Pricing Privacy Leakage in Location-Based Services

Fenghua Li[1,2], Jiawen Liu[3], Liang Fang[1,4],
Ben Niu[1], Kui Geng[1(✉)], and Hui Li[5]

[1] State Key Laboratory of Information Security,
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{lfh,niuben,gengkui}@iie.ac.cn, Fangliang_iie@163.com
[2] School of Cyber Security, University of Chinese Academy of Sciences,
Beijing, China
[3] Central University of Financial and Economics, Beijing, China
liujiawen11@outlook.com
[4] School of CyberSpace Security,
Beijing University of Posts and Telecommunications, Beijing, China
[5] National Key Laboratory of Integrated Networks Services,
Xidian University, Xi'an, China
lihui@mail.xidian.edu.cn

Abstract. Quantifying location privacy is an interesting and hot topic in Location-Based Services (LBSs). However, existing schemes only consider the privacy leakage to the untrusted LBS servers, leaving out the leakage during the transportation phase. In this paper, we propose a privacy-preserving scheme to help the LBS user to select optimal privacy strategy with considering the aforementioned problem for the first time. In order to measure the efficacy of different kinds of Privacy-Preserving Mechanisms (PPMs) including cryptographic and non-cryptographic types, we first quantify the revenue of two kinds of aforementioned PPMs by considering the privacy loss and privacy leakage probability on the channel and LBS server, as well as the accumulated leakage previously, simultaneously. Then, we take the consumption of different PPMs into account, to compute the investment. Evaluation results illustrate the effectiveness and efficiency of our proposed scheme.

1 Introduction

With the proliferation of mobile devices, Location-Based Services (LBSs) play an increasingly significant role in our daily life and bring us more conveniences. We can utilize smart devices to obtain various applications to enrich our life, such as Google maps, Foursquare, Yelp!, etc. In order to enjoy the convenience provided by the LBS service providers, mobile users have to submit their location data to untrusted servers of LBSs through unreliable channels. During the process, any untrusted parts are capable of inferring mobile users' their private information (e.g., ID, occupation, home address, behavior pattern, interests, etc.) through obtaining these data [5,7,14]. Therefore, we need to pay more attention on it.

L. Ma et al. (Eds.): WASA 2017, LNCS 10251, pp. 406–418, 2017.
DOI: 10.1007/978-3-319-60033-8_36

During the past decade years, a lot of schemes have been proposed to solve such privacy issues in LBSs. Existing works can be classified into two main categories, cryptographic schemes [2] and non-cryptographic based schemes including obfuscation-based mechanisms [3], dummy-based mechanisms [9,11] and anonymization-based mechanisms [18,19]. By utilizing methods above, some systems have been designed to achieve different optimal points in the trade-offs between the service quality or energy consumption and the privacy degree [17]. In the meantime, some researchers aim at quantifying the privacy. For example, Shokri *et al.* proposed a set of measurements to quantify mobile user's privacy in LBSs [16], in web search service [6] and in the database [15], respectively.

However, most of existing schemes leave out three essential problems. Firstly, users' location information has to go through unreliable channels and arrive at an untrusted server. This leads to the risk of information leakage to both eavesdroppers and untrusted server, thus causes severe damage to users. Yet current methods either aim only to protect the information from the untrusted server and ignore the transportation, or guard only against the eavesdroppers. Secondly, the influence of a single leakage is closely related to the accumulated leakage before this single item, while most of existing methods ignore the previous leakage. Thirdly, their quantification methods are incomprehensible for public.

In this paper, we propose a scheme to help mobile users selecting the most appropriate privacy-preserving strategy based on existing PPMs, where service providers are generally untrusted, and the channels are unreliable. Specifically, we price mobile users' privacy leakage, which is used to measure the benefit of each privacy strategy. This leakage is measured from two aspects through an easy-to-understand way: (1) both the leakage during the transportation phase and on the untrusted servers are considered, (2) the previous information leakage is also taken into account. Then, their consumptions are quantified as users' investments. Based on consumption and privacy leakage quantified above, we finally compute the Return on Investment (ROI) for different kinds of PPMs, which can be viewed as the overall evaluation value of each privacy strategy to help user select a proper one.

The contributions of this paper are summarized as follows:

- We borrow the concept of ROI from microeconomics to evaluate the benefits obtained from different kinds of PPMs in LBSs, which is a very suitable concept here in measuring benefits of adopting these PPMs. The benefit is measured by considering several factors, including the privacy benefits and costs of applying different privacy strategies. Additionally, our model can measure different types of PPMs, including the cryptographic approaches and non-cryptographic solutions in a same range.
- Since leaking different location in different phases and conditions will cause different privacy loss, we consider three aspect in privacy loss: (1) the accumulated leakage before every single location activity, (2) the leakage during both the transportation phase and (3) to the untrusted LBS server. This can properly measure the amount of information leaked to adversaries.

– We provide performance analysis of our proposed scheme and demonstrate its effectiveness in balancing the trade-off between privacy and consumptions.

The rest of this paper is organized as follows. Section 2 reviews current related work. Section 3 gives some preliminaries including motivation and basic concepts. Section 4 describes our scheme in detail. Section 5 presents evaluation of our results from experiments. Finally, the conclusion is drawn in Sect. 6.

2 Related Work

2.1 Location Privacy Preserving Systems

Most researchers aime at constructing privacy preserving systems or mechanisms to solve specific issues. They will also define the privacy in their papers, in order to demonstrate the effectiveness of their schemes.

Mechanisms are designed to solve specific problems. Li *et al.* [7] provided a transparent privacy control under different context. They quantified their privacy by assigning different levels to different locations. Niu *et al.* [10] adopted a different protocol in their designed system for uploading and aggregating data anonymously. They prove their guarantees on location privacy in face of side information, using the zero-knowledge. Bindschaedler and Shokri [3] generated synthetic trace to cope with the location inference attacks, where they quantify their privacy as statistical dissimilarity between the synthetic trace and its seed. Zhang *et al.* [19] redesigned the *k-anonymity*, to provide location privacy for privacy-sensitive users and simulated other privacy-indifferent users. Methods above have three problems: (1) their proposed PPMs are designed to solve one certain problem in LBS, which aren't applicable to other problems, (2) their quantification methods were biased in favor of their own PPM, some even assigned subjectively, (3) most of them are designed only against the untrusted or half-trusted server, by assuming the transportation will be safe as long as using the cryptographic methods.

System are designed to solve some comprehensive problems. Fawaz *et al.* [4] analyzed the location access control from more than 400 location-aware apps and proposed an effective location access control tool in the same time maintaining the app's function. Bilogrevic *et al.* [1] constructed a system, firstly predicting the motivation behind users' location sharing through machine learning. Then they construct the relation between the utility and privacy, utility and motivation separately. Finally, they obfuscate the check-in information in a proper degree according to this trade off relation. However, they have a common drawback that only one PPM can be chose in their system, namely, ways to protect the privacy are very limited and their quantification methods are incompletely.

2.2 Quantifying Location Privacy

Shokri *et al.* [16] measured location privacy by formalizing the adversary's performance, considering the prior information available to the attacker, and various

attacks that can be performed. They quantified the privacy as the success probability of adversaries in their location-inference attacks. Gervais *et al.* [6] proposed generic quantitative method for evaluating users' web-search privacy. They used machine-learning algorithms to learn the link-ability between user queries and quantify privacy of users with respect to linkage attacks. Olteanu *et al.* [12] quantified the effect of co-location information on location privacy, considering an adversary who has access to these data. They quantified their location privacy by the expected error of the adversary when performing a localization attack.

Most of the methods above had three defects: (1) their quantification methods are incapable of measuring different types of PPMs in the same dimensions, (2) most of them either do not consider the effect of the previously leakage to current leakage, or leave out the privacy leakage on the transportation, (3) all of their quantification methods are incomprehensible for public.

3 Preliminaries

3.1 Basic Concepts

Location Privacy Strategy (LPS) refers to a particular location PPM with its parameter. In this paper, we use a set $LPS = \{lps_1, lps_2, \cdots\}$ to represent all the PPMs with their parameters, where lps_i is a tuple $\langle ppm_i, \langle para, \cdots \rangle \rangle$, ppm_i indicates a PPM and $\langle para, \cdots \rangle$ indicates ppm_i's parameters configuration. For instance, *k-anonymity* (k=10) mechanism is represented as $lps_1 = \langle k\text{-}anonymity, \langle 10 \rangle \rangle$.

Privacy Leakage Probability refers to the probability the real location information can be reconstructed by an adversary, after this adversary obtained the observed location.

Privacy Loss refers to the amount of users' personal information that can be analyzed and inferred by adversary utilizing this leaked real location.

ROI refers to the ratio of the return to investment. Specifically, the reduction of the privacy risk can be viewed as the return of privacy strategy, and the consumption of adopting that strategy is defined as the investment.

Privacy Leakage refers to the expected privacy loss, which is decided by the privacy loss and privacy leakage probability.

Location Activity refers to a specific event, where user issued a specific query containing a specific location during a certain time period to LBS server. This is formalized in Sect. 3.2.

3.2 User and Adversary

We consider a scenario where users move in an area partitioned into M discrete regions $G = \{g_1, \ldots, g_j, \ldots, g_M\}$. A location activity is represented by $loc_{i,j,l}$, which means user u_i has been the location g_j during time period t_l. The profile of mobile user u_i can be denoted as: $profile_i = \{\langle g_1, n_{i,1} \rangle, \langle g_2, n_{i,2} \rangle, \cdots\}$, where $n_{i,j}$ means the times that user u_i move in region g_j. Apparently, a $\langle g_j, n_{i,j} \rangle$ is composed of several *loc*s.

Generally, the channel is untrusted, adversaries can easily eavesdrop the communication channels and obtain these protected information. As LBS users are sporadic, the knowledge that the adversary can accumulate by continuous eavesdropping is users' issuing probability distribution over different regions. We assume that the LBS servers are untrusted but honest. That is to say the server will follow the protocol to provide service to users using their location information, but may attempt to learn more information than allowed, more specifically, to reconstruct users' integral location profiles.

3.3 Motivation

Figure 1 illustrates the general architecture and processes of current LBSs. To enjoy the convenience provided by LBS applications, mobile user *Alice* needs to pay electricity fee to keep her smartphone alive and another part of money for her data plan to suffer the internet. She really wonders these costs can be worthwhile for enjoying the service while protecting her privacy. However, existing metrics in privacy protection is obscure. It is necessary to make it be easy-to-understanding by public. Since money is always considered as a directly way to represent the benefit, it makes sense to introduce ROI into our measurement. On the other hand, quantification methods always emphasizing on some specific topics, such as privacy preservation to the untrusted LBS server, and ignore the privacy leakage on the transportation phase. Therefore, it is interesting and meaningful to design a comprehensive model to measure user's privacy. As shown in Fig. 1, within *Alice*'s phone (the left dotted rectangle), different PPMs brings various resource consumptions, which mean the cost that we need to pay for our privacy protection, it plays an important role in deciding whether this PPM is economical. Out of her phone (the right dotted rectangle), *Alice* suffers from two unsafe points, the untrusted LBS servers and the unreliable communication channels. The key problem in such two points is to price the privacy leakage, which is vital to compute privacy leakage revenue after adopting a specific PPM. Therefore, we need to comprehensively study the privacy loss and the privacy leakage probability over different phase.

Generally, the privacy leakage probability varies in different phases and PPMs. If users adopt *k-anonymity* [8] to protect their locations, these will be leaked to the eavesdropper and the untrusted LBS server in same probability. However, if users adopt an cryptographic method such as RSA algorithm to

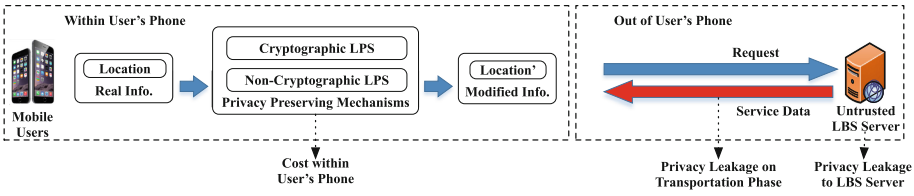


Fig. 1. Our motivation

encrypt their locations, the probabilities for the eavesdroppers and untrusted servers to guess the real locations are obviously different.

It is also hard to measure the privacy loss, because it is affected by different phases and different amount of previous leakage (i.e., adversary's knowledge). To be specific, if adversaries already get 8 *loc*s of a particular user, they might not know a lot of this person. However, if adversaries can get the 9th *loc*, they may re-identify this user in a very high probability. Apparently, the 9th *loc* can obviously cause larger privacy loss than previous 8 *loc*s. In other words, adversaries can re-identify user to different extent by combining different previous leaked information with current information.

3.4 Our Basic Idea

Based on observation above, concept of ROI is borrowed from microeconomics to design a metric reflecting the profits brought by different privacy strategies. The key problem is to formalize the ROI in a proper manner to measure the PPMs of cryptographic and non-cryptographic privacy-preserving schemes in a same range. We price the return after applying a specific location privacy strategy, as well as the investment. Then the ratio of the return to the investment can clearly represent the ROI of this strategy. Finally, the location privacy strategy with the highest ROI is our recommended strategy. When our metrics are used, users only need to input there current location and we can automatically output the most suitable privacy strategy to them.

4 Our Proposed Scheme

4.1 System Overview

Figure 2 shows the structure of our scheme, and illustrates how to compute the ROI of a specific location privacy strategy *lps* for a certain location activity $loc_{i,j,l}$. The steps are summarized as follows:

(i) In Sect. 4.2, we quantify the privacy leakage probability as $Pr(lps_i)_{trans}$ and $Pr(lps_i)_{server}$ separately for every $lps_i \in LPS$. Note that these probabilities are only related to the LPSs.

(ii) Next, in Sect. 4.2, we formalize the privacy loss in the two phases separately for different location activity as $loss(loc_{i,j,l})_{server}$ and $loss(loc_{i,j,l})_{trans}$. These are related to different location activity and different previous leakage, and have to be calculated every time.

(iii) Utilizing the leakage probabilities and the privacy losses in two phases, we calculate the *return* of applying a specific *lps* in the third part of the Sect. 4.2. The $Pr(lps_i)_{trans}$ and $loss(loc_{i,j,l})_{trans}$ are used to compute the privacy leakage in transportation, and $Pr(lps_i)_{server}$ and $loss(loc_{i,j,l})_{server}$ are used to compute the privacy leakage in LBS server. Then, the change of the total privacy leakage before and after the adoption of lps_i is *return*.

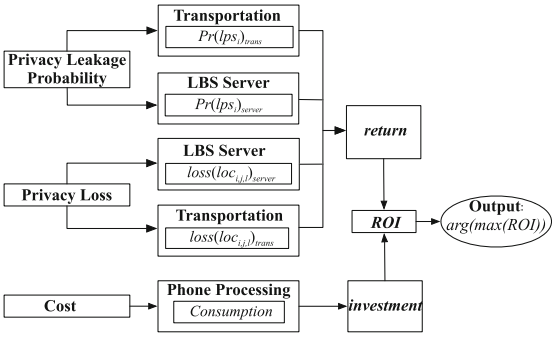


Fig. 2. Scheme overview

(iv) Then the resource consumptions of every *lps* are monitored in advance, which is used to compute the investment of the adoption of LPS in Sect. 4.3.
(v) Based on the the *return* and *investment* above, the ROI is calculated to measure the profit rate of every *lps* in Sect. 4.4. We finally output the best strategy for mobile users.

4.2 Return

In this section, firstly, we define the leakage probability as Pr. This measures the probability of leaking the location information to the attacker. Then we define the privacy loss as $loss$, to measure the amount of privacy loss after the real location information being leaked to adversaries. Finally, we design leakage ($leakage$) as expectation loss to measure privacy loss in the whole LBS process.

$$leakage = \sum Pr * loss.$$

Intuitively, after applying a specific LPS, information leakage will reduce. So, we define the amount of this leakage decreased after protection as the $return$:

$$return = \Delta leakage = leakage_{before} - leakage_{after},$$

where triangle symbol is used for difference, $leakage_{before}$ and $leakage_{after}$ means the $leakage$ before and after applying the privacy strategy.

Privacy Leakage Probability (Pr). We assume a strong attacker has the ability to obtain the modified message. Then leakage probability is the probability that the attacker can successfully reconstruct the real location from the modified location. This is based only on different LPSs, as well as different phases.

Cryptographic LPSs: We use subset $LPS_{en} \subsetneqq LPS$ to represent the cryptographic LPSs.

In the phase of transportation, attackers can get the encrypted location. He needs to reconstruct the private key in order to reconstruct the real location.

We use the probability of successfully reconstruct the private key to define the leakage probability of LPS_{en}. This is detailed as follows. The LPS_{en} can be divided into two categories, the 1st is the LPSs that generalized their extraction of root into the intractability of factoring large numbers and the 2nd is these that generalized their attack process into intractability of extracting discrete logarithms (EDL) over finite groups. The way to solve and reconstruct the plaintext is to factor the large number (FLN), whose complexity is $\sqrt{large\ number}$, and extract discrete logarithms (EDL) over finite groups whose complexity is $para_i$. Since the probability of reconstructing the private key is nearly to zero, we define there leakage probability as: $Pr(lps_i)_{trans} = 0$.

In the phase of LBS server, since untrusted servers have the corresponding private key to decrypt, the probability of reconstructing the real location is apparently 1. Namely, $Pr(lps_i)_{server} = 1$, $lps_i \in LPS_{en}$. Moreover, some cryptographic LPSs are homomorphic, the leakage probability here will be the same as the transportation, namely the $Pr(lps_i)_{server} = Pr(lps_i)_{trans}$.

Non-cryptographic LPSs: We use subset $LPS_{non-en} \subsetneqq LPS$ to represent the non-cryptographic LPSs in LBS including the dummy, obfuscation and anonymization. Because the untrusted server also has no way to figure out the real location from the modified location information, these LPSs have the same effect in the phase of transportation and LBS server. This means they have the same leakage probability in the two phases. Taking the *k-anonymity* to illustrate, with parameter $para_i = k$, we can have $Pr(\langle k\text{-}anonymity, k\rangle)_{trans} = Pr(\langle k\text{-}anonymity, k\rangle)_{server} = \frac{1}{k}$.

Privacy Loss (*loss*). We use location profiles defined in Sect. 3.2 composed of several location activity (*loc*) to represent users' privacy. Obviously, a single leakage to adversary can be harmless, while accumulated leakage can cause severe damage. When adversary has already obtained some *loc*s of a user, the leakage of the next *loc* may cause larger privacy loss than previous. That is to say, different *loc*s leaked in different phases under different adversary knowledges can cause different privacy losses. As a result, we first define the total loss $LOSS$, then the loss of a single location activity $loc_{i,j,l}$ can be calculated as:

$$loss(loc_{i,j,l}) = \Delta LOSS. \tag{1}$$

It means the difference of the total loss before and after leaking $loc_{i,j,l}$ to attacker.

From Sect. 3.1, we can learn that $LOSS$ is the amount of privacy leakage when all accurate location has been revealed to adversary. To be more secure we assume a strong adversary that the real location activities are revealed as long as been eavesdropped. Then, there will be a user's profile $profile'_i$ collected by the adversary: $profile'_i = \{\langle g_1, n'_{i,1}\rangle, \langle g_2, n'_{i,2}\rangle, \cdots\}$.

Then, we can use similarity between the user u_i's $profile'_i$ obtained by the adversary and his/her original profile $profile_i$ to represent the total loss $LOSS$:

$$LOSS(profile'_i) = \sum_j \frac{n_{i,j}}{\sum_j n_{i,j}} * sim(\langle g_j, n_{i,j}\rangle, \langle g_j, n'_{i,j}\rangle). \tag{2}$$

To be more accurately, considering the time effect, we can divide the tuple $\langle g_j, n_{i,j} \rangle$ by time periods. Then we will have a time sequence for every location: $\langle g_j, n_{i,j} \rangle = \langle (t_1, n_{i,j,1}), (t_2, n_{i,j,2}), \cdots \rangle$ where $(t_l, n_{i,j,l})$ is the number of $loc_{i,j,l}$ in a certain time periods t_l. In the same way, the adversary can also construct a similar time sequence for every eavesdropped location: $\langle g_j, n'_{i,j} \rangle = \langle (t_1, n'_{i,j,1}), (t_2, n'_{i,j,2}), \cdots \rangle$. We can calculate their similarity by the adjusted cosine similarity as:

$$\frac{\sum_l (n'_{i,j,l} - \overline{n'_{i,j}})(n_{i,j,l} - \overline{n_{i,j}})}{\sqrt{\sum_l (n'_{i,j,l} - \overline{n'_{i,j}})^2} + \sqrt{\sum_l (n_{i,j,l} - \overline{n'_{i,j}})^2}}. \tag{3}$$

Then, using the total loss before and after leaking a specific location activity $loc_{i,j,l}$, we can calculate the privacy loss of a single leakage as:

$$loss(loc_{i,j,l}) = LOSS(profile'_i + loc_{i,j,l}) - LOSS(profile'_i),$$

where $profile'_i + g_j$ is the $profile'_i$ after the g_j leaked to adversary.

Return. After adopting a specific LPS lps_i to protect a specific location g_i, we can firstly calculate the *leakage*:

$$leakage(lps_i, loc_{i,j,l}) = \sum_{tans,server} Pr(lps_i) * loss(loc_{i,j,l}).$$

Apparently, before adopting the lps_i, the leakage of getting the LBS using the unprotected location g_i is:

$$leakage(\cdot, loc_{i,j,l}) = \sum_{tans,server} Pr(\cdot) * loss(loc_{i,j,l}).$$

where the leakage probability of an unprotected location is 1, namely $Pr(\cdot) = 1$.

Then the return denoted as $return(lps_i, loc_{i,j,l})$ means using this lps_i to protect the location activity $loc_{i,j,l}$ can easily be calculated as:

$$leakage(\cdot, loc_{i,j,l}) - leakage(lps_i, loc_{i,j,l}).$$

4.3 Investment

There will be different cost when applying different LPSs with different parameter configuration. Their costs can justifiably be viewed as investments, including the power consumption $E(lps_i)$ (energy) and data consumption $D(lps_i)$. Then converting these consumptions into money by multiple their tariff, we can define investment as the sum of all these cost:

$$investment(lps_i, loc_{i,j,l}) = E + D.$$

4.4 ROI

Using the return and investment calculated above, ROI is calculated as:

$$ROI(lps_i, loc_{i,j,l}) = \frac{return(lps_i, loc_{i,j,l})}{investment(lps_i, loc_{i,j,l})}.$$

This concept can easily be understood by anyone who even know nothing about privacy protection. People can learn about why they must use these PPMs to protect their location and what they can obtain by using these PPMs.

5 Performance Evaluations

5.1 Setup

Profile Generation. Users' real profiles that we use belong to 100 randomly chosen mobile users from dataset [13]. Each $profile_i$ contains the issuing times within different locations of a user every 120 min for 8 h. The area within which the user move is divided into 40 regions forming a 5×8 grid. In order to have a strongest adversary, we feed the adversary with users' accurate history location.

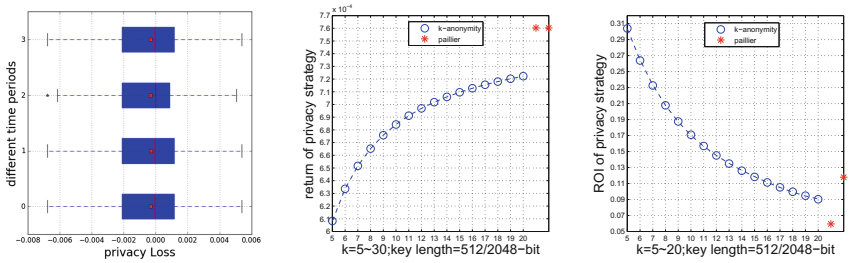
Table 1. User's original profile and profile observed by adversary

	$Profile_i$				$Profile'_i$			
Time period	t_1	t_2	$\cdots$	t_4	t_1	t_2	$\cdots$	t_4
g_1	18	16	$\cdots$	10	16	2	$\cdots$	1
g_2	10	7	$\cdots$	7	6	2	$\cdots$	0
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g_{40}	18	25	16	23	4	19	12	5

Privacy Loss Measurement. Figure 3(a) showed the privacy loss of different location in our the time periods.

In our instance, we randomly chose a location activity (g_3, t_2) as user's current activity and computed its privacy loss. This event is represented as $loc_{i,3,2}$. The profile observed by the eavesdropper is constructed in Table 1, denoted as $profile'_{i,ea}$, and observed by the server is denoted as $profile'_{i,se}$. $LOSS_{before,ea} = 0.41463$, $LOSS_{after,ea} = 0.415038$, $LOSS_{before,se} = 0.99964766$, $LOSS_{before,se} = 1$. Then we can have the loss of $loc_{i,3,2}$ on the transportation as: $loss(loc_{i,3,2})_{trans} = 0.000408$, and loss on the server $loss(loc_{i,3,2})_{server} = 0.0003523$.

Return. We use the *k-anonymity* with parameter $k = 5 \sim 20$ [8] to instance the non-cryptographic LPSs and the paillier [2] with key_length = 2048-bit and 512-bit to instance the cryptographic LPSs. *return*s of the two LPSs under different parameters are showed in Fig. 3(b). The red points represent *return* of paillier under 512-bit and 2048-bit key_length. Red points have nearly the same value.



(a) privacy loss of different location (b) *return* of privacy strategies (c) *ROI* of privacy strategies

Fig. 3. *Return* and *ROI* and *privacy loss* of *k-anonymity* and paillier with their parameters (Color figure online)

ROI. Under 'WiFi', the original data is 2KB, we monitored the energy consumption and data consumption of the *k-anonymity* with the parameter $k = 5 \sim 20$ and the paillier with key_length = 2048-bit and 512-bit. We collected ten groups of data for 1000 times and average them, showed in Table 2. Using these consumptions, we compute their investments under current fee standards as: $investment(lps_i, loc_{i,j,l}) = E * 5.88 * 10^{-7} + D * 2 * 10^{-4} = 2.005 * 10^{-3}$. Finally the ROI is computed as: $ROI(\langle k - anonymity, 10\rangle, loc_{i,3,2}) = \frac{return(\langle k-anonymity,10\rangle,loc_{i,3,2})}{investment(lps_i,loc_{i,j,l})} = 0.314$. The rest of ROIs are presented in Fig. 3(c). The first red point in Fig. 3(c) is the ROI of paillier under key_length = 512-bit, the second one is under key_length = 2048-bit.

Table 2. Consumption of privacy strategies

	k-anonymity (para = k)					*Paillier (para = key_length)*	
Parameter value	5	6	7	···	20	512-bit	2048-bit
D **(in *mAh*)**	1.83	1.84	3.72	···	3.64	7.42	81.86
E **(in *KB*)**	10	12	14	···	40	64	32

5.2 Results

The result tallied with the fact that $k - anonymity$ with $k = 5$ has the highest ROI. From the ROIs of different privacy strategies above, we can draw some conclusions. Even though some LPSs (such as paillier) have the overwhelm advantage over others (such as *k-anonymity*) intuitively, yet their ROIs are not necessary higher. This is resulted from our consideration of both the privacy leakage on the transportation and LBS servers, as well as the consumption in our scheme.

6 Conclusions

In this paper, we priced mobile user's privacy with our proposed Return on Investment (ROI), which is a new and easily-to-understand definition in LBSs. We considered two possible ways to reveal user's privacy, including the privacy loss during the transportation phase and to the untrusted LBS servers. We also quantified the LBS user's consumption within the smart phone. Based on these information, we inferred and formalized the ROI. The evaluation results showed that our newly-defined ROI can effectively measure different kinds of PPMs in the same range.

Acknowledgement. This work was supported by the General Program of National Natural Science Foundation of China (61672515), the National Key Research and Development Program of China (2016YFB0800303) and the National Natural Science Foundation of China (61502489).

References

1. Bilogrevic, I., Huguenin, K., Mihaila, S., Shokri, R., Hubaux, J.P.: Predicting users' motivations behind location check-ins and utility implications of privacy protection mechanisms. In: Proceedings of ISOC NDSS (2015)
2. Bilogrevic, I., Jadliwala, M., Kalkan, K., Hubaux, J.-P., Aad, I.: Privacy in mobile computing for location-sharing-based services. In: Fischer-Hübner, S., Hopper, N. (eds.) PETS 2011. LNCS, vol. 6794, pp. 77–96. Springer, Heidelberg (2011). doi:10.1007/978-3-642-22263-4_5
3. Bindschaedler, V., Shokri, R.: Synthesizing plausible privacy-preserving location traces. In: Proceedings of IEEE S&P (2016)
4. Fawaz, K., Feng, H., Shin, K.G.: Anatomization and protection of mobile apps' location privacy threats. In: Proceedings of USENIX Association USENIX Security (2015)
5. Fechner, T., Kray, C.: Attacking location privacy: exploring human strategies. In: Proceedings of ACM UbiComp (2012)
6. Gervais, A., Shokri, R., Singla, A., Capkun, S., Lenders, V.: Quantifying web-search privacy. In: Proceedings of ACM CCS (2014)
7. Li, H., Zhu, H., Du, S., Liang, X., Shen, X.: Privacy leakage of location sharing in mobile social networks: attacks and defense. IEEE Trans. Dependable Secure Comput. (2016)
8. Niu, B., Li, Q., Zhu, X., Cao, G., Li, H.: Achieving k-anonymity in privacy-aware location-based services. In: Proceedings of IEEE INFOCOM (2014)
9. Niu, B., Li, Q., Zhu, X., Cao, G., Li, H.: Enhancing privacy through caching in location-based services. In: Proceedings of IEEE INFOCOM (2015)
10. Niu, B., Zhu, X., Lei, X., Zhang, W., Li, H.: Eps: encounter-based privacy-preserving scheme for location-based services. In: Proceedings of IEEE Globecom (2013)
11. Niu, B., Zhu, X., Li, W., Li, H.: Epcloak: an efficient and privacy-preserving spatial cloaking scheme for lbss. In: Proceedings of IEEE MASS (2014)
12. Olteanu, A.M., Huguenin, K., Shokri, R., Humbert, M., Hubaux, J.P.: Quantifying interdependent privacy risks with location data. IEEE Trans. Mob. Comput. **10**(1109), 1536–1233 (2016)

13. Piorkowski, M., Sarafijanovoc-Djukic, N., Grossglauser, M.: A parsimonious model of mobile partitioned networks with clustering. In: Proceedings of COMSNETS (2009). http://www.comsnets.org
14. Rizoiu, M.A., Xie, L., Caetano, T., Cebrian, M.: Evolution of privacy loss in wikipedia. In: Proceedings of ACM WSDM (2015)
15. Sankar, L., Rajagopalan, S.R., Poor, H.V.: Utility-privacy tradeoffs in databases: an information-theoretic approach. IEEE Trans. Inf. Forensics Secur. **8**(6), 838–852 (2013)
16. Shokri, R., Theodorakopoulos, G., Boudec, J.Y.L., Hubaux, J.P.: Quantifying location privacy. In: Proceedings of IEEE S&P (2011)
17. Shokri, R., Theodorakopoulos, G., Troncoso, C., Hubaux, J.P., Le Boudec, J.Y.: Protecting location privacy: optimal strategy against localization attacks. In: Proceedings of IEEE CCS (2012)
18. Zhang, S., Yang, H., Singh, L.: Anonymizing query logs by differential privacy. In: Proceedings ACM SIGIR (2016)
19. Zhang, Y., Tong, W., Zhong, S.: On designing satisfaction-ratio-aware truthful incentive mechanisms for k-anonymity location privacy. IEEE Trans. Inf. Forensics Secur. **11**(11), 2528–2541 (2016)