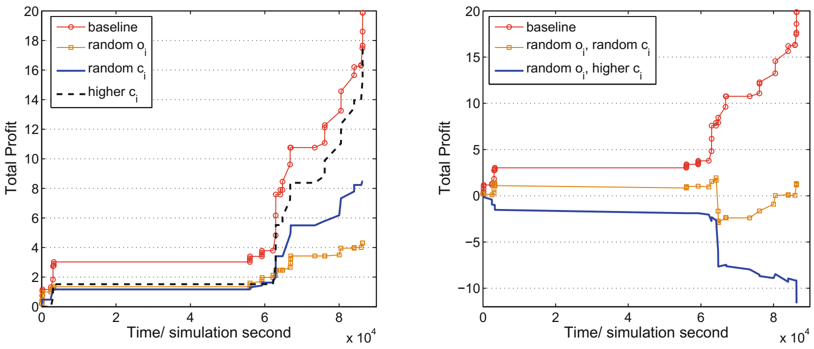
Fig. 3. Impact of general dishonest reporting (15%) on discovered truth

According to Fig. 3, the evaluation results with a 15% general dishonest reporting ratio is similar: the cumulative distribution of discovered sensing truth is not significantly affected by either single non-objective factor or multiple non-objective factors, and the maximum deviation of the average sensing truth is 2.04%, which is also negligible.

To summarize, the evaluation results indicate that IADR can effectively guarantee the MCS sensing accuracy in MCSs with dishonest reporting.

4.3 Impact of Dishonest Reporting on User Profit

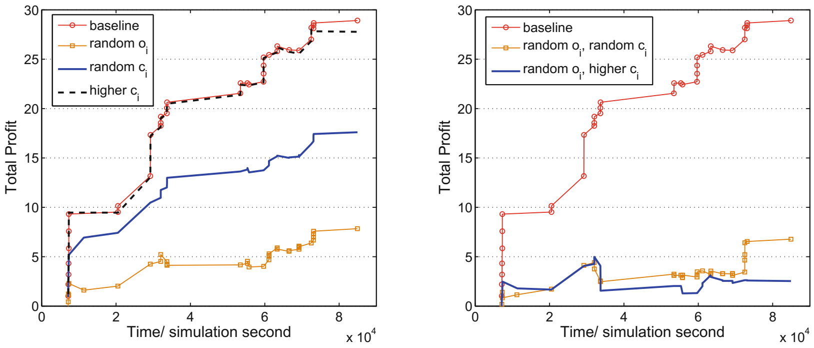
Considering the fact that the essential reason for mobile users to participate in MCS tasks is to obtain profit for sensing services offered, we investigate the impact of a user's dishonest reporting on its own serving profit in this set of experiments. Specifically, we conducted three groups of simulations, where the user (i) participates in the most number of MCS tasks (i.e., the TopC user), (ii) obtains the most serving profit (i.e., the TopP user), and (iii) obtains less serving profit (i.e., the LessP user), in the baseline scenario was set to perform dishonest reporting in all MCS tasks, respectively. It should be reasonable for us to evaluate these representative users for a thorough understanding on IADR's performance. The variations of the total serving profit of these users along an entire simulation round were collected, which are depicted in Figs. 4, 5, and 6.



(a) Single Factor Impact

(b) Multiple Factors Impact

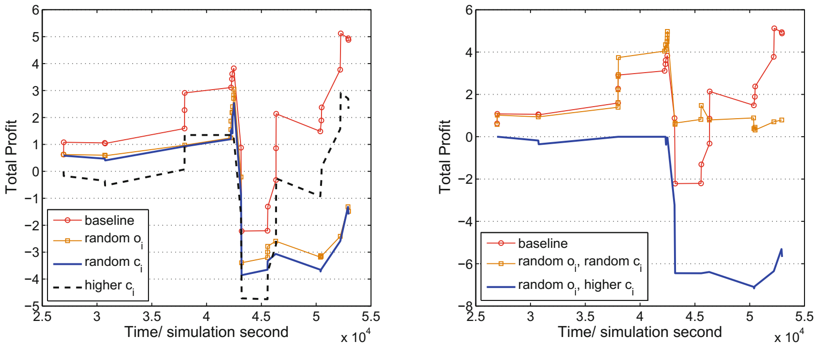
Fig. 4. Impact of TopC user's dishonest reporting on its total profit



(a) Single Factor Impact

(b) Multiple Factors Impact

Fig. 5. Impact of TopP user's dishonest reporting on its total profit



(a) Single Factor Impact

(b) Multiple Factors Impact

Fig. 6. Impact of LessP user's dishonest reporting on its total profit

According to Fig. 4, we can observe that the total profit of the TopC user is severely downgraded as long as it reports non-objective factor/factors. In detail, in the 'baseline' scenario, its total profit at the end of the simulation round is 19.87, and that of other scenarios are: (i) random o_i: 4.32 (−78.26%), (ii) random c_i: 8.49 (−57.27%), (iii) higher c_i: 17.58 (−11.52%), (iv) random o_i and random c_i: 1.33 (−93.31%), (v) random o_i and higher c_i: −11.63 (−158.53%). Although that the TopC user is one of the most active users in the MCS, its serving profit is still dominated by the quality of its reports.

According to Fig. 5, we can see that as long as the TopP user performs non-objective reporting, its total profit will be severely downgraded. Considering the fact that the TopP user is one of those who provides the most quality sensing reports in the MCS, objective reporting is demonstrated to be effective in enhancing a user's serving profit.

According to Fig. 6, the total profit of the LessP user is also severely downgraded if it uploads non-objective reports. In addition, since the LessP user can represent the majority of MCS participants (e.g., mediocre ones), the simulation results indicate that, with the adoption of IADR, the LessP user cannot obtain higher profit by uploading non-objective reports.

To summarize, our results demonstrate that IADR achieves effective user incentive against dishonest reporting in MCSs.

5 Conclusion

In this paper, we developed a user incentive-based scheme against dishonest reporting in privacy-preserving MCSs, which encourages mobile users to honestly report sensing information. To be specific, we first developed an online mechanism for the MCS server to estimate the quality of reported data. We then constructed a serving profit model, which would maximize the profit of honest users. Further, we developed a mechanism for the MCS server to autonomously reward honest users, while reprimanding those who are dishonest. To demonstrate the effectiveness of our proposed scheme, we performed an extensive performance evaluation using real-world crowdsensing data. Our experimental results demonstrated that our scheme can ensure MCS sensing accuracy when there exists harsh dishonest reporting, meanwhile it can effectively reprimand users who report dishonest sensing information.

References

1. Guo, B., Wang, Z., Yu, Z., Wang, Y., Yen, N., Huang, R., Zhou, X.: Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm. ACM CSUR **48**(1), 7 (2015)
2. Duan, Z., Li, W., Cai, Z.: Distributed auctions for task assignment and scheduling in mobile crowdsensing systems. In: Proceedings of IEEE ICDCS (2017)
3. Capezzuto, L., Abbamonte, L., De Vito, S., Massera, E.: A maker friendly mobile and social sensing approach to urban air quality monitoring. In: Proceedings of IEEE Sensors, pp. 12–16 (2014)

4. Gao, R., Zhao, M., Ye, T., Ye, F., Wang, Y., Bian, K., Wang, T., Li, X.: Jigsaw: indoor floor plan reconstruction via mobile crowdsensing. In: Proceedings of ACM Mobicom, pp. 249–260 (2014)
5. Bakht, M., Trower, M., Kravets, R.: Searchlight: won't you be my neighbor? In: Proceedings of ACM Mobicom, pp. 185–196 (2012)
6. Li, J., Cai, Z., Yan, M., Li, Y.: Using crowdsourced data in location-based social networks to explore influence maximization. In: Proceedings of IEEE Infocom (2016)
7. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on internet of things: architecture, enabling technologies, security and privacy, and applications. IEEE Internet-of-Things (IoT) J. (2017)
8. Ren, X., Yang, X., Lin, J., Yu, W.: On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems. IEEE Trans. Parallel Distrib. Syst. **27**(10), 2967–2983 (2016)
9. Yurur, O., Liu, C., Sheng, Z., Leung, V.: Context-awareness for mobile sensing: a survey and future directions. IEEE Commun. Surv. Tuts. **18**(1), 68–93 (2016)
10. Duan, Z., Yan, M., Cai, Z., Wang, X., Han, M., Li, Y.: Truthful incentive mechanisms for social cost minimization in mobile crowdsourcing systems. Sensors **16**(4), 481 (2016)
11. Zhao, C., Yang, S., Yang, X., McCann, J.: Rapid, user-transparent, and trustworthy device pairing for D2D-enabled mobile crowdsourcing. IEEE Trans. Mob. Comput. (99), 1 (2016)
12. Na, R., Gao, L., Zhu, H., Jia, W., Li, X., Hu, Q.: Toward optimal dos-resistant authentication in crowdsensing networks via evolutionary game. In: Proceedings of IEEE ICDCS, pp. 364–373 (2016)
13. He, D., Chan, S., Guizani, M.: User privacy and data trustworthiness in mobile crowd sensing. IEEE Wirel. Commun. **22**(1), 28–34 (2015)
14. Wang, Y., Cai, Z., Ying, G., Gao, Y., Tong, X., Wu, G.: An incentive mechanism with privacy protection in mobile crowdsourcing systems. Comput. Netw. **102**, 157–171 (2016)
15. Wang, X., Cheng, W., Mohapatra, P., Abdelzaher, T.: Enabling reputation and trust in privacy-preserving mobile sensing. IEEE Trans. Mob. Comput. **13**(12), 2777–2790 (2014)
16. Wang, W., Zhang, Q.: Location privacy preservation in collaborative spectrum sensing. In: Proceedings of IEEE Infocom, pp. 729–737 (2012)
17. To, H., Ghinita, G., Shahabi, C.: A framework for protecting worker location privacy in spatial crowdsourcing. Proc. VLDB Endow. **7**(10), 919–930 (2014)
18. Li, Q., Cao, G.: Providing efficient privacy-aware incentives for mobile sensing. In: Proceedings of IEEE ICDCS, pp. 208–217 (2014)
19. Ling, Z., Yang, M., Lou, J., Fu, X., Yu, W.: De-anonymizing and countermeasures in anonymous communication networks. IEEE Commun. Mag. **53**(4), 60–66 (2015)
20. Pingley, A., Yu, W., Zhang, N., Fu, X., Zhao, W.: Cap: a context-aware privacy protection system for location-based services. In: Proceedings of IEEE ICDCS, pp. 49–57 (2009)
21. Yu, W., Fu, X., Graham, S., Xuan, D., Zhao, W.: DSSS-based flow marking technique for invisible traceback. In: Proceedings of IEEE S&P, pp. 18–32 (2007)
22. Ling, Z., Luo, J., Yu, W., Fu, X., Xuan, D., Jia, W.: A new cell-counting-based attack against Tor. IEEE/ACM Trans. Netw. **20**(4), 1245–1261 (2012)
23. Zhao, C., Yang, X., Yu, W., Yao, X., Lin, J., Li, X.: Cheating-resilient incentive scheme for mobile crowdsensing systems. In: Proceedings of IEEE CCNC, pp. 1–6 (2017)

24. Yang, S., Adeel, U., McCann, J.: Backpressure meets taxes: faithful data collection in stochastic mobile phone sensing systems. In: Proceedings of IEEE Infocom, pp. 1490–1498 (2015)
25. Alswailim, M.A,. Hassanein, H.S., Zulkernine, M.: CRAWDAD dataset queensu/crowd_temperature (v.2015-11-20) (2015). http://crawdad.org/queensu/crowd_temperature/20151120
26. Li, X., Zhou, F., Yang, X.: Scalable feedback aggregating (SFA) overlay for large-scale P2P trust management. IEEE Trans. Parallel Distrib. Syst. **23**(10), 1944–1957 (2012)
27. Shen, H., Lin, Y., Sapra, K., Li, Z.: Enhancing collusion resilience in reputation systems. IEEE Trans. Parallel Distrib. Syst. **27**(8), 2274–2287 (2016)