IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 25, 2019, accepted September 4, 2019, date of publication September 9, 2019,
date of current version September 20, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2940096

A Differential Game Model for Data Utility and Privacy-Preserving in Mobile Crowdsensing

HONGJIE GAO[1], HAITAO XU[1], LONG ZHANG[2], AND XIANWEI ZHOU[1]
[1]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
[2]School of Information and Electrical Engineering, Hebei University of Engineering, Handan 056038, China

Corresponding author: Haitao Xu (alex_xuht@hotmail.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61971032, in part by the Fundamental Research Funds for the Central Universities under Grant FRF-TP-18-008A3, in part by the Natural Science Foundation of Hebei Province under Grant F2019402206, and in part by the Research Program for Top-Notch Young Talents in Higher Education Institutions of Hebei Province, China, under Grant BJ2017037.

ABSTRACT Mobile crowdsensing (MCS) is becoming an extremely pervasive sensing paradigm with the popularization of intelligent devices, which needs users to release their data to the sensing platform. But to the MCS system, user's privacy-preserving demands may be time-varying in the data releasing process. In addition, protecting data privacy and ensuring data utility is becoming a contradictory and critical issue, which results in a trade-off problem that needs to be solved. In this article, we construct a differential game model to solve the trade-off problem between the data utility and privacy preserving in mobile crowdsensing system, and solve the feedback Nash equilibrium solutions based on the dynamic programming in the MCS system. Based on the feedback Nash equilibrium solutions, users and the platform can achieve maximization of privacy requirement and data utility, respectively. Ultimately, a numerical simulation has been made to show the correctness of the proposed differential game model.

INDEX TERMS Mobile crowdsensing, data utility, time-varying, privacy-preserving, differential game.

I. INTRODUCTION

Mobile crowdsensing (MCS) is becoming a very popular paradigm, which uses the tremendous sensing capability of various sensors (e.g., camera, tape-recorder, video camera, GPS) to complete various sensing tasks (e.g., personal health monitoring, pricing auditing, monitoring noise and ambiance, real-time traffic conditions) [1] in a cost-effective approach. In a typical MCS application scenario, the sensing servers or sensing platforms publish different perceptual tasks to users, who have intelligent equipments to collect and release perceptual data. Then the sensing platforms aggregate, process, analyze and share the data to service requesters for different purposes [2]. In this process, some incentive mechanisms are needed for the sensing platforms to recruit users' participation. On the one hand, the sensing data released to task platform may contain personal sensitive information like user's location data and accelerometer data. In addition, with the location data, attackers can derive user's private information (e.g., habits and customs, health condition, social relation) by linking attack [3], hence, the behavior that carried out by attackers may violate users' privacy [4]. On the other hand, in order to complete perceptual tasks motivated by the sensing platforms, users may have some additional consumptions, such as battery, storage, and so on [5]. Meanwhile, the privacy requirements may be varied over time to users even for the same tasks [6]. In order to introduce the dynamic requirement about users more clearly, we take a simple example as follows.

Example 1: For some medical research purposes, the sensing platform needs to collect medical data (e.g., blood pressure, heart rate et al.) abundantly from users for a period. Some users may want to disclose more information when they are ill to get a better monitor. Meanwhile, they can get some rewards from the sensing platforms by sharing their health data. In the above process, the privacy-preserving requirements of users are lower than the other cases. Once the users get cured, they will decrease the amount of the shared data information despite the reward, because they want to have a higher privacy-preserving requirement for the uploaded data.

In the MCS system, we assume that the sensing platform is not a trustworthy third party [7], in which scenes the recruited users are permitted to perturb their raw data locally by

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

adding some different grades noise before releasing the data to the platform according to the dynamic changing privacy demands, in order to protect their sensitive information [8]. Noise addition behavior will result in a decline in data utility (the ratio of available data to total data) to both the user portion and platform portion respectively. For the users, they want to add enough noise to maximize their data privacy, which will reduce the data utility. The sensing platform wants to maximize the data utility to have a better realization of data value but will reduce the data privacy. Hence, the trade-off problem between data privacy and data utility [9] arises that needs to be solved dynamically.

In order to solve the trade-off problem, we design a non-cooperative differential game model [10], [11] to find if there exist an optimal strategies for the players, that is, to find Nash Equilibrium solutions for the trade-off problem to users and platform over time, no matter what noise addition mechanism has been used for data perturbation and what data aggregation mechanism has been adopted for data value to be implemented. Generally, game theory can be used to settle the trade-off matters. For instance, Wu *et al.* [9] cast the trade-off problem between privacy and utility as a game problem in a static scenario, where the privacy level of data set is fixed. Different from the above scheme, we formulate a non-cooperative differential game model to solve the trade-off problem between privacy and utility in MCS based on a dynamic privacy requirement condition. The main contributions of the paper are as follows.

1) We design a non-cooperative differential game-based model for the trade-off problem of data privacy and data utility.

2) By attaining the Nash equilibrium solutions, we get the verdict that the optimum condition was existent, which gives a certain reference for users to set their privacy requirements so as to maximize the remuneration, and for platform to achieve a better value of the data.

The following section is devised as follows: Sect.2 is the related works. Sect.3 is the preliminaries for the paper. Sect.4 is the system model and game formulation of the proposed problem. The feedback Nash Equilibrium solution of the proposed game model are given in sect.5. Sect.6 is numerical simulations and analysis, and there is conclusion and future work in sect.7.

II. RELATED WORK

Lots of the work has been done to the privacy-preserving issues in the domain of mobile crowdsensing [6], [12]–[18]. In MCS, to protect sensitive information, users may submit perturbation data or unreliable data to the platform, the identification about privacy-preserving truthful values from all the sensing data while protecting individual private data problem are emerged. To solve the issue, Miao *et al.* [12] proposes a cloud-based privacy-preserving truth discovery framework, which not only protects user's sensitive information, but also derives the reliable score of the sensing data that is provided by individual, but the true discovery framework ignore the sensing data may have a vary reliability degree due to different topics.

Ma *et al.* [13] formulates a fine grained truth discovery model named FaitCrowd by using a probabilistic model to estimate topical expertise and true answers concurrently.

Su *et al.* [14] presents a decision aggregation framework GDA, which can take advantage of all the messages, and has no assumption about the availability level of ground truth label information.

Xiao *et al.* [15] proposes a stackelberg game between intelligent devices owner and MCS server, firstly, the server determines and broadcasts its payment policy for each sensing accuracy. And then each user chooses the sensing effort and the sensing accuracy to receive the payment.

In addition, in one place, there may exist multiple sensing works, which makes the privacy of the sensing users' harder to be guaranteed. Meanwhile, the introduction of incentive mechanisms (auction mechanisms, monetary mechanisms, game mechanisms) [16], [17] in MCS privacy issues makes it more challenging to be satisfied. To solve it, Zhang *et al.* [18] proposes two privacy-preserving market mechanisms to protect the privacy.

We see that all the above literatures assume that user's privacy protection requirements are fixed by time. Zhang *et al.* [6] solves the dynamic pricing problem in MCS system by using a reinforcement learning approach shows that the requirements may be time-varying. Based on the above, we can see the issue that improving the data utility while protecting data private as a trade-off problem. In order to solve the trade-off problem, we need to consider the dynamic variation in the MCS system, which can be built as a differential game.

III. PRELIMINARIES

A. DIFFERENTIAL PRIVACY

Definition 1 (Differential Privacy [19]–[21]): A randomized me-chanism M gives ε-differential privacy for every set of data outputs S, and for any input neighboring datasets $D_1 = (d_1, d_2, \cdots, d_n)$ and $D_0 = (d_1^{'}, d_2^{'}, \cdots, d_n^{'})$, which has n data entries, if they are different only in the i^{th} data entry [18], i.e. for $i \in N = \{1, 2, \cdots, n\}$, We can express it as $D_1 = (d_1, d_2, \cdots d_{i-1}, d_i, d_{i+1}, \cdots, d_n)$ and $D_0 = (d_1, d_2, \cdots d_{i-1}, d_i^{'}, d_{i+1}, \cdots, d_n)$. If M satisfies:

$$P_r\left[M(D_1) \in S\right] \leq \exp(\varepsilon) \cdot P_r\left[M(D_0) \in S\right]. \tag{1}$$

In definition 1, parameter ε is defined as the privacy budget [20], which dominates the level of differential privacy, in other words, it's a measure of the information leakage. A smaller ε represents a stronger privacy, which means the harder for attackers to infer the sensitive information that belong to users, and then the data utility may be lower due to the stronger privacy. Based on this, in the following sections, we let $u_i(t) = \varepsilon_i(t)$ denotes the privacy loss that the user i can tolerated at time instant t.

For the randomized mechanism M, it has two privacy composition theorems: sequential composition and parallel

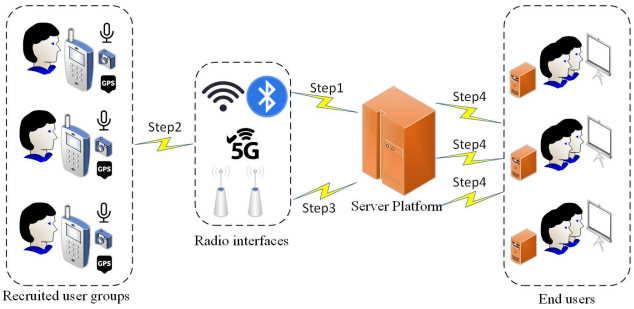

FIGURE 1. Architecture of MCS.

composition [22]. In this paper, we will introduce the parallel composition only.

Lemma 1 (Parallel Composition): Assuming that each of the privacy-preserving mechanisms M_i gives ε_i privacy guarantee for $M = \{M_1, M_2, \cdots, M_n\}$ on a set of disjoint data sets $D_i \in D = \{D_1, D_2, \cdots, D_n\}$, then M will provide $\max(\varepsilon_i)$-differential privacy.

B. LAPLACE MECHANISM

Definition 2 (Laplace Mechanism [20]): A randomized mechanism M is defined as a Laplace mechanism, when M gives ε-differential privacy and a randomized function $g : D \to R$ for every set of data D, if it follows

$$M(D) = g(D) + Lap(\frac{\Delta g}{\varepsilon}). \tag{2}$$

where $Lap(x) = \frac{1}{2b}e^{(-\frac{|x|}{b})}$ is the Laplace noise that subordinated the Laplace distribution, which is centered at 0 with scaling b. Furthermore, $\Delta g = \max_{D_0, D_1} |g(D_0) - g(D_1)|$ is the global sensitivity, which is the biggest difference between the adjacent dataset D_0 and D_1.

C. LINKING ATTACK

Definition 3 (Linking Attack [3], [23]): An attacker uses the background knowledge, which is any information that an attacker possesses, to connect external data with data containing personal privacy in some ways. The aboved process that may leads to the privacy information be disclosure is called linking attack.

D. MOBILE CROWDSENSING NETWORK ARCHITEC-TURE

In this section, we will introduce the architecture of the rese-arched mobile crowdsensing network. Based on [1], the overall operation process of a typical mobile crowdsensing system is shown in Figure 1, which contains four steps.

Step 1: The platform releases one or more tasks, and then the user checks the task and decides whether to accept the task for collecting and contributing their data or not, the data which contains their sensitive information like location data and accelerometer data. In this process, in order to encourage users' participation, platform may use certain incentive mechanisms to encourage more subscribers to upload their data to the platform.

Step 2: The participators take the assignment and collect the related data according to distinct task requirements, then store and process them locally to prevent some attacks like linking attack, finally, submit their data to the platform periodically, irregularly or immediately.

Step 3: The platform stores and gathers the data from all the users, and then releases the aggregation data to the end users after analytical process them according to different privacy requirements and different purpose.

Step 4: The end users get the corresponding data according to different demands, and the data value has been realized. Furthermore, the platform gets some payoff through providing the aggregation data to end users, while the users recruited by the platform get their payoff based on the incentive mechanism setting on step 1.

IV. SYSTEM MODEL

In order to solve the data utility and data privacy tradeoff problem, a differential game theory-based model has been built. Assuming that there exists one platform in the mobile crowdsensing network, meanwhile, the number of users recruited by the platform is N $= \{1, 2, \ldots, n\}$. Here, the platform and the users are the players of the tradeoff game between data utility and data privacy, which will be considered as an N+1 non-cooperative differential game. The privacy loss of the data for user i ($i \in N$) can tolerates at time instant t ($t \in [t_0, T]$) is denoted as $u_i(t)$, and $v(t)$ is the data utility of the total data that collected by the platform during the time interval $[t_0, t](t \in [t_0, T])$. Moreover, let $x(t)$ denotes the total data that reported by all of the users in the period from task start to time t ($t \in [t_0, T]$). Furthermore, based on the basic knowledge in section III, by adding the Laplace noise to the raw data, a perturbated data is obtained, and through the parallel composition, we can get the aggregation data [24]. Here, we assume that we don't care what noise for users added to perturb their raw data to protect the sensitive information, and what methods f(x) for platform used to aggregate the collected data, that is, we only focus on the results about all of the players. The process for data flow is shown as Figure 2 [6].

The variation for total data $x(t)$ at time t relies not only on the data itself, but also the data utility for the platform to achieve the values of the data, as well as the privacy that the users can bear to publish their information to a third party. We assume that a>0 is the growth rate of the total data for the platform due to the (positive) network effect [25], which means the phenomenon that a good, e.g., telephone number has a higher value when it is used by the platform than used by the individual. If the users are participants in the mobile crowdsensing network, the actions of them can be thought as the 'good' with the network effect positively. Then the variations of the data are governed by the following

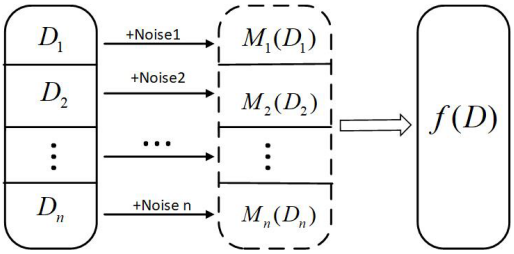

FIGURE 2. The process of data perturbation and data aggregation.

differential equation,

$$\begin{cases} \dfrac{dx(t)}{dt} = ax(t) + \sum_{i=1}^{n} u_i(t)\,[v(t) + \psi_i] + kv(t) \\ x(t_0) = x_0. \end{cases} \tag{3}$$

where ψ_i denotes the effect rate of the data provided by vary users that has different level of privacy to the total number of the data, and $k > 0$ means the effect of data utility to the total data. Furthermore, the trade-off game between the data utility and the privacy loss value can also cause the change to the total data number.

The purposes of users are to maximize the individual's profits through providing data. Meanwhile, to minimize the privacy value $u_i(t)$ for decreasing the leakage of sensitive information. In the process of data aggregation, users can get some rewards, and the total income of users can be described as follows,

$$Q_1 = \begin{cases} p_i u_i(t), & x(t) < \theta \\ [p_i - \mu u_i(t)]u_i(t), & x(t) \geq \theta. \end{cases} \tag{4}$$

where $p_i > 0$ denotes the platform-specified unit price of data for user i due to its privacy setting per unit. θ is the bounds of the number of the data that can be used for the platform, when the total data $x(t)$ exceeded θ, the data is useful, otherwise, it's useless. μ means that the platform gives users a decreasing amount of privacy budget per unit when the data reaches a certain amount. Here we just consider the situation that the data is useful in the subsequent section.

During the game period, there have additional cost for users to protect their sensitive information. The cost function of the privacy protection is related to the privacy loss that the user can accept, and the total data that the platform collected, which can be defined as,

$$Q_2 = c_i u_i(t) + \sigma_i x(t). \tag{5}$$

where c_i is the unit privacy cost of user i. σ_i is the impact rate of total data on user cost. Furthermore, inspired by [26], when user sets its privacy value, it may consider the rewards and the possible data summation, then the cost can be modelled as a varying function about the total data.

When the aggregation data is in stability, the profits of user i at time t is seen as the difference between the income and the cost, which is,

$$Q_3 = [p_i - \mu u_i(t)]u_i(t) - c_i u_i(t) - \sigma_i x(t). \tag{6}$$

Then, for each user $i \in N$, it seeks to

$$\max_{u_i(t)} \int_{t_0}^{T} [(p_i - \mu u_i(t))\,u_i(t) - c_i u_i(t) - \sigma_i x(t)]e^{-r(t-t_0)}dt + q_1 x(T)e^{-r(T-t_0)}. \tag{7}$$

The objective of the platform is to maximize its profits through achieving the values of the aggregated data, which reflects in maximizing the data utility. In mobile crowdsensing, the procedure during the data aggregation, there is a variety of cost expenditure for the platform. The cost function is contained of three portions, that is, the cost of platform for the data further processing, the payments to the users for providing different privacy according to variation standards, and the probability cost of data utility caused by the data summation. The cost function for the platform is shown as,

$$G_1 = \sum_{i=1}^{n} m_i u_i(t) + \sum_{i=1}^{n} (p_i - \mu u_i(t))u_i(t) + \xi x(t). \tag{8}$$

where ξ is the positive parameters, m_i is the unit price of platform for different privacy data processing per unit.

The purpose of the platform for task publish is to obtain benefit during the task process, which can be denoted by the difference between the revenue and the cost. Inspired by the relationship between supply, demand and price in economics, the income function for platform can be shown as,

$$G_2 = [\delta - \zeta v(t)]v(t), \quad (\delta \geq \sum_{i=1}^{n} p_i). \tag{9}$$

where $\delta > 0$ is the platform-specified price for the data resource, ζ is the damping ratio for data utility over time.

According to the analysis of the above, the instantaneous profits of platform at time t can be represented as,

$$G_3 = [\delta - \zeta v(t)]v(t) - \sum_{i=1}^{n} m_i u_i(t) - \sum_{i=1}^{n} (p_i - \mu u_i(t))u_i(t) - \xi x(t). \tag{10}$$

Based on the above analysis, the platform can obtain a optimal solution in which platform seeks to

$$J_p = \max_{v(t)} \int_{t_0}^{T} e^{-r(t-t_0)}\{ [\delta - \zeta v(t)]v(t) - \sum_{i=1}^{n} m_i u_i(t) - \sum_{i=1}^{n} (p_i - \mu u_i(t))u_i(t) - \xi x(t)\}dt + q_2 x(T)e^{-r(T-t_0)}. \tag{11}$$

V. FEEDBACK NASH EQUILIBRIUM SOLUTION OF THE GAME

Based on the non-cooperative differential game model established for the mobile crowdsensing network in section IV, in this section, we try to solve the proposed model given in (3), (7), and (11), to find the feedback Nash equilibrium

solutions, which will be considered as the optimal bounds for the data utility to platform, and the optimal bounds for the data privacy to the users.

For each user, an n-tuple of strategies $\left\{u_i^*(t)\right\}_{i\in N} = \{\phi_i(t,x),$ for $t \in [t_0,T]\}_{i\in N}$ provides a feedback Nash equilibrium solution to the game (3) and (7), if there exists continuously differentiable functions satisfying the following partial differential equations [27],

$$-V_t^i(t,x) = \max_{u_i(t)}\{e^{-r(t-t_0)}[(p_i-\mu u_i(t))u_i(t)-c_iu_i(t)-\sigma_i x(t)] + V_x^i(t,x)[ax(t)+\sum_{i=1}^{n}u_i(t)(v(t)+\psi_i)+kv(t)]\}. \tag{12}$$

$$V^i(T,x) = e^{-r(\mathrm{T}-\mathrm{t}_0)}q_1x(T). \tag{13}$$

Through performing the first order derivation on formula (12), and making it equal to 0, we can get the solution,

$$u_i(t) = \frac{p_i - c_i + e^{r(\mathrm{t}-\mathrm{t}_0)}V_x^i(t,x)[v(t)+\psi_i]}{2\mu}. \tag{14}$$

For the platform, a set of policy $\left\{v^*(t)\right\}_{i\in N} = \{\varphi(t,x),$ for $\mathrm{t} \in [t_0,T]\}_{i\in N}$ provides a feedback Nash equilibrium solution to the game (3) and (11), if there exists continuously differentiable functions $W^i(t,x):[t_0,T]\times R\to R$ satisfying the following partial differential equations [28],

$$-W_t^i(t,x) = \max_{v(t)}\{e^{-r(t-t_0)}[(\delta-\zeta v(t))v(t) - \sum_{i=1}^{n}m_iu_i(t) - \sum_{i=1}^{n}(p_i-\mu u_i(t))u_i(t) - \xi x(t)]\} + W_x^i(t,x)[ax(t)+\sum_{i=1}^{n}u_i(t)(v(t)+\psi_i)+kv(t)]. \tag{15}$$

$$W^i(T,x) = q_2x(T)e^{-r(\mathrm{T}-\mathrm{t}_0)}. \tag{16}$$

Through performing the first order derivation on formula (15) about $v(t)$, and making it equal to 0, we can get the solution

$$v(t) = \frac{\delta + e^{r(t-t_0)}W_x^i(t,x)\cdot[\sum_{i=1}^{n}u_i(t)+k]}{2\zeta}. \tag{17}$$

Lemma 2: The solutions for the two systems (12-13) and (15-16) are

$$V^i(\mathrm{t},x) = e^{-r(t-t_0)}[A_i(t)x+B_i(t)]. \tag{18}$$

$$W^i(\mathrm{t},x) = e^{-r(t-t_0)}[A_{1i}(t)x+B_{1i}(t)]. \tag{19}$$

with $\{A_1(t),A_2(t),\cdots,A_n(t)\}$, $\{B_1(t),B_2(t),\cdots,B_n(t)\}$ and $\{A_{11}(t),A_{12}(t),\cdots,A_{1n}(t)\}$, $\{B_{11}(t),B_{12}(t),\cdots,B_{1n}(t)\}$ satisfying the equations as the following,

$$A_i(t) = \frac{\exp\ [(r-a)^*\varpi(i,t)]-\sigma_i}{r-a},$$

for

$$\varpi(i,t) = T - t + \frac{\ln\ [(r-a)^*q1+\sigma_i]}{r-a}. \tag{20}$$

$$A_i(T) = q_1. \tag{21}$$

And

$$A_{1i}(t) = \frac{\exp\ [(r-a)^*\ell(t)]-\xi}{r-a},$$

for

$$\ell(t) = T - t + \frac{\ln\ [(r-a)^*q2+\xi]}{r-a}. \tag{22}$$

$$A_{1i}(\mathrm{T}) = q_2. \tag{23}$$

Furthermore, referring to [10] and seeing from v(t) in (14) and $u_i(t)$ in (17), we get that v(t) and $u_i(t)$ has no more relation with $B_i(t)$ and $B_{1i}(t)$, so the expression of both is omitted here.

Proof: Based on the formula (18) and (19), we get the derivation of x and t respectively

$$V_t^i(t,x) = e^{-r(\mathrm{t}-\mathrm{t}_0)}[-rA_i(t)x-rB_i(t)+\dot{A}_i(t)x+\dot{B}_i(t)]. \tag{24}$$

$$V_x^i(t,x) = e^{-r(\mathrm{t}-\mathrm{t}_0)}A_i(t). \tag{25}$$

$$W_t^i(t,x) = e^{-r(\mathrm{t}-\mathrm{t}_0)}[-rA_{1i}(t)\,x - rB_{1i}(t)+\dot{A}_{1i}(t)\cdot x+\dot{B}_{1i}(t)] \tag{26}$$

$$W_x^i(t,x) = e^{-r(\mathrm{t}-\mathrm{t}_0)}A_{1i}(t). \tag{27}$$

Using (12-19), we can get,

$$\begin{aligned} &e^{-r(\mathrm{t}-\mathrm{t}_0)}[(p_i-\mu u_i(t))u_i(t) - c_iu_i(t) - \sigma_ix(t)] \\ &\quad + e^{-r(\mathrm{t}-\mathrm{t}_0)}A_i(t)^*[ax(t)+\sum_{i=1}^{n}u_i(t)(v(t)+\psi_i)+kv(t)] \\ &= e^{-r(\mathrm{t}-\mathrm{t}_0)}[rA_i(t)x + rB_i(t) - \dot{A}_i(t)x - \dot{B}_i(t)]. \end{aligned} \tag{28}$$

And,

$$\begin{aligned} &e^{-r(t-t_0)}[(\delta-\zeta v(t))v(t) - \sum_{i=1}^{n}m_iu_i(t) - \sum_{i=1}^{n}(p_i-\mu u_i(t))u_i(t) \\ &\quad - \xi^*x(t)] + e^{-r(t-t_0)}A_{1i}(t)[ax(t) \\ &\quad + \sum_{i=1}^{n}u_i(t)(v(t)+\psi_i)+kv(t)] \\ &= e^{-r(\mathrm{t}-\mathrm{t}_0)}[rA_{1i}(t)x + rB_{1i}(t) - \dot{A}_{1i}(t)\cdot x - \dot{B}_{1i}(t)]. \end{aligned} \tag{29}$$

For (28) and (29) to be hold, it should be satisfied that,

$$\begin{cases}\dot{A}_i(t)+(a-r)A_i(t) = \sigma_i \\ A_i(\mathrm{T}) = q_1.\end{cases} \tag{30}$$

And,

$$\begin{cases}\dot{A}_{1i}(t)+(a-r)A_{1i}(t) = \xi \\ A_{1i}(\mathrm{T}) = q_2.\end{cases} \tag{31}$$

Then we have,

$$A_i(t) = \frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\varpi(i,t)]-\sigma_i}{r-a},$$

$$\varpi(i,t) = T - t + \frac{\ln\ [(\mathrm{r}-\mathrm{a})^*q1+\sigma_i]}{r-a}. \tag{32}$$

TABLE 1. Parameters setting.

	p_i	c_i	σ_i	a	r	q_1	T	ψ_i	μ	δ	ξ	q_2	k	ζ
i=1	0.98	0.2	0.56	0.036	0.05	0.6	5	0.99	0.02	30	0.75	0.8	0.8	0.055
i=2	0.9	0.35	0.6					0.8						
i=3	0.85	0.4	0.66					0.7						
i=4	0.8	0.5	0.8					0.6						

$$A_{1i}(t) = \frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\ell(t)] - \xi}{r-a},$$
$$\ell(t) = T - t + \frac{\ln\ [(\mathrm{r}-\mathrm{a})^* q2 + \xi]}{r-a}. \tag{33}$$

□

From (14), (25), (32) and (17), (27), (33), we can get the solutions to the users and the platform, respectively,

$$u_i(t) = \frac{p_i - c_i + [\frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\varpi(i,t)]-\sigma_i}{r-a}] \cdot\ [v(t)+\psi_i]}{2\mu}. \tag{34}$$

$$v(t) = \frac{\delta + [\frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\ell(t)]-\xi}{r-a}] \cdot [\sum_{i=1}^{n} u_i(t) + k]}{2\zeta}. \tag{35}$$

Using (34) and (35), we can get the optimal control strategies $u_i^*(t)$ and $v^*(t)$ for the users and the platform, respectively,

$$u_i^*(t) = H + G^* \frac{M + N^* \sum_{i=1}^{n} H}{1 - N^* \sum_{i=1}^{n} G}. \tag{36}$$

$$v^*(t) = \frac{M + N^* \sum_{i=1}^{n} H}{1 - N^* \sum_{i=1}^{n} G}. \tag{37}$$

where,

$$H = \frac{p_i - c_i(t) + \left[\frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\varpi(i,t)]-\sigma_i}{r-a}\right]^* \psi_i}{2\mu},$$
$$G = \frac{\frac{\exp\ [(r-a)^*\varpi(i,t)]-\sigma_i}{r-a}}{2\mu},$$
$$M = \frac{\delta + \left[\frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\ell(t)]-\xi}{r-a}\right]^* k}{2\zeta},$$
$$N = \frac{\frac{\exp\ [(\mathrm{r}-\mathrm{a})^*\ell(t)]-\xi}{r-a}}{2\zeta}.$$

Through submitting the formula (36) and (37) into the equation of state expression (3), we get the optimal state in the non-cooperative differential game, which is written as follows,

$$\begin{cases} \dfrac{dx^*(t)}{dt} = ax^*(t) - \sum_{i=1}^{n} [H + G^* \dfrac{M + N^* \sum_{i=1}^{n} H}{1 - N^* \sum_{i=1}^{n} G}]^* \\ \quad \{[\dfrac{M + N^* \sum_{i=1}^{n} H}{1 - N^* \sum_{i=1}^{n} G}] + \psi_i\} + k[\dfrac{M + N^* \sum_{i=1}^{n} H}{1 - N^* \sum_{i=1}^{n} G}] \\ x(t_0) = x_0. \end{cases} \tag{38}$$

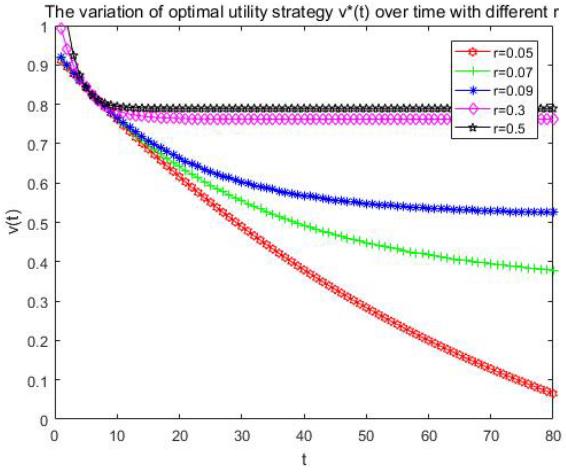

FIGURE 3. The variation of optimal utility strategy v*(t) over time with different r.

VI. NUMERICAL SIMULATIONS AND ANALYSIS

In this section, numerical simulations are made to test the performance of the game model given in the above sections. For the parameters setting, we set up two data for the simulation as an illustration, the growth rate that brought by the positive network effect a is set to be 0.036, for people participating in the recruitment tasks, to some extent, due to the effect, which may not be the main reason for users to complete the perceptual tasks, though the individual value can be embodied in a group than be the personal one. Moreover, the discount rate r that represent the value of possible future benefits in the present, when it takes different values, the convergence rate is different with time. It is obvious that the bigger the r is, the faster the convergence rate is for the

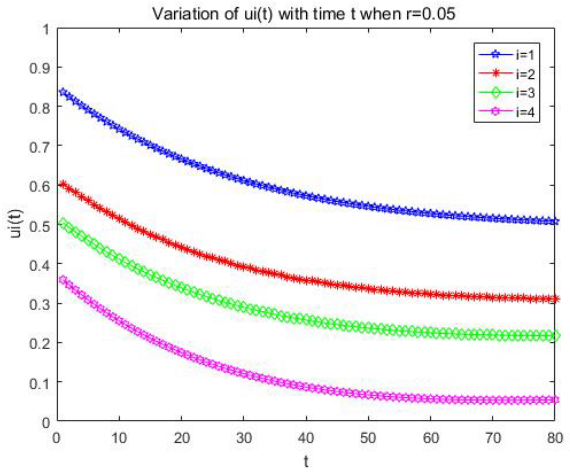

FIGURE 4. The variation of $u_i(t)$ with time t when r = 0.05.

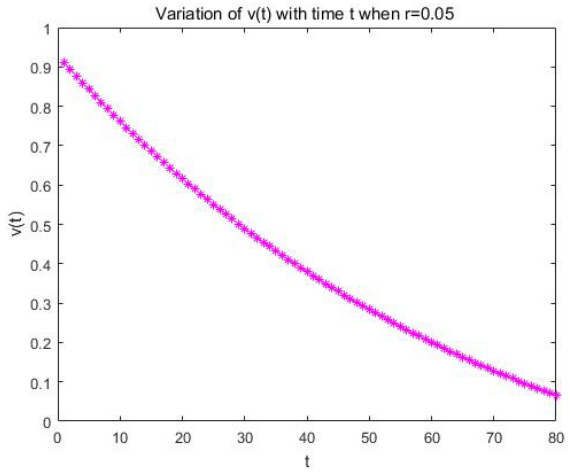

FIGURE 5. The variation of v(t) with time t when r = 0.05.

optimal utility strategy, which is shown in Figure 3. The same as [29], the discount rate here is set to be r = 0.05. The other parameters to users and the platform are set as follows in Table 1.

From the simulation results, we get the variation of the optimal strategies for the users and platform, which is exhibited in Figure 4 and Figure 5, respectively. From Fig.4, we see that the privacy $u_i(t)$ to each user is decreased with time. For the smaller the value of $u_i(t)$ is, a stronger privacy requirement that needs to be achieved. With time goes by, more and more individual information may be leaked, so users who submit individual data to platform may not want to participate in the sensing task.

From Figure 5, the variation of v(t) with time t is also declining, for users, with it is privacy needs stronger than the beginning, and the stronger the privacy is, the weaker the utility is, all of which results in the decline of the data utility for platform with time, so the total number of the data to platform collected is coming down, which is illustrated in the Figure 6.

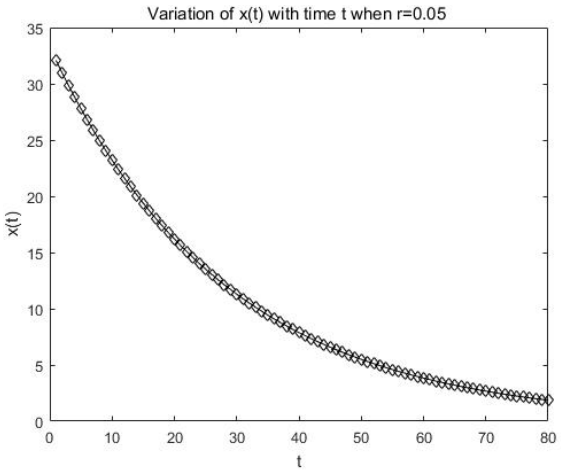

FIGURE 6. The variation of x(t) with time t when r = 0.05.

Based on the result shown as above, it is also shown that a better incentives mechanism should be designed to motivate users to participate in different sensing tasks to implement the profit maximized of the data.

VII. CONCLUSION AND FUTURE WORK

In order to implement data privacy-preserving in mobile crowdsensing, there are two aspects that needs to be considered, the first one is how to guarantee privacy in data application phase, and the second aspect is how to be beneficial to the application of data. So, it's a trade-off problem between getting a good data utility and protecting individual privacy, which is also a contradictional and important problem.

In this paper, to address the above problem when privacy requirement for users may time-varying due to distinct purpose, firstly, we formulate a non-cooperative differential game model to verify whether there exists an equilibrium state for data utility and user privacy. Secondly, by solving the model, we get the unique Nash equilibriums. And finally, numerical simulations have been made to show the correctness of the model we have devised.

In the future research work, firstly, a more effective incentive mechanism for platform will be devised to irritate more users partake. Secondly, a more suitable data aggregation mechanism and data perturbation mechanism will be designed to have a maximization for both privacy and utility. Finally, we plan to implement a realistic MCS platform based on the game model and the suitable incentive, data aggregation and data perturbation mechanism to realize a better performance against linking attacks in MCS for user's privacy-preserving demands, which may be time-varying in the data releasing process.

REFERENCES

[1] D. Christin, A. Reinhardt, S. S. Kanhere, and M. Hollick, "A survey on privacy in mobile participatory sensing applications," *J. Syst. Softw.*, vol. 84, no. 11, pp. 1928–1946, Nov. 2011.

[2] J. Wang, M. Li, Y. He, H. Li, K. Xiao, and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications," *IEEE Access*, vol. 6, pp. 17545–17556, 2018.

[3] P. Samarati, "Protecting respondents' identities in microdata release," *IEEE Trans. Knowl. Data Eng.*, vol. 13, no. 6, pp. 1010–1027, Nov. 2001.

[4] G. Loukides and J. Shao, "Capturing data usefulness and privacy protection in K-anonymisation," in *Proc. ACM Symp. Appl. Comput.*, New York, NY, USA, Mar. 2007, pp. 370–374.

[5] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "INCEPTION: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proc. ACM 17th Int. Symp. Mobile Ad Hoc Netw. Comput.*, New York, NY, USA, Jul. 2016, pp. 341–350.

[6] M. Zhang, J. Chen, L. Yang, and J. Zhang, "Dynamic pricing for privacy-preserving mobile crowdsensing: A reinforcement learning approach," *IEEE Netw.*, vol. 33, no. 2, pp. 160–165, Mar./Apr. 2019.

[7] W. Wang, L. Ying, and J. Zhang, "The value of privacy: Strategic data subjects, incentive mechanisms and fundamental limits," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 44, no. 1, pp. 249–260, Ju. 2016.

[8] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. Theory Cryptogr. Conf.*, Berlin, Germany, 2006, pp. 265–284.

[9] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," *IEEE Trans. Big Data*, to be published.

[10] Z.-M. Cheng, X.-W. Zhou, and Y. Ding, "A transmission rate control algorithm based on non-cooperative differential game model in deep space networks," *Wireless Pers. Commun.*, vol. 71, no. 3, pp. 1915–1929, Aug. 2013.

[11] D. W. K. Yeung and L. A. Petrosjan, *Cooperative Stochastic Differential Games*. New York, NY, USA: Springer, 2006. doi: 10.1007/0-387-27622-X.

[12] C. Miao, W. Jiang, L. Su, Y. Li, S. Guo, Z. Qin, H. Xiao, J. Gao, and K. Ren, "Cloud-enabled privacy-preserving truth discovery in crowd sensing systems," in *Proc. 13th ACM Conf. Embedded Netw. Sensor Syst.*, New York, NY, USA, Nov. 2015, pp. 183–196.

[13] F. Ma, Y. Li, Q. Li, M. Qiu, J. Gao, S. Zhi, L. Su, B. Zhao, H. Ji, and J. Han, "FaitCrowd: Fine grained truth discovery for crowdsourced data aggregation," in *Proc. 21th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, New York, NY, USA, Aug. 2015, pp. 745–754.

[14] L. Su, Q. Li, S. Hu, S. Wang, J. Gao, H. Liu, J. Han, T. F. Abdelzaher, X. Liu, Y. Gao, and L. Kaplan, "Generalized decision aggregation in distributed sensing systems," in *Proc. IEEE Real-Time Syst. Symp.*, Rome, Italy, Dec. 2014, pp. 1–10.

[15] L. Xiao, Y. Li, G. Han, H. Dai, and H. V. Poor, "A secure mobile crowdsensing game with deep reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 35–47, Jan. 2018.

[16] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 54–67, 1st Quart., 2016.

[17] L. G. Jaimes, I. J. Vergara-Laurens, and A. Raij, "A survey of incentive techniques for mobile crowd sensing," *IEEE Internet Things J.*, vol. 2, no. 5, pp. 370–380, Oct. 2015.

[18] Y. Zhang, Y. Mao, H. Zhang, and S. Zhong, "Privacy preserving market schemes for mobile sensing," in *Proc. 44th Int. Conf. Parallel Process. (ICPP)*, Beijing, China, Sep. 2015, pp. 909–918.

[19] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*, vol. 4052, Venice, Italy, 2006, pp. 1–12. doi: 10.1007/11787006_1.

[20] T. Zhu, G. Li, W. Zhou, and P. S. Yu, *Differential Privacy and Applications*, vol. 69. Cham, Switzerland, 2017. doi: 10.1007/978-3-319-62004-6.

[21] D. Vu and A. Slavkovic, "Differential privacy for clinical trial data: Preliminary evaluations," in *Proc. IEEE Int. Conf. Data Mining Workshops*, Miami, FL, USA, Dec. 2009, pp. 138–143.

[22] F. D. McSherry, "Privacy integrated queries: An extensible platform for privacy-preserving data analysis," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, New York, NY, USA, Jul. 2009, pp. 19–30.

[23] D. J. Martin, D. Kifer, A. Machanavajjhala, J. Gehrke, and J. Y. Halpern, "Worst-case background knowledge for privacy-preserving data publishing," in *Proc. IEEE 23rd Int. Conf. Data Eng.*, Istanbul, Turkey, Apr. 2007, pp. 126–135.

[24] L. Yang, M. Zhang, S. He, M. Li, and J. Zhang, "Crowd-empowered privacy-preserving data aggregation for mobile crowdsensing," in *Proc. ACM 18th Int. Symp. Mobile Ad Hoc Netw. Comput.*, Los Angeles, CA, USA, Jul. 2018, pp. 151–160.

[25] M. Zhang, L. Yang, X. Gong, and J. Zhang, "Privacy-preserving crowdsensing: Privacy valuation, network effect, and profit maximization," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.

[26] H. Xu, X. Zhou, and Y. Chen, "A differential game model of automatic load balancing in LTE networks," *Wireless Pers. Commun.*, vol. 71, no. 1, pp. 165–180, Jul. 2013.

[27] L. Miao and S. Li, "A differential game-theoretic approach for the intrusion prevention systems and attackers in wireless networks," *Wireless Pers. Commun.*, vol. 103, no. 3, pp. 1993–2003, Dec. 2018.

[28] X. An, F. Lin, S. Xu, L. Miao, and C. Gong, "A novel differential game model-based intrusion response strategy in fog computing," *Secur. Commun. Netw.*, vol. 2018, Aug. 2018, Art. no. 1821804.

[29] H. Xu, Z. He, and X. Zhou, "Load balancing algorithm of ultra-dense networks: A stochastic differential game based scheme," *KSII Trans. Internet Inf. Syst.*, vol. 9, no. 7, pp. 2454–2467, Jul. 2015.

HONGJIE GAO received the M.S. degree from the School of Mathematics and Physics, University of Science and Technology Beijing, China, in 2017, where she is currently pursuing the Ph.D. degree with the School of Computer and Communication Engineering. Her research interests include game theory, data privacy, and security in mobile crowdsensing.

HAITAO XU received the B.S. degree in communication engineering from Sun Yat-sen University, in 2007, the M.S. degree in communication system and signal processing from the University of Bristol, in 2009, and the Ph.D. degree from the University of Science and Technology Beijing (USTB), in 2014. He was engaged in postdoctoral study with the Department of Software Engineering, USTB, from 2014 to 2016. He was a Visiting Professor with the Electrical and Computer Engineering Department, University of Houston, from October 2016 to April 2017. He is currently an Associate Professor with USTB. He has published 50 articles, and one book for cyber security. His research interests include wireless communications, game theory, secure communications, cognitive radio, and mobile edge computing.

LONG ZHANG received the B.E. degree in communication engineering from the China University of Geosciences, Wuhan, China, in 2006, and the Ph.D. degree in communication and information systems from the University of Science and Technology Beijing, Beijing, China, in 2012. In 2017, he was a Visiting Scholar with the School of Computing, Tokyo Institute of Technology, Tokyo, Japan. He is currently an Associate Professor with the School of Information and Electrical Engineering, Hebei University of Engineering, Handan, China, and also a Visiting Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX, USA. His research interests include cognitive radio, vehicular networks, UAV assisted wireless networks, network functions virtualization, fog/edge computing, deep space communications, space-terrestrial integrated networks, AI enabled networks, radio resource allocation, machine learning, and hypergraph.

XIANWEI ZHOU is currently a Professor with the Department of Communication Engineering, School of Computer and Communication Engineering, University of Science and Technology Beijing. His research interests include the security of communication networks, next-generation networks, mobile computing, scheduling theory, and game theory.