Computer Networks 135 (2018) 32–43

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems☆

Yingjie Wang[a,b], Zhipeng Cai[c,d,*], Xiangrong Tong[b], Yang Gao[b], Guisheng Yin[c]

[a] School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China
[b] School of Computer and Control Engineering, Yantai University, Yantai 264005, China
[c] College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
[d] Department of Computer Science, Georgia State University, Atlanta, GA 30303, USA

ARTICLE INFO

Article history:
Received 26 October 2017
Revised 11 February 2018
Accepted 12 February 2018
Available online 13 February 2018

Keywords:
Mobile crowdsourcing
Incentive mechanism
Auction algorithm
K-anonymity
Differential privacy

ABSTRACT

With the rapid development of mobile devices, mobile crowdsourcing has become an important research focus. In order to improve the efficiency and truthfulness of mobile crowdsourcing systems, this paper proposes a truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems. The improved two-stage auction algorithm based on trust degree and privacy sensibility (TATP) is proposed. In addition, the $k-\varepsilon$-differential privacy-preserving is proposed to prevent users' location information from being leaked. Through comparison experiments, the effectiveness of the proposed incentive mechanism is verified. The proposed incentive mechanism with location privacy-preserving can inspire users to participate sensing tasks, and protect users' location privacy effectively.

1. Introduction

With the rapid development of mobile devices, mobile crowdsourcing has attracted more and more attention in Mobile Crowd Sensing Networks (MCSS). In traditional commercial crowdsourcing systems, such as Amazon Mechanical Turk, oDesk, etc., one requester submits a task to the crowdsourcing platform and defines how much the workers will be paid per task and how the workers have to provide proof of a completed task. Different from traditional crowdsourcing marketplaces, in mobile crowdsourcing markets, crowd workers are paid to perform micro-tasks utilizing their mobile devices [1]. In mobile crowdsourcing, it is common that workers are coming and bidding for a specific task sequentially, and the decision on accepting or denying a worker's bidding must be made by the platform instantly upon the worker's arrival. Therefore, compared with the traditional commercial crowdsourcing systems, mobile crowdsourcing systems need higher real-time performance. How to inspire workers to participate tasks and upload truthful data have become the research focus. In recent years, researchers have proposed many incentive mechanism to improve the efficiency of mobile crowdsourcing systems. However, static incentive mechanism of traditional crowdsourcing is not appropriate for mobile crowdsourcing. It cannot satisfy the real-time property of mobile crowdsourcing, thus how to design dynamic incentive mechanism methods become the research focus in mobile crowdsourcing.

Private information indicates the information that an individual is unwilling to disclose [2]. This information includes individual's behavior pattern, interests, locations, physical condition and so on. Location privacy represents one's location information or other associated information (such as home address, working location, living habit and so on) deduced from location information [3,4]. Therefore, privacy-preserving mechanism should insulate users' sensitive information, and prevent attackers from deducing other associated information through one's location information [5,6]. In conclusion, it is challenging to protect users' privacy and hence privacy-preserving in mobile crowdsourcing has become an important research focus [7]. Some of the major challenges in mobile crowdsourcing are summarized as followings:

1. The real-time property of mobile crowdsourcing systems should be further considered when designing incentive mechanism. In addition, trust degree and privacy sensibility also should be considered in order to guarantee the long-term and sensibility of participation.
2. The interaction influences between social relationships and locations information make the privacy-preserving models more

☆ Fully documented templates are available in the elsarticle package on CTAN.

* Corresponding author: Department of Computer Science, Georgia State University, Atlanta, GA, 30303, USA.
E-mail addresses: wangyingjie@ytu.edu.cn (Y. Wang), zcai@gsu.edu (Z. Cai), txr@ytu.edu.cn (X. Tong), yinguisheng@hrbeu.edu.cn (G. Yin).

https://doi.org/10.1016/j.comnet.2018.02.008
1389-1286/

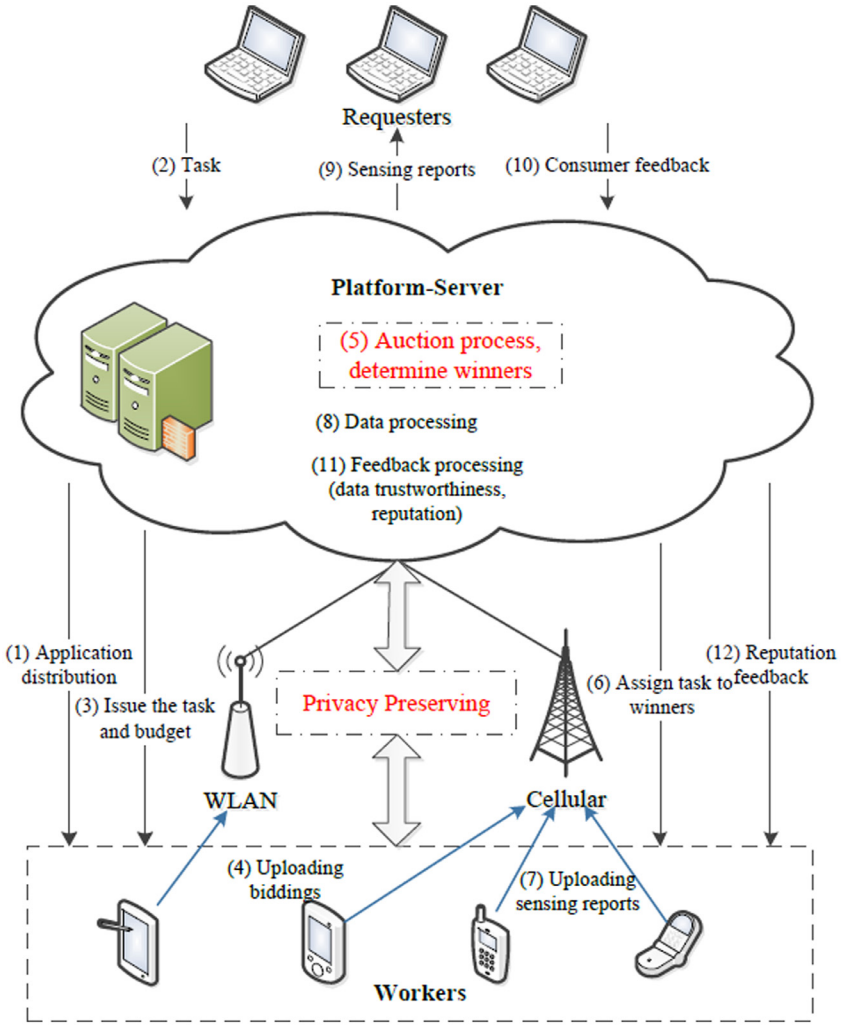

Fig. 1. Architecture of a mobile crowdsourcing system.

complex. Existing privacy-preserving technologies cannot adapt to the complex and online mobile crowdsourcing systems.

3. Developed model should anonymously process user's location information as the attackers might deduce users' private information from their location information. The location privacy-preserving method should be researched in order to resist continuous attack.

Fig. 1 shows the architecture of a mobile crowdsourcing system. In the process of crowdsourcing, we research the auction process with privacy-preserving to improve the efficiency of mobile crowdsourcing system. In order to inspire workers to participate sensing tasks actively, the auction algorithm is researched. Because of the importance of worker's privacy, we also add the privacy-preserving into the proposed incentive mechanism, which can inspire workers to participate sensing tasks [8]. The contributions of this paper are shown as follows.

1. The improved two-stage auction algorithm based on trust degree and privacy sensibility (TATP) is discussed. The proposed method can guarantee the dynamics and fairness for online incentive mechanism.
2. Workers' location privacy-preserving is researched in this paper. In order to solve homogeneity attack problem, we propose $k - \varepsilon$-differential privacy-preserving, which the Gaussian white noise is applied into differential privacy-preserving, and combined with k-anonymity to protect worker's location information.
3. Analytical and empirical validations are done to show that the proposed mechanism achieves the anonymity and security objectives. We utilize data sets of mobility traces of taxis in Beijing and New York to verify the effectiveness of the proposed location privacy-preserving respectively. In addition, we verify the effectiveness of the proposed auction algorithm through comparison experiments.

The rest of the paper is organized as follows. Section 2 presents the related works. Section 3 introduces the proposed incentive mechanism for mobile crowdsourcing systems, which includes the improved two-stage auction algorithm-TATP and $k - \varepsilon$-differential privacy-preserving. Section 4 illustrates the simulations, along with the parameter settings, followed by the result analysis and discussions. Finally, Section 5 concludes this paper.

2. Related works

In this section, we review related works from two aspects, auction algorithms and location privacy-preserving mechanisms.

2.1. On the aspect of auction algorithms

In order to inspire workers to participate tasks and behave truthfully, building effective auction algorithms has become

research focus. The main auction algorithms applied in mobile crowdsourcing systems include RA (reverse auction) [9], CA (combinatorial auction) [10], MAA (multi-attributive auction) [11], AA (all-pay auction) [12], DA (double auction) [13] and VCG (vickrey-clarke-groves auction) [14]. Lee and Hoh [9] applied RA into the incentive mechanisms of MCSS, which can guarantee the minimized payment cost and high participation rate. However, this method failed to consider the trustworthy of workers, which will result in decrease of data quality. Krontiris and Albers [11] considered both participation rate and data quality based on MAA. In order to increase bidding price, participants will improve their data quality according to auction feedback results. However, authors failed to consider user's privacy sensibility, which will decrease the participation rate of users with high privacy sensibility. Yang et al. [13] adopted DA to inspire participant to participate *k*-anonymity privacy protection. In crowd sensing, participants have different location privacy-sensitivity levels, thus DA can inspire the participants with low location privacy-sensitivity to participate *k*-anonymity privacy protection in order to protect the location information of participants with high location privacy-sensitivity. According to multiple tasks, Feng et al. [10] adopted CA to inspire participant. Participant can bid multiple tasks based on his location and sensing range. The winners will be determined by platform based on overall biddings. However, this incentive mechanism was designed for offline scenario.

In addition, an auction-based incentive mechanism was proposed in [15]. The authors utilized the announced total reward R (budget) and user i's sensing plan t_i (user i's willingness on how long he wants to participate in the sensing task) to design a novel auction based on submodular function. In [16], the authors designed incentive compatible mechanisms that maximize a requester's objective under a budget. It is known as *budget feasibility* where the mechanism must be designed so that the sum of its payments does not exceed the budget. Therefore, budget and sensing plan are two important factors for designing an effective auction algorithm in crowdsourcing systems, such as Amazon Mechanical Turk, a successful crowdsourcing system that performs under a budget. Chen et al. [17] proposed a truthful incentive-based on online auction mechanism (TOAM) with the consideration of ex-post service quality. However, in the above mechanisms, most of the auction thresholds are static and cannot be changed dynamically.

According to online auction mechanism, the two-stage auction algorithm is applied widely [18]. The process of a two-stage auction algorithm indicates that the first batch of users is rejected and used as the sample which enables making an informed decision on whether to accept the rest of the users. However, this method fails to guarantee the consumer sovereignty, since the first batch of users has no chance to win the auction no matter how low the cost is. This method automatically rejects the first batch of users, so that it encourages users to arrive late. In other words, the users who arrive early have no incentive to report their biddings, which may hinder the users' competition or even result in task starvation [19]. In addition, the aforementioned works failed to consider worker's trust degree and privacy sensibility, which may influent network's trust and efficiency.

2.2. On the aspect of location privacy-preserving mechanisms

According to the location privacy-preserving strategies, the main methods include dummy location method [20,21], spatio-temporal cloaking method [22,23] and spatial encryption method [24]. In order to protect user's location, dummy location method publishes a dummy location to the platform, *i.e.*, the location privacy is protected through publishing a dummy location. Privacy preserving level and service quality are associated with the distance between dummy location and real location. As the distance between dummy location and real location gets farther, the service quality gets worse but the privacy preserving level increases. On the contrary, if the distance between dummy location and real location is small, the service quality is better but the privacy preserving level is lower. In summary, dummy location method has low computational cost and good service quality but also low privacy preserving level. Spatio-temporal cloaking method utilizes a spatial range to transmit instead of user's real location. *k*-anonymity preserving is the most typical technology in spatio-temporal cloaking method. Gedik and Liu [25] proposed a privacy personalization framework to support location *k*-anonymity for a wide range of mobile clients with context-sensitive privacy requirements. The advantages of spatio-temporal cloaking method is that the service quality and privacy preserving achieve a good balance. However, it is difficult to achieve optimal anonymous for spatio-temporal cloaking method. In the case of continuous attack, *k*-anonymity still has the risk of privacy leak. Spatial encryption method achieves anonymous purpose through encrypting location. SpaceTransform [25] and PrivateQuery [26] technologies are two typical technologies in spatial encryption method. Spatial encryption method has better privacy preserving, but bigger processing cost.

However, most of the privacy-preserving methods failed to define attack model, which cannot quantize the knowledge that attackers owned [27]. According to this problem, Dwork et al. [28] proposed differential privacy to solve the problem. To et al. [29] proposed a mechanism based on differential privacy and geocasting that achieves effective Spatial Crowdsourcing services while offering privacy guarantees to workers. Differential privacy defines attack model strictly, which can reduce the risk of privacy leak. In differential privacy, there is no connection between the added amount of noise and the scale of dataset. According to big scale of data set, it only needs to add a little noise and obtains high level privacy protection [30]. However, if the adversary knows the noise distribution and a set of likely positions (including the true location) for the user, the adversary can compute the probability of generating the observed perturbation from each of the likely positions. The adversary will confidently infer the user position if the probability is significantly high for the true location.

2.3. Summary

According to the discussions for aforementioned methods, most of incentive mechanisms were proposed for offline scenario, which cannot adapt online network environment. In addition, incentive mechanisms for MCSS not only should increase participation rate, but also should consider the long-term and sensibility of participation. Therefore, we research the auction algorithm based on two-stage auction in real-time dynamic environments through considering trust degree and privacy sensibility in order to improve efficiency and trust degree of mobile crowdsourcing systems.

Most of existing privacy-preserving mechanisms cannot resolve continuous attack problem and background knowledge problem effectively. According to the above problems, we research privacy-preserving mechanism through combining *k*-anonymity and differential privacy. In order to better protect worker's privacy information, the differential privacy based on Gaussian white noise are applied into *k*-anonymity in this paper.

3. The proposed incentive mechanism for mobile crowdsourcing systems

In this section, we propose a truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems. We give the system model firstly. Platform announces a set

$\Phi = (\varphi_1, \varphi_2, ..., \varphi_n)$ of tasks for workers to select. According to the selected task φ_j, worker i has a *contribution value* $v_{i,j} > 0$ to the platform, and also has an *associated cost* $c_{i,j}$, which is private and other workers do not know it. Worker i's *bidding* is represented by $b_{i,j}$, where $b_{i,j}$ is the reserved price that worker i wants to get. We set $t_{i,j}$ as the *sensing time* of worker i, which is the number of the time units during which worker i can provide the sensing service. According to φ_j, we define $pr_{i,j}$ as the *privacy sensibility* that worker i announced. And $tr_{i,j}$ describes worker i's *trust degree*, which is computed by platform according to worker i's historical information. Based on the special task, worker i first submits $b_{i,j}$ and $pr_{i,j}$ to the platform. Upon receiving biddings and sensing plans from workers, the platform computes his trust degree $tr_{i,j}$, and selects a *subset of workers as winners* W_j and determines the *payment* $p_{i,j}$ for worker i. Therefore, the *utility of worker i* based on the submitted sensing plan is shown by Eq. (1).

$$u_{i,j} = \begin{cases} p_{i,j} - c_{i,j}, & if\ i \in W_j \\ 0, & otherwise \end{cases} \tag{1}$$

In practical applications, the sensing time satisfies: $t_{i,j} \geq 0$, where $t_{i,j} = 0$ indicates that worker i does not participate in φ_j. In our mobile crowdsourcing, the cost of worker i is defined as $c_{i,j} = \tau \times t_{i,j}$, where τ is the unit cost when sensing tasks, and $0 < \tau < 1$. In addition, $p_{i,j}$ is determined by sensing time $t_{i,j}$ and the budget B_j, where B_j is *the budget* for φ_j determined by the platform.

In Eq. (1), $c_{i,j}$ is determined by $t_{i,j}$ and τ. However, the sensing time $t_{i,j}$ may change after sensing φ_j, which will lead to the change of $c_{i,j}$. Thus, the *actual utility* of worker i after sensing φ_j is obtained by Eq. (2).

$$u_{i,j}' = \begin{cases} p_{i,j} - c_{i,j}', & if\ i \in W_j \\ 0, & otherwise \end{cases} \tag{2}$$

where $c_{i,j}'$ indicates the *actual cost* that computed by $c_{i,j}' = \tau \times t_{i,j}'$, and $t_{i,j}'$ means the *actual sensing time* of work i. In our system model, we determine $p_{i,j}$ by Eq. (3).

$$p_{i,j} = \frac{t_{i,j}}{T_j} \times B_j \tag{3}$$

where T_j expresses the *total sensing time* for φ_j, and it satisfies: $\frac{B_j}{T_j} \geq 1$. Thus, the *utility of platform* is determined by Eq. (4) according to φ_j.

$$\bar{u_j} = V(W_j) - P(W_j) \tag{4}$$

where $V(W_j) = \sum_{i \in W_j} v_{i,j}$ indicates the *total utility of platform*, and $P(W_j) = \sum_{i \in W_j} p_{i,j}$ expresses the *total payments for workers*. And $v_{i,j}$ means the *specific contribution* that worker i brings to this mobile crowdsourcing system.

3.1. The improved two-stage auction algorithm-TATP

In this paper, we propose an improved two-stage auction algorithm based on *trust degree* and *privacy sensibility* (TATP). The proposed improved two-stage auction algorithm is designed to determine winners in real-time for platform. In our previous proposed auction algorithm ITA [31], the two-stage auction algorithm was improved. However, ITA failed to consider worker's trust degree and privacy sensibility. In order to improve the efficiency of system, we consider the trust degree and privacy sensibility when designing auction algorithm. Let $tr_{i,m}$ be the *global trust degree* of worker i in his mth crowd sensing, it will be computed by platform according to the historic behaviors of worker i. In this paper, we compute $tr_{i,m}$ based on worker i's historic behaviors and time decay factor, which is shown by Eq. (11).

$$tr_{i,m} = \begin{cases} \frac{\sum_{j=1}^{m-1} tr_i^j \cdot \beta_j}{\sum_{j=1}^{m-1} \beta_j}, m \neq 0 \\ 0, m = 0 \end{cases} \tag{5}$$

where tr_i^j represents the *specific trust degree* of worker i according to his jth crowd sensing result, m is the total times of crowd sensing for worker i. And β_j indicates time decay factor in the jth crowd sensing, which is given based on Ebbinghaus Forgetting Curve [32]. With the passage of time, the influence of history mutual information weakens gradually. It decays to a stable value that tends to 0, as shown by Eq. (6)

$$\beta_j = \begin{cases} 1, j = m \\ e^{-\frac{1}{j}}, 1 \leq j < m \end{cases} \tag{6}$$

The changing rule of time decay factor is that if the time is closer to the current transaction, the influence is greater to the current transaction, the smaller the contrast. In real situation, bidders have different privacy sensitivities. In this mechanism, worker i will announce his privacy sensibility $pr_{i,m}$ when uploading his biddings to platform.

In this stage, worker i will upload their biddings to platform, which include $b_{i,m}$, $pr_{i,m}$. After receiving biddings, platform will compute worker i's trust degree $tr_{i,m}$. Let Tr_m be the *bound trust degree* of φ_m, and Pr_m be the *bound privacy sensibility* of φ_m. According to φ_m, when worker i uploads his bidding, platform will judge whether his trust degree and privacy sensibility satisfy following conditions: $tr_{i,m} \geq Tr_m$ and $pr_{i,m} \leq Pr_m$.

TATP improves traditional two-stage auction by solving the unfairness problem for earlier arriving workers and improve the efficiency and truthfulness of auction. We divide the auction stage into two stages, which is summarized in Algorithm 1 according to task φ_m. The first stage is the sample collection stage that establishes the base for the second stage, which is shown between Lines 1–14 in Algorithm 1. Different from the traditional two-stage auction algorithm, the first batch of workers also have chance to win the auction in order to solve the unfairness problem. This design can encourage workers to arrive in time. The second stage is the competition stage shown between Lines 15–27 in Algorithm 1 that adjusts the bidding threshold in each transaction dynamically based on the result from the sample collection stage. The specific process is shown as follows.

1. The platform announces budget B_m for φ_m and the maximal sensing time T_m, based on which by combining the historic experience, the platform determines threshold κ_m for biddings.
2. The platform determines *marginal budget* B_m' for stage 1 based on T_m and B_m. Let $P_m{}' = \sum_{i \in W_m} p_{i,m}$ be the payment sum in stage 1, where W_m represents the *winner set* according to φ_m. If $\frac{b_{i,m}}{t_{i,m}} \leq \kappa_m$, and $tr_{i,m} \geq Tr_m$, $pr_{i,m} \leq Pr_m$, the platform will accept worker i, otherwise, the platform will reject worker i. This process is repeated in stage 1 until $P_m{}' > B_m'$. In addition, Line 2 expresses the value of B_m' based on the *multiple-stage sampling-accepting* process [19] which determines the sample size dynamically. We also define T_m' as the limited time in stage 1, which is shown by Line 3.
3. After stage 1, the auction enters stage 2. We obtain the total utility of the platform $V(W_m)$ in stage 1 in Line 11. In stage 2, for new arriving worker j, $v_{j,m}$ is shown by Line 20, where $v_{j,m}$ represents the marginal utility of platform, as well as the specific contribution value that worker j brings to platform. With new arriving workers, we also judge whether their trust degrees and privacy sensibilities satisfy corresponding conditions, which is shown by Line 21. Then platform will adjust the bidding threshold each time based on marginal density.

Algorithm 1 Improved two-stage auction algorithm (TATP).

Input:

n, B_m, T_m, κ_m, Tr_m, Pr_m

Output:

Winners

1: Stage 1:
2: $B'_m = \lfloor \frac{B_m}{2^{\lfloor \ln T_m \rfloor}} \rfloor$;
3: $T'_m = \lfloor \frac{T_m}{2^{\lfloor \ln T_m \rfloor}} \rfloor$;
4: $i = 1$; $P'_m = 0$; $V(W_m) = 0$;
5: **while** $i \le n$ and $P' \le B'_m$ **do**
6: $b_{i,m} = b_{i,m}$; $t_{i,m} = t_{i,m}$; $tr_{i,m} = tr_{i,m}$; $pr_{i,m} = pr_{i,m}$;
7: **if** $\frac{b_{i,m}}{t_{i,m}} \le \kappa_m$, $b_{i,m} \le p_{i,m}$, $tr_{i,m} \ge Tr_m$ and $pr_{i,m} \le Pr_m$ **then**
8: $W_m \leftarrow W_m \bigcup \{i\}$;
9: $p_{i,m} \leftarrow \frac{t_{i,m}}{T_m} \times B_m$;
10: $P'_m \leftarrow P'_m + p_{i,m}$;
11: $V(W_m) \leftarrow V(W_m) + v_{i,m}$;
12: **end if**
13: $i \leftarrow i + 1$;
14: **end while**
15: Stage 2:
16: $P(W_m) \leftarrow P'_m$;
17: $j = 1$;
18: **while** $j \le n$ and $P(W_m) \le B_m$ **do**
19: $b_{j,m} = b_{j,m}$; $t_{j,m} = t_{j,m}$; $tr_{j,m} = tr_{j,m}$; $pr_{j,m} = pr_{j,m}$;
20: $v_{j,m} = V(W_m \bigcup \{j\}) - V(W_m)$; $p_{j,m} = \frac{t_{j,m}}{T_m} \times B_m$;
21: **if** $\frac{v_{j,m}}{p_{j,m}} \ge \frac{V(W_m)}{P(W_m)}$, $b_{j,m} \le p_{j,m}$, $tr_{j,m} \ge Tr_m$ and $pr_{j,m} \le Pr_m$ **then**
22: $W_m \leftarrow W_m \bigcup \{j\}$;
23: $P(W_m) \leftarrow P(W_m) + p_{j,m}$;
24: $V(W_m) \leftarrow V(W_m) + v_{j,m}$;
25: **end if**
26: $j \leftarrow j + 1$;
27: **end while**

In this paper, we utilize *marginal utility* to determine whether accept the worker [31]. Therefore, the density of marginal utility for worker j is $\frac{v_{j,m}}{p_{j,m}}$, which can reflect the increasing density or diminishing density. If $\frac{v_{j,m}}{p_{j,m}} \ge \frac{V(W_m)}{P(W_m)}$, $b_{j,m} \le p_{j,m}$, $tr_{j,m} \ge Tr_m$ and $pr_{j,m} \le Pr_m$, the platform accepts worker j, otherwise, it rejects worker j, which are shown from Lines 21 to 25. Once a new worker arrives, the platform computes its marginal density each time, and compares its marginal density with the previous workers' global result. This process is repeated until $\sum_{j \in W_m} p_{j,m} > B_m$.

3.2. The proposed $k - \varepsilon$-differential privacy-preserving

In this paper, we propose $k - \varepsilon$-differential privacy-preserving through combining k-anonymity and ε-differential privacy-preserving. According to worker's location privacy, we research k-anonymity privacy-preserving, and add Gaussian white noise into differential privacy-preserving.

In this paper, we apply personalized location k-anonymity to protect worker's location information. According to the location information l_i of worker i, the location anonymity server transforms each message received from worker into a perturbed message L_i that can be safely forwarded to the location-based Service (LBS) provider. We denote the set of location information received from workers as S. According to worker i, his locations l_i in set S is shown as follows.

$l_i \in S : \langle i, \{tc_i, x_i, y_i\}, k, \{d_{tc_i}, d_{x_i}, d_{y_i}\} \rangle$.

This location information l_i contains following contents: tc_i, x_i and y_i denote the 3D spatio-temporal location point of this message. The coordinate (x_i, y_i) refers to the spatial position of worker i in the 2D space, and the time stamp tc_i refers to the time point at which worker i was present at that position. The k value of the location information indicates the desired minimum anonymity level and hence $k \ge 1$. Therefore, $k = 1$ indicates that anonymity is not required for the location information. When $k > 1$, it means that the perturbed message will be assigned a spatio-temporal cloaking box that is indistinguishable from at least $k - 1$ other perturbed messages, each from a different worker. Thus, larger k values indicate higher privacy degrees. d_{tc_i}, d_{x_i} and d_{y_i} represent the tolerance that the perturbed message should have a spatio-temporal cloaking box whose projection on the spatial dimension and temporal dimension does not contain any point more than corresponding d_{tc_i}, d_{x_i} and d_{y_i} distance away from tc_i, x_i and y_i. These three parameters are determined by workers' preferences with regard to QoS. Larger spatial tolerance indicates less accurate results for worker's location. Similarly, larger temporal tolerance indicates higher latencies of worker's location information. According to spatio-temporal tolerance, the cloaking intervals should be $\Phi(tc_i, d_{tc_i}) = [tc_i - d_{tc_i}, tc_i + d_{tc_i}]$, $\Phi(x_i, d_{x_i}) = [x_i - d_{x_i}, x_i + d_{x_i}]$ and $\Phi(y_i, d_{y_i}) = [y_i - d_{y_i}, y_i + d_{y_i}]$. In this paper, we define $B_{con}(l_i)$ as the *spatio-temporal constraint box* of worker i's location information, where $B_{con}(l_i) = (\Phi(tc_i, d_{t_i}), \Phi(x_i, d_{x_i}), \Phi(y_i, d_{y_i}))$.

In order to protect worker's location information, we define L_i as the perturbed or anonymized location information. We denote the set of perturbed or anonymized location information as I. According to worker i, his perturbed or anonymized location information L_i in set S is shown as follows:

$L_i \in I : \langle i, \{[tc_i^{\min}, tc_i^{\max}], [x_i^{\min}, x_i^{\max}], [y_i^{\min}, y_i^{\max}]\} \rangle$.

According to l_i and L_i, there exists mapping between them which is represented as $L_i = R(l_i)$. Correspondingly, $B_{clo}(L_i)$ is defined as the *spatio-temporal cloaking box* of worker i's location information. Therefore, $B_{clo}(L_i)$ is expressed as $B_{clo}(L_i) = ([tc_i^{\min}, tc_i^{\max}], [x_i^{\min}, x_i^{\max}], [y_i^{\min}, y_i^{\max}])$.

In this mechanism, l_i in S and L_i in I satisfy the following properties according to worker i' location information.

1. *Spatial containment*: $x_i \in [x_i^{\min}, x_i^{\max}]$, $y_i \in [y_i^{\min}, y_i^{\max}]$.
2. *Spatial resolution*: $[x_i^{\min}, x_i^{\max}] \subseteq \Phi(x_i, d_{x_i})$, $[y_i^{\min}, y_i^{\max}] \subseteq \Phi(y_i, d_{y_i})$.
3. *Temporal containment*: $tc_i \in [tc_i^{\min}, tc_i^{\max}]$.
4. *Temporal resolution*: $[tc_i^{\min}, tc_i^{\max}] \subseteq \Phi(tc_i, d_{tc_i})$.

Spatial containment and temporal containment signify that the spatio-temporal cloaking box $B_{clo}(L_i)$ contains the real position of worker i: (tc_i, x_i, y_i). Spatial resolution and temporal resolution indicate that the spatio-temporal cloaking box $B_{clo}(L_i)$ contains the spatio-temporal constraint box $B_{con}(l_i)$, that is to say, $B_{con}(l_i) \subseteq B_{clo}(L_i)$.

According to the above analysis, we can denote that this mechanism is *location k-anonymity*. The k-anonymity requirement demands that, for the perturbed location information $L_i = R(l_i)$ of worker i, there exist at least $k - 1$ other perturbed location information with the same spatio-temporal cloaking box, each from a different worker. We give an example in Fig. 2 to prove its property of location k-anonymity. In this example, there are two spatio-temporal cloaking boxes, which are shown as area A and area B. In area A, there are five workers, $k = 5$, and their routes are denoted as r_1, r_2, r_3, r_4 and r_5. If no personalized location k-anonymity is applied in mobile crowdsourcing systems, the following linking attack can be easily performed by an adversary. For a worker, if he has been spotted at the position marked x, then the route r_2 can be associated with this worker since no other route cross the point x.

However, if the personalized location k-anonymity is applied in this mobile crowdsourcing system, the worker cannot be

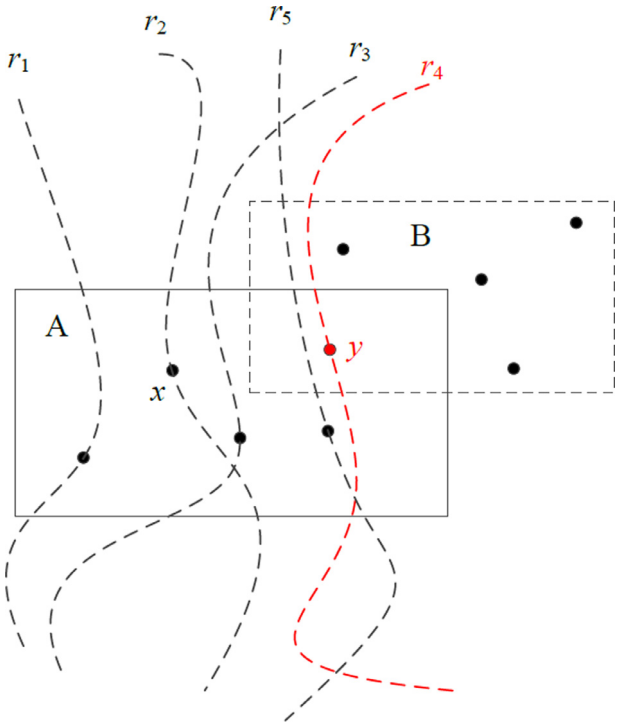

Fig. 2. Linking attack.

associated with the point x because of the location perturbation. Point x is included in the spatio-temporal cloaking box, so the linking attack is not effective in this mechanism. Therefore, even if the attacker can infer approximate routes, he cannot link the identity binding with one of the routes with certainty because the point x links with five different location information, each with probability $k^{-1} = \frac{1}{5}$. By applying this mechanism, attacker cannot associate location information with the right worker. Therefore, this mechanism is location k-anonymity.

Through above analysis, this personalized location k-anonymity has following properties.

1. *Spatial containment.*
2. *Spatial resolution.*
3. *Temporal containment.*
4. *Temporal resolution.*
5. *Location k-anonymity.*

However, in Fig. 2, we can see that the worker with route r_4 is included in both A and B spatio-temporal cloaking box. It is easy to link route r_4 with this worker for attackers because there is only one worker included in these two spatio-temporal cloaking boxes. Therefore, in order to solve this problem, we improve personalized location k-anonymity based on *Clique* (LKAC). In order to solve the overlapping problem, workers should select his preferred area, *i.e.*, spatio-temporal cloaking box. Therefore, the desired minimum anonymity level k should be changed dynamically. For example, in Fig. 2, if the worker with route r_4 selects area B as his spatio-temporal cloaking box, we could set $k(A) = 4$ and $k(B) = 5$. Therefore, worker i's location information l_i in set S is improved as follows:

$l_i \in S : \langle i, \{tc_i, x_i, y_i\}, k_i, \{d_{tc_i}, d_{x_i}, d_{y_i}\}\rangle$, where k_i is different according to different workers.

Because in mobile crowdsourcing system, the privacy degree and task assignment are two contradictory problems, we should balance workers' privacy preserving and task assignment. Therefore, how to determine the value of k is the key problem in real applications. The determination for k depends on the types of mobile crowdsourdcing systems, *e.g.*, some mobile crowdsourcing systems need to know workers' locations to assign sensing tasks. Therefore, if the privacy degree is high, it is hard to assign suited tasks for workers. According to this problem, we will further discuss the selection for k in future.

However, in the case of continuous attack, k-anonymity still has the risk of privacy leak. In addition, if the attacker has some background knowledge about the worker, worker's location also can be identified accurately. Therefore, in order to solve homogeneity attack problem, we combine the proposed location k-anonymity and ε-differential privacy-preserving to protect worker's location information. In a location range, we apply location k-anonymity into this privacy-preserving, thus the probability to find this worker is $\frac{1}{k}$. Then, we improve differential privacy-preserving to combine with location k-anonymity in order to solve homogeneity attack problem in mobile crowdsourcing systems.

Lemma 1. *For two datasets D_1 and D_2, the difference between them is up to one record. Let Range(K) represent the range of random function K, $Pr[E_v]$ is the leaking risk of event E_v. If K provides ε-differential privacy-preserving, the ε-differential privacy-preserving should satisfy Eq. (7), and $V \subseteq Range(K)$.*

$$Pr[K(D_1) \in V] \leq exp(\varepsilon) \times Pr[K(D_2) \in V] \tag{7}$$

Fig. 3(a) shows the curves of privacy leaking risk on D_1 and D_2, which there is up to one record difference between these two data sets. The random function K is not related with attacker's knowledge. As long as K meets Lemma 1, it can protect data privacy in dataset, although attacker has obtained all the other data. Let f be the query function, X be the dataset, and $f(X)$ be the real query result. The function K can protect data privacy through adding suitable random noise on $f(X)$. Therefore, K is ε-differential privacy-preserving function. The response value of K is computed by Eq. (8), where $\triangle f$ indicates the sensitivity of f. $Gau(\frac{\triangle f}{\varepsilon})$ indicates Gaussian white noise, and h is system parameter. The calculated method of $\triangle f$ is shown by Eq. (9).

$$f(X) + \left(Gau\left(\frac{\triangle f}{\varepsilon}\right)\right)^h \tag{8}$$

$$\triangle f = \max_{D_1, D_2} \| f(D_1) - f(D_2) \| \tag{9}$$

According to most of query functions f, $\triangle f$ is very small. Sensitivity is an important property of function f, which is not related with dataset. Therefore, we will not discuss $\triangle f$ in this paper.

In this paper, we utilize Gaussian white noise to research ε-differential privacy-preserving. Gaussian white noise is statistical noise having a Probability Density Function (PDF) equal to that of the normal distribution, which is also known as the Gaussian distribution. In other words, the values that the noise can take on are Gaussian-distributed. According to normal distribution property of Gaussian white noise, the noise function is shown by Eq. (10). It obeys $N(0, \varepsilon^2)$ normal distribution. The added noise is proportional to $\triangle f$, and inversely proportional to ε. That is to say, when $\triangle f$ is smaller, the performance of algorithm is better because of less added-noise.

$$Gau\left(\frac{\triangle f}{\varepsilon}\right) = \frac{1}{\sqrt{2\pi}\varepsilon} exp\left(-\frac{x^2}{2\varepsilon^2}\right) \tag{10}$$

Through adjusting the value of ε, the privacy-preserving level could be adjusted. When ε is smaller, the curve is more flat. The changing curves of Gaussian white noise is shown in Fig. 3(b). Therefore, if ε is smaller, the added noise is more, *i.e.*, the privacy-preserving level is higher. We divide privacy-preserving levels through adjusting the value of ε in this paper. Therefore, through

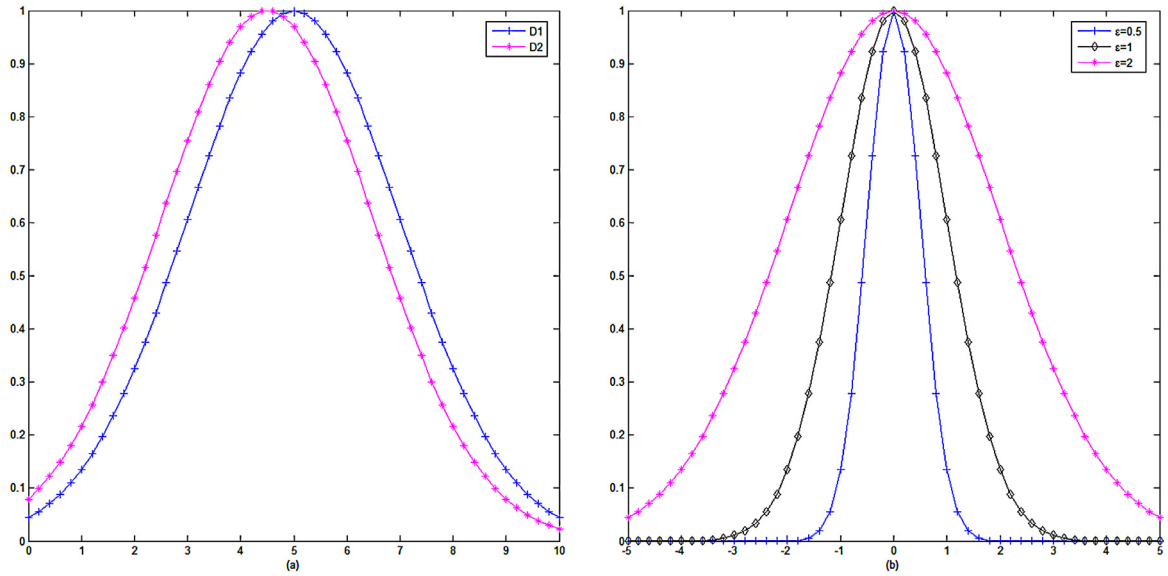

Fig. 3. (a) The curves of privacy leaking risk on D1 and D2. (b) The probability density functions of Gaussian white noise.

adding Gaussian white noise into the personalized location k-anonymity, the proposed $k-\varepsilon$-differential privacy-preserving is obtained.

Theorem 1. *The proposed $k-\varepsilon$-differential privacy-preserving is ε-differential privacy-preserving.*

Proof. For two location ranges L_1 and L_2, which there is up to one record difference between these two location ranges. We give the following proof: $\frac{Pr[K(L_1)\in V]}{Pr[K(L_2)\in V]} = \frac{p(x-f(L_1))}{p(x-f(L_2))} = \frac{\prod_{i=1}^{k} p(x_i-f(L_1)_i)}{\prod_{i=1}^{k} p(x_i-f(L_2)_i)} = \frac{\prod_{i=1}^{k} \frac{1}{\sqrt{2\pi}\varepsilon} exp(-\frac{(x_i-f(L_1)_i)}{2\varepsilon^2})}{\prod_{i=1}^{k} \frac{1}{\sqrt{2\pi}\varepsilon} exp(-\frac{(x_i-f(L_2)_i)}{2\varepsilon^2})} = exp(\frac{\sum_{i=1}^{k}((x_i-f(L_2)_i)^2-(x_i-f(L_1)_i)^2)}{2\varepsilon^2}) = exp(\varepsilon \cdot \frac{\sum_{i=1}^{k}((x_i-f(L_2)_i)^2-(x_i-f(L_1)_i)^2)}{2\varepsilon^3}) \le \exp(\varepsilon)$. Because of independence, the multiplication could be revised as addition according to the fourth equality. According to the continuous attack, *i.e.*, tracking work's trajectory, this method can prevent worker's location information from being leaked through adding noise. Therefore, the proposed $k-\varepsilon$-differential privacy-preserving is ε-differential privacy-preserving. □

3.3. Properties of the proposed incentive mechanism

Lemma 2. *The proposed incentive mechanism is computationally efficient.*

Proof. Let n be the total number of crowd workers. The while-loop is of $O(n)$ time complexity at most in TATP, *i.e.*, the proposed auction algorithm can be computed in polynomial time. Therefore, the proposed incentive mechanism is computationally efficient. □

Lemma 3. *The proposed incentive mechanism is individually rational.*

Proof. In our mobile crowdsourcing, the platform pays sensing worker i before performing sensing task φ_j, *i.e.*, the *ex-ante* case. Therefore, worker i will obtain payment $p_{i,j} = \frac{t_{i,j}}{T_j} \times B_j$. We have defined $\frac{B}{T} \ge 1$ in Eq. (3), and $c_{i,j} = \tau \times t_{i,j}$, $0 < \tau < 1$. The utility of worker i is $u_{i,j} = p_{i,j} - c_{i,j} = (\frac{B_j}{T_j} - \tau) \times t_{i,j} > 0$, thus, the proposed incentive mechanism is individually rational. □

Lemma 4. *The proposed incentive mechanism is profitable.*

Proof. For a sensing task φ_j, we have $\bar{u_j} > 0$. In TATP, the trust degree $tr_{i,j}$ of worker i who wants participate φ_j, will be considered. Workers should behave truthfully in order to increase their trust degrees, so that participate more sensing tasks. Therefore, platform will have nonnegative utility, *i.e.*, the proposed incentive mechanism is profitable. □

Lemma 5. *The proposed incentive mechanism is truthful.*

Proof. In TATP, workers will behave truthfully in order to participate more sensing tasks. Once they behave unreliably, their trust degrees will decrease, which leads to be rejected by platform. Thus, the proposed incentive mechanism is truthful. □

4. Performance evaluation

In this section, we conduct corresponding experiments to evaluate the effectiveness of the proposed incentive mechanism. First of all, we verify the efficiency of TATP through comparing it with other classic auction algorithms. Then, the effectiveness of the proposed privacy-preserving is verified by utilizing two data sets of mobility traces of taxis in Beijing and New York.

All the experiments were conducted on Windows 10 operating system with Intel Core (TM) Duo 2.66 GHz CPU, 12GB Memory and Matlab 7.0 simulation platform. All the experiments are event-based simulations. Each measurement is averaged over 50 instances.

4.1. The effectiveness of TATP

In order to verify the efficiency of TATP, we simulate three tasks with different budgets and required total sensing times. The budgets of the three tasks are set to be 50, 100 and 200 respectively. Accordingly, the required total sensing times are set to be 25, 50 and 100 respectively. The numbers of worker candidates are 40, 60 and 80 respectively. In these experiments, we set $\kappa = 2$, $Tr_m = 0.5$ and $Pr_m = 5$ based on the expertise. In order to specialize the settings of parameters, we set the corresponding parameters in Table 1.

In these simulations, we compare the proposed two-stage auction algorithm TATP with a general auction algorithm, a traditional two-stage auction algorithm and an improved two-stage auction algorithm ITA. The general auction algorithm has a defined

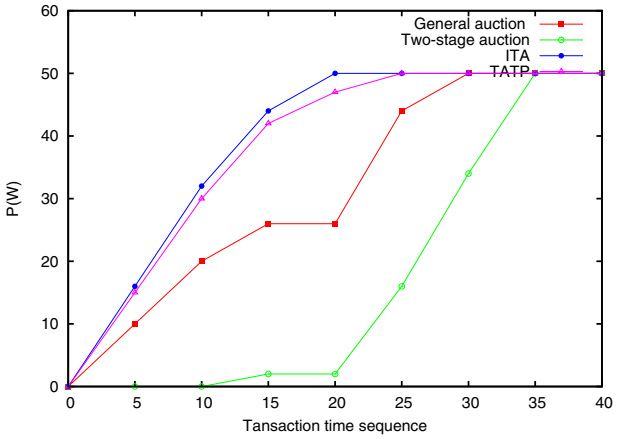

Fig. 4. The comparison of auction efficiencies when task budget is 50.

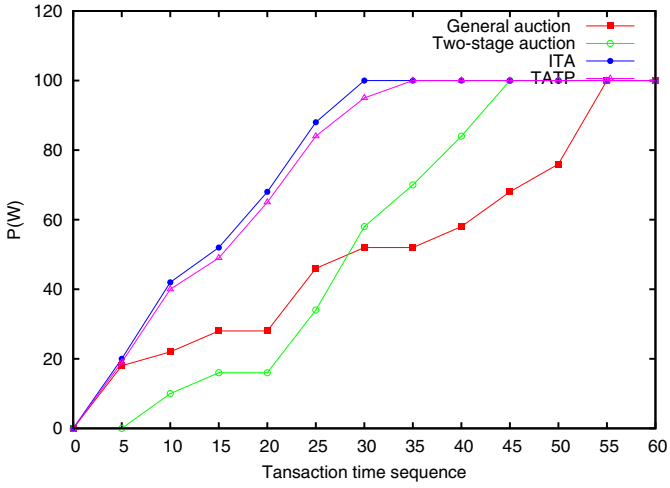

Fig. 5. The comparison of auction efficiencies when task budget is 100.

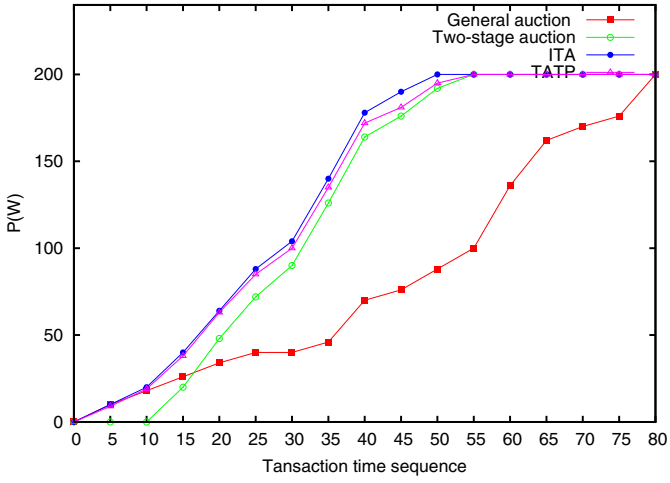

Fig. 6. The comparison of auction efficiencies when task budget is 200.

Table 1
The settings of parameters for TATP.

	First group	*Second group*	*Third group*
n	40	60	80
B_m	50	100	200
T_m	25	50	100
κ	2	2	2
Tr_m	0.5	0.5	0.5
Pr_m	5	5	5

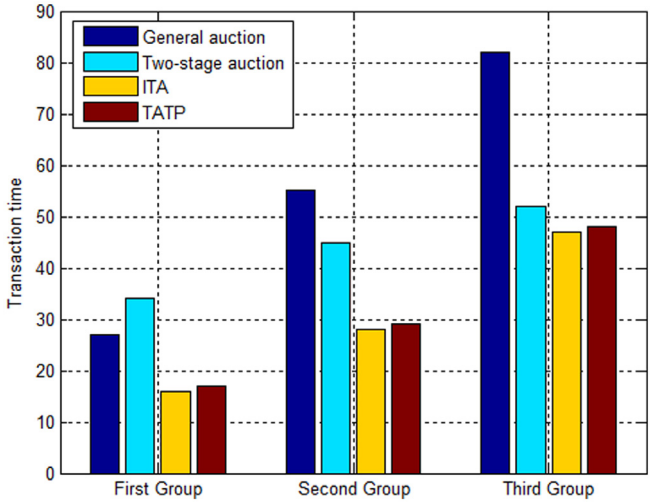

Fig. 7. The comparative results of time consumptions.

threshold. Once the bidding from a worker exceeds this threshold, the platform will reject this worker, otherwise, it will accept this worker. We select the auction algorithm in [33] as the general auction algorithm to compare in the comparison experiments. The traditional two-stage auction algorithm, in [18], rejects the first batch of workers which is used as the sample. The improved two-stage auction algorithm ITA was proposed by our contribution [31], however does not consider trust degree and privacy sensibility. In order to compare the efficiencies of the algorithms better, we compute the total payments for the workers: $P(W)$ in these simulations. The x-coordinate indicates the transaction time sequence, and y-coordinate shows the values of $P(W)$. Under different budgets, the algorithm has higher efficiency which can reach the budget value faster. Therefore, through the comparison on the values of $P(W)$, we can deduce the efficiencies that the task be completed under different algorithms.

Fig. 4 expresses the comparison of auction efficiencies when task budget is 50. From the experimental results, it can be seen that ITA and TATP has the best auction efficiencies, and traditional two-stage auction performs worst. This is because that the traditional two-stage auction algorithm discards some early arriving workers, so that they have to take more time to complete a task. In addition, the proposed TATP performs not better than ITA, this is because that we consider trust degree and privacy degree in TATP. Some workers may be rejected because of unsatisfied trust degree or privacy degree. However, the whole trust degree of mobile crowdsourcing systems could be improved under TATP.

Fig. 5 expresses the comparison of auction efficiencies when task budget is 100. From the experimental result, we can see that ITA and TATP also have the best performances. Before 27 rounds, general auction algorithm performs better than traditional two-stage auction algorithm. However, after 27 rounds, traditional two-stage auction algorithm has better performance compared with general auction algorithm. The cause is that the traditional two-stage auction algorithm discards some early arriving workers in the initial several rounds, after that, it performs better than general auction algorithm.

Fig. 6 expresses the comparison of auction efficiencies when task budget is 200. The experimental result also indicates that ITA and TATP can obtain the best results. However, if the required total sensing time is long enough, traditional two-stage auction algorithm performs better than general auction algorithm. In addition, from Fig. 6, it can be seen that ITA, TATP and the traditional two-stage auction algorithm have the similar experimental results

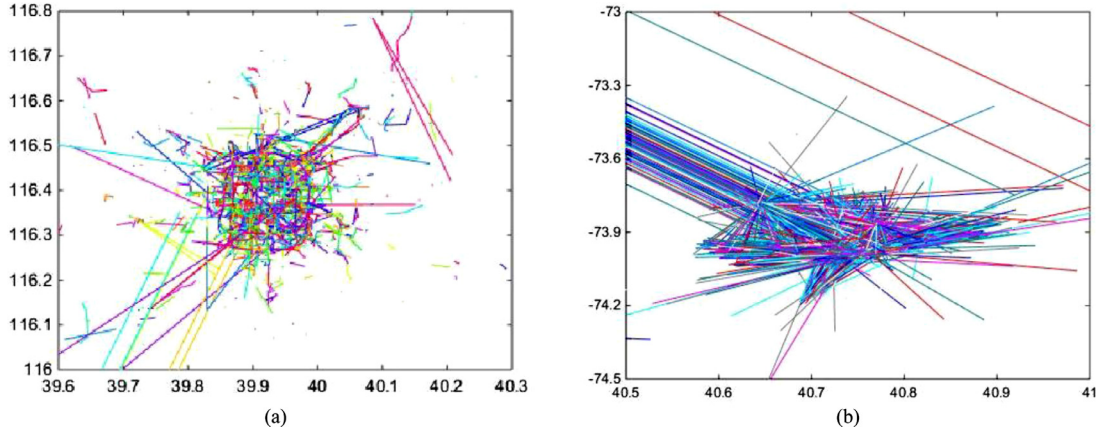

Fig. 8. (a) The data set of mobility traces of taxi cabs in Beijing. (b) The data set of mobility traces of taxi cabs in New York.

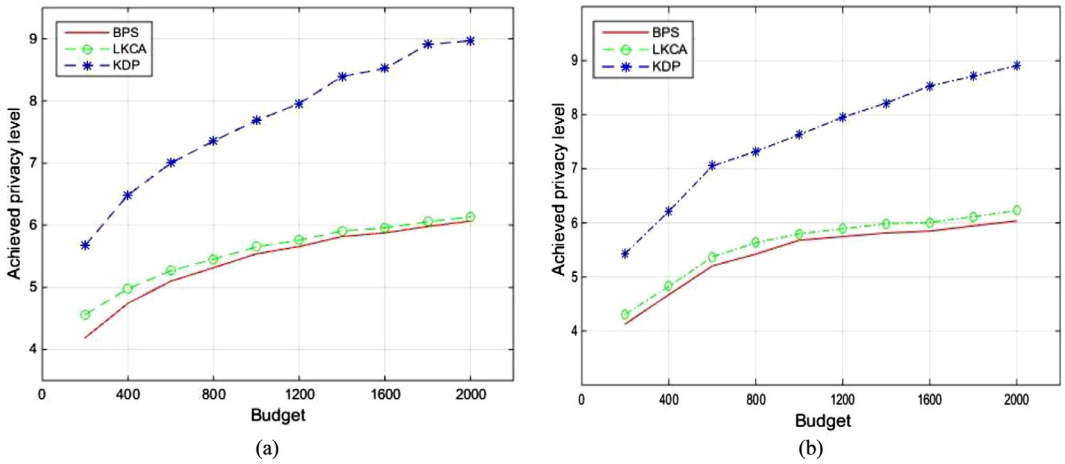

Fig. 9. (a) The comparison experiment for privacy levels with different budgets on Beijing data set. (b) The comparison experiment for privacy levels with different budgets on New York data set.

under this condition. This is because that the discarded earlier transactions have little influence to the experimental result if the budget and required total sensing time are adequate.

In order to compare the efficiencies better, we design an experiment to show the transaction times with different auction algorithms and budgets which is shown by Fig. 7. In Fig. 7, the actual time consumptions of the four algorithms under different conditions are shown, which corresponds to 50, 100 and 200 required total sensing time respectively. We can see that ITA and TATP can always the highest efficiencies compared with other two auction algorithms. However, TATP can guarantee the truthfulness of mobile crowdsourcing system compared with ITA.

4.2. The effectiveness of $k - \varepsilon$-differential privacy-preserving

In this paper, we utilize two data sets of mobility traces of taxis in Beijing and New York to verify the effectiveness of the proposed $k - \varepsilon$-differential privacy-preserving. The two data sets contain GPS coordinates of approximately 2000 taxis collected over 10 min intervals respectively. Each trajectory is marked by a sequence of time-stamped GPS points that contain taxi driver id, time stamp, and drivers' position (latitude and longitude). Fig. 8(a) shows the traces of taxi cabs in Beijing, and the traces of taxi cabs in New York are described by Fig. 8(b).

According to the privacy metrics proposed in [34], which is based on the entropy theory. Entropy is a measure of unpredictability in information theory. Let X be the set of selected workers. We denote that in a time slot T, worker i has uploaded a total amount of data is d_i. The total amount of data collected is denoted as $D_T(X)$. Consider that we have D pieces of uploaded data tagged with locations, privacy is maximized when the platform sees all workers with equal probability of reporting a piece of data. In this way, the platform will not identify the owner of the data. Therefore, the degree of anonymity depends on the distribution of the probabilities for the D pieces of uploaded data tagged. Let $H(X)$ be the privacy level provided by selecting X. The evaluation method for privacy level is shown in Eq. (11).

$$H(X) = -\sum_{i \in X} \frac{d_i}{D_T(X)} \log_2 \frac{d_i}{D_T(X)} \tag{11}$$

We compare our proposed privacy-preserving mechanism for locations, referred as KDP in figure, with the location k-anonymity based on *Clique* (LKAC) method and location-based Service (BPS) method proposed by Zhang et al. [35]. According to Beijing data set and New York data set, we compare the three methods with different budgets respectively. Fig. 9(a) shows the comparison result on Beijing data set. In this experiment, x-coordinate represents different budget amounts, and y-coordinate indicates privacy levels. From the comparison results, we can see that the privacy levels

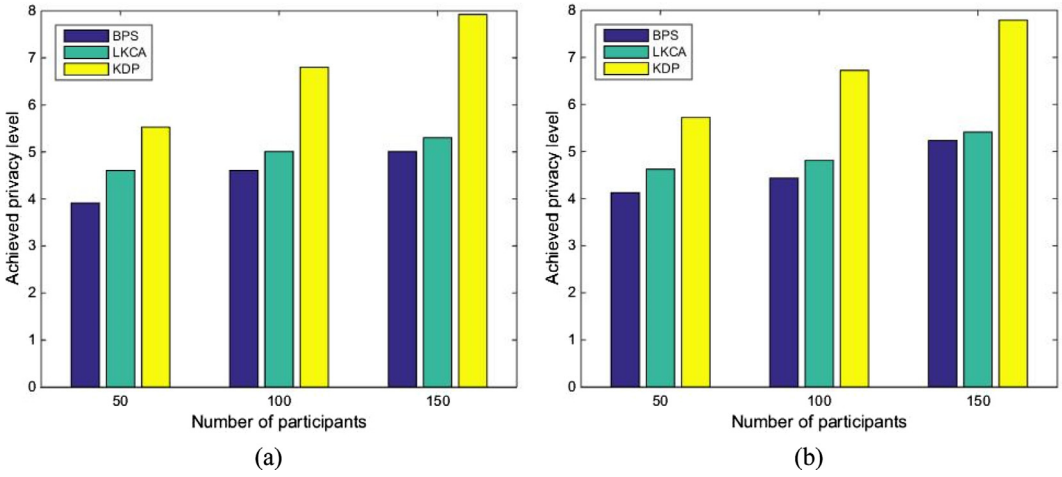

Fig. 10. (a) The comparison experiment for privacy levels with different numbers of participants on Beijing data set. (b) The comparison experiment for privacy levels with different numbers of participants on New York data set.

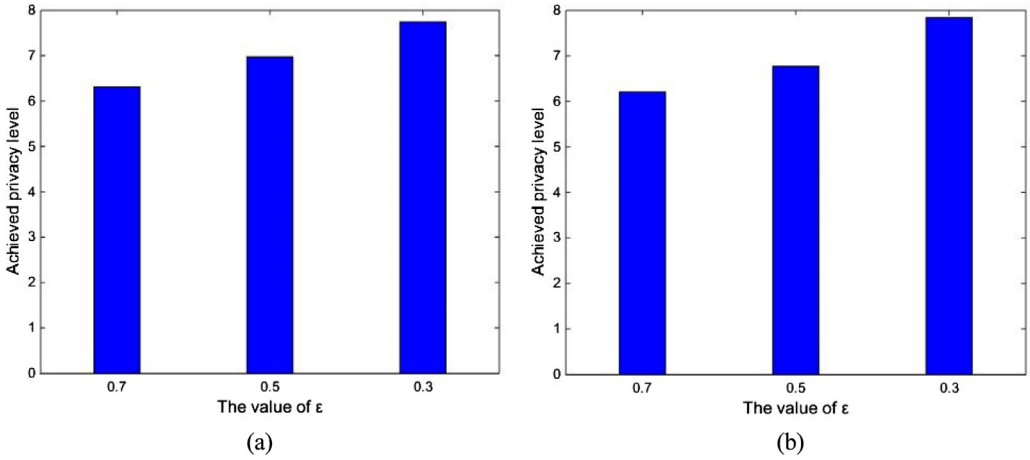

Fig. 11. (a) The influences for privacy levels with different values of ε on Beijing data set. (b) The influences for privacy levels with different values of ε on New York data set.

increase with the increase of budget. When compared with LKAC method and BPS method, the proposed KDP has higher privacy level. And the comparison result on New York data set is shown in Fig. 9(b). From Fig. 9(b), it also can be seen that the proposed KDP has better privacy level through compared with LKAC and BPS. The reason is that KDP has better performance for mobility traces, especially for continuity attack and some background knowledge.

We also compare the privacy levels with different numbers of participants, which are set as 50, 100 and 150 respectively. According to the two data sets, the experimental results are shown by Fig. 10. Fig. 10(a) shows the comparison result on Beijing data set, it can be seen that the proposed KDP has best performance through compared with LKAC and BPS methods. With the arriving of participants, the privacy levels also increase under the three methods. And the comparison result on New York data set is shown in Fig. 10(b). From the experimental result, we can see that KDP also has better privacy-preserving performance than LKAC and BPS methods. It also can be seen that with the increase of workers, the privacy information of workers can be protected better.

In addition, the influences for privacy levels with different values of ε are verified by Fig. 11. The experimental result on Beijing data set is shown in Fig. 11(a). According to New York data set, the experimental result is shown in Fig. 11(b). From the results, it can be seen that the privacy-preserving levels could be adjusted through adjusting the values of ε. The results also express that ε is inversely proportional to privacy-preserving level. This is because that if ε is smaller, the added noise is more, *i.e.*, the privacy-preserving level is higher. Therefore, the influence of parameter ε is verified by the experiments.

5. Conclusion

With the development of mobile crowdsourcing systems, how to establish truthful incentive mechanism and effective privacy-preserving become very important. This paper researched the improved two-stage auction algorithm based on trust degree and privacy degree (TATP) to inspire workers to participate tasks and behavior truthfully. In order to protect workers' location privacy, the $k-\varepsilon$-differential privacy-preserving was proposed through combining k-anonymity privacy-preserving and differential privacy-preserving. The efficiency and effectiveness of the proposed incentive mechanism is verified effectively through comparison experiments. In addition, the security is guaranteed under this incentive mechanism.

In future works, we will focus on how to improve the task assignment and auction algorithm. According to the value of k in $k-\varepsilon$-differential privacy-preserving, we will compute it in order to solve the conflict between service quality and privacy protection. In addition, we will further investigate how to compute worker's trust degree effectively in order to guarantee the truthfulness of mobile crowdsourcing systems better.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants No.61502410, No. 61572418, No. 61602399, No. 61702439, No. 61502116, the China Postdoctoral Science Foundation under Grant No. 2017M622691, the National Science Foundation (NSF) under Grants No. 1704287, 1252292, 1741277, the Natural Science Foundation of Shandong Province under Grant No. ZR2014FQ026, No.ZR2016FM42, the Project of Shandong Province Higher Educational Science and Technology Program under Grant No.J15LN09.

References

[1] Z. Duan, W. Li, Z. Cai, Distributed auctions for task assignment and scheduling in mobile crowdsensing systems, in: The 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017), Atlanta, GA, USA, 2017, pp. 635–644, doi:10.1109/ICDCS.2017.121.

[2] Y. Liang, Z. Cai, Q. Han, Y. Li, Location privacy leakage through sensory data, Secur. Commun. Netw. J. (2017) 1–12, doi:10.1155/2017/7576307.

[3] G. Sun, Y. Xie, D. Liao, H. Yu, V. Chang, User-defined privacy location-sharing system in mobile online social networks, J. Netw. Comput. Appl. 86 (2017) 34–45, doi:10.1016/j.jnca.2016.11.024.

[4] Z. He, Z. Cai, J. Yu, Latent-data privacy preserving with customized data utility for social network data, IEEE Trans. Veh. Technol. (2017), doi:10.1109/TVT.2017.2738018.

[5] J. Li, Z. Cai, M. Yan, Y. Li, Using crowdsourced data in location-based social networks to explore influence maximization, in: The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 2016, pp. 1–9, doi:10.1109/INFOCOM.2016.7524471.

[6] G. Sun, V. Chang, Z. Sun, G. Li, H. Yu, D. Liao, Efficient location privacy algorithm for internet of things (IoT) services and applications, J. Netw. Comput. Appl. 89 (2017) 3–13, doi:10.1016/j.jnca.2016.10.011.

[7] L. Zhang, Z. Cai, X. Wang, Fake Mask: a novel privacy preserving approach for smartphones, IEEE Trans. Netw. Serv. Manag. 13 (2016) 335–348, doi:10.1109/TNSM.2016.2559448.

[8] J. Li, Z. Cai, J. Wang, M. Han, Y. Li, Truthful incentive mechanisms for geographical position conflicting mobile crowdsensing systems, IEEE Trans. Comput. Social Syst. 99 (2018) 1–11, doi:10.1109/TCSS.2018.2797225.

[9] J.S. Lee, B. Hoh, Sell your experiences: a market mechanism based incentive for participatory sensing, in: IEEE International Conference on Pervasive Computing and Communications, Mannheim, Germany, 2010, pp. 60–68, doi:10.1109/PERCOM.2010.5466993.

[10] Z. Feng, Y. Zhu, Q. Zhang, L.M. Ni, A.V. Vasilakos, TRAC: truthful auction for location-aware collaborative sensing in mobile crowdsourcing, in: IEEE International Conference on Pervasive Computing and Communications, Mannheim, Germany, 2010, pp. 60–68, doi:10.1109/PERCOM.2010.5466993.

[11] I. Krontiris, A. Albers, Monetary incentives in participatory sensing using multi-attributive auctions, Int. J. Parallel Emerg.Distrib. Syst. 27 (2012) 317–336, doi:10.1080/17445760.2012.686170.

[12] T. Luo, H.P. Tan, L. Xia, Profit-maximizing incentive for participatory sensing, in: The 33rd IEEE Conference on Computer Communications, Toronto, ON, Canada, 2014, pp. 127–135, doi:10.1109/INFOCOM.2014.6847932.

[13] D. Yang, X. Fang, G. Xue, Truthful incentive mechanisms for k-anonymity location privacy, in: The 32nd IEEE Conference on Computer Communications, Turin, 2013, pp. 2994–3002, doi:10.1109/INFCOM.2013.6567111.

[14] L. Gao, F. Hou, J. Huang, Providing long-term participation incentive in participatory sensing, in: The 34th IEEE Conference on Computer Communications, Kowloon, Hong Kong, 2015, pp. 2803–2811, doi:10.1109/INFOCOM.2015.7218673.

[15] D. Yang, G. Xue, X. Fang, J. Tang, Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing, in: The 18th Annual International Conference on Mobile Computing and Networking, Istanbul, Turkey, 2013, pp. 173–184, doi:10.1145/2348543.2348567.

[16] Y. Singer, M. Mittal, Pricing mechanisms for crowdsourcing markets, in: The 22nd International Conference on World Wide Web, Rio de Janeiro, Brazil, 2013, pp. 1157–1166, doi:10.1145/2488388.2488489.

[17] X. Chen, M. Liu, Y. Zhou, Z. Li, S. Chen, X. He, A truthful incentive mechanism for online recruitment in mobile crowd sensing system, Sensors 17 (2017) 79, doi:10.3390/s17010079.

[18] M. Bateni, M. Hajiaghayi, M. Zadimoghaddam, Submodular secretary problem and extensions, ACM Trans. Algorithms 9 (2013) 39–52, doi:10.1145/2500121.

[19] D. Zhao, X. Li, H. Ma, How to crowdsource tasks truthfully without sacrificing utility: online incentive mechanisms with budget constraint, in: The 33rd IEEE Conference on Computer Communications, Toronto, ON, Canada, 2014, pp. 1213–1221, doi:10.1109/INFOCOM.2014.6848053.

[20] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, K. Tan, Private queries in location based services: anonymizers are not necessary, in: The 28th ACM International Conference on Management of Data (SIGMOD), New York, NY, USA, 2008, pp. 121–132, doi:10.1145/1376616.1376631.

[21] B. Niu, Z. Zhang, X. Li, H. Li, Privacy-area aware dummy generation algorithms for location-based services, in: Proceedings of 2014 IEEE International Conference on Communications, Sydney, NSW, Australia, 2014, pp. 957–962, doi:10.1109/ICC.2014.6883443.

[22] B. Gedik, L. Liu, Location privacy in mobile systems: a personalized anonymization model, in: The 25th IEEE International Conference on Distributed Computing Systems, Washington, DC, USA, 2005, pp. 620–629, doi:10.1109/ICDCS.2005.48.

[23] M. Fridman, A. Farsi, Y. Okawachi, A.L. Gaeta, Demonstration of temporal cloaking, Nature 481 (2012) 62–65, doi:10.1038/nature10695.

[24] B. Bamba, L. Liu, Supporting anonymous location queries in mobile environments with privacygrid, in: The 17th International Conference on World Wide Web (WWW'08), Beijing, China, 2008, pp. 237–246, doi:10.1145/1367497.1367531.

[25] B. Gedik, L. Liu, Protecting location privacy with personalized k-anonymity: architecture and algorithms, IEEE Trans. Mob. Comput. 7 (2008) 1–18, doi:10.1109/TMC.2007.1062.

[26] H. Kido, Y. Yanagisawa, T. Satoh, An anonymous communication technique using dummies for location-based services, in: IEEE International Conference on Pervasive Services(ICPS'05), Santorini, Greece, 2005, pp. 88–97, doi:10.1109/PERSER.2005.1506394.

[27] X. Zheng, Z. Cai, J. Li, H. Gao, Location-privacy-aware review publication mechanism for local business service systems, in: The 36th Annual IEEE International Conference on Computer Communications, Atlanta, GA, USA, 2017, pp. 1–9, doi:10.1109/INFOCOM.2017.8056976.

[28] C. Dwork, M. Naor, T. Pitassi, G.N. Rothblum, Differential privacy under continual observation, in: The 2010 ACM International Symposium on Theory of Computing, New York, USA, 2010, pp. 715–724, doi:10.1145/1806689.1806787.

[29] H. To, G. Ghinita, C. Shahabi, A framework for protecting worker location privacy in spatial crowdsourcing, VLDB Endow. 7 (2014) 919–930, doi:10.14778/2732951.2732966.

[30] R. Dewri, Local differential perturbations: location privacy under approximate knowledge attackers, IEEE Trans. Mob. Comput. 12 (2013) 2360–2372, doi:10.1109/TMC.2012.208.

[31] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, G. Wu, An incentive mechanism with privacy protection in mobile crowdsourcing systems, Comput. Netw. 102 (2016) 157–171, doi:10.1016/j.comnet.2016.03.016.

[32] G. Yin, Y. Wang, Y. Dong, H. Dong, Wright-fisher multi-strategy trust evolution model with white noise for internetware, Expert Syst. Appl. 40 (2013) 7367–7380, doi:10.1016/j.eswa.2013.07.026.

[33] C.Z. Zheng, High bids and broke winners, J. Econ. Theory 100 (2001) 129–171, doi:10.1006/jeth.2000.2715.

[34] I. Boutsis, V. Kalogeraki, Privacy preservation for participatory sensing data, in: 2013 IEEE International Conference on Pervasive Computing and Communications (PerCom), San Diego, CA, 2013, pp. 103–113, doi:10.1109/PerCom.2013.6526720.

[35] B. Zhang, C. Liu, J. Lu, Z. Song, Z. Ren, J. Ma, Privacy-preserving QoI-aware participant coordination for mobile crowdsourcing, Comput. Netw. 101 (2016) 29–41, doi:10.1016/j.comnet.2015.12.022.

Yingjie Wang was born in 1986, China. She received the Ph.D. degree in computer science and technology from Harbin Engineering University. She visited Georgia State University from 2013/09 to 2014/09 as a visiting scholar. Dr. Wang is currently an Assistant Professor in the School of Computer and Control Engineering at Yantai University. She is a Postdoc in South China University of Technology. Her research interests are mobile crowdsourcing, privacy protection and trust computing. She has published more than 20 papers in well known journals and conferences in her research field, which include an ESI high cited paper. In addition, she has presided 1 National Natural Science Foundation of China projects and 1 China Postdoctoral Science Foundation, and joined 3 National Natural Science Foundation of China projects and 1 Natural Science Foundation of Shandong Province project.

Zhipeng Cai received his Ph.D. and M.S. degree in Department of Computing Science at University of Alberta, and B.S. degree from Department of Computer Science and Engineering at Beijing Institute of Technology. Dr. Cai is currently an Assistant Professor in the Department of Computer Science at Georgia State University. Prior to joining GSU, Dr. Cai was a research faculty in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Dr. Cai's research areas focus on Networking and Big data. Dr. Cai is the recipient of an NSF CAREER Award.

Xiangrong Tong was born in 1975, China. He received the Ph.D. degree in computer science and technology from Beijing Jiaotong University. He is a Full Professor of Yantai University. His research interests are computer science, intelligent information processing and social networks. He has published more than 30 papers in well known journals and conferences. In addition, he has presided and joined 3 national projects and 3 provincial projects.

Yang Gao was born in 1985, China. He received the Master degree in computer science and technology from Northeast Forest University. He is currently a teacher of Yantai University. His research interests are computer science, social networks and wireless sensor networks. He has published some papers in well known journals and International conferences.

Guisheng Yin was born in 1964, China. He received the Ph.D. degree in automatic control from Harbin Engineering University, where he is a Full Professor and Doctoral tutor, the Dean of College of Computer Science and Technology and the Dean of School of Software Engineering. He ever worked in Tokyo University before he joined the current university. His research interests are trustworthy software, information security, Internetware and so on. He has published more than 100 papers in well known journals and conferences. In addition, he has presided 4 national projects and 5 provincial projects.