A Privacy-aware Framework for Online Advertisement Targeting

Linlin Yang[†], Wei Wang[‡], Yanjiao Chen[‡], Qian Zhang[‡]
[†]Fok Ying Tung Graduate School, [‡]Department of Computer Science and Engineering
Hong Kong University of Science and Technology, Hong Kong
Email: {lyangah, gswwang, chenyanjiao, qianzh}@ust.hk

***Abstract*—With the prosperity of the Internet, many advertisers choose to deliver their advertisements by online targeting, where the ad broker is responsible for matching advertisements with users who are likely to be interested in the underlying products or services. However, this online advertisement targeting system requires user profile information and may fail due to privacy issues. In light of growing privacy concerns, we propose a privacy-aware framework for online advertisement targeting, where users are compensated for their privacy leakage and motivated to click more advertisements. In the framework, an ad broker pays a varying amount of money to users for clicking different advertisements due to distinct privacy leakage. Meanwhile advertisers send advertisements to the ad broker and determine the price per user click they need to pay. We model the interactions among advertisers, the ad broker and users as a three-stage game, where every player aims at maximizing its own utility, and Nash Equilibrium is achieved by backward induction. We further analyze the optimal strategies for advertisers, the ad broker and users. Numerical results have shown that the proposed privacy-aware framework is effective as it enables all advertisers, the ad broker and users to maximize their utilities in case of different levels of user privacy sensitivities. In addition, the proposed framework produces higher profits for advertisers and the ad broker than the traditional "paid to click" system.**

I. Introduction

As the Internet is an efficient way for advertisements to reach users, nowadays many advertisers are choosing to deliver their advertisements by online targeting. In most existing online advertisement targeting systems, the ad broker makes use of users' online behavior to match advertisements with users who are likely to be interested in the underlying products or services [1]. For example, Google Adwords, which is a huge success, leverages users' search items to show advertisements.

However, these online targeting systems raise severe privacy concerns. Firstly, to obtain user profile information, the ad broker usually tracks users' online behavior, where user private information is leaked. For example, frequent visits to luxury goods websites indicate the user may be wealthy, while searching for a certain kind of medicine implies the user has a related disease. Hence, private information like financial and physical status is leaked, which exponentially increase the risks like being identified and behavior being predicted. What is more, the ad broker rarely guarantees that its private information is kept safe and not shared with a third party. In 2009, private documents were exposed due to a bug in Google Docs [2]. If malicious entities obtain these information, user safety is threatened. Thus, with growing consciousness about privacy, many users think the risks of having their profile information revealed outweigh the benefits of targeted advertising, so they no longer have the incentive to participate in an advertisement targeting system. Therefore, considering the privacy issue, it is essential to design a mechanism that encourages users to participate and click advertisements.

There are mainly two existing works [3] [4] trying to encourage users to involve themselves in an advertisement targeting system by designing mechanisms that can preserve users' privacy. However, the mechanism in [3] can not fully protect users' privacy and the mechanism in [4] protects users' privacy at a loss in advertisers' satisfaction. In their frameworks, advertisements are targeted without private profile information leaving users' own devices. As reports about which advertisements are clicked reveal users' interests, in order not to compromise users' privacy, a new entity dealer needs to be introduced in [3] to count the number of clicks by proxying all communication between users and the ad broker in an anonymous way. In this system, users' privacy can only be preserved on the condition that the dealer does not collaborate with the the ad broker, for which, however, there is no guarantee. And users are not aware whether there is collusion between the dealer and the ad broker. In [4], users send falsified click information to an ad broker according to predetermined rules. An algorithm to estimate the actual number of clicks is proposed for the ad broker. Though the system preserves users' privacy, advertisers may be dissatisfied as the numbers of clicks is inaccurate, which determine how much they will pay.

The aforementioned shortcomings of the existing mechanisms motivate us to solve the privacy issues by economic incentives. In our privacy-aware framework, we try to preserve users' privacy to a large extent and compensate them for the privacy leaked in their reports about which advertisements are clicked. As users can get paid from clicking, they are stimulated to click more advertisements. In this way, advertisers get an accurate number of clicks for their advertisements; and users, aware of privacy leakage, are compensated and motivated to click advertisements. The system structure is shown in Fig.1 and it works as follows.

- Advertisers send advertisements to the ad broker and determine the price of every click for their advertisements according to the revenue they can gain from each click.
- Without user profile information, the ad broker receives

978-1-4799-1353-4/13/$31.00 ©2013 IEEE

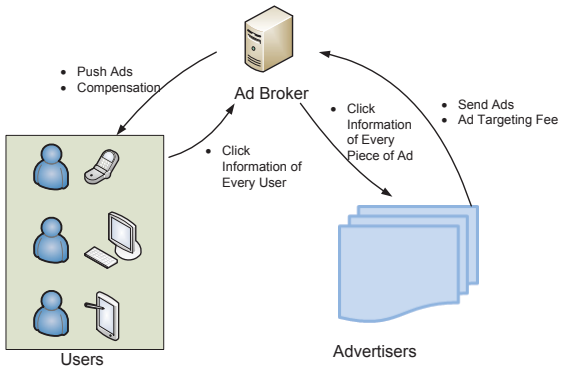


Fig. 1. Structure of privacy-aware advertisement targeting system

advertisements from advertisers and forwards them directly to users without matching. Accurate reports about which advertisements are clicked are sent by users and the ad broker counts the total number of clicks for every advertisement according to these reports. To compensate for privacy leakage and motivate ad clicking, the ad broker pays a varying amount of money to all users for clicking different advertisements due to distinct privacy leakage.

- Users keep their profile information on their own devices. After receiving advertisements from the ad broker, the devices determine the set of advertisements their owners may be interested in and display them when possible. Users make the decision about whether to click advertisements balancing the amount of money they receive and the privacy they leak.

Since all advertisers, the ad broker and users are rational and selfish players, the framework can be formulated as a three-stage game, where every player targets at maximizing their own utilities. Firstly, knowing how the ad broker and users will react, advertisers can determine the optimal price of every click for their advertisements. Then, observing advertisers' prices, the ad broker can determine the optimal amount of money paid to users for every advertisement, based on the knowledge of users' behavior. Finally, the users determine whether to click certain advertisements, according to the price given by the ad broker. We use backward induction to derive the Nash Equilibrium and analyze the optimal strategies of advertisers, the ad broker and users. Numerical results, considering Gaussian-distributed users' privacy sensitivities, have shown that all advertisers, the ad broker and users can optimize their utilities and this framework outperforms modified traditional "paid to click" system concerning the profits of advertisers and the ad broker as more users are stimulated to click advertisements.

The main contributions of this paper are as follows. 1) A novel privacy-aware framework for online advertisement targeting is proposed. Aware of the privacy leakage, users are compensated so that they are motivated to click more advertisements, which in turn increases the revenues of advertisers and the ad broker. 2) We model the framework as a three-stage game and theoretically analyze the Nash Equilibrium as well as the optimal strategies of advertisers, the ad broker and users. 3) Numerical results show that advertisers can make a constant profit when only the mean of users' privacy sensitivity levels change and the ad broker can actually gain higher profit when only the standard deviation of users' privacy sensitivity levels rise. Compared with modified traditional "paid to click" system, our framework produces higher profits for advertisers and the ad broker as more users are encouraged to click advertisements.

The rest of the paper is organized as follows. In Section II, we describe the system model, introducing the concept of privacy sensitivity and analyzing the utilities of advertisers, the ad broker and users. In Section III, we model the framework as a three-stage game and theoretically analyze the optimal strategies of advertisers, the ad broker and users. Simulation results are shown in Section IV and related works are reviewed in Section V. We summarize the paper in Section VI.

II. SYSTEM MODEL

In this section, we first describe the framework of our advertisement targeting system. Then, the concept of privacy sensitivity is introduced. Finally, we define the utility functions of advertisers, the ad broker and users.

A. Framework

The advertisement targeting system consists of multiple advertisers, one ad broker and multiple users, as shown in Fig.1. Every advertiser has one piece of advertisement. So we use the term advertiser and advertisement interchangeably. We assume that there are a total of K advertisers and N users. Let $\{A_j : j = 1, ..., K\}$ represent the set of advertisements and $\{S_i : i = 1, ..., N\}$ represent the set of users. All advertisers, ad broker and users, who want to maximize their own utilities, are rational and selfish.

The ad broker runs an advertising platform, collecting advertisements from different advertisers and delivering them to users. Meanwhile, the ad broker counts the number of clicks on every advertisement and charges the advertisers for each click. As users' advertisement click information, considered private information, is revealed to the ad broker, the ad broker pays users a certain amount of money to compensate for the privacy leakage and motivate them to click more advertisements. Users make the decision of whether to click advertisements according to their privacy sensitivities and the money they can get for clicking.

B. Privacy Sensitivity

Researchers have proposed several definitions of privacy sensitivity [5]–[7]. In view of their definitions, in our model, we define privacy sensitivity as the amount of compensation money needed for every unit of privacy leakage in a click. Privacy leakage is a relatively subjective concept. Clicking different kinds of advertisements leads to different levels of privacy leakage. For example, clicking a medical advertisement may indicate that you have certain kind of disease, which brings about a high level of privacy leakage. Whereas

clicking an umbrella advertisement only means you need an umbrella, leading to a low level of privacy leakage. Thus according to the nature of an advertisement A_j, we assume a privacy factor α_j for it. Meanwhile, privacy leakage for clicking an advertisement is also negatively related to the total number of clicks on the advertisement, which means the more users that click the the same advertisement, the lower the privacy leakage for every user who clicks it. For example, during a certain period, when influenza is highly prevalent, many people may click medicine advertisements related to influenza, therefore having influenza is not considered to be highly private. However, when there are few people affected by influenza and the number of clicks on related medicine advertisements is small, having influenza is of relatively high privacy so that the privacy leakage related these advertisements is considered higher. Thus, we define privacy leakage of advertisement A_j as α_j/n_j, where n_j is the total number of users who click advertisement A_j.

Studies have shown that different people have different privacy sensitivities [5]–[7]. Factors like gender, education and age affect privacy sensitivity [8]. Accordingly, let $\{\omega_i : i = 1, ..., N\}$ represent privacy sensitivities of different users.

C. Utility Functions

Advertisers gain revenue from clicks. After users view advertisements, they may become interested in the underlying products or services so that they will buy them. We assume that for every click, advertiser A_j gains an average revenue of Q_j. The expense of advertisers is the money they pay to the ad broker. For every click, advertiser A_j pays P_j, which is its strategy.

The utility of advertiser A_j is defined as its revenue from clicks minus the fee it pays to the the ad broker

$$U_j^a = Q_j n_j - P_j n_j, \tag{1}$$

in which n_j is the number of clicks on advertisement A_j.

The ad broker receives money from advertisers and decides the total amount M_j to be paid to all users for clicking advertisement A_j. The money is then allocated equally to every user who clicks advertisement A_j.

The utility of the ad broker is defined as the total revenue from all advertisers minus the total money paid to users

$$U^b = \sum_j P_j n_j - \sum_j M_j. \tag{2}$$

User's strategy is whether to click the advertisement. $R_{i,j} = 0$ means user S_i decides not to click advertisement A_j and $R_{i,j} = 1$ means user S_i decides to click advertisement A_j. Then the total number of clicks for advertisement A_j is $n_j = \sum_q R_{q,j}$. As described above, the money every user get for all the advertisements is

$$\sum_j M_j \frac{R_{i,j}}{\sum_q R_{q,j}}. \tag{3}$$

User's loss is its privacy because the ad broker gets to know its advertisement preference. As described in SectionII-B, every user has a privacy sensitivity level ω_i which is defined as the amount of money needed to compensate for every unit of privacy leakage. Privacy leakage of clicking on advertisement A_j is $\alpha_j/n_j = \alpha_j/\sum_q R_{q,j}$. Therefore, the amount of money needed to compensate for user's privacy leakage is

$$\omega_i \frac{\alpha_j R_{i,j}}{\sum_q R_{q,j}}. \tag{4}$$

Then, the utility of user S_i is defined as the amount of money it receives from the ad broker minus the amount of money needed to compensate for the privacy leakage

$$U_i^c = \sum_j M_j \frac{R_{i,j}}{\sum_q R_{q,j}} - \omega_i \sum_j \frac{\alpha_j R_{i,j}}{\sum_q R_{q,j}}. \tag{5}$$

III. GAME THEORY ANALYSIS

In this section, the framework of advertisement targeting system is formulated as a three-stage game. In the first stage of the game, knowing how the ad broker and users will react to its decision, each advertiser determines simultaneously the price of each advertisement click they will pay to the ad broker, aiming at maximizing its own utility. In the second stage, observing the price it receives for every click, the ad broker tries to maximize its utility by adjusting the amount of money it pays to all users for clicking each advertisement based on the knowledge of how users' behavior will be influenced. In the last stage, noticing the amount of money the ad broker will pay, users determine simultaneously whether to click the advertisements. All advertisers and users act in a non-cooperative way as they make decisions independently.

We use backward induction to derive Nash Equilibrium, where the optimal strategies for advertisers, the ad broker and users are given accordingly.

A. User Click Decision Game

We first analyze users' decision making process. User S_i's utility not only depends on its own decision, but also on other players' choices. Let $\{R_{i,j} : j = 1, ..., K\}$ denote user S_i's strategy and $\{R_{-i,j} : j = 1, ..., K\}$ denote the strategies of all the other users. Utility of user S_i is $U_i^c(R_{i,j}, R_{-i,j})$. The best response of S_i is

$$R_{i,j}^* = \arg\max_{R_{i,j}} U_i^c(R_{i,j}, R_{-i,j}). \tag{6}$$

The best response of S_i is its optimal strategy, given the strategies of other players. S_i will not deviate from its best response unilaterally as it can gain nothing. If every user adopts the best response, Nash Equilibrium is reached.

Proposition 1: When the following condition

$$\frac{M_j}{\alpha_j} \geq \min_i \{\omega_i\} \tag{7}$$

is satisfied, there exists a Nash Equilibrium for the game among users and the the optimal strategy of S_i is

$$R_{i,j}^* = \begin{cases} 1, & \omega_i \leq \frac{M_j}{\alpha_j} \\ 0, & \omega_i > \frac{M_j}{\alpha_j} \end{cases}. \tag{8}$$

Proof: From equation (5), we have

$$U_i^c = \sum_j (M_j - \omega_i \alpha_j) \frac{R_{i,j}}{\sum_q R_{q,j}}. \tag{9}$$

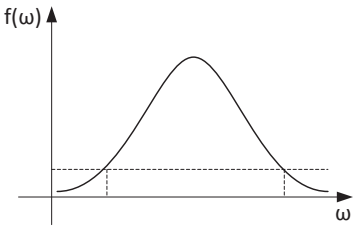


Fig. 2. Shape of probability distribution function

When $M_j \geq \omega_i \alpha_j$, choosing $R_{i,j} = 1$ can increase S_i's utility. Whereas, if $M_j < \omega_i \alpha_j$, choosing $R_{i,j} = 0$ can avoid decreasing S_i's utility. So U_i^c can be maximized when S_i decides the value of $R_{i,j}$ according to equation (8), which is S_i's optimal strategy. Equation (7) guarantees the denominator of equation (9) is not zero. Every user can get its optimal strategy by this mechanism. Nash Equilibrium is reached when they all adopt the optimal strategy. ■

B. Optimal Strategy of the Ad Broker

The ad broker is conscious of users' reactions to its strategy. When the ad broker decides its strategy $\{M_j : j = 1, ...K\}$, users will make their decisions according to proposition 1. Consequently, the ad broker can determine the optimal strategy.

Proposition 2: The ad broker has a unique optimal strategy that can maximize its utility.

Proof: From equation (2), we have

$$U^b = \sum_j (P_j n_j - M_j), \tag{10}$$

where $n_j = \sum_i R_{i,j} = \#\{\omega_i \leq \frac{M_j}{\alpha_j} : i = 1, 2..., N\}$. Assume $\{\omega_1, \omega_2, ..., \omega_N\}$ follow a certain kind of distribution, whose probability distribution function is $f(\omega)$. As N is a very large number (there are many end users in the system), n_j can be calculated in this way

$$n_j = N \int_0^{\frac{M_j}{\alpha_j}} f(\omega) d\omega. \tag{11}$$

So we have

$$U^b = \sum_j (P_j N \int_0^{\frac{M_j}{\alpha_j}} f(\omega) d\omega - M_j), \tag{12}$$

$$\frac{dU^b}{dM_j} = \sum_j (\frac{P_j N}{\alpha_j} f(\frac{M_j}{\alpha_j}) - 1), \tag{13}$$

$$\frac{d^2 U^b}{dM_j^2} = \sum_j (\frac{P_j N}{\alpha_j^2} f'(\frac{M_j}{\alpha_j})). \tag{14}$$

Fig.2 shows the shape of most probability distribution functions. As N is very large, there exists 2 points where $f(\omega) = \frac{\alpha_j}{P_j N}$. Only the right one has a negative derivative, so there exists a unique set of $\{M_j : j = 1, ...K\}$, that makes $\frac{dU^b}{dM_j} = 0$ and $\frac{d^2 U^b}{dM_j^2} < 0$. To sum up, the ad broker can maximize its utility by the following unique strategy

$$M_j^* = \alpha_j f^{-1}(\frac{\alpha_j}{P_j N}), \tag{15}$$

where we select the larger value of $f^{-1}(\frac{\alpha_j}{P_j N})$. ■

To get a close form of the ad broker's optimal strategy M_j^*, we assume that users' privacy sensitivities follow Gaussian distribution $N(\mu, \sigma^2)$, which is commonly used to model real-value random variables. In accordance with the 3-sigma rule, the probability that a variable lies within $[\mu - 3\sigma, \mu + 3\sigma]$ is 99.74% so that we can ignore the values outside this interval. Hence we can use Gaussian distribution $N(\mu, \sigma^2)$ to model users' privacy sensitivities (which are positive), assuming $\mu > 3\sigma$. Under this circumstance, the ad broker's optimal strategy is

$$M_j^* = \alpha_j (\mu + \sqrt{2\sigma^2 ln \frac{P_j N}{\alpha_j \sqrt{2\pi\sigma^2}}}). \tag{16}$$

C. Optimal Strategies of Advertisers

Advertisers know the ad broker's reaction to their strategies, based on which, advertisers can choose their optimal strategies.

Proposition 3: There exists optimal strategies for advertisers, and when users' privacy sensitivities follow Gaussian distribution, the optimal strategy for every advertiser is unique.

Proof: From equation (1) and (11), we have

$$U_j^a = (Q_j - P_j) N \int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega. \tag{17}$$

It is easy to prove that $U_j^a(P_j)$ is a continuous function and its upper bound is Q_j. So there exists P_j^*, which is the optimal strategy that maximizes U_j^a.

We further analyze the circumstance where $\{\omega_i : i = 1, ..., N\}$ follow the Gaussian distribution $N(\mu, \sigma^2)$. To simplify analysis, it is equal to consider function lnU_j^a. We have

$$\frac{d(lnU_j^a)}{dP_j} = \frac{-1}{Q_j - P_j} + \frac{f(\frac{M_j^*}{\alpha_j})}{\int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega} \frac{d(\frac{M_j^*}{\alpha_j})}{dP_j}, \tag{18}$$

where $P_j \in (0, Q_j)$. Together with equation (16), we get

$$\frac{d(lnU_j^a)}{dP_j} = \frac{-1}{Q_j - P_j} + \frac{\alpha_j \sigma^2}{N P_j^2 \sqrt{2\sigma^2 ln \frac{N P_j}{\alpha_j \sqrt{2\pi\sigma^2}}} \int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega}. \tag{19}$$

It is obvious that $\frac{d(lnU_j^a)}{dP_j}$ is a decreasing function with regard to P_j, that is $\frac{d^2(lnU_j^a)}{dP_j^2} < 0$, and the following two equations

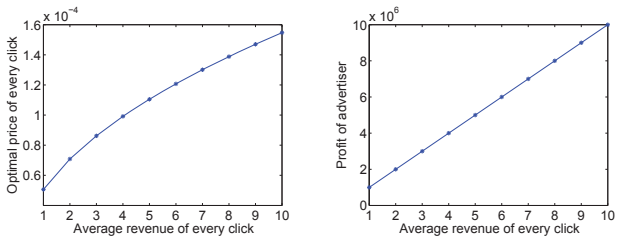
$$\lim_{P_j \to 0^+} \frac{d(lnU_j^a)}{dP_j} = +\infty, \tag{20}$$

$$\lim_{P_j \to Q_j^-} \frac{d(lnU_j^a)}{dP_j} = -\infty. \tag{21}$$

hold. So there is one unique P_j^*, where $\frac{d(lnU_j^a)}{dP_j} = 0$, and this P_j^* is the unique optimal strategy for advertiser A_j. ■

IV. Simulation Results

In this section we present the simulation results to show how different characteristics of advertisements and users will influence the best strategies and utilities of every player. We consider a model where users' privacy sensitivities $\{\omega_1, ..., \omega_N\}$ follow the Gaussian distribution $N(\mu, \sigma^2)$, for which $\mu > 3\sigma$ (so that we can ignore the interval where $\omega < 0$). As



(a) (b)

Fig. 3. Strategy and profit of advertiser versus revenue of every click

advertisers are independent from each other in our model, we analyze one advertiser A_j for simplicity. The value of parameters used in the simulation are shown in table I.

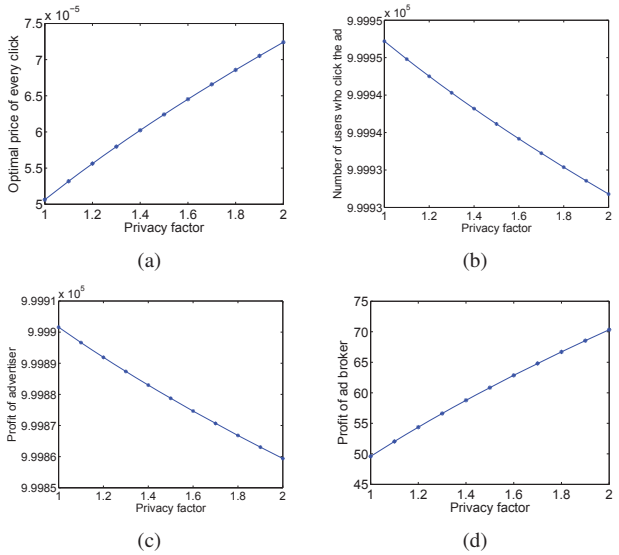
TABLE I
SIMULATION PARAMETER

Parameter	Description	value
Q_j	Average revenue of every click	1
α_j	Privacy factor	1
μ	Mean of users' privacy sensitivities	1
σ	Standard deviation of users' privacy sensitivities	0.01
N	Number of users	1000000

Fig. 3 shows that the optimal price of every click and the profit (utility) of A_j increase with Q_j, the average revenue A_j can gain from every click. A larger Q_j means a higher profit margin, so that the more users that click the advertisement, the higher the profit A_j can gain. Thus A_j has the incentive to pay a higher price to ultimately motivate more users to click, which in turn brings about higher profit. Simulation results show the profits of the ad broker also increase with Q_j (due to space limitation, we do not present it), which indicates the ad broker prefers to push advertisements with higher profit margin.

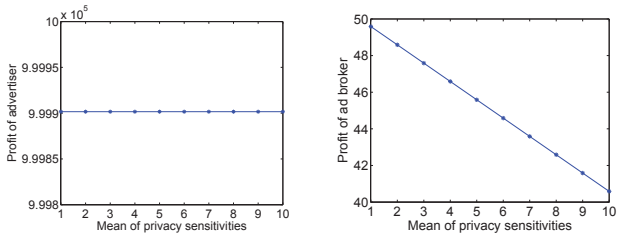
When the privacy factor α_j rises, which means clicking A_j leads to higher privacy leakage, the advertiser has to pay higher price to compensate and motivate users as shown in Fig. 4. The maximum profit decreases as the number of clicks declines. However, maximized profit of the ad broker increases with α_j. Thus, this system has less friction for advertisements with smaller privacy factors as the ad broker obtains less money from advertiser when α_j is smaller.

When the mean of users' privacy sensitivities rises, advertisers can make a constant profit while the ad broker's profit decreases as shown in Fig.5. It is indicated in equation (11) and (15) that when the shape of distribution $f(\omega)$ does not change as is the case here, the relationship between n_j and P_j stays the same. Advertiser A_j's profit is only affected by Q_j, n_j and P_j, where Q_j is a constant number, so that its strategy remains the same with the increase in μ, which in turn makes n_j and advertiser's profit constant. So it is the ad broker who pays for the users' increasing privacy sensitivities. The ad broker has to spend more money to motivate users when they become more sensitive to their privacy and consequently the ad broker's profit decreases. Therefore, when the mean of users' privacy sensitivities increase while the standard deviation remains constant, advertisers can make a constant profit while the ad broker's profit decreases.



(a) (b) (c) (d)

Fig. 4. Strategy and profit of advertiser, number of clicks and profit of the ad broker versus privacy factor



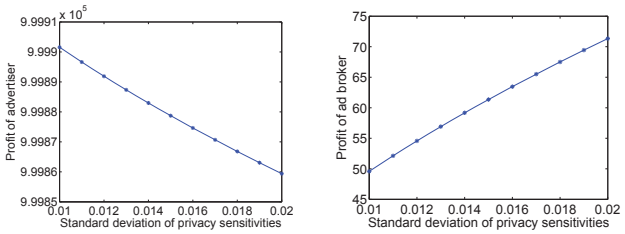
(a) (b)

Fig. 5. Profit of advertiser and the ad broker versus mean of users' privacy sensitivities

Fig.6(a) shows that when the standard deviation of users' privacy sensitivities varies from 0.01 to 0.02, advertiser profit declines. Under this scenario, advertisers have the incentive to increase its offer to encourage the ad broker to pay more to users. As analyzed in Section III-B, the optimal point is on the right half of the probability distribution function, which means that advertisers and the ad brokers are more concerned about 50% of the users, whose privacy sensitivities are higher than average as the other half are always successfully incentivized to click. With the increase in the standard deviation, the privacy sensitivity level of the "concerned group" is rising so that both advertisers and the ad broker raise their offers. An interesting finding here is that advertisers increase the price in a larger margin so that the ad broker can actually make a increasing profit as shown in Fig.6(b).

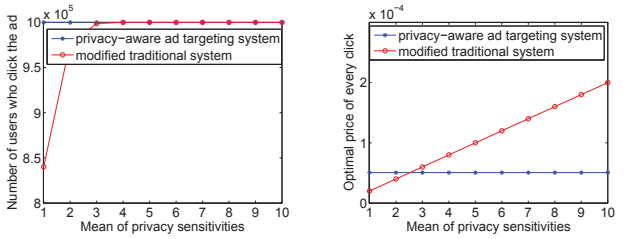
The traditional "paid to click" system requires a fixed price Pt_1 from all advertisers and pays a settled price Pt_2 to users for every click. To compare the performance, we modify the traditional system, where Pt_1 and Pt_2 are fixed to a certain user group and are linearly related to the mean of users' privacy sensitivities.

When the mean of privacy sensitivities varies, we try to set parameters (the linear coefficients of Pt_1 and Pt_2 with regard



(a) (b)

Fig. 6. Profit of advertiser and the ad broker versus standard deviation of users' privacy sensitivities



(a) (b)

Fig. 7. Comparison with modified traditional system when mean changes

to mean) that make the number of clicks similar under the two systems (as shown in Fig.7(a)). However, the price the advertiser has to pay is much higher in the traditional system leading to a much lower profit. When the standard deviation of privacy sensitivities changes, Pt_1 and Pt_2 remain constant. The number of users who click the advertisements decreases quickly(as shown in Fig.8) and the profits of advertisers and the ad broker drop accordingly at a high speed. To sum up, our system performs better concerning the profits of advertisers and the ad brokers.

V. Related Work

There is some existing research about advertisement targeting. One category mainly focuses on the interaction between advertisers and the the ad broker, where privacy is ignored. The authors in [9]–[11] discuss the problem of how a search engine maximizes its revenue when matching advertisements with each query. An auction is used to model this problem, where budget constraints of the bidders are taken into consideration. Mehta et al., in [9], propose an optimal algorithm, where a competitive ratio of $1 - 1/e$ is achieved. Based on previous online algorithms, [11] [12] derive a primal-dual framework which matches the competitive ratio of [9]. Devanur and Hayes [10] solve the problem under a random permutation.

Another category concerns users' privacy and tries to p-reserve it [3] [4]. In their systems, users' profiles are created and kept locally, the model of which is adopted in our system. As discussed in Section I, [3] and [4] propose two kinds of mechanisms that prevent users' privacy from leaking when reporting which advertisements are clicked. In [3], when the dealer colludes with the the ad broker, users' privacy is no longer safe. In [4], privacy is preserved at the expense of advertisers' satisfaction. Both works try to tackle the problem from a technical point of view, while our framework uses economic incentives to deal with the privacy problem.

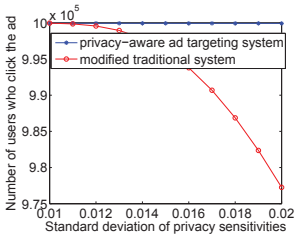


Fig. 8. Comparison with modified traditional system when standard deviation changes

VI. Conclusion

In this paper, we propose a novel privacy-aware framework for online advertisement targeting. Users, aware of their privacy leakage when clicking different advertisements, are compensated for the leakage and encouraged to click more advertisements. They decide whether to click an advertisement making a trade-off between the privacy leakage and the compensation they receive. Advertisers decide the price per user click, while the the ad broker decides the amount of money paid to the users. We model the framework as a three-stage game, for which the existence of Nash Equilibrium is proved. Also we theoretically analyze the optimal strategies of advertisers, the ad broker and users. Numerical results show that when privacy is taken into consideration, our system yields higher profits for both advertisers and the ad broker.

VII. Acknowledgement

The research was supportedl in part by grants from RGC under the contracts CERG 622410, HKUST grant S-RFI11FYT01, the grant from Huawei-HKUST joint lab, the National Natural Science Foundation of China under Grants No. 60933012 and 973 project 2013CB32900X.

References

[1] J. Yan, N. Liu, G. Wang, W. Zhang, Y. Jiang, and Z. Chen, "How much can behavioral targeting help online advertising?" in *Proc. WWW*, 2009, pp. 261–270.

[2] Google software bug shared private online documents. http://news.theage.com.au/breaking-news-technology/google-software-bug-shared-private-online-documents-20090310-8tup.html.

[3] S. Guha, A. Reznichenko, K. Tang, H. Haddadi, and P. Francis, "Serving ads from localhost for performance, privacy, and profit," in *Proc. ACM HotNets*, 2009.

[4] M. Kodialam, T. Lakshman, and S. Mukherjee, "Effective ad targeting with concealed profiles," in *Proc. IEEE INFOCOM*, 2012.

[5] J. P. Lawler, *A study of customer loyalty and privacy on the web*. Pace University, 2002.

[6] A. A. Hamilton, *Development and validation of a methodology to assess privacy sensitivity*. George Washington University, 2005.

[7] D. W. Bedford, *Empirical investigation of the acceptance and intended use of mobile commerce: location, personal privacy and trust*. Mississippi State University, 2005.

[8] B. P. Clifford, *Online privacy sensitivity and gender— A case study of a highly-educated adult population*. Capella University, 2009.

[9] A. Mehta, A. Saberi, U. Vazirani, and V. Vazirani, "Adwords and generalized online matching," *J. ACM*, vol. 54, no. 5, p. 22, 2007.

[10] N. Devanur and T. Hayes, "The adwords problem: online keyword matching with budgeted bidders under random permutations," in *Proc. ACM EC*, 2009, pp. 71–78.

[11] N. Buchbinder, K. Jain, and J. S. Naor, "Online primal-dual algorithms for maximizing ad-auctions revenue," in *Proc. European conference on Algorithms*, ser. ESA'07, 2007.

[12] N. Buchbinder and J. Naor, "Online primal-dual algorithms for covering and packing problems," in *Proc. European conference on Algorithms*, ser. ESA'05, 2005.