Kim *EURASIP Journal on Wireless Communications and Networking* (2019) 2019:158
https://doi.org/10.1186/s13638-019-1479-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A new differential privacy preserving crowdsensing scheme based on the Owen value

Sungwook Kim

Abstract

The Internet of Everything (IoE) paradigm makes the Internet more pervasive, interconnecting every devices of everyday life, and it is a promising solution for the development of 5G network services. Nowadays, Internet-connected devices are equipped with various built-in sensors. Therefore, the concept of mobile crowdsensing (MC) has been introduced to the IoE-driven situation where mobile devices gather data with the aim of performing a specific application. In this paper, we propose a new cooperative game model for the privacy-driven device collaboration in the MC system. The major goal of our approach is to incentivize the participating devices for effective data acquisitions while protecting each individual privacy based on each device's preference. According to the Owen value mechanism, the proposed scheme provides an effective payment solution for each MC participating device under privacy considered IoE environments. The main merit possessed by our MC control approach is to guide the cooperation of mobile devices in providing MC services. Performance evaluation reveals the superiority of our proposed scheme in terms of task success ratio, MC participating ratio, and payoff fairness. Finally, we provide the guidance on the future research direction of the MC system including other issues.

Keywords: Internet of everything, Mobile crowdsensing, Differential privacy, Owen value, Cooperative game theory

1 Introduction

The highly distributed Internet of Everything (IoE) paradigm envisions everyday life devices to be smart to communicate with each other, and extends ubiquity of the Internet through integrating each mobile device for the interaction via embedded systems. IoE devices are uniquely identifiable and are equipped with multiple types of sensors. These IoE devices can be used to sense and collect data dynamically from the surrounding environment, without the need to build new infrastructures. The collected data can be delivered to the centralized server, where they can be further aggregated to get a collective intelligence. Taking advantage of the variety data generated by these devices will foster the development of innovative applications in a broad range of domains [1–4].

All above-mentioned properties make IoE a perfect choice for the mobile crowdsensing (MC). MC is a pervasive sensing paradigm where mobile devices can often replace static sensing infrastructures, and considerably advantageous for applications such as healthcare analytics, route planners, and social-related applications [5]. In MC operations, devices, i.e., smartphones, tablets, and IoE devices like wearables, serve data generated from embedded sensors. Usually, the performance of MC depends on the number of participating devices, which are contributing to complete sensing tasks. Therefore, how to recruit mobile devices while fulfill sensing tasks with high accuracy is a key challenge in MC systems. Recently, several recruitment policies have been proposed in the literature with the aim of addressing the MC operations [6].

Proper recruitment policies can successfully assemble mobile devices that are able to fulfill sensing tasks while minimizing system costs [6]. Therefore, MC schemes should incorporate efficient payment mechanisms to recruit devices for their MC contributions. Currently, the payment issue in MC systems has been extensively studied by giving devices' rewards to cover their

Correspondence: swkim01@sogang.ac.kr
Department of Computer Science, Sogang University, 35 Baekbeom-ro (Sinsu-dong), Mapo-gu, Seoul 04107, South Korea

contributions of individual sensing activities. Different kinds of devices may have diverse sensing contributions due to the difference in device mobility, ambient noise, energy consumed for sensing, etc. Thus, rather than treating all participating devices equally, we consider devices' actual contributions and their individual conditions to design a reward-based payment mechanism.

During MC operations, sensing devices potentially collect sensitive data of individuals. Therefore, privacy issue also arises as another key problem. For example, the GPS embedded device usually senses the private information of individual commuting routes and locations. By sharing the GPS measurements, end users' privacy can be revealed. Hence, it is important and necessary to preserve the security and privacy of each individual. Even though privacy protection is a principal issue, it has not yet been well addressed, especially in the MC system. Few existing work systematically investigates the privacy protection problem considering the tradeoff between privacy preservation and sensed data accuracy [7–10].

Differential privacy (DP) has been introduced and gained popularity as a formal quantifiable measure of privacy risk. Usually, the DP captures the increased risk to one's privacy incurred by participating in a database. In particular, it measures how much the outcome of a procedure changes probabilistically by the presence or absence of any single subject in the original data; the measure provides an upper bound on privacy loss regardless of any prior knowledge an adversary might have. While the DP has been applied in various research fields, it has become a hot research topic in MC systems. In this paper, we integrate the DP technique into the MC system while providing effective payments to participating devices. This approach can ensure a strong protection against various types of possible attacks in security, and conduces implicit collaboration of participating devices [11–14].

To design a novel DP-based MC control scheme, we need a game-theoretic payment mechanism. Generally, payment mechanisms are characterized using the cooperative game theory. Currently, game theory is extensively used for the model and analysis of competition and cooperation situations between the rational agents. Being the control theory of multiple goal-driven agents, game theory can provide effective solutions for dealing with the DP-based MC situation and questions. Motivated by this factor, we have adopted a novel cooperative game-based payment approach to design a new practical MC control scheme. This approach is a more practical and justified method for real world MC operations [15].

In this study, we address the challenges of MC algorithm, payment algorithm, and DP algorithm. These algorithms are combined in an integrated scheme in order to strike the appropriate performance balance between contradictory requirements. To adapt dynamically changing MC environments, our holistic scheme is designed to harness the synergies between competitive and cooperative interactions among MC agents. To adaptively responsive to individual MC agents, our payment process is operated according to the cooperative game manner, especially the Owen value. As an extension of the Shapley value, Owen value was defined as an efficient solution for cooperative games with coalition structure; it has been successfully applied in many engineering fields [16]. The proposed scheme mainly considers how to estimate an individual payment for each device. Based on the Owen value approach, our scheme achieves greater and reciprocal advantages while offering a well-balanced solution in MC operations. Although several MC algorithms including the DP concept have been proposed, no systematic study has been conducted. The contributions of this study can be summarized as follows:

- Owen value implementation: we introduce a novel cooperative game model while capturing dynamic interactions of MC agents depending on their different viewpoints. This approach is generic and applicable to implement real-world MC operations.
- Payment mechanism for devices: we implement a payment mechanism based on the Owen value. To attract enough mobile devices' participations, their resource consumption and the risk of privacy exposure are compensated with rewards through our payment mechanism.
- Differential privacy algorithm: we employ the basic concept of DP to formalize the notion of devices' privacy. To protect the sensitive information that needs to be released, our DP algorithm can preserve devices' private data by data anonymization. The level of data protection will accordingly be used to set the rewarding payment to encourage their true data.
- The synergy of combined algorithms: we explore the sequential interaction of MC, payment and DP algorithms, and jointly design an integrated scheme to strike an appropriate performance balance between conflicting requirements. The synergy effect lies in its responsiveness to the reciprocal combination of different control algorithms.
- Practical implementation: we investigate the dynamic MC environment based on the step-by-step distributed cooperative game process. This is a suitable and practical approach for real-world MC operations.
- Performance analysis: we evaluate the performance of the proposed scheme based on the simulation model. Numerical study demonstrates that the

overall system performance of our proposed scheme can be significantly improved by comparing to the existing [17–19] schemes.

The rest of the paper is structured as follows. Next section, we review the related work. Section 3 describes the principal of the MC platform, presents the problem formulation, and proposes the Owen value-based MC control scheme. In addition, we show the main steps of the proposed scheme to increase readability. The simulation scenario and the experimental results while comparing with some existing methods are detailed in Section 4. Section 5 concludes the paper. In this section, we also discuss the remaining open challenges in this research area along with possible solutions.

2 Related work

There has been considerable research into the implementation of privacy-based MC algorithms. In [20], Yuichi Sei et al. proposed a new anonymized data-collection scheme that can estimate data distributions more accurately. They prove that their proposed method can reduce the mean squared error and the Jensen-Shannon divergence compared with other existing studies [20]. In [17], Jian Lin et al. proposed the *BidGuard* scheme for privacy-preserving MC incentive mechanisms. This scheme is a general privacy-preserving scheme for incentivizing MC while achieving computational efficiency, individual rationality, truthfulness, differential privacy, and approximating the social cost minimization. It works with two score functions, i.e., linear and log functions, for selecting users. The authors prove that the *BidGuard* scheme with log score function is asymptotically optimal in terms of the social cost and can validate the desired properties [17].

The authors in [18] propose a new accuracy privacy trade-off MC (APMC) scheme for achieving high service accuracy while protecting privacy based on user preferences [18]. This scheme proposes a coalition strategy that allows users (i) to cooperate in providing their data under one identity, (ii) to increase their anonymity privacy protection, and (iii) to share the resulting payoff. In particular, users are incentivized to provide true data by being paid based on their individual contributions to the overall service accuracy. The *APMC* scheme provides answers to three questions; (i) how does the MC service define the contributions and payoff allocations of users with varying privacy levels? (ii) Do MC coalitions change the attained privacy of the cooperative users? (iii) How do cooperative users divide the coalition payoff among themselves? Through extensive simulation and real testbed results, authors show the performance of the APMC scheme [18].

The paper [19] proposes the privacy protection-oriented MC (PPMC) scheme to continually provide the high-quality data in the MC process. First, the PPMC scheme gives a formal definition of the sensing user's contribution based on the accuracy in data analysis. Based on the reputation incentive mechanism, the PPMC scheme considers the privacy protection of the sensing data and encourages more sensing users. In this scheme, new users and users who provide high-quality data can receive their reputation rewards, and reputation punishments for users who quit the sensing tasks. Therefore, the PPMC scheme can motivate more users to participate in sensing tasks and provides high-quality data over a long period of time. Finally, an efficient solution is given by the prisoner's dilemma between the service provider and the mediator [19].

Some earlier studies [17–20] have attracted considerable attention while introducing unique challenges in handling the MC control problems. In this paper, we demonstrate that our proposed scheme significantly outperforms these existing *BidGuard* [17], APMC [18], and PPMC [19] schemes.

3 The proposed integrated MC control scheme

In this section, we present the privacy preserving MC system architecture and develop a cooperative game model to calculate the payment for each mobile device. Our game approach is inherent in the proposed MC control scheme, and a desirable solution is achieved during the interactions among independent decision makers.

3.1 Cooperative game model for the MC system

In this study, we consider that MC infrastructure is a new dimension of privacy preserving platform, which is consisting of mobile user devices, access points, and MC server. There are multiple sensing task requests from the MC server. Each mobile device individually submits his contribution to the corresponding access point. From the data analytics perspective, the contribution of each device is defined based on the quality of the sensing data and its privacy-protecting level [18]. Between the MC server and MC participating devices, the access point works as a mediator to effectively decide the payment of MC participating devices. In this study, our major goal is to design a cooperative game model for the dynamic MC control scheme while balancing conflict interests among system entities. The main entities of our scheme are defined as follows:

Mobile user devices (MUDs): MUDs, i.e., mobile phones and IoT gadgets, are the MC participants which collect the sensing data, and report this information to the MC server. $\mathbb{M}$ is the set of MUDs where $MUD_{1 \le i \le m} \in \mathbb{M} = \{MUD_1 \dots MUD_m\}$. According to their own preferences, MUDs also select their levels of privacy protection. When a MUD chooses a higher level of privacy protection, his MC contribution is reduced. Naturally, individual MUD's payoff is proportional to his contribution. Therefore, each rational MUD needs to trade-off between the level of privacy protection and his payoff maximization.

Access point (AP): AC is a networking agent that allows MUDs to connect to a wired network. Usually, APs are situated around high MUD density hotspots to improve communication capacity. In our scheme, AP is also working as a payment management entity that controls the exchange of sensing data between multiple MUDs and the MC server. Based on the MUD's contribution, the AP decides each MUD's payment according to the Owen value algorithm.

MC server (MCS): MCS gets the sensing data and provides the reward through the AP. Finally, the MCS delivers a final service to MC customers by analyzing the sensing data.

Application tasks: $\mathbb{A} = \{ A_1 \ldots A_v \}$ is the set of MC sensing tasks.

In our game model, MUDs, APs, and MCS work together as game players, and act cooperatively with each other. The MCS generates multiple MC sensing tasks, and wants to obtain and analyze the sensing data to satisfy sensing tasks. Each AP offers the fair-efficient payment solution to MC participating MUDs in its coverage area. Under the dynamic MC environments, individual MUDs are enforced to contribute the MC process cooperatively while considering their DP features.

3.2 Differential privacy algorithm for MC

Privacy preservation is one of the greatest concerns in the MC system. In the last couple of years, it has been one of the most serious problems, which hampers the further growth of MC. In 2006, Cynthia Dwork first proposed a mathematically rigorous mechanism, called DP, which formally guarantees specific levels of privacy, even from powerful adversaries with side information. The concept of DP is the state-of-the-art privacy notion that assures a strong and provable privacy guarantee for the aggregated data. It requires a negligible change of computation results, when a single data subject had opted out of the data collection. Therefore, a common way of achieving DP is a perturbation of aggregated statistics by calibrated noise [21, 22].

As a protection mechanism, the DP adds random noises to public information in such a way it is not too sensitive to the response of any single participant; this assures an individual that any computation results will not unveil the presence (or absence) of its record. Specifically, it is a mathematical definition for the privacy loss that results to individuals when their private information is used in the creation of a data product [21, 22]. Recently, the DP has been extended to control systems where streams of data that evolve over time are collected in order to generate control signals that can drive states to desired values [21].

Definition 1: *A randomized algorithm* $\mathfrak{N}$ *has* ε-*differential privacy if for any two input sets* $\mathcal{A}$ *and* $\mathcal{B}$ *differing on a single entry, and for any set of outcomes* $\mathcal{R} \in Range(\mathcal{A})$ [23].

$$\mathbb{P}[\mathfrak{N}(\mathcal{A}) \in \mathcal{R}] \leq exp(\varepsilon) \times \mathbb{P}[\mathfrak{N}(\mathcal{B}) \in \mathcal{R}] \tag{1}$$

Informally, the DP means that the outcome of two nearly identical input datasets, i.e., different for a single component, should also be nearly identical. Therefore, individual information can hardly be inferred by comparing the query result of $\mathcal{A}$ and $\mathcal{B}$. The privacy ε is the parameter to measure the privacy level of the algorithm. The choice of ε is a tradeoff between the privacy and the accuracy of the output [23].

Generally, the DP is a probabilistic concept. Therefore, it is necessarily randomized to realize the DP. Recently, Laplace mechanism has been proposed by adding controlled noise to the DP function that we want to compute. Compared to the other mechanisms, the Laplace mechanism is fit to numeric data manipulation [21]. The Laplace mechanism involves adding random noise that conforms to the Laplace statistical distribution. The Laplace distribution (Lap(·)) can be expressed by probability density function given by;

$$\mathrm{Lap}(\mathcal{X}|\psi) = \frac{1}{2 \times \psi} \times \ exp\left(-\frac{|\mathcal{X}|}{\psi}\right) \tag{2}$$

where $\mathcal{X}$ is a support and ψ is a scale parameter, sometimes referred to as the diversity; the value of ψ depends on the privacy parameter ε. In the MC process, the risk to the most different individual of having their private information teased out of the data. This can be defined mathematically, and is known as the sensitivity ($\triangle\oint$) of the query function $\oint$;

$$\triangle\oint = \max_{\mathcal{A},\mathcal{B}} \left\| \oint(\mathcal{A}) - \oint(\mathcal{B}) \right\| \tag{3}$$

Let noise from the Laplace distribution denote the Laplace noise, which is obtained where $\psi = \triangle \oint / \varepsilon$ in the Laplace distribution. According to the new study of C. Dwork, there is a proof that the ε-DP is guaranteed to a sensing task by adding a random Laplace noise [24]. Thus, the balance of DP between privacy and accuracy has been extensively researched. In this study, we focus on the availability of MC services based on the DP idea. According to the game theory, the service availability of MUD is defined by using a quantity associated utility function, which can construct the relationship of DP and MC availability.

3.3 The Owen value of cooperative game

In the classical cooperative game theory, payment mechanism to coalitions of game players is one of main issues. Many solution concepts have been proposed to answer this problem, each kind of which satisfies a certain rational behavior and reasonable principle. Among the solutions that have been used in actual payment allocation problems, the value was introduced and axiomatized by L. Shapley. Since then, a number of alternative axiomatizations have been proposed. Recently, weighted values have been studied, and their computation complexities have been considered for specific problems. In 1977, G. Owen defined an efficient solution for cooperative games with coalition structure that also extends the traditional Shapley value, and it has been widely used in many practical applications [16, 25].

Based on the idea of the classical value solution, Owen value has many characterized axioms; *efficiency*, *symmetry*, *additivity*, *dummy*, *balanced contributions among players and coalitions*, *monotonicity among players and coalitions*, and *marginality among players and coalitions*. In addition, other interesting feature is to characterize the level structure value according to efficiency and the principle of balanced contributions. Therefore, the Owen value is formally captured using the notion of a consistency with a coalition structure [16, 25, 26].

To define the Owen value, we introduce some notations. Let ($\mathbb{N}$, $\mathcal{V}$) be a game with transferable utility, where $\mathbb{N}$= { a_1, a_2,..., a_n } is the set of players and $\mathcal{V}$ is the characteristic function, which assigns a real number $\mathcal{V}$ ($\mathcal{C}$) to every coalition $\mathcal{C}\subseteq\mathbb{N}$. A coalition structure for $\mathbb{N}$ is a partition $\mathbb{C}$= { $\mathcal{C}_1$,..., $\mathcal{C}_h$ }, i.e., $\mathcal{C}_{1\le k\le h}\cap\mathcal{C}_{1\le l\le h}=\varnothing$ if $k\neq l$ and $\cup_{k=1}^{h}\mathcal{C}_k=\mathbb{N}$. Let $\Omega(\mathbb{N})$ be the set of all permutations on $\mathbb{N}$. We say that $\pi\in\Omega(\mathbb{N})$ is admissible with respect to the coalition structure $\mathcal{C}$ if for any a_i, a_j, $a_k\in\mathbb{N}$, a_i, $a_k\in\mathcal{C}_l\in\mathbb{C}$, and $\pi(a_i)<\pi(a_j)<\pi(a_k)$ imply that $a_j\in\mathcal{C}_l$, where $\pi(a_i)$, $\pi(a_j)$, $\pi(a_k)$ denote the position of a_i, a_j, and a_k in the permutation π. We denote by $\Omega(\mathbb{N},\mathbb{C})$ the set of all admissible permutations on $\mathcal{N}$ with respect to $\mathbb{C}$. Given $\mathbb{N}$, $\mathbb{C}$, and $\mathcal{V}$ (·), the Owen value of a_i ($\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})$) is defined as follows [26];

$$\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=\left(\frac{1}{\|\Omega(\mathbb{N},\mathbb{C})\|}\right)\times\sum\nolimits_{\pi\in\Omega(\mathbb{N},\mathbb{C})}\left[\mathcal{V}\left(\mathfrak{P}_{a_i}^{\pi}\cup\{a_i\}\right)-\mathcal{V}\left(\mathfrak{P}_{a_i}^{\pi}\right)\right],\quad \text{for all } a_i\in\mathbb{N} \tag{4}$$

where $\mathfrak{P}_{a_i}^{\pi}=\{a_j\in\mathbb{N}|\pi(a_j)<\pi(a_i)\}$ and $\|\Omega(\mathbb{N},\mathbb{C})\|$ denotes the cardinality of the set $\Omega(\mathbb{N},\mathbb{C})$. If $\mathcal{C}=\{\{a_1\},\ldots,\{a_n\}\}$ or $\mathbb{C}=\{\mathbb{N}\}$ then the Owen value is given by [26].

$$\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=\sum_{\boldsymbol{S}\subseteq\mathbb{N}\setminus\{a_i\}}\left(\left(\frac{(|\boldsymbol{S}|-1)!(n-|\boldsymbol{S}|)!}{n!}\right)\times(\mathcal{V}(\boldsymbol{S}\cup\{a_i\})-\mathcal{V}(\boldsymbol{S}))\right) \tag{5}$$

which coincides with the Shapley value of the $\mathcal{V}$ (·) function. Owen et al. proved that there exists a unique mapping, the Owen value, from the space of all coalitional games to $\mathbb{R}^{N}$, that satisfies the below axioms [16, 26]. Let $\mathfrak{C}$ be the set of all cooperative games with coalition structure, and $\mathbb{C}|_{\boldsymbol{S}}$ is the restriction of $\mathbb{C}$ to the members of coalition $\boldsymbol{S}$, i.e., $\mathbb{C}|_{\boldsymbol{S}}=\{\mathcal{C}_l\cap\boldsymbol{S}|\mathcal{C}_l\in\mathbb{C}\text{ and }\mathcal{C}_l\cap\boldsymbol{S}\neq\phi\}$.

- *efficiency*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) $\in\mathfrak{C}$, $\sum_{a_i\in\mathcal{N}}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=\mathcal{V}(\mathbb{N})$.
- *symmetry*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) $\in\mathfrak{C}$ and for all symmetric coalitions $\mathcal{C}_k$, $\mathcal{C}_l\in\mathbb{C}$, then $\sum_{a_i\in\mathcal{C}_k}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=\sum_{a_i\in\mathcal{C}_l}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})$.
- *dummy*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) $\in\mathfrak{C}$ and for all $a_i\in\mathbb{N}$, $\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=0$ if a_i is a null player.
- *additivity*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) and ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}'$) $\in\mathfrak{C}$, and for all $a_i\in\mathbb{N}$, $\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V}+\mathcal{V}')=\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})+\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V}')$ where $(\mathcal{V}+\mathcal{V}')(\boldsymbol{S})=\mathcal{V}(\boldsymbol{S})+\mathcal{V}'(\boldsymbol{S})$ for any $\boldsymbol{S}\subset\mathbb{N}$.
- *Balanced contributions among coalitions*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) $\in\mathfrak{C}$ and $\mathcal{C}_k,\mathcal{C}_l\in\mathbb{C}$, $\sum_{a_i\in\mathcal{C}_k}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})-\sum_{a_i\in\mathcal{C}_k}\mathcal{X}_{a_i}(\mathbb{N}\setminus\mathcal{C}_l,\mathbb{C}|_{\mathbb{N}\setminus\mathcal{C}_l},\mathcal{V}|_{\mathbb{N}\setminus\mathcal{C}_l})=\sum_{a_i\in\mathcal{C}_l}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})-\sum_{a_i\in\mathcal{C}_l}\mathcal{X}_{a_i}(\mathbb{N}\setminus\mathcal{C}_k,\mathbb{C}|_{\mathbb{N}\setminus\mathcal{C}_k},\mathcal{V}|_{\mathbb{N}\setminus\mathcal{C}_k})$.
- *Balanced contributions among players*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) $\in\mathfrak{C}$ and $\mathcal{C}_k,\mathcal{C}_l\in\mathbb{C}$, $\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})-\chi_{a_i}(\mathbb{N}\setminus a_j,\mathbb{C}_{-a_j},\mathcal{V}_{-a_j})=\chi_{a_j}(\mathbb{N},\mathbb{C},\mathcal{V})-\chi_{a_j}(\mathbb{N}\setminus a_i,\mathbb{C}_{-a_i},\mathcal{V}_{-a_i})$.
- *monotonicity among coalitions*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) and ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}'$) $\in\mathfrak{C}$, $\sum_{a_i\in\mathcal{C}_k}\mathcal{X}_{a_i}(\mathbb{N},\mathcal{C},\mathcal{V})\ge\sum_{a_i\in\mathcal{C}_l}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V}')$ if $\mathcal{V}(\boldsymbol{S}\cup\mathcal{C}_k)-\mathcal{V}(\boldsymbol{S})\ge\mathcal{V}'(\boldsymbol{S}\cup\mathcal{C}_k)-\mathcal{V}'(\boldsymbol{S})$ for all $\boldsymbol{S}\subseteq\mathcal{N}\setminus\mathcal{C}_k$.
- *monotonicity among players*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) and ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}'$) $\in\mathfrak{C}$, $\chi_{a_i}(\mathcal{N},\mathbb{C},\mathcal{V})\ge\chi_{a_i}(\mathbb{N},\mathcal{C},\mathcal{V}')$ if $\mathcal{V}(\boldsymbol{S}\cup\{a_i\})-\mathcal{V}(\boldsymbol{S})\ge\mathcal{V}'(\boldsymbol{S}\cup\{a_i\})-\mathcal{V}'(\boldsymbol{S})$ for all $\boldsymbol{S}\subseteq\mathbb{N}\setminus\{a_i\}$.
- *marginality among coalitions*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) and ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}'$) $\in\mathfrak{C}$, $\sum_{a_i\in\mathcal{C}_k}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=\sum_{a_i\in\mathcal{C}_l}\mathcal{X}_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V}')$ if $\mathcal{V}(\boldsymbol{S}\cup\mathcal{C}_k)-\mathcal{V}(\boldsymbol{S})=\mathcal{V}'(\boldsymbol{S}\cup\mathcal{C}_k)-\mathcal{V}'(\boldsymbol{S})$ for all $\boldsymbol{S}\subseteq\mathbb{N}\setminus\mathcal{C}_k$.
- *marginality among players*: for all ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}$) and ($\mathbb{N}$, $\mathbb{C}$, $\mathcal{V}'$) $\in\mathfrak{C}$, $\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V})=\chi_{a_i}(\mathbb{N},\mathbb{C},\mathcal{V}')$ if $\mathcal{V}(\boldsymbol{S}\cup\{a_i\})-\mathcal{V}(\boldsymbol{S})=\mathcal{V}'(\boldsymbol{S}\cup\{a_i\})-\mathcal{V}'(\boldsymbol{S})$ for all $\boldsymbol{S}\subseteq\mathbb{N}\setminus\{a_i\}$.

Based on the above properties, the Owen value can be obtained by considering the following a heuristic development in two steps of bargaining: the first one among the coalitions and the second one into each coalition [27].

Simply, we present the computation example for the Owen value. Prerequisite is that the members of the coalition improve their payoff by forming a union; if we assume that $\mathbb{N} = \{a_1, a_2, a_3\}, \mathcal{V} \quad (\{a_1\}) = 20, \mathcal{V}(\{a_2\}) = 30, \mathcal{V}(\{a_3\}) = 40, \mathcal{V}(\{a_1, a_2\}) = 90, \mathcal{V}(\{a_1, a_3\}) = 80, \mathcal{V} \ (\{a_2, a_3\}) = 70$ and $\mathcal{V}(\{a_1 \ , a_2, a_3\}) = 120$, then the Table 1 shows an example of the computation of the Owen value.

3.4 Main steps of our integrated MC control scheme

Similar to the most MC systems, our MCS sequentially generates sensing tasks, and assigns each task to a specific AP, which is distributed regionally. MUDs, who are interested in performing sensing tasks, are associated with their DP value (ε). Within the AP's covering area, each MUD performs a sensing task $(A \in \mathbb{A})$ and reports his actual sensing contribution $\mathfrak{A}_{MUD}^{A}$ to the corresponding AP. For the task A_ν in $\mathbb{A}$, a set $\mathcal{N}_{A_\nu}$, i.e., $\mathcal{N}_{A_\nu} \subseteq \mathbb{M}$, is created by the MUDs, who are actively participating the MC service to complete the task A_ν. In the $\mathcal{N}_{A_\nu}$, multiple coalitions are formed according to MUDs' ε values. Therefore, a coalition $(\mathcal{C})$ in the $\mathcal{N}_{A_\nu}$ has represented a subset of MUDs, who have the same ε value. Usually, the different coalitions are intended to work independently of each other based on their privacy preserving levels. Finally, the AP calculates the payment $\mathcal{P}_{MUD}^{A_\nu}$ for each MC participating MUD. Based on the MUD's actual contribution, $\mathcal{P}_{MUD}^{A_\nu}$ is estimated using the Owen value. In this study, the characteristic function $\mathcal{V}$ for the coalition $\mathcal{C}_l$ $(\mathcal{V}(\mathcal{C}_l))$ is defined based on the bankruptcy game model in [28].

$$\mathcal{V}(\mathcal{C}_l) = \ \mathbf{max}\left(0, \mathrm{M}_{\mathcal{T}^{A_\nu}} - \sum_{a_i \notin \mathcal{C}_l} \mathfrak{A}_{MUD_i}\right)$$
$$\text{s.t.,} \begin{cases} \mathrm{M}_{\mathcal{T}^{A_\nu}} = \psi_{A_\nu} \times \displaystyle\sum_{MUD_k \in \mathcal{N}_{A_\nu} \subset \mathbb{M}} \mathfrak{A}_{MUD_k}^{A_\nu} \\ \mathfrak{A}_{MUD_i}^{A_\nu} = \left(\left(1 + \ \log\left(\dfrac{\left(e^{\varepsilon_{MUD_i}} + 1\right)^2}{e^{\varepsilon_{MUD_i}}}\right)\right) \times \left(\partial_{MUD_i}^{A_\nu} \times \dfrac{\partial_{MUD_i}^{A_\nu}}{\mathcal{T}^{A_\nu}}\right)\right) \end{cases} \tag{6}$$

where ψ_{A_ν} is the control factor for the A_ν and ε_{MUD_i} is the MUD_i's DP value (ε). $\partial_{MUD_i}^{A_\nu}$ and $\mathcal{T}^{A_\nu}$ are the MUD_i's MC sensing outcome and the total MC requirement to complete the A_ν, respectively. $\mathfrak{A}_{MUD_i}^{A_\nu}$ indicates the MUD_i's actual MC contribution; it depends on the MUD_i's DP value $(e^{\varepsilon_{MUD_i}})$, $\partial_{MUD_i}^{A_\nu}$ and $\mathcal{T}^{A_\nu}$. Based on the $\mathcal{V}(\mathbb{C}^{A_\nu})$ where $\mathbb{C}^{A_\nu}$ is the set of all coalitions in the $\mathcal{N}_{A_\nu}$, we can calculate the Owen value $\boldsymbol{\chi}$=[$\chi_{MUD_1}(\mathcal{N}_{A_\nu}, \mathbb{C}^{A_\nu}, \mathcal{V})\ldots \chi_{MUD_i}(\mathcal{N}_{A_\nu}, \mathbb{C}^{A_\nu}, \mathcal{V})\ldots\chi_{MUD_n}(\mathcal{N}_{A_\nu}, \mathbb{C}^{A_\nu}, \mathcal{V})$] according to (4) where n is the cardinality of $\mathcal{N}_{A_\nu}$. In the proposed scheme, the $\mathcal{P}_{MUD_i}^{A_\nu}$ is $\chi_{MUD_i}(\mathcal{N}_{A_\nu}, \mathbb{C}^{A_\nu}, \mathcal{V})$ in $\boldsymbol{\chi}$, and the AP can distribute payments to MUDs in $\mathcal{N}_{A_\nu}$ based on the Owen value $\boldsymbol{\chi}$.

For privacy-reserving applications, our prime focus is to combine the DP and payment algorithms comprehensively to get a full synergy of dynamic MC system operations. Inspired by the Owen value, the proposed MC control scheme plays a crucial role to tradeoff privacy and MC accuracy while satisfying the different goals of MUDs and MCS. Based on the cooperative game model, MUDs, AP, and MCS can capture the current MC system condition and determine their best strategies to maximize their payoffs. Through a step-by-step distributed cooperative game process, they can benefit from joining in the MC process, and a win-win situation can be achieved; it is a promising approach to implement the real-world MC services. The main steps of the proposed MC control scheme are described as follows.

Step 1: At the initial time, application features and system parameters are determined by the simulation scenario and Table 2.
Step 2: Each MUD has its own privacy preserving level (ε); it is fixed for each sensing task application.
Step 3: The MCS generates MC sensing tasks, sequentially. These task applications are operated through local APs. Each AP works as a mediator

Table 1 Example of the computation of the Owen value

Set of coalitions	$\mathbb{C} = \{\mathcal{C}_1 = \{a_1, a_2\}, \mathcal{C}_2 = \{a_3\}\}$		
Permutation	a_1	a_2	a_3
$a_1 \leftarrow a_2 \leftarrow a_3$	$\mathcal{V}(\{a_1\})$ - $\mathcal{V}(\varphi)$ =20	$\mathcal{V}(\{a_1, a_2\})$ - $\mathcal{V}(\{a_1\})$ = 70	$\mathcal{V}(\{a_1, a_2, a_3\})$ - $\mathcal{V}(\{a_1, a_2\})$ = 30
$a_1 \leftarrow a_3 \leftarrow a_2$	N/A; $\pi(a_1) < \pi(a_3) < \pi(a_2)$ and $a_1, a_2 \in \mathcal{C}_1$ but $a_3 \notin \mathcal{C}_1$		
$a_2 \leftarrow a_1 \leftarrow a_3$	$\mathcal{V}(\{a_1, a_2\})$- $\mathcal{V}(\{a_2\})$ =60	$\mathcal{V}(\{a_2\})$- $\mathcal{V}(\varphi)$ =30	$\mathcal{V}(\{a_1, a_2, a_3\})$- $\mathcal{V}(\{a_1, a_2\})$ =30
$a_2 \leftarrow a_3 \leftarrow a_1$	N/A; $\pi(a_2) < \pi(a_3) < \pi(a_1)$ and $a_2, a_1 \in \mathcal{C}_1$ but $a_3 \notin \mathcal{C}_1$		
$a_3 \leftarrow a_1 \leftarrow a_2$	$\mathcal{V}(\{a_1, a_3\})$- $\mathcal{V}(\{a_3\})$ =40	$\mathcal{V}(\{a_1, a_2, a_3\})$- $\mathcal{V}(\{a_1, a_3\})$ =40	$\mathcal{V}(\{a_3\})$- $\mathcal{V}(\varphi)$ =40
$a_3 \leftarrow a_2 \leftarrow a_1$	$\mathcal{V}(\{a_1, a_2, a_3\})$- $\mathcal{V}(\{a_2, a_3\})$ =50	$\mathcal{V}(\{a_2, a_3\})$- $\mathcal{V}(\{a_3\})$ =30	$\mathcal{V}(\{a_3\})$- $\mathcal{V}(\varphi)$ =40
Total	$20 + 60 + 40 + 50 = 170$	$70 + 30 + 40 + 30 = 170$	$30 + 30 + 40 + 40 = 140$
Owen value $\chi_a(\mathbb{N}, \mathcal{C}_1, \mathcal{V})$	$170/4 = 42.5$	$170/4 = 42.5$	$140/4 = 35$

Table 2 System parameters used in the simulation experiments

Sensing tasks	ψ	MC cycles per MUD	Total MC cycles ($\mathcal{T}^{A_v}$)	Service duration
$A_v = \tau_1$	0.95	180 cycles/s	750 cycles/s	2400 s (40 min)
$A_v = \tau_2$	0.9	200 cycles/s	1000 cycles/s	2700 s (45 min)
$A_v = \tau_3$	0.85	220 cycles/s	1250 cycles/s	2880 s (48 min)
$A_v = \tau_4$	0.8	250 cycles/s	1500 cycles/s	3000 s (50 min)
Parameter	Value	Description		
m	100	The number of physical mobile devices		
$\|AP\|$	10	The number of access points		

between the MCS and MUDs while calculating their payments.

Step 4: The task A_v is assigned to a specific AP, and MUDs around that AP create the set $\mathcal{N}_{A_v}$ while actively participating the MC service. At this time, MUDs in $\mathcal{N}_{A_v}$ form multiple coalitions according to their privacy preserving level (ε).

Step 5: Using (2) and (3), each MUD generates the Laplace noise, and adds it to the actual MC outcome while satisfying the Eq. (1); it guarantees the MUD's DP.

Step 6: In a distributed manner, the AP monitors only MUDs in its own coverage area, and estimates each MUD's actual MC contribution ($\mathfrak{A}$) according to (6).

Step 7: Based on the Eq. (4), the AP calculates the Owen value for each individual MUD; $\mathbb{C}$ for each task is localized at each AP. Therefore, the computation overhead can be practically reduced.

Step 8: Based on the step-by-step distributed cooperative game process, the AP, MCS, and MUDs interact with one another, and cause a cascade of interactions.

Step 9: Under the dynamic MC system environment, the MCS is constantly generates MC tasks; proceeds to step 2 for the next cooperative game iteration.

4 Performance evaluation

In this section, we evaluate the performance of our proposed protocol, and compare it with that of the existing *BidGuard* [17], APMC [18], and PPMC [19] schemes. Based on the simulation results, we confirm the superiority of the proposed approach.

4.1 Experimental method

In this study, we have used the simulation tool MATLAB to develop our simulation model. MATLAB is one of the most widely used tools in a number of scientific simulation fields; its high-level syntax and dynamic types are ideal for model prototyping. To ensure a fair comparison, the following simulation assumptions and MC system scenario are used.

- 100 MUDs are used in which these devices are distributed randomly.
- 10 APs are located evenly in a geographical region.
- Each MUD's ε value for its PD is randomly decided among {0.85, 0.9, 0.95}. According to the DP mechanism, the proposed approach cannot achieve a complete privacy protection, but provide a partially protected privacy based on the ε value.
- Simply, we consider four cases of MUD capacity to proceed the MC service; 100 cycles/s, 150 cycles/s, 200 cycles/s, and 250 cycles/s. MC capacity of each individual MUD is randomly selected from the above four cases.
- There are four different sensing task applications, i.e., $\{\tau_1, \tau_2, \tau_3, \tau_4\}$, which are specified according to the sensing requirements. They are generated with equal probability.
- Sensing tasks $\mathbb{A}$ are generated based on the Poisson process, which is with rate λ (tasks/s), and the range is varied from 0 to 3.
- All application tasks need a specific local region information. This region is randomly selected, and the MC task is assigned to the corresponding AP.
- System performance measures obtained on basis of 100 simulation runs are plotted as functions of the sensing task generation rate.
- For simplicity, we assume the absence of physical obstacles in the experiments.

To demonstrate the validity of our proposed method, we measured the task success ratio, MC participating ratio, and MUD's payoff fairness. Table 2 shows the system parameters used in the simulation. Major system control parameters of the simulation, presented in Table 2, facilitate the development and implementation of our simulator.

4.2 Result analysis

Figure 1 gives the performance comparison of each scheme in terms of the task success ratio. In this simulation study, the task success ratio is defined as the ratio of the total number of sensing tasks applications which have been generated by the MCS to the number of task applications which are successfully completed. Compared with other existing schemes, MUDs and MCS in our scheme can reach jointly a mutually acceptable agreement to complete the request tasks; it leads a higher task success ratio. From low to high task request distributions, it is easy to see that the scheme which is designed in this paper has the best performance.

Figure 2 presents the MC participating ratio for each scheme. In the simulation result, we can see that all schemes exhibit a similar trend. However, we can align the goals of selfish individual MUDs while revealing their private information as well as to take appropriate actions. This stimulates MUDs to actively participate the MC process. For this reason, the proposed scheme can attain the better MC participating ratio to other schemes. The curves in Fig. 3 indicate the MUD's payoff fairness. From the viewpoint of social welfare, it is a main concern and important performance criterion. Therefore, during the MC operations, the most proper combination of the efficiency and fairness is the major issue. In this paper, the concept of fairness is defined as an equitable payoff rate for the MC participating MUDs. To characterize this fairness notion, we follow the Jain's fairness index (F_{index}) [29], which has been frequently used to measure the fairness of network management.

$$F_{index} = \frac{\left(\sum_{MUD_k \in \mathcal{N}_{A_v} \subset \mathbb{M}} \left(\chi_{MUD_k}\left(\mathcal{N}_{A_v}, \mathbb{C}^{A_v}, \mathcal{V}\right) \Big/ \mathfrak{A}_{MUD_k} \right)\right)^2}{\left(\|\mathcal{N}_{A_v}\| \times \sum_{MUD_k \in \mathcal{N}_{A_v} \subset \mathbb{M}} \left(\chi_{MUD_k}\left(\mathcal{N}_{A_v}, \mathbb{C}^{A_v}, \mathcal{V}\right) \Big/ \mathfrak{A}_{MUD_k} \right)^2 \right)} \tag{7}$$

where $\|\mathcal{N}_{A_v}\|$ is the cardinality of the set $\mathcal{N}_{A_v}$. From the Fig. 3, we can see that the proposed scheme achieves a higher and stable fairness during different task request intensities. In our scheme, the AP distributes payments according to the Owen value; it correlates with the fairness provisioning.

In summary, simulation results shown in Figs. 1, 2, and 3 demonstrate that the proposed scheme can monitor the current MC system conditions and leverages the DP and payment algorithms to get the full synergy of MC processing operations. Through cooperative game theoretic operations and functionality, MUDs, AP, and MCS are mutually dependent, and coordinate with each other in order to get the best solution for all. To provide a suitable tradeoff between conflicting requirements, it is a suitable approach. In conclusion, simulation results show that our scheme attains an attractive MC system performance, something that the *BidGuard* [17], APMC [18], and PPMC

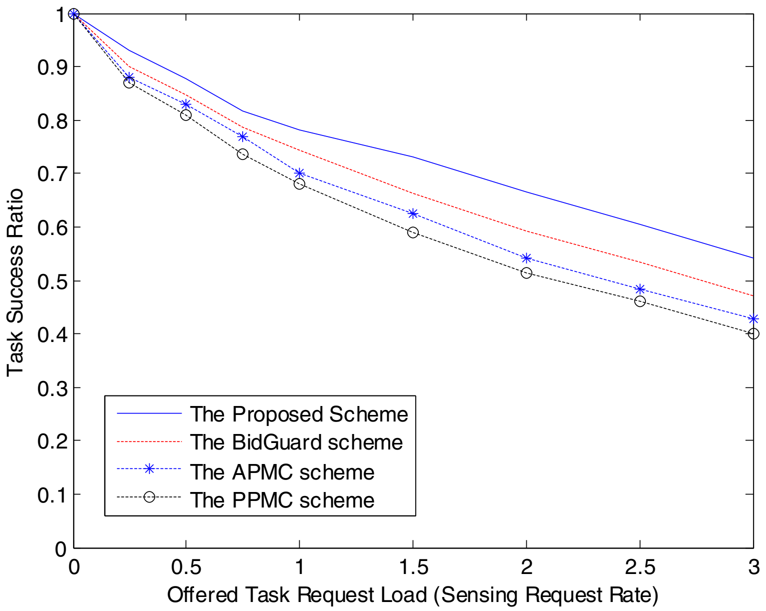

Fig. 1 MC task success ratio. The task success ratio is defined as the ratio of the total number of sensing tasks applications which have been generated by the MCS to the number of task applications which are successfully completed

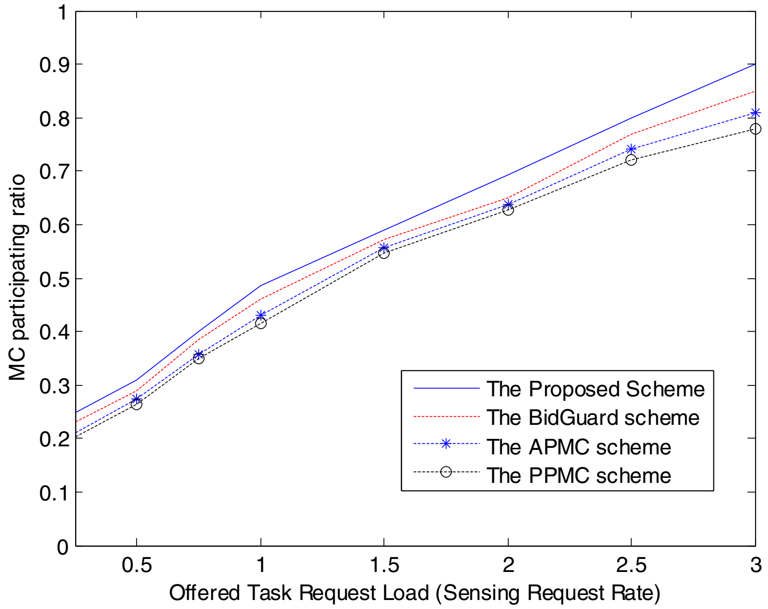

Fig. 2 MC participating ratio. For each scheme, the MC participating ratio is estimated from low to high task request distributions

[19] schemes cannot offer. In addition, it is also interesting to see that we consistently maintain the operational excellence from low to high task request intensities.

5 Results and discussions

Recently, the MC is growing in popularity as an emerging paradigm that requires an implicit collaboration of mobile devices, which sense data with the aim of performing a specific application. However, sensing data may be privacy-sensitive. Therefore, the state-of-the-art scheme, which can encourage devices to participate MC while ensuring privacy protection, is necessary. In this article, we have proposed an integrated MC control scheme by effectively combining the payment algorithm and DP algorithm. In particular, we formulate the privacy protective MC control scheme as a cooperative game process that models the relations among MC agents to successfully complete application tasks. Using

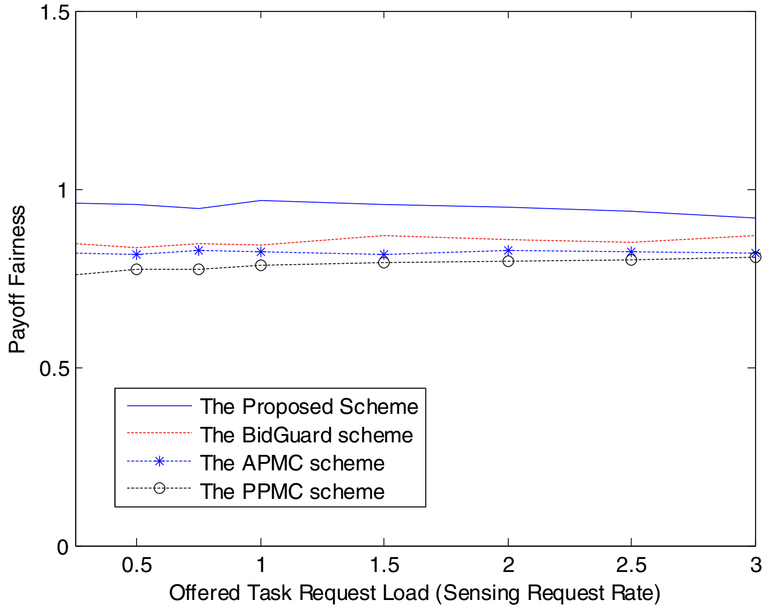

Fig. 3 MUD payoff fairness. To characterize this fairness notion, the Jain's fairness index is adopted; it has been frequently used to measure the fairness of network management

the step-by-step distributed game process, we explore effective answers to the fundamental questions of how to design a payment algorithm, and how to provide a differential privacy while considering the impact of payoff. Under the situation characterized by the MC system, our method is a practical and suitable approach. Compared to the existing protocols, simulation results are presented to show the superiority of our proposed scheme. For the future research, there are a series of possible ways to extend the results in this study. New research issues will focus on the in-depth study of challenges and techniques, solutions for the MC systems while providing case studies. Furthermore, more heterogeneous devices will be tested, in order to assess the proposed approach in different conditions. In the current research, machine learning issue still lacks exploration. Therefore, another interesting direction is to address the learning and AI issues in the MC system from the operator's perspective.

Abbreviations

AP: Access point; APMC: Accuracy privacy trade-off MC; DP: Differential privacy; IoE: Internet of everything; MC: Mobile crowdsensing; MCS: MC server; MUDs: Mobile user devices; PPMC: Privacy protection-oriented MC

Acknowledgements

This research was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00498, A Development of Deidentification Technique based on Differential privacy) and by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2018-0-01799) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation).

Author's contributions

The sole author, SK, contributes all this research work. The author read and approved the final manuscript.

Author's information

Sungwook Kim received the BS, MS degrees in computer science from the Sogang University, Seoul, in 1993 and 1995, respectively. In 2003, he received the PhD degree in computer science from the Syracuse University, Syracuse, New York, supervised by Prof. Pramod K. Varshney in 2003. He is currently a Professor of Department of Computer Science & Engineering, and is a research director of the Network Research Laboratory. His current research interests are in game theory and network design applications.

Funding

MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center).

Availability of data and materials

Please contact the corresponding author at swkim01@sogang.ac.kr.

Competing interests

The author declares that he has no competing interests.

Received: 27 December 2017 Accepted: 29 May 2019
Published online: 14 June 2019

References

1. Z. Duan, L. Tian, M. Yan, Z. Cai, Q. Han, G. Yin, Practical incentive mechanisms for IoT-based mobile crowdsensing systems. IEEE Access **5**, 20383–20392 (2017)
2. C. Fiandrino, B. Kantarci, F. Anjomshoa, D. Kliazovich, P. Bouvry, J. Matthews, in *IEEE GLOBECOM'2016*. Sociability-driven user recruitment in mobile crowdsensing internet of things platforms (2016), pp. 1–6
3. K.S. Kim, S. Uno, M.W. Kim, Adaptive QoS mechanism for wireless mobile network. JCSE **4**(2), 153–172 (2010)
4. I. Jang, D. Pyeon, S. Kim, H. Yoon, A survey on communication protocols for wireless sensor networks. JCSE **7**(4), 231–241 (2013)
5. L. Atzori, R. Girau, S. Martis, V. Pilloni, M. Uras, in *IEEE ICIN'2017*. A SIoT-aware approach to the resource management issue in mobile crowdsensing (2017), pp. 232–237
6. M. Pouryazdan, C. Fiandrino, B. Kantarci, D. Kliazovich, T. Soyata, P. Bouvry, in *IEEE GLOBECOM'2016*. Game-theoretic recruitment of sensing service providers for trustworthy cloud-centric internet-of-things (IoT) applications (2016), pp. 1–6
7. J. Liu, H. Shen, X. Zhang, in *IEEE ICCCN'2016*. A survey of mobile crowdsensing techniques: A critical component for the internet of things (2016), pp. 1–6
8. Y. Liu, Y. Sun, J. Ryoo, S. Rizvi, A.V. Vasilakos, A survey of security and privacy challenges in cloud computing: solutions and future directions. JCSE **9**(3), 119–133 (2015)
9. T. Kang, X. Li, C. Yu, J. Kim, A survey of security mechanisms with direct sequence spread spectrum signals. JCSE **7**(3), 187–197 (2013)
10. A. Gkoulalas-Divanis, K. Liu, V.S. Verykios, R. Wolff, Preface for the special issue on privacy-aspects of data mining. JCSE **5**(3), 167–168 (2011)
11. L. Wang, D. Zhang, D. Yang, B.Y. Lim, X. Ma, in *IEEE ICDM'2016*. Differential location privacy for sparse mobile crowdsensing (2016), pp. 1257–1262
12. S. Blasco, J. Bustos-Jimenez, G. Font, A. Hevia, M. Grazia Prato, in *IEEE SCCC'2015*. A three-layer approach for protecting smart-citizens privacy in crowdsensing projects (2015), pp. 1–5
13. J. Hamm, A.C. Champion, G. Chen, M. Belkin, D. Xuan, in *IEEE ICDCS'2015*. Crowd-ML: a privacy-preserving learning framework for a crowd of smart devices (2015), pp. 11–20
14. H.H. Nguyen, J. Kim, Y. Kim, Differential privacy in practice. JCSE **7**(3), 177–186 (2013)
15. S. Kim, *Game theory applications in network design* (IGI Global, Hershey, 2014)
16. S. Lorenzo-Freire, On new characterizations of the Owen value. Oper. Res. Lett. **44**(4), 491–494 (2016)
17. J. Lin, D. Yang, M. Li, J. Xu, G. Xue, in *IEEE CNS'2016*. BidGuard: a framework for privacy-preserving crowdsensing incentive mechanisms (2016), pp. 145–153
18. M.A. Alsheikh, Y. Jiao, D. Niyato, P. Wang, D. Leong, Z. Han, The accuracy-privacy trade-off of mobile crowdsensing. IEEE Commun. Mag. **55**(6), 132–139 (2017)
19. R. Ma, J. Xiong, M. Lin, Z. Yao, H. Lin, A. Ye, in *IEEE Trustcom/BigDataSE/ICESS'2017*. Privacy protection-oriented mobile crowdsensing analysis based on game theory (2017), pp. 990–995
20. Y. Sei, A. Ohsuga, Differential private data collection and analysis based on randomized multiple dummies for untrusted mobile crowdsensing. IEEE Trans. Inf. Forensics Secur. **12**(4), 926–939 (2017)
21. H. Liu, Z. Wu, L. Zhang, in *IEEE NaNA'2016*. A differential privacy incentive compatible mechanism and equilibrium analysis (2016), pp. 260–266
22. J. Giraldo, A. Cardenas, M. Kantarcioglu, in *IEEE CCTA'2017*. Security and privacy trade-offs in CPS by leveraging inherent differential privacy (2017), pp. 1313–1318
23. P. Zhou, Y. Zhou, D. Wu, H. Jin, Differentially private online learning for cloud-based video recommendation with multimedia big data in social networks. IEEE Trans. Multimedia **18**(6), 1217–1229 (2016)
24. C. Dwork, A firm foundation for private data analysis. Commun. ACM **54**(1), 86–95 (2011)
25. C.-G. E, Q.-L. Li, S.-Y. Li, The Owen value of stochastic cooperative game. Sci. World J. **2014**, 1–7 (2014)
26. J. Vidal-Puga, G. Bergantiños, An implementation of the Owen value. Games Econom. Behav. **44**, 412–427 (2003)
27. M.G. Fiestras-Janeiro, J.M. Gallardo, A. Jiménez-Losada, M.A. Mosquera, Cooperative games and coalition cohesion indices: the Choquet–Owen value. IEEE Trans. Fuzzy Syst. **24**(2), 444–455 (2016)
28. D. Niyato, E. Hossain, in *IEEE International Conference on Communications*. A cooperative game framework for bandwidth allocation in 4G heterogeneous wireless networks (2006), pp. 4357–4362
29. M. Dianati, X. Shen, S. Naik, A new fairness index for radio resource allocation in wireless networks. IEEE WCNC **2**, 712–715 (2005)

6 Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.