2014 IEEE 11th Intl Conf on Ubiquitous Intelligence & Computing and 2014 IEEE 11th Intl Conf on Autonomic & Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops

Privacy Perceptive Wireless Service Game Model

Weiwei Li
School of Computer Science and Technology
Shandong University
Jinan, China
Email: 541730863@qq.com

Yuqing Sun*
School of Computer Science and Technology
Shandong University
Jinan, China
Email: sun_yuqing@sdu.edu.cn

***Abstract*—Wireless applications are taking an important role in our lives. More and more merchants begin to provide wireless connection so as to attract customers. For business purpose, they often ask customers to provide their personal information for using wireless, which may threat customer privacy. So, it is desired to make a tradeoff between the competitive profits of both service providers and user privacy. In this paper, we introduce a privacy perceptive service model based on game theory, which takes into account the interests of all stakeholders. Considering the characteristics of customer behavior in practice, we design the complete information and sequential game. Users are allowed to provide different levels of personal information as their preferences, while a merchant assigns different wireless bandwidth based on customer provided information. The Nash Equilibriums are discussed so as to find the acceptable strategy. Quantitative study is performed on the impact of each parameter in the game, which could help merchants to design appropriate policies.**

***Keywords*—privacy, game theory, wireless connection**

I. Introduction

With the widely adopted intelligent mobile devices, wireless applications are more and more popular such that people are used to accessing Internet everywhere. Facing these requirements, merchants such as restaurants and shops begin to provide wireless network access so as to attract more guests. Since the adoption of wireless facility increases the cost, merchants often ask guests either to accept advertisements or to provide personal information for further business promotion. For example, some merchants ask a user to register on their web sites, such as providing user name, gender, age, birthday and etc., and then send a pin code for accessing wireless network to user. By this way, they get users' personal information. This threats user privacy. Furthermore, if a merchant requires much personal information for accessing wireless, guests may refuse to provide or even choose not to come back again, which deviates from merchant's initial purpose. So it is important to choose an appropriate strategy that benefits both guests and merchants.

There are similar problems when a merchant launches a new business model or a wireless application. With the increasing fierce competition, more and more merchants design and provide new services. To counteract the cost of application facilities, merchants often ask guests personal information for future business promotion. Justifying whether a wireless business model is appropriate is necessary before we apply this model.

In the above scenario, merchant and users have different considerations. Service providers care about the cost of wireless facilities, the benefits on attraction of user being here and the usage of user personal information, which decide whether to provide wireless connection or how much the bandwidth they provide. From the aspect of users, the considerations are the sensitivity of personal information and the convenience of accessing wireless, which together determine whether to provide the required personal information for accessing wireless network. So, it is a challenging problem to satisfy these competitive requirements.

In this paper, we try to take into account all stockholders benefits in an integrated strategy by game theory. We consider the privacy protection in a concrete wireless connection service scenario, where customers and merchants are players with different considerations. Compared to previous works in privacy protection, a distinct character of our method is introducing the $win-win$ idea. Merchants and guests are modeled as players and their considerations are formalized as quantitative utility functions. To well present the flexible service applications, an iterative game process is designed as sequential strategies. Quantitative evaluation on equilibrium is performed by simulation experiments and detailed analyses is discussed on user choices under practical context. Although it is based on the wireless applications, it can also be applied to other similar business applications.

The rest of this paper is organized as follows.In section II, we introduce the related work. Section III presents the basic concepts and the game model. In section IV, we present the first round game and the multiple round game, and then analyze the Nash Equilibrium in different situations. Synthesized experiments are performed in Section V. Finally, section VI concludes the whole paper.

Yuqing Sun*, corresponding author

978-1-4799-7646-1/14 $31.00 © 2014 IEEE
DOI 10.1109/UIC-ATC-ScalCom.2014.116

II. Related work

Recently, game theory is adopted more and more frequently in privacy protection[2], [11],[12], [14]. It often models privacy protection as a competitive process and the purpose is to find out the Nash Equilibrium[3], [15], [16]. To be fully defined, a game must specify the following elements: the players, the strategy for each player, and the payoff for each outcome[19]. The following are representative methods.

The Stackelberg game model: Giuseppe $et\ al.$[1] study that the information disclosure will bring damages to customers and service providers. They propose a damage-sharing strategy to protect customer privacy, which makes service providers take some loss if user privacy is clearly disclosed.

The auction game model: Bugatti $et\ al.$[4] adopt auction theory to protect the user privacy in e-commerce for the first time. They use the Victory auction game model to find out the best service provider who requires minimal privacy information. In that way, auction game model creates a competitive context to the multiple service providers, such that they can not obtain as much information as their expectation.

The cooperation game model: In the context, if a user prohibits everyone from accessing his own album but his/her friends let them to access, user privacy can easily leak. Akira $et\ al.$[10] give an overview of the unexpected users information disclosure. They propose three attacking scenarios which are revealing the hidden friend-lists, posting messages, and exploiting sensitive information. Finally, they discuss countermeasures in terms of implementation and human behavior.

The two-player zero-sum game model: In an attack scenario, a defender uses K-anonymity to hide a user location. An attacker obtains defender information and predicts his location. Grossklags $et\ al.$[13] present a two-player zero-sum game to protect defender local information from attackers. They present a unique mixed strategy Nash equilibrium.

Although these work analyze and solve the issues of privacy protection in social networks and e-commerce, but they are not suitable for the assignment of wireless. In this paper, we propose a privacy perceptive wireless service game model to solve this problem.

III. The Privacy Perceptive Wireless service Model

A. Requirements Analysis

In this paper, we consider the scenario that only one merchant provides wireless services and multiple users require the wireless utility. There are four characteristics of this application. The first is that user using wireless is a continuous process. A user comes to a shop many times and may want to access wireless more than once. The second is privacy collection is progressive. If a user wants to access the wireless, he/she must provide more and higher level privacy if he/she does not provide enough last time. The third is that the amount of collected privacy should be limited. A merchant may ask for user privacy in a gradual manner, but the total amount of required information should be limited. The fourth is the limitation of network bandwidth. If there are multiple users in a shop, the bandwidth for each user is limited also.

B. Basic Conception and Problem Definition

Definition 1 (Merchant)**.** A merchant denotes a subject in a system, who provides the wireless application.

Definition 2 (User)**.** A user (also called customer) denotes a person who uses the wireless service in a system. Let C denote the set of all users in a system.

Definition 3 (User Privacy)**.** User privacy is a set of user's sensitive information denoted by Φ, such as name, age, ID number, and so on.

Definition 4 (Privacy Classification)**.** User privacy can be classified into several non-intersect subsets, $\Phi = \{\rho_1, \cdots, \rho_n\}$, where $n \in N^+$ denotes the number of sensitivity levels in a system, $\rho_i \in \Phi, i \in [1..n]$ is the set of privacy information in sensitivity level i. Each level is associated with a score $c_i \in N^+$, $i \in [1..n]$ to quantify information sensitivity. For convenience, all ρ_i are ranged according to their sensitivity levels. For $1 < i < j < n$, the information in ρ_i is less sensitive than the information in ρ_j and $c_i < c_{i+1}$.

Actually, privacy sensitivity is a general classification on how much a user cares about his/her privacy information. According to the surveys [18][20], user privacy is generally classified into three sensitivity levels: $General$, $Sensitive$ and $Secret$, whose sensitivities are in an ascending order. The information of $General$ level often includes character, interest, religion, etc. $Sensitive$ information often consists height, weight, family background and so on. $Secret$ is about the information that people do not want to share, such as ID number, bank account, etc.

Definition 5 (User Privacy Loss)**.** Given a user $u \in C$, a privacy information set $\rho_i \in \Phi$, the user privacy loss $P_{ui} \in R^+$ describes how much u considers the importance of ρ_i.

It is easy to understand that for any user $u \in C$, the higher the level of privacy, the higher user privacy loss . Formally, for $\rho_i, \rho_j \in \Phi, i < j$, $P_{ui} < P_{uj}$ holds.

Definition 6 (Utility of Privacy Information)**.** Given a set of privacy information $\rho \in \Phi$ in a system with one merchant, the utility of ρ ($U_\rho \in R^+$) denotes how much benefit this merchant can get from ρ .

Obviously, the higher the level of privacy, the more utility. Formally, for $\rho_i, \rho_j \in \Phi, i < j$, $U_{\rho_i} < U_{\rho_j}$ holds.

Definition 7 (Players)**.** The players are the people who take part in a game. Let P denotes the set of players in a system. In the game of wireless service model, the players include both users and the merchant.

TABLE I: The Utility Matrix

C \ M	w_1	w_2	w_3	R
A_1	$(U_{w_1} - P_{u1}, U_{\rho_1} - C_{w_1})$	$(U_{w_2} - P_{u1}, U_{\rho_1} - C_{w_2})$	$(U_{w_3} - P_{u1}, U_{\rho_1} - C_{w_3})$	$(-P_{u1}, U_{\rho_1})$
A_2	$(U_{w_1} - P_{u2}, U_{\rho_2} - C_{w_1})$	$(U_{w_2} - P_{u2}, U_{\rho_2} - C_{w_2})$	$(U_{w_3} - P_{u2}, U_{\rho_2} - C_{w_3})$	$(-P_{u2}, U_{\rho_2})$
A_3	$(U_{w_1} - P_{u3}, U_{\rho_3} - C_{w_1})$	$(U_{w_2} - P_{u3}, U_{\rho_3} - C_{w_2})$	$(U_{w_3} - P_{u3}, U_{\rho_3} - C_{w_3})$	$(-P_{u3}, U_{\rho_3})$
R	$(U_{w_1}, -C_{w_1})$	$(U_{w_2}, -C_{w_2})$	$(U_{w_3}, -C_{w_3})$	$(0, 0)$

Definition 8 (Player Strategy)**.** Player strategy is a kind of player behaviors. The set of strategies is a policy set.

Based on the above requirements, we propose a two-player non-zero-sum game model. There are three parts: players, strategies and equilibrium. Users and merchants are modeled as players. Each player has its own strategy. The strategy of a merchant includes four cases: not to provide the wireless, providing a bandwidth W_1 of wireless connection, providing a bandwidth W_2 of wireless connection, providing a bandwidth W_3 of wireless connection, denoted as $S_m = \{R, W_1, W_2, W_3\}$. The strategy of a user includes four parts: to reject to give his/her different personal information, or to provide level 1, 2, 3 privacy information for accessing wireless. Let the strategy of a user u denote as $S_c = \{R, A_1, A_2, A_3\}$, where $A_i, i \in [1, 2, 3]$ means that a user gives his/her $level_i$ privacy to the merchant. Since different users care about their sensitive information in different degree, they are allowed to have different strategies. Further since the sensitivity level of information is different, the strategy on different information is different correspondingly.

The purpose of such game is to find the equilibrium to make each player gain largest benefit.

Definition 9 (Privacy Release)**.** Privacy release refers to the sum of sensitivity scores of the information that a specific user provide. Formally, for user u and his/her released information set I_u, the privacy release is computed as g_u=$\sum_{\iota \in I_u} c_\iota$, where c_ι is the predicate to map the information ι to its privacy sensitivity score.

Definition 10 (Upper Bound of Privacy Release)**.** The upper bound of privacy release g_{max} is the maximum that a merchant may ask from a user.

For some user $u \in C$, if $g_u > g_{max}$, u can get the bandwidth for accessing wireless. Otherwise, u should further provide privacy information and can get the corresponding bandwidth of wireless. How to set g_{max} is important. If a merchant sets g_{max} too high, any user would not accept. If g_{max} is low, the merchant could not get enough usable information.

Since the wireless bandwidth of a merchant is limited, more users using wireless can cause the network speed lower. So we introduce the concept of minimum bandwidth. In this game, we design the bandwidth assignments strategy as: in the same game, the more information one provides, the larger bandwidth is assigned. For example, if the basic bandwidth is w_0, then w_0, $2w_0$ and $3w_0$ are set for users who provide information of $level_1$, $level_2$ and $level_3$. So, given a set of users C and a bandwidth W, the minimum bandwidth is computed as $w_0 = \frac{W}{3*|C|}$. So the wireless usage problem is transformed to determine how to assign bandwidth to each user.

C. Game Process

Based on the above analysis, we introduce the wireless utility game.

Definition 11 (The Wireless Utility Game)**.** The wireless utility game is defined as a tuple $G = (P, S, U)$, where $P = C \bigcup M$ is the set of players, S is the set of player strategies $S = (S_C^u, S_M)$, $S_C^u = \{A_1, A_2, A_3, R\}, S_M = \{W, R\}$. $U = \{U(c), U(M)\}$ is the set of quantitative utility on each strategy, where $U(u \in C, s \in S_C^u) = U_{w_s} - P_{us}$ denotes the utility customer u acquires after providing the level s of privacy information, U_{w_s} denotes the user benefit by using the wireless w_s. $U(M) = U_{\rho_s} - C_{w_s}$ is the utility of merchant after it obtains user's privacy information of level and w_s is the cost of the provided bandwidth. C_{w_s} denotes the cost which merchant should pay for providing wireless utility w_s to a user.

The game process is as follows:

- Firstly, the merchant asks for a user privacy when this user requires wireless connection.
- The user chooses either to provide the necessary information or to abandon the wireless requirement based on his/her privacy preferences.
- If this user provides enough privacy information, the merchant gives the bandwidth to this user.
- If this user next time requires this wireless connection, he/she and merchant will begin the subsequent game.

There are two key points in this model. One is how to quantify the merchant utility and user privacy preference. With the different strategy of users and merchant, the utility matrix can be derived as TABLE I.

Another is how to find the Nash Equilibrium, namely the optimal strategy combination. Nash Equilibrium[5],[6] is a solution concept of a non-cooperative game involving two or more players, in which each player is assumed to know the equilibrium strategies of the other players, and no player would gain more by changing his/her own strategy. We will discuss how to find the Nash Equilibrium in the following sections.

IV. Nash Equilibrium Analysis

In this section, we analyze the Nash Equilibrium in different situations, the first-round game and subsequent game.

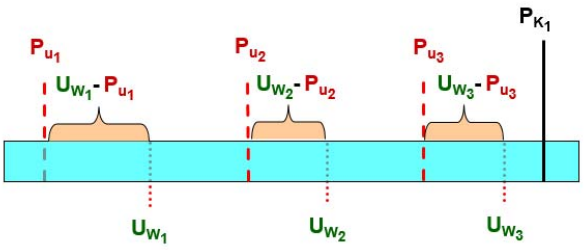


Fig. 1: Nash Equilibrium Analysis

A. The First-Round Game

The first-round game refers to the case where users access wireless for the first time. We firstly analyze one customer game. The following theorem determines all Nash Equilibrium in the first game for a specific user.

Theorem 1 For a specific user u whose privacy preferences $\{p_{u1}, p_{u2}, p_{u3}\}$ are given, there is a single pure strategy Nash Equilibrium in his/her first game with the merchant:

$$S_C^u, S_M = \begin{cases} (A_1, W_1) & U_{w_1} - P_{u1} = max \\ & \{U_{w_1} - P_{u1}, U_{w_2} - P_{u2}, U_{w_3} - P_{u3}\} \\ & \cap U_{w_1} > P_{u1} \\ (A_2, W_2) & U_{w_2} - P_{u2} = max \\ & \{U_{w_1} - P_{u1}, U_{w_2} - P_{u2}, U_{w_3} - P_{u3}\} \\ & \cap U_{w_2} > P_{u2} \\ (A_3, W_3) & U_{w_3} - P_{u3} = max \\ & \{U_{w_1} - P_{u1}, U_{w_2} - P_{u2}, U_{w_3} - P_{u3}\} \\ & \cap U_{w_3} > P_{u3} \\ (R, R) & (U_{w_3} < P_{u1}) \end{cases}$$

Proof: We prove this theorem by the dominated-release method[7], which resides on two sides. Firstly, $U(c)$ and $U(M)$ must be positive. Otherwise, either users or the merchant will change their strategies.

Secondly, we remove the obvious dominated cases. From the aspect of user, according to the definition of privacy sensitivity, $P_{u1} < P_{u2} < P_{u3}$ holds. We first analyze the first column. $U_{w_1} - P_{u1} < U_{w_1} - P_{u2} < U_{w_1} - P_{u3}$ is a tautology. According to the first column of the utility matrix, the first line dominates the other two lines. That is to say, (A_1, W_1) is the dominate choice. Which means, for the same wireless utility, the user would like to provide less privacy information. Similarly, $U_{w_2} - P_{u1} < U_{w_2} - P_{u2} < U_{w_2} - P_{u3}$ and $U_{w_3} - P_{u1} < U_{w_3} - P_{u2} < U_{w_3} - P_{u3}$ also hold. So we have the same conclusions for the other two cases w_2 and w_3.

From the aspect of merchant, according to the definition of wireless cost, $C_{w_1} < C_{w_2} < C_{w_3}$ holds. So $U_{\rho_1} - C_{w_1} > U_{\rho_1} - C_{w_2} > U_{\rho_1} - C_{w_3}$ is a tautology. According to the first column of the utility matrix, the first row dominates the other two lines. That is to say, (A_1, W_1) is the dominate choice, which means, for the same benefit on user information, the merchant would like to provide less wireless utility such as the bandwidth and usage time. Similarly, $U_{\rho_2} - C_{w_1} > U_{\rho_2} - C_{w_2} > U_{\rho_1} - C_{w_3}$ and $U_{\rho_3} - C_{w_1} > U_{\rho_3} - C_{w_2} > U_{\rho_3} - C_{w_3}$ also hold. So we have the same conclusions for the other two rows.

Thirdly, we discuss when the Nash Equilibrium is achieved in different cases. Since users have different privacy preferences and the merchant's wireless cost and utility are not fixed, we need to analyze how these parameters influence the Nash Equilibrium in details. Let's have a look at the merchant first. We say that $U_{\rho_1} - C_{w_1} = U_{\rho_2} - C_{w_2} = U_{\rho_3} - C_{w_3}$ should hold, which is verified by the contradiction. Suppose $U_{\rho_i} - C_{w_i}$ is the smallest one of the three. In practice, a merchant could not know the choices of users in advance. If all users choose this w_i wireless utility, the merchant would benefit less than other menus. This deviates the merchant initial purpose.

Then we discuss user parameter. If $U_{w_1} - P_{u1} = max\{U_{w_1} - P_{u1}, U_{w_2} - P_{u2}, U_{w_3} - P_{u3}\} \cap U_{w_1} > P_{u1}$, choosing the wireless utility w_1 is the best choice since a user can get the highest benefit. This is the first case (A_1, w_1) of the Nash Equilibrium. We show this in the Fig.1. Similarly, we can prove the other two cases (A_2, W_2) and (A_3, W_3). For the third case $(U_{w_3} < P_{u1})$, no matter the user choose strategy A_1 or A_2 or A_3, $U(c)$ is always less than zero. Then, the user rejects giving privacy information and the merchant rejects providing wireless, so that the Nash Equilibrium is (*R*,*R*).

■

B. Subsequent Game

When a user reuses the merchant's wireless, he/she begins a subsequent game. This can be categorized into the following three cases.

Case 1: If users only give level 1 privacy to the merchant at the last round, users should provide level 2 or level 3 privacy to get the wireless. The utilities of both users $U(C_u)$ and the merchant $U(M)$ are shown as TABLE II. To be mentioned here, we only remains the dominate strategy combinations and let w denote all the cases of merchant providing wireless utility.

TABLE II: The Utility Matrix

C \ M	W	R
A_2	$(U_{w_1} - P_{u2}, U_{\rho_2} - C_{w_1})$	$(-P_{u2}, U_{\rho_2})$
A_3	$(U_{w_3} - P_{u3}, U_{\rho_3} - C_{w_3})$	$(-P_{u3}, U_{\rho_3})$
R	$(U_{w_i}, -C_{w_i})\ i \in 1, 2, 3$	$(0, 0)$

Case 2: If the user has provided level 2 privacy to merchant at last round game, the user needs to provide level 3 privacy to get wireless. $U(c)$ and $U(M)$ are shown as TABLE III

Case 3: If users have given level 3 privacy to the merchant in the last round game, users access to bandwidth by providing any level privacy.

TABLE III: The Utility Matrix

C \ M	W	R
A_3	$(U_{w_3} - P_{u3}, U_{\rho 3} - C_{w_3})$	$(-P_{u3}, U_{\rho 3})$
R	$(U_{w_i}, -C_{w_i})\ i \in 1,2,3$	$(0,0)$

Considering the above three cases, if $g_u > g_{max}$, this user becomes a VIP in this shop, and obtains a new Nash Equilibrium. $U(c)$ and $U(M)$ will change as TABLE IV

TABLE IV: The Utility Matrix

C \ M	W
R	$(U_{w_i}, -C_{w_i})$

The new Nash Equilibrium is as follow:

$$S_C^u, S_M = (R, W)(\sum g_u > g_{max}) \tag{1}$$

C. Multi players Game

Now, we will analyze multi players game (C_Z game). C_Z game can be defined as the game which Z players take part in at the same time. Since each player strategy is independent to the group's strategy, so the best response of C_Z game should be get by the sum of individual optimal responses. This Nash Equilibrium can be defined as Z Nash Equilibriums of the single player game:

$$S_C, S_M = \sum_{u=1}^{z} (S_C^u, S_M) \tag{2}$$

D. Discussion

In the above discussion, we argue that $U_{\rho_1} - C_{w_1} = U_{\rho_2} - C_{w_2} = U_{\rho_3} - C_{w_3}$ should hold since a merchant could not know the choices of users in advance. This is applied to the case of initializing a new program, such as providing wireless utility to users. After a period of time, the merchant has collected a large amount of data about user habits, which may include a large number of users and many times usages for each user. So the merchant can adjust his strategies according to user choice distribution. For example, if most users choose the second level of wireless utility by providing level 2 privacy, the merchant can ask for more information for this kind of utility so as to acquire more utility, namely increasing $U_{\rho_2} - C_{w_2}$. This can benefit the merchant more without reducing user benefits.

V. Experimental Analysis

In order to analyze the practical application of the game model, we perform both empirical investigations and quantitative experiments. Aimed at the relevant mobile application and the item of privacy, the questionnaire whereby we obtain necessary data consists of four parts: individual data-age, the frequency of use of wireless application protocol (WAP), tolerance to privacy leakage, the willingness in some certain circumstances. The respondents consist of university students, employees, civil servants and etc., who have professional backgrounds and use mobile phones very frequently. Their native places also gain diversity, for instance, Shandong, Heilongjiang, Hebei, Guangdong, Yunnan, and Tianjin. According to the statistics, we choose the corresponding parameters to perform quantitative experiments on synthesized data. In that way, merchant benefits and users' selection will get to be studied respectively. In order to conveniently perform quantitative experiments, we set that the merchant provides wireless utility W_0, $2W_0$, $3W_0$, if a user gives level $1, 2, 3$ privacy to merchant.

The experiment in this paper functions in Matlab and is executed on a machine with 4G memory, Intel i5 CPU, installed with 64-bit Windows system.

A. User privacy preference and Nash Equilibrium

We first analyze how user privacy preference setting influences the Nash Equilibrium. The parameters are that the total number of customers $C = 40$, the total bandwidth $W = 100$, the online time $T = 1(h)$, utility of privacy information ($U_1 = 1$, $U_2 = 2.2$, $U_3 = 3.6$), which are summarized in TABLE V. Further, We randomly generate 50 pairs of $P_1 < P_2 < P_3$ from $[0, 3]$. Nash Equilibrium is computed according to the method of Section IV. Through the simulation data, customer strategy is broadly in line with the increase of the degree of P_{ui} and affected by bandwidth they get.

B. Utility of privacy information and utility of players

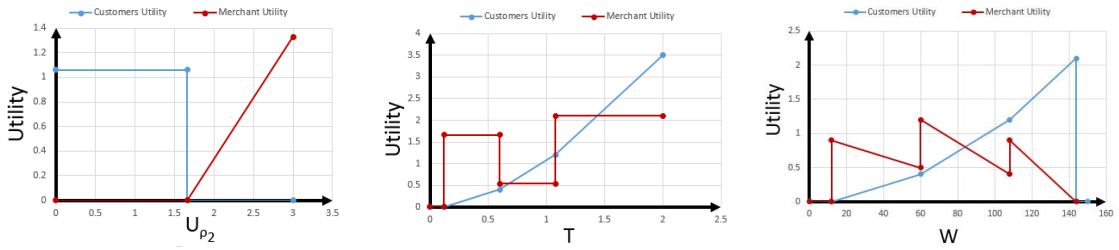
Then we analyze the impact of $U\rho_i$ to the utility of a user and merchant. We set W, T, $P_1 < P_2 < P_3$ fixed as TABLE V. $U\rho_2$ is on behalf of $U\rho_1$, $U\rho_2$, $U\rho_3$. If we choose $U\rho_2$, we consider that the customer gives level 2 privacy to the merchant. In Fig.2, we get that the customer utility $U(c)$ is always 1.06 and merchants utility $U(M)$ is always zero, if $U\rho_2 < 1.66$. If $U\rho_2 > 1.66$, $U(c)$ is zero, but $U(M)$ increases linearly.

TABLE V: Parameter Setting

C	W	T	$U\rho_1$	$U\rho_2$	$U\rho_3$	P_{u1}	P_{u2}	P_{u3}
40	100	1	1	2.2	3.6	0.1	0.6	1.5

C. Online time and players strategy

We consider the impact of T on the user and merchant strategy. Firstly, we set other parameters fixed as TABLE V. Secondly, we change T. The utility of the user and merchant are shown as Fig.2. If $T \in [0, 10/83]$, the user benefit by using the wireless is less than privacy loss, so the customer refuses to give the privacy information, and $U(c)$ and $U(M)$ are zero. If $T \in [10/83, 50/83]$, $T \in (50/83, 90/83]$, or $T \in (50/83, \infty]$, the customer strategy is A_1, A_2, A_3. With T increasing, both $U(c)$ and slope of $U(c)$ will increase. $U(M)$ is a constant value, if T is in the above intervals. So T influences customer strategy which has indirect effects on $U(M)$.



(a)The influence of U_{ρ_2} (b)The influence of T (c)The influence of W

Fig. 2: The utility of customer and merchant

D. The total bandwidth and players utility

Then we consider the impact of W on $U(c)$ and $U(M)$. Firstly, we set other parameters fixed as TABLE V. Secondly, we change W. $U(c)$ and $U(M)$, shown as Fig.2. If $W \in [0, 12]$, $W \in (12, 60]$, $W \in (60, 108]$, or $W \in (108, 144]$, the customer's strategy is R, A_1, A_2, A_3. With W increasing, the customer will give higher level of privacy to the merchant, but $U(M)$ will decrease if W is in the above intervals. If bandwidth is greater than $144M/s$, the merchant will no longer provide bandwidth, because utility of privacy information is less than costs, so the user utility is zero.

VI. Conclusion

In this paper, we introduce a privacy perceptive service model based on game theory, which takes into account the interests of all stakeholders. Considering the characteristics of customer behavior in practice, we design the complete information and sequential game. Users are allowed to provide different levels of personal information as their preferences, while a merchant assigns different wireless bandwidth based on information provided by customers. The Nash Equilibriums is discussed so as to find the acceptable strategy. Quantitative study is performed on the impact of each parameter in the game, which could help merchants to design appropriate policies.

Acknowledgments

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of this paper. This work is supported by the National Natural Science Foundation of China (61173140), the National Science & Technology Pillar Program (2012BAF10B03-3), Special Program on Independent Innovation and Achievements Transformation of Shandong Province (2014ZZCX03301), and Science & Technology Development Program of Shandong Province (2014GGX101046)

References

[1] Giuseppe D'Acquisto, Marta Flamini, and Maurizio Naldi. A Game-Theoretic Formulation of Security Investment Decisions under Ex-ante Regulation. SEC 2012, IFIP AICT 376, pp. 412-423, 2012.

[2] Roughgarden T. Algorithmic game theory[J]. Communications of the ACM, 2010, 53(7): 78-86.

[3] Henry Hazlitt.Economics in One Lesson, 1946 by Harper.

[4] Piero A. Bonatti, Marco Faella, Clemente Galdi and Luigi Sauro. Towards a Mechanism for Incentivating Privacy. In: ESORICS, Vol. 6879Springer (2011), p. 472-488.

[5] Humbert M, Manshaei M H, Freudiger J, et al. Tracking games in mobile networks[M]//Decision and Game Theory for Security. Springer Berlin Heidelberg, 2010: 38-57.

[6] Ken Binmore. Playing for Real: A Text on Game Theory.,2007.

[7] Maskin E. Nash equilibrium and welfare optimality*[J]. The Review of Economic Studies, 1999, 66(1): 23-38.

[8] Slobodkin L B, Rapoport A. An optimal strategy of evolution[J]. Quarterly Review of Biology, 1974: 181-200.

[9] http://www.sojump.com/report/3433757.aspx

[10] Akira Yamada, Tiffany Hyun-Jin Kim, and Adrian Perrig. Exploiting Privacy Policy Conflicts in Online Social Networks. CMU-CyLab-12-005. February 23, 2012

[11] V. Torra, Y. Narukawa, and M. Daumas . Rational Privacy Disclosure in Social Networks.MDAI 2010, LNAI 6408, pp. 255-265, 2010.

[12] J. Grossklags and J. Walrand (Eds.): Incentives and Security in Electricity Distribution Networks.GameSec 2012, LNCS 7638, pp. 264-280, 2012.

[13] J. Grossklags and J. Walrand . Where to Hide the Bits? GameSec 2012, LNCS 7638, pp. 1-17, 2012.

[14] S.U.Das,C.Nita-Rotaru,and M.Kantarcioglu . Optimizing Active Cyber Defense. GameSec 2013, LNCS 8252, pp. 206-225, 2013.

[15] Aron Laszka and Assane Gueye. Quantifying Network Topology Robustness Under Budget Constraints: General Model and Computational Complexity. :GameSec 2013, LNCS 8252, pp. 154-174, 2013.

[16] Aron Laszka, Benjamin Johnson,and Jens Grossklags (Eds.): Mitigation of Targeted and Non-Targeted Covert Attacks as a Timing Game. GameSec 2013, LNCS 8252, pp. 175-191, 2013.

[17] Minkyong,Kim David,Kotz.Periodic properties of user mobility and access-point popularity.Pers Ubiquit Comput (2007) 11:465C479.

[18] Bonatti, P.A., Faella, M., Galdi, C., Sauro, L.: Towards a Mechanism for Incentivizing Privacy. In ESORICS 2012, LNCS, vol. 6879, pp.472C488. Springer, Heidelberg(2012)

[19] $http://en.wikipedia.org/wiki/Game-theory.$

[20] Yuqing Sun,Ninghui Li,Elisa Bertino.:Proactive Defense of Insider Threats through Authorization Management.Copyright 2011 ACM 978-1-4503-0932-5/11/09.