Improvement of Location-based Algorithm in the Internet of Things

Naser ghadimkhani
Department of Computer Engineering. Ahar Branch, Islamic Azad University, Ahar, Iran.
Email: nasergh204@yahoo.com,

Abstract

Location Based Services [LBS] has become an important field of research with the rapid development of Internet-based Information Technology [IOT], technology and also; everywhere that we use smartphones and social networks in our everyday lives. Although users can enjoy the flexibility, facility, facility and location-based services [LBS] with the Internet of Things, they may lose their privacy. An untrusted and malicious LBS server can track all user information by using different methods or publish personal information to a third person. In this study, we have an algorithm [DLS] to select the currently constructed location, which is an efficient preservation privacy approach, as well as the DLP's privacy policy, which is used to protect the privacy of the user's location, taking into account both. We analyze the computational costs and different requirements of the privacy of the various users and further enhance the privacy level by optimizing the DLP algorithm, which continues with extensive simulations. That has been performed the privacy level and the timing of the algorithms are compared and analyzed. Then the simulation results, indicate the privacy level of our optimized algorithm [ODLP] has increased

Keywords: Internet of Things, location-based services, privacy.

1. Introduction

Internet of Things [IOT] is a highly interconnected network of heterogeneous devices in which it seems that all types of communications may be, even those that are unauthorized. As a result, security needs for such a network are critical [1]. The Internet of Things in our lives becomes more and more popular every day. Since more people and devices can be connected to each other, it can lead to significant development in emerging smart cities and large data applications [2]. A great deal of information from various sources is collected and processed, Internet activities of objects may have a significant impact on the privacy of users. In addition, due to the growing trend of collecting more personal and personal data on the Internet, there are many problems with the impact on the privacy of individuals from a legal point of view [3]. Investigating data or processing the Internet The objects are largely fused, and are subject to pressure from the location information, and in its turn, it greatly affects the privacy of the place. As information about the location of a major corporation in efficient supply chains, efficient transportation systems, mobile-aware applications, and object-oriented Internet systems [4].

Privacy attacks and harmful consequences can disclose time sensitive location information without user consent. These challenges will affect the security

and privacy of the Internet of Things. Location-based developments and location-based mobile communication technologies have made applications more popular with more. The reasons for privacy and the lack of trust in LBS providers, K-Anonymity techniques and L diversity have been widely used to protect the privacy of users in the LBS-distributed architecture of the Internet of Things [2]. With the rise of the Internet of Things, privacy has become a major challenge [5, 6]. The locations and actions of each user in the Internet services of objects can be tracked and even monitored. Due to the evolution of mobile communication and communication technologies, LBS [7, 8] has rapidly expanded applications and location-based services, and more people are using these services. As we know, the LBS applications system on the Internet has been involved in various objects, including transportation, treatment, social networking, entertainment, and so on [2]. Though users enjoy the convenience of the services provided by LBS providers on the Internet, they potentially risk losing their privacy [9, 10].

The location or path privacy may be disclosed to other sections [5, 6]. Therefore, they are endangered by malicious attackers, thus at the expense of the users' vital interests. For example, if malicious attacks recognize the user's private location, as well as other privacy, they can easily get more comprehensive information through some analytics. Then they can hide their property through Internet or counterfeit communications. In addition, people increasingly focus on privacy security issues. Therefore, the problem of privacy protection in LBS on the Internet of Things must be solved [2].

2. Internet of Things

On the Internet, a large amount of information is collected and processed from various sources [3]. The locations and actions of each user in the Internet services of objects can be tracked and even monitored.

2.1. Infra-structure Internet of Things

The Internet of Things requires an open architecture to maximize inter-operability between heterogeneous systems and distributed resources, including providers and consumers of information and services [including humans, software, smart objects, or other devices].

In Fig. 1, we see an example of infra-structure and Internet architecture of objects.

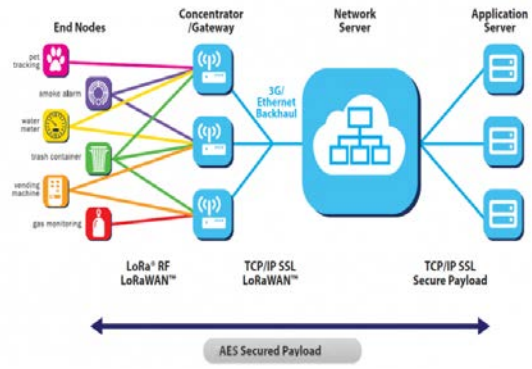

Fig.1. The architecture and structure of the Internet of Things

2.2. Layers Internet of Things

The Internet architecture of objects consists of four layers: the layer of perception, the network layer, the data management layer, the applied layer.

Data Perception Layer: The most basic layer of data perception is called, which is related to hardware issues. Millions of

objects are interconnected when data is collected from the environment. The main components in this layer are sensors, which convert the physical world into a digital world.

Network Layer: This layer is responsible for the secure transfer of information collected by the lower layer. Data transmission is done by networks such as cellular communications, satellite networks, wireless networks and other networks.

Data Layer: This layer is responsible for data management, which creates a reliable framework for application layer. On this framework, a variety of smart calculations are organized through a computer network and cloud computing to process bulk information. This layer acts as an interface between the application layer and the network layer.

Application layer: The highest layer called the application layer provides a variety of intelligent services that meet the needs of individuals. One of these services can be electronic health, smart hauling, and smart home and smart purchases. People can access these applications using personal computers, cell phones and smart TVs.

2.3. Challenges Internet of Things

There are several challenges to the Internet of things that are still in the research phase. This is a challenge, Are issues of the game created for two main reasons:

1. The massive amount of information collected for each object
2. Relationship between hardware systems

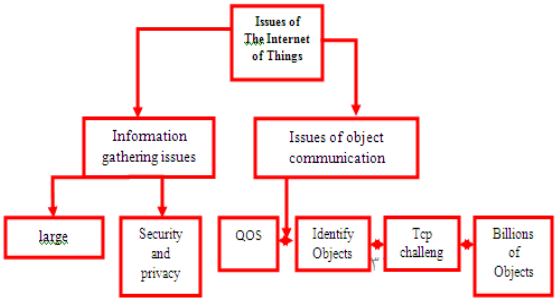

Fig.2. Categorization of IOT Challenges

The most important challenge in the Internet of Things is the presentation and acceptance of a comprehensive architecture that, in addition to covering communication and functional issues, also addresses security, privacy and trust issues.

2.4 Privacy

Defines privacy as "the access restriction of others to a person". Reason more data from different sources is gathered using devices. The Internet of Things can have a significant impact on the privacy of individuals with an additional potential for massive surveillance of individuals without their knowledge or consent. In other words, the Internet of Things is the promise of a new era of computing, by which any imaginable object is equipped, or connected to an intelligent device that allows the collection of data and communications over the Internet.

The Internet of Things challenges people's privacy in terms of collecting and using personal information. Privacy defines the rules under which each user should access what information. Privacy issues include the privacy of the object, location, and man.

2.4.1 Privacy Protection Methods

There are six basic method for privacy protection systems that are:
1. Awareness 2. Selection and satisfaction 3. Anonymity 4. Proximity and locality 5. Security requirements 6. Access.

2.5. Location Based Services [LBS]

Base location service is a software-based service that uses geo-location data to control some software features.
In fact, LBS is an information service that today uses various applications as information from geographic location - whether for entertainment or security purposes - on social networks used on mobile phones and through a mobile network. LBS includes services that identify the location of a person or object.

2.6.Privacy issues in base location services

Location-based systems [LBS] can transform many aspects of everyday life. The key challenge is how to protect privacy and confidentiality issues while using location-based services. In an emergency, everyone is interested in technology that automatically informs emergency services about the situation. However, if personal information is transferred to anyone interested in knowing this information, people will not feel well. The privacy of individuals is recognized as a fundamental human right and the protection of digital information on private affairs is an important element of the privacy of individuals that is called Data Protection or Fair Information Practice.
Awareness of the person's position can be used to infer other personal information about that person. Similarly, location-centric systems are not always a good indicator of a person's position.

2.7 review the privacy history of places on the Internet objects

In recent years, the rapid development of mobile technology has resulted in new types of mobile devices and social networks as well as the development of Internet services emerging objects [11, 12]. Many of these developments relies on LBS location services or LBS applications. A large number of techniques [13, 14] have been presented to address privacy issues in location-based services. Recent research has been conducted to protect privacy for services based on the Internet of Things [15, 16]. In order to handle a huge amount of information, the most compelling federated solution is the Internet of Things and cloud computing. Henz et al. Provided a user-based privacy-based approach to cloud-based services on the Internet, focusing on privacy for the end-user [15]. The authors proposed [17] PAGIOT, enabling a secure privacy accumulation protocol for Internet settings for objects and multi-index aggregation for a group of individuals. While allowing for privacy a solidarity value. A privacy styling model is designed to minimize privacy loss in the presence of unreliable service providers, so that providers can prevent disclosure of information to third parties for secondary use [18]. A conditional privacy authentication with the ability to access the link [PAL] for the roaming service, to

provide universal service and multi-level privacy [19]. Writers in [20] the cost of breaking the public key of cryptographic systems when the enemy is limited by resources and time available and the silent trade between the processing times for an Internet-based object of objects against the optimal period of privacy protection. Jane et al. Provided a framework for smart cities through the Internet of Things, which provided complete urban information system as a transport section of the existing cyber-physics system [21]. The authors in [22] provided a PDL [Privacy Imaging] framework that could help software engineers systematically evaluate the privacy capabilities of Internet applications for objects and middleware, resulting in the proposed PBD framework It can also be used to design the Internet operating system of new objects.

The K-Anonymity model is presented in [23]. This model enables the user to have different privacy requirements in different contexts, and different users can adopt different levels of privacy in the same field. In the model presented in [23], server anonymity trust is an efficient disruptive messaging engine that performs site anonymity with respect to the trade between location privacy and quality of service [QOS]. A hidden algorithm based on K Anonymity and L of variation is presented in [24]. The time to build a hidden area is at least K of the vehicle [K unknown] and the L [L Anonymity] road segment, which can effectively protect the privacy of the user's premises. The authors studied the problem of how to protect the privacy of the premises under various privacy threats, and the proposal of the privacy privacy of the place using the K-Anonymous and pseudo-anonymous methodology to provide efficient privacy protection. The proximity graph is based on the hidden K-weighted anonymity method in [25], which can search K's nearest neighbor without disclosing private information from the beginning of the query. The algorithm in [25] not only ensures user privacy, but also reduces bandwidth usage. The concept of the mixed region is presented for the first time in [26]. A mixing area refers to a location area in which each registered user refers to each contact of the application. The authors in [10] are allowed to exchange their nicknames when they are in a mixed region, which prevents users from using a nickname for a long time. Therefore, the relationship between aliases and locations can be broken, but exchanges the nickname.

Primary politics and encryption are based on approaches [27, 28] protecting user privacy by using cryptographic techniques. The authors in [29] provided a privacy framework [PLAM] for local mobile social networks. The PLAM framework not only requests a privacy accumulation protocol with K-Anonymity or L-diversity properties to help protect privacy, which prioritizes users without trusting an anonymous server that requests the service by location. Hybrid Linking The Dummy Identity

Method integrates the location of users to achieve the privacy of identity and privacy. The PLAM framework can not only meet the requirements of optimal privacy, but also resist external attacks against authentication, data integrity, and availability. To protect user privacy, authors in [30] presented a dummy construct idiom, in which multiple mock identifiers were searched in a variety of ways to disconnect the link between the true identity of users and the path. In [31], the authors have provided a LBS privacy style [FINE] framework for mobile devices. The FINE Framework not only supports a text encryption policy based on the encryption method to achieve light access control, the privacy of the location, the confidentiality of the LBS data and its access rule, and the exact result of the LBS query without the intervention of any trusted third party, but It integrates cryptographic and cryptographic switching keys and so on. For many computational tasks, providers LBS and users have migrated to the cloud server. In [32], the authors of the K's nearest neighbor [KNN] have studied the search for LBS-based mobile users about nearby K [POLS] points of interest based on their current location, and then a solution to the key encryption system General style to protect the privacy of the location and privacy of data in the KNN query from mobile users. The authors in [33] designed a private block retrieval protocol, and provided a safe and secure location based on the system's services. In the proposed system, users can retrieve information of interest to the service provider with regard to the location without communicating their location information. Existing methods [4, 34] are working to effectively generate bogus locations that cannot be detected by the LBS server. The authors in [39] offer an algorithm for locating dummy location DLS to protect the privacy of the location. The information that may be misleading by attackers is considered. In [4], authors first studied the behavior of their interested users in the LBS siblings from a game theory point of view. After formulating the elliptical game in both static and time-aware fields, the work analyzed the existence and properties of the elliptic NASH equilibrium for two models. An DLS algorithm for locating dummy locations in [35] is provided to obtain anonymity K for use by LBS users. The authors in [35] also presented an advanced DLS algorithm that can make the hidden area larger, while keeping the privacy level similar to the DLS algorithm. The authors in [36] provided two circle-based and network-based dummy manufacturing methods, which are inside the account required by the privacy zone. In [36] the authors presented two dummy solutions for reaching K obscurity for informational users in the LBS privacy zone, given that this side information may be used by the enemy. In [2], a location-based algorithm, which includes three key protocols: user requests aggregation protocol, binary identity transfer protocol and

improved PLAM protocol, is presented. In [12], a site caching scheme is presented based on a fake query in a continuous location service. To prevent an attacker from tracking a mobile user by continuous queries, some fake queries are accidentally injected by a third party. This paper [37] analyzes the well-known DLS algorithm, which provides site privacy protection for an Internet-based data service of user queries on LBS. Then, discusses the attack algorithm for DLS [ADLS] with a goal of identifying the real location of users of Internet-based data-based services from the selection of fictitious locations in the LBS. It also designs a privacy algorithm based on the DLP's built-in location to protect the privacy of the location on the LBS. An Entropy-based DLP algorithm is proposed by selecting a dummy location in a greedy way for an exchange between computational cost and privacy requirements for the Internet-based data-service object on the LBS.

3. materials and methods

In this section, we describe the main basic concepts and the system model.

3.1. Side Information

As mentioned in previous section, the side information [38] may be query probability of users related to location and time, or information related to the semantics of the query such as the gender and social status of the user. In this paper, the side information is considered to be the query probability of users related to location, called query probability. A particular user's query probability at a certain location can be denoted by the ratio of the number of current location queries to the number of total queries of all locations, as shown in Equation [1].

$$qi = \frac{\text{number of queries in location i}}{\text{numberof queries in all locations}} \quad [1]$$

Generally, users can get two kinds of side information from a system: partial information and global information. Partial information denotes the information collected by other users, for example, a particular user may know the query probabilities related to some locations. Since the LBS server can receive the LBS queries of all users, the LBS server can obtain the global information [i.e., the query probabilities related to all locations]. For a particular user, it's necessary to design an optimal strategy to select dummy locations for protecting his/her location privacy under the condition of knowing the global information. In this paper, the LBS server is responsible for disseminating and updating the global side information so that users can get this information from a well-known place [e.g., local database of LBS application].

3.2 .Entropy-based Privacy Metric

In this work, the degree of privacy is measured by the entropy. It can be seen as the uncertainty in identifying a user's real location out from the chosen dummy locations [39]. When calculating the entropy, each dummy location should have a probability, which can be the history query probability of users related to location.

We use p i to denote the historic query probability of users related to location i. According to the set of dummy locations and the historic query probabilities, we can define the entropy H of a user as in Equation [2].

$$H = -\sum_{i=1}^{k} qi \log_2 qi \qquad [2]$$

, is the normalized query probability of location i; and the sum of all p i is equal to 1.Since the greater the entropy the higher the uncertainty in identifying the user's real location from the dummy locations set, our goal is to obtain enough entropy. In particular, when all of the k dummy locations have the same historical query probability, we can achieve the maximum entropy H max = log 2 k.

3.3 Service based System Model for IoT

More and more mobile technologies support smart location based services including smart phones, manufacturing industries, smart home technologies, and smart cities. LBS is the key for achieving our future aim of smart living. The system architecture model shown in Fig. 3 illustrates our approach towards service-oriented design and implementation for the proposed algorithm.

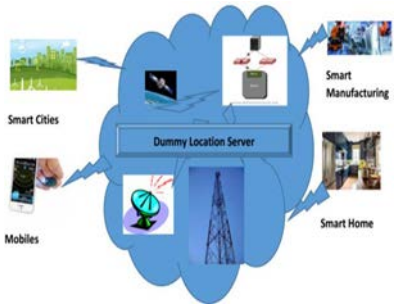

Fig.3. Service based System Model for IoT

We design our model for LBS based on the system architecture in [40]. The system mainly consists of two parties: the LBS server and LBS users with mobile devices.

1] LBS server: The LBS server can be a service provider, which not only stores all kinds of service databases, but also can
update the service data and provide users with various services. In our system, the LBS server is responsible to receive service queries from users, search for requested service data in the database, and reply with the search results back to the users. In addition, the LBS server is able to obtain the global information based on queries of all users at all locations, which can be the historical query probabilities of users related to all locations. Moreover, the LBS server is responsible for disseminating and updating the global side information so that users can get this information from a well-known place [e.g., local database of LBS application].

2] LBS users: The system typically consists of users who are equipped with mobile devices [e.g., smart phones or tablets], with built-in GPS modules that can be used to obtain user's location data. Due to the rapid development of mobile devices and social networks, a variety of LBS applications can be accessible for users. If users want to get services from LBS servers, they need to send queries to LBS server, which include their identity, location information, interests, and the query range [e.g., 1000m]. In order to protect user's

location privacy, user's location information not only includes user's real location, but also includes many other dummy locations.

4. Analysis of the DLS Algorithm

4.1. Review the DLS Algorithm

The main purpose of Dummy-Location Selection [DLS] algorithm [35] is to generate a set of realistic dummy locations to protect user's location privacy. Given the degree of anonymity k, the DLS algorithm needs to select other k-1 dummy locations based on the side information. The following shows the 5 steps how the DLS algorithm addresses this problem:

1. In the first step, a particular user needs to determine the degree of anonymity k.

2.Then, the algorithm reads all of the obtained query probabilities and then sorts the query probabilities of all locations in ascending order.

3. In the sorted list, the algorithm needs to choose 2k candidate locations, whose history query probabilities are similar to the user's real location. In the 2k candidate locations, it randomly selects k –1 locations. Then, it derives m sets, each set contains k locations. For each set, one location is user's real location and the other k−1 locations are randomly chosen from the 2k candidates.

4. Finally, the algorithm has to determine an optimal location set with the biggest entropy to effectively achieve k-anonymity for the user.

Table 1. Summary of key notations

Notation	Meaning
N	Number of all locations.
K	The privacy level requirement of user.
P[N]	The historical query probabilities in all locations.
M	Number of randomly selecting k–1 locations from 2k locations.
P_i	The historical query probability at location i.
l_{real}	The real location of user.
$P_i[2k]$	The chosen 2k candidates at location i, where k candidates are left before L real and the other k candidates are right after L real in the sorted list.
$C_i[k]$	The chosen optimal location set at location i.
K'	The number of locations which have the same historical query probability as L real in Pi.

Algorithm: dummy-location selection algorithm

Input : query probabilities in history q_i, real location L_{real}, number of sets m, k

Output: an optimal set of dummy locations

1 sort cells based on their query probability;

2 choosw 2k dummy candidates among which k candidates are right befor L_{real} and k candidates are right after L_{real} in the sorted list;

3 **for** [j = 1; j ≤ m; j + +] **do**

4 construct set C_j which contains L_{real} and k-1

other cells randomly selected

from the 2k candidates;

5 compute the normalized probability p_{ji} for

each cell c_{ji} in the set;

6 $Hj \longleftarrow -\sum_{i=1}^{k} pji \ . \log_2 pji$;

7 **end**

8 output arg max H_j;

4.2 DLP Algorithm Design and Analysis

In this section, we give the detailed descriptions for the DLP algorithm, and present the performance evaluations.

4.2.1 DLP Algorithm Description

The basic idea of Dummy Location Privacy-preserving [DLP] algorithm is to select the optimal dummy locations considering that the adversary may exploit some side information, and make different choice for different privacy requirements of different users. We adopt a greedy approach to search a large database to find an optimal set of dummy locations. For achieving k-anonymity, we successively select k-1 other locations from all locations in the location map, which must make sure that the current entropy is the biggest. For example, if the DLP algorithm has already chosen i locations [where i < k], when choosing the [i+1] th location, it must ensure that H i+1 is the largest for all residual locations. H i+1 is
defined in Equation [10].

$$H_{i+1} = -\sum_{j=1}^{i+1} \frac{pj}{\sum_{l=1}^{i+1} pl} \log_2 \sum_{j=1}^{i+1} \frac{pj}{\sum_{l=1}^{i+1} pl} \quad [10]$$

Where p_j denotes the users' historical query probability at location j. The following shows how the proposed DLP algorithm works.

1. First, a user needs to set a proper anonymity degree k, which is closely related to the user's requirement on location privacy. Although a bigger k leads to higher anonymity degree, it also causes a higher overhead due to the cost for selecting dummy locations.

2. At the beginning, the DLP algorithm needs to read all the obtained query probabilities from the LBS server and then sort the query probabilities in ascending order. Let p denote the query probability of the user's real location. For the sorted list, the DLP algorithm calculates the number of locations which have the same query probability as p, which is denoted by k^{-}. If $k^{-}$is large enough, it puts half of them before and the other half of them after the real location.

3. If $k^{-} \geq$ k, DLP algorithm selects k-1 locations which have the same query probability as p from the sorted list. Then, it outputs the chosen k-1 dummy location and the user's real location.

4. If $k/4 \leq \bar{k} \leq k$, the algorithm selects $\bar{k}$-1 locations which have the same query probability as p from the sorted list. We use set C to denote the $\bar{k}$-1 dummy locations and the user real location. In the sorted list, the algorithm selects k- $\bar{k}$ locations left before and other k- $\bar{k}$ locations right after the real location as 2[k- $\bar{k}$] candidate locations, whose query probabilities are different from p. Let set S denotes the 2[k- $\bar{k}$] candidates. The reason for choosing 2[k- $\bar{k}$] candidates for dummy locations is to make sure to get large enough entropy. Otherwise, it goes to Step 7.

5. To achieve k-anonymity, it needs to successively select residual k- $\bar{k}$ locations from set S. For the i^{th} [$\bar{k} < i \leq k$] dummy location, it must ensure that the H_i is maximum for all residual locations in set S.

6. When the size of C is k, DLP outputs the set C.

7. If $\bar{k} < k/4$, the DLP chooses 2k-ε locations left before and other 2k-ω locations right after the real location as 4k-ω-ε candidates from the sorted list. We use set $\bar{S}$ to denote the 4k-ω-ε candidates. Both ω and ε are set by users based on their privacy requirements. Generally, ω is smaller than ε. Let set $\bar{C}$ denote a user's real location. It randomly selects one location as a dummy location from set S, and put this location into set $\bar{C}$.

8. For achieving k-anonymity, the successively selects residual k-2 locations from set $\bar{S}$. For the i^{th} [$2 < i \leq k$] dummy location, it must ensure that H_i is the largest for all residual locations in set $\bar{S}$.

9. When the size of $\bar{C}$ is k, DLP outputs the set $\bar{C}$.

4.3 Presented the proposed algorithm ODLP

We present an optimal ODLP algorithm in this section and compare this algorithm with DLS and DLP algorithms in terms of privacy level and runtime.
Our goal is to optimize the ODLP algorithm and to increase the privacy level of the algorithms mentioned in the previous sections.
Since the level of privacy of the algorithms is measured and entropies with entropy, we must increase entropy to increase the level of privacy. In this algorithm, we try to choose how to select a collection of dummy places in a way that increases entropy and places that increase entropy. To achieve this goal, by carefully examining entropy, we find that entropy is directly related to the probability distances of the places with the probability of the user's actual location. So, for better convenience and a better selection of mock-up locations, we reduce the probability of a user's actual location from each other's probabilities in other places. After doing this, we sort the list up, the resulting list consists of all probability distances from the real-world probability that the places that are at the beginning of the list in our method will prioritize the choice of relative to There are next places because these

places are less spaced and thus increase entropy and hence the level of privacy. We can remove the location from the first list of distances from the first to randomly select the optimal 2K locations and select K-1 randomly from this list. Of course, in this way, the level of privacy is relatively less than the time when we select all the places from the first list in the order.
We'll see the steps in implementing the code below:

Input: 1-History Probability Query Set, P. 2. Real user location
Output: Optimal mock-up locations, C
1. Sort the collection P upwards

2. Select locations in a sorted set whose probabilities are as real as the query is and place it in H.

3. If the size H is greater than 2, perform steps four to seven

4. Reduce the probability of a real work location from all locations in P and positive all elements and put it in A
5. Sort the collection A upward

6. Place 2K locations from the beginning of the ordered list of distances in the CC

7. Select the random K-1 location in the actual location and place it in the C set.

8. If the size of H is not greater than 2, perform step 9.

9. K-1 Place the location from the beginning of the ordered list of spaces, in addition to the actual location, and put inside the C set.

10. The set of constructed places C, which includes the real place, is given as output.

In the ODLP algorithm, when the size of H is greater than 2, it does not exist when there is no place in the list, the query probability of that location is the same as the actual query probability. From the direct selection of K, we use the distance from the beginning of the ordered list, because in this situation the entropy of the algorithm decreases, and we try to increase the level of privacy by choosing all K-1 places of high priority.

5. Simulation Environment

we divide the location map into N*N cells with equal size. Each cell has a query probability based on the query history. We conduct simulations on the following three scenarios to evaluate the performance of the DLP algorithm.

- Scenario A: Let user be located in a cell such that there are many [more than k] cells that have the same historical query probability as the user’s current location. In this scenario, the chosen dummy locations have the same query probability as that of the user’s real location.
- Scenario B: Let user be located in a cell such that the number of cells that have the same historical query probability as that of the user’s current location is slightly less than k but greater than one quarter of k.

In this scenario, it can guarantee that there are enough locations have the same query probability as that of the user's real location in the chosen dummy locations.

- Scenario C: Let user be located in a cell such that there are a few [i.e., less than one quarter of k] cells have same historical query probability as that of the user's current location. In this scenario, there are few locations that have the same query probability as that of the user's real location in the chosen dummy locations.

6. Simulation Results

6.1 Generate dummy locations using DLS , DLP AND ODLP algorithms

In Figs. 4, 5 and 6, we see the dummy locations generated by the DLS and DLP and ODLP algorithms in a simulation environment in which the value of N is 10, the reds refer to the artificial and blue locations associated with the actual user's location. Be This is a scenario one. The simulation environment is identical in all simulations.

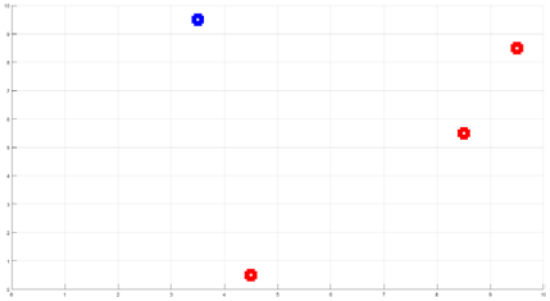

Fig.4. Dummy locations related to the DLS algorithm.

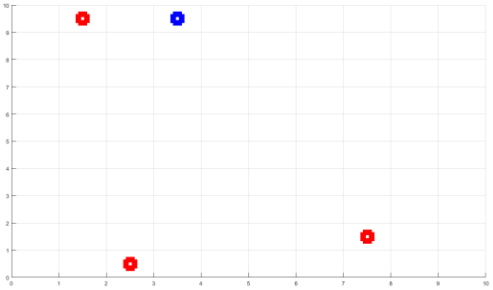

Fig.5. Dummy locations related to the DLP algorithm.

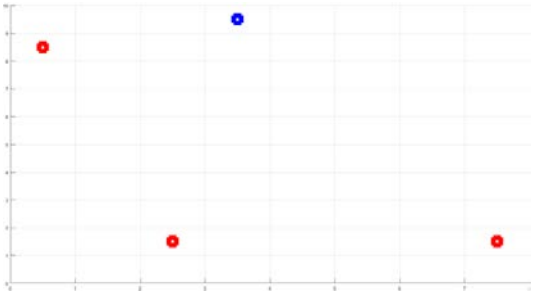

Fig.6. Dummy locations related to the ODLP algorithm.

6.2 Comparison of DLS and DLP Algorithms

Figs. 7-9 show the results of the DLP and DLS algorithms. Results of runtime and privacy level are shown in terms of entropy in different scenarios. In Fig. 7, the DLS algorithm and the DLP algorithm have a similar entropy, but they differ greatly in execution time. Additionally, the execution time of the DLS algorithm increases with increasing magnitude K of anonymity level, but the execution time of the DLP algorithm is slightly different. The reason is that the DLS algorithm selects the counting method and selects the structural locations that increase the entropy, while the DLP algorithm uses the greedy method to continuously K to select a mock location.

The computational complexity of the DLS algorithm increases with increasing K, but the computational complexity of the DLP algorithm remains almost constant. Fig. 8 and Fig. 9 show that scenario B and scenario C have similar trends in scenario A results. We should also note that the largest entropy appears in scenario A, and the smallest entropy in scenario C occurs for both DLS and DLP algorithms.

This is because there are places over K that their query probability history is the same as the user's actual position in scenario A, but only enough or there are few places that their probabilistic history is the same as the actual user's location. Scenario B or C. In addition, we can obtain the maximum entropy $H_{MAX} = \log_2 K$ in scenario A. In scenario A, they have a larger entropy than scenario B or C.

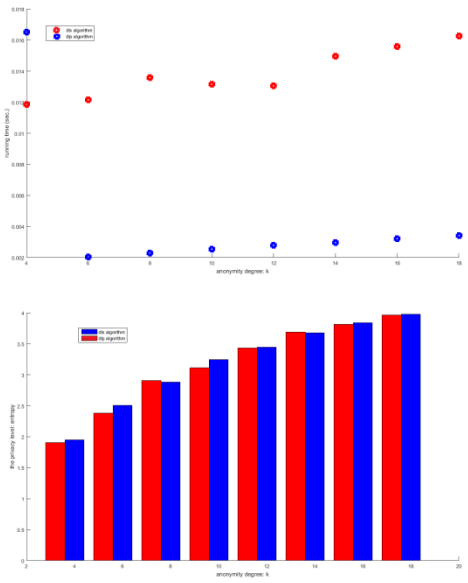

Fig.7. Entropy and Runtime of DLS and DLP Algorithms in Scenario A

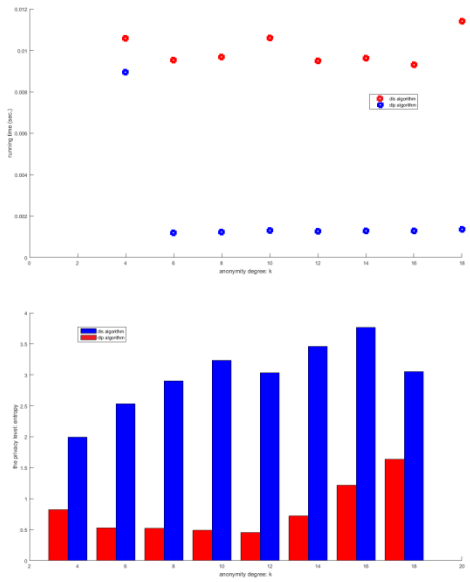

Fig.8. Entropy and Runtime of DLS and DLP Algorithms in Scenario B

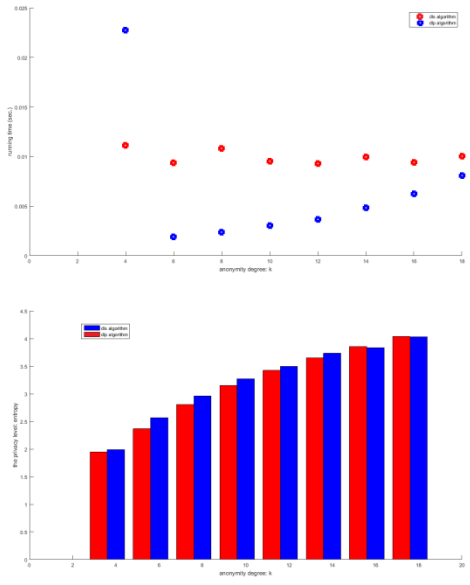

Fig.9. Entropy and Runtime of DLS and DLP Algorithms in Scenario C

6.3. Comparison of proposed ODLP algorithm with both DLS and DLP algorithms

As we see in the graphs below, we compare the ODLP algorithm in terms of privacy and runtime with both DLS and DLP algorithms. In all the graphs, the privacy level of the optimal ODLP algorithm is

more than the privacy level of the DLS and DLP algorithms, indicating that the ODLP algorithm has the potential to maintain privacy in relation to the algorithms mentioned.

Therefore, our ODLP algorithm has met our goal of optimizing the privacy of the DLP algorithm. But as you will see in the runtime graphs, the implementation time of the proposed algorithm is greater than the DLS and DLP algorithms, and time spent more on constructing mock locations than the mentioned algorithms. And this time increasing with the increase in the degree of obsolescence K. But in the diagram shown in Fig. 12, because of the direct selection of K, the space from the beginning of the arranged list is less time consuming and time-consuming than the DLP algorithm.

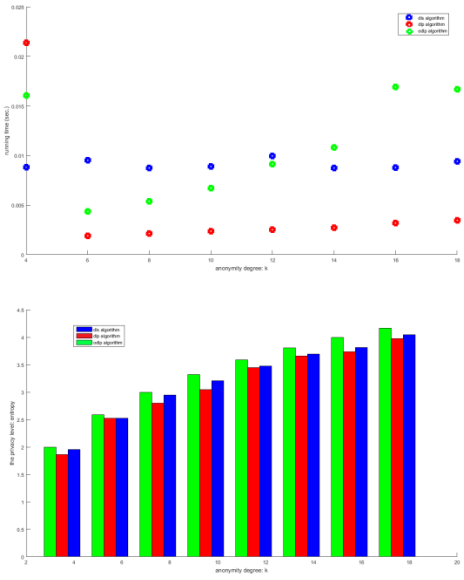

Fig.10. Entropy and Runtime of DLS, DLP, and ODLP Algorithms in Scenario A

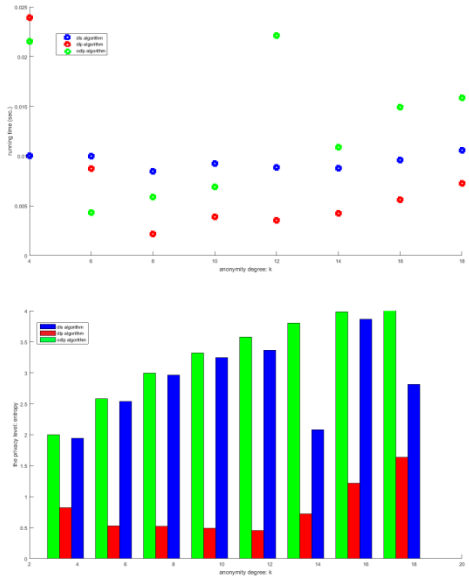

Fig.11. Entropy and Runtime of DLS, DLP, and ODLP Algorithms in Scenario B

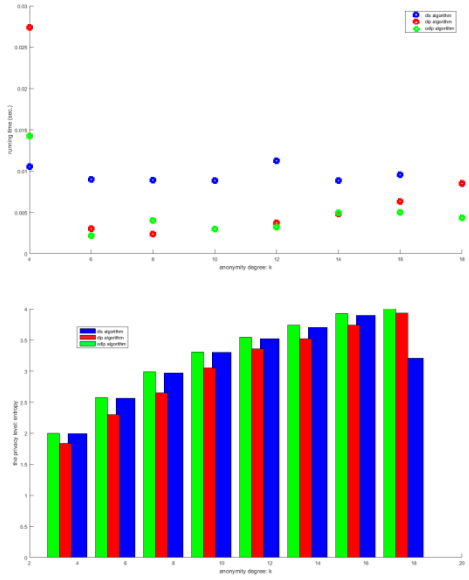

Fig.12. Entropy and Runtime of DLS, DLP, and ODLP Algorithms in Scenario C

7. Discussion and Conclusion

Due to the increasing growth of the Internet of objects and the growing involvement in the dimensions of our lives and tools around us, protecting privacy, which is one of the security dimensions, has become a major

challenge and urgency. Protecting privacy is a serious and important debate. Because the data processing or processing of the Internet has been largely fused, and is subject to pressure from the location information, and in its turn, it greatly affects the privacy of the place. As information about the location of a major corporation in efficient supply chains, efficient transportation systems, mobile-aware applications, and object-oriented Internet systems [4]. The DLS and DLP algorithms are two of the most important and most efficient algorithms that place privacy on their way through the production of artificial locations and the use of anonymity K. In such algorithms, parameters such as privacy level and runtime are very important and valuable. These two algorithms are designed and constructed with these parameters and are evaluated and compared using them. Our goal in this research was to increase and improve the privacy level of the DLP algorithm. To achieve this, we have achieved an entropy that is directly related to the privacy level and obtained results that we can achieve by using the level Improvement of privacy in the algorithm, and how it interrelates query probabilities and calculation of entropy. By calculating the list of distances and by choosing the optimal selection of simulated locations from the places with the highest priority in this list, we were able to ascertain, as in the conclusions of the simulations that were presented in three scenarios and with the change in the anonymity level K, the surface we increase privacy considerably. However, the runtime of our ODLP algorithm will increase with DLS and DLP algorithms. In future work, we can optimize this runtime algorithm, as well as improve the privacy level, and obtain a robust algorithm.

References

[1] Nguyen KT, Laurent M, Oualha N. Survey on secure communication protocols for the Internet of Things. Ad Hoc Networks. 2015;32[Supplement C]:17-31.

[2] Sun G, Liao D, Li H, Yu H, Chang V. L2P2: A location-label based approach for privacy preserving in LBS. Future Generation Computer Systems. 2017;74[Supplement C]:375-84.

[3] Shu T, Chen Y, Yang J. Protecting Multi-Lateral Localization Privacy in Pervasive Environments. IEEE/ACM Transactions on Networking. 2015;23[5]:1688-701.

[4] Liu X, Liu K, Guo L, Li X, Fang Y, editors. A game-theoretic approach for achieving k-anonymity in Location Based Services. 2013 Proceedings IEEE INFOCOM; 2013 14-19 April 2013.

[5] Sun Y, Chen M, Hu L, Qian Y, Hassan MM. ASA: Against statistical attacks for privacy-aware users in Location Based Service. Future Generation Computer Systems. 2017;70[Supplement C]:48-58.

[6] Niu B, Zhu X, Li Q, Chen J, Li H. A novel attack to spatial cloaking schemes in location-based services. Future Generation Computer Systems. 2015;49[Supplement C]:125-32.

[7] Li Y, Yiu ML. Route-Saver: Leveraging Route APIs for Accurate and Efficient Query Processing at Location-Based Services. IEEE Transactions on Knowledge and Data Engineering. 2015;27[1]:235-49.

[8] Xin M, Lu M, Li W. An adaptive collaboration evaluation model and its algorithm oriented to multi-domain location-based services. Expert Systems with Applications. 2015;42[5]:2798-807.

[9] Niu B, Li Q, Zhu X, Cao G, Li H, editors. Enhancing privacy through caching in location-based services. 2015 IEEE Conference on Computer Communications [INFOCOM]; 2015 April 26 2015-May 1 2015.

[10] Xinxin L, Han Z, Miao P, Hao Y, Xiaolin L, Yuguang F, editors. Traffic-aware multiple mix zone placement for protecting location privacy. 2012 Proceedings IEEE INFOCOM; 2012 25-30 March 2012.

[11] Mokbel MF, Chow C-Y, Aref WG. The new Casper: query processing for location services without compromising privacy. Proceedings of the 32nd international conference on Very large data bases; Seoul, Korea. 1164193: VLDB Endowment; 2006. p. 763-74.

[12] Ye A, Li Y, Xu L. A novel location privacy-preserving scheme based on l-queries for continuous LBS. Computer Communications. 2017;98[Supplement C]:1-10.

[13] Kalnis P, Ghinita G, Mouratidis K, Papadias D. Preventing Location-Based Identity Inference in Anonymous Spatial Queries. IEEE Transactions on Knowledge and Data Engineering. 2007;19[12]:1719-33.

[14] Ni W, Gu M, Chen X. Location privacy-preserving k nearest neighbor query under user's preference. Knowledge-Based Systems. 2016;103[Supplement C]:19-27.

[15] Henze M, Hermerschmidt L, Kerpen D, Häußling R, Rumpe B, Wehrle K. A comprehensive approach to privacy in the cloud-based Internet of Things. Future Generation Computer Systems. 2016;56[Supplement C]:701-18.

[16] Sadeghi AR, Wachsmann C, Waidner M, editors. Security and privacy challenges in industrial Internet of Things. 2015 52nd ACM/EDAC/IEEE Design Automation Conference [DAC]; 2015 8-12 June 2015.

[17] González-Manzano L, Fuentes JMd, Pastrana S, Peris-Lopez P, Hernández-Encinas L. PAgIoT – Privacy-preserving Aggregation protocol for Internet of Things. Journal of Network and Computer Applications. 2016;71[Supplement C]:59-71.

[18] Appavoo P, Chan MC, Bhojan A, Chang EC, editors. Efficient and privacy-preserving access to sensor data for Internet of Things [IoT] based services. 2016 8th International Conference on Communication Systems and Networks [COMSNETS]; 2016 5-10 Jan. 2016.

[19] Lai C, Li H, Liang X, Lu R, Zhang K, Shen X. CPAL: A Conditional Privacy-Preserving Authentication With Access Linkability for Roaming Service. IEEE Internet of Things Journal. 2014;1[1]:46-57.

[20] Premnath SN, Haas ZJ. Security and Privacy in the Internet-of-Things Under Time-and-Budget-Limited Adversary Model. IEEE Wireless Communications Letters. 2015;4[3]:277-80.

[21] Jin J, Gubbi J, Marusic S, Palaniswami M. An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet of Things Journal. 2014;1[2]:112-21.

[22] Perera CM, Ciaran; Bandara, Arosha K.; Price, Blaine A.; Nuseibeh, Bashar. Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms.

[23] Gedik B, Liu L. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms. IEEE Transactions on Mobile Computing. 2008;7[1]:1-18.

[24] Ying B, Makrakis D, editors. Protecting Location Privacy with Clustering Anonymization in vehicular networks. 2014 IEEE Conference on Computer Communications Workshops [INFOCOM WKSHPS]; 2014 April 27 2014-May 2 2014.

[25] Hossain A, Hossain AA, Jang SJ, Chang JW, editors. Privacy-Aware Cloaking Technique in Location-Based Services. 2012 IEEE First International Conference on Mobile Services; 2012 24-29 June 2012.

[26] Beresford AR, Stajano F. Location privacy in pervasive computing. IEEE Pervasive Computing. 2003;2[1]:46-55.

[27] Jung T, Li XY, Wan Z, Wan M, editors. Privacy preserving cloud data access with multi-authorities. 2013 Proceedings IEEE INFOCOM; 2013 14-19 April 2013.

[28] Li XY, Jung T, editors. Search me if you can: Privacy-preserving location query service. 2013 Proceedings IEEE INFOCOM; 2013 14-19 April 2013.

[29] Lu R, Lin X, Shi Z, Shao J, editors. PLAM: A privacy-preserving framework for local-area mobile social networks. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications; 2014 April 27 2014-May 2 2014.

[30] Zhu X, Chi H, Jiang S, Lei X, Li H, editors. Using dynamic pseudo-IDs to protect privacy

in location-based services. 2014 IEEE International Conference on Communications [ICC]; 2014 10-14 June 2014.

[31] Shao J, Lu R, Lin X, editors. FINE: A fine-grained privacy-preserving location-based service framework for mobile devices. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications; 2014 April 27 2014-May 2 2014.

[32] Yi X, Paulet R, Bertino E, Varadharajan V. Practical Approximate k Nearest Neighbor Queries with Location and Query Privacy. IEEE Transactions on Knowledge and Data Engineering. 2016;28[6]:1546-59.

[33] Zhu H, Lu R, Huang C, Chen L, Li H. An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud. IEEE Transactions on Vehicular Technology. 2016;65[9]:7729-39.

[34] Khuong V, Rong Z, Jie G, editors. Efficient algorithms for K-anonymous location privacy in participatory sensing. 2012 Proceedings IEEE INFOCOM; 2012 25-30 March 2012.

[35] Niu B, Li Q, Zhu X, Cao G, Li H, editors. Achieving k-anonymity in privacy-aware location-based services. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications; 2014 April 27 2014-May 2 2014.

[36] Lu H, Jensen CS, Yiu ML. PAD: privacy-area aware, dummy-based location privacy in mobile services. Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access; Vancouver, Canada. 1626540: ACM; 2008. p. 16-23.

[37] Sun G, Chang V, Ramachandran M, Sun Z, Li G, Yu H, et al. Efficient location privacy algorithm for Internet of Things [IoT] services and applications. Journal of Network and Computer Applications. 2017;89[Supplement C]:3-13.

[38] Ma CYT, Yau DKY, Yip NK, Rao NSV. Privacy Vulnerability of Published Anonymous Mobility Traces. IEEE/ACM Transactions on Networking. 2013;21[3]:720-33.

[39] Serjantov A, Danezis G. Towards an Information Theoretic Metric for Anonymity. In: Dingledine R, Syverson P, editors. Privacy Enhancing Technologies: Second International Workshop, PET 2002 San Francisco, CA, USA, April 14–15, 2002 Revised Papers. Berlin, Heidelberg: Springer Berlin Heidelberg; 2003. p. 41-53.

[40] Zhu X, Chi H, Niu B, Weidong Z, Zan L, Li H, editors. MobiCache: When k-anonymity meets cache. 2013 IEEE Global Communications Conference [GLOBECOM]; 2013 9-13 Dec. 2013.