Gather or Scatter: Stackelberg Game Based Task Decision for Blockchain-Assisted Socially-Aware Crowdsensing Framework

Sijie Huang, Guoju Gao, He Huang, *IEEE Member,* Yu-E Sun, *IEEE Member*, Yang Du, Mingjun Xiao, *IEEE Member*, Jie Wu, *IEEE Fellow*, and Yihuai Wang

Abstract—Mobile Crowdsensing (MC), an excellent solution to large-scale spatio-temporal data sensing problems, has recently received lots of attention from both industry and academia. In the MC system, any requester can acquire the sensing data for his points of interest (PoIs) by offering some payments to attract a group of mobile users capable of completing these PoI-related sensing tasks. However, the current MC work neglected three vital factors, more or less. First, they assume that these distributed users are mutually independent in MC, ignoring the social effects. Actually, the sensing data collected by one user may be corroborated by others' sensing data, so-called "*information corroboration*". Second, all rational and selfish users are inclined to gather to perform these tasks due to information corroboration. Meanwhile, they may be strategic about their participation levels to maximize profits. However, more similar sensing data will undoubtedly lower the *information value*, so any user has a tradeoff between gather and scatter. Third, although mobile users can obtain some payments, privacy issues may still prevent them from participating in MC. In this paper, we propose a secure blockchain-assisted socially-aware MC framework by adopting the smart contract technique of Ethereum. For this framework, we further devise a two-stage Stackelberg game model to assist the requester (i.e., the leader in the game) in properly pricing each PoI-related sensing task, so that mobile users (i.e., the followers in the game) can exactly select their tasks and determine their participation levels. To analyze the game equilibrium, we extend the traditional Hessian matrix method to a multi-dimension case involving the multi-user multi-task hyperspace setting. We conduct extensive experiments to prove the equilibrium and effectiveness of the proposed solution. We also implement a prototype and deploy the smart contract to an official Ethereum test network to demonstrate the practicability of the proposed framework.

Index Terms—Blockchain-based crowdsensing, social effects, game theory, information corroboration, privacy preservation.

1 Introduction

Over the past few years, the proliferation of mobile smart devices has prompted Mobile Crowdsensing (MC) to become one of the most promising solutions to large-scale data sensing and collection problems, e.g., intelligent transportation and environmental monitoring [1–4]. A typical MC system consists of three parties: task requester, many mobile users, and a platform such as CitizenMe, DataExchange, Datacoup, etc. The requester can recruit mobile users through the MC platform by posting the PoI-related [5, 6] tasks and offering payment to get their interested data. Mobile users then leverage their carry-on smartphones or tablets to provide location-based services (e.g., collect sensing data). During this process, users may face potential privacy threats and inevitably consume some resources such as CPU computing power, storage memory, battery energy, etc., so it is necessary to design an effective pricing mechanism to motivate users to well participate in MC.

Although lots of existing research on MC focuses on designing the incentive mechanism to maximize the social welfare [7, 8], or stress on resource allocation to ensure data service quality [9, 10], they more or less ignore three significant factors. First, most of the existing work assumes that mobile users are mutually independent in the MC system [5]. However, we argue that the social effects among mobile users cannot be simply ignored. As a member of a social group, mobile users will produce a mutual influence on each other through social communication. When several users are assigned to perform the same PoI-related sensing task simultaneously, one user may improve another one's information credibility through the social effects. We call this "information corroboration". For example, in the crowdsensing application for collecting road traffic information, mobile users can contact their friends who also join in this sensing scenario to share the collected data, so that they can obtain more comprehensive traffic information with less

- *S. Huang, G. Gao*, H. Huang*, Y. Du, and Y. Wang are with the School of Computer Science and Technology, Soochow University, Suzhou, China. G. Gao and H. Huang are the corresponding authors. E-mail: gjgao@suda.edu.cn & huangh@suda.edu.cn*
- *Y. Sun is with the School of Rail Transportation, Soochow University, Suzhou, China. E-mail: sunye12@suda.edu.cn*
- *M. Xiao is with the School of Computer Science and Technology / Suzhou Institute for Advanced Study, University of Science and Technology of China, Hefei, P. R. China. Email: xiaomj@ustc.edu.cn*
- *J. Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122. E-mail: jiewu@temple.edu*

The work of S. Huang, G. Gao, H. Huang, Y. Sun, Y. Du, and Y. Wang was supported by the National Natural Science Foundation of China (NSFC) under Grant U20A20182, 62102275, 61873177, 62072322, in part by the NSF of Jiangsu in China under Grant BK20210704, and in part by the NSF of the Jiangsu Higher Education Institutions of China under Grant 21KJB520025. The work of M. Xiao was supported by the NSFC under Grant 62172386, 61872330, 61936015, and U1709217. The work of J. Wu was supported by NSF Grants CPS 2128378, CNS 2107014, CNS 2150152, CNS 1824440, CNS 1828363, and CNS 1757533.

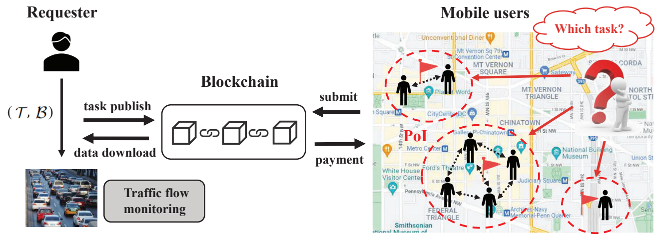

Fig. 1. Secure blockchain-based socially-aware crowdsensing system.

effort. In addition, the participation of one's friends will further promote her motivation for contributing and sharing more information in such crowdsensing services. Therefore, social influence among socially-connected users plays a significant role in socially-aware crowdsensing services.

Second, considering the effect of information corroboration, these mobile users, as rational and selfish individuals, tend to gather at the same point to perform the same sensing task. This is because other social network users can enhance their sensing contribution. However, with the increase in the similarity and substitutability of the sensing data, too many users congregating on the same PoI-related task will inevitably bring redundant data and reduce the information value. Here, the term "information value" refers to the rarity and unsubstitutability of sensing data. The common economic phenomenon indicates that the price of a commodity will decrease if there are too many suppliers of it. Specifically, for one sensing task with many participants, the data provided by one user is usually replaceable and cheaper, which means the information value is lower. In contrast, for the sensing task with fewer participants, each user needs to consume more resources to compensate for the lack of social effect benefits, and thus the obtained data is more precious. For mobile users, task decision is a tradeoff problem, because there is a contradiction between the information value of sensing data and positive effects from the crowd in the social network. In particular, mobile users are not only collaborators but also competitors to each other. The challenge lies in how the requester determines a task pricing strategy to attract an appropriate number of users for each PoI-related task to avoid unbalanced participation.

Third, privacy protection is also a pivotal issue in the MC system [11–13]. Since the requester's PoIs are highly related to the location information, mobile users will undoubtedly be concerned about their location privacy. On the other hand, the MC platform might be untrusted, which will result in the leak of users' sensitive information, including date of birth, home address, disease, etc. Therefore, how efficiently protecting users' location and data privacy in the MC system is quite important.

Inspired by the above considerations, we propose a Secure Blockchain-assisted Socially-aware Mobile Crowdsensing (SBS-MC) framework in this paper, as shown in Fig.1. For SBS-MC, we take the social effects and information value into consideration. Based on this, we model the task decision problem as a special Stackelberg game, in which the requester and mobile users are seen as the leader and followers, respectively. Also, we bring in the blockchain technique to protect mobile users' location and data privacy. Here, some special complex programs are deployed on the blockchain, called smart contracts, which can automatically perform operations according to the conditions of the transaction treaty, forcing participants to perform their obligations [14]. More specifically, the requester launches some PoI-related sensing tasks and submits her deposit to the smart contract. Then users are recruited by the smart contract to perform these tasks. Here, the users will encrypt the collected data and store it on the blockchain, and finally send the address to the smart contract to get the payoff.

Our contribution in this paper is three-fold:

1) We introduce the concepts of information corroboration and information value in the MC system, and further study their impact on mobile users' task decision strategy and sensing data quality. Meanwhile, we are also concerned about mobile users' location and data privacy. To the best of our knowledge, we are the first to consider these three factors together in the MC system. To this end, we propose the SBS-MC framework, in which the smart contract technique of blockchain is used to protect users' privacy. For SBS-MC, we model the interaction between the requester and users as a hierarchical Stackelberg game, where the requester and users are seen as the leader and followers in the game, respectively.
2) We extend the Hessian matrix to a multi-dimension case to handle the optimization problem in SBS-MC, which actually involves the multi-user multi-task hyperspace setting. We further prove the problem is concave and has the optimal solution. We derive the explicit-form expressions of the most beneficial task pricing strategy for the requester and the optimal decision strategy for mobile users. In addition, we analyze the existence and uniqueness of the Stackelberg Equilibrium (SE), based on which we propose an algorithm to obtain the SE.
3) We conduct extensive experiments to verify the significant performance of the proposed solution for the SBS-MC framework. The experimental results show that the social effects will promote higher participation levels and bring higher revenues to the requester. Moreover, we implement a prototype and deploy the smart contract to an official Ethereum test network to demonstrate the practicability of our SBS-MC framework.

This paper is organized as follows. Section II describes the system model and game formulation. Section III gives the analysis of the equilibrium and optimal solution. Section IV introduces the blockchain and devises the protocol based on the smart contract. In Section V, numerical experiments are conducted to evaluate SBS-MC. We discuss the related work in Section VI and give a conclusion in Section VII.

2 Framework and Problem Formulation

2.1 Socially-Aware Crowdsensing Framework

We first introduce the SBS-MC framework, which consists of a requester, some mobile users, and a smart contract deployed on the blockchain, as shown in Fig. 1. The requester leverages the blockchain to publish their PoI-related sensing tasks and then recruits some mobile users to complete these tasks, based on which the location and data privacy for users can be protected. Influenced by the social network effect, mobile users would prefer gathering to obtain more support from others under the same participation level, which is called information corroboration. However, the aggregation phenomenon for users will undoubtedly lower the information value of the collected data. Hence, any mobile user has to face a tradeoff between gather and scatter. We model the interaction between the requester and mobile users as a hierarchical Stackelberg game.

Let $\mathcal{T} = \{1, 2 \cdots, l\}$ denote the requester's l sensing tasks. In order to ensure the completion quality of each task, the requester has a minimum participation threshold for each task, denoted as $Q = \{q_1, q_2, \cdots, q_l\}$. For the convenience of description, we use k to represent the index for one sensing task. Meanwhile, we use $\mathcal{N} = \{1, 2, \cdots, n\}$ to denote n mobile users in the framework. Since each task is location-sensitive and incompatible with each other, each user can only complete one task at a time. Each user $i \in \mathcal{N}$ will choose a task to execute and determine her participation level, denoted as user i's strategy profile $\beta_i \triangleq \left(k, x_i^k\right)$ where $k \in \mathcal{T}$. Here, k denotes the sensing task index that user i selects, and the participation level x_i^k depends on user i's sensing time, data transmission frequency, etc., which is highly related to the completion quality and the consumed cost. Since each sensing task k has a minimum participation threshold q_k, we have the constraint $\sum_{i \in \Phi_k} x_i^k \geq q_k$ for $\forall k \in \mathcal{T}$, in which Φ_k means the set of mobile users that will select the task k. Note that, under the influence of potential social networks, one user's completion quality on a task (also called "contribution") depends not only on her individual participation level but also on the other users' participation levels in the social networks. We introduce the concept of the users' contribution as follows.

2.2 Mobile User's Contribution

Based on the user i's strategy $\beta_i = \left(k, x_i^k\right)$, we use $\mathcal{X}_i^k$ to denote user i's contribution to task k, that is,

$$\mathcal{X}_i^k = f_i\left(x_i^k\right) + \Gamma\left(x_i^k, \mathbf{x}_{-i}\right), \tag{1}$$

where $\mathbf{x}_{-i}$ denotes the participation level vector of all users excluding user i. In Eq. (1), $f_i\left(x_i^k\right)$ represents the contribution made by user i's own participation irrespective of other users. It can for simplicity be formulated as $f_i\left(x_i^k\right) = a_i x_i^k - b_i {x_i^k}^2$, where $a_i > 0$ and $b_i > 0$ are the coefficients that capture the intrinsic value of the participation to heterogeneous mobile users [15]. When the value of x_i^k satisfies $x_i^k \in (0, \frac{a_i}{2b_i}]$, we have that $f_i : (0, \frac{a_i}{2b_i}] \to \mathbb{R}$ is a submodular function. More specifically, $f_i\left(x_i^k\right)$ grows up with the increment of x_i^k, while the growth rate of $f_i\left(x_i^k\right)$ decreases accordingly. This is in line with the impact of the people's effort on result quality in reality. $\Gamma\left(x_i^k, \mathbf{x}_{-i}\right)$ denotes the external influence gained from other mobile users through social effects. Motivated by the idea of social effects in [16], we represent the relationship between two entities in a social network by the adjacency matrix $\mathbf{G} = [g_{ij}]_{i,j \in \mathcal{N}}$. The ij-th entry of $\mathbf{G}$, denoted as $g_{ij} \in [0, 1]$, indicates the influence strength of the user j on user i. Therefore, we adopt $\Gamma\left(x_i^k, \mathbf{x}_{-i}\right) = \sum_{j \in \mathcal{N}} g_{ij} x_i^k x_j^k$ to represent the additional benefits obtained from the social network effects.

TABLE 1
Description of commonly-used notations.

Variable	Description
$\mathcal{N}$	The set of mobile users.
$\mathcal{T}$	The set of PoI-related sensing tasks.
i, k	The indexes for user and task, respectively.
x_i^k	The participation level of user i for task k.
$\mathcal{X}_i^k$	The user i's contribution to the task k.
$\mathbf{x}$	The participation levels of all mobile users.
$\mathbf{x}_{-i}$	The participation levels of all users excepting i.
β_i, $\vec{\beta}_{-i}$	The strategy profile of user i and others excepting i.
Ψ	The budget of the requester.
B_k, $\mathcal{B}$	The pricing for task k and the pricing vector.
q_k / $\mathcal{Q}$	Participation threshold for task k / all tasks.
g_{ij}	The influence of user j on user i.
τ_i^k	The probability of user i selecting the task k.
c	The unit cost of executing sensing task.
$\Phi_k/\lvert\Phi_k\rvert$	The set / number of users who choose task k.
U_i / Ω	The utility of user i / the requester.

Like the previous research [15, 16], we consider that bilateral interactions are symmetric, that is, $g_{ij} = g_{ji}$ and $g_{ii} = 0$. Note that the proposed model can be easily extended to the setting of asymmetric social influences. Now, the sensing contribution of user i to task t_k is formulated as follows:

$$\mathcal{X}_i^k = a_i x_i^k - b_i {x_i^k}^2 + \sum_{j \in \mathcal{N}} g_{ij} x_i^k x_j^k, \text{ where } x_i^k \in (0, \frac{a_i}{2b_i}]. \tag{2}$$

Here, the characteristic attributes of each user, i.e., a_i and b_i, are known as public information in the crowdsensing framework, which is prior knowledge derived from the user's accumulation participation in the previous mobile crowdsensing process.

2.3 Information Value of Sensing Data

Due to the influence of social communication, users may strategically adjust their participation level and tend to gather at the same point to maximize their profits. Similar to the value law of commodities, users' gathering action will reduce the value of information. Therefore, the requester needs to adjust her pricing strategy dynamically to attract more mobile users to participate in PoI-related sensing tasks and guide mobile users to gather reasonably. In the SBS-MC framework, the requester first claims the sensing tasks with different PoIs and meanwhile gives the pricing vector for each sensing task, denoted as $\mathcal{B} = (B_1, B_2, \cdots, B_l)$. The value of unit sensing data for task k can be denoted as:

$$V_k = B_k / \left|\Phi_k\right|. \tag{3}$$

Note that the pricing strategy B_k is the investment ratio adjustment made by the requester to compensate mobile users for performing the task k. The value of B_k is not related to the importance of one task. V_k changes dynamically with the number of people participating in task k.

2.4 Mobile User's Utility

In the SBS-MC framework, mobile users' payments are affected by the information value of sensing data and their contribution to the sensing tasks. We formulate the user's payment (denoted as R_i) as the information value of sensing data multiplied by his contribution:

$$R_i = V_k \cdot \mathcal{X}_i^k. \tag{4}$$

Now, we introduce mobile users' utility which is determined by the payment received from the requester and the consumed cost. Let c denote the unit cost associated with the user's participation level, so the user i's cost is cx_i. By replacing the values of V_k and $\mathcal{X}_i^k$, we have user i's utility as follows:

$$U_i = \frac{B_k}{|\Phi_k|} \cdot \left(a_i x_i^k - b_i {x_i^k}^2 + \sum\nolimits_{j \in \mathcal{N}} g_{ij} x_i^k x_j^k \right) - c x_i^k. \tag{5}$$

Eq. (5) represents that, on the one hand, the user who devotes more participation level leads to a higher total contribution to the sensing results but also brings more cost consumption. On the other hand, the user gathering in the crowd may complete the sensing task more efficiently, but it reduces the information value of sensing data.

2.5 Requester's Utility

After receiving the data from mobile users, the requester can obtain these related points' desired sensing information. The requester benefits from the sensing data, which monotonically increases with the user's participation level. Due to the heterogeneous characteristics of mobile devices, they may contribute differently to the sensing quality for a given amount of sensing time. To capture this setting, we use $h_i > 0$ to indicate the contribution of unit sensing time to the data quality that user i makes. The utility for the requester is given by the rewards of total aggregated PoI-related sensing data from all users minus the total payment, i.e.,

$$\Omega = \sum\nolimits_{k \in \mathcal{T}} \sum\nolimits_{i \in \Phi_k} \left(h_i x_i^k - V_k \cdot \mathcal{X}_i^k \right). \tag{6}$$

The first part of Eq. (6) is the reward function associated with user i. We here use the linear function to profile the relationship between the users' participation level and the monetary benefit of the requester. The requester will obtain higher rewards when facing the users with a higher quality of sensing data.

2.6 Two-Stage Stackelberg Game

We model the interaction between the requester and users as a hierarchical two-stage Stackelberg game, where the requester acts as the leader in the first stage who publishes PoI-related sensing tasks. The requester will also give the pricing vector for each task to attract enough users according to some requirements. In the second stage, mobile users determine which task to complete and their participation levels according to potential social effects and the pricing vector of the requester.

Definition 1 *Let $\mathbf{x}^*$ and $\mathcal{B}^*$ denote the optimal participation level vector of all users and the optimal pricing vector of the requester. The point $(\mathbf{x}^*, \mathcal{B}^*)$ is the Stackelberg equilibrium if the following two conditions are satisfied:*

$$\Omega\left(\mathcal{B}^*, \mathbf{x}^*\right) \geq \Omega\left(\mathcal{B}^{'}, \mathbf{x}^*\right), \tag{7}$$

$$U_i\left(x_i^*, \mathbf{x}_{-i}^*, \mathcal{B}^*\right) \geq U_i\left(x_i^{'}, \mathbf{x}_{-i}^*, \mathcal{B}^*\right). \tag{8}$$

Here, $\mathbf{x}_{-i}^*$ is the best response participation level vector for all users excluding i. In the next section, we will analyze the game equilibrium in the above model, based on which we design the asynchronous response algorithm.

3 Stackelberg Game Equilibrium Analysis

We analyze the optimal participation level strategy of all users and the utility maximization of the requester under the Stackelberg game with a complete information model. Note that since the above model involves the multi-dimension vector space problem, we extend the Hessian matrix method to the multi-dimension case in this paper. We first analyze the users' participation equilibrium problem in Stage II and then study the pricing strategy of the requester in Stage I, according to the general game work [5, 16].

3.1 Stage II: Users' Participation Equilibrium

Each user's response includes two parts: choosing which task to perform and the specific participation level, i.e., $\beta_i = \left(k, x_i^k\right)$. Since each user is selfish and aims at maximizing their own payoff, the competition among users can be formulated as a non-cooperative game, called users' sub-game, whose solution is the well-known Nash equilibrium. Based on the definition of Stackelberg game equilibrium, as the pricing strategy of the requester is given, each user determines his participation level for one sensing task as the best response. We first introduce the definition of the best response.

Definition 2 $\beta_i^* \triangleq \left(k^*, x_i^{k^*}\right)$ *is user i's optimal response in the users' sub-game if $U_i\left(\beta_i^*, \vec{\beta}_{-i}^*, \mathcal{B}^*\right) \geq U_i\left(\beta_i^{'}, \vec{\beta}_{-i}^*, \mathcal{B}^*\right)$, where $\vec{\beta}_{-i}^*$ is the best response vector of all users except i.*

Since k is a discrete variable, in order to facilitate analysis and calculation, we let $\tau_i^k \geq 0$ denote the probability of user i choosing task k. Based on this, we transform the discrete optimization problem into a continuous problem. Then, the strategy space of each user is extended to a strictly non-empty compact subset of the Euclidean space, and the utility function is a continuous and quasi-concave function as follows:

$$\begin{aligned} U_i &= \sum\nolimits_{k \in \mathcal{T}} \tau_i^k \left(V_k \cdot \mathcal{X}_i^k - c x_i^k \right) \\ &= \sum_{k \in \mathcal{T}} \tau_i^k \Big[\frac{B_k}{|\Phi_k|} \Big(a_i x_i^k - b_i {x_i^k}^2 + \sum_{j \in \mathcal{N}} g_{ij} x_i^k x_j^k \Big) - c x_i^k \Big]. \end{aligned} \tag{9}$$

Here, we use $|\Phi_k| = \sum_{i \in \mathcal{N}} \tau_i^k$ to denote the probability of selecting task k for all users, and $\left|\Phi_{-i}^k\right|$ means the sum of all users' probability (except user i) for task k. The user's competition with each other to maximize their own utility in stage II can be modeled as the non-cooperative sub-game problem.

Problem 1.

$$\begin{aligned} &\text{maximize} \quad U_i\left(\beta_i, \vec{\beta}_{-i}^*, \mathcal{B}^*\right) \\ &\text{subject to} \quad x_i^k > 0, \ \sum\nolimits_{k \in \mathcal{T}} \tau_i^k = 1 \end{aligned} \tag{10}$$

Next, we prove that there exists a game equilibrium in our model, as described in Theorem 1.

Theorem 1 *The existence and uniqueness of users' participation equilibrium, i.e., the Nash equilibrium of Stage II, can be*

$$det(\mathbf{H}_{k,k}) = \frac{\partial^2 U_i}{\partial(\tau_i^k)^2} \cdot \frac{\partial^2 U_i}{\partial(x_i^k)^2} - \left(\frac{\partial^2 U_i}{\partial \tau_i^k \partial x_i^l}\right)^2 \tag{15}$$

$$= 4b_i (B_k)^2 \cdot \frac{\tau_i^k |\Phi_{-i}^k|}{|\Phi_k|^4} \cdot \mathcal{X}_i^k - \frac{(B_k)^2 \cdot |\Phi_{-i}^k|^2}{(|\Phi_k|)^4} \left(A_i - 2b_i x_i^k\right)^2 + 2c \cdot \frac{B_k \cdot |\Phi_{-i}^k|}{(|\Phi_k|)^2} \left(A_i - 2b_i x_i^k\right) - c^2 \tag{16}$$

$$= \frac{(B_k)^2 |\Phi_{-i}^k|}{|\Phi_k|^4} \left[4b_i \tau_i^k \mathcal{X}_i^k - |\Phi_{-i}^k| \left(A_i - 2b_i x_i^k\right)^2 + 2c \cdot \frac{|\Phi_k|^2}{B_k} \left(A_i - 2b_i x_i^k\right) - \frac{c^2 \cdot |\Phi_k|^4}{(B_k)^2 |\Phi_{-i}^k|}\right] \tag{17}$$

$$= \frac{(B_k)^2 |\Phi_{-i}^k|}{|\Phi_k|^4} \left[4b_i \tau_i^k \left(A_i x_i^k - b_i {x_i^k}^2\right) - |\Phi_{-i}^k| \left(A_i^2 - 4A_i b_i x_i^k + 4{b_i}^2 {x_i^k}^2\right) + 2c \cdot \frac{|\Phi_k|^2}{B_k} \left(A_i - 2b_i x_i^k\right) - \frac{c^2 \cdot |\Phi_k|^4}{(B_k)^2 |\Phi_{-i}^k|}\right] \tag{18}$$

$$= \frac{(B_k)^2 |\Phi_{-i}^k|}{|\Phi_k|^4} \left[4b_i x_i^k \underbrace{(\tau_i^k - |\Phi_{-i}^k|)}_{<0} \underbrace{(A_i - b_i x_i^k)}_{>0} - |\Phi_{-i}^k| \cdot A_i^2 + 2c \cdot \frac{|\Phi_k|^2}{B_k} \underbrace{(A_i - 2b_i x_i^k)}_{<0} - \frac{c^2 \cdot |\Phi_k|^4}{(B_k)^2 |\Phi_{-i}^k|}\right] \leq 0. \tag{19}$$

guaranteed, if there exists $b_i x_i^k < A_i < 2b_i x_i^k \quad for\ \forall i \in \mathcal{N},\ where\ A_i = a_i + \sum_{j\in\mathcal{N}} g_{ij} x_j^k$.

Proof: The domain of the user's utility function is a multidimensional vector space, i.e., $\mathbb{R}^{2\times l} \to \mathbb{R}$. We use the Hessian matrix to verify the concave characteristic of Eq. (9). The Hessian matrix $\mathbf{H}_{s,t} : 2 \times 2$ is defined as:

$$\mathbf{H}_{s,t} = \begin{bmatrix} \frac{\partial^2 U_i}{\partial \tau_i^s \partial \tau_i^t} & \frac{\partial^2 U_i}{\partial \tau_i^s \partial x_i^t} \\ \frac{\partial^2 U_i}{\partial \tau_i^t \partial x_i^s} & \frac{\partial^2 U_i}{\partial x_i^s \partial x_i^t} \end{bmatrix} \tag{11}$$

Then, the Hessian matrix of user's utility function Eq. (9) is formulated as $\mathbf{H} = [\mathbf{H}_{s,t}] \in \mathbb{R}^{l\times l}$, i.e.,

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{1,1} & \mathbf{H}_{1,2} & \cdots & \mathbf{H}_{1,l} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{H}_{l,1} & \mathbf{H}_{l,2} & \cdots & \mathbf{H}_{l,l} \end{bmatrix} \tag{12}$$

We only need to prove $det(\mathbf{H}) < 0$ to draw a conclusion that the function Eq. (9) is a concave optimization problem and it has an optimal response in the user's subgame. It's obvious that $\mathbf{H}_{s,t} = \mathbf{O}$ for $s \neq t$. Thus, Eq. (12) equals to $\mathbf{H} = diag[\mathbf{H}_{1,1}, \mathbf{H}_{2,2}, \ldots, \mathbf{H}_{l,l}]$. We take the second order derivatives of Eq. (9) with respect to τ_i^k and x_i^k as follows:

$$\frac{\partial^2 U_i}{\partial(\tau_i^k)^2} = -2B_k \frac{|\Phi_{-i}^k|}{(|\Phi_k|)^3} \cdot \mathcal{X}_i^k, \quad \frac{\partial^2 U_i}{\partial(x_i^k)^2} = -2b_i \tau_i^k \frac{B_k}{|\Phi_k|}. \tag{13}$$

$$\begin{aligned} \frac{\partial^2 U_i}{\partial \tau_i^k \partial x_i^k} &= \frac{\partial^2 U_i}{\partial x_i^k \partial \tau_i^k} \\ &= \frac{B_k \cdot |\Phi_{-i}^k|}{(|\Phi_k|)^2} \Big(a_i - 2b_i x_i^k + \sum_{j\in\mathcal{N}} g_{ij} x_j^k\Big) - c. \end{aligned} \tag{14}$$

To simplify the notation, we denote $A_i = a_i + \sum_{j\in\mathcal{N}} g_{ij} x_j^k$ in the following equation. Thus, $det(\mathbf{H}_{k,k})$ can be formulated as Eq. (15) to Eq. (19). We can conclude that Eq. (19) < 0 with the constraint in Theorem 1, which indicates that Eq. (9) is a concave function and Theorem 1 holds. ■

Theorem 2 *Given any feasible pricing strategy $\mathcal{B}$ announced by the requester, the optimal participation level vector* x* *for all users in the Nash equilibrium satisfies:*

$$\mathbf{x}_i^{k^*} = \frac{1}{2b_i}(A_i - \frac{c}{V_k}), \tag{20}$$

$$\mathbf{k}^* = \text{argmax}_{k\in\mathcal{T}} (V_k \cdot \mathcal{X}_i^k - c\mathbf{x}_i^{k^*}). \tag{21}$$

Proof: Using Lagrange's multipliers λ_1, λ_2 for the constraints in Eq. (10), the problem is converted to the form:

$$\begin{aligned} L_i = \sum_{k\in\mathcal{T}} \tau_i^k \left[V_k\left(A_i x_i^k - b_i {x_i^k}^2\right) - c x_i^k\right] \\ -\lambda_0\Big(\sum_{k\in\mathcal{T}} \tau_i^k - 1\Big) + \sum_{k\in\mathcal{T}} \lambda_k x_i^k. \end{aligned}$$

and the complementary slackness conditions are

$$\frac{\partial L_i}{\partial x_i^k} = 0 \quad \text{for } \forall i \in \mathcal{N} \tag{22}$$

$$\lambda_0(\sum_{k\in\mathcal{T}} \tau_i^k - 1) = 0, \quad \lambda_k x_i^k = 0$$

$$\lambda_0, \lambda_k \geq 0, x_i^k > 0$$

Due to $x_i^k > 0$, we can obtain $\lambda_k = 0$ for $\forall k \in \mathcal{T}$. Thus, Eq. (22) can be converted to

$$\tau_i^k \left[V_k\left(A_i - 2b_i x_i^k\right) - c\right] = 0.$$

Since $\tau_i^k \geq 0$ and $\sum_{k\in\mathcal{T}} \tau_i^k = 1$, for any $\tau_i^k > 0$, we have

$$\left[\frac{B_k}{|\Phi_k|}\left(A_i - 2b_i x_i^k\right) - c\right] = 0,$$

$$\mathbf{x}_i^{k^*} = \frac{1}{2b_i}\left(A_i - \frac{c}{V_k}\right).$$

Theorem 2 holds. ■

From Theorem 2, users can adjust their participation strategies according to the requester's pricing strategies and obtain the maximum payoffs.

3.2 Stage I: Optimal Pricing Strategy for the Requester

The user's choice of sensing task depends on two aspects, one is the return on revenue, and another is the geographic location of interest. Therefore, the requester can manipulate the user's choice to a certain extent by adjusting the pricing strategy, so as to better achieve the task completion quality. Based on the Nash equilibrium of the participation level in the user's sub-game in Stage II, the leader of the Stackelberg game, i.e., the requester, can optimize its pricing strategy in Stage I to maximize its profit defined in Eq. (6).

Definition 3 *The pricing strategy $\mathcal{B}^*$ is the optimal pricing strategy if the following condition is satisfied:*

$$\Omega(\mathcal{B}^*, \vec{\beta}^*) \geq \Omega(\mathcal{B}', \vec{\beta}^*). \tag{23}$$

The revenue maximization problem for the requester can be formulated as follows:

Problem 2.

$$\begin{aligned} &\text{maximize} \quad \Omega\left(\mathcal{B},\vec{\beta}^*\right) \\ &\text{subject to} \quad \sum_{k\in\mathcal{T}}\sum_{i\in\mathcal{N}} V_k\cdot\mathcal{X}_i^k \le \Psi,\ \sum_{i\in\Phi_k} x_i^k \ge q_k,\ \forall k\in\mathcal{T} \end{aligned} \tag{24}$$

Theorem 3 *There exist an optimal pricing strategy for the requester in Nash equilibrium.*

Proof: By substituting $\mathcal{X}_i^k$ and Eq. (23) into Eq. (6), we have

$$\begin{aligned} \Omega &= \sum_{k\in\mathcal{T}}\sum_{i\in\Phi_k}\left[h_i x_i^k - V_k\left(A_i x_i^k - b_i {x_i^k}^2\right)\right] \\ &= \sum_{k\in\mathcal{T}}\sum_{i\in\Phi_k} x_i^k\left(h_i - V_k\cdot A_i + V_k\cdot b_i x_i^k\right) \\ &= \sum_{k\in\mathcal{T}}\sum_{i\in\Phi_k}\frac{1}{2b_i}\left(A_i - \frac{c}{V_k}\right)\left(h_i - V_k A_i + \frac{1}{2}\left(A_i V_k - c\right)\right) \\ &= \sum_{k\in\mathcal{T}}\sum_{i\in\Phi_k}\frac{1}{2b_i}\left(A_i - \frac{c}{V_k}\right)\left(h_i - \frac{c}{2} - \frac{A_i}{2}V_k\right). \end{aligned}$$

The strategy sets are closed and bounded. We also use the Hessian matrix to verify the concave of Eq. (25). We take the first and second derivative of the function $\Omega(\mathcal{B})$ as follows:

$$\begin{aligned} \frac{\partial\Omega}{\partial B_k} &= \frac{\partial\Omega}{\partial V_k}\cdot\frac{\partial V_k}{\partial B_k} \\ &= \frac{1}{|\Phi_k|}\sum_{i\in\Phi_k}\frac{1}{2b_i}\left[\frac{c}{{V_k}^2}\left(h_i - \frac{c}{2} - \frac{A_i}{2}V_k\right) - \frac{A_i}{2}\left(A_i - \frac{c}{V_k}\right)\right] \end{aligned} \tag{25}$$

$$\begin{aligned} \frac{\partial^2\Omega}{\partial\left(B_k\right)^2} &= -\frac{1}{|\Phi_k|^2}\sum_{i\in\Phi_k}\frac{1}{2b_i}\left[\frac{2c}{{V_k}^3}\left(h_i - \frac{c}{2} - \frac{A_i}{2}V_k\right) + \frac{A_i c}{{V_k}^2}\right] \\ &= -\frac{c}{|\Phi_k|^2 {V_k}^3}\sum\nolimits_{i\in\Phi_k}\frac{1}{b_i}\left(h_i - \frac{c}{2}\right). \\ \frac{\partial^2\Omega}{\partial B_k \partial B_l} &= 0. \end{aligned}$$

Therefore, under the condition $h_i - \frac{c}{2} \ge 0$, we have Hessian matrix $H(\Omega) \ge 0$, which means that the utility function of the requester $\Omega(\mathcal{B})$ is a concave function and thus exists an optimal pricing strategy for the requester. We take partial derivative of the objective function $\frac{\partial\Omega}{\partial B_k} = 0$ in Eq. (25), and we obtain ${B_k}^* = |\Phi_k|\frac{\sqrt{2\bar{h}c - c^2}}{\bar{A}}$, where $\bar{h} = \frac{\sum_{i\in\Phi_k} h_i}{|\Phi_k|}$ and $\bar{A} = \frac{\sum_{i\in\Phi_k} A_i}{|\Phi_k|}$. Since ${B_k}^*$ is positively related to $|\Phi_k|$, the requester can control the number of participants in each sensing task by adjusting the pricing strategy to achieve the desired data sensing task quality q_k. ■

We take advantage of a classic distributed algorithm called Two-Stage Asynchronous Best Response (Algorithm 1) to find the approximate Nash equilibrium point in this game, where users iteratively update their strategies based on their best response function in Eq. (20). As mentioned above, the characteristic attributes of each user, i.e., a_i and b_i, are well-known by other users and requester, so they can iteratively speculate other participations' optimal responses. In Algorithm 1, the inputs include the random feasible pricing strategy of the requester, user's random participation levels, and the threshold values (ϵ_1 and ϵ_2). The game starts in stage II. After receiving the initial pricing strategy of the requester, each user predicts other participants' optimal participation levels under the given pricing strategy, and then updates his strategy for each sensing task according to the results of the previous iteration round (Line 5-9). If the gap between the strategy results in two rounds, which is measured by Frobenius norms, is less than the threshold ϵ_1, we consider the users' sub-game in stage II to achieve the approximate Nash equilibrium. Next, the requester checks whether the quality of the received data sensing service meets the required boundary value. Similarly, suppose the difference between the requester's utility value obtained in this round and the previous round is less than the threshold ϵ_2. In that case, the Stackelberg game between requester and users can be regarded as converged to a Stackelberg equilibrium point. We refer to the above operation process as iterative convergence, where participants' strategies are adjusted by repeated iterations to converge to a certain range. Note that the proposed algorithm's convergence speed depends on the precision threshold value. The smaller the threshold, the more iterations are required before convergence. In Algorithm 1, the time complexity of each iteration round for the users' subgame phase is bounded by $O\left(l * n^2\right)$.

Algorithm 1: Two-Stage Asynchronous Best Response Algorithm

Input: Any feasible pricing vector of the requester, $\mathcal{B} = \{B_1, B_2, \ldots, B_l\}$, and the threshold ϵ_1, ϵ_2

```
1  for iteration s do
2      Storing the pricing vector of last iteration B^[s-1];
       Stage II:
3      Initializing iteration index t = 1 for mobile users;
4      while ||x_i^[t] - x_i^[t-1]||_1 > ε_1 do
5          for each user i do
6              for each sensing task ∀k ∈ T do
7                  Predicting the optimal participation
                   level vector of other users;
8                  x_i^k[t] = 1/(2b_i) ( a_i + Σ_{j∈N} g_ij x_j^k[t-1] − c/(V_k^[s-1]) );
9              Deciding which task to execute in Eq. (21);
10         t ← t + 1;
11     Sending x* to the requester;
12     Stage I:
13     Computing the requester's utility based on Eq.
       (6);
14     if Σ_{i∈Φ_k} x_i^k ≥ q_k, ∀k∈T and ||Ω^[s] − Ω^[s-1]||_1 < ε_2
       then
15         Returning B and x;
16     else
17         Adjusting B and sending it to all mobile
           users;
18     s ← s + 1;
```

4 Privacy Preservation in SBS-MC

In section III, we discussed the Stackelberg game between users and the requester. In our mechanism, The requester can obtain data by offering some payment, which can be considered as a buyer. Users collect the crowdsensing data and provide it to the requester for payment, which can be considered as sellers. The interaction between the requester

RequsterInitiate ($\mathcal{T}, \mathcal{Q}, \mathcal{B}, pk$) payable:
1. Require $msg.value \geq \$threshold$
2. Set $requester = msg.sender$ and store $\mathcal{T}, \mathcal{Q}, \mathcal{B}, pk$.
3. Trigger $Notify$ event to inform the registered users.

DataSubmit ($\beta_i, DataAddress$):
1. Require $\beta_i, DataAddress \neq null$
2. Set $UserMap(msg.sender) = (\beta_i)$.
3. Add $DataAddress\ to\ AddressList$.

Transaction ( ):
1. Require $len(AddressList) == |\mathcal{N}|$.
2. Send $DataList$ to requester.
3. for $user_i$ in $\mathcal{N}$:
   Count payment $\mathcal{P}(user_i)$.
   Transfer $\$budget$ to $msg.sender$.

Refund ( ):
1. Require $msg.sender = requester$.
2. Compute the remain budget:
   $\$budget = \$budget - \sum_{i \in \mathcal{N}} \mathcal{P}(user_i)$
3. Transfer $\$budget$ to $msg.sender$.

Fig. 2. Main Functions in Smart Contract.

and users can be regarded as a data transaction. To prevent users from maliciously obtaining the privacy of others or providing false data during the gaming process, in this section, we deploy the crowdsensing data transaction in a smart contract on Ethereum to protect the users' location and data privacy. In addition, Ethereum can ensure that the crowdsensing data transaction is carried out automatically and effectively, which is called SBS-MC.

4.1 Ethereum and Smart Contracts

Blockchain, a newly-emerging decentralized distributed storage technology, is often used to solve the problems of privacy protection and transaction fairness in data transactions [17]. Ethereum is an open-source public blockchain platform with smart contract functions [18]. It provides a decentralized Ethereum virtual machine to process peer-to-peer contracts through its dedicated cryptocurrency, i.e., Ether. There are the following concepts in Ethereum.

1) **Ethereum Accounts:** In Ethereum, each account is uniquely identified by a 20-byte address, the transfer of value and information between accounts can change the state of Ethereum.
2) **Ether and wei:** "**Ether**" and "**wei**" are the main internal digital currency of Ethereum, and are used to pay transaction fees. Here, 1 **ether** = 10^{18} **wei**.
3) **Message and Transaction:** Transaction is a signed package of data sent from an externally owned account that contains the recipient of the message, a signature identifying the sender, the amount of ether and the data to send, and two values: START GAS and GAS PRICE.
4) **Smart Contracts:** One of the core technologies of blockchain is a computer protocol that digitally facilitates, verifies, or executes the negotiation or performance of a contract digitally. Smart contracts allow for trusted execution without a third party.

TABLE 2
Description of notations for smart contract.

Variable	Description
ether, wei	the virtual currency units on blockchain.
msg	a transaction on a smart contract.
$msg.sender$	the launcher of msg.
$msg.value$	the amount of ether sent in msg.
$payable$	the specific keyword in the smart contract.
$\$threshold$	the minimum entry fee to participate.
$\$budget$	the prepayments of the requester.
$userMap$	dictionary-type storage to record users' strategy.
$AddressList$	a list for storing addresses of encrypted data.

To protect the user's location and data privacy and to prevent malicious competition caused by game strategy leakage, we transform this crowdsensing data transaction process into the smart contract in the form of program. The smart contract acts as the broker of data transaction that separates the requester and users from each other, thereby shielding users' sensitive information from the process of data transmission.

4.2 Smart Contrast Protocol for SBS-MC Framework

In this part, we introduce the specific process of the SBC-MC system in detail. The interactions among the requester, mobile users, and the smart contract are presented in Protocol 1 and also demonstrated in Fig. 2. For ease of reference, we list the major notations of the smart contract in Table II.

Phase 1: Initialization. Consider a data transaction scenario where a data requester wants to collect sensed data from some PoIs through the SBS-MC framework. The requester first creates a pair of public and private keys using homomorphic encryption. Then, he starts the transaction by invoking the smart contract and transferring his public key pk and his budget. Meanwhile, the requester demonstrates the details of his requirement, including the quality requirement $\mathcal{Q}$, sensing task list $\mathcal{T}$ and the pricing vector $\mathcal{B}$. This process is presented programmatically in function $ConsumerInitiate()$. The contract will check whether the budget offered by the requester ($msg.value$) is no less than $\$threshold$, i.e., the margin minimum entry fee to participate in the data transaction. Then, the contract records the parameter information of the sender as notation $requester$ and further triggers the $Notify$ event to awake the recruited users for data collection.

Phase 2: Data collection. After receiving the information, each mobile user will decide their strategy and move to the corresponding positions to start data sensing. After completing the data collection, users will encrypt their sensed data using the requester's public key and upload it to the blockchain to protect their privacy. Next, each user invokes the function $DataSubmit$ to deliver the data address to contract. The contract uses the dictionary-type storage $UserMap$ to record the strategy of each user to calculate his payment later and adds the data address to budget of $addressList$.

Phase 3: Transaction. If all users have submitted the data address, the smart contract sends $AddressList$ to the requester. The requester downloads the encrypted data from the blockchain and decrypts them with his private key. And

Protocol 1: Secure Blockchain-Assisted Game-Based Task Decision Protocol

Input: A Smart Contract: $\mathcal{S}$, the Requester: (pk), and Mobile Users: $Dataaddress$

1. The requester creates a pair of public and private keys with homomorphic encryption.
2. The requester sends the job description $\mathcal{T}$,$\mathcal{Q}$, $\mathcal{B}$ and public key pk to the smart contract to start the data transaction by invoking $RequesterInitiate()$.
3. After receiving the event notification from the contract, the participating users begin to execute the tasks and encrypt the data with pk. Then, users store the encrypted data on blockchain and send $DataAddress$ to the smart contract by invoking $DataSubmit$.
4. The smart contract checks whether all users have submitted the data address, and then delivers $AddressList$ to requester. The requester downloads the encrypted data from data address on blockchian and decrypts the data with his private key.
5. The contract calculates the payment of users according to their strategy and transfers the payment to them.
6. The requester invokes the $Refund()$ to terminate the transaction and get the balance from the smart contract.

then, the contract calculates each user's payment according to his strategy, which was stored in $UserMap$ previously.

Phase 4: Final Stage. After the transaction, the smart contract will refund the balance to the requester if there is any remaining budget and terminate this data sensing transaction.

5 Performance Evaluation

In this section, we evaluate the performance of the proposed solutions in the following two parts. First, we conduct a series of simulations to evaluate Algorithm 1 on the Stackelberg game and investigate the impacts of different parameters. Second, we verify the feasibility of the SBS-MC system by developing the smart contract program and deploying it on the blockchain to evaluate the gas consumption and running time. We conduct the simulations on a computer with Inter(R) Core(TM) i7-10700 CPU @2.90GHz 2.90GHz and 16.0 GB RAM under a Windows platform. The smart contract is deployed to a local simulated network TestRPC using Ethereum development tool Remix. The simulated network is much like the real Ethereum environment, irrespective of the time-consuming mining process and the complex network circumstances in Ethereum.

5.1 Evaluation on Stackelberg game of SBS-MC

Consider a Stackelberg game of one requester and N users in this SBS-MC framework. The intrinsic parameters of users, i.e., a_i, b_i, h_i, follow the normal distribution $\mathcal{N}(\mu_a, 1)$, $\mathcal{N}(\mu_b, 1)$, $\mathcal{N}(\mu_h, 1)$. In addition, the social tie g_{ij} between any two users i and j follows a truncated normal distribution $\mathcal{N}(\mu_g, 1)$. We set the intrinsic parameters of users as default value, i.e., $\mu_a = 2$, $\mu_b = 3$, $\mu_h = 200$, and $c = 15$. The number of tasks is set as $l = 3$. The average pricing for each task, denoted as B_{avg}, is generated from the range $[600, 950]$ and we set $B_{avg} = 600$ in default. The influence factor between user i and j follows the normal distribution $\mathcal{N}(\mu_g, 1)$. We set $\mu_g = 0.5$ in default and it varies from 0.2 to 0.8 in Fig. 5.

We evaluate the impact of different pricing of sensing tasks on participants' utility with different numbers of users. As illustrated in Fig. 3 and Fig. 4, the bottom axis represents the total budget of all sensing tasks, i.e., $B = \sum_{k\in\mathcal{T}} B_k$. When the budget increases, users obtain higher revenue, but the requester has the opposite effect. The reason is that the value of unit sensing data, i.e., V_k, will increase if the requester raises the price of each sensing task. Thus, each mobile user earns higher revenue accordingly. However, for the requester, the higher price per sensing task means increased spending for pursuing data. Still, there is no significant increase in mobile users' engagement, leading to the requester's decreased utility. Fig. 3 and Fig. 4 also show that with the increase in the number of users, both requester and users obtain higher revenue. Owing to the information corroboration via the underlying social network, one user's performance will be positively affected by other participants. The more participants indicate, the more social interactions among users. Thus the collected data will be more comprehensive and have better quality. Meanwhile, the utility of the requester will increase. On the other hand, for mobile users, the increased number of competitors leads to the lower unit data value as Eq. (3), so the revenue of each user decreases accordingly.

Fig. 5 shows the decision-making process of a user's participation in different tasks over the iterations, corresponding to Lines 4 to 10 in Algorithm 1. Initially, we randomly set different participation levels for each task. With the increase of iteration rounds, the user's participation level in each task will be adjusted according to the equation in Line 8. When the iteration rounds exceed 25, the user's participation level in each task tends to be stable. The user will finally choose a task with the highest income among multiple tasks as the optimal response.

Fig. 6 depicts the impact of the average value of social network effects on two entities of this network, i.e., the requester and mobile users. We observe that as the social network effects become stronger, the users' total utilities and the requester's revenue also increase. Since the strength of the social tie is stronger, the additional benefits obtained from social network effects are greater. The users are motivated by their social neighbors to have higher participation levels, and the total utilities of the two parties are both improved.

We compare our predicted and actual participants numbers for each sensing task in Fig. 7. According to the best response pricing strategy of the requester in section 2, we predict that the number of participants in each task is proportional to the price of the input. We set different prices for each task and observed the actual number of participants. The results show that our predicted value is consistent with the actual value. We also reveal the benefits of both requester and users under the different number of tasks in Fig. 8. We set the total number of users as $N = 50$ and the contribution of unit sensing time to the task as $h = 100$. The number

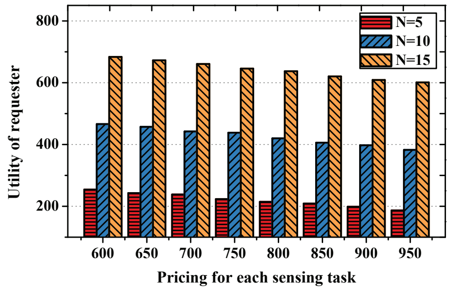

Fig. 3. Requester's Utility vs. Budget.

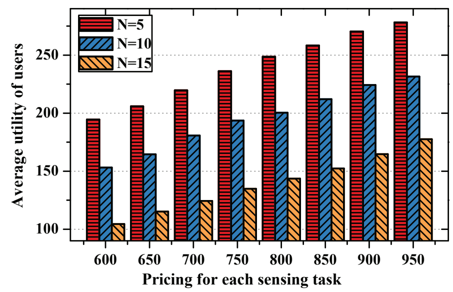

Fig. 4. Users' Utility vs. Budget.

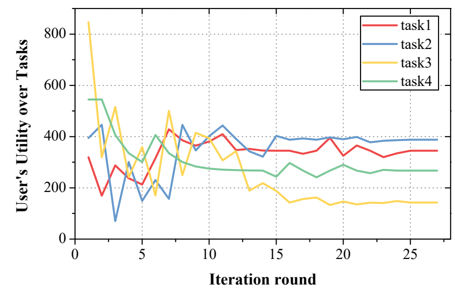

Fig. 5. Users' Utility over Tasks.

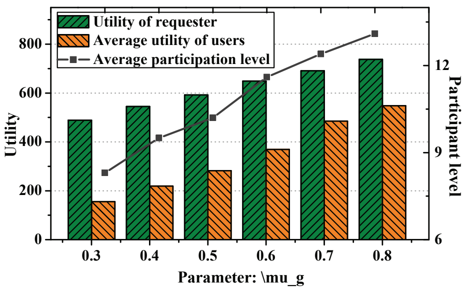

Fig. 6. Utility vs. Social Effects (μ_g).

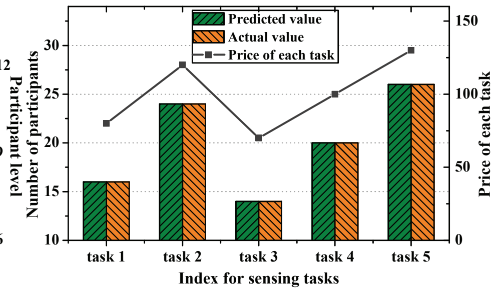

Fig. 7. Price of tasks vs. Number of participants.

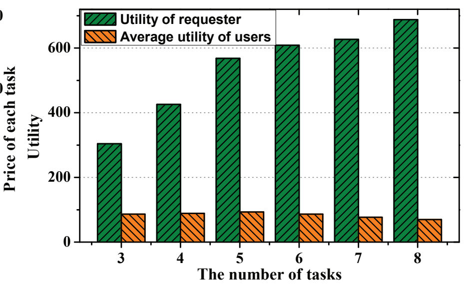

Fig. 8. Utility vs. Number of tasks.

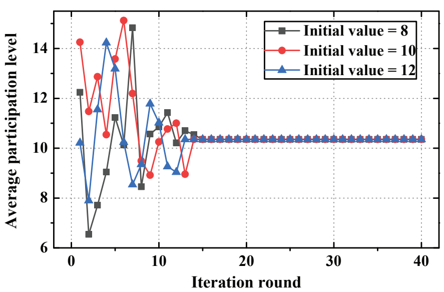

Fig. 9. Iteration results.

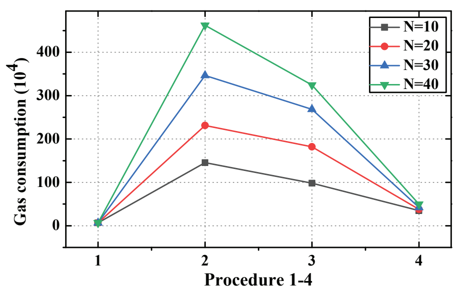

Fig. 10. Gas consumption of each procedure.

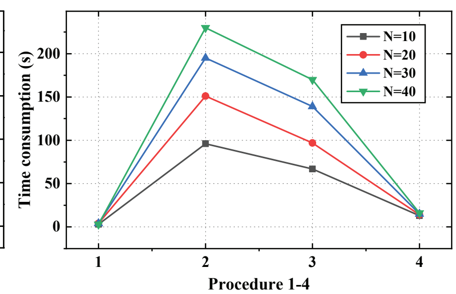

Fig. 11. Time consumption.

of tasks varies from 3 to 8. The increase in the number of tasks will lead to a rise in the utility of the requester. On the contrary, the average utility of users appeared to have a slight downward trend. That's because more tasks mean that in the case of the same number of users, the distribution of users is more scattered, reducing the effect of collaboration. Hence, the user needs to consume more costs to perform a task, and then the income will decrease accordingly. However, at the same time, the decrease in the number of users performing a specific task will also increase the information value of the task, thereby resulting in a certain degree of increase in revenue. That's why users' earnings have generally stabilized but slightly declined.

Furthermore, we verified the convergence of Algorithm 1 in Fig. 9. With the consistent value of other parameters, we set different initial strategies of users as input of Algorithm 1. After about 10 to 15 iterations, the user's result finally stabilizes at the same value, indicating that our proposed algorithm can achieve the Nash equilibrium of users' participation sub-game.

5.2 Evaluation of Smart Contract on Simulated Network

In addition, we evaluate the performance of the SBS-MC system through extensive simulations on the blockchain. The smart contract coordinates the requester and users to realize the data initialization, transaction, data committing, and refunding phases based on the four main functions as illustrated in Fig. 2. The smart contract is deployed to a local simulated network TestRPC using Ethereum development tool Remix [19]. We use two special metrics: gas consumption and time consumption, to evaluate the performance of the smart contract on the simulated network. We use Procedures 1-4 in Fig. 10 and Fig. 11 to indicate the total gas consumption and time consumption after all invocations of each function, respectively. For example, in Fig. 10, the total gas consumed by Procedure 2 is the accumulated gas consumed by N mobile users who invoke the function of $DataCommit$.

Each computational step in the smart contract will be charged some gas fee as a reward for miners packing blocks on the blockchain. The more complicated the procedure is, the more gas and time it will consume. The operations to create and write storage data are relatively expensive. As shown in Fig. 10 and Fig. 11, Procedure 2 and 3 consume higher gas fees and time costs. This is because Procedure 2 needs to store sensing data on blockchain, and Procedure 3 needs to calculate the payment of each user and transfer the payment to them.

6 Related Work

In this section, we mainly review the related work from the following three aspects.

6.1 Task Allocation and Incentive Mechanism in MC

To jointly promote the participation of users and facilitate the reasonable allocation of tasks in sensing services/applications, there have been a number of studies devising the task allocation and incentive mechanisms in mobile crowdsensing [20–25]. Among them, [26] proposed a reward-based collaboration scheme. The requester offers the total reward to entice users for data acquisition and allocates the sensing tasks by setting different rewards. [2] focused on incentivizing user participation and assigning location-dependent sensing tasks with a capacity budget. On the other hand, game theory is widely used to solve crowdsensing problems. [27] formulated a Stackelberg game to model the interactions between the requester and mobile users, where the requester determines the reward and the users decide on the working time. [28] adopted the Stackelberg game to design a threshold revenue model for mobile users. Meanwhile, auction is also an excellent solution for designing an incentive mechanism for crowdsensing. For example, [29] proposed the auction-based incentive mechanism for user-centric mobile crowdsensing system by considering the quality of sensing data. However, only a few work [9, 16, 30] has studied the incentive mechanism for crowdsensing and exploited social network effects in combination. Among them, [16] modeled the rewarding and participating for MC system as a two-stage single-leader multiple-follower game, in which the rewarding design took the underlying social network effects into account. [30] investigated the behaviors of mobile users under global network effects, which is not appropriate for the structure of an underlying social domain.

6.2 Social Effect in Crowdsensing

Social effects refer to the case where a participant's sensing strategy can be directly influenced by others which frequently exists in densely connected social relationships. Traditionally, social effects refer to the phenomenon that public goods or services are more valuable if more users adopt them. In the crowdsensing framework, mobile users are more willing to participate if the number of their social friends performing the sensing tasks is greater. Adopting the network effects reasonably and effectively will be critical criteria for promoting crowdsensing quality. There have been many studies focusing on this issue. [16] leveraged the underlying social network effects to attract participants to the crowdsensing platform. [31] considered a reward mechanism design for the service provider to achieve diversity in the collected data by exploiting the users' social relationships. [32] considered a non-cooperative vehicular crowdsensing that combines the social network effect with incentive mechanism design. Vehicles are incentivized by dynamically priced tasks and social network effects aiming at maximizing the overall utility of vehicle drivers. [33] considered network effects as a contributing factor to intrinsic rewards and studied the impact of participation level with social network effect in an MCS system. [34] proposed a dynamic pricing scheme that exploits the network effects in the mobile users' behaviors that boost the social data demand. The mobile network operator sequentially and repeatedly offers a certain price in multiple time periods. Compared with the static pricing scheme, the dynamic pricing scheme can help the operator gain more revenue.

6.3 Blockchain-based Privacy Preservation in MC

Privacy preservation is also a significant issue in mobile crowdsensing [35–37]. Due to anonymity, non-tampering, traceability, etc., blockchain is widely used in information security [12, 38, 39]. Mobile users can access the blockchain through a pair of key generated by asymmetric encryption. There are some attempts to apply blockchain technology to mobile crowdsensing. [40] proposed a blockchain-based crowdsensing scheme in industrial systems, where the miners are exploited to verify the sensory data. However, this work ignores the dynamic cooperation among participants. [41] proposed a practical decentralized MC system based on a distributed auction process and the blockchain system. [6] replaced the data transaction broker with blockchain to guarantee the trustworthiness of the data transaction. [38] presented a trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing.

Unlike the current work, we study the interactions between the requester and mobile users for the blockchain-assisted socially-aware crowdsensing framework, where the blockchain is used to protect the users' data and location privacy and also can protect the requester's identity information. Due to the information corroboration of social effects and the information value for the rarity and unsubstitutability of sensed data, each user has to face a tradeoff between gather and scatter. We model this problem as a two-stage Stackelberg game. Since the game model in this paper involves the multi-dimension vector space problem, we extend the Hessian matrix method to the multi-dimension case to analyze it.

7 Conclusion

In this paper, we apply a two-stage Stackelberg game to design a crowdsensing mechanism by considering the effect of social networks on mobile users' participant level. We also study the information value of sensing data when mobile users gather or scatter in different points, which is always overlooked in the previous research. Further, we propose a secure blockchain-based socially-aware crowdsensing framework by introducing the smart contract of Ethereum to ensure that the data transaction is executed automatically and fairly. We implement a prototype to describe the data transaction process and deploy it to an official Ethereum test network. Experimental results on Ethereum also verify our proposed protocol's practicability and privacy-preserving performance. In the future, we will continue our research of user decisions in the context of multiple social networks. In addition, we will further improve the mechanism to avoid malicious competition and manipulation of social networks by users.

References

[1] K. Yang, K. Zhang, J. Ren, and X. Shen, "Security and privacy in mobile crowdsourcing networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 75–81, 2015.

[2] P. Zhou, Y. Zheng, and M. Li, "How long to wait? predicting bus arrival time with mobile phone based participatory sensing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 6, pp. 1228–1241, 2014.
[3] T. Jung, X.-Y. Li, W. Huang, J. Qian, L. Chen, J. Han, J. Hou, and C. Su, "Accounttrade: Accountable protocols for big data trading against dishonest consumers," in *IEEE INFOCOM*, 2017.
[4] E. Wang, M. Zhang, X. Cheng, Y. Yang, W. Liu, H. Yu, L. Wang, and J. Zhang, "Deep learning-enabled sparse industrial crowdsensing and prediction," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 6170–6181, 2021.
[5] Y. Zhan, C. H. Liu, Y. Zhao, J. Zhang, and J. Tang, "Free market of multi-leader multi-follower mobile crowdsensing: An incentive mechanism design by deep reinforcement learning," *IEEE Transactions on Mobile Computing*, vol. 19, no. 10, pp. 2316–2329, 2020.
[6] B. An, M. Xiao, A. Liu, Y. Xu, X. Zhang, and Q. Li, "Secure crowdsensed data trading based on blockchain," *IEEE Transactions on Mobile Computing*, vol. 22, no. 3, pp. 1763–1778, 2023.
[7] C.-L. Hu, K.-Y. Lin, and C. K. Chang, "Incentive mechanism for mobile crowdsensing with two-stage stackelberg game," *IEEE Transactions on Services Computing*, pp. 1–14, 2022.
[8] G. Gao, M. Xiao, J. Wu, L. Huang, and C. Hu, "Truthful incentive mechanism for nondeterministic crowdsensing with vehicles," *IEEE Transactions on Mobile Computing*, vol. 17, no. 12, pp. 2982–2997, 2018.
[9] W. Tan, L. Zhao, B. Li, L. D. Xu, and Y. Yang, "Multiple cooperative task allocation in group-oriented social mobile crowdsensing," *IEEE Transactions on Services Computing*, vol. 15, no. 6, pp. 3387–3401, 2022.
[10] W. Liu, Y. Yang, E. Wang, and J. Wu, "Dynamic user recruitment with truthful pricing for mobile crowdsensing," in *IEEE INFOCOM*, 2020.
[11] W. Jin, M. Xiao, M. Li, and L. Guo, "If you do not care about it, sell it: Trading location privacy in mobile crowd sensing," in *IEEE INFOCOM*, 2019.
[12] Z. Ning, S. Sun, X. Wang, L. Guo, S. Guo, X. Hu, B. Hu, and R. Kwok, "Blockchain-enabled intelligent transportation systems: A distributed crowdsensing framework," *IEEE Transactions on Mobile Computing*, vol. 21, no. 12, pp. 4201–4217, 2022.
[13] X. Pang, Z. Wang, J. Li, R. Zhou, J. Ren, and Z. Li, "Towards online privacy-preserving computation offloading in mobile edge computing," in *IEEE INFOCOM*, 2022.
[14] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *IEEE Symposium on Security and Privacy*, 2016.
[15] O. Candogan, K. Bimpikis, and A. Ozdaglar, "Optimal pricing in networks with externalities," *Operations Research*, vol. 60, no. 4, pp. 883–905, 2012.
[16] J. Nie, J. Luo, Z. Xiong, D. Niyato, and P. Wang, "A stackelberg game approach toward socially-aware incentive mechanisms for mobile crowdsensing," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 724–738, 2019.
[17] S. Nakamoto, "A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf 2008.
[18] V. Buterin, "A next-generation smart contract and decentralized application platform," *White paper*, 2014.
[19] M. Knobel, "Remix, literacy and creativity: An analytic review of the research literature," *Eesti Haridusteaduste Ajakiri. Estonian Journal of Education*, vol. 5, no. 2, pp. 31–53, 2017.
[20] Q. Xu and R. Zheng, "When data acquisition meets data analytics: A distributed active learning framework for optimal budgeted mobile crowdsensing," in *IEEE INFOCOM*, 2017.
[21] X. Wang, R. Jia, X. Tian, and X. Gan, "Dynamic task assignment in crowdsensing with location awareness and location diversity," in *IEEE INFOCOM*, 2018.
[22] E. Wang, Y. Yang, J. Wu, W. Liu, and X. Wang, "An efficient prediction-based user recruitment for mobile crowdsensing," *IEEE Transactions on Mobile Computing*, vol. 17, no. 1, pp. 16–28, 2018.
[23] Y. Xu, M. Xiao, J. Wu, S. Zhang, and G. Gao, "Incentive mechanism for spatial crowdsourcing with unknown social-aware workers: A three-stage stackelberg game approach," *IEEE Transactions on Mobile Computing*, 2022.
[24] H. Zhou, T. Wu, H. Zhang, and J. Wu, "Incentive-driven deep reinforcement learning for content caching and d2d offloading," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 8, pp. 2445–2460, 2021.
[25] H. Zhou, X. Chen, S. He, J. Chen, and J. Wu, "Draim: A novel delay-constraint and reverse auction-based incentive mechanism for wifi offloading," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 4, pp. 711–722, 2020.
[26] R. Zhou, Z. Li, and C. Wu, "A truthful online mechanism for location-aware tasks in mobile crowd sensing," *IEEE Transactions on Mobile Computing*, vol. 17, no. 8, pp. 1737–1749, 2018.
[27] T. Luo, S. S. Kanhere, J. Huang, S. K. Das, and F. Wu, "Sustainable incentives for mobile crowdsensing: Auctions, lotteries, and trust and reputation systems," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 68–74, 2017.
[28] L. Duan, T. Kubo, K. Sugiyama, J. Huang, T. Hasegawa, and J. Walrand, "Motivating smartphone collaboration in data acquisition and distributed computing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2320–2333, 2014.
[29] D. Yang, G. Xue, X. Fang, and J. Tang, "Incentive mechanisms for crowdsensing: Crowdsourcing with smartphones," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1732–1744, 2016.
[30] Y. Chen, B. Li, and Q. Zhang, "Incentivizing crowdsourcing systems with network effects," in *IEEE INFOCOM*, 2016.
[31] M. H. Cheung, F. Hou, and J. Huang, "Make a difference: Diversity-driven social mobile crowdsensing," in *IEEE INFOCOM*, 2017.
[32] Y. Zhao and C. H. Liu, "Social-aware incentive mechanism for vehicular crowdsensing by deep reinforcement learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2314–2325, 2021.
[33] Y. Chen, B. Li, and Q. Zhang, "Incentivizing crowdsourcing systems with network effects," in *IEEE INFOCOM*, 2016.
[34] Z. Xiong, D. Niyato, P. Wang, Z. Han, and Y. Zhang, "Dynamic pricing for revenue maximization in mobile social data market with network effects," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1722–1737, 2020.
[35] X. Zhang, R. Lu, J. Shao, F. Wang, H. Zhu, and A. A. Ghorbani, "Fedsky: An efficient and privacy-preserving scheme for federated mobile crowdsensing," *IEEE Internet of Things Journal*, vol. 9, no. 7, pp. 5344–5356, 2022.
[36] J. Shu, X. Jia, K. Yang, and H. Wang, "Privacy-preserving task recommendation services for crowdsourcing," *IEEE Transactions on Services Computing*, vol. 14, no. 1, pp. 235–247, 2021.
[37] J. Shu, K. Yang, X. Jia, X. Liu, C. Wang, and R. H. Deng, "Proxy-free privacy-preserving task matching with efficient revocation in crowdsourcing," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 1, pp. 117–130, 2021.
[38] S. Gao, X. Chen, J. Zhu, X. Dong, and J. Ma, "Trustworker:

A trustworthy and privacy-preserving worker selection scheme for blockchain-based crowdsensing," *IEEE Transactions on Services Computing*, vol. 15, no. 6, pp. 3577–3590, 2022.

[39] Q. Wang and R. Li, "A weak consensus algorithm and its application to high-performance blockchain," in *IEEE INFOCOM*, 2021.

[40] J. Huang, L. Kong, H.-N. Dai, W. Ding, L. Cheng, G. Chen, X. Jin, and P. Zeng, "Blockchain-based mobile crowd sensing in industrial systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6553–6563, 2020.

[41] Z. Feng and J. Chen, "Blockchain based mobile crowd sensing for reliable data sharing in iot systems," in *IFIP Networking Conference*, 2021.

Sijie Huang received the B.S. degree from the School of Computer Science and Technology at Xidian University, Xi'an, China, in 2018. She is currently pursuing the M.S. degree on electronic information with the School of Computer Science and Technology, Soochow University, Soochow, China. Her research interests include blockchain, mobile-edge computing, crowdsourcing and incentive mechanism.

Guoju Gao is an assistant professor in the School of Computer Science and Technology at the Soochow University. He received his Ph.D. degree in computer science and technology with the School of Computer Science and Technology, University of Science and Technology of China, Hefei, China. He visited Temple University, USA, from Jan. 2019 to Jan. 2020. His research interests include game theory, privacy preservation, and traffic measurement. He has published 40 articles in referred journals and conferences, including IEEE TMC, ToN, TPDS, TSC, INFOCOM, etc.

He Huang is currently a professor in the School of Computer Science and Technology at Soochow University, P. R. China. He received his Ph.D. degree in School of Computer Science and Technology from University of Science and Technology of China (USTC), China, in 2011. From 2019 to 2020, he was a Visiting Research Scholar with Florida University, Gainesville, USA. He has authored over 100 papers in related international conference proceedings and journals. His current research interests include traffic measurement, computer networks, and algorithmic game theory. Dr. Huang is a Member of both IEEE and the Association for Computing Machinery (ACM). He received the best paper awards from Bigcom 2016, IEEE MSN 2018, and Bigcom 2018. He has served as the Technical Program Committee Member of several conferences, including IEEE INFOCOM, IEEE MASS, IEEE ICC, and IEEE Globecom.

Yu-E Sun is a professor of School of Rail Transportation, Soochow University, P.R. China. She received her Ph.D. degree in Shenyang Institute of Computing Technology from Chinese Academy of Science. From 2019 to 2020, she was a Postdoc Research Scholar with Florida University, Gainesville, USA. She has authored over 80 papers in related international conference proceedings and journals. Her current research interests span traffic measurement, privacy preserving, algorithm design and analysis for wireless networks. She is a Member of both IEEE and ACM. She received the best paper awards from Bigcom 2016, IEEE MSN 2018, and Bigcom 2018. She has served as the Technical Program Committee Co-Chairs of ACM MSCC-MobiHoc 2016.

Yang Du is currently a postdoctoral fellow in Soochow University. He received his B.E. degree from the Soochow University in 2015 and Ph.D. degree from University of Science and Technology of China in 2020. His research interests include network traffic measurement, mobile crowdsensing, and truth discovery.

Mingjun Xiao is a professor in the School of Computer Science and Technology at the University of Science and Technology of China (USTC). He received his Ph.D. from USTC in 2004. His research interests include crowdsourcing, mobile social networks, mobile cloud computing, blockchain, data security and privacy. He has published more over 80 papers in referred journals and conferences, including TMC, TC, TPDS, TKDE, TSC, INFOCOM, ICNP, etc. He served as the TPC member of INFOCOM'20, DASFAA'20, INFOCOM'19, ICDCS'19, DASFAA'19, etc. He is on the reviewer board of several top journals such as TMC, TON, TPDS, TSC, TVT, TCC, etc.

Jie Wu is the Director of the Center for Networked Computing and Laura H. Carnell professor at Temple University. He also serves as the Director of International Affairs at College of Science and Technology. He served as Chair of Department of Computer and Information Sciences from the summer of 2009 to the summer of 2016 and Associate Vice Provost for International Affairs from the fall of 2015 to the summer of 2017. Prior to joining Temple University, he was a program director at the National Science Foundation and was a distinguished professor at Florida Atlantic University. His current research interests include mobile computing and wireless net- works, routing protocols, cloud and green computing, network trust and security, and social network applications. Dr. Wu regularly publishes in scholarly journals, conference proceedings, and books. He serves on several editorial boards, including IEEE Transactions on Service Computing and the Journal of Parallel and Distributed Computing. Dr. Wu was general co-chair for IEEE MASS 2006, IEEE IPDPS 2008, IEEE ICDCS 2013, ACM MobiHoc 2014, ICPP 2016, and IEEE CNS 2016, as well as program co-chair for IEEE INFOCOM 2011 and CCF CNCC 2013. He was an IEEE Computer Society Distinguished Visitor, ACM Distinguished Speaker, and chair for the IEEE Technical Committee on Distributed Processing (TCDP). Dr. Wu is a CCF Distinguished Speaker and a Fellow of the IEEE. He is the recipient of the 2011 China Computer Federation (CCF) Overseas Outstanding Achievement Award.

Yihuai Wang received the Ph.D. degree from Hohai University, Nanjing, China. He is currently a Professor with Soochow University, Suzhou, China. He is the Director of the Embedded System and the Internet of Things Technical Committee, Jiangsu Computer Federation. He is also the Director of the Embedded System and the Internet of Things Research Institute, Soochow University. His research mainly focuses on parallel systems, software engineering, embedded system and application, artificial intelligence, and pattern recognition. He is a Senior Member of CCF.