PEAK: Privacy-Enhanced Incentive Mechanism for Distributed *K*-Anonymity in LBS

Man Zhang, Xinghua Li, *Member, IEEE,* Yinbin Miao, Bin Luo, Yanbing Ren, and Siqi Ma

Abstract—To motivate users' assistance for protecting others' location privacy by distributed *K*-anonymity in Location-Based Service (LBS), many incentive mechanisms have been proposed, where users obtain monetary compensation for their assistance. However, most existing distributed *K*-anonymity incentive mechanisms rely on trusted third parties and ignore users' malicious strategies, which destroys LBS's distributed structure as well as leads to users' privacy leakage and incentive ineffectiveness. To solve the above problems, we propose a Privacy-Enhanced incentive mechAnism for distributed *K*-anonymity (PEAK). With determining the monetary transaction relationship and location transmission between users, PEAK enables the anonymous cloaking region construction without the trusted server. Meanwhile, PEAK devises role identification mechanism and accountability mechanism to restrain and punish malicious users, which protects users' location privacy and implements effective motivation on users' assistance. Theoretical analysis based on the game theory shows that PEAK constrains users' malicious strategies while satisfying individual rationality, computational efficiency, and satisfaction ratio. Extensive experiments based on the real-world dataset demonstrate that PEAK improves security and feasibility, especially reaching the success rate of anonymous cloaking region construction to more than 90% and decreasing the malicious users' utilities significantly.

Index Terms—location privacy, distributed *K*-anonymity, Location-Based Service, incentive mechanisms, game theory.

1 Introduction

With the development of wireless network and location technology, users can obtain information related to spatial locations by querying the Location-Based Service (LBS) [1]–[4], which plays an indispensable role in our daily life [5], [6]. For example, during the outbreak of COVID-19, the requester can query the distribution of neighbouring patients to obtain the secure travel arrangements [7]. This query process requires the requester to send his location information (*e.g.*, office) to the Location Service Provider (LSP) [8] as shown in Fig.1. However, the requester's location privacy is threatened by LSP that may infer and disclose requester's privacy information (*e.g.*, job category) due to interest motivation [9]–[13]. Thus, to prevent LSP from snooping requester's location, the distributed *K*-anonymity has been proposed [14], which allows the requester to search for $K-1$ cooperators' locations and construct anonymous cloaking region consisting of all these K locations of cooperators and requester. This representative spatial cloaking technique can resist location tracking attacks [14] without the complex cryptographic operations and a third party while returning accurate query results. Thus, it has been widely discussed and adopted in LBS [15]–[17]. Nevertheless, this assistance incurs communication or battery energy burdens on cooperators, which makes cooperators be unwilling to submit their locations and leads the fail of the anonymous cloaking region construction [18]. Fortunately, the incentive mechanism allows the cooperators to be compensated by the requesters, which effectively motivates the cooperators' assistance. Thus, to enjoy the multiple advantages of this spatial cloaking technique, the distributed *K*-anonymity incentive mechanisms have been extensively studied [19]–[22].

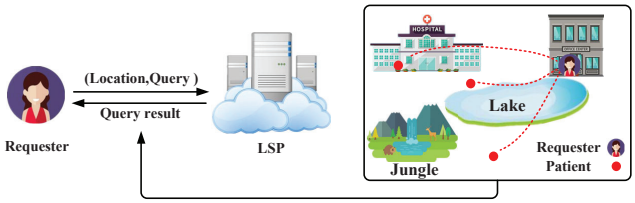
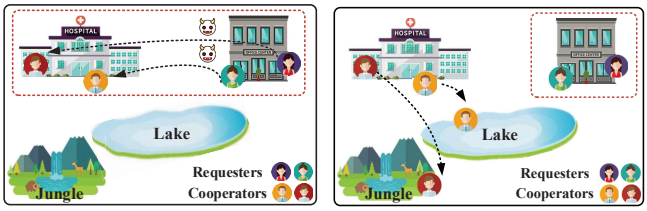


Fig. 1. **Patient distribution query process.**

However, the existing distributed *K*-anonymity incentive mechanisms still have some shortcomings. *Most of them rely on the trusted server to implement the anonymous cloaking region construction.* Depending on the trusted third party, the existing mechanisms determine the monetary transaction relationship between requesters and cooperators [19]–[21]. Meanwhile, the trusted server generally gathers locations of requesters and cooperators to construct the anonymous cloaking region. This approach destroys the structure of the distributed *K*-anonymity and thus does not scale well in LBS architecture where the trusted server is hard to find [17]. Thus, the existing distributed *K*-anonymity incentive mechanisms are impractical in LBS.

In addition, *the existing mechanisms ignore users' malicious strategies that threaten users' location privacy and the incentive mechanism's effectiveness.* Specifically, when obtaining the cooperators' locations, the requester may disclose them to gain additional profits. For example, in Fig.2(a), receiving cooperators'

- *This work was supported by the National Natural Science Foundation of China under Grant U1708262, U1736203 and 61872449.*
- *Corresponding Author: Xinghua Li.*
- *M. Zhang, X. Li, Y. Miao, B. Luo and Y. Ren are with State Key Laboratory of Integrated Services Networks, and the School of Cyber Engineering, Xidian University, Xi'an, 710071, China (e-mail: mzhang0517@outlook.com; xhli1@mail.xidian.edu.cn; ybmiao@xidian.edu.cn; luobin2127-@hotmail.com; yanbing_ren@foxmail.com).*
- *S. Ma is with the School of Information Technology and Electrical Engineering at the University of Queensland, St Lucia QLD 4072, Australia (e-mail: xdmasiqi@hotmail.com).*



(a) The requesters' malicious strategy. (b) The cooperators' malicious strategy.

Fig. 2. **The users' malicious strategies in the incentive mechanism.** The requesters seek cooperators' locations to construct anonymous cloaking region. In (a), to gain additional profits, the malicious requesters disclose received locations, leading cooperators' privacy leakage. In (b), to protect the true locations (*e.g.*, hospital) from the requesters, the malicious cooperators provide the false locations in the center of lake and jungle, respectively. Thus the anonymous cloaking region can be shrunk in the range of office, and the requesters' locations are snooped.

locations (e.g., hospital) to construct the anonymous cloaking region, the requesters may disclose this information to the adversary. If the adversary realizes that these cooperators locate in the hospital, he can infer that cooperators' physical condition is not encouraging. It threatens the cooperators' sensitive privacy and discouraged cooperators' assistance. Besides, the requester may falsely claim that he is a cooperator and participate in the incentive mechanism, enabling him to join the anonymous cloaking region for free or even profit [19]. This role cheating attack harms the incentive effectiveness seriously. In addition, for protecting the location privacy, the cooperator may provide false location while still obtaining monetary compensation [17], as shown in Fig.2(b). This malicious strategy leads to the shrink of the anonymous cloaking region by LSP and requesters' location privacy leakage.

To solve the above problems, we propose a **P**rivacy-**E**nhanced incentive mech**A**nism for distributed ***K***-anonymity (PEAK). Based on the auction theory, PEAK motivates cooperators' assistance with the monetary compensation. Meanwhile, without a trusted third party, PEAK protects requesters' and cooperators' location privacy while constructing the anonymous cloaking region. The main contributions of this paper are summarized as follows:

1) We propose a distributed K-anonymity inventive mechanism PEAK to motivate cooperators' assistance for anonymous cloaking region construction without trusted server. According to the auction theory, PEAK determines the monetary transaction relationship between requesters and cooperators, where LSP acts as the auctioneer. In addition, PEAK realizes the location transmission from cooperators to requesters, which enables the anonymous cloaking region construction.
2) We devise the *role identification* and *accountability mechanism* to constrain users' malicious strategies. Specifically, by recording users' auction roles, the *role identification mechanism* prevents requesters' role cheating attack, guaranteeing incentive effectiveness. The *accountability mechanism* implements the negative utilities of cooperators submitting false locations and requesters leaking locations.
3) We show the theoretical analysis based on the game theory, which shows that PEAK constrains users' malicious strategies while satisfying individual rationality, computational efficiency, and satisfaction ratio. We implement extensive experiments using the real-world dataset to show that PEAK achieves a higher anonymous cloaking region construction success rate which is over 90%. At the same time, we prove that PEAK avoids the trajectory information leakage, single point of failure and decreases the malicious users' utilities effectively.

The remainder of this paper is organized as follows. Section. 2 reviews the related existing works. Section. 3 presents the system model, problem definition, threat model, and design goals. Section. 4 explains PEAK in detail, including anonymous cloaking region construction, role identification and accountability mechanism. Section. 5 and Section. 6 give theoretical analysis and experimental results, respectively. Finally, Section. 7 concludes PEAK.

2 Related Work

2.1 Distributed *K*-Anonymity

The distributed K-anonymity was first proposed by Chow *et al.* [14], where the requesters are able to seek cooperators by the peer-to-peer communication technologies. Inspired by this method, Ghinita *et al.* [23] further adopted Hilbert space-filling curve to construct the anonymous cloaking region, which guarantees the users' query anonymity. Adopting this distributed model, Huang *et al.* [24] elaborated the process of spatial cloaking for location privacy by introducing a communication chain. Subsequently, Sun *et al.* [25] introduced the location label into anonymous cloaking region construction to protect requesters' preference privacy. To decrease the query frequency and the privacy leakage risk, Gupta *et al.* [26] allowed users to access his peers' caches for the querying results once the trust relationship between them is evaluated. Similarly, Zhang *et al.* [27] selected K cache cells based on requesters' query probability and formed spatial K-anonymity for requesters' local query. Tu *et al.* [28] first introduced semantic attack to trajectory privacy preservation and devised an algorithm to against both semantic attack and re-identification attack based on K-anonymity. While constructing the K anonymous cloaking region, Luo *et al.* [17] took users' trust degree into account, which prevents malicious users and protects users' location privacy effectively. Meanwhile, another common approach to achieve K-anonymity is generating $K-1$ dummy locations. Referring geo-indistinguishability and K-anonymity to construct anonymity sets, Niu *et al.* [16] devised Eclipse to against long-term observation attacks. Nevertheless, the authenticity of dummy is less than cooperators' real locations and the adversary can shrink the anonymous cloaking region by identifying dummy.

However, the anonymous cloaking region construction requires for the cooperators' aid, which brings communication or battery energy burdens [18], [29]. This fact leads that the cooperators are unwilling to assist and the ineffectiveness of above works' implementation.

2.2 Incentive Mechanism for *K*-anonymity

To motivate cooperators' assistance, many K-anonymity incentive mechanisms have been proposed. Based on the reciprocity method, Li *et al.* [22] claimed that the user can get assistance if the ratio of the times assisting others to the times requiring help exceeds a certain threshold. However, the reciprocity incentive only motivates privacy-sensitive users' assistance so it is invalid because of little amount of privacy-sensitive users [30]. To solve this problem, Yang *et al.* [21] proposed the first monetary K-anonymity incentive mechanism which allows the sellers to sell their locations to requesters for fees through the sealed-bid double auction. Nevertheless, they did not consider the satisfaction ratio,

TABLE 1
A comparative summary between our schemes and the existing schemes.

Items / *Works*	Locations	IM	CM	WT
Ghinita *et al.* [23]	True	None	✗	✓
Huang *et al.* [24]	True	None	✗	✓
Gupta *et al.* [26]	\	None	✗	✓
Zhang *et al.* [27]	\	None	✗	✗
Luo *et al.* [17]	True	None	✓	✓
Niu et al. [16]	Dummy	None	✗	✓
Zhang *et al.* [19]	True	Monetary	✗	✗
Li *et al.* [22]	True	Reciprocity	✗	✓
Fei *et al.* [20]	Dummy	Monetary	✗	✓
PEAK	True	Monetary	✓	✓

Note: IM: Incentive method, CM: Constraint of malicious strategies, WT: Without trusted third parties.

the ratio of winning requesters' number to all requesters' number. Thus, Zhang *et al.* [19] used the greedy algorithm to improve satisfaction ratio at the expense of the auctioneer's deficit. With turning the auction winner selection problem into an integer linear programming problem, Wang *et al.* [31] avoided the privacy leakage of users' bids [19] via differential privacy. Beside, in *K*-anonymity based on dummy, Wu *et al.* [32] supposed that a user with a trajectory similar to the dummy one could get the desired query results from the requester if he/she compensates requesters according to reverse auction. Similar to [32], Fei *et al.* [20] grouped all users according to their query probabilities. Based on the auction, the proxy who is responsible for the anonymity of group members is compensated by others.

However, most of the above incentive mechanisms rely on the trusted party. Moreover, these works only motivate cooperators' assistance rather than users' honest strategies. Therefore, the existing incentive mechanisms cannot be directly applied in *K*-anonymity implementation. TABLE 1 shows the comparison of various indexes about PEAK and existing schemes.

3 Problem Formulation

In this section, we first give the system model of PEAK. Then, we define two processes of the anonymous cloaking region construction, including monetary transaction and location transmission, as the auction and location transmission game respectively. Subsequently, we propose the design goals and threat model of PEAK. Prior to detail descriptions, we give some notation definitions in TABLE 2.

3.1 System Model

Consistent with existing schemes [19], [21], PEAK considers a multiple requesters and cooperators scenario. As shown in Fig. 3, the system model mainly consists of three entities, namely Requesters, Cooperators and Location Service Provider (LSP). The role of each entity and the anonymous cloaking region construction process (step 1-6 in Fig. 3) are shown as follows.

- *Requesters*: The requesters who seek assistance to construct anonymous cloaking region first submit their identities IDs, the size of the required anonymous cloaking region and *Offers* to LSP (step 1). After the auction, the winning requesters give *Payments* LSP (step 2).
- *Cooperators*: The cooperators first submit their IDs and *Asks* to LSP (step 1). After the auction, winning cooperators send their locations to winning requesters according to the location transmission relationship (step 5). At last, the cooperators can receive *Gains* from LSP only if the requesters confirm that they do not submit false locations (step 6).
- *LSP*: Acting as the auctioneer, the *honest-but-curious* LSP is responsible for determining auction result. After that, LSP issues the signed role certificate to winning users (step 3), decides the location transmission relationship according to the pre-designed allocation strategy, signs it and then sends it to the winning cooperators (step 4).

TABLE 2
Main Notations.

Notations	*Descriptions*
$\mathcal{R}=\{r_1,r_2,...,r_m\}$	Requester set
$\mathcal{C}=\{c_1,c_2,...,c_n\}$	Cooperator set
$U=\{U^+,U^-\}$	Users' utilities in the case of winning/losing
k_i	Anonymity requirement size of requester r_i
o_i, a_j	Requesters r_i's *Offer*, cooperator c_j's *Ask*
v_i, σ_j	Requester r_i's Privacy *Value*, cooperator c_j's *Cost* for assistance
x, $k-x$	Number of winning requesters/cooperators
$W_{\mathcal{R}}=\{r_1,r_2,...,r_x\}$	Winning requester set
$W_{\mathcal{C}}=\{c_1,c_2,...,c_{k-x}\}$	Winning cooperator set
p_i, g_j	Winning requester r_i's *Payment*, winning cooperator c_j's *Gain*
$Cert=\{\mathrm{ID},Role\}$	Certificates recording the users' identities and roles
$\gamma\in\mathcal{R}$, $\tilde{U}_\gamma$	Malicious requesters cheating on role and his utility
R_h, R_c	Historical/current location transmission record
$\mu^*=\{\mu^{(t)},\mu^{(p)}\}$	Nash Equilibrium in the location transmission game

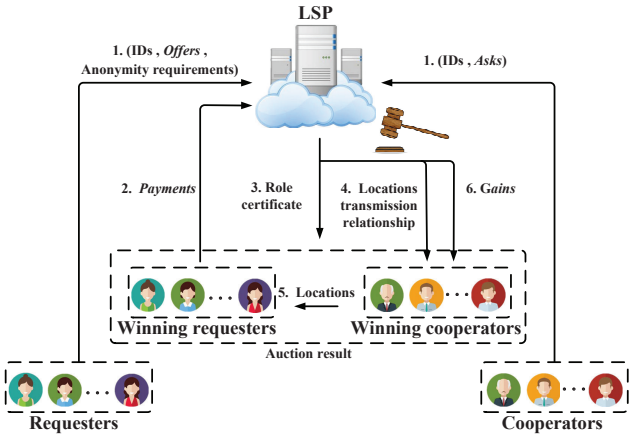


Fig. 3. **System model.**

3.2 Problem Definition

To construct anonymous cloaking region, we first determine the monetary transaction between requesters and cooperators and then realize the location transmission between winning requesters and

cooperators. The former is achieved by the sealed-bid double auction [19], and the latter can be seen as a game between them, which are defined as follows.

Definition 1 (Sealed-bid double auction). The sealed-bid double auction proposed in [19] can be viewed as a tuple $\Gamma_1 = \langle \mathcal{R}, \mathcal{C}, Bids, U \rangle$, where $\mathcal{R} = \{r_1, r_2, ..., r_m\}$ and $\mathcal{C} = \{c_1, c_2, ..., c_n\}$ are respectively requesters and cooperators, $Bids = \{o_i, a_j\}$ is the set of players' strategies and $U = \{U^+, U^-\}$ represents the players' utilities when they win and fail.

Specifically, each requester r_i owns the location privacy value v_i and each cooperator c_j bears the cost σ_j for assistance, where σ_j includes the communication cost σ_j^{com} and the privacy cost σ_j^{pri}, so that

$$\sigma_j = \sigma_j^{com} + \sigma_j^{pri}. \tag{1}$$

In the sealed-bid double auction, the requester r_i submits his offer o_i to describe the maximum amount that he is willing to pay for privacy value, and the cooperator c_j submits his ask a_j to describe the minimum compensation that he is willing to accept for the cost of assistance. Receiving all bids from users, the auctioneer determines the winning users. Each winning requester r_i needs to pay certain payments p_i for his privacy value. Each winning cooperator c_j can get certain gains g_j to compensate his cost. In addition,

$$U^+ = \{U_{r_i}^+, U_{c_j}^+\} \tag{2}$$

represents requesters' and cooperators' utilities when they win the auction, and

$$U^- = \{U_{r_i}^-, U_{c_j}^-\} \tag{3}$$

when they fail. Therefore, the utility of the losing requester r_i who will not get any privacy value or pay any payment is denoted by $U_{r_i}^- = 0$. $U_{c_j}^- = 0$ denotes the utility of losing cooperator c_j who will not get any gain or pay any cost. The utilities of winning players are related to the game of location transmission and will be described later.

After determining the monetary transaction, we define the game of location transmission between winning players in Γ_1 as follows.

Definition 2 (Game of location transmission). The game of location transmission can be regarded as a tuple $\Gamma_2 = \langle W_{\mathcal{R}}, W_{\mathcal{C}}, \mu, U^+ \rangle$, where $W_{\mathcal{R}} = \{r_1, r_2, ..., r_x\}$ and $W_{\mathcal{C}} = \{c_1, c_2, ..., c_{k-x}\}$ are respectively winning requester set and cooperator set in Γ_1, $\mu = \{\mu_{\mathcal{R}}, \mu_{\mathcal{C}}\}$ presents players' strategies and $U^+ = \{U_{r_i}^+, U_{c_j}^+\}$ describes players' utilities.

In the game of location transmission, the requesters' strategies

$$\mu_{\mathcal{R}} = \{\mu^{(l)}, \mu^{(p)}\}, \tag{4}$$

where $\mu^{(l)}$ means that the requester leaks the received location information and $\mu^{(p)}$ means preserving it. The cooperators' strategies

$$\mu_{\mathcal{C}} = \{\mu^{(f)}, \mu^{(t)}\}, \tag{5}$$

in which $\mu^{(f)}$ explains that the cooperator submits a false location information and $\mu^{(t)}$ means that the cooperator submits a true one. $U^+ = \{U_{r_i}^+, U_{c_j}^+\}$ describes the utilities of winning requester r_i and winning cooperator c_j in Γ_1. According to above analysis, considering two types of players and four types of player's strategies, the players' utilities in Γ_2 are described as follows.

Utilities of requester: $U_{r_i}^+ = \{U_{r_i\_1}^+, U_{r_i\_2}^+, U_{r_i\_3}^+, U_{r_i\_4}^+\}$ is the utility set of winning requester $r_i \in W_{\mathcal{R}}$ under the different strategies. Let $U_{r_i}^{leak}$ be the utility of location information leakage.

- $U_{r_i\_1}^+ = -p_i + U_{r_i}^{leak}$ denotes r_i's utility when c_j submits a false location and r_i leaks it;
- $U_{r_i\_2}^+ = -p_i$ denotes r_i's utility when c_j submits a false location and r_i preserves it;
- $U_{r_i\_3}^+ = v_i - p_i + U_{r_i}^{leak}$ denotes r_i's utility when c_j submits a true location and r_i leaks it;
- $U_{r_i\_4}^+ = v_i - p_i$ denotes r_i's utility when c_j submits a true location and r_i preserves it.

Meanwhile, $\tilde{U}_\gamma$ is the utility of malicious requester $\gamma \in \mathcal{R}$ who falsely claim that he is a cooperator and participates in the incentive mechanism, so that

$$\tilde{U}_\gamma = v_i + U_c^+, \tag{6}$$

where he can get privacy protection v_i for free and even obtain a normal cooperator's utility U_c^+.

Remark 1. If c_j submits false location, r_i cannot gain privacy value under any strategy. Thus, r_i's utility is the sum of $-p_i$ and $U_{r_i}^{leak}$ when leaking the location information, and $-p_i$ when preserving. Moreover, due to c_j's true location, r_i gets privacy value under both strategies. Therefore, r_i's utility is the sum of v_i, $-p_i$ and $U_{r_i}^{leak}$ when leaking location, and the sum of v_i and $-p_i$ if he preserves location.
Based on the above utility analysis, r_i's utility is higher when he discloses cooperators' location or falsely claims that he is a cooperator, that is,

$$\begin{cases} U_{r_i\_1}^+ > U_{r_i\_2}^+, \\ U_{r_i\_3}^+ > U_{r_i\_4}^+, \\ \tilde{U}_\gamma > U_r^+. \end{cases} \tag{7}$$

Thus, the rational requester may choose the malicious strategies to maximize his utility.

Utilities of cooperator: $U_{c_j}^+ = \{U_{c_j\_1}^+, U_{c_j\_2}^+, U_{c_j\_3}^+, U_{c_j\_4}^+\}$ is the utility set of winning cooperator $c_j \in W_{\mathcal{C}}$ under the different strategies. Here,

- $U_{c_j\_1}^+ = g_j - \sigma_j^{com}$ denotes c_j's utility when r_i leaks the location and c_j submits a false one;
- $U_{c_j\_2}^+ = g_j - \sigma_j^{com}$ denotes c_j's utility when r_i preserves the location and c_j submits a false one;
- $U_{c_j\_3}^+ = g_j - \sigma_j^{com} - \sigma_j^{pri}$ denotes c_j's utility when r_i leaks the location and c_j submits a true one;
- $U_{c_j\_4}^+ = g_j - \sigma_j^{com}$ denotes c_j's utility when r_i preserves the location and c_j submits a true one.

Remark 2. On account of the location leakage caused by r_i, there will be no privacy cost when c_j submits a false one, where c_j's utility is the sum of g_j and $-\sigma_j^{com}$. When c_j submits the true one, his utility is the sum of g_j, $-\sigma_j^{com}$, and $-\sigma_j^{pri}$. In addition, when r_i preserves the location information, c_j's utility is the sum of g_j and $-\sigma_j^{com}$ whatever strategy he chooses.
Based on the above utility analysis, c_j's utility is higher when he chooses the malicious strategy, that is,

$$\begin{cases} U_{c_j\_1}^+ > U_{c_j\_3}^+, \\ U_{c_j\_2}^+ = U_{c_j\_4}^+; \end{cases} \tag{8}$$

Thus, the rational cooperator may submit false location to maximize his utility.

3.3 Threat Model

PEAK considers LSP to be an *honest-but-curious* party, implying that LSP would follow the auction protocol strictly but may be interested in users' location privacy. In addition, there're no trusted relationship among malicious users, which means that users may maximize their personal utilities according to malicious strategies. Here we introduce two external adversaries, including $\mathcal{A}$ and $\mathcal{A}^*$. Specifically, $\mathcal{A}$ can persuade the *honest-but-curious* LSP to leak users' locations. $\mathcal{A}^*$ can persuade malicious users to threaten other users' location privacy and affect incentive effectiveness. $\mathcal{A}$ will attack with the following capability:

- $\mathcal{A}$ may compromise LSP to infer to the location information of all users.

And $\mathcal{A}^*$'s capabilities are defined as follows.

- $\mathcal{A}^*$ may compromise the requesters to pose as cooperators to participate in the auction;
- $\mathcal{A}^*$ may compromise the winning requesters to reveal the location information they receive;
- $\mathcal{A}^*$ may compromise the winning cooperators to submit false locations in the anonymous cloaking region construction.

To obtain the users' location privacy, the adversaries $\mathcal{A}$ and $\mathcal{A}^*$ could collude to exchange the users' location information.

3.4 Design Goals

On the basis of the formulation of games above, PEAK should satisfy auction goals and privacy goals shown as follows.

Auction goals. Most potential cooperators are motivated to participate in the auction and assist with the anonymous cloaking region construction. The similar goals [19] that the auction pursues are described as follows.

- *Individual rationality:* The users' utilities should be non-negative when submitting the true offer o_i and ask a_j that equal value v_i and cost σ_j respectively;
- *Truthfulness:* Neither requesters nor cooperators can improve their utilities by submitting o_i and a_j falsely, that is, the utilities should be maximized when they bid truthfully;
- *Computational efficiency:* The auction results should be determined in the polynomial time;
- *Satisfaction ratio:* The number of users who are satisfied in auction should be maximized.

Besides, we consider that the auction should resist the role cheating attack which is defined as follows.

- *Resistance of role cheating attack:* Malicious requesters who cheat their roles cannot get any privacy protection, which means that $\tilde{U}_\gamma = U_c^+$.

Privacy goals. The privacy goals include

- *Requester's privacy:* Winning requesters can collect true locations from cooperators and construct the anonymous cloaking region to protect their location privacy.
- *Cooperator's privacy:* Winning cooperators' locations cannot be disclosed by winning requesters.

It means that the Nash Equilibrium of location transmission game Γ_2 is players' honest strategies, where

$$\mu^* = \{\mu^{(t)}, \mu^{(p)}\}. \tag{9}$$

4 Our Proposed Scheme

Although existing incentive mechanisms [19]–[21] can motivate most users to participate in the anonymous cloaking region, they still rely on trusted third parties and ignore users' malicious strategies. To solve the above problems, we propose an incentive mechanism PEAK to encourage users' assistance while restraining users' malicious strategies without the trusted server. This section first gives the overview of PEAK and then describes it in detail.

4.1 Overview of PEAK

PEAK consists of three modules including *anonymous cloaking region construction*, *role identification mechanism* and *accountability mechanism* shown as Fig. 4. The first module guarantees the success of construction, including **auction process** and **location transmission process**. The latter two modules constrain users' malicious strategies in *anonymous cloaking region construction*. That is, in **auction process**, the requester may falsely claim that he is a cooperator, damaging the incentive effectiveness. In **location transmission process**, the cooperators may submit false locations and the requester may disclose received locations, which threatens users' location privacy. Thus, it is necessary to provide *role identification mechanism* and *accountability mechanism* in the process of *anonymous cloaking region construction*. The overview of PEAK is shown as follows.

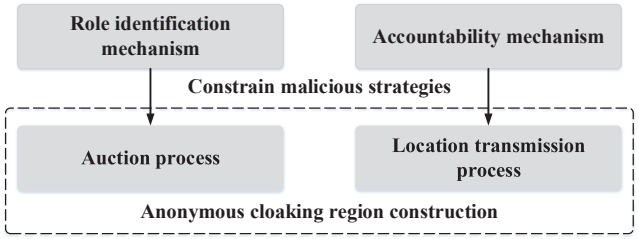


Fig. 4. **The overview of PEAK.**

Anonymous cloaking region construction: During the **auction process**, once the monetary transaction are determined, the winning cooperators submit locations to winning requesters directly in **location transmission process**, instead of trusted third parties. Winning requesters construct the anonymous cloaking region.

Then, to constrain users' malicious strategies in **auction process** and **location transmission process** of *anonymous cloaking region construction*, we devise two mechanisms shown as follows.

- *Role identification mechanism:* Users' roles in **auction process** of *anonymous cloaking region construction* module are recorded. Thus, only the user who holds the requester's role certificate signed by LSP can initiate LBS queries anonymously.
- *Accountability mechanism:* Based on **location transmission process** in *anonymous cloaking region construction* module, location transmission relationship is recorded and users who find their location privacy leakage causing by construction module can prosecute and punish malicious users according to accountability mechanism.

4.2 Anonymous Cloaking Region Construction

To construct the anonymous cloaking region, on the basis of problem definition in Section. 3, we describe two processes respectively, namely auction process and location transmission process.

1) Auction process

The auction process consists of two stages including winner determination and account calculation. To elaborate the auction process clearly, here we describe the situation that the requester $r_i \in \mathcal{R}$ $(i = 1,2,...,m)$ submits his ID$_i$, anonymity requirement size k_i and offer o_i to LSP, where $k_1 = k_2 = ...$=$k_m = k$. The cooperator $c_j \in \mathcal{C}$ $(j = 1,2,...,n)$ submits his ID$_j$ and ask a_j to LSP, too.

(a) Winner determination

The anonymity requirement size and the number of the requesters affect the winner determination process. Thus, receiving the bidding information from the requesters and the cooperators, LSP first explores the magnitude relationship between k and m, and then determines the winners based on the following two situations.

- The number of requesters is larger than that of anonymity requirement size, that is, $m \geq k$.

Here, the requesters can construct the anonymous cloaking region by themselves directly, implying that all requesters are winners and all cooperators lose, that is,

$$\begin{cases} \forall r_i \in W_{\mathcal{R}}, i = 1,2,...m; \\ \forall c_j \notin W_{\mathcal{C}}, j = 1,2,...n. \end{cases} \tag{10}$$

- The number of requesters is smaller than that of anonymity requirement size, that is, $m < k$.

The requesters need to construct anonymous cloaking region with the assistance of cooperators in this situation. Thus, LSP sorts the requesters in a decreasing order by their offers, note that the requester set $\mathcal{R} = \{r_1, r_2, ..., r_m\}$ has corresponding offer set $O = \{o_1 > o_2 > ... > o_m\}$. Then, LSP sorts the cooperators in an increasing order according to their asks, note that the cooperator set $\mathcal{C} = \{c_1, c_2, ..., c_n\}$ has corresponding ask set $A = \{a_1 < a_2 < ... < a_n\}$. When requesters and cooperators submit the same bid, they are sorted in the order based on their arrival time. Obviously, a_j is the j-th smallest ask in A and o_i is the i-th highest offer in O.

To ensure that users' utilities U_{c_j} and U_{r_i} are non-negative (individual rationality) and largest only when they bid truly (truthfulness), the number of winning requesters is maximized (satisfaction ratio), the following objective function should be satisfied.

$$Maximize\ x \tag{11}$$

$$\text{s.t.} \quad xo_x \geq (k-x)\, a_{k-x+1}, \tag{12}$$

where x is the sequence number of the winning requester whose offer o_i is smallest in the winning requester set $W_{\mathcal{R}} = \{r_1, r_2, ..., r_x\}$. o_x is r_x's offer and is called as "*pivot offer*". As the result of the anonymity requirement size k minus the number of winning requesters x, $k-x$ is the number of winning cooperators, that is, there's winning cooperator set $W_{\mathcal{C}} = \{c_1, c_2, ..., c_{k-x}\}$. a_{k-x+1} is c_{k-x+1}'s ask and we call it "*pivot ask*". The establishment of this objective function can effectively guarantee individual rationality, truthfulness, and satisfaction ratio, which is proved in Section. 5 in detail.

To clarify how to find out the winners satisfying the above formula, here the winner determination process is shown in Fig. 5. Sorting the requesters/cooperators in a non-increasing/non-decreasing order by their offers/asks, LSP obtains a requester set $\mathcal{R} = \{r_1, r_2, r_3, r_4\}$, where $o_1 = 12, o_2 = 10, o_3 = 9, o_4 = 2$, and a cooperator set $\mathcal{C} = \{c_1, c_2, c_3, c_4\}$, where $a_1 = 1, a_2 = 2, a_3 = 6, a_4 = 8$. Then, LSP first assumes that r_4 is the winning bidder

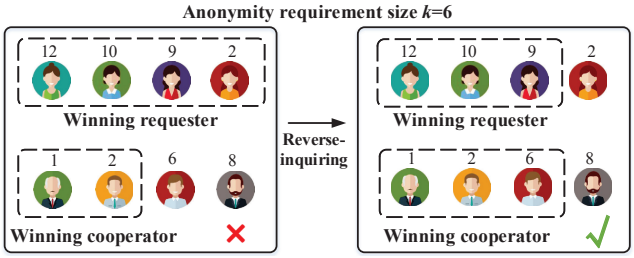


Fig. 5. **An example of winner determination.**

with the lowest offer. At this time, there're winning requester set $W_{\mathcal{R}} = \{r_1, r_2, r_3, r_4\}$ and winning cooperator set $W_{\mathcal{C}} = \{c_1, c_2\}$. Thus, there exists

$$(xo_x = 4 \times 2) < ((k-x)a_{k-x+1} = 2 \times 6), \tag{13}$$

which does not satisfy Eq. (12). Then LSP discuss the possibility that there're winning requester set $W_{\mathcal{R}} = \{r_1, r_2, r_3\}$ and winning cooperator set $W_{\mathcal{C}} = \{c_1, c_2, c_3\}$. There exists

$$(xo_x = 3 \times 9) > ((k-x)a_{k-x+1} = 3 \times 8), \tag{14}$$

which satisfies Eq. (12). So the max winning requester set is $W_{\mathcal{R}} = \{r_1, r_2, r_3\}$ and the winning cooperator set is $W_{\mathcal{C}} = \{c_1, c_2, c_3\}$, where $x = 3$.

(b) Account calculation

The account calculation process is also based on the magnitude between the anonymity requirement size and the number of the requesters. Thus, LSP calculates each winning requester's/cooperator's payment/gain based on the following two situations.

- The number of requesters is larger than that of anonymity requirement size, that is, $m \geq k$.

In this case, all requesters do not need to cost any payment and all cooperators cannot get any gain, that is,

$$\begin{cases} \forall p_i = 0, i = 1,2,...m; \\ \forall g_j = 0, j = 1,2,...n. \end{cases} \tag{15}$$

- The number of requesters is smaller than that of anonymity requirement size, that is, $m < k$.

In this case, the requesters need to construct anonymous cloaking region through auction and LSP charges each winning requester equally, which means that $\forall r_i \in W_{\mathcal{R}}$ bear the total amount paid to $\forall c_j \in W_{\mathcal{C}}$ jointly and equally.

Thus, each winning requester $r_i \in W_{\mathcal{R}}$ needs to pay LSP

$$p_i = \frac{(k-x)a_{k-x+1}}{x}. \tag{16}$$

Then, LSP would pay the winning cooperators who choose the honest strategy. So each honest $c_j \in W_{\mathcal{C}}$ can get gain from LSP

$$g_j = \max\ a_{k-x+1}. \tag{17}$$

After collecting all payments, LSP waits for a while T rather than distributing gains g_j to the winning cooperators $\forall c_j \in W_{\mathcal{C}}$ immediately. With the anonymous cloaking region, if any $r_i \in W_{\mathcal{R}}$ queries successfully and there are no malicious cooperators, LSP will pay the winning cooperators who choose the honest strategy.

We discuss the auction process that the requesters have the same anonymity requirements. When they are different, the auction process can be conducted by grouping requesters according to their anonymity requirements.

Algorithm 1 Determination of Transmission Relationship

Input: $Q_{\mathcal{R}}$,$Q_{\mathcal{C}}$
Output: R_c
Initialization: $i = 1$ and $j = 1$

while $Q_{\mathcal{C}}$ is not empty **do**
  Search R_h
  if $\{c_j \to r_i\} \notin R_h$ **then**
    $R_c = R_c \bigcup \{c_j \to r_i\}$ // *Location transmission relationship is built up between c_j and r_i.*
    $R_h = R_h \bigcup \{c_j \to r_i\}$ // *Update the historical transmission record.*
    pop c_j from $Q_{\mathcal{C}}$, r_i from $Q_{\mathcal{R}}$
    insert r_i in $Q_{\mathcal{R}}$
    $j = j + 1$
  else
    if $i = x$ **then**
      $i = 1$
      $R_c = R_c \bigcup \{c_j \to r_i\}$ // *Location transmission relationship is built up between c_j and r_i.*
      pop c_j from $Q_{\mathcal{C}}$, r_i from $Q_{\mathcal{R}}$
      insert r_i in $Q_{\mathcal{R}}$
      $j = j + 1$
    else
      $i = i + 1$
    end if
  end if
end while
return $R_c = \{c_j \to r_i | j \in [1, k-x], i \in [1, x]\}$

2) Location transmission process

In PEAK, the location transmission includes two types namely the transmission between cooperators and requesters, and the transmission between requesters themselves.

(a) The location transmission between cooperators and requesters

After the auction process, the cooperator c_j provides his location information to construct the anonymous cloaking region. There're several situations that lead to c_j's privacy leakage and r_i's heavy burden.

- If $c_j \in W_{\mathcal{C}}$ sends his location to multiple requesters who leak received locations, c_j's rights cannot be protected by the accountability mechanism.
- If $c_j \in W_{\mathcal{C}}$ sends his different locations to the same requester r_i multiple times, c_j's trajectory privacy will be disclosed.
- If $\forall c_j \in W_{\mathcal{C}}$ send their locations to the same requester r_i, r_i's burden will be extremely heavy, which leads to single point of failure.

To prevent the above situations, we propose the following demands to the location transmission between cooperators and requesters:

- Each winning cooperator $c_j \in W_{\mathcal{C}}$ sends his location information to the winning requester $r_i \in W_{\mathcal{R}}$ who never receives his location;
- Each winning requester $r_i \in W_{\mathcal{R}}$ receives as little location information as possible.

To realize the above aims, we design the corresponding allocation policy. Inputting the winning requester set $W_{\mathcal{R}}$, the winning cooperator set $W_{\mathcal{C}}$ and historical transmission record R_h, LSP can get the current transmission relationship $R_c = \{c_j \to r_i | j \in [1, k-x], i \in [1, x]\}$ to guide c_j to sends his location. The specific processes are shown as follows.

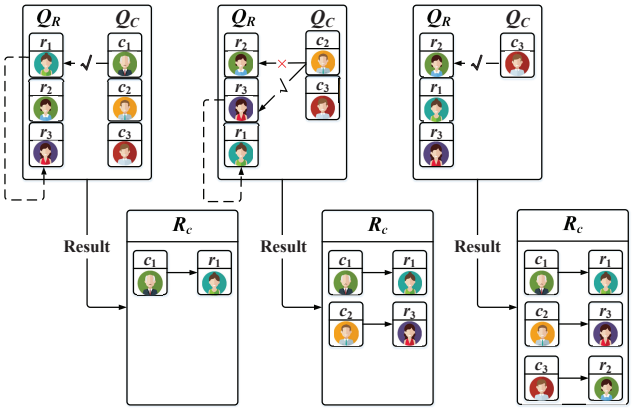


Fig. 6. **Example of location transmission process.**

- *Initialization:* LSP sorts winners based on their transaction times recorded on R_h, including
  - sorting the winning cooperators $c_j \in W_{\mathcal{C}}$ in descending order based on their number of sending locations, which ensures that the winning cooperators who send more times have the priority to choose the target winning requester, and putting the sorted winning cooperator set into the queue $Q_{\mathcal{C}}$.
  - sorting the winning requesters $r_i \in W_{\mathcal{R}}$ in increasing order based on their number of receiving locations, which guarantees that the winning requesters who receive fewer times have the priority to be chosen as the target winning requester, and putting the sorted winning requester set into the queue $Q_{\mathcal{R}}$.

  Thus, LSP gets the sorted winning cooperator queue $Q_{\mathcal{C}} = \{c_1, c_2, ..., c_{k-x}\}$ and the sorted winning requester queue $Q_{\mathcal{R}} = \{r_1, r_2, ...r_x\}$.
- *Determination of transmission relationship:* Using $Q_{\mathcal{C}}$, $Q_{\mathcal{R}}$ and R_h, LSP can get R_c according to Algorithm 1. Here we take Fig. 6 as an example to illustrate the policy process. To demonstrate the algorithm execution steps in the case of successful match and unsuccessful match, we assume that there are no transmission record between c_1 and r_1, c_2 and r_3, c_3 and r_2 and there exists a transmission record between c_2 and r_2.

After determining all the transmission relationship $R_c = \{c_j \to r_i | j \in [1, k-x], i \in [1, x]\}$, LSP records it in the historical transmission record R_h, signs it with his private key K_{apriv} to get $[R_c]_{K_{apriv}}$ and sends $[R_c]_{K_{apriv}}$ to $\forall c_j \in W_{\mathcal{C}}$. Thus, $c_j \in W_{\mathcal{C}}$ sends his location to the targeted winning requester according to $[R_c]_{K_{apriv}}$.

(b) The location transmission among requesters

When all winning cooperators $c_j \in W_{\mathcal{C}}$ send their locations to the targeted requesters successfully, LSP chooses a random winning requester $U_{agency} \in W_{\mathcal{R}}$ as the query agency, who is only one requester owning the total anonymous cloaking region information and querying for all winning requesters. There are two types of r_i, including

- $r_i \in W_{\mathcal{R}}$ who does not receive the cooperators' location information

The winning requester $r_i \in W_{\mathcal{R}}$ sends his location information to U_{agency} directly;

- $r_i \in W_{\mathcal{R}}$ who receives the cooperators' location information

r_i should be responsible for the privacy preservation of the received locations. That is, the cooperator's location should be anonymous to everyone except for r_i. Specifically, upon receiving y locations from winning cooperators, r_i anonymizes the cooperators' identity information and sends his and cooperators' locations to U_{agency}. This anonymity method makes it impossible for U_{agency} to connect users' locations to their identity information.

After the above steps are completed, U_{agency} can carry out LBS query using the anonymous cloaking region.

4.3 Role Identification Mechanism

To avoid the role cheating attack, the role identification mechanism is proposed. After the auction process finishes, once the winning requester pays LSP the correct amount, LSP will issue a signed role certificate $Cert^{(r_i)}$ to him by Eq. (18)

$$Cert^{(r_i)} = \{\mathrm{ID}_{r_i}, \mathcal{R}\}_{K_{apriv}}, \tag{18}$$

where ID_{r_i} is the identity of $r_i \in W_{\mathcal{R}}$ that can identify him uniquely, and $\mathcal{R}$ is the role bit. It indicates that a user named ID_{r_i} wins the auction as the role of requester and pays for cooperators' locations correctly. After finishing the construction of the anonymous cloaking region, only the winning requester r_i holding $Cert^{(r_i)}$ can send query content to U_{agency} and request LBS with anonymous cloaking region.

Similarly, after winning cooperator $c_j \in W_{\mathcal{C}}$ submits his location, LSP issues a signed role certificate $Cert^{(c_j)}$ to him by Eq. (19)

$$Cert^{(c_j)} = \{\mathrm{ID}_{c_j}, \mathcal{C}\}_{K_{apriv}}, \tag{19}$$

where ID_{c_j} is the identity of $c_j \in W_{\mathcal{C}}$ and $\mathcal{C}$ is the role bit. It confirms that a user named ID_{c_j} wins the auction as the role of cooperator and submits his location. After winning requesters finish querying successfully, only the winning cooperator c_j who behaves honestly and has signed role certificate $Cert^{(c_j)}$ can get gains from LSP.

4.4 Accountability Mechanism

It has been pointed out that users' location privacy leakage can be discovered by themselves based on their bothered daily lives. Specifically, [33] pointed out that the adversary usually provides LBS users' locations to the advertisers for acquiring additional illegal revenue, and the advertisers place targeted advertisements on the snooped users. Besides, the China Consumers Association once pointed out that the snooped users may receive a number of fraud calls, spam emails[1], and financial or time loss [34].

Therefore, when realizing their privacy leakage, the requester r_i and the cooperator c_j can detect and punish malicious users who lead users' location privacy leakage via the accountability mechanism. There're two types of malicious users, including c_j and r_i.

1) Malicious cooperators who submit false location

The malicious cooperator c_j may submit false location to protect his location privacy. Querying with the unreasonable anonymous cloaking region constructed by c_j's false location, r_i finds that his privacy has been threatened and reports this situation to LSP. Therefore, LSP detects which location in anonymous cloaking region is false according to [17]. Once c_j is found, LSP punishes him by refusing to pay, which means that c_j's utility

$$U_{c_j}^{+} = -\sigma_j^{com}. \tag{20}$$

2) Malicious requesters who leak the location information

The malicious requester r_i may disclose received locations to gain additional profits. $r_i \in W_{\mathcal{R}}$ and $c_j \in W_{\mathcal{C}}$ who suffer from it can all complain as follows.

- $r_i \in W_{\mathcal{R}}$ can complain with LSP if he finds he is snooped. In the anonymous cloaking region construction process, $r_i \in W_{\mathcal{R}}$ only sends his location information to U_{agency}, thus LSP can assume that U_{agency} discloses the location information.
- $c_j \in W_{\mathcal{C}}$ can complain with LSP if he finds he is snooped. c_j only sends his location to one winning requester $r_i \in W_{\mathcal{R}}$ who is responsible for c_j's privacy preservation. That is, the c_j's location should be anonymous to everyone except for r_i. Based on it, c_j's privacy leakage is necessarily caused by r_i due to either r_i's deliberate leaking or r_i's incautious privacy-preservation. Thus, LSP identifies r_i as the malicious one and punishes him.

When the malicious requester r_i is found, LSP prevents r_i from participating in PEAK again for requiring location privacy protection. It is fatal for a privacy-sensitive user in LBS, leading r_i's utility

$$U_{r_i}^{+} = -\infty. \tag{21}$$

Once $r_i \in W_{\mathcal{R}}$ and $c_j \in W_{\mathcal{C}}$ lodge a complaint to LSP, they cannot gain any extra profits. Therefore, there are no malicious complaints from users in PEAK as they are all rational in game theory.

Besides, if users themselves do not realize that they have been snooped, their participation enthusiasm will not be affected. Thus, though PEAK does not implement the accountability mechanism when users cannot detect their privacy leakage, PEAK's incentive effectiveness will not be affected and users can still be motivated to participate in the next construction.

5 Scheme Analysis

We first prove that PEAK satisfies design goals and then analyze PEAK's computational complexity.

5.1 Design Goals Analysis

Design goals of PEAK include auction goals and privacy goals. We prove that PEAK satisfies the above design goals, which are shown as follows. The proofs of the following theorems are given in Appendix A.

Auction Goals: PEAK refers the auction model designed in [19], where some auction goals such as *truthfulness* and *satisfaction ratio* are not our priorities and have been proved before. Therefore, the analysis focuses on others, including *individual rationality*, *computational efficiency*, and *resistance of role cheating attack*.

Theorem 1. PEAK's auction process satisfies *individual rationality* proposed in Section. 3.4.

1. Investigation report on App personal information leakage. https://www.cca.org.cn/jmxf/detail/28180.html.

TABLE 3
Comparison of various indexes.

Schemes / *Indexes*	PEAK	Zhang [19]	Fei [20]	Luo [17]
Locations	true	true	dummy	true
CM	✓	✗	✗	✓
MA	✓	✓	✓	✗
MH	✓	✗	✗	✗
WT	✓	✗	✓	✓
CC	$O(x^2)$	$O(m\log m)$	$O(x^2)$	$O(n)$

x: the number of winning requester; m: the number of requesters; n: the number of winning cooperators. CM: Consideration of malicious strategies, MA: Motivation of assistance, MH: Motivation of honest strategies, WT: Without trusted third parties, CC: Computational complexity.

Theorem 2. PEAK's auction process satisfies *computational efficiency* proposed in Section. 3.4.

Theorem 3. PEAK's auction process satisfies *resistance of role cheating attack* proposed in Section. 3.4.

Privacy Goals:

Theorem 4. PEAK satisfies privacy goals proposed in Section. 3.4.

5.2 Computational Complexity Analysis

In this subsection, we analyze the computational complexity of PEAK, whose calculation part mainly includes auction process and location transmission process. Auction process's computational complexity has been analyzed in *Theorem 2* and the location transmission process's is shown as follows.

The location transmission includes sorting process and traversal matching process. The time complexity of sorting process using Quicksort is $O(x\log x+(k-x)\log(k-x))$ and the matching process which needs to be conducted less than $x(k-x)$ times is $O(x(k-x))=O(x^2+kx)$. Therefore, the time complexity of the location transmission process is $O(x\log x+(k-x)\log(k-x))+O(x^2+kx)\approx O(x^2)$.

To sum up, TABLE 3 shows the comparison of various indexes about PEAK and closely related schemes [17], [19], [20]. Specifically, similar to PEAK, both [19], [20] adopt the auction theory to motivate the cooperators' assistance in anonymous cloaking region. Besides, PEAK and [17] all focus on users' malicious strategies that affect the anonymous cloaking region construction. Thus, we compare PEAK with [17], [19], [20] and demonstrate the similarities and the differences between them.

6 Performance Evaluation

In this section, we first exhibit the experimental setup and then explain the experimental results.

6.1 Experimental Setup

Experimental environment: Python language was adopted. Furthermore, the experiment environment is: Intel(R) Core(TM) i7-6700 CPU @ 3.40 GHz, 8192MB RAM, and the Operating System is Windows 7.

Datasets and parameters setup: To implement the performance evaluation reasonably, we adopt the simulated dataset and real-world dataset. In the simulation experiment, we assume that there are 1000 users in the random region, including 500 requesters and 500 cooperators. Meanwhile, we utilize two real-world datasets, including Gowalla [35] and Urban Data Release V2 [36]. Specifically, the Gowalla Dataset [35] records the check-in information of 6442890 users on Gowalla (a location-based social network where users share their locations via check-ins). We extract a total of 15,000 check-in data from the dataset to simulate LBS users. Moreover, Urban Data Release V2 [36] contains 7GB multiple kinds data in the Chinese City Shenzhen. We extract a total of 2000 Cellphone CDR Data to simulate LBS users, which consists SIM card ID, time, latitude, and longitude. According to the proportion of the privacy-sensitive users [30], we divide all the users in above two datasets into the requester set (20% of the total number) and the cooperator set (80% of the total number). These two classical location-based datasets are generally adopted by a large number of the existing works that are related with the location information, guaranteing our experiments' persuasion and rationality. Besides, the Gowalla Dataset [35] is also adopted by [19], which is the compared work of PEAK. Thus, we utilize the Gowalla Dataset to implement the comparison experiments to realize the fairness. The detailed parameters setup is shown in TABLE 4.

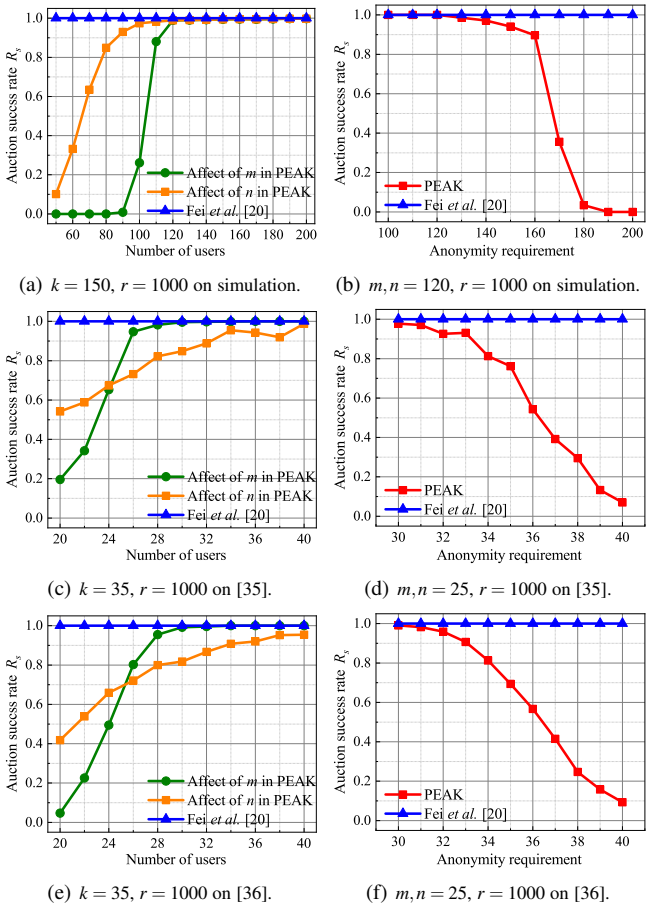
TABLE 4
The parameters setup.

Parameter	Simulation dataset	Real world dataset
m,n	$50,60,...,190,200$	$20,22,...,38,40$
o_i	$(0,2]$	$(0,2]$
a_j	$(0,1]$	$(0,1]$
k	$100,110,...,190,200$	$30,31,...,39,40$
r	$1000,1100,...,9900,10000$	$500,600,...,1400,1500$

Comparison indexes: To demonstrate PEAK's superiority, we adopt [19] and [20] as comparisons and both of them focus on the incentive mechanism in the LBS privacy-preservation, which are similar to PEAK. Specifically, we test the following indexes.

- Incentive effectiveness: PEAK adopts the auction theory to implement the incentive mechanism, which motivates users to not only participate in the anonymous cloaking region construction, but also quit the malicious strategies. The first motivation is determined by the **auction success rate**, where the cooperators can be motivated only if the auction succeeds. The second motivation is reflected by the **users' utilities**, where malicious users will be restrained if their utilities are less than honest one's. Because the auctions adopted by PEAK and [19] are same, we compare PEAK with [20] on the first motivation. Meanwhile, we further compare PEAK with [19] and [20] on the second motivation.

- Design effectiveness: PEAK designs the locations transmission process that may lead to cooperators' trajectory leakage and requesters' heavy burden explained in the Section. 4. Thus, to verify PEAK's design effectiveness, we test the **trajectory information leakage rate** of the cooperators, and **average maximum number of received location** of the requesters. Moreover, to construct the anonymous cloaking region, [19] relies on the trusted third party and [20] requires the dummy but not real locations. Thus, these two works have no such problems

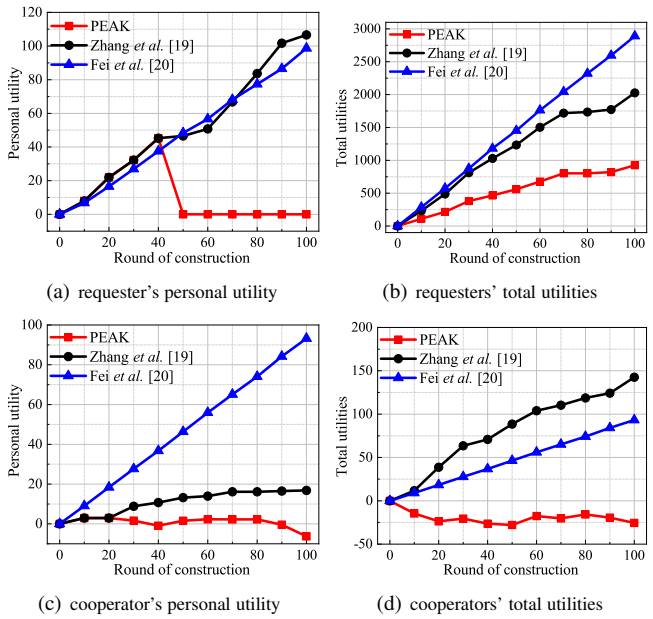


(a) $k = 150$, $r = 1000$ on simulation. (b) $m,n = 120$, $r = 1000$ on simulation.

(c) $k = 35$, $r = 1000$ on [35]. (d) $m,n = 25$, $r = 1000$ on [35].

(e) $k = 35$, $r = 1000$ on [36]. (f) $m,n = 25$, $r = 1000$ on [36].

Fig. 7. Auction success rate R_s



(a) requester's personal utility (b) requesters' total utilities

(c) cooperator's personal utility (d) cooperators' total utilities

Fig. 8. Users' utilities

we mentioned above, which is the reason of the absence of comparison experiment in this part.

- Computational delay: The scheme cannot be applied in reality if its computational process is excessively complicated. Thus, we test the **computational delay** of PEAK and further compare PEAK with [19] and [20] to reflect the above works' computational feasibility. Note that here we ignore the transmission delay because it is too tiny with the coming of 6G era.

6.2 Incentive Effectiveness

6.2.1 *Auction Success Rate*

Defining the auction success rate as $R_s = \frac{r^+}{r}$, where r is the round of continuous anonymous cloaking region construction and r^+ is the time of success, we investigated the influence of the users' number and the anonymity requirements on the auction success rate R_s in PEAK and [20].

The experiment results are shown in Fig. 7. In PEAK, when the requesters' number is small, we find that $R_s \to 0$, indicating that the auction can succeed seldomly. The reason is that requesters cannot afford more cooperators when the number of requesters is too small and the anonymity requirements is high. When the number of requesters increases, R_s increases quickly and is close to 1. When the number of requesters is greater than that of anonymity requirements, the requesters can construct the anonymous cloaking region by themselves without the cooperators' assistance so that $R_s = 1$. Besides, with the increase of the number of cooperators, R_s increases gradually and approach 1 indefinitely. Fig. 7(b), (d), and (f) show the impact of anonymity requirements k on the auction success rate R_s. At this time, we can find that as k increases, the number of cooperators required by requesters also increases, and requesters are unable to afford them gradually. Thus, R_s decreases. Aiming at [20], we can find that with the increase of users' number and the anonymity requirement, $R_s = 1$ always exists. The reason is that [20] designs the auction where the user bidding lowest wins the auction and other users compensate this winning user. This winning determination strategy guarantees the auction can always success because there necessarily exists a user with the lowest bid.

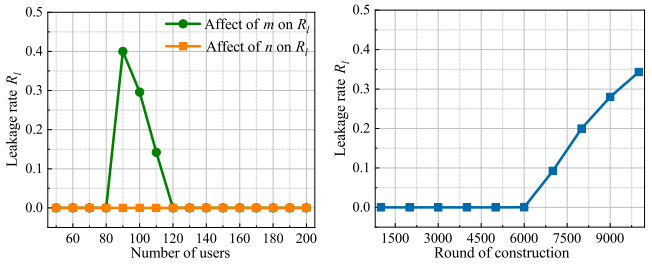
Due to the proper adoption of the sealed-bid double auction, with reasonable numbers of users and anonymity requirements, PEAK's auction success rate is more than 90%. Thus, PEAK is able to motivate the cooperators to participate in the anonymous cloaking region construction effectively.

6.2.2 *Users' utilities*

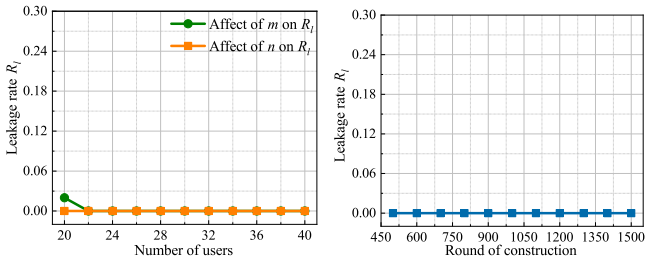
To indicate PEAK's incentive effectiveness on the honest strategies, we test users' utilities in PEAK, the work [19] and the work [20] in 100 rounds of anonymous cloaking region construction based on the real-world dataset Gowalla [35].

Users' utilities in different works are shown in Fig.8. When users choose malicious strategies randomly, personal utility and total utilities in the work [20] and the work [19] increase steadily, which indicates that malicious requesters is not punished. However, as shown in Fig.8(a), in 40-50 th round, requester's utility drops to 0 because of malicious strategy in PEAK. And Fig.8(b) shows that requesters' total utilities are also increasing slowly in PEAK compared with other works. Fig.8(c) and Fig.8(d) indicate that when cooperators choose malicious strategies randomly, their utilities decrease quickly and even to negative.

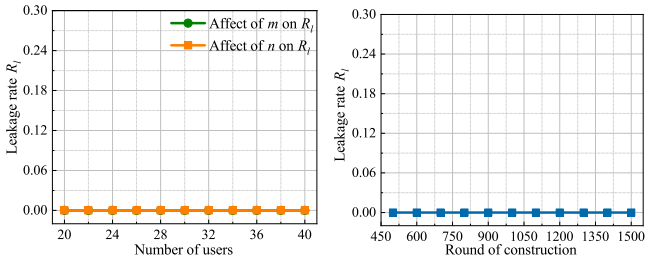
Thus, PEAK can punish and restrain malicious users. Rational users who seek for maximized utilities will not choose malicious strategies.



(a) $k = 150$, $r = 10000$ on simulation. (b) $m,n = 120$, $k = 150$ on simulation.

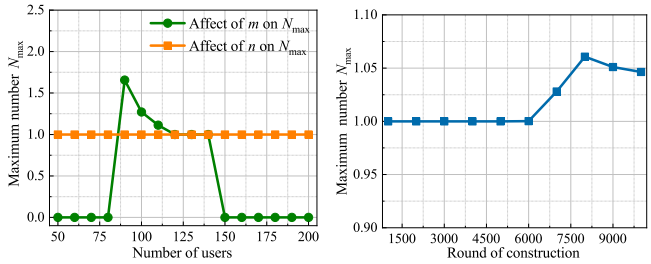


(c) $k = 35$, $r = 1000$ on [35]. (d) $m,n = 25$, $k = 35$ on [35].

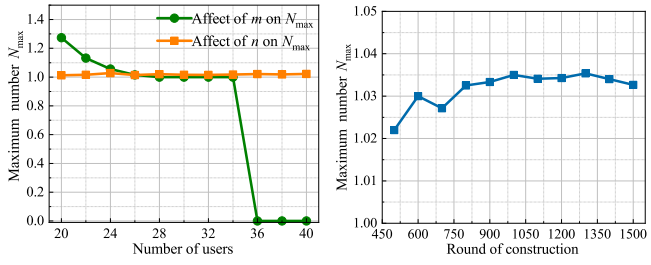


(e) $k = 35$, $r = 1000$ on [36]. (f) $m,n = 25$, $k = 35$ on [36].

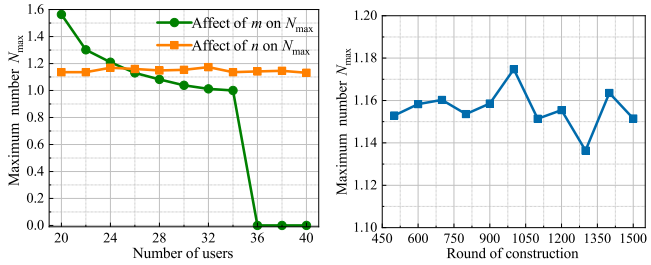
Fig. 9. Trajectory information leakage rate R_l



(a) $k = 150$, $r = 5000$ on simulation. (b) $m,n = 120$, $k = 150$ on simulation.



(c) $k = 35$, $r = 1000$ on [35]. (d) $m,n = 25$, $k = 35$ on [35].



(e) $k = 35$, $r = 1000$ on [36]. (f) $m,n = 25$, $k = 35$ on [36].

Fig. 10. Average maximum number of received location $N_{\max}$

6.3 Design Effectiveness

6.3.1 Trajectory Information Leakage Rate

The leakage rate is defined as $R_l = \frac{r^*}{r}$, in which r is the round of continuous anonymous cloaking region construction and r^* is the round when the winning cooperator submits his location to the same winning requester. We study the influence of the users' number and the round of continuous anonymous cloaking region construction on the trajectory information leakage rate R_l respectively.

Fig. 9 (a), (c), (e) show the influence of the users' number on R_l. We conclude that R_l is high slightly when $m = 90$ in the Fig. 9(a). This is because there are few targeted requesters to select for the cooperators. As the number of requesters increases, R_l decreases significantly. In addition, R_l is not affected by the cooperators' number very much. When the number of requesters is reasonable, R_l always keeps 0 with the increase of the cooperators' number. This tendency can be discovered in the experiments based on both simulation dataset and real-world dataset. Fig. 9 (b), (d), (f) shows the influence of r on R_l. In Fig. 9(b), when $r = 6000$, PEAK can still guarantee $R_l = 0$, and when $r = 10000$, $R_l < 0.35$. Meanwhile, under the real-world dataset, PEAK always holds $R_l = 0$, which means that PEAK can guarantee the privacy of user's trajectory after 1500 anonymous cloaking regions are constructed continuously.

Due to the proper location transmission between users, PEAK prevents the cooperators from submitting their multiple locations to the same requester. Therefore, in general, PEAK can still guarantee a low trajectory information leakage rate R_l after constructing anonymous cloaking regions for several times.

6.3.2 Average Maximum Number of Received Location

Here we investigate the influence of the users' number, the round of continuous anonymous cloaking region construction on the average maximum number of location $N_{\max}$ received by the winning requester.

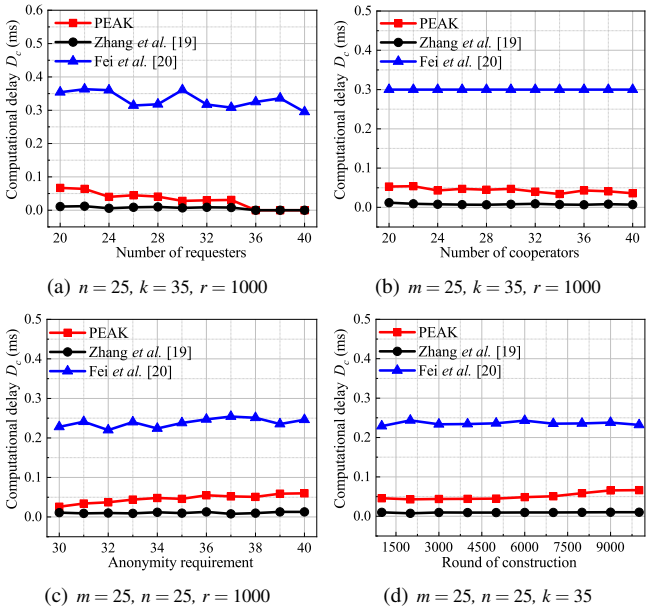
The influence of the users' number on $N_{\max}$ can be discovered in Fig. 10(a), (c), (e). We find that when the auction succeeds, $N_{\max}$ decreases with the increase of the requesters' number. When the number of requesters is small, $N_{\max}$ is slightly high (1.7 in Fig. 10(a), 1.3 in Fig. 10(c), and 1.6 in Fig. 10(e)). When the requesters' number is slightly increasing, $N_{\max} = 1$. Note that when $m \geq 150$ in Fig.10(a) and $m \geq 35$ in Fig.10(c), (e), the requesters can construct the anonymous cloaking region so that they will not receive any location from the cooperators, meaning $N_{\max} = 0$. Meanwhile, the cooperators' number cannot make much difference to $N_{\max}$, which is pretty much stable at 1 with the increase of n. Besides, Fig. 10(b), (d), (f) show the influence of r on $N_{\max}$. In the Fig 10(b), with $6000 < r \leq 10000$, the maximum of $N_{\max}$ is less than 1.1, which means that almost all winning requesters receive no more than one location information. Moreover, under the real-world dataset in the Fig. 10 (d), (f), the maximum of $N_{\max}$ is also close to 1.

Because of the proper location transmission, PEAK forbids all the cooperators to submit their locations to one requester. Thus, PEAK can control the amount of location received by each

winning requester while protecting the cooperators' trajectory privacy ($R_l = 0$) after constructing anonymous cloaking regions for several rounds, so as to avoid the single point of failure.

6.4 Computational Delay

Based on the real-world dataset Gowalla [35], we investigate the influence of the users' number, the anonymity requirements and the round of continuous anonymous cloaking region construction on the computational delay D_c required to construct an anonymous cloaking region.



(a) $n = 25$, $k = 35$, $r = 1000$ (b) $m = 25$, $k = 35$, $r = 1000$

(c) $m = 25$, $n = 25$, $r = 1000$ (d) $m = 25$, $n = 25$, $k = 35$

Fig. 11. Computational delay D_c

Fig.11(a) indicates the influence of the requesters' number on D_c. When the number of requesters increases, D_c of PEAK and the work [19] decrease gradually. Besides, PEAK's D_c is 0.05ms ahead of the work [19]'s, which is negligible. When $m > 35$, indicating that the number of requesters is no less than that of anonymity requirements, the anonymous cloaking regions can be constructed successfully without an auction so that D_c is 0. The work [20]'s D_c remains at 0.3ms and is hardly affected by the requesters' number.

Fig.11(b) shows the influence of the cooperators' number on D_c. Because the work [20] has only one cooperator in any case, we show D_c of it when $n = 1$. It is worth noticing that the number of cooperators have seldom influence on D_c under three works. D_c of PEAK and the work [19] is in 0.1ms with the change of the cooperators' number.

Fig.11(c) explains the influence of k on D_c under three works. When $k > m$, D_c increases with k and D_c of the PEAK is only increased by 0.05ms compared with the work [19], which is acceptable. In work [20], with the increase of k, more dummies need to be constructed. Thus, D_c is increasing slightly.

Fig.11(d) provides the influence of r on D_c. We can find that r has little influence on D_c under the work [19] and the work [20]. However, in PEAK, the continuously multiple constructions of anonymous cloaking region make the historical transmission record R_h more abundant, and it is more difficult to determine the transmission relationship of location between users. Thus, D_c increases with r slightly, which can still be kept below 0.1ms after 10000 rounds of constructions and is acceptable.

Therefore, with many advantages, PEAK can also guarantee a low computational delay D_c compared with existing works.

7 Conclusion and Future Work

In this paper, we proposed a privacy-enhanced incentive mechanism for K-anonymity location preservation PEAK without the trusted server. Referring to the auction theory, PEAK first determined the monetary transaction between the requesters and the cooperators. Then, PEAK realized the location transmission between winning requesters and cooperators to construct the anonymous cloaking region. With the proposed role identification and accountability mechanisms, PEAK constrained users' malicious strategies, which protects users' location privacy while motivating cooperators' assistance effectively. Extensive experiments demonstrated that PEAK achieved a high anonymous cloaking region construction success rate, avoided the trajectory information leakage, single point of failure efficiently and decreased the malicious users' utilities significantly.

However, PEAK can only motivate users' honest strategies based on the condition that the users all crave the higher utilities, which means that users are all rational. As part of future work, we will further take the fully malicious or non-rational users into consideration so that such users can also be encouraged to participate in the anonymous cloaking region construction and quit the malicious strategies.

References

[1] Google, "Google maps," [EB/OL], http://www.gugeditu.net Accessed December 14, 2020.
[2] Dianping, "Dianping," [EB/OL], https://www.dianping.com/ Accessed December 14, 2020.
[3] Foursquare, "Foursquare," [EB/OL], https://foursquare.com/ Accessed December 14, 2020.
[4] gowalla, "gowalla," [EB/OL], https://go.gowalla.com/ Accessed December 14, 2020.
[5] Y. Chen, T. Zhou, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Save: Efficient privacy-preserving location-based service bundle authentication in self-organizing vehicular social networks," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–15, 2021, doi: 10.1109/TITS.2021.3106783.
[6] W. Chen, Z. Yin, and T. He, "Enabling global cooperation for heterogeneous networks via reliable concurrent cross technology communications," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021, doi: 10.1109/TMC.2021.3066568.
[7] G. of India, "Aarogya setu," [EB/OL], https://www.aarogyasetu.gov.in/ Accessed September 14, 2021.
[8] G. Cui, Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang, "Location privacy protection via delocalization in 5g mobile edge computing environment," *IEEE Transactions on Services Computing*, pp. 1–1, 2021, doi: 10.1109/TSC.2021.3112659.
[9] J. Tang, H. Zhu, R. Lu, X. Lin, H. Li, and F. Wang, "Dlp: Achieve customizable location privacy with deceptive dummy techniques in lbs applications," *IEEE Internet of Things Journal*, pp. 1–1, 2021, doi: 10.1109/JIOT.2021.3115849.
[10] W. Luo, Y. Lu, D. Zhao, and H. Jiang, "On location and trace privacy of the moving object using the negative survey," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 1, no. 2, pp. 125–134, 2017.
[11] S. Zhao, X. Luo, B. Bai, X. Ma, W. Zou, X. Qiu, and M. Au, "I know where you all are! exploiting mobile social apps for large-scale location privacy probing," in *Proc. Australasian Conference on Information Security and Privacy. (ACISP'16)*, 2016, pp. 3–19.
[12] Z. Wang, D. Zhang, X. Zhou, D. Yang, Z. Yu, and Z. Yu, "Discovering and profiling overlapping communities in location-based social networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 4, pp. 499–509, 2014.
[13] X. Chen, J. Pang, and R. Xue, "Constructing and comparing user mobility profiles for location-based services," in *Proc. ACM Symposium on Applied Computing. (SAC'13)*, 2013, pp. 261–266.

[14] C. Chow, M. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based service," in *Proc. Acm International Symposium on Advances in Geographic Information Systems. (GIS'06)*, 2006, pp. 171–178.
[15] J. Kang, D. Steiert, D. Lin, and Y. Fu, "Movewithme: Location privacy preservation for smartphone users," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 711–724, 2020.
[16] B. NIU, Y. Chen, Z. Wang, f. li, B. Wang, and H. Li, "Eclipse: Preserving differential location privacy against long-term observation attacks," *IEEE Transactions on Mobile Computing*, 2020, doi: 10.1109/TMC.2020.3000730.
[17] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in vanet," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020.
[18] S. Reddy, D. Estrin, and M. H. Hansen, "Examining micro-payments for participatory sensing data collections," in *Proc. ACM international conference on Ubiquitous computing. (UbiComp'10)*, 2010, pp. 33–36.
[19] Y. Zhang, W. Tong, and S. Zhong, "On designing satisfaction-ratio-aware truthful incentive mechanisms for k -anonymity location privacy," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2528–2541, 2016.
[20] F. Fei, S. Li, H. Dai, C. Hu, W. Dou, and Q. Ni, "A k-anonymity based schema for location privacy preservation," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 2, pp. 156–167, 2019.
[21] D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *Proc. IEEE Conference on Computer Communications. (INFOCOM'13)*, 2013, pp. 2994–3002.
[22] X. Li, M. Miao, H. Liu, J. Ma, and K. Li, "An incentive mechanism for k-anonymity in lbs privacy protection based on credit mechanism," *Soft Computing*, vol. 21, no. 14, pp. 3907–3917, 2017.
[23] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: anonymous location-based queries in distributed mobile systems," in *Proceedings of the 16th International Conference on World Wide Web, WWW 2007, Banff, Alberta, Canada, May 8-12, 2007*. ACM, 2007, pp. 371–380.
[24] H. Zhangwei and X. Mingjun, "A distributed spatial cloaking protocol for location privacy," in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, 2010, pp. 468–471.
[25] G. Sun, D. Liao, H. Li, H. Yu, and V. I. Chang, "L2P2: A location-label based approach for privacy preserving in LBS," *Future Gener. Comput. Syst.*, vol. 74, pp. 375–384, 2017.
[26] R. Gupta and U. P. Rao, "Achieving location privacy through CAST in location based services," *J. Commun. Networks*, vol. 19, no. 3, pp. 239–249, 2017.
[27] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial k-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Gener. Comput. Syst.*, vol. 94, pp. 40–50, 2019.
[28] Z. Tu, K. Zhao, F. Xu, Y. Li, L. Su, and D. Jin, "Protecting trajectory from semantic attack considering k-anonymity, l-diversity, and t-closeness," *IEEE Trans. Netw. Serv. Manag.*, vol. 16, no. 1, pp. 264–278, 2019.
[29] X. Zhang, Z. Yang, W. Sun, Y. Liu, S. Tang, K. Xing, and X. Mao, "Incentives for mobile crowd sensing: A survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 54–67, 2016.
[30] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.
[31] Z. Wang, J. Li, J. Hu, J. Ren, Z. Li, and Y. Li, "Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform," in *Proc. IEEE Conference on Computer Communications. (INFOCOM'19)*, 2019, pp. 2053–2061.
[32] X. Wu, S. Li, J. Yang, and W. Dou, "A cost sharing mechanism for location privacy preservation in big trajectory data," in *Proc. IEEE International Conference on Communications. (ICC'17)*, 2017, pp. 1–6.
[33] H. Kaldestad, "Out of control," https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf.
[34] M. Li, Y. Chen, N. Kumar, C. Lal, M. Conti, and M. Alazab, "Quantifying location privacy for navigation services in sustainable vehicular networks," *IEEE Transactions on Green Communications and Networking*, pp. 1–1, 2022.
[35] E. Cho, S. Myers, and J. Leskovec, "Friendship and mobility: User movement in location-based social networks," in *Proc. ACM SIGKDD international conference on Knowledge discovery and data mining. (KDD'17)*, 2011, pp. 1082–1090.
[36] D. Zhang, J. Zhao, F. Zhang, and T. He, "Urbancps: a cyber-physical system based on multi-source big infrastructure data for heterogeneous model integration," in *Proceedings of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems, ICCPS 2015, Seattle, WA, USA, April 14-16, 2015*. ACM, 2015, pp. 238–247.
[37] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the First International Conference on Mobile Systems, Applications, and Services, MobiSys 2003, San Francisco, CA, USA, May 5-8, 2003*, D. P. Siewiorek, M. Baker, and R. T. Morris, Eds. USENIX, 2003, pp. 31–42.

APPENDIX A
DESIGN GOALS ANALYSIS

Auction Goals:

Theorem 1. PEAK's auction process satisfies *individual rationality* proposed in Section. 3.4.

Proof: Each winning requester $r_i \in W_{\mathcal{R}}$ needs to pay $p_i = \frac{(k-x)a_{k-x+1}}{x}$, where the "*pivot ask*" a_{k-x+1} satisfies $xo_x \geq (k-x)a_{k-x+1}$, so we can conclude that

$$p_i = \frac{(k-x)a_{k-x+1}}{x} \leq \frac{(k-x)}{x} \cdot \frac{xo_x}{(k-x)} = o_x \leq o_i. \tag{22}$$

That is, the payment p_i of winning requester $r_i \in W_{\mathcal{R}}$ is less than his offer $o_i = v_i$ when he bids honestly, thus r_i's utility is

$$U_{r_i}^{+} = v_i - p_i = o_i - p_i \geq 0,\ \forall r_i \in W_{\mathcal{R}}. \tag{23}$$

Each losing requester $r_i \notin W_{\mathcal{R}}$ does not need to pay any payment, and the privacy value he gets is also zero. Thus, his utility is

$$U_{r_i}^{-} = 0,\ \forall r_i \notin W_{\mathcal{R}}. \tag{24}$$

Therefore, PEAK satisfies the requesters' individual rationality, that is, $U_{r_i} \geq 0, \forall r_i \in \mathcal{R}$.

Each winning cooperator $c_j \in W_{\mathcal{C}}$ will pay the cost $\sigma_j = \sigma_j^{com} + \sigma_j^{pri}$ ($\sigma^{pri} = 0$ when his location information is preserved) and get gain $g_j = \max a_{k-x+1}$, with $a_{k-x+1} > a_{k-x}$ and a_{k-x} is the highest ask in all winning requesters, thus we can conclude that

$$g_j = \max a_{k-x+1} \geq a_{k-x+1} > a_{k-x} \geq a_j. \tag{25}$$

That is, c_j's gain g_j is more than his ask a_j equaling $\sigma_j = \sigma_j^{com} + \sigma_j^{pri}$ when he bids honestly, thus c_j's utility is

$$U_{c_j}^{+} = g_j - \sigma_j = g_j - a_j \geq 0,\ \forall c_j \in W_{\mathcal{C}}. \tag{26}$$

Each losing cooperator $c_j \notin W_{\mathcal{C}}$ does not need to pay any cost, and the gain he gets is also zero, then his utility is

$$U_{c_j}^{-} = 0,\ \forall c_j \notin W_{\mathcal{C}}. \tag{27}$$

Therefore, PEAK satisfies the cooperators' individual rationality, that is, $U_{c_j} \geq 0, \forall c_j \in \mathcal{C}$. □

Theorem 2. PEAK's auction process satisfies *computational efficiency* proposed in Section. 3.4.

Proof: The auction process includes two steps, sorting and reverse search. Thus when we use Quicksort to sort the requesters and cooperators according to their bids, including m requesters and n cooperators, the time complexity of this process is $O(m\log m + n\log n)$. In addition, the time complexity of reverse search for determining winning requesters and cooperators is $O(1)$. Therefore, the time complexity of the auction process is $O(m\log m + n\log n) + O(1) \approx O(m\log m + n\log n)$ and the auction can be finished in the polynomial time, which means that it satisfies computational efficiency. □

Theorem 3. PEAK's auction process satisfies *resistance of role cheating attack* proposed in Section. 3.4.

Proof: With the role identification mechanism, the utility of the malicious requester $\gamma \in \mathcal{R}$ launching the role cheating attack is

$$\tilde{U}_\gamma = g_i{}' - \sigma_i = g_i{}' - (\sigma_i^{com} + \sigma_i^{pri}), \tag{28}$$

which means that γ can only obtain the utilities as the normal cooperators, instead of the privacy protection services they desire. However, the requesters are rational and their basic purposes of participation in the auction are privacy-preserving services. Therefore, rational requesters will not choose the role cheating attack. □

Privacy Goals:

Theorem 4. PEAK satisfies privacy goals proposed in Section. 3.4.

Proof: With the accountability mechanism, the malicious users' utilities are as follows.

When the winning cooperator sends the false location information, the winning requester's utility is defined as

$$U^+_{r_i\_1} = (-p_i + U^{leak}_{r_i}) \geq U^+_{r_i\_2} = -p_i. \tag{29}$$

Note that we cannot punish the malicious requester as the cooperator just sends the false location information, and the malicious requester's utility is same as the analysis in Section.3.

When the winning cooperator sends the true location information, the winning requester's utility is defined as

$$U^+_{r_i\_3} = -\infty \leq U^+_{r_i\_4} = (v_i - p_i), \tag{30}$$

which means that the requester can be detected and punished when leaking the true location. For example, the malicious requester is refused to participate in the auction again to gain location privacy protection, which makes his utility negative infinity. On the other hand, if the requester preserves the location information, his utility is $v_i - p_i$ which is more than the malicious utility.

If the winning requester leaks the received location information, the winning cooperator's utility is defined as

$$U^+_{c_j\_1} = -\sigma_j^{com} \leq U^+_{c_j\_3} = (g_j - \sigma_j^{com} - \sigma_j^{pri}). \tag{31}$$

When the cooperator submits the false location, he can be punished and get no gain. His utility is defined as $g_j - \sigma_j = g_j - \sigma_j^{com} - \sigma_j^{pri}$ when submitting the true location.

If the winning requester preserves the received location information, the winning cooperator's utility is defined as

$$U^+_{c_j\_2} = -\sigma_j^{com} \leq U^+_{c_j\_4} = (g_j - \sigma_j^{com}). \tag{32}$$

When the cooperator submits the false location, he still get no gain. His utility is defined as $g_j - \sigma_j^{com}$ when submitting the true location.

Based on the above analysis, both requesters and cooperators will choose honest strategies rationally and satisfy their utilities in PEAK. Thereby, the Nash Equilibrium of the location transmission game between users is defined as $\mu^* = \{\mu^{(t)}, \mu^{(p)}\}$ and PEAK satisfies privacy goals. □

Moreover, except for the attacks defined in the Section. 3.3, PEAK can also resist some well-known privacy attacks, including **the restricted space identification** and **the location tracking** [37]. These two attacks claim that the adversary can spy on users' privacy information (e.g. political affiliations, alternative lifestyles, and medical problems).

1) Resist the restricted space identification

The restricted space identification claims that if the adversary knows that the location $\mathcal{L}$ exclusively belongs to the user, then the adversary learns that the user is in $\mathcal{L}$ and has sent message $\mathcal{M}$. For example, when the owner of the office queries the distribution of neighbouring patients, his location can be correlated with a database of geocoded postal addresses, revealing this office owner's identify that may just be the originator of the distribution query. However, in PEAK, the requesters' location tuple is K-anonymous, which means that K-anonymity is realized and the adversary cannot identify the originator of the distribution query of neighbouring patients among K locations. Meanwhile, [37] has proved that K-anonymity can effectively resist the restricted space identification. Without anymore information, the requesters' location leakage probability is no more than $\frac{1}{K}$. Thus, PEAK is able to resist the restricted space identification.

2) Resist the location tracking

Besides, the location tracking claims that if the adversary can identify the user at location $\mathcal{L}_i$ as well as link series of locations $\mathcal{L}_1$, $\mathcal{L}_2$, ..., $\mathcal{L}_i$, ..., $\mathcal{L}_n$ to the user, then the adversary learns that the user visited all locations above. For example, when the user queries the distribution of neighbouring patients at his office and residence, his daily moving trajectory can be snooped. However, in PEAK, each round of querying is based on the K-anonymous cloaking region. Meanwhile, [37] has proved that K-anonymity can effectively resist the location tracking, meaning that the adversary can hardly recognize the user's real location from the anonymous cloaking region which consists of $K-1$ locations. Though user enjoys LBS for multiple times, it's difficult for the adversary to trace the user's daily trajectory. Thus, PEAK is able to resist the location tracking.