Enhancing the Trajectory Privacy with Laplace Mechanism

Daiyong Quan ,Lihua Yin,Yunchuan Guo
Institute of Information Engineering, Chinese Academy of Sciences
Beijing, China
e-mail:{quandaiyong,yinlihua,guoyunchuan} @iie.ac.cn

***Abstract*—Mobile-aware service systems are dramatically increasing the amount of personal data released to service providers as well as to third parties. Data may reveal individuals' physical conditions, habits, and sensitive information. It raises serious privacy concerns. Current approaches to mitigate the privacy concerns rely on the randomization. However, it is difficult to guarantee privacy levels with random noise. In this paper, we propose a data obfuscation mechanism based on the generalized version of the notion of differential privacy. We extend the standard definition to the settings where the inputs belong to an arbitrary domain of secrets. Then we enhance the mobility signature privacy with our mechanism. By adopting the expected distance as an indicator to measure the service quality loss, we compare our mechanism with the (k,δ)-anonymity random method. On the real dataset, the results reveal that our mechanism adds less noise under the same privacy guarantee.**

Keywords- obfuscation mechanism; differential privacy; mobile-aware service systems; trajectory privacy protection

I. INTRODUCTION

Currently, mobile-aware service systems are dramatically increasing the amount of personal data released to service providers as well as to third parties. Examples of these apps are location and context-aware tourist apps, navigation apps, proximity based recommendation and advertisement apps. More and more users are also appreciating the ability to share location data in terms of check-in based mechanisms (like Foursquare or Facebook Places) or even through continuous location reporting (e.g., fleet management, friend-finders, co-operative navigation). The association of a user with a specific location at a given time can reveal health problems, affiliations, habits, etc. The availability of locations in real time as well as the historical data about user movements even introduces threats such as assault. For example, the notorious case is the young girl in Shenzhen China was killed because of the location information disclosure. GeoSNs exacerbate the risks, as the spread of location information occurs more easily and is less controllable.

However, the ever-increasing usage of these personal communication devices and mobile applications, although providing convenience to their owners, comes at a very high cost to their privacy. Interacting with location-based services (LBSs) leaves an almost indelible digital trace of users' whereabouts. Moreover, the contextual information attached to these traces can reveal users' personal habits, interests, activities, and relationships. Consequently, exposure of this private information to third parties escalates their power on individuals, and opens the door to various misuses of users' personal data. We have the right, and should also have the means to control the amount of their private information that is disclosed to others. Current approaches to mitigate the privacy concerns rely on the randomization. However, it is difficult to guarantee privacy levels with random noise. Data obfuscating is a prevalent approach to protecting users' privacy in mobile-aware service systems where a user shares her data (e.g., location) to obtain a personalized (e.g., location-based) service. Data obfuscation is a mechanism for hiding private data in misleading, false, or ambiguous information with the intention of confusing an adversary [1]. A data obfuscation mechanism, whether implemented as input or output perturbation [3][4], can be modeled as an information channel between a user's private data (secret) to an observer that receives the obfuscated information.

To guarantee a non-negligible level of privacy, the random value cannot be generated naively. It is urgent need to obfuscate the data with controllable noise. In this paper, we extend the definition of standard differential privacy to the settings where the inputs are not databases at all, but belong to an arbitrary domain of secrets. Then we protect the mobility pattern privacy with our mechanism by adding Laplace random noise. By adopting the expected distance as an indicator to measure the service quality loss, we compare our mechanism with the (k,δ)-anonymity random method. On the real dataset, the results reveal that our mechanism adds less noise under the same privacy guarantee.

The contributions of this paper are threefold:

- We extend the standard definition to the settings where the inputs belong to an arbitrary domain of secrets. Based on the extended definition, we can manipulate the amplitude of the noise by adjusting the privacy parameters.
- We obfuscate the longitude data by our Laplace Mechanism. In the settings of strong privacy required, the privacy parameter is small (eps=0.1), and we add more noise; in the settings of weak privacy guarantee required, the privacy parameter is large (eps=1.9), and we add less noise; while there is no privacy preference, we release the raw data without noise.
- We evaluate our mechanism by adopting the expected distance as an indicator to measure the service quality loss. Moreover, we compare our mechanism with the (k,δ)-anonymity (k=10). On the real dataset, the results reveal that our mechanism adds less noise under the same privacy guarantee.

978-1-4673-7952-6/15 $31.00 © 2015 IEEE
DOI 10.1109/Trustcom.2015.508

The rest of this paper is organized as follows. In Section II, we describe our definitions, notations, and assumptions. The proposed obfuscation mechanism is described in Section III. Section IV is the experiment of our proposed approach on the real dataset. Section V presents the related work. Finally, Section VI provides our concluding remarks.

II. OBFUSCATION MECHANISM FOR MOBILE-AWARE SERVICE SYSTEMS

In this section, we present a model served as the basis for exploring the relation between the real value and the obfuscated one. Then we state definitions of our obfuscation mechanism.

A. Assumptions

We assume users exposing their data through a service system in order to obtain some service (utility) based on their shared data. We also assume that users want to protect their sensitive information, while they share their data with untrusted entities. For example, in the case of sharing location-tagged data with a service provider, a user might want to hide the exact visited locations, their semantics, or the activities that can be inferred from the visited locations. We refer to the user's sensitive information as the secret. To protect the user privacy, we assume that user obfuscates her data before sharing or publishing it. Fig. 1 illustrates the information flow that we assume in this paper.

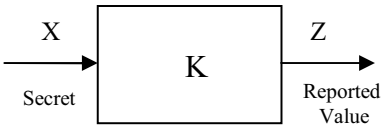

Figure 1. Obfuscation mechanism K

Let K be a randomized function from X to Z. The obfuscation mechanism is a probabilistic function $K : X \to P(X)$, where X is the set of possible secrets, and $P(X)$ denotes the set of probability distributions over X. K takes a secret x as input, and produces a reported z which is communicated to the service provider. We denote this as $K(z|x)$. From the perspective of quantitative information flow, a channel with input x and output z can model the obfuscation mechanism.

The input to the protection mechanism is a secret $x \in X$, where X is the set of all possible values that x can take. The output, the set of Z, can in general be a member of the power set of X. In a more generic case, the members of Z can also contain a subset of secrets. For example, the protection mechanism can generalize the secret, by reducing its granularity.

B. Definitions

Differential Privacy is a notion of privacy from the area of statistical databases. Its goal is to protect an individual's data while publishing aggregate information about the database. According to the original definition of differential privacy[11],a randomized function K (that acts as the privacy protection mechanism) provides -differential privacy if for all data sets D and D', that differ on at most one element, and all $Y \subseteq$Range(K), the following inequality holds:

$$\Pr\{K(D) \in Y\} \le e^{\varepsilon} \cdot \Pr\{K(D') \in Y\} \quad (1)$$

where is a privacy parameter, known as a privacy budget.

Differential privacy is not limited to statistical databases. Many works consider differential privacy in various settings where various types of adjacency relations capture the context dependent privacy. It has also been proposed for arbitrary secrets [25].

We state our definition of secret-indistinguishability. Intuitively, a privacy requirement is a constraint on the distributions $K(x)$, $K(x')$ produced by two different secrets x,x'. Let $d(\cdot,\cdot)$ denote the arbitrary distance function on the secrets. It could be a semantic distance between different values of secrets and $d(x,x')$ represents the distinguishable level of the two secrets. Similarly, $d(x,z)$ reflects the privacy risk of z on user when her secret is x. The highest risk is usually associated with the case when the estimated z is equal to the secret x, i.e. $d(x,z)=0$ .The shorter, the harder to distinguish them. According to this idea, two different probability distributions can also be represented by the distance function. For example, let (ε,d) -privacy be that for any x,x',s.t. $d(x,x') \le d$, the distance $d(K(x),K(x'))$ between the corresponding distributions should be at most $\varepsilon \cdot d$. Then, requiring ·d-privacy for all secrets within the scope of d force the two distributions to be indistinguishable, while beyond the scope, allowing the service providers to distinguish the secrets.

DEFINITION 2.1 (d_x -privacy) A protection mechanism K satisfies d_x -privacy if for all $x,x' \in X$, with distance $d(x,x')$ and for all reported $z \in Z$, the following inequality holds:

$$K(z|x) \le e^{\varepsilon \cdot d(x,x')} \cdot K(z|x') \quad (2)$$

Intuitively, the definition requires that secrets close to each other with respect to d_x should produce outcomes with similar probability. In fact, d_x -privacy is an instance of a generalized variant of differential privacy, using an arbitrary metric between secrets. The differential privacy metric guarantees that, given the observation, there is not enough convincing evidence to prefer one secret to other similar ones (given d). The definition of differential privacy (CF. equation (1)) can be directly expressed as a property of the channel: it satisfies -differential privacy iff

$$K(z|x) \le e^{\varepsilon \cdot 1} \cdot K(z|x') \text{ for all } z \in Z, x, x' \in X, \text{and } d(x,x') = 1$$

According to the Definition 2.1, an extended metric (allowing $d_x(x,x') = \infty$) can be useful in cases when we allow two secrets to be completely distinguished. Similarly, an extended metric (allowing $d_x(x,x') = 0 \ for \ x \neq x'$) could be meaningful when we want some secrets to be completely indistinguishable.

DEFINITION 2.2 Given a metric d on X, the expected distortion between the real value x and the reported value z is:

$$dis(K,d) = \sum_{x,z} K(z|x) \cdot d(x,z) \quad (3)$$

DEFINITION 2.3 Quality Loss. From the user's point of view, we want to quantify the quality of service (utility) produced by the mechanism *K*. Given a quality metric d on secrets, such that $d_{dis}(x,z)$ measures how much the quality decreases by reporting z when the real secret is x, we can naturally define the quality loss as the expected distortion between the real and the reported secrets.

$$QL(K,d) = dis(K,d) \quad (4)$$

The QL can also be viewed as the (inverse of the) utility of the mechanism.

III. OUR PROPOSED MECHANISM

In this section we present a method to generate noise to satisfy d_x -privacy. We apply our generalized notion of differential privacy, instantiated with the Euclidean metric, to the trajectory privacy protection. Specifically, we need to address two stumbling blocks: How much noise is added and how to extract the noise randomly.

A. Laplace Mechanism

The essential property of d_x -privacy is that whenever the actual secret is x, we report an obfuscated value z generated randomly according to the obfuscating function. The latter needs to be such that the probabilities of reporting a secret in a certain space around z, when the actual secrets are x,x' respectively, differs at most by a multiplicative factor $e^{-\varepsilon \cdot d(x,x')}$. We can achieve this property by requiring that the probability of generating a secret in the space around x decreases exponentially with the distance from the actual secret x. In a linear space this is exactly the behavior of the Laplace distribution, whose probability density function (pdf) is $\varepsilon/2 \cdot e^{(-\varepsilon|x-\mu|)}$. Equivalently, the multivariate Laplacian is obtained from the standard Laplacian by replacing |x-μ| with d(x,μ), i.e. $\varepsilon/2 \cdot e^{(-\varepsilon \cdot d(x,\mu))}$.

Let X, Z be two sets, and let d_x be a metric on $X \cup Z$. Let $\lambda : Z \to [0,\infty)$ be a scaling function such that $D(z|x) = \lambda(z) \cdot e^{(-d_x(x,z))}$ is a probability density function for all $x \in X$ (implying that $\int D(z|x)dz = 1$).Then the mechanism $K(z|x)$ described by the pdf $D(z|x)$, is called a Laplace mechanism from (X, d_x) to *Z*. According the Definition 2.1, any Laplace mechanism from (X, d_x) to *Z* satisfies d_x -privacy. Note that in the framework of d_x -privacy, we can express the privacy of the mechanism itself, on its own domain, without the need to consider a query or a notion of sensitivity, thus obtaining a simple and elegant presentation. There is a neat proof [25] that shows that by adding a random Laplace, d-differential privacy is guaranteed.

By properly adjusting λ(z), we can provide instantiations of the general definition for various choices of(X,Z) and d_x. In fact, for each choice of the metric d_x (such as we adopt the Euclidean distance in the next subsection), we define a family of mechanisms, one for each scaled version εd_x, so the scaling function will depend on ε.

TABLE I. LAPLACE TYPE MECHANISM

Setting #	Table Column Head		
	X	***Z***	$\lambda_\varepsilon(z)$
one-dimensional continuous	$\mathbb{R}$	$\mathbb{R}$	$\varepsilon/2$
two-dimensional continuous[a]	$\mathbb{R}^2$	$\mathbb{R}^2$	$\varepsilon^2/2\pi$

a. Measuring the distance between points using the Euclidean metric

B. Drawing Laplace Noise

We adopt the way to draw Laplace noise proposed in literature [9], given the parameter $\varepsilon \in \mathbb{R}^+$, and the real value $x \in \mathbb{R}^2$, the pdf of our noise mechanism, on any reported value $z \in \mathbb{R}^2$, is:

$$D_\varepsilon(z|x) = \frac{\varepsilon^2}{2\pi} e^{-\varepsilon d(x,z)} \quad (5)$$

where $\varepsilon^2/2\pi$ is a normalization factor.

We illustrate how to draw a random point from the pdf defined in (5). First of all, we note that the pdf of the Laplacian depends only on the distance from x. It will be convenient, therefore, to switch to a system of polar coordinates with origin in x. A point z will be represented as a point (r,θ), where r is the distance of z from x, and θ is the angle that the line xz forms with respect to the horizontal axis of the Cartesian system. Following the standard transformation formula, the pdf of the polar Laplacian centered at the origin (x) is:

$$D_\varepsilon(r,\theta) = \frac{\varepsilon^2}{2\pi} r e^{-\varepsilon r} \quad (6)$$

We note that the polar Laplacian defined above enjoys a property that is very convenient for drawing in an efficient way: the two random variables that represent the radius and the angle are independent. Hence, we draw a point (r,θ)from the polar Laplacian through a two-step method:

1) draw θ uniformly in [0,2π)
2) draw p uniformly in [0,1)

and then we solve the following formula (7) to obtain the corresponding radius.

We consider the cumulative distribution function $C_\varepsilon(r)$ from the marginal ($\varepsilon^2 re^{(-\varepsilon r)}$): $\int_0^r \varepsilon^2 \rho e^{-\varepsilon\rho} d\rho = 1-(1+\varepsilon r)e^{-\varepsilon r}$ Intuitively, $C_\varepsilon(r)$ represents the probability that the radius of the random point falls between 0 and r. Let $C_\varepsilon(r)$ be p in the two-step method above. i.e.,

$$1-(1+\varepsilon r)e^{-\varepsilon r} = p \tag{7}$$

The solution of formula (7) is $C_\varepsilon^{-1}(p) = -\frac{1}{\varepsilon}\left(W_{-1}\left(\frac{p-1}{e}\right)+1\right)$ where W_{-1} is the Lambert W function (the -1 branch).

In summary, our complete mechanism is shown as follow:

Input: x,ε
Output: Sanitized version z of input x
1. draw θ unif. in [0,2π)
2. draw p unif. in [0,1),set $r \leftarrow C_\varepsilon^{-1}(p)$
3. $z \leftarrow x + \langle r\cos\theta, r\sin\theta \rangle$
4.return z

IV. ENHANCING THE TRAJECTORY PRIVACY WITH DX-PRIVACY

In this section we evaluate our mechanism described in the previous sections. We perform our evaluation on the widely used dataset: GeoLife[26][27][28]. This trajectory dataset can be used in many research fields, such as mobility pattern mining, user activity recognition, location-based social networks, location privacy, and location recommendation.

A. Dataset

The GeoLife GPS Trajectories dataset contains 17621 traces from 182 users, moving mainly in the northwest of Beijing, China, in a period of over three years (from April 2007 to August 2012). The traces show users performing routinary tasks (like going to and from work), and also traveling, shopping, and doing other kinds of entertainment or unusual activities. Besides, the traces were logged by users with different means of transportation, like walking, public transport or bike. More than 90% of the traces were logged in a dense representation, meaning that the individual points in the trace were reported every 1-5 seconds.

B. Privacy Calculation

We can regard the locations over the period [1:n] as a tuple x, so that x[i] represents the location at the time i. Using our d_x -privacy metric, we can provide a meaningful privacy guarantee by protecting the accuracy of the values. Some privacy will still be lost, but the mobility pattern will be protected.

Currently, we just obfuscate the latitude and longitude data to prevent the user from tracking. Due to space limitations, we obfuscated the longitude data by our Laplace Mechanism. In the settings of strong privacy required, the user adds more noise and the privacy parameter is small (such as 0.1); In the settings of weak privacy guarantee required, the user adds less noise and the privacy parameter is large (such as 1.9); while there is no privacy preference, the user release the raw data trajectory.

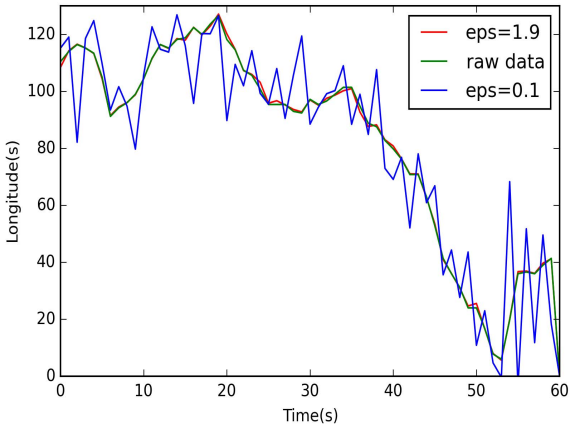

Figure 2. Longitude raw data (green) and its noisy reporting with varied privacy parameters.

Fig. 2 illustrates the application our method to distort the digital signature of GPS longitude data selected randomly from the GeoLife Dataset. The green line in Figure 2 represents the real longitude tract within two minutes (from 2008-05-26 13:01:02 to 13:03:03 sampling interval=2s). The red line is (the approximation of) the signature produced by a user that reports the true readings with the privacy parameter ε=1.9, which corresponding the weak privacy guarantee. The blue line is the obfuscated longitude tract obtained by adding Laplace noise to the true readings with the privacy parameter ε=0.1, which is corresponding the strong privacy guarantee. As we can see, especially in the case of ε=0.1, the signature (mobility pattern) is not recognizable. Hence, the malicious adversary cannot recognize the mobility patterns by observing the trajectory. Thus he is unable to infer the user's privacy, such as the address privacy. We also can see as the privacy parameter decreases (from ε=1.9 to ε=0.1), the bias becomes increasingly random. Conversely, as ε increases, the noise distribution starts to match the raw data more closely.

C. Quality Loss Analysis

Our ultimate goal is not only to protect the user's mobility patterns privacy, but look for a good balance between privacy and utility. Hence, we compare the quality loss of our mechanism with that of other ones proposed in the literature. Those generated the random noise naively. As stated in Definition 2.3, the expected distance is used as an indicator to measure the service quality loss.

Fig. 3 depicts the distortion varied with different privacy parameters. The horizontal axis represents the percentage of noisy points within the corresponding distance region.

For example, the dot (0.6, 30.223) in red line means that 60% obfuscated points is within the area (Distance

<30.223m). Similarly, we obfuscate almost all (Confidence=0.99) the values within the area (Distance<76.38m). As we can see, the stronger privacy guarantee (ε=0.1) will incur a larger distortion. Accordingly, the quality loss will decrease more.

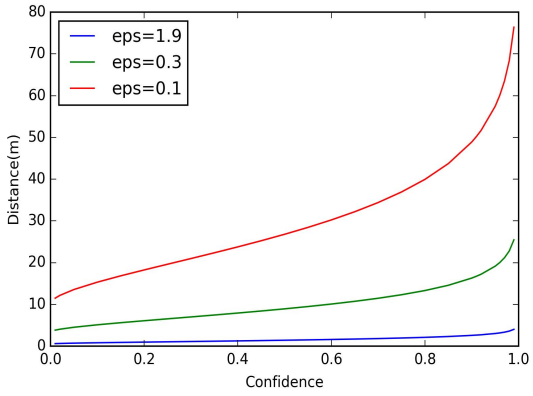

Fig. 4 shows the three pairs of comparison results under the same distance. The blue bar represents the expected distortion as 36.388652372m within the Distance<4.02m (ε=1.9) and under the condition with the probability distribution is

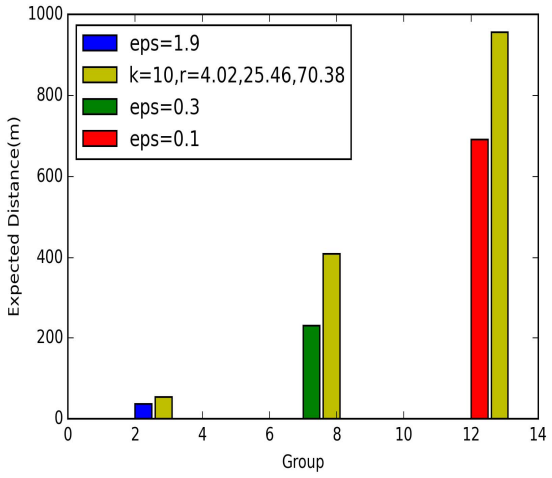

Figure 4. The comparison results

p=(0.01,0.02,0.05,0.1,0.15,0.2,0.25,0.3,0.35,0.4,0.45,0.5, 0.55,0.6,0.65,0.7,0.75,0.8,0.85,0.9,0.91,0.92,0.95,0.96,0.97,0 .98,0.99). Within the same Distance (δ=4.02m), we randomly select k=10 locations around the same real location. The expected distortion is 54.23m.Similary, the green bar represents the expected distortion as 230m and the red bar represents the expected distortion as 691m. While the corresponding distortions of (k,δ)-anonymity are 409m and 905m, respectively. The results reveal that Laplace mechanism adds less amplitude noise than the (k,δ)-anonymity under the same privacy guarantee.

V. RELATED WORK

Our work involves three areas of related works that concerns designing obfuscation mechanisms, e.g., in the context of quantitative information flow [5] [3] [6], quantitative privacy in mobile-aware service systems [7][8] [9] [10], as well as differential privacy[11] [12] [13][14]. The concept of differential privacy due to Dwork[11] has emerged as a strong guarantee of privacy. The generalization of differential privacy to arbitrary metrics was considered also in [15][9]. In those works, however, the purpose of extending the definition was to protect the single value (locations or a set of points (the example of the smart meters). Another work closely related to ours is[16] in which an extended definition of differential privacy is used to capture the notion of fairness in classification. A metric d is used to model the fact that certain individuals are required to be classified similarly, other approaches for privacy preservation include the use of encryption and multi-party computation [17].These techniques are usually computationally expensive and we are not aware of any proposal for their applications to the problem we are considering.

A series of techniques aim to protect a user from the privacy leak caused by the disclosure of the user's trajectories [18] [19].This kind of technology tries to blur a user's location, while ensuring the quality of a service or the utility of the trajectory data. There are two major scenarios that we need to protect a user's trajectory data from the privacy leak.

One is in real-time continuous location-based services, e.g. tell me the traffic condition that is 1km around me. In this scenario, a user may not want to exactly disclose her current location when using a service. Different from the simple location privacy, the spatiotemporal correlation between consecutive samples in a trajectory may help infer the exact location of a user. Techniques trying to protect the privacy leak in this scenario include, spatial cloaking [2], mix-zones [20], Path confusion [21], Euler histogram-based on short IDs [22], dummy trajectories [23], etc.

The second is the publication of historical trajectories. Collecting many trajectories of an individual may allow attackers to infer her home and work places, therefore identifying the individual's identity. Major techniques for protecting users' privacy in such scenario include, clustering-based [18], generalization-based [24], suppression-based [1]. According to the above classification, our work belongs to the second category, but we have introduced the notion of differential privacy.

A formal model named k-anonymity was proposed by Samarati and Sweeney two decades ago [29]. It measures the privacy of a released microdata set. The idea is to focus on the set of attributes called quasi-identifiers. If each combination of values of quasi-identifier attributes is shared by at least k records, k-anonymity holds. In this case, the probability of re-identifying a respondent by linking with external identified data sets is at most 1/k. The popularity of k-anonymity has led to extensions for specific types of data, like spatial-temporal data. One of these extensions is (k, δ)-

anonymity [1] and [30]. In this privacy notion, parameter k has the same meaning as in k-anonymity, while δ represents a lower bound of the uncertainty radius when recording the locations of trajectories.

VI. CONCLUSION

In the paper, we present a model served as the basis for exploring the relation between the real value and the reported value. Then we introduce d_x -privacy, a generalized version of the well-known concept of differential privacy for mobile aware service systems that provide strong theoretical guarantees on the privacy of released data. Furthermore, we present a Laplace mechanism by adding Laplace random noise to achieve the trajectory privacy. On the real GeoLife dataset, we can see as the privacy parameter decreases (from ε=1.9 to ε= 0.1), the bias becomes increasingly random. By adopting the expected distance as an indicator to measure the service quality loss, we compare our Laplace Mechanism with the random method (k=10). The results reveal that Laplace mechanism adds less noise amplitude than the random method under the same privacy guarantee.

ACKNOWLEDGMENT

This work was supported in part by the National High Technology Research and Development Program of China (863 Program) (No. 2013AA014002).

REFERENCES

[1] O. Abul, F. Bonchi, M. Nanni, Never walk alone: uncertainty for anonymity in moving objects databases, in: Proceedings of the 24th International Conference on Data Engineering, ICDE 2008, Cancun, Mexico, 7–12 April 2008, IEEE, 2008, pp. 376–385.

[2] F. Brunton and H. Nissenbaum. Vernacular resistance to data collection and analysis: A political theory of obfuscation. First Monday, 16(5),2011

[3] M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differen-tial privacy: On the trade-off between utility and information leakage," Lect. Notes Com-put. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7140 LNCS, pp. 39–54, 2012.

[4] S. Chawla, C. Dwork, F. Mcsherry, A. Smith, and H. Wee, "Toward Privacy in Public Da-tabases," Theory Cryptogr., pp. 363–385, 2005.

[5] P. Mardziel and M. Alvim, "Quantifying information flow for dynamic secrets," Univ. Maryl. …, 2014.

[6] M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," Proc. Comput. Secur. Found. Work., pp. 265–279, 2012.

[7] G. Barthe, G. Danezis, B. Gregoire, C. Kunz, and S. Zanella-Beguelin, "Verified computa-tional differential privacy with applications to smart metering," Proc. Comput. Secur. Found. Work., pp. 287–301, 2013.

[8] G. Michaela, "Privacy-Aware Personalization for Mobile Advertising.".

[9] M. Andrés and N. Bordenabe, "Geo-indistinguishability: Differential privacy for location-based systems," Proc. …, pp. 901–914, 2013.

[10] R. Shokri, G. Theodorakopoulos, J. Y. Le Boudec, and J. P. Hubaux, "Quantifying location privacy," Proc. - IEEE Symp. Secur. Priv., pp. 247–262, 2011.

[11] Dwork C, Differential Privacy.Proceedings of the 33rd Internationla Colloquium on Automata, Languages and Programming(ICALP). Venice, Italy,2006:1-12.

[12] G. Barthe and K. Boris, "Information-theoretic Bounds for Di ff erentially Private Mecha-nisms," 2010.

[13] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, "Optimizing linear counting que-ries under differential privacy," Proc. twenty-ninth ACM SIGMOD-SIGACT-SIGART Symp. Princ. database Syst. data - Pod. '10, p. 123, 2010.

[14] S. Alvim, M. E. Andr, K. Chatzikokolakis, S. Alvim, M. E. Andr, K. Chatzikokolakis, and P. Degano, "On the information leakage of differentially-private mechanisms To cite this version : On the information leakage of differentially-private mechanisms," 2015..

[15] G. Danezis, M. Kohlweiss, and A. Rial, "Differentially private billing with rebates," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformat-ics), vol. 6958 LNCS, pp. 148–162, 2011.

[16] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, "Fairness Through Aware-ness," 2011.

[17] C. Gentry, "Implementing Gentry ' s Fully-Homomorphic Encryption Scheme Preliminary Report," Organization, pp. 1–30, 2010.

[18] O. Abul, F. Bonchi, and M. Nanni, "Never walk alone: Uncertainty for anonymity in mov-ing objects databases," Proc. - Int. Conf. Data Eng., vol. 00, pp. 376–385, 2008.

[19] A. Y. Xue, R. Zhang, Y. Zheng, X. Xie, J. Huang, and Z. Xu, "Destination prediction by sub-trajectory synthesis and privacy protection against such prediction," Proc. - Int. Conf. Data Eng., pp. 254–265, 2013.

[20] a. R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Perva-sive Comput., vol. 2, pp. 46–55, 2003.

[21] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Achieving guaranteed anonymity in gps traces via uncertainty-aware path cloaking," IEEE Trans. Mob. Comput., vol. 9, no. 8, pp. 1089–1107, 2010.

[22] H. Xie, L. Kulik, and E. Tanin, "Privacy-Aware Traffic Monitoring," vol. 11, no. 1, pp. 61–70, 2010.

[23] H. Kido, Y. Yanagisawa, and T. Satoh, "An anonymous communication technique using dummies for location-based services," Proc. - Int. Conf. Pervasive Serv. ICPS '05, vol. 2005, pp. 88–97, 2005.

[24] Y. Saygin, Y. Saygin, M. E. Nergiz, M. E. Nergiz, M. Atzori, M. Atzori, B. Guc, and B. Guc, "Towards Trajectory Anonymization:a Generalization-Based Approach," Trans. Data Priv., vol. 2, no. 106, pp. 47–75, 2009.

[25] K. Chatzikokolakis, M. E. Andrés, N. E. Bordenabe, and C. Palamidessi, "Broadening the scope of differential privacy using metrics," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7981 LNCS, pp. 82–102, 2013.

[26] Y. Zheng, Q. Li, Y. Chen, X. Xie, and W.-Y. Ma, "Understanding mobility based on GPS data," Proc. 10th Int. Conf. Ubiquitous Comput. - UbiComp '08, no. 49, p. 312, 2008.

[27] Y. Zheng, L. Zhang, X. Xie, and W.-Y. Ma, "Mining interesting locations and travel se-quences from GPS trajectories," Proc. 18th Int. Conf. World wide web - WWW '09, no. 49, p. 791, 2009.

[28] Y. Zheng, X. Xie, and W. Ma, "GeoLife: A Collaborative Social Networking Service among User, Location and Trajectory.," IEEE Data Eng. Bull., vol. 33, no. 49, pp. 32–40, 2010.

[29] P. Samarati, L. Sweeney, Protecting Privacy when Disclosing Information: k-anonymity and its Enforcement through Generalization and Suppression, Technical Report SRI-CSL-98-04, SRI Computer Science Laboratory, 1998.

[30] O. Abul, F. Bonchi, M. NanniAnonymization of moving objects databases by clustering and perturbation Information Systems, 35 (8) (2010), pp. 884–9109.