Privacy-Preserving Dynamic Incentive Mechanism in Mobile Crowdsensing: Postprint

Authors: Liang Yan, An Jian, Hu Xianzhi, Si Haifeng

Date: 2018-10-11T00:00:00+00:00

Abstract

To address the conflict between high-quality sensing data and participant user privacy in mobile crowdsensing, a privacy-preserving dynamic incentive mechanism is proposed. First, a lightweight privacy protection method is adopted, which utilizes a secure cryptographic hash function to generate a variable address sequence of no less than 256 bits for bidding users, and combines random numbers to conceal and constrain the utility bids of candidate user nodes; second, by defining multi-dimensional parameters such as regional heat, temporal heat, data integrity rate, and data quality, dynamic equilibrium between task value and user utility bids is achieved; finally, based on the utility bids submitted by users and the task budget, and leveraging the reverse auction concept, optimal selection and dynamic incentive of task participation nodes are accomplished. Simulation experiments conducted on a mobile crowdsensing system simulation platform demonstrate that the proposed mechanism not only enhances the level of privacy protection and data accuracy, but also improves time efficiency and incentive effectiveness.

Full Text

Preamble

Dynamic Incentive Mechanism with Privacy-Preserving in Mobile Crowd Sensing

Liang Yan[1,2], An Jian[2]†, Hu Xianzhi[3], Si Haifeng[1]
(1. School of Technology, Xi' an Siyuan University, Xi' an 710038, China;
2. Shenzhen Research Institute of Xi' an Jiaotong University, Shenzhen Guangdong 518057, China;
3. Center of Network Information & Management, Xi' an University of Technology, Xi' an 710048, China)

Abstract: To address the contradiction between high-quality perception data and user privacy in mobile crowd sensing systems, this paper proposes a dynamic incentive mechanism with privacy-preserving. First, it employs a lightweight privacy-preserving method that utilizes a secure encryption hash function to generate a variable address sequence of no less than 256 bits for bidding users, combined with random numbers to conceal and constrain the utility quotes of candidate user nodes. Second, by defining multi-dimensional parameters such as regional heat, temporal heat, data integrity rate, and data quality, it achieves dynamic balance between task value and user utility quotes. Finally, based on the utility quotes submitted by users and the task budget, and leveraging reverse auction principles, it completes optimal selection and dynamic incentive of task participation nodes. Simulation experiments on a crowd sensing system platform demonstrate that the proposed mechanism not only enhances privacy protection and data accuracy, but also improves time efficiency and incentive effectiveness.

Keywords: mobile crowd sensing; privacy-preserving; incentive mechanism; reverse auction; utility quote

0 Introduction

In recent years, with the rapid development of mobile Internet, sensor networks, and social networks, mobile crowd sensing (MCS) has emerged as a cutting-edge research topic in the field of ubiquitous computing. Mobile crowd sensing utilizes ordinary users' mobile terminal devices as basic sensing units to achieve large-scale complex social sensing tasks through conscious or unconscious collaboration via mobile Internet for task distribution and data collection. However, while participating in sensing activities, users consume their own device resources including power, computation, storage, and communication, and face the risk of personal privacy leakage, which has become a significant factor hindering user participation in recent years. Therefore, designing reasonable incentive mechanisms that can effectively protect user privacy is crucial for promoting the long-term stable development of mobile crowd sensing platforms.

Current research has extensively investigated privacy protection issues at various stages of crowd sensing, such as group statistics, location obfuscation, k-anonymity, and differential privacy. However, these solutions typically introduce registration authorities/trusted third parties or aggregation servers to protect sensing data, users, or user locations, with most failing to consider the leakage of bidding participants' quote privacy. This paper aims to supplement existing privacy schemes by protecting participants'identity and quote privacy in more general environments to achieve better anonymity and privacy protection. We propose a dynamic incentive mechanism that supports privacy-preserving, using secure encryption hash functions to generate variable address sequences of no less than 256 bits for bidding participants as registration IDs to enable anonymous participation. Combined with random numbers, the mechanism conceals and constrains participants' utility quotes to achieve privacy protection

during bidding. Utility quotes are determined by multi-dimensional parameters including participants' data integrity rate, data quality, and ideal quotes. The platform selects optimal participation nodes and makes payments based on utility quotes and task budgets, while providing certain compensation to unsuccessful bidders according to the remaining task budget. The mechanism employs lightweight privacy-preserving methods and data encryption technology, combined with reasonable payment approaches, to achieve its incentive effects.

1 Related Work

Regarding incentive mechanisms in crowd sensing, numerous valuable studies have emerged in recent years. Current payment-based incentives employ game-theoretic methods, with micro-payment forms rewarding participants' sensing data being the most commonly used approach, among which reverse auction models are widely applied. Reference [4] first applied reverse auction from economics to crowd sensing incentive mechanism research, proposing a reverse auction dynamic price-virtual participation credit (RADP-VPC) mechanism that selects participants with the lowest quotes as winners while minimizing payment costs, and introduces the concept of virtual participation credits to prevent participants who repeatedly fail in bidding from exiting. Reference [5] proposed a location-based incentive model on the basis of RADP-VPC, selecting participant sets with maximum area coverage under fixed budget constraints, though user-centric area coverage cannot adapt to the dynamic variability and diversity of user locations. Reference [6] adopted a multi-attribute auction mechanism in reverse auctions, considering not only participation rates but also sensing data quality, enabling the server platform to influence data quality through the auction process while allowing participants to improve their sensing data quality and bidding prices through auction result feedback. However, these incentive mechanisms do not consider participant privacy protection.

Regarding privacy protection in crowd sensing, scholars have studied various techniques, mainly divided into four categories: group statistics, third-party verification, K-anonymity, and digital encryption. Reference [7] proposed the PriSense privacy protection scheme, including a process of segmentation and recombination and binary search, which supports various non-incremental data aggregation and quickly obtains aggregate values while balancing privacy protection strength and energy consumption. Reference [8] utilizes a trusted third party to provide anonymous services for participants, where participants register their sensing devices and install sensing software at the trusted third party, which maps participants' personal information to a new user space after verification, with the trusted third party responsible for participants' data transmission. Reference [9] proposed a demand-aware location privacy protection model DALP for continuous LBS requests, minimizing the anonymous area formed by common users' historical footprints by deleting the farthest footprints and narrowing anonymous area boundaries to reduce query delay and server load, thereby im-

proving user request service quality. Reference [10] employs an identity-based encryption method for participant data privacy protection, which does not rely on traditional public key infrastructure PKI and certification centers to bind public keys to participants. Participants' identity information (such as phone numbers, ID numbers, email addresses, etc.) can directly serve as their public keys, with private keys managed and issued by a trusted private key generator PKG, providing effective and secure communication for mobile nodes and requesters. Although these privacy protection schemes protect participants' data using different technologies, none consider how to incentivize participants to submit high-quality sensing data. Therefore, this paper proposes a dynamic incentive mechanism that both supports participant data privacy protection and incentivizes participants to submit high-quality sensing data.

2 System Model and Problem Analysis

2.1 System Model

This study is based on a generic mobile crowd sensing system comprising three roles: task publishers, task participants (workers or users), and auction infrastructure. These three roles are elaborated as follows:

a) **Task Publisher**: Organizations or individuals interested in or requiring sensing data, who specify time validity periods, locations or regions, and the remuneration they are willing to pay for obtaining sensing data.

b) **Task Participant**: Personnel who use various mobile sensing devices such as smartphones to collect sensing data according to task publishers' requirements, also called task workers or users.

c) **Auction Infrastructure**: Composed of three different servers belonging to the same mobile crowd sensing platform: Task Server (TS), Auction Server (AS), and Report Server (RS). The Task Server is responsible for publishing sensing tasks; the Auction Server runs the auction process, during which participants can initiate bids to the Auction Server; the Report Server collects sensing data from winners and forwards the data to task publishers.

[Figure 1: see original paper] describes the three working stages of the generic mobile crowd sensing system. First, the TS publishes sensing tasks from task publishers ( ), and participants' mobile devices regularly access the TS to search for suitable tasks and selectively download them ( ). Then, participants arrive at the destination to complete sensing tasks according to the task attributes provided by the task publisher ( ). Workers who complete tasks can register with the AS and initiate bids during the auction phase, with the proposed mechanism providing encryption protection for registration information and utility quotes to enable anonymous participation ( ). After the auction ends, the AS selects winners based on participants' utility quotes and the publisher' s task budget ( ). Finally, winners submit sensing data to the RS ( ), and after verification by

the RS, the AS pays remuneration to the winners ( ).

2.2.1 Privacy and Fairness Requirements

1) Participant Privacy: Before bidding ends, participants need to remain anonymous, and all quotes must be confidential, meaning participants' identity information cannot be linked to their submitted quotes in any way. This requires privacy protection measures to ensure participants complete bidding without revealing identity or device identifiers, and others cannot infer any information about participants. This paper' s privacy protection method uses secure encryption hash functions to encrypt and conceal participants' identities and quotes, differing from previous heavyweight cryptographic operations and primitives (such as secret sharing, multi-party computation, homomorphic encryption) [11]. It is a lightweight yet secure method that supports anonymous participant involvement.

2) Fairness and Impartiality: The bidding process requires that participants cannot determine their own quotes based on others' bidding information, and once utility quotes are submitted, they cannot be denied or modified to ensure bidding fairness. After bidding ends, the process enters an open phase where the bidding process should be verifiable by any participant to ensure bidding validity and winner selection impartiality. Therefore, commitment measures are needed to constrain participants' bidding behavior and provide a fair and just auction environment for all participants. The scheme includes commitment measures, and the use of hash functions and random numbers can ensure participants' commitment to their utility quotes during bidding.

2.2.2 Winner Selection and Payment

Since sensing tasks vary in form and collection environments are changeable, in the absence of objective evaluation standards, it is difficult for task publishers and participants to assess task value subjectively. This may result in task budgets that fail to satisfy participants, while participants struggle to provide reasonable quotes when bidding. Therefore, it is necessary to design a module that can objectively evaluate task value as a reference for publishers and participants. This mechanism provides a task value evaluation strategy for the mobile crowd sensing platform, where the auction server publishes task values in the message window to provide references for task publishers to set appropriate task budgets and for participants to set reasonable quotes.

When selecting winners, considering only participants with the lowest quotes may lead to low-quality sensing data that fails to meet task publishers' requirements. Therefore, the platform cannot focus solely on quotes when selecting winners; it must also consider participants' data quality and prioritize participants who provide high-quality data at reasonable quotes. Consequently, the mechanism selects winners based on participants' utility quotes and publishers' task budgets, where utility quotes are derived from participants' data utility val-

ues (determined by data integrity rate and data quality) and quotes proposed after referencing task values. To maintain high participation rates, remuneration is also distributed to unsuccessful bidders, with the remaining budget after paying winners evenly distributed among each loser to prevent participants who repeatedly fail in bidding from exiting.

3.1 Task Value

In evaluating task value, participant check-in data is obtained through location-based social networks (LBSN) applications [12]. This check-in data is used to analyze participants' spatiotemporal characteristic patterns, which are then combined with task spatiotemporal characteristics to calculate task value. Two factors influence task value assessment: regional heat and temporal heat. Regional heat measures the frequency of participant visits to the task' s region, while temporal heat measures the frequency of participant visits during the task' s valid time period. These two factors are calculated based on participant check-in data in information space and the spatiotemporal characteristics of sensing tasks in physical space.

Regional heat L(O) is calculated by analyzing check-in locations of participants in LBSN online data, as shown in Equation (1):

$$L(O) = \frac{\sum_{x \in U, j \in O} N_{x,j}}{\sum_{x \in U, j \in \tau} N_{x,j}} \times E(X) \quad (1)$$

$$E(X) = -\sum p(x_i) \times \log_2 p(x_i) \quad (2)$$

where O represents the task region specified by the publisher, Nx,j represents the number of check-ins by participant x at location j, U represents the set of all participants, and represents the set of all check-in locations. E(X) in Equation (1) is calculated by Equation (2). E(X) represents the diversity of participants accessing region O, obtained by calculating regional information entropy. X represents the set of participants checking in region O, X = {x , x , ···, x }. p(x) represents the probability of participant x checking in region O, i.e., the ratio of check-ins by participant x in region O to total check-ins across all regions.

If the regional information entropy is larger, the information provided by participants checking in that region is greater, meaning higher diversity of participants checking in that region. Regional heat is normalized to a range of 0~1, where larger values indicate more visitors to the region and higher check-in frequency.

Temporal heat T(Z) is calculated by analyzing the temporal distribution of participant check-ins in LBSN online data, with values between 0~1, as shown in Equation (3):

$$T(Z) = \sum_{z \in Z} PV_z \quad (3)$$

$$PV_z = \frac{\sum_{x \in U, j \in O} N_{x,z,j}}{\sum_{x \in U, k \in A, j \in O} N_{x,k,j}} \quad (4)$$

Since participant check-in times have certain flexibility, for accurate task assessment, one day is divided into 24 time periods using one hour as the unit. In Equation (4), A represents the 24 time periods, A = {1, 2, ···, 24}. PVz represents the probability of all participants accessing region O during time period z. Nx,z,j represents the number of times participant x accessed location j during time period z. In Equation (3), Z represents the set of time periods covered by the task, Z A.

Based on regional heat and temporal heat, the task value V for any task can be calculated by Equation (5):

$$V = \frac{LA}{L(O)} \times \frac{TA}{T(Z)} \quad (5)$$

LA represents the average regional heat of all regional rectangular blocks obtained from participant check-in data via Equation (1), and TA represents the average temporal heat of all participants' check-ins obtained via Equations (3) and (4). The task value is defined as the baseline value of 1 when regional heat equals LA and temporal heat equals TA, representing the unit value of the task. Equation (5) indicates that task value is negatively correlated with regional heat and temporal heat of its location. In other words, for a task, if the time and region where participants collect data have higher heat, the task is easier to complete, and correspondingly, the task value is lower; conversely, the task value is higher.

Once a task' s value is evaluated and determined by the platform, it is promptly published in the message window for all participants' reference and to facilitate dynamic adjustment of task budgets by task publishers.

3.2 Data Utility Value

Task workers' performance significantly impacts data quality. This paper uses data utility value as a metric for data quality, which is measured based on two main factors: data integrity rate and quality indicators.

1) Data Integrity Rate (CR): Data integrity rate is defined as the ratio of completed task volume to required total task volume. CR measures the task completion volume of workers. For tasks with a predefined point set P, sensing points collected by workers can be grouped using a method based on the shortest distance to each point in P. If the shortest distance exceeds threshold r, the sensing point is considered unrelated to the task; otherwise, it is grouped to the associated point in P. The CR value for a worker regarding set P can then

be calculated based on the number of task coverage points TWP, as shown in Equation (6):

$$CR_w = \frac{|TWP|}{|P|} \quad (6)$$

2) Quality Indicator (QI): Measuring data quality is challenging. This paper discusses only the quality measurement of numerical data. For each data group G, the distance from each member to its group center can be calculated. For each data point, the individual QI is represented by 1 minus the ratio of the average distance to the maximum distance in its group. The average value of all data from a task worker then represents this worker' s data quality indicator QI (0 < QI 1), calculated as shown in Equation (7). Assuming a worker' s complete data set is Dw = {d , d , ···, d }:

$$QI_w = \frac{1}{n}\sum_{i=1}^{n}\left(1 - \frac{dist(d_i, G(d_i).center)}{MaxDis(G(d_i))}\right) \quad (7)$$

3) Data Utility Value (DU): Based on the two factors of data integrity rate CR and quality indicator QI, the data utility value DUw for a task worker can be derived, as shown in Equation (8):

$$DU_w = CR_w \times QI_w \quad (8)$$

3.3 Utility Bidding

To win in bidding, participants need to provide reasonable quotes. Therefore, they must combine their own data utility values with the task value provided by the platform to ensure a higher winning probability. Participants propose an ideal bidding price BV by referencing the platform' s task value V, then calculate their utility quote for bidding. The utility quote BUw is calculated by Equation (9):

$$BU_w = BV \times (1 - DU_w) \quad (9)$$

3.4 Auction

The auction process includes three main phases: registration, bidding, and opening. In the registration phase, each participant registers anonymously to protect their identity privacy. In the bidding phase, each participant' s utility quote is ensured to be invisible to other participants. In the opening phase, the auction server publicly reveals each participant' s utility quote while keeping participant identity information concealed, and determines anonymous winners based

on utility quotes. Once winners upload their sensing data and it is verified by the report server, they receive corresponding remuneration.

Assume there is a "contract message window" on the auction server for information exchange between the server and participants. Once a message is published to the message window, any participant can read it but cannot delete or modify it. Therefore, the contract message window is a broadcast program module where any participant can receive broadcast messages, and messages can be verified by any participant. The auction server' s public key k is announced to each participant through the message window, which participants can use to encrypt information sent to the auction server and verify messages signed by the server. Let Hash() denote a secure encryption hash function with no less than 256-bit output. "Secure" means Hash() is one-way and collision-resistant. Therefore, inverting the hash function or finding x and y satisfying Hash(x) = Hash(y) is computationally infeasible.

3.4.1 Registration

Before bidding begins, the auction server publishes its public key and various auction parameters, such as auction ID and start/end times of each auction phase, to the message window. Once registration begins, each participant sends an anonymous ID BidderID to the AS within the specified registration time to identify themselves in the bidding. BidderID is generated from the hash value Hash(k) of a randomly selected one-time temporary public key k by the participant. After receiving it, the AS publishes this information to the message window, allowing each participant to verify whether their BidderID has been successfully registered for this bidding.

Definition 1: If (k, k ^{1}) is an entity A' s key pair, then Sig , ^{1}(m) represents the digital signature created by entity A on message m using private key k ^{1}, denoted by , i.e., = Sig , ^{1}(m). Sig.verify , (m,) represents the verification result (true or false) of decrypting the digital signature on message m using A' s public key k.

Algorithm 1. Anonymous Registration for Participants
Input: Participant b' s one-time temporary public key k .
Output: Participant b' s anonymously registered ID BidderID signed and authorized by auction server A.

1. h = Hash(k), where h is b' s anonymous registration ID BidderID;
2. h* = r × h mod N , where r is a new random number, e is A' s public key, N is the encryption algorithm modulus, and h* is the encrypted BidderID;
3. b → A: h* and = Sig_b, ^{1}(h*);
4. if Sig.verify_b, (h*,) = true then
5. A → *: h and Sig , ^{1}(h);
6. end if
7. ' = r ^{1} × * mod N , where b obtains the digital signature ' from A about h.

Algorithm 1 not only supports anonymous participant registration but also ultimately generates an authorized temporary public key k for participants. As long as participants provide such credentials during the sensing data submission phase, they are considered authorized users. Therefore, this approach also serves as a method for verifying temporary keys.

3.4.3 Opening

When the auction server announces the end of bidding, the true value of each participant' s utility quote BUw is revealed. After receiving BUw and rw, the auction server evaluates Commit(BUw, rw) = H(rw||BUw) and continues to use the temporary key associated with the participant to verify the signature _b. After verifying the quotes, the auction server selects the top n participants with the lowest BUw values as winners based on the task budget. Then, it broadcasts a signed message in the message window containing the winners' anonymous IDs BidderID, temporary public keys, and utility quotes BUw. Therefore, any participant can verify the correctness of this bidding by calculating H(rw||BUw), ensuring fairness and impartiality in the auction process.

Algorithm 2. Bidding-Opening
Input: Participant b' s utility quote BUw and a new random number rw.
Output: Auction server' s signed message of n winner nodes.

1. Commit = H(rw||BUw), where b obtains CBUw;
2. b → AS: _b = Sig_b, [1](ActionID||BidderID' ||CBUw);
3. Initialize set S = ;
4. for b from b to b do
5. m = (ActionID||BidderID' ||H(rw||BUw));
6. if Sig.verify_b, (m , _b) = true then
7. `S = S + {m };`
8. end if
9. end for
10. Sort set S in ascending order by BUw value to obtain new set S' and publish S' content to the message window;
11. Initialize: winner set W = , current number of nodes in W n = 0, total number of winner nodes N;
12. x = S' .FirstElement();
13. while TotalB > 0 and n < N do
14. W = W + {x};
15. n = n + 1;

16. TotalB = TotalB - TotalBx;
17. x = S' .NextElement();
18. end while
19. return W, with winner nodes published to the message window, i.e., AS → *: Sig (AuctionID, (BidderID , k , BUw , rw), ···).

3.5 Payment Measures

Selected winners can transmit sensing data to the report server, which verifies the received data. If qualified, payment is made according to the winners' utility quotes. After completing payment to all winners who uploaded qualified data, if the task budget has a surplus, it is distributed equally among unsuccessful bidders as compensation.

The lightweight privacy-preserving method can both ensure the concealment of bids and constrain participants from arbitrarily denying or changing quotes. Moreover, quotes are published in the message window so that any participant can verify that their quotes have been correctly submitted to the auction server. When the auction server receives _b, it can determine that it is from a legitimate platform participant because verification is completed using the public key with their signature. Therefore, the temporary key serves as an authorization credential, allowing the server to implicitly verify participants without identifying them.

4 Performance Analysis

The scheme' s performance is analyzed from aspects of privacy confidentiality, correctness, non-repudiation, unlinkability, and incentive effectiveness.

1) Privacy Confidentiality: Since participants use a secure encryption hash function Hash() to generate a hash value of no less than 256 bits from their one-time temporary public key to identify their bidding identity during registration, and Hash() is collision-resistant, ensuring the uniqueness of each participant' s registration ID, participants' identity privacy information can be well protected. Additionally, because utility quotes appear in bidding in the form H(rw||BUw), the one-way property of hash function H and the use of random number rw ensure that utility quotes remain concealed and cannot be inferred by other participants, while also eliminating the possibility of collusion. Therefore, the scheme provides privacy confidentiality for participants' bidding prices.

2) Correctness: Since all participants' utility quotes BUw and used random numbers rw are published in the message window after bidding ends, any participant can verify the correctness of the bidding. Therefore, false quotes cannot appear or existing quotes be altered (due to the collision resistance of hash function H), ensuring bidding correctness and fairness.

3) Non-repudiation: Since each quote carries the participant' s digital signature, and the collision resistance of hash functions ensures it is impossible to find a set (r' , BU') such that H(r' ||BU') = H(r||BU), participants cannot deny or modify their quotes once bidding begins. Moreover, if bidding disputes arise, bidding commitments can be used to resolve them, with commitment values (r, BU) and participants' digital signatures used to prove bidding authenticity. Thus, participants' bidding behavior can be well constrained.

4) Bidding Unlinkability: This property relates to participant identity privacy. To ensure that two quotes submitted by the same participant in different bidding rounds cannot be linked, this scheme supports participants using different anonymous IDs and public keys for each bidding round, guaranteeing unlinkability between participants and quotes.

5) Incentive Effectiveness: Since winner selection considers multi-dimensional parameters including participants' data utility values and ideal quotes referencing task value, rather than considering only the lowest quote, and provides certain compensation to unsuccessful bidders, the scheme achieves optimal winner selection. The reward remuneration can satisfy winners' needs, ultimately providing effective incentives for both winners and losers.

5 Experimental Validation

To evaluate the scheme' s effectiveness, verification is conducted from aspects of privacy protection degree, data accuracy, time efficiency, and incentive effect.

5.1 Experimental Data and Environment

The experimental process employs simulation experiments, with simulation data generated by a crowd sensing system simulation platform. The simulation platform successively released 50 sensing tasks at different campus locations over three months and recruited a certain number of students to participate. For each sensing task, the registration number ranged from 100 to 1000 people. After 50 rounds of task release, auction, and payment, the platform accumulated a large amount of simulation data.

The experimental environment consists of an Intel i5-7200U 2.5GHz CPU, 4GB memory, Windows 7 operating system, with algorithms implemented in Objective-C.

5.2 Evaluation Metrics

1) Privacy Protection Degree: Participants' privacy leakage probability P_reveal is defined as the ratio of leaked bidding privacy volume to total bidding privacy requiring protection, as shown in Equation (12):

$$P_{\text{reveal}} = \frac{n_{\text{reveal}}}{N_{\text{protect}}} \quad (12)$$

where n_reveal is the volume of leaked bidding privacy, and N_protect is the total volume of bidding privacy requiring protection.

Privacy protection degree Privacy_Degree is defined as:

$$\text{Privacy\_Degree} = 1 - P_{\text{reveal}} \quad (13)$$

Higher privacy protection degree indicates stronger protection levels for privacy data.

2) Data Accuracy: Due to privacy protection concerns, the accuracy of anonymous identity data and encrypted quote data submitted by participants may be affected. Data accuracy refers to the difference between the anonymous dataset and the original dataset, typically measured by SSE (sum of squared errors). SSE represents the sum of squared attribute distances between all records in the anonymous dataset and the original dataset, as shown in Equation (14):

$$\text{SSE} = \sum_{i=1}^{n} \left(dist(a_i^n, (a_i^n)')\right)^2$$

where a_i^n is the nth attribute of the ith record in the original dataset, and (a_i^n)' is the nth attribute of the ith record in the anonymous dataset. dist() is the distance function. Smaller SSE values indicate higher data accuracy and better data usability.

3) Time Efficiency: Auction time Ti is defined as the running time from registration start to winner selection, as shown in Equation (15):

$$T_i = t_{\text{win}} - t_{\text{reg}} \quad (1 \le i \le n) \quad (15)$$

where t_win represents the moment winners are selected, t_reg represents the moment registration begins, n represents the total number of auctions, and i represents the ith auction.

Algorithm time efficiency is measured by T(n), the average time of n auctions, as shown in Equation (16). Smaller T(n) values indicate higher time efficiency.

$$T(n) = \frac{\sum_{i=1}^{n}(T_i)}{n} \quad (16)$$

4) Incentive Effect: User participation rate and satisfaction can reflect the scheme's incentive effect. User participation rate P_work is defined as the ratio of bidding participants to registered participants, as shown in Equation (17):

$$P_{\text{work}} = \frac{n_{\text{bid}}}{N_{\text{reg}}} \quad (17)$$

where n_bid represents the number of bidding participants, and N_reg represents the number of registered participants.

Users who complete sensing tasks and receive corresponding remuneration evaluate the platform, with evaluation results e set at two levels, as shown in Equation (18):

$$e = \begin{cases} 1 & \text{satisfied} \\ 0 & \text{dissatisfied} \end{cases}$$

User satisfaction S is defined as the ratio of users giving evaluation result "1" to the total number of evaluating users, as shown in Equation (19):

$$S = \frac{n(e=1)}{N_{\text{evaluate}}} \quad (19)$$

where n(e=1) represents the number of users giving evaluation result "1" , and N_evaluate represents the total number of evaluating users.

5.3 Experimental Results and Analysis

For testing privacy protection degree, data accuracy, and time efficiency, under the same simulation data and experimental environment, this paper' s algorithm is compared with two privacy protection schemes: PRIDE and TTP. PRIDE [13] is a privacy-preserving spectrum auction scheme in cognitive radio networks that utilizes complex cryptographic techniques (such as secure multi-party computation, order-preserving encryption, and oblivious transfer protocols) to obtain the lowest quote while protecting quote privacy. TTP (Trusted Third Party) [8] is a trusted third-party group mechanism that introduces a completely trusted third party to execute group bidding, with all participant information such as quotes, IDs, and spatiotemporal matrices being transparent to the TTP, making participants' privacy entirely dependent on the TTP.

By setting privacy thresholds from 0.1 to 1.0, a comparison of privacy protection degrees among the three algorithms is obtained, as shown in [Figure 2: see original paper].

[FIGURE:2 shows that as the privacy threshold increases, the privacy protection degrees of all three algorithms show an upward trend. This is because higher privacy thresholds lead to stronger protection levels for participants' privacy data. Under the same privacy threshold conditions, this paper' s algorithm achieves higher privacy protection degree than both PRIDE and TTP. Since this paper' s algorithm uses participants' temporary public keys with a collision-resistant secure encryption hash function to generate variable address sequences of more than 256 bits to protect participant identity, and combines random numbers to conceal candidate participation nodes' utility quotes, while PRIDE

and TTP algorithms lack collision resistance and the capability to generate variable address sequences, this paper' s algorithm provides stronger privacy protection and superior privacy protection degree.]

[Figure 3: see original paper] shows a comparison of data accuracy among the three algorithms, with privacy thresholds also set from 0.1 to 1.0.

[FIGURE:3 shows that as the privacy threshold increases, the data accuracy of both PRIDE and TTP algorithms shows a downward trend, while this paper' s algorithm' s data accuracy remains close to 100%. This is because the PRIDE algorithm uses complex cryptographic techniques for quote privacy protection; larger privacy thresholds increase encryption complexity and concealment degree, leading to greater data accuracy degradation. The TTP algorithm uses a trusted third party to protect all participant privacy, and as the privacy threshold increases, the trusted third party' s protection level also increases, resulting in higher confusion through group bidding to conceal real participant identities and causing significant data accuracy degradation. This paper' s algorithm employs lightweight data encryption technology, achieving privacy protection for participant identity and quote data without complex encryption operations, so data accuracy is less affected by the privacy threshold.]

[Figure 4: see original paper] shows a comparison of time efficiency among the three algorithms.

[FIGURE:4 shows that as the number of registered participants increases, T(n) for all three algorithms increases accordingly, because algorithm running time increases with population size. However, this paper' s algorithm shows only a slight increase in T(n) as registration numbers grow, while PRIDE and TTP algorithms have higher T(n) values than this paper' s algorithm, with PRIDE showing the largest increase 幅度. This demonstrates that under the same test conditions, this paper' s algorithm has greater advantages in time efficiency.]

For incentive effect testing, this mechanism is compared with two incentive mechanisms: the dynamic price reverse auction mechanism RADP proposed by Lee et al. [13] and the fixed-price random selection mechanism RSFP. Both RADP and RSFP mechanisms only pay remuneration to winners and do not consider participant privacy protection. Using the same simulation data (i.e., 50 campus sensing tasks' release, auction, and payment) with registered participants ranging from 100 to 1000, the three mechanisms are tested, yielding user participation rate and satisfaction comparisons shown in [Figure 5: see original paper] and [Figure 6: see original paper] respectively.

[FIGURE:5 shows that as the number of registered participants increases, this mechanism' s user participation rate remains above 95%, while both RADP and RSFP mechanisms show downward trends, dropping below 90% when registration reaches 1000. This is because this mechanism considers not only participants' data integrity rate and data quality but also selects winners optimally based on utility quotes, provides remuneration to unsuccessful bidders, and protects participant identity and quote privacy throughout the auction pro-

cess. This demonstrates that this mechanism achieves higher user participation rates, indicating better effectiveness in motivating users to participate in sensing tasks.]

[FIGURE:6 shows that when the number of evaluating users is 200, 400, 600, 800, and 1000, this mechanism' s user satisfaction is higher than both RADP and RSFP, with an average satisfaction of 95.22%, compared to RADP's 85.16% and RSFP' s 81.84%. This indicates that participants highly approve of this mechanism' s incentive approach.]

The experimental results shown in [Figure 2: see original paper] through [Figure 6: see original paper] conclude that this mechanism offers superior performance compared to existing incentive mechanisms in terms of privacy protection degree, data accuracy, time efficiency, and incentive effectiveness, demonstrating its effectiveness.

6 Conclusion

This paper proposes a dynamic incentive mechanism with privacy-preserving to address the poor effectiveness of crowd sensing incentive mechanisms caused by user privacy leakage and other reasons. The mechanism employs lightweight privacy-preserving methods combined with data encryption technology to support anonymous participant registration and provides privacy protection for participants' utility quotes during the bidding phase. Utility quotes are determined by multi-dimensional parameters including participants' data integrity rate, data quality, and ideal quotes. Finally, winners are selected and paid based on utility quotes, with certain compensation provided to unsuccessful bidders to exert incentive effects. Simulation experiments demonstrate that the mechanism exhibits superior performance compared to similar schemes in privacy protection degree, data accuracy, time efficiency, and incentive effect. In future research, we will attempt to incorporate privacy protection for data during the remuneration payment phase into the mechanism' s protection scope to make the mechanism more complete.

References

[1] Guo Bin, Chen Huihui, Yu Zhiwen, et al. Fliermeet: a mobile crowdsensing system for cross-space public information reposting, tagging, and sharing [J]. IEEE Trans on Mobile Computing, 2015, 14 (10): 2020-2033.

[2] Ganti R K, Ye Fan, Lei Hui. Mobile crowdsensing: Current state and future challenges [J]. IEEE Communications Magazine, 2011, 49 (11): 32-39.

[3] Wang Yu, Xu Dingbang, Li Fan. Providing location-aware location privacy protection for mobile location-based services [J]. Tsinghua Science and Technology, 2016, 21 (3): 243-259.

[4] Lee J S, Hoh B. Sell your experiences: A market mechanism based incentive for participatory sensing [C]// Proc of IEEE International Conference on Pervasive Computing and Communications. 2010: 60-68.

[5] Jaimes L G, Vergara-Laurens I, Labrador M A. A location-based incentive mechanism for participatory sensing systems with budget constraints [C]// Proc of IEEE International Conference on Pervasive Computing and Communications. 2012: 103-108.

[6] Krontiris I, Albers A. Monetary incentives in participatory sensing using multi-attributive auctions [J]. Parallel Algorithms & Applications, 2012, 27 (4): 317-336.

[7] Shi Jing, Zhang Rui, Liu Yunzhong, et al. PriSense: privacy-preserving data aggregation in people-centric urban sensing systems [C]// Proc of IEEE INFOCOM. 2010: 758-766.

[8] Cristofaro E D, Soriente C. Participatory privacy: enabling privacy in participatory sensing [J]. IEEE Network, 2013, 27 (1): 32-36.

[9] Li Xinghua, Wang Ermeng, Yang Weidong, et al. DALP: a demand-aware location privacy protection scheme in continuous location-based services [J]. Concurrency & Computation Practice & Experience, 2016, 28 (4): 1219-1230.

[10] Cristofaro E D, Soriente C. Extended capabilities for a privacy-enhanced participatory sensing infrastructure (PEPSI) [J]. IEEE Trans on Information Forensics and Security, 2013, 8 (12): 2021-2033.

[11] Nojoumian M, Stinson D R. Efficient sealed-bid auction protocols using verifiable secret sharing [C]// Proc of International Conference on Information Security Practice & Experience. 2014: 302-317.

[12] 南文倩, 郭斌, 陈荟慧, 等. 基于跨空间多元交互的群智感知动态激励模型 [J]. 计算机学报, 2015, 38 (12): 2412-2425. (Nan Wenqian, Guo Bin, Chen Huihui, et al. A cross-space, multi-interaction-based dynamic incentive mechanism for mobile crowd sensing [J]. Chinese Journal of Computers, 2015, 38 (12): 2412-2425.)

[13] Wu Fan, Huang Qianyi, Tao Yixin, et al. Towards privacy preservation in strategy-proof spectrum auction mechanisms for noncooperative wireless networks [J]. IEEE//ACM Trans on Networking, 2015, 23 (4): 1271-1285.

[14] 沈楠, 袁科, 贾春福. 一种增强的位置分享隐私保护方案 [J]. 计算机应用研究, 2017, 34 (3): 862-866, 887. (Shen Nan, Yuan Ke, Jia Chunfu. Enhanced privacy-preserving location sharing mechanism [J]. Application Research of Computers, 2017, 34 (3): 862-866, 887.)

Note: Figure translations are in progress. See original paper for figures.