A Privacy-aware Framework for Online Ad Targeting

Linlin Yang, Wei Wang, Qian Zhang
The Hong Kong University of Science and Technology
Email: {lyangah, gswwang, qianzh}@ust.hk

***Abstract*—With the prosperity of Internet, many advertisers choose to deliver their ads by online targeting, where ad broker, the intermediary, is responsible for matching ads with users who are likely to be interested in the underlying products or services. This existing advertising fashion may fail due to privacy problems. In the light of the growing importance of privacy problems, we propose a privacy-aware framework for online ad targeting, where users are compensated for their privacy leakage. In our framework, a varying amount of money, according to ad broker's strategy, is paid to users for clicking different ads due to distinct privacy leakage caused. Advertisers sending ads to ad broker have the right to determine the price for every click they pay to ad broker. We model this system as a three-stage game, where every player aims at maximizing its own utility, and Nash Equilibrium is achieved in theoretical analysis. Based on the analysis, we discuss the optimal strategies for advertisers, ad broker and users. The numerical results have shown our privacy-aware framework is promising as all advertisers, ad broker and users can maximize their utilities with different levels of users' privacy sensitivities. And this framework performs better than modified traditional "paid to click" system.**

***Index Terms*—Ad targeting, privacy, profit.**

I. Introduction

Internet is an efficient way for ads to reach users so that many advertisers choose to deliver their ads by online targeting nowadays. In most existing online ad targeting systems, ad broker, the intermediary, makes use of users' online behavior to match ads with users who are likely to be interested in the underlying products or services. For example, Google Adwords, which is a huge success, leverages users' search items to show ads. However, with growing consciousness of privacy, many users resist to reveal their profile information. And some steps are taken to protect users' online privacy. The Do Not Track (DNT) header which disables tracking was proposed in 2009 [1]. Main browsers, Mozilla's Firefox, Internet Explorer, Apple's Safari, Opera and Google Chrome, have all supported for the DNT mechanism. This poses great challenges to online ad targeting as ad brokers may have no idea of users' interests. Thus it is essential to take privacy into consideration for online ad targeting.

There are mainly two works [2] [3] tackle the privacy problem about online ad targeting. In their frameworks, ads are targeted without users' private profile information leaving their own devices. As report about which ads are clicked will reveal user's interest, to count the number of clicks for every piece of ad without compromising users' privacy, [3] introduces a new entity dealer to proxy all communication between users and ad broker in an anonymous way. In this system, only when dealer does not collaborate with ad broker, can users' privacy be preserve, for which however there is no guarantee. In [2], users send falsified click information to ad broker according to some predetermined rules. An algorithm to estimate actual number of clicks for every piece of ad is proposed for ad broker. This system preserves users' privacy, but advertisers may be unsatisfied with it as number of clicks are inaccurate, based on which they will pay.

In our privacy-aware framework, we try to preserve users' privacy to a large extent and compensate them for the privacy leakage involved in their reports about which ads are clicked. In this way, advertisers get the accurate number of clicks for their ads and users, aware of their privacy leakage, are compensated and motivated to click ads. The system structure is shown in Fig.1 and it works as follows.

1. Advertisers send ads to ad broker and have the right to determine the price of every click for their ads according to the revenues they can gain from every click.

2. Ad broker does not have users' profile information in our framework. It receives ads from advertisers and push them directly to users without matching. Accurate reports about which ads are clicked are sent from users and ad broker count the number of clicks for every piece of ad according to it. To compensate for privacy leakage and motivate clicking, ad broker pays a varying amount of money to all users for clicking different ads due to distinct privacy leakage.

3. Users have their profile information kept on their own devices. Once receive ads from ad broker, the devices determine the set of ads their owners may be interested in and display them when possible. Users make the decision whether to click ads balancing the amount of money they will receive and the privacy they will leak.

Assume all advertisers, ad broker and users are rational and selfish, the framework can be analyzed by a three-stage game, where every player's utility is maximized. Knowing how ad broker and users will react to their decisions, advertisers first optimize their strategies (the price of every click). Observing advertisers' strategies, ad broker determines the optimal amount of money paid to users for every piece of ad based on the knowledge how users' behavior (whether to click ads) will be influenced. We use backward induction to prove the existence of Nash Equilibrium and analyze the optimal strategies of advertisers, ad broker and users. Numerical results under the assumption that users' privacy sensitivities follow

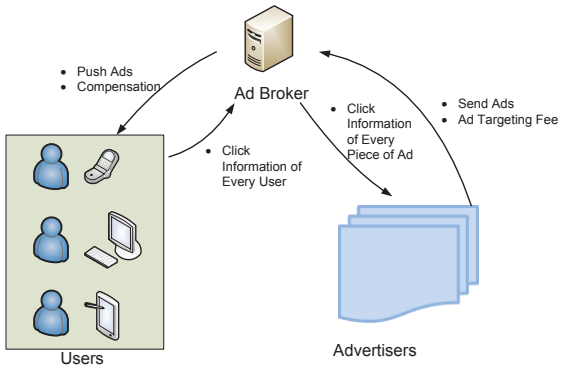


Fig. 1. Structure of privacy-aware ad targeting system

Gaussian distribution have shown that all advertisers, ad broker and users can optimize their utilities and this framework performs much better than modified traditional "paid to click" system.

There are some existing research about advertisement targeting. One category mainly focuses on the interaction between advertisers and ad broker, where privacy is ignored. [4]–[6] discuss the problem how can a search engine maximize its revenue when matching ads with each query. Auction is used to model this problem, where budget constraint of the bidders are taken into consideration. [4] proposes an optimal algorithm, where a competitive ratio of $1 - 1/e$ is achieved. Based on previous online algorithm [7], [6] derives a primal-dual framework which matches the competitive ratio of [4]. [5] solved the problem under a random permutation.

Another category concerns users' privacy and tries to preserve users' privacy [2] [3]. In their systems, users' profiles are created and kept locally, which is adopted in our system. As discussed above, [2] and [3] propose two kinds of mechanisms that prevent users' privacy from leaking when reporting which ads are clicked. In [3], when dealer collaborate with ad broker, users' privacy is no longer safe. In [2], privacy is preserved at the expense of advertisers' satisfaction. They both try to tackle the problem from technical point of view. Our framework uses economic tools to deal with the privacy problem.

The main contributions of this paper are as follows. 1) A novel privacy-aware framework for online ad targeting is proposed. Users, aware of the privacy leakage, are compensated for it so that they are motivated to click more ads, which in turn will increase the revenue of advertisers and ad broker. 2) We model the framework as a three-stage game and theoretically analyze the Nash Equilibrium for the game as well as optimal strategies of advertisers, ad broker and users; 3) Via simulation, we evaluate the performance of our framework when users' privacy sensitivity levels change. Numerical results show advertisers can make a constant profit when only the mean of users' privacy sensitivity levels change and ad broker can actually has higher profit when only the standard deviation of users' privacy sensitivity levels rise. We also compare our framework with modified traditional "paid to click" system. Results show our framework has better performance.

The rest of the paper is organized as follows. In Section II, we introduce system model, proposing the concept of privacy sensitivity and analyzing the utilities of advertisers, ad broker and users. In Section III we model the system as a three-stage game and theoretically analyze the optimal strategies of advertisers, ad broker and users. Simulation results are shown in IV and we made a conclusion in V.

II. SYSTEM MODEL

In this section, we first introduce the framework of our ad targeting system. Then, the concept of privacy sensitivity is put forward. Finally, we analyze the utilities of advertisers, ad broker and users.

A. Framework

The ad targeting system (shown in Fig.1) consists of multiple advertisers, one ad broker and multiple users. Every advertiser has one piece of advertisement. So we will use the term advertiser and advertisement interchangeably. We assume there are totally K advertisers and N users in concern. 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 are rational and selfish, who want to maximize their own utilities.

Ad broker runs an advertising platform, collecting ads from different advertisers and deliver them to users. Meanwhile, ad broker counts the clicks of every piece of ad and charges advertisers for every click. As ad click information of every user, which is a kind of private information, is revealed to ad broker, ad broker pays users a certain amount of money to compensate for their privacy leaking and motivate them to click. Users make the decision whether to click ads according to their privacy sensitivity and the money they can get for clicking.

B. Privacy Sensitivity

Researchers have proposed several definitions of privacy sensitivity [8] [9] [10]. We define privacy sensitivity as the amount of money needed to compensate for every unit of privacy leakage in clicks. Privacy leakage is a relatively subjective concept. Clicking different kinds of ads lead to different levels of privacy leakage. For example, clicking a medicine ad may indicate that you have certain kind of disease, which cause a high level of privacy leakage. While clicking an umbrella ad only means you need an umbrella, leading to a low level of privacy leakage. Thus according to the nature of an ad A_j, we assume a privacy factor α_j for it. Meanwhile, privacy leakage for clicking an ad is also negatively related to the total number of clicks of the ad, which means the more users click the the same ad, the less privacy leakage for every user who clicks it. For example, during a certain period, when influenza is prevalent, many people may click medicine ads related to influenza and having influenza is not of high privacy under this circumstance. But when there is few people affected by influenza and number of clicks of related medicine ads is

small, the information of having influenza is of relatively high privacy so that the privacy leakage of clicking these ads is higher. Thus, we define privacy leakage of ad A_j as $\frac{\alpha_j}{n_j}$, where n_j is total number of users who click ad A_j.

Studies have shown that different people have different privacy sensitivities [8] [9] [10]. Factors like gender, education and age contribute to privacy sensitivity [11]. Accordingly, let $\{\omega_i : i = 1, ..., N\}$, which may different from each other, represent privacy sensitivities of users.

C. Utility Functions

Advertisers gains revenue from clicks. After users watching ads, they may become interested in the underlying products or services so that they will buy them. Assume for every click, advertiser A_j gains a revenue of Q_j on average.The expense of advertisers is the money they pays to 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 ad broker

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

in which n_j is the number of clicks of ad j.

Ad broker receives money from advertisers, which is its revenue, and decides the total amount M_j it pays to all users for clicking ad A_j. The the money is then allocated evenly to every user who clicks ad A_j.

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

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

Users' strategies is whether to click the ad. Suppose $R_{i,j} = 0$ means user i decides not to click ad j and $R_{i,j} = 1$ means user i decides to click ad j. Then the total number of clicks for ad j is $n = \sum_q R_{q,j}$. As described above, the amount of money every user get for all the ads is

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

User's loss is its privacy as ad broker gets to know its ad preference. As described in "Privacy Sensitivity", every user has a privacy sensitivity level ω_i and privacy leakage of clicking ad A_j is $\frac{\alpha_j}{n_j} = \frac{\alpha_j}{\sum_q R_{q,j}}$. Therefor, the amount of money needed to compensate for user's privacy leakage is

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

The utility of user S_i is defined as the amount of money it receivers from ad broker minus the amount of money it needs to compensate for its 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 ANALYSIS

In this section, the framework of ad targeting system is formulated as a three-stage game. We use backward induction to prove the existence of Nash Equilibrium, where the optimal strategies for advertisers, ad broker and users are defined accordingly.

In the first stage of the game, knowing how ad broker and users will react to its decision, every advertiser determines simultaneously the price of every ad click they will pay to ad broker, with the aim of maximizing its own utility. In the second stage, observing the price it will receive for every click of ads, ad broker tries to maximize its utility by adjusting the amount of money it will pay to all users for clicking each piece of ad based on the knowledge how users' behavior will be influenced. In the last stage, noticing the amount of money ad broker will pay, users determines simultaneously whether to click the ads. All advertisers and users act in a non-cooperative way as they make decisions independently.

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 others' choices. Let $\{R_{i,j} : j = 1, ..., K\}$ denote user S_i's strategy and $\{R_{-i,j} : j = 1, ..., K\}$ denote 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 and S_i will not deviate from this best responese as it can gain nothing by changing its strategy unilaterally in a non-cooperative game. 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

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

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 every one adopts the optimal strategy. ■

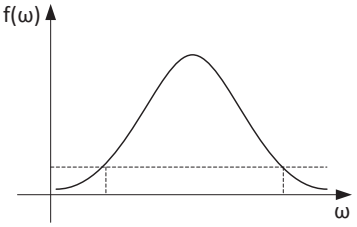


Fig. 2. Shape of probability distribution function

B. Optimal Strategy of Ad Broker

Ad Broker is conscious of users' reaction to its strategy. When ad broker decides its strategy $\{M_j : j = 1, ...K\}$, users will make their decisions in the light of proposition 1. Consequently, ad broker can select the optimal strategy.

$Proposition$ 2: 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 $\{\omega_1, \omega_2, ..., \omega_N\}$ obey 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

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

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

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

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 negative derivative. So there exists a unique set of $\{M_j : j = 1, ...K\}$, that makes $\frac{dU^b}{dM_j} = 0$ and $\frac{d^2U^b}{dM_j^2} < 0$. To sum up, 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 $f^{-1}(\frac{\alpha_j}{P_j N})$. ■

Gaussian distribution $N(\mu, \sigma^2)$ is usually used to model real-value random variables. In accordance with 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 outside intervals. Thence we can use Gaussian distribution $N(\mu, \sigma^2)$ to model user's privacy sensitivities (which are positive), assuming $\mu > 3\sigma$. Under this circumstance, 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

Similar to ad broker, advertisers know ad broker's reaction to their strategies. Basing on this, advertisers can choose the optimal strategies.

$Proposition$ 3: There exists optimal strategies for advertisers. And when users' privacy sensitivity levels 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 maximize U_j^a.

Further analyze the circumstance where $\{\omega_i : i = 1, ..., N\}$ follow the Gaussian distribution $N(\mu, \sigma^2)$. To simplify analysis, it's 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 (18), we get

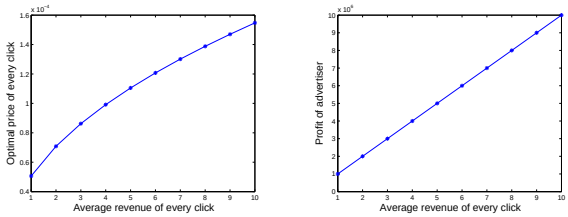
$$\frac{d(lnU_j^a)}{dP_j} = \frac{-1}{Q_j - P_j} + \frac{\alpha_j \sigma^2}{N P_j^2 \sqrt{2\sigma^2 ln \frac{NP_j}{\alpha_j \sqrt{2\pi\sigma^2}}} \int_0^{\frac{M_j^*}{\alpha_j}} f(\omega) d\omega}. \tag{19}$$

It is obvious $\frac{d(lnU_j^a)}{dP_j}$ 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. ■



(a) (b)

Fig. 3. Simulation results when revenue of every click changes

IV. Simulation Results

In this section we show simulation results to unveil how different characteristics of ads 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 Gaussian distribution $N(\mu, \sigma^2)$ where $\mu > 3\sigma$ (so that we can ignore the interval where $\omega < 0$). As different advertisers do not interfere with each other in our model, we analyze one advertiser A_j here for simplicity. The value of parameters used in the simulation are shown in table I.

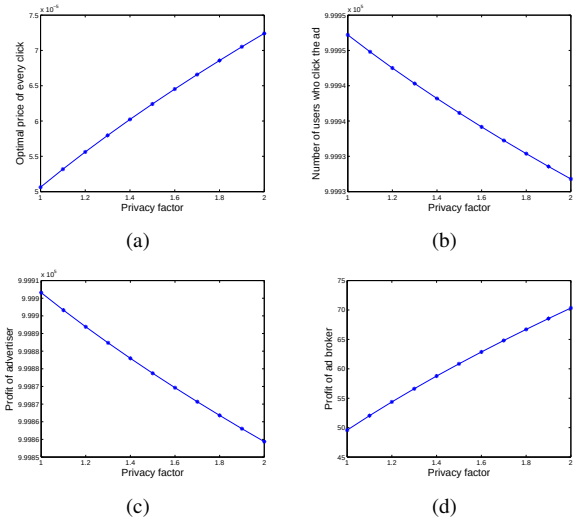
TABLE I
Simulation Parameter

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 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 higher profit margin so that the more users click the ad the higher 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 brought about higher profit. Simulation results show profit of ad broker also increase with Q_j (due to space limitation, we do not present it), which indicates ad broker will prefer to push ads with higher profit margin.

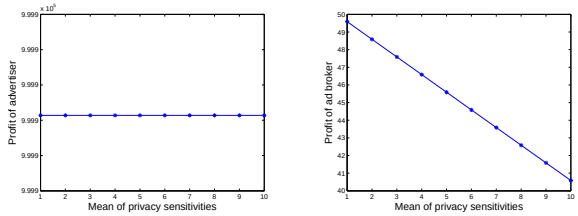
When the privacy factor of A_j, α_j, rises, which means clicking A_j leads to higher privacy leakage, advertiser has to pay higher price to compensate and motivate users as shown in Fig. 4. Its maximized profit decreases as number of clicks declines. However, maximized profit of ad broker increases with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

When the mean of users' privacy sensitivities rises, advertiser can make a constant profit while ad broker's profit decreases as shown in Fig.5. It is indicated in equation (11) and (15) when the shape of distribution $f(\omega)$ do not change, which is the case here, the relationship between n_j and P_j keeps the same. Advertiser's profit is only affected by Q_j, n_j and P_j, where Q_j is a constant number, so that its strategy keeps the same with the increase in μ, which in turn makes



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

Fig. 4. Simulation results when privacy factor changes



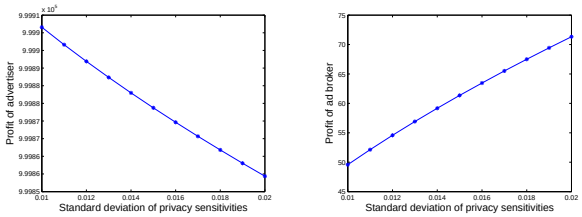
(a) (b)

Fig. 5. Simulation results when mean of users' privacy sensitivities changes

n_j and advertiser's profit constant. So it is ad broker that pay for users' increasing privacy sensitivities. Ad broker has to spend more money on motivating users when they become more sensitive with their privacy and consequently ad broker's profit decreases. Therefore, when the mean of users' privacy sensitivities increase while the standard deviation keeps constant, advertiser can make a constant profit while ad broker's profit decreases.

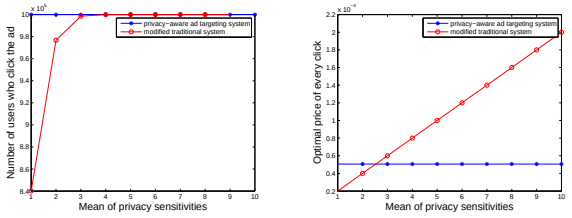
Fig.6(a) shows when the standard deviation of users' privacy sensitivities varies from 0.01 to 0.02, profit of advertisers declines. Under this scenario, advertiser has the incentive to increase its offer to stimulate ad broker paying more to users. As analyzed in Section III.B, the optimal point is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



(a) (b)

Fig. 6. Simulation results when standard deviation of users' privacy sensitivities changes



(a) (b)

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

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 tried to set parameters (the linear coefficients of Pt_1 and Pt_2 with regard to mean) that make the number of clicks similar under the two systems (as shown in Fig.7). But the price advertiser has to pay is much higher in the traditional system so that its profit is much lower. When the standard deviation of privacy sensitivities changes, Pt_1 and Pt_2 keep constant. The number of users who click decrease quickly(as shown in Fig.8) and the profit of advertisers and ad broker drop in a high speed accordingly. To sum up, our system performs better concerning the profit of advertisers and ad brokers.

V. Conclusion

In this paper, we propose a novel privacy-aware framework for online ad targeting. Users are aware of their privacy leakage when clicking different ads and are compensated for it. They make the decision whether to click an ad balancing the privacy leakage and compensation they receive. This system guarantees higher number of clicks and profits of advertisers and ad broker are maximized. We model the framework as a three-stage game, for which the existence of Nash Equilibrium is proved. And theoretically we analyze the optimal strategies of advertisers, ad broker and users, which is consistent with simulation results. Via simulation, we evaluate the performance of our framework with different characteristics of ads and users. Results show when take privacy into consideration, our system derives higher profits for both advertisers and ad broker.

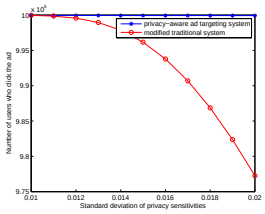


Fig. 8. Comparison with modified traditional system when standard deviation changes

References

[1] H. Tschofenig and R. van Eijk, "Do not track."

[2] M. Kodialam, T. Lakshman, and S. Mukherjee, "Effective ad targeting with concealed profiles," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 2237–2245.

[3] S. Guha, A. Reznichenko, K. Tang, H. Haddadi, and P. Francis, "Serving ads from localhost for performance, privacy, and profit," in *Proceedings of the 8th Workshop on Hot Topics in Networks (HotNets 09), New York, NY*, 2009.

[4] A. Mehta, A. Saberi, U. Vazirani, and V. Vazirani, "Adwords and generalized online matching," *Journal of the ACM (JACM)*, vol. 54, no. 5, p. 22, 2007.

[5] N. Devanur and T. Hayes, "The adwords problem: online keyword matching with budgeted bidders under random permutations," in *ACM Conference on Electronic Commerce*. ACM, 2009, pp. 71–78.

[6] N. Buchbinder, K. Jain, and J. Naor, "Online primal-dual algorithms for maximizing ad-auctions revenue," *Algorithms–ESA 2007*, pp. 253–264, 2007.

[7] N. Buchbinder and J. Naor, "Online primal-dual algorithms for covering and packing problems," *Algorithms–ESA 2005*, pp. 689–701, 2005.

[8] J. P. Lawler and B. Adviser-Raggad, "A study of customer loyalty and privacy on the web," 2002.

[9] A. A. Hamilton and M. J. Director-Granger, *Development and validation of a methodology to assess privacy sensitivity*. George Washington University, 2005.

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

[11] B. P. Clifford, "Online privacy sensitivity and gender— a case study of a highly-educated adult population," Ph.D. dissertation, CAPELLA UNIVERSITY, 2009.