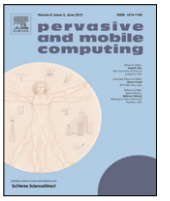
Pervasive and Mobile Computing 9 (2013) 598–612

Contents lists available at SciVerse ScienceDirect

Pervasive and Mobile Computing

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



Fast track article

Trading privacy with incentives in mobile commerce: A game theoretic approach

Anil Kumar Chorppath [a,*], Tansu Alpcan [b]

[a] Lehrstuhl für Theoretische Informationstechnik, Technical University of Munich, 80333 Munich, Germany

[b] Department of Electrical and Electronic Engineering, The University of Melbourne, VIC 3010, Australia

ARTICLE INFO

Article history:
Available online 7 August 2012

Keywords:
Game theory
Mobile commerce
Privacy
Mechanism design
Information theoretic metrics

ABSTRACT

In mobile commerce, companies provide location based services to mobile users, who report their locations with a certain level of granularity to maintain a degree of anonymity. This level of granularity depends on their perceived risk as well as the incentives they receive in the form of monetary benefits or improved mobile services. This paper formulates a quantitative model in which information theoretic metrics such as entropy, quantify the anonymity level of mobile users. The individual perceived risks of users and the benefits they obtain are defined as functions of their chosen location information granularity. The interaction between the mobile commerce company and its users is investigated using mechanism design techniques as a privacy game. The user best responses and optimal strategies for the company are derived under budgetary constraints on incentives, which are provided to users in order to convince them to share their private information at the desired level of granularity. Information limitations in the system are analyzed to capture more realistic scenarios where the companies do not have access to user utility functions. Iterative distributed algorithm and regression learning methods are investigated to design mechanisms that overcome these limitations. The results obtained are demonstrated with a numerical example and simulations based on real GPS data.

1. Introduction

We consider a mobile commerce environment in which the users or customers get benefits from a company (service provider) by disclosing their location with certain degree of accuracy. At the same time, disclosing their location information brings users certain risks and compromises their privacy. Therefore, users have a motivation to maintain anonymity by giving less granular information about their location or no information at all. In this paper, we propose a *mechanism design* [1] approach in which the company acts as a designer and properly motivates its users through the benefits in terms of payment [2] provided to them, in order to obtain desired *granularity of location information* from all the users. We refer to the mechanisms in this setting as *privacy mechanisms*.

The benefits offered by the company to the users can be the location based service resources, discount coupons or monetary awards. We assume that the more accurate the information, the more valuable it is for the company. For example, street level information leads to contextual advertisements while city level granularity is less valuable. Concurrently, by being less anonymous, the users take a privacy risk. We take a commodity view of the privacy here, where the users can trade their privacy to obtain benefits from the company in an individual risk aware way.

* Corresponding author.
E-mail addresses: anilkchorppath@gmail.com, anil.chorppath@tum.de (A.K. Chorppath), tansu.alpcan@unimelb.edu.au (T. Alpcan).

1574-1192/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.pmcj.2012.07.011

The Fair Information Practice Principle (FIPP) is the global standard that addresses consumer privacy risks. There are three main approaches [3] to implement FIPP: government regulation, self regulation by industry and Privacy Enhancing Technologies (PETs). The Privacy Enhancing Technologies (PETs) try to preserve the privacy of users while giving targeted advertisements and services using personal data. We consider our approach as complimentary to PETs, rather than as a substitute. The advertising and service provider industry is moving towards more self regulation which will enhance innovation and competition and ensure benefits for users in addition to safe guards provided by the government regulation [4]. The market based approach presented here models the incentive mechanisms behind this trend.

This paper presents an analytical model and a quantitative approach towards the risk-benefit trade-off of users and the goal of the companies. It uses metrics from information theory to quantify the anonymity level of users, concepts from game theory [5] to model the interaction of users among themselves and the company, convex optimization techniques for solution and learning theory to learn the user risk levels and utility functions of the users by the designer.

In this paper, we use an *information theoretic* approach [6] to quantify the *anonymity level* of the individual mobile users. The size of the crowd in which a user prefers to belong can be mapped to the desired anonymity level which can be further mapped to the granularity of location information. Therefore, the users have the power to make decisions on the level of granularity of location information reported to the service provider who gives them benefits based on that. An incentive or pricing mechanism is designed to achieve the company's goal of extracting the desired level of granularity of information. The company tries to move the Nash Equilibrium (NE) point vector of granularity of information in the underlying game to a desirable point as done in [7].

We provide an analytical model with general concave utility functions and scalar risk levels for the users. A motivating example is given with logarithmic utility functions and in this case the designer needs to know the risk levels for the implementation of the privacy mechanism. A method to learn the risk levels is presented in which a properly selected sample benefit vector is used by the designer. For general concave utility functions, a distributed implementation is provided using an iterative algorithm to drive the system to optimal level of granularity vectors. For a scenario in which the designer don't know the general concave utility functions and scalar risk levels of the users, a regression learning method [8] is presented to learn the marginal utilities of the users and to take the system to the optimum.

The next section presents the underlying system privacy model and various parameters. Section 3 introduces the game theoretic and mechanism design concepts into the privacy model. Section 4 analyzes the privacy mechanism design problem and the solution. Then in Section 4.2 a learning method for learning the risk factors of users by the designer is discussed. In Section 5 an iterative distributed algorithm based on the gradient approach is proposed to learn the utilities of the users by the designer. The convergence analysis of the proposed mechanism is also given. Then in Section 6, the regression learning techniques are used to obtain the optimal granularity level by the company without knowing the risk factor or the utility functions of the users. Numerical simulations and their results are shown in Section 7. Section 8 gives the literature review. The paper concludes with remarks in Section 9.

2. Privacy model

Consider a mobile network composed of a set of mobile users with cardinality N. Around user i at any time t, let a group of $n_i(t)$ mobile users, A, be in close proximity in an area. The service provider gives location based applications to the mobile users. Therefore, it asks for the location information from the mobiles.

We use an information theoretic approach to quantify the anonymity level of the individual mobile users while giving the location information. The uncertainty of service provider about the location information of user i is defined using the entropy term

$$A_i = \sum_{i=1}^{n_i(t)} p_i \log_2 \frac{1}{p_i}$$

where probability p_i corresponds to the probability that a user is in a location. The parameter A_i concurrently quantifies the anonymity level of a users i. We can see that $p_i = \frac{1}{\log_2 n_i(t)}$. Then A_i simply boils down to,

$$A_i = \log_2 n_i(t). \tag{1}$$

We next define a metric called *granularity of location information*, g_i, for the ith user as

$$g_i = 1 - \frac{A_i}{\log_2 N}. \tag{2}$$

The value of g_i is between zero and one for each user. The anonymity level obtained by user i by reporting with a granularity level g_i is

$$A_i = (1 - g_i)\ \log_2 N.$$

Here, $g_i = 0$ means the user i keeps its location completely private and $g_i = 1$ means the user gives an exact location to the mobile company. We can see that the greater the value of g, the less anonymous the users. With a given value of g_i the users

Table 1
Values of $n_i(t)$, N and g.

$n_i(t)$	N	g
10^1	10^3	$\frac{2}{3}$
10^3	10^6	$\frac{1}{2}$
10^6	10^9	$\frac{1}{3}$

specify the size of the crowd they belong to, i.e., $n_i(t)$. The Table 1 gives values of g for different combinations of $n_i(t)$ and N. We can see that as the size of the population N increases the users become more anonymous.

The users decide on the value of g which they report to the company. In the scenario considered in this model, the users have a continuous decision space resulting from a risk-benefit trade-off optimization, i.e. the allowed decisions are not just full or null information. This allows the designer to provide benefit based on the level of information given by the users.

There is a cost of perceived risk c_i associated with the user's privacy when they give location information, which linearly increases with the granularity of information, i.e.,

$$c_i = r_i g_i,$$

where r_i is the risk factor. The risk factor may result from disclosing your daily routine or behavior to unknown parties. For example, the users may not like others to know when they are in their office or home or they may simply care about their privacy on principle. The users estimate or learn about their risk level from past experiences or from reliable sources or by exchanging information with other users such as the value of g with which they report to the designer.

While gaining on location privacy, each user loses on the benefits of location based applications/services due to the anonymity. For example, while depending on whether users are in office, home or a particular street or city, they might be targeted with different kinds of offers and services. When they give incorrect information they are given incorrect services and offers. The total benefit obtained by user i can be quantified as

$$s_i = b_i(g)U_i(g_i),$$

where $b_i(g) \in R^+$ is the benefit or subsidy factor provided by the company and $U_i(.)$ is any user specific nondecreasing, concave and differentiable function. Note that the benefit factor b_i provided for user i is designed based on the granularity level chosen by all the users. In other words, the company provides benefit factors based on the total available information in the actual "information market" for a location based application. The users are assumed to be price taking here and therefore they take the benefit factors as constants when they decide on their optimal granularity level. The company requires some minimum level of location information to run an application. Hence the marginal utility provided to the user in the low granularity level region is higher since the marginal increase in the value of her location information is higher in this region. Therefore we model total benefit provided to the user as a nondecreasing, concave function of her granularity level. We take the logarithmic assumption in this paper but it can be generalized to any nondecreasing, concave function.

We now summarize the definitions of some of the terms discussed so far.

1. *(Location) privacy*: (Location) privacy of an individual user refers to how she discloses and controls the dissemination of her personal (location) data.
2. *Anonymity (location)*: Anonymity of a user i, A_i, is the uncertainty of the service provider about the user's location.
$$A_i = \sum_{i=1}^{n_i(t)} p_i \log_2 \frac{1}{p_i}.$$
3. *Granularity of information*: Granularity of information is the level of granularity with which a user i reports its location.
$$g_i = 1 - \frac{A_i}{\log_2 N}.$$
4. *Perceived risk (cost)*: It is the total cost perceived by user i as a result of reporting her location with a certain level of granularity of information, which is modeled as linear in g_i,
$$c_i = r_i g_i.$$
5. *Benefit*: The total subsidy or reward user i obtains from the mobile commerce company by disclosing her location with a certain level of granularity of information,
$$s_i = b_i(g)U_i(g_i).$$

3. Privacy games and mechanisms

In a mechanism design setting, there is a *designer D* at the center who influences *N players* participating in a *strategic (non cooperative) game*. Let us define the interaction of the users in the close proximity in the above setting as an N-player

strategic game, G, where each player $i \in A$ has a respective *decision variable* g_i such that

$$g = [g_1, \ldots, g_N] \in X \subset N,$$

where X is the decision space of all players. The cost of each mobile user i will be the risk it perceives minus the benefits it obtains from the company, i.e.,

$$J_i(g) = r_i g_i - b_i U_i(g_i) \quad \forall i.$$

Each mobile user then solves her own optimization problem

$$\min_{g_i} J_i(g). \tag{3}$$

Note that from the user perspective the benefit b_i is a constant designed by the company since each user has an information constraint and cannot know the granularity level of other users to calculate its own benefit. The users just take best response given the benefit provided by the company.

The *Nash equilibrium* (NE) is a widely-accepted and useful solution concept in strategic games, where no player has an incentive to deviate from it while others play according to their NE strategies. The NE g^* of the game G is formally defined as

$$g_i^* := \arg\min_{g_i} J_i(g_i, g_{-i}^*), \quad \forall i \in A,$$

where $g_{-i}^* = [g_1^*, \ldots, g_{i-1}^*, g_{i+1}^*, \ldots, g_N^*]$. The NE is at the same time the intersection point of players' best responses obtained by solving user problems individually.

The company acts here as the mechanism designer and has the goal of obtaining a desired level of location information granularity from the users. In this work, the designer has an unconventional objective compared to other works in mechanism design where the designer usually looks for social welfare or designer revenue maximization. The designer or company here wants to improve the precision of location information from each user, which is captured by a designer objective function that takes granularity of information of all the users as its argument. The designer objective we consider here is,

$$\max_b W = \max_b \sum_{i=1}^{N} w_i V(g_i(b_i)), \tag{4}$$

subject to a budget or resource constraint

$$\sum_{i=1}^{N} b_i \leq B$$

where w_i's are the weights given to individual users as desired by the designer, V is any concave function depending on the goal of the designer and B is the total budget. The weights depend on how much the company values the location information from different types of users.

It is important to note here that the designer (the mobile commerce company) tries to achieves its objective indirectly by providing benefits to users b as it naturally does not have control on their behavior, i.e. g. Essentially, the company tries to move the NE point vector of g of the resulting game to a desirable point by using the benefits provided to the users.

4. Privacy mechanism

In a privacy mechanism, each user decides on the location privacy level to be reported, i.e., g_i, depending on its risk level perception as a best response to the benefit set by the company by minimizing individual cost. The underlying game may converge to a Nash equilibrium, which may not be desirable to the service provider because the required level of location information not obtained. Therefore, the designer employs a pricing or subsidy mechanism to motivate the users by properly selecting the benefits delivered to each user by solving a global objective.

For a general concave utility function, the user optimization problem will be to find the action level which minimizes his individual cost given in Eq. (3), i.e.,

$$\min_{g_i} \; r_i g_i - b_i U_i(g_i).$$

Consequently, the general condition for player best response obtained from the first order derivative is

$$r_i - b_i dU_i(g_i)/dg_i = 0, \quad \forall i \in A. \tag{5}$$

The best response will be,

$$g_i = U_i'^{-1}(r_i/b_i), \quad \forall i \in A \tag{6}$$

where $U_i' = dU_i(g_i)/dg_i$.

The social objective is,

$$V = \max_b w_i V(U_i'^{-1}(r_i/b_i)),$$

such that

$$\sum_i b_i \leq B$$

and

$$r_i/U_i'(0) \leq b_i \leq r_i/U_i'(1). \tag{7}$$

The constraint in Eq. (7) comes from the fact that $0 \leq g_i \leq 1$. From Eq. (15) the Lagrangian is given by

$$L = \sum_i w_i V(U_i'^{-1}(r_i/b_i)) + \nu\left(\sum_i b_i - B\right) + \sum_i \lambda_i(b_i - r_i/U_i'(0)) + \sum_i \mu_i(r_i/U_i'(1) - b_i), \tag{8}$$

the resulting Karush–Kuhn–Tucker (KKT) conditions are

$$V_i'(U_i'^{-1}(r_i/b_i)) = \nu + \lambda_i - \mu_i, \quad \forall i \in A, \tag{9}$$

and

$$\nu\left(\sum_i b_i - B\right) = 0,$$
$$\lambda_i(b_i - r_i/U_i'(0)) = 0, \quad \forall i,$$
$$\mu_i(r_i/U_i'(1) - b_i) = 0, \quad \forall i,$$

where $V_i' = \frac{dV}{db_i}$.

Let

$$f_i = V_i'(U_i'^{-1}(r_i/b_i))^{-1} \tag{10}$$

and then Eq. (9) can be rewritten as,

$$b_i = f_i(\nu + \lambda_i - \mu_i), \quad \forall i \in A. \tag{11}$$

The above equation gives the benefits to be provided to the users by the designer to extract the optimum level of granularity level from the users.

4.1. Example

Consider as an example that the utility function of the users is taken as, $U_i(g_i) = \log(1 + g_i)$ and also the designer objective function is $W = \sum_{i=1}^{N} w_i \log(1 + g_i)$. Then the best response of the user i from the first order optimality condition of the convex optimization in Eq. (3) is

$$g_i = \begin{cases} 0, & \text{if } b_i \leq r_i \\ \dfrac{b_i}{r_i} - 1, & \text{if } r_i \leq b_i \leq 2r_i \\ 1, & \text{if } b_i \geq 2r_i. \end{cases} \tag{12}$$

We can observe that the user reports her location with a nonzero granularity of information only when the subsidy factor is greater than the risk factor. Also, the designer does not gain anything by giving the users a subsidy greater than twice their risk factor.

To solve the user problems and designer problem concurrently, we substitute the best response of all users given above in the designer objective in (4). Using these substitutions the designer objective can be written in terms of the vector b and the designer problem becomes

$$\max_b V = \max_b \sum_i w_i \log\left(\frac{b_i}{r_i}\right), \tag{13}$$

subject to

$$\sum_i b_i \leq B$$

and

$$r_i \leq b_i \leq 2r_i \quad \forall i. \tag{14}$$

The Lagrangian of this convex optimization problem is;

$$L = \sum_i w_i \log\left(\frac{b_i}{r_i}\right) + \nu\left(\sum_i b_i - B\right) + \sum_i \lambda_i(b_i - 2r_i) + \sum_i \mu_i(r_i - b_i), \tag{15}$$

where ν, λ_i, μ_i are the unique Lagrange multipliers.

The resulting Karush–Kuhn–Tucker (KKT) conditions will give,

$$\frac{w_i}{b_i} = \nu + \lambda_i - \mu_i, \quad \forall i \in A, \tag{16}$$

and

$$\nu\left(\sum_i b_i - B\right) = 0,$$
$$\lambda_i(b_i - 2r_i) = 0, \quad \forall i,$$
$$\mu_i(r_i - b_i) = 0, \quad \forall i.$$

Since the individual concave utility functions are concave and non-decreasing, the optimum point will be a boundary solution. Therefore,

$$\sum_i b_i = B$$

and using the KKT condition in (16),

$$\sum_i \frac{w_i}{\nu + \lambda_i - \mu_i} = B \quad \forall i \in A. \tag{17}$$

We obtain the optimum benefit for each user as,

$$b_i^* = \frac{w_i}{\nu^* + \lambda_i^* - \mu_i^*}, \quad \forall i \in A, \tag{18}$$

where ν^*, λ_i^*, μ_i^* are solutions to (17). Then, the optimal granularity level of each user will be,

$$g_i = \begin{cases} 0, & \text{if } b_i \le r_i \\ \dfrac{w_i}{(\nu^* + \lambda_i^* - \mu_i^*)r_i} - 1, & \text{if } r_i \le b_i \le 2r_i \\ 1, & \text{if } b_i \ge 2r_i. \end{cases} \tag{19}$$

If the solution is inner, i.e., constraints in (14) are satisfied with strict inequality and $\lambda_i = \mu_i = 0, \ \forall i$. We obtain

$$\nu = \frac{\sum_i w_i}{B}$$

and benefit for each user as

$$b_i = \frac{w_i B}{\sum_i w_i}.$$

Thus, the optimal granularity level of each user in the case of an inner solution is,

$$g_i = \frac{w_i B}{r_i \sum_i w_i} - 1 \quad \forall i.$$

When all the users are perceived equally by the designer, i.e. $w_i = w_j \ \forall i, j$, the benefits are equally divided among them. In such a symmetric case,

$$b_i = \frac{B}{N},$$

and

$$g_i = \begin{cases} 0, & \text{if } b_i \le r_i \\ \dfrac{B}{Nr_i} - 1, & \text{if } r_i \le b_i \le 2r_i \\ 1, & \text{if } b_i \ge 2r_i. \end{cases} \tag{20}$$

The designer can obtain desired granularity of information from each user by properly selecting the functions in the global objective and the weights in the function. Note that to formulate the objective and for imposing the constraints on the global problem, the designer needs to know the user r's. This she can obtain using a learning method which will be considered next.

4.2. Learning the risk factor

The designer can learn the risk factor from the best response of the users towards a sample subsidy factor vector b given by her to the users if the shape of the utility function is known. For the example in the previous section we can see that from the best response of the users given in (3), the risk factor of user i is obtained as,

$$r_i = \begin{cases} \dfrac{b_i}{2}, & \text{if } r_i \leq \dfrac{b_i}{2} \\ \dfrac{b_i}{1+g_i^*}, & \text{if } \dfrac{b_i}{2} \leq r_i \leq b_i \\ b_i, & \text{if } r_i \geq b_i \end{cases} \tag{21}$$

for any benefit b_i given by the designer and the best granularity level response g_i^* taken by her. If the value of the risk factor calculated from best response is given in the range,

$$\frac{b_i}{2} < r_i < b_i,$$

then it is the true value. If $r_i = \frac{b_i}{2}$, then the designer needs to reduce the benefit b_i given to the user i until $r_i > \frac{b_i}{2}$. Similarly, if $r_i = b_i$ then it needs to increase b_i until $r_i < b_i$.

If the shape of the benefit part of the cost function is a general concave function unknown to the designer, an iterative algorithm can be used to estimate the function in each step, which is given in the next section. Alternatively, the designer can employ an online regression learning algorithm [8] given in the Section 6.

5. Iterative distributed algorithm

When we have the utility or benefit obtained by the individual users for the granularity level provided by them to the company as a general concave utility function, the company cannot achieve its objective in a single shot. Instead, it needs to employ an iterative algorithm which modifies the granularity level of the users towards the direction of optimal point. For the algorithm the risk factor of the users are first assumed to be known to the designer. We relax this assumption later.

We propose a gradient update iterative distributed algorithm similar to the one in [9] to implement the pricing mechanism obtained above. This mechanism does a gradient update of the granularity level by the users and the benefits by the designer.

The iterative pricing mechanism M^a is defined as

$$b_i(k+1) = f_i(\nu(k) + \lambda_i(k) - \mu_i(k)), \quad \forall i \in A \tag{22}$$

$$g_i(k+1) = \left[g_i(k) - \kappa_i \frac{\partial J_i}{\partial g_i}(b_i(k+1)) \right]^+ \quad \forall i \in A, \tag{23}$$

$$\nu(k+1) = \left[\nu(k) + \kappa_{D1} \left(\sum_i b_i(k+1) - B \right) \right]_+, \tag{24}$$

$$\lambda_i(k+1) = \left[\lambda_i(k) + \kappa_{D2i} \left(b_i(k+1) - \frac{r_i}{U_i'(0)} \right) \right]_+, \tag{25}$$

$$\mu_i(k+1) = \left[\mu_i(k) + \kappa_{D3i} \left(\frac{r_i}{U_i'(1)} - b_i(k+1) \right) \right]_+, \tag{26}$$

where $f_i(.)$ is defined in Eq. (10) and $[x]^+$ is the projection mapping defined as,

$$[x]^+ = \arg\min_{z \in S} \|z - x\|_2$$

where S is the feasible set and $[x]_+ = \max(x, 0)$. The updates of the Lagrange multipliers and benefits by the designer happen in a smaller time scale allowing the g update by the users to converge first. This is also more realistic since the benefits update by the company happens slowly compared to the g update by the users.

Remark. For the updates in Eqs. (25) and (26) the designer needs to know the risk vectors and values of $U_i'(0)$ and $U_i'(1)$ of all the users. We assume that they are obtained as side information. Alternatively, if the total budget of the designer and the risk vectors of all the users are sufficiently large, the users can always obtain a feasible solution for Eq. (23). Therefore, the designer need not use the Eqs. (25) and (26) which ensures $0 \leq g_i \leq 1, \forall i$. The modified algorithm will have only updates according to Eqs. (22)–(24).

The algorithm which also shows the information flow for the iterative method is given below in Algorithm 1.

Algorithm 1: Iterative Pricing Mechanism M^a

Input: *Designer (Company)*: Maximum budget B and the designer objective W
Input: *Users*: Cost function J_i
Result: Optimum granularity levels g^* and benefits b^*
Initial granularity levels $g(0)$ and Lagrange multiplier $\nu(0)$;
repeat
  begin *Designer:*
    Observe user granularity levels g and Lagrange multiplier ν;
    Compute the benefits according to (22) ;
    Update ν's according to (24) .
  end
  Send each user i respective benefits $b_i^{(n)}$.
until *end of iteration*;
begin *Users:*
  foreach *User i* **do**
    Compute granularity level g_i from (23) ;
  end
end

5.1. Convergence analysis of iterative distributed algorithm

In this section we analyze the convergence of the iterative distributed algorithm given in previous section.

Theorem 1. *In the iterative pricing mechanism M^a given above defined by the set of Eqs. (22)–(26) converges to a unique point in the constraint set individually if $0 < \kappa_i < \frac{2}{M_1}, \forall i, 0 < \kappa_D < \frac{2}{M_2}, 0 < \kappa_{D2} < \frac{2}{M_3}$ and $0 < \kappa_{D3i} < \frac{2}{M_4 i}, \forall i$ where M_1 is the constant which bounds $\|D(\delta J_i(g))\|, \forall x \in S$, M_2 is the constant which bounds $\|D(\delta L(\nu))\|, \forall \nu \in R_n^+$, M_{3i} is the constant which bounds $\|D(\delta L(\lambda_i))\|, \forall \lambda_i \in R_n^+$, M_{4i} is the constant which bounds $\|D(\delta L(\mu_i))\|, \forall \mu_i \in R_n^+$, D is the Jacobian matrix and $\|.\|$ refers to the L_2 norm. The algorithm converges to a unique point with Lagrange multiplier update happening in a slower time scale than the granularity level update.*

Proof. In [10], for analyzing constraint optimization problems the infeasible points are projected back to the feasible region. The projection mapping is defined as,

$$[g]^+ = \arg\min_{z \in S} \|z - g\|_2$$

where S is the feasible set.

For the convergence of the gradient projection algorithm the relaxations of Assumptions 3.1 given in [10, p. 213] are to be satisfied as sufficient conditions. The relaxed Assumption 3.1 says that $F(g) > c, \forall x \in S$ for a $c \in R$ for any F to be minimized. Both user cost function and the global objective satisfy this. The second assumption is the Lipschitz continuity condition given by,

$$\|\delta J_i(g) - \delta J_i(h)\| \leq K\|g - h\|, \quad \forall g,\ h \in S.$$

The user cost functions are twice continuously differentiable due to the presence of a noise term in the denominator of the interference term. Therefore, we can use the mean value theorem for vector valued functions which states that,

$$\delta J_i(g) - \delta J_i(h) = \left(\int_0^1 D(\delta J_i(y + t\rho)dt) \right) \cdot (x - y), \quad \forall g,\ h \in S,\ \forall i$$

where $\rho = g - h \in X$, $0 \leq t \leq 1$ and D is the $N \times N$ Jacobian matrix. The Jacobian matrix D is defined as,

$$D(\delta J_i(g)) := \begin{pmatrix} c_1 & c_{12} & \cdots & c_{1N} \\ c_{21} & c_2 & \cdots & c_{2N} \\ \vdots & & \ddots & \vdots \\ c_{N1} & c_{N2} & \cdots & c_N \end{pmatrix} \tag{27}$$

where $c_m := \frac{\partial^2 J_i}{\partial g_m^2}$ and $c_{lk} := \frac{\partial^2 J_i}{\partial g_l \partial x_m}$.

Using the Cauchy–Schwarz inequality,

$$\|\delta J_i(g) - \delta J_i(h)\| \leq M_1 \|g - h\|, \quad \forall x, y \in S, \ \forall i, \tag{28}$$

where M_1 is the constant which bounds $\|D(\delta J_i(g))\|, \forall g \in S$. The set S is convex and $(h + t\rho) \in S$ for t between 0 and 1. For $g \in S$, M_1 is bounded when the boundaries of S are finite. Therefore, the power update according to Eq. (23) converges if $0 < \kappa_i < \frac{2}{M_1}$, $\forall i$ for given λ and thus prices.

In the algorithm, we do the distributed implementation by the alignment of users and designer problems through the benefits. When the designer updates the benefits according to (23),

$$\frac{dJ_i}{dg_i} = -\frac{dW}{dg_i}.$$

Since both the gradients are equal, the gradient update in (23) by the users is according to the gradient update of the global objective.

The Lagrange function of the global objective is given Eq. (8) subject to the condition that $\nu, \lambda_i, \mu_i \geq 0, \ \forall i$. The gradient descent equation for L is given by

$$\nu(k+1) = \left[\nu(k) + \kappa_{D1}\left(\sum_i b_i(k+1) - B\right)\right]_+, \tag{29}$$

$$\lambda_i(k+1) = \left[\lambda_i(k) + \kappa_{D2i}\left(b_i(k+1) - \frac{r_i}{U_i'(0)}\right)\right]_+, \tag{30}$$

$$\mu_i(k+1) = \left[\mu_i(k) + \kappa_{D3i}\left(\frac{r_i}{U_i'(1)} - b_i(k+1)\right)\right]_+. \tag{31}$$

The Eq. (29) is equivalent to Eq. (26).

Also, we need to prove the Lipschitz continuity of the Lagrange function of global objective w.r.t. the λ vector. From the mean value theorem,

$$\delta L(\nu^{(1)}) - \delta L(\nu^{(2)}) = \left(\int_0^1 D(\delta L(\nu^{(2)} + t\pi)dt)\right) \cdot (\nu^{(1)} - \nu^{(2)}), \quad \forall \nu^{(1)}, \nu^{(2)} \in R_+^n$$

and

$$\|\delta L(\nu^{(1)}) - \delta L(\nu^{(2)})\| \leq M_2 \|\nu^{(1)} - \nu^{(2)}\|, \quad \forall \nu^{(1)}, \nu^{(2)} \in R_+^n.$$

Therefore, the Lagrange multiplier ν update according to Eq. (26) converges if $0 < \kappa_{D1} < \frac{2}{M_2}$, for given granularity vector. Similarly, we can define vectors M_3 and M_4 such that $0 < \kappa_{D_{2i}} < \frac{2}{M_{3i}}$ and $0 < \kappa_{D3i} < \frac{2}{M_{4i}}$, $\forall i$. Gradient descent equations under the above assumptions converges according to Proposition 3.4. in [10, p. 214].

Since user cost function and Lagrange function of the global objective are convex, the equations converges to a unique point in the constraint set according to Proposition 3.5 in [10].

The g update happens in a faster timescale and it converges for any given value of the Lagrange multipliers. Lagrange multiplier update happens in the direction of global optimum once in several time steps of the granularity level update. Therefore, the algorithm converges to a unique point with Lagrange multiplier update happening in a slower time scale than the granularity level update, hence proved. □

6. Regression learning of the user utility

We have assumed for the iterative algorithm that the user's risk vector and the boundary points of the marginal utility functions are known to the company. When we consider the case where the user's risk vector, marginal utility functions and the boundary points of the marginal utility functions are known to the company, then the company has to learn these values and bring the system to the optimal point. In this section, Gaussian Process (GP) regression learning techniques are used by the designer for implementation of privacy mechanism given in previous sections.

A Gaussian Process is formally defined as a collection of random variables, any finite number of which have a joint Gaussian distribution. It is completely specified by its mean function $m(x)$ and covariance function $C(x, \tilde{x})$, where

$$m(x) = E[\hat{f}(x)]$$

and

$$C(x, \tilde{x}) = E[(\hat{f}(x) - m(x))(\hat{f}(\tilde{x}) - m(\tilde{x}))], \quad \forall x, \ \tilde{x} \in D.$$

Let us for simplicity choose $m(x) = 0$. Then, the GP is characterized entirely by its covariance function $C(x, \tilde{x})$. Since the noise in observation vector y is also Gaussian, the covariance function can be defined as the sum of a *kernel function* $G(x, \tilde{x})$

and the diagonal noise variance

$$C(x, \tilde{x}) = G(x, \tilde{x}) + \sigma I, \quad \forall x, \tilde{x} \in D, \tag{32}$$

where I is the identity matrix. While it is possible to choose here any (positive definite) kernel $G(\cdot, \cdot)$, one classical choice is

$$G(x, \tilde{x}) = \exp\left[-\frac{1}{2}\left\|x - \tilde{x}\right\|^2\right]. \tag{33}$$

Note that GP makes use of the well-known *kernel trick* here by representing an infinite dimensional continuous function using a (finite) set of continuous basis functions and associated vector of real parameters in accordance with the *representer theorem* [11].

The training set (D, y) is used to define the corresponding GP, $GP(0, C(D))$, through the $M \times M$ covariance function $C(D) = G + \sigma I$, where the conditional Gaussian distribution of any point outside the training set, $\bar{y} \in X, \bar{y} \notin D$, given the training data (D, t) can be computed as follows. Define the vector

$$k(\bar{x}) = [G(x_1, \bar{x}), \ldots, G(x_M, \bar{x})] \tag{34}$$

and scalar

$$\kappa = G(\bar{x}, \bar{x}) + \sigma. \tag{35}$$

Then, the conditional distribution $p(\bar{y} \mid y)$ that characterizes the $GP(0, C)$ is a Gaussian $N(\hat{f}, v)$ with mean $\hat{f}$ and variance v,

$$\hat{f}(\bar{x}) = k^T C^{-1} y \quad \text{and} \quad v(\bar{x}) = \kappa - k^T C^{-1} k. \tag{36}$$

This is a key result that defines GP regression. The mean function $\hat{f}(x)$ of the GP provides a prediction of the objective function $f(x)$. Furthermore, the variance function $v(x)$ can be used to measure the uncertainty level of the predictions with the mean value $\hat{f}$.

Here the designer learns the marginal utility functions U_i' of each user using their best response bids or actions as data points.

The users are not considered to be price anticipating here because we consider a distributed scenario in which there is an information asymmetry between the users and the company. The users do not know the action and utility function of other users or the nature of the benefit function. Hence, they cannot anticipate the exact impact of their action on the benefit function and they just adopt a best response strategy by taking the price as a constant given by the designer. The benefits are designed by the company to bring the Nash Equilibrium of the resulting game to an efficient point.

Since the company would like to bring the granularity level towards an optimal level by giving as much as possible benefits to the users, the optimum point will ensure a boundary solution with respect to the budget. By comparing (9) and (5), we conclude that for aligning designer and user objectives, the designer needs to set benefit according to Eq. (11) for every user to solve designer and user problems. Therefore, from the criterion of full resource usage, it follows that

$$\sum_i b_i^* = \sum_i f_i(\nu^* + \lambda_i^* - \mu_i^*) = B \tag{37}$$

where b^* and ν^*, λ^*, μ^* are the optimal points.

Each user i sends a response to the sample benefits $\{b_{i1}, \ldots, b_{iM}\}$ set by the company which contains the granularity action vector $\{g_{i1}, \ldots, g_{iM}\}$. From the best response given by Eq. (5)

$$b_{im} = \frac{U_i'(g_{im})}{r_i}, \quad \forall i \in A \text{ and } m = 1, \ldots, M. \tag{38}$$

The corresponding value of the ratio of scalar marginal utility values and the risk factor at the points of best response is available. Assume that the observations are distorted by a zero-mean Gaussian noise, n with variance $\sigma \sim N(0, \sigma)$. Now let the Gaussian vector obtained in the case of user i is $\{y_{i1}, \ldots, y_{iM}\}$, where

$$y_{im} = \frac{U_i'(g_{im})}{r_i} + n_i \quad \forall i.$$

A Gaussian regression technique as described above is used to estimate the function which is the ratio of marginal utility functions and the risk factors $\frac{\tilde{U_i'}}{r_i}$. After that, the estimated values of $\frac{U_i'(0)}{r_i}$ and $\frac{U_i'(1)}{r_i}$ are obtained from the estimated function. These values are used to satisfy the constraint on b_i given in Eq. (7) while setting benefits for the online algorithm given below.

Now the ν, λ, μ values are updated according to the Eqs. (24)–(26), starting from an initial point until $\sum_i b_i = B$. From these converging values of ν, λ, μ and using Eq. (11) we have

$$f_i^{-1}(b_i) = \nu + \lambda_i - \mu_i, \quad \forall i \in A. \tag{39}$$

This value of b can be added to the initial data points to refine the estimate of the function $\frac{U_i'}{r_i}$. For different initial values the updates will converge to different b vector and corresponding f_i^{-1}'s. Therefore, the function f_i^{-1}, $\forall i$ can be obtained using regression technique. Once these curves are obtained, a b vector is searched for which

$$f_i^{-1}(b_i^*) = f_j^{-1}(b_j^*), \quad \forall i, j$$

and $\sum_i b_i^* = B$.

The algorithm which also shows the information flow for the regression learning method is given below in Algorithm 2.

Algorithm 2: Regression Learning in Privacy Mechanisms

Input: *Designer or Company*: Global objective G and the budget B.
Input: *Users)*: Cost functions J_i
Result: Optimal benefit vector and optimal granularity vector g^*

Initialization: The designer obtains initial data points by selecting values for the benefits b and makes an initial estimate of $\frac{U_i'}{r_i}$ for each user i using GP by setting the benefits accordingly and observing user responses;
repeat
  begin *Designer:*
    Find the estimated values of $\frac{U_i'(0)}{r_i}$ and $\frac{U_i'(1)}{r_i}$. Starting from random initial points ν, ł, μ values are updated according to the Eqs. (24)–(26). Continue until $\sum_i b_i = B$ and denote the corresponding ν_k, ł$_k$, μ_k as ν_{new}, ł$_{new}$, μ_{new};
    Find from 39, find $f_i^{-1}(b_i)$ from ν_{new}, ł$_{new}$, μ_{new} ;
    Set value of b as the benefit vector to users. **begin** *Players:*
      foreach *Player i* **do**
        Take action g_{inew} as response to the benefits b_i;
      end
    end
    Observe the player actions g_{inew} $\forall i, m$;
    Add the values of g_{new} to the initial data set points;
    Update the estimates of estimates $\frac{U_i'(1)}{r_i}$ and variances v_i for all the users based on the updated data set using GP;
  end
until *Enough Data Points*;
begin *Designer:*
  Estimate the function f_i^{-1}, $\forall i$ using regression technique from the data points. Search b vector such that

$$f_i^{-1}(b_i^*) = f_j^{-1}(b_j^*), \forall i, j$$

  and $\sum_i b_i^* = B$.
end

Note that by using the online learning algorithm as above, when the user preferences or parameters in utility function change in the course of time, the designer can estimate the new functions and can move the system to optimal point. The numerical results which illustrate the learned functions and convergence of the algorithm are given in Section 7. We can see that by using this online learning algorithm, the designer can adapt the estimation if the utility functions or utility parameters of the players change in the course of time.

7. Numerical analysis

7.1. Numerical example

The privacy mechanism given in Section 4 is illustrated with a numerical example in this section. We considered 5 users having logarithmic utilities and their risk factors are randomly generated between 0 and 2. The risk vector in an instance is taken as

$$r = [0.18\ 0.45\ 0.89\ 0.98\ 1.1693].$$

The weights given to the users in the global objective is taken as

$$w = [1.78\ 0.945\ 0.99\ 1.098\ 0.869]$$

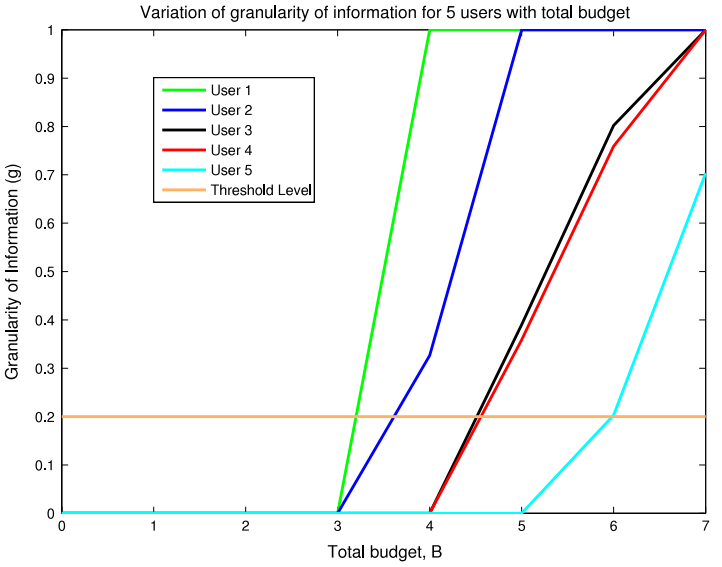


Fig. 1. Granularity of information of 5 users with the total budget.

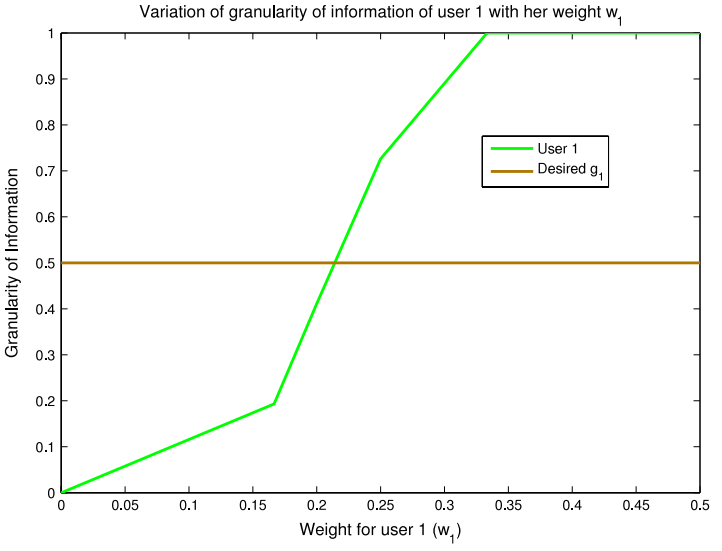


Fig. 2. Variation of granularity of information of user 1 with the weight in the global objective.

and it is assumed that the company has no control over these weights to manipulate them. The company (designer) learns the value of the risk factor of users by giving a sample value of subsidies to different users and observing their best response as explained in Section 4.2. We first plotted the variation of the best response granularity level of the users with the total budget of the company in Fig. 1.

We can observe in Fig. 1 that there is a critical budget below which the company cannot extract any location information from the users. We could also observe from Fig. 1 that the company can extract more and more granularity of information by increasing the total budget, as expected. The threshold level of granularity for all the users which is the minimum level required to provide the service is taken to be 0.2. The level of budget required for extracting more than this threshold level of granularity from all the users, can be obtained from Fig. 1. For the instance considered in the plot, the critical level of budget is given as 6.

Next, we consider the case where the company can adjust the weight given to different users in the global objective. In Fig. 2, the setting remains as in the Fig. 1 except that the company varies the weight of the first user. From this plot, the weight required to get the desired level of granularity of information can be obtained. For user 1 the desired level of granularity of information is obtained with $w_1 = 0.21$.

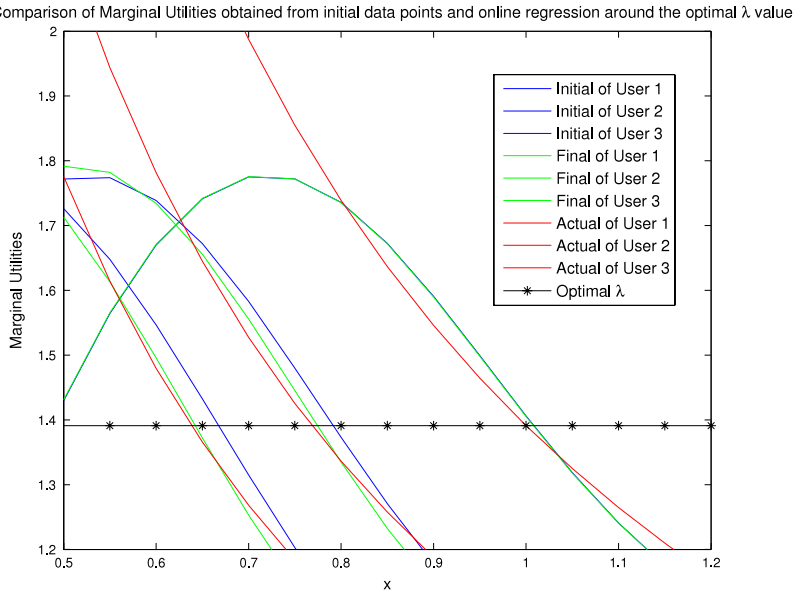


Fig. 3. Ratio of marginal utility curve and risk factor in the case of logarithmic utilities constructed using initial data points and the online algorithm given in Algorithm 2.

Finally, the regression learning of the user utilities presented in Section 6 is numerically demonstrated. We consider a system with 3 users having logarithmic utility functions and risk vector

$$r = [0.18\ 0.45\ 0.89]$$

for visualizing the results. In Fig. 3, the actual ratio of marginal utility curve and risk factor and the ratio from the marginal utility curves constructed using 15 initial data points are plotted. Then ratios of marginal utility curve and risk factor are obtained from the marginal utility curves constructed with the online algorithm given in Algorithm 2. We compared these curves with each other in Fig. 3. We can observe that near the optimal value the estimation of the function is better with the online algorithm than with only initial data points, as expected.

7.2. Simulation results

We construct the location of large number of users and the crowd around them from their reported granularity level using real dataset here. We use the GPS trajectory dataset [12–14] which was collected in (Microsoft Research Asia) Geolife project by 167 users in a period of over three years from April 2007 to December 2010. These data sets give context information to the systems and help to develop innovative mobile and web application. They also help to infer the user transportation modes and mobility patterns. But the users need to be incentivised to share their location for obtaining these data sets. The data set which gives the latitude and longitude of 160 users at different times from 2007 to 2010 is imported for a particular time. Using this latitude and longitude information, the exact of the users are plotted in the Fig. 4. We obtained the best response granularity level of the users from the privacy mechanism in Section 4 for the case of logarithmic utility function for a particular risk vector and budget. These best response granularity levels are mapped back to the size of the crowd $(n_i(t))$ from the Eqs. (1) and (2) given in Section 2 and reported locations are constructed from them. The location anonymity of the users due to the granularity level they reported in equilibrium are represented as the circles around the actual locations using the data set in the Fig. 4. The blue circle around a user contains the crowd of users around that particular user. We can observe that users have a different size of crowd around them depending on the risk factor they have. From the plot we can understand that if we consider the users do not share their actual location but act according to the privacy mechanism, we get a map of users with the blue circles instead of the read dots. The company will have to modify the location based application taking this into consideration.

Next we plot the anonymity levels chosen by the users in the equilibrium. Depending on the values of n_i, each user i will have a number of users around her and the anonymity levels according to that. The anonymity levels of the 100 users are plotted as a bar graph in the Fig. 5.

Remark. The plots and results in Section 7.1 can be extended like in this section with the real data set.

8. Literature review

A wireless location privacy protecting system is analyzed and an information theoretic approach to define anonymity is proposed in [15]. In [16], the interaction between the local adversary deploying eavesdropping stations to track mobile users

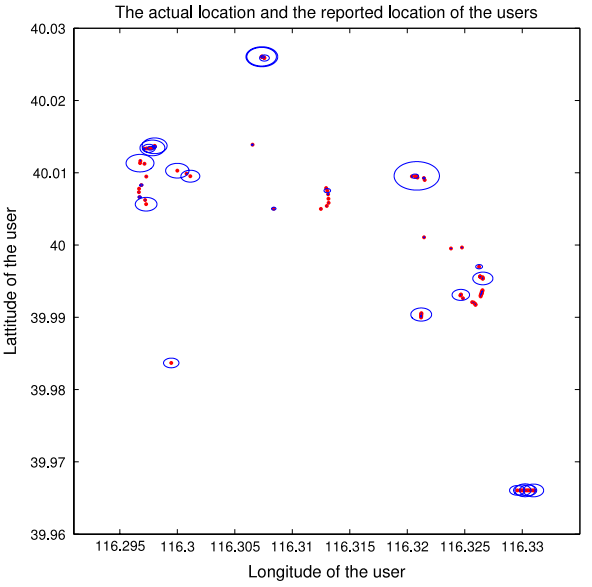


Fig. 4. Location of users: actual and reported.

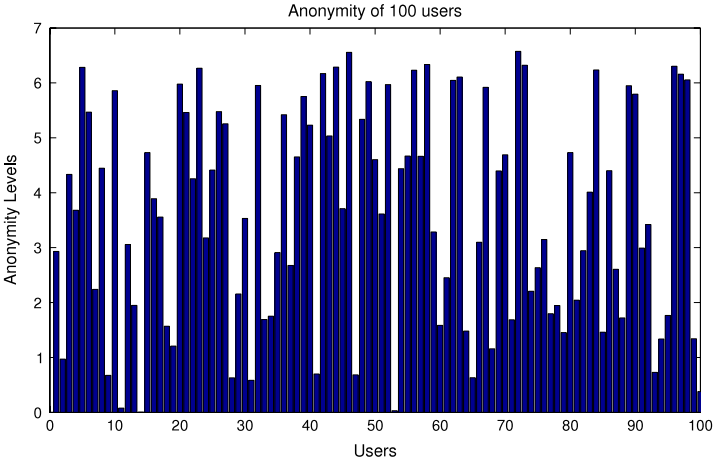


Fig. 5. Anonymity levels of users.

and mobile users deploying mix zones to protect their location privacy is studied using a game-theoretic model. MobiAd, a system for personalized, localized and targeted advertising on smart phones is proposed in [17]. Utilizing the rich set of information available on the phone, MobiAd presents the user with local advertisements in a privacy-preserving way by routing the information through a delay tolerant network. In this work they suggest the service provider to give discounts to motivate users to use the MobiAd system. In [18] a proposal is made to provide users with rewards such as free "minutes" to motivate them to accept advertisements.

In [19], a game theoretic model of privacy in a community-based social networking mobile applications is proposed, in which the users take decisions on the level of granularity with which they share their location information to others. In that model, there is no service provider and the individual members of the community use their collective knowledge for personal or social goals. A Pareto improvement of the Nash equilibrium is also achieved by making the users contribute more information to the collective knowledge, using a tit-for-tat mechanism.

In [20], the authors reduce mechanism design problems to standard algorithmic problems using techniques from sample complexity. They considered a prior-free setting for revenue maximization. The approach in [21] considers a learning phase followed by an accepting phase, and is careful to handle incentive issues for agents in both the phases. They study a limited-supply online auction problem, and construct value- and time-strategyproof auctions. The scenario when the users are strategic and they may manipulate the labeling for their individual benefit is considered in [22]. In [23], Gaussian regression learning techniques are used in the general context of mechanism design. In this paper, we use Gaussian regression learning method [8] to learn the utilities by the designer by observing the actions of the users in the privacy mechanism.

9. Conclusion

This paper models and analyzes the interaction of a mobile commerce company with its users who obtain location based services, as a strategic game. A privacy mechanism is designed where the company motivates users to report their location information at a granularity level desired by the company. In return, monetary benefits are obtained by a user depending on the granularity level taken by them and on the weight the designer gives for them in the global objective. The users report their location with nonzero granularity level of information when the subsidy by the company exceeds their perceived risk factor. The total budget required to obtain the desired minimum level of granularity of location information from all the users was obtained. As expected, the granularity of location information selected by the users decreases with increasing risk factor. Iterative distributed algorithms and regression learning methods are used to learn different unknowns by the designer and to take the mechanism to optimal point of equilibrium. We used real GPS data on location information to obtain the simulation results. A map of users is constructed from their reported granularity level of information and the actual GPS data.

Acknowledgments

This work has been supported by Deutsche Telekom Laboratories, Berlin, Germany. An earlier version of this work has appeared in the proceedings of the D-SPAN 2011 workshop, in conjunction with IEEE WoWMoM 2011 June 20, 2011, Lucca, Italy.

References

[1] V. Krishna, Auction Theory, first ed., Academic Press, 2002, Amazon.
[2] R. Srikant, The Mathematics of Internet Congestion Control, in: Systems & Control: Foundations & Applications, Birkhäuser, Boston, MA, 2004.
[3] J.W. Bagby, Heng Xu, T.R. Melonas, Regulating privacy in wireless advertising messaging: FIPP compliance by policy vs. by design, in: The 9th Privacy Enhancing Technologies Symposium, PETS 2009, pp. 19–36.
[4] Governments 'not ready' for new European privacy law, 2011.
[5] T. Başar, G.J. Olsder, Dynamic Noncooperative Game Theory, second ed., SIAM, Philadelphia, PA, 1999.
[6] A. Serjantov, G. Danezis, Towards an information theoretic metric for anonymity, in: Proceedings of the 2nd International Conference on Privacy Enhancing Technologies, PET'02, Springer-Verlag, Berlin, Heidelberg, 2003, pp. 41–53.
[7] T. Alpcan, L. Pavel, Nash equilibrium design and optimization, in: Proc. of Intl. Conf. on Game Theory for Networks, GameNets 2009, Istanbul, Turkey.
[8] C.E. Rasmussen, C.K.I. Williams, Gaussian Processes for Machine Learning, in: Adaptive Computation and Machine Learning, The MIT Press, 2005.
[9] M. Chiang, Balancing transport and physical layers in wireless multihop networks: jointly optimal congestion control and power control, IEEE Journal on Selected Areas in Communications 23 (2005) 104–116.
[10] D.P. Bertsekas, J. Tsitsiklis, Parallel and Distributed Computation: Numerical Methods, first ed., Athena Scientific, 1997.
[11] B. Scholkopf, A.J. Smola, Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond, MIT Press, Cambridge, MA, USA, 2001.
[12] Y. Zheng, L. Zhang, X. Xie, W.-Y. Ma, Mining interesting locations and travel sequences from GPS trajectories, in: Proceedings of International Conference on World Wild Web, WWW 2009, Madrid, Spain, pp. 791–800.
[13] Y. Zheng, Q. Li, Y. Chen, X. Xie, W.-Y. Ma, Understanding mobility based on GPS data, in: Proceedings of ACM Conference on Ubiquitous Computing, UbiComp 2008, Seoul, Korea, pp. 312–321.
[14] Y. Zheng, X. Xie, W.-Y. Ma, Geolife: a collaborative social networking service among user, location and trajectory, IEEE Data Engineering Bulletin (2010) 32–40.
[15] L. Huang, H. Yamane, K. Matsuura, K. Sezaki, Towards modeling wireless location privacy, in: Proceedings of Privacy Enhancing Technology, PET, pp. 59–77.
[16] M. Humbert, M.H. Manshaei, J. Freudiger, J.-P. Hubaux, Tracking games in mobile networks, in: GameSec'10, pp. 38–57.
[17] P. Hui, T. Henderson, I. Brown, H. Haddadi, Targeted advertising on the handset: privacy and security challenges, in: Pervasive Advertising, in: Springer Human–Computer Interaction Series, 2011.
[18] M. Himmel, H. Rodriguez, N. Smith, C. Spinac, Method and system for schedule based advertising on a mobile phone, 2005.
[19] H. Liu, B. Krishnamachari, M. Annavaram, Game theoretic approach to location sharing with privacy in a community-based mobile safety application, in: Proceedings of the 11th International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM'08, ACM, New York, NY, USA, 2008, pp. 229–238.
[20] M.-F. Balcan, A. Blum, J.D. Hartline, Y. Mansour, Reducing mechanism design to algorithm design via machine learning, Journal of Computer and System Sciences 74 (2008) 1245–1270.
[21] M.T. Hajiaghayi, R. Kleinberg, D.C. Parkes, Adaptive limited-supply online auctions, in: Proceedings of the 5th ACM Conference on Electronic Commerce, ACM Press, 2004, pp. 71–80.
[22] O. Dekel, F. Fischer, A.D. Procaccia, Incentive compatible regression learning, in: Proceedings of the Nineteenth Annual ACM–SIAM Symposium on Discrete Algorithms, SODA'08, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2008, pp. 884–893.
[23] A.K. Chorppath, T. Alpcan, Learning user preferences in mechanism design, in: Proc. of 50th IEEE Conference on Decision and Control and European Control Conference, Orlando, Florida.