Cost Effective Dummy Generation Scheme in Non-Trusted LBS

Sanghun Choi, Shuichiro Haruta, Hiromu Asahina, and Iwao Sasase
Dept. of Information and Computer Science, Keio University
3-14-1 Hiyoshi, Kohoku, Yokohama, Kanagawa 223-8522, Japan,
Email: choi@sasase.ics.keio.ac.jp

***Abstract*—Although a LBS(Location Based Service) is quite convenient and usually used these days, the location privacy of the user is not guaranteed from the LBS. If LBS itself is malicious, it is dangerous what the user's raw location data sends to the LBS. The promising approach to protect the user's location privacy is utilizing the dummy which is the fake location of the user. In the conventional schemes, the users themselves or the TTPS (Trusted Third Party Server) generates the dummies and sends them to the LBS with his/her real location. However, these schemes have shortcomings. In case of the user generates the dummies, the computational cost is high on the user's mobile devices. In these cases, the communication cost is also high since the user must receive all data of the dummies locations from the LBS.**

In this paper, in order to overcome shortcomings what mentioned above, we propose a Cost Effective Dummy Generation Scheme in Non-Trusted LBS. The main idea of our scheme is that Non-Trusted LBS creates dummy locations which includes the user's real location for reducing the user's communication cost. In spite of allowing LBS to generate the dummy location, the user's location privacy is protected. Through the XOR operation, the user's value is restored and protected from the LBS which is malicious. Since the LBS receives all of random number and the user's converted coordinate and performs the XOR operation, the LBS can generate multiple dummy locations which include his/her real location. Furthermore, in order to reduce communication cost, we combine our scheme with PIR-based method. Our method is enable the user to receive only him/her data by hiding the information which is him/her searched places from the LBS. We demonstrate the reduction of the communication cost and the reliability of our scheme by the computer simulation and the analysis.

I. Introduction

Our life is more comfortable with the growth of the smartphone technology. A user can obtain any information which the user wants through the internet on the smartphone. The user searches information about good restaurants and shops when the user goes to the trip or unknown places. In that time, the smartphone sends the query what the user wants to find information with his/her location data to the LBS (Location Based Service) server. The LBS searches the data based on the user location information and returns searched results to him/her device. Since the user casually send their location information to the LBS, the LBS can know easily where the user is. If LBS is malicious, the user location privacy may be used for strange activities such as a stoking etc. Moreover, even if the LBS is not malicious, it might happen the situation, when the LBS server is hacked from the attacker who try to use the user location data maliciously. In order to protect the user's location privacy, many researchers have been researched about this issue [1]–[13]. We can categorize these methods into two approaches. First one is Dummy Generation approach. By placing the dummies which are the fake location of the user, the LBS cannot identify the real location of the user. There are two types of the dummy generation schemes. The type 1 includes methods which the user generates dummy [1]–[5]. In these schemes, the communication cost is high since the user has to create dummies with his/her mobile devices. The type 2 is called the TTPS (Trusted Third Party Server). It generates the dummies instead of the user to solve the shortcomings which is mentioned above Type 1 [6]–[10]. However, the management cost of the TTPS is higher than the type 1. Second one includes Private Information Retrieval(PIR)-based approach [11]–[13]. PIR-based methods are used the privacy security using the Moore Curve with the Homomorphic Encryption. In that method, the Non-Trusted LBS generates the grids of the cells based on the user's area. The user generates Public key, Private key, Shift key for Homomorphic Encryption. the Non-Trusted LBS encrypts the Point Of Interest(POI) table based on the user's public key and shifts POI table by using encrypted shift key. In that process, the Trusted LBS cannot inspect the user location in the POI table. In the PIR-based method, the user location is protected from the Non-Trusted LBS. However, the user's location data be leaked to the Non-Trusted. The Non-Trusted LBS can know the area where his/her stays. Moreover, the grids of the cells are not fixable to change when the user moves to the new area.

In this paper, in order to overcome shortcomings what mentioned above, we propose the Cost Effective Dummy Generation Scheme in Non-Trusted LBS. The main idea of our scheme is that Non-Trusted LBS creates dummy locations which includes the user's real location instead of the grids in the PIR-based methods. In our method, In spite of allowing dummy generation method, the user's location privacy is protected from the privacy attack. It is possible to protect the user's location privacy through the XOR operation. In our scheme, the user generates multiple random numbers and performs XOR operation with his/her location coordinate and one of generated random number. Since the Non-Trusted LBS receives all of random number with the users converted coordinate and performs XOR, the Non-Trusted LBS can generate multiple dummy locations which includes the user's real location. Furthermore, in order to reduce communication

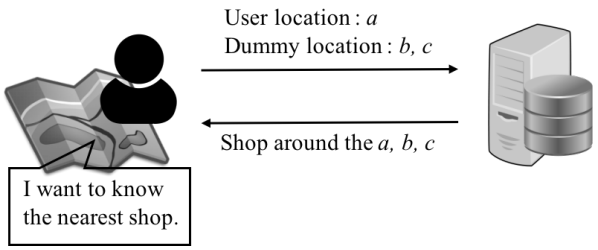


Fig. 1: Example of Dummy-based LBS

cost, we combine our scheme with the dummy generation and the PIR-based method for covering the user's location privacy. It enables the user to receive only him/her location data from the Non-Trusted LBS. The rest of this paper is constructed as the follows. Section II describes the concept of the dummy generation and the system model and the attacker model. The related work is introduced in Section III. The proposed scheme is described in Section IV. Simulation results and evaluations are shown in Section V. Finally we conclude our research in Section VI.

II. Preliminaries

A. Dummy Generation

For resolving the problem about the exposure of the user local area, we deal with the dummy generation. Fig1 shows how the dummy-based method operates. the dummy generation can hide the user's local area by using the dummy location from an attacker. Before sending the location data to the server, the user generates the fake location called dummy. Then, the user sends dummies with the data which the user wants to find information to the server. The server searches the information based on the dummy locations. And the server combines the searched information and the dummy locations. The user downloads all of data from the server. We adopt the improved dummy generation to the our scheme. The enhanced dummy generation is discussed in Section 4.

B. System Model

In this section, we explain the system model of the location service. When the user wants to know the nearest restaurants, the user sends his/her location to the LBS by using the user's devices like smart phone. Then, the LBS searches the restaurants based on the user's location in data store. After searching the restaurants around the user's location, the LBS sends the information of the around restaurants to the user. The user can know the nearest restaurants around his/her location.

C. Attacker Model

In our attacker model, we assume there are two attackers.
1. Server itself.
2. Someone who tries to hack server.

As the first model, since the administer managements all of the data in the LBS, although the user assumes the administer as the Trusted Third Party(TTP), the administer can know every locations data. If the administer is an attacker, his/her location will be leaked.

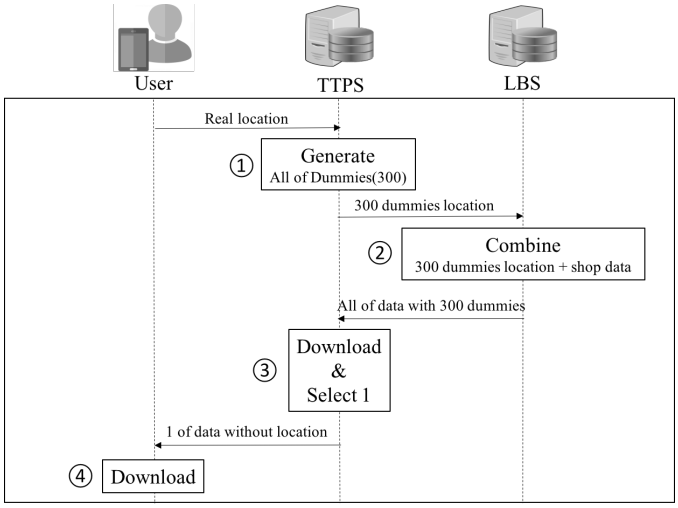


Fig. 2: Sequence of TTPS method

D. XOR Operation

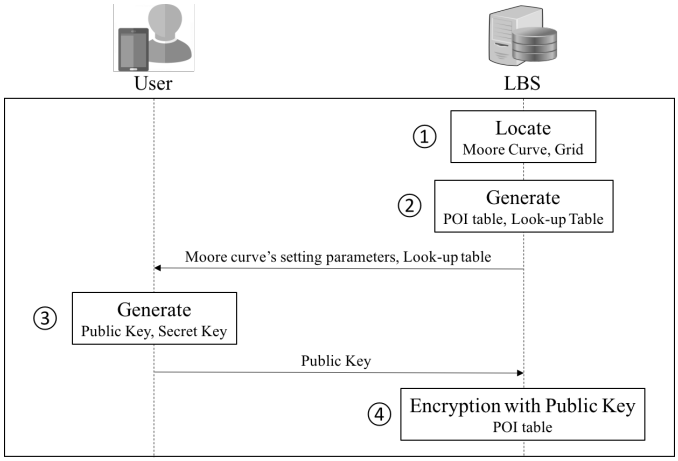
The XOR Operation takes two bit patterns of the equal length and the perform of the logical exclusive the XOR operation on each pair of the corresponding bits. The result in each position is 1 if only the first bit is 1 or only the second bit is 1, but will be 0 if both are 0 or both are 1. We perform the comparison of two bits, being 1 if the two bits are different, and 0 if they are the same. We adopt XOR to the our dummy generation scheme. The user makes a fake location using the XOR operation. Then, The user sends the fake location to the server. The server generates dummies by operating the XOR with the fake location. Through the XOR operation, the user can inspect the itself location in the dummy locations.

III. Related work

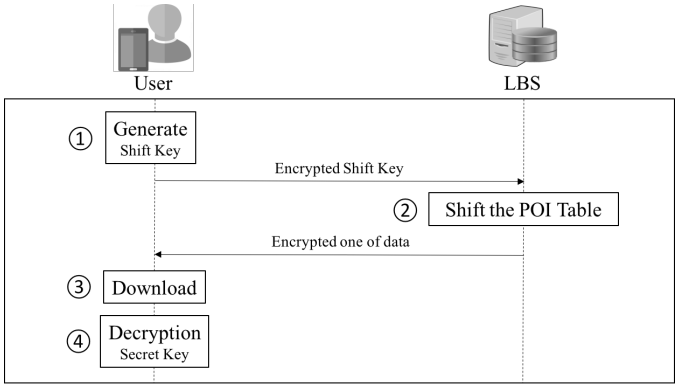
There are two methods for protecting users location privacy. 1.Dummy location generating methods [1]–[10]. 2.PIR based methods [11]–[13].

A. Dummy Location Generation Method

The dummy location generation method generates the dummy consisting of the random coordinates. Since the user sends his/her real location with the dummies, the LBS can not identify what the user real location is [1]–[5]. The LBS searches the POI based on the received dummy. Then the user transmits a set of the dummy and the search result to the user. Since the user knows his/her own location, the user can identify the result corresponding to his/her real location. One of most active challenges in the dummy generating methods is to reduce the communication cost and computation cost on the user side. Since the user generates, transmits and receives the dummies, the communication cost and the computation of the user device increases as the number of dummies increase. For reducing the computation and communication cost on the user



(a) Process 1



(b) Process 2

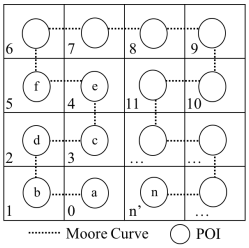
Fig. 3: Sequence of PCQP

side, the Trusted Third Party Server (TTPS) is utilized [6]–[10]. In this methods, TTPS generates the dummies instead of the user, thus the the cost of the user is only the communication cost for sending the single user's real location.

Fig 2 shows the sequence of the TTPS. First, the user sends his/her location to the TTPS. Seconds, the TTPS generates the dummies based on the his/her real location, and transmits them to the LBS. Third, the LBS searches the POIs which corresponding to the dummies and transmits the search results to the TTPS. Finally, the TTPS selects the one of the information of the user based on his/her location. The TTPS transmits the one of information to the user. In the TTPS process, the user transmits a single user real location and receives a single result. Therefore the communication cost of the user is lower than the conventional dummy-based schemes. However, the TTPS method has a serious problem. If the TTPS is an attacker or hacked by an attacker, the user's location will be leaked. TTPS can not guarantee the privacy of the location data. Moreover, the TTPS's management cost is very high.

B. Private Circular Query Protocol(PCQP)

In order to receive one POI which corresponds to the user's real location from LBS without leaking a user's location,



(a) Moore Curve on Grid

H-index	POI-info
$0'$	a
$1'$	d
$2'$	c
$3'$	d
$4'$	e
$5'$	f
...	...
n'	n

(b) POI table

H-value	H-index
1	$0'$
2	$1'$
3	$2'$
4	$3'$
5	$4'$
6	$5'$
...	...
n''	n'

(c) Look-up table

Fig. 4: Example of location informations on LBS

we pay attention to PCQP which is a Private-Information-Retrieval(PIR)-based scheme proposed by Lien et all [11]. The PIR-based methods enable a user to retrieve single POI while keeping it from LBS by shifting the POI table in a ciphered state. For realizing this, [11] adopts the Paillier cryptosystem which is an additive homomorphic cryptosystem [14]–[16]. To adopts the Paillier cryptosystem, authors define $\varepsilon_{\kappa p}(m;r)$ and $\mathcal{D}_{\kappa s}$ $(\varepsilon_{\kappa p}(m;r))$ encryption of a message m with encryption key κp and a pseudo random number r, and the decryption of that with a decryption key κs. $+_c$ and $\times_c$ defines the operator of the additive homomorphism. For given texts $m1$ and $m2$, pseudo random numbers $r1$ and $r2$, a public key κp, and a private key κs, (1) and (2) are satisfied in homomorphic cryptography.

$$\mathcal{D}_{\kappa s}(\varepsilon_{\kappa p}(m_1;r_1) +_c \varepsilon_{\kappa p}(m_2;r_2)) = m_1 + m_2. \quad (1)$$

$$\mathcal{D}_{\kappa s}(\varepsilon_{\kappa p}(m_1;r_1) \times_c \varepsilon_{\kappa p}(m_2;r_2)) = m_1 \times m_2. \quad (2)$$

The scheme perfectly supporting the additive homomorphisms. Since the user knows the amount of shift, it can specify the single POI his/her demands. On the other hand, the LBS can not identify the entry before shifting the table of POI corresponds to the entry specified by the user. Since the amount of shifts is encrypted. Fig 3 indicates the sequence of [11]. The LBS sends a grid and the lookup table, which consists of indexes of the gird cells (*H-value*) and POI table (*H-index*), to the user. Since POI table based on the coordinates of the cells in the grid, the user identifies which cell the user belongs to, i.e., what his/her *H-index* is. Fig 4 shows how the processes are working in the PCQP. Then, the user generates their public key κ_p and secret key κ_s based on the Paillier cryptosystem. Then, the user transmits only the κ_p to the LBS. After the LBS receiving κ_p, the LBS encrypts the POI table with κ_s. The user generates t-offset circular shift permutation matrix P^t as a shift key, which is defined as

$$P^t = [P_{i,j}]_{0 \le i,j \le n_p - 1}. \quad (3)$$

$$P_{i,j} = \begin{cases} 1 & (j = (i + n_p - t) \bmod n_p), \\ 0 & (otherwise). \end{cases} \quad (4)$$

Where n_p denotes the number of all entries in a POI table. Let $\varepsilon_{\kappa_p}(m,r)$ and $\mathcal{D}_{\kappa_s}(\varepsilon_{\kappa_p}(m,r))$ denote the encryption of a message m with a public key κ_p and a pseudo-random

number r and the decryption of that with a secret key κ_s, respectively. The user encrypts P^t to hide the amount of shifts by performing $\varepsilon_{\kappa_p}(P^t, r)$ and transmits it to the LBS. The LBS receives P^t and generates the shifted POI table by multiplying $\varepsilon_{\kappa_p}(P^t, r)$ by the POI table. The i-th entry of the shifted POI table I_i^t defined as

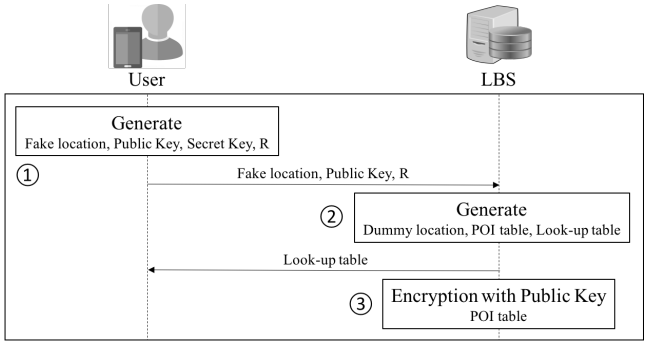
$$I_i^t = \prod_{j=0}^{n_p-1} \varepsilon_{\kappa_p}(P_{i-1,j}, r_j)^{I_{j+1}}. \tag{5}$$

Where I_j and r_j denotes j-th entry of the POI table and a set of pseudo-random numbers $\mathbf{r} = \{r_0, ..., r_{n_p-1}\}$. By the homomorphic properties of the Paillier cryptosystem, the I_i^t is still encrypted. Only the user's possessing corresponding secret key κ_s can decrypt the I_j^t by performing $\mathcal{D}_{\kappa_s}(I_j^t)$.

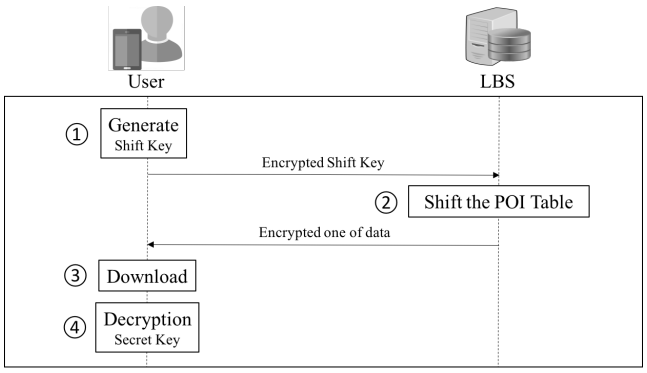
The PCQP has shortcomings that the LBS can identify the area where the user locates in the gird area. Since the coverage of the grid for the POI Table depends on the user's real location, a rough location (e.g., the user locates at Tokyo) can be identified from the LBS. However, in order to conceal rough location of the user, it is necessary to expand the grid area, it increases the computation cost of the user. This is because, the user has to find his/her location by searching from all of the H-value of the look-up table. The number of gird cells increase as the grids size increases. For example, if the user want to expand the grid size from the area of Tokyo in Japan, the number of gird cells increases from 10000 to 1720000 [12]. Moreover, if the user moves to somewhere, the LBS has to recalculate the grid and Moore Curve based on the user area. The user receives new look-up table from the LBS. And the LBS has to inspect his/her location again in the look-up table.

IV. Proposed Scheme

In order to overcome the shortcomings mentioned in Section III, we propose a Cost Effective Dummy Generation Scheme in Non-Trusted LBS. The main idea of our scheme is that the user's location is protected in spite of allowing Non-Trusted Server(NTS) generates the dummy locations which include the user's real location. This scheme is realized by the XOR operation. Since the user converts his/her location by the XOR with random number $r_{\mathrm{u}} \in R$ and sends converted location as the fake location and R to the NTS, the NTS can generate dummies which include the user's real location by XOR with the fake location and R. In this case, since the user's location already is converted the real location to the fake location, the user's real location is not identifiable from the NTS. the NTS generates the dummy location by using the fake location not the user's real location. Then, the user's location exists as the dummy location in the NTS process. Therefore, the NTS does not know where his/her location is in the R correspond with the r_{u}. Furthermore, in order to reduce the communication cost on the user side, homomorphic encryption is utilized. This enables the user to receive only one data data which is his/her information through the XOR operation and the PCQP from the NTS. As Fig 5 shows the our proposed scheme, we divide our proposed scheme in two processes. The process 1 is about dummy generation. The process 2 shows the same sequence of the PCQP.



(a) Process 1



(b) Process 2

Fig. 5: Sequence of Proposed Scheme

A. Process 1: Dummy Generation by XOR

As the user side, the user generates integer random number sequence R and decides $\mathbf{r}_{\mathrm{u}} \in R$. R and $\mathbf{r}_{\mathrm{u}}$ are defined as follows:

$$\begin{aligned} R &= \{\mathbf{r_1}, \mathbf{r_2}, \ldots, \mathbf{r_i}, \ldots, \mathbf{r_n}\}, \\ \mathbf{r_i} &= \{r_{i1}, r_{i2}, r_{i3}\}. \end{aligned} \tag{6}$$

Next, the user converts his/her location by the XOR operation. The XOR operation can be only defined between two integers. Since general location coordinate is floating point number, we use the integer part and the integerlized floating point number part of the coordinate. Assuming that $\alpha = (x, y)$, a, and b denote his/her real location, the integer part of x, and that of y, respectively, $d_x = x - a$ and $d_y = y - b$ are described as the floating point number of the coordinate. Furthermore, we define $f(.)$ as the integerlizing function such as $f(0.00545) = 545$. Then, we convert the user's location as follows:

$$\begin{aligned} \beta &= (x', y'), \\ x' &= (a \oplus r_{u1}) + (f^{-1}(f(d_x) \oplus r_{u3})), \\ y' &= (b \oplus r_{u2}) + (f^{-1}(f(d_y) \oplus r_{u3})). \end{aligned} \tag{7}$$

TABLE I: Look-up Table

Dummy coordinate	D-index
d_1	1
d_2	2
d_3	3
...	...
d_n	n

TABLE II: D-POI Table

(a) POI table

D-index	POI-info
1	l_1
2	l_2
3	l_3
...	...
n	l_n

(b) Encrpyed POI Table

D-index	POI-info
1	$\varepsilon_{\kappa p}(l_1)$
2	$\varepsilon_{\kappa p}(l_2)$
3	$\varepsilon_{\kappa p}(l_3)$
...	...
n	$\varepsilon_{\kappa p}(l_n)$

(c) Shifted POI Table

D-index	POI-info
1	$\varepsilon_{\kappa p}(l_3)$
2	$\varepsilon_{\kappa p}(l_4)$
3	$\varepsilon_{\kappa p}(l_5)$
...	...
n	$\varepsilon_{\kappa p}(l_{n-2})$

where β and $\oplus$ denote the converted location of user and XOR operation, respectively. Finally, the user sends β and R to NTS. Simultaneously, the user sends his/her public key κ_p. In the NTS side, NTS generates dummy locations based on β and R. For all of the elements in R, NTS calculates formula (7) for creating dummy locations. We demonstrate the case of r_{u} for x-coordinate of β. Since x-coordinate of β is $x' = (a \oplus r_{u1}) + f^{-1}(f(d_x) \oplus r_{u3})$, we can replace a and d_x in (7) to $a \oplus r_{u1}$ and $f^{-1}(f(d_x) \oplus r_{u3})$, respectively. That is,

$$\begin{aligned} x'' &= ((a \oplus r_{u1}) \oplus r_{u1}) + \\ &\quad f^{-1}(f(f^{-1}(f(d_x) \oplus r_{u3})) \oplus r_{u3}) \\ &= a + f^{-1}(f(d_x) \oplus r_{u3} \oplus r_{u3}) \\ &= a + f^{-1}(f(d_x)) \\ &= a + d_x = x. \end{aligned} \tag{8}$$

$$\mathbf{r}_{\mathrm{u}} \in R. \tag{9}$$

As shown above, we can guarantee that one of the dummies corresponds to the user's real location. Assuming that $d_1, d_2, \ldots, d_n$ denote dummy coordinates created by the NTS, the dummy locations and their indexes have relations shown as Table I. After that, the NTS searches the information like shops or restaurants based on all of dummy locations and creates the POI table shown in Table II(a).

B. Process 2 : PCQP

After generates the POI table by using dummy location in the LBS, Homomorphic Encryption is operated by the PCQP. Our process 2 follows the process 2 sequence of PCQP in III. Through the PCQP, the POI table is encrypted as Table II(b). The user can get his/her information from the LBS since the encrypted POI table is shifted by using shift key made by the user.

C. The solution of the fixed the dummy

When LBS generates dummies, there must generate one of location as the real user. If the user requests query to server when the user moves to another place, the LBS regenerates dummies. In that process, every dummy locations are changed by the LBS's dummy regeneration excluding one of the real location. If the user sends query to the LBS twice, one of the real location is fixed in dummy generation in the LBS. Attacker can know what the real location is look through the fixed one location. To solve this problem, we used the look-up table on the user side again in the process 1 in the proposed scheme. In the look-up table, there already all of the dummy locations are recorded by the LBS. Besides, if the user's location is not changed, It is not necessary to convert to his/her real location to the fake location on the user side. Therefore, when the user moves to another place, the user just transmits all of the dummy location in the look-up table again to the LBS. After the LBS receiving all of the dummies locations, the LBS does not regenerate dummies. the LBS just recombines all of location and the data of the restaurants. Through the this solution, the LBS and the attacker cannot inspect his/her real location despite of the user sends the same query again at the same place.

V. Scheme Analysis And Result

Our analysis method has three purposes. First one is reliability of the dummy generation. In order to confirm how many dummy locations needed for protecting his/her locations, we calculate the counts of dummy locations at the case of Japan. Second one is the reduction of the communication cost. We compare the proposed dummy generation and the conventional dummy generation which is the user's dummy generation for checking the reduction of communication cost on the user side. Third one is the solution the fixed dummy location. Since the user sends query to the LBS at the same location twice, one of dummy location must regenerate same place on the map.

A. Reliability of the Dummy Generation

In our scheme, the user generates one of the dummy location only one time. LBS creates the dummies in the range of R after earning one of dummy location and R from the user. In that process, since the dummies are randomly generated and located by the Non-Trusted LBS, we inspect how many dummies need for protecting the user privacy. We calculated as follows:

$$\begin{aligned} d &> \frac{x}{p}, \\ p &= \frac{\sum_{i=1}^{r} \pi r_i^2}{s}. \end{aligned} \tag{10}$$

where d means the counts of dummies. x is a reliability counts which will be placed where people are staying. the dummies will be located in the whole of land. P is the count of the dummies located place where people lives. r is an area of group of cities. We adopt that formula in Japan. The area

TABLE III: The format of data size : byte

(a) Common Data

Common Coordinate	One of POI
4	10000

(b) PCQP data

Public key	Shift Key	`r1`	First row of Look-up table
256	256	12	8

TABLE IV: The communication cost on the user

(a) Sending byte

D	50	100	150	200	250	300
A	200	400	600	800	1000	1200
B	1116	1716	2316	2916	3516	4116

(b) Receving byte

D	50	100	150	200	250	300
A	500000	1000000	1500000	2000000	2500000	3000000
B	10400	10800	11200	11600	12000	12400

(c) Total byte

D	50	100	150	200	250	300
A	500200	1000400	1500600	2000800	2501000	3001200
B	12516	13516	14516	15516	16516	17516

of Japan is 37,790,000ha. In that area, The area of forest is 25,100,000ha that is the 67% of the Japan. We assume people lives in 12,690,000ha. For example, in Japan, if the server creates 300 dummies, those will be located every place where people can stay. The counts of dummies based on area of country. According to calculations, If the LBS generate 300 dummies, 99% dummies can be located in place where people stays. We knows how many dummies need for protecting user privacy in area where the user lives in their country.

B. Reduction of Communication Cost

In order to compare the reduction of the communication cost, we prepare the data formats for calculating the communication cost. The format follows below table. The data formats are based on the single dummy generation query In the Table III. The common data is used the proposed dummy generation and the conventional dummy generation on the both user side. the PCQP data be used in the proposed scheme only.

In the table IV, where D, A, B denote the number of dummies and the conventional dummy generation and the proposed dummy generation, respectively. Since proposed dummy generation sends public key and shift key and `r1` to the LBS for the PCQP operation, the sending communication cost is higher than the conventional dummy generation. However, our proposed method only downloads one of the POI which is based on his/her location from the LBS, the receiving and total communication costs are much lower than the conventional dummy generation. Our proposed method can reduce the communication cost of the user drastically.

VI. Conclusion

In this work, we have proposed the Cost Effective Dummy Generation Scheme in Non-Trusted LBS. Our scheme is as secure as the conventional scheme since the process on NTS is performed by the XOR operation and Homomorphic Cryptosystem. We calculate the communication cost of the user side and the number of dummy location as necessary. The results show that our scheme reduces the communication cost. It is possible to protect the user location and reduce the communication cost of the user in our scheme through the XOR dummy generation in NTS with the PIR-based process.

References

[1] Schlegel, R., Chow, C. Y., Huang, Q., Wong, D. S. (2015). User-Defined Privacy Grid System for Continuous Location-Based Services. IEEE Transactions on Mobile Computing, 14(10), 21582172.

[2] Niu, B., Zhang, Z., Li, X.,Li, H. (2014). Privacy-area aware dummy generation algorithms for location-based services. 2014 IEEE International Conference on Communications, ICC 2014, 957962

[3] Do, H. J., Jeong, Y. S., Choi, H. J., Kim, K. (2016). Another dummy generation technique in location-based services. 2016 International Conference on Big Data and Smart Computing, BigComp 2016, 532538.

[4] Lu, H., Jensen, C. S. (2008). PAD: Privacy-Area Aware, Dummy-Based Location Privacy in Mobile Services. MobiDE, 1623.

[5] Hara, T., Member, S., Suzuki, A., Iwata, M. (2016). Dummy-Based User Location Anonymization Under Real-World Constraints, 4, 673687

[6] Niu, B., Li, Q., Zhu, X.,Li, H. (2014). A fine-grained spatial cloaking scheme for privacy-aware users in Location-Based Services. Proceedings - International Conference on Computer Communications and Networks, ICCCN.

[7] Lee, H., Oh, B.-S., Kim, H.-I.,Chang, J. (2012). Grid-based cloaking area creation scheme supporting continuous location-based services. Proceedings of the ACM Symposium on Applied Computing, 537543.

[8] Um, J., Kim, H., Choi, Y., Chang, J. (2009). A new grid-based cloaking algorithm for privacy protection in location-based services. 2009 11th IEEE International Conference on High Performance Computing and Communications, HPCC 2009, 362368.

[9] Hossain, A., Hossain, A. A., Jang, S. J., Chang, J. W. (2012). Privacy-aware cloaking technique in location-based services. Proceedings - 2012 IEEE 1st International Conference on Mobile Services, MS 2012, (Lc), 916.

[10] Ghaffari, M., Ghadiri, N., Manshaei, M. H., Lahijani, M. S. (2016). P4QS: A Peer to Peer Privacy Preserving Query Service for Location-Based Mobile Applications.

[11] Lien, I. T., Lin, Y. H., Shieh, J. R., Wu, J. L. (2013). A novel privacy preserving location-based service protocol with secret circular shift for k-NN search. IEEE Transactions on Information Forensics and Security, 8(6), 863-873.

[12] Utsunomiya, Y., Toyoda, K., Sasase, I. (2016). LPCQP: Lightweight Private Circular Query Protocol with Divided POI-table and Somewhat Homomorphic Encryption

[13] Papadopoulos, S., Bakiras, S. and Papadias, D.: Nearest Neighbor Search with Strong Location Privacy, Proc. the VLDB Endowment, Vol.3, No.12, pp.619629 (2010)

[14] P. Paillier, Public-key cryptosystems based on composite de- gree residuosity classes, in Advances in Cryptology Eurocrypt 1999.New York, NY, USA: Springer-Verlag, 1999, pp. 223238.

[15] J. Hoffstein, J. Pipher, and J. H. Silverman, Ntru: A ring-based public key cryptosystem, in ANTS, ser. Lecture Notes in Computer Science, J. Buhler, Ed. New York, NY, USA: Springer, 1998, vol. 1423, pp. 267288

[16] Gentry, C.: Fully Homomorphic Encryption Using Ideal Lattices, Proc. the Forty-first Annual ACMSymposium on Theory of Computing (STOC 09), STOC09, pp.169178, ACM(2009).