A Privacy-Preserving Mechanism Based on Local Differential Privacy in Edge Computing

Mengnan Bi[1], Yingjie Wang[1,*], Zhipeng Cai[2], Xiangrong Tong[1]

[1] School of Computer and Control Engineering, Yantai University, Yantai 264005, China
[2] Department of Computer Science, Georgia State University, Atlanta, GA 30303, USA
* The corresponding author, email: towangyingjie@163.com

Abstract: With the development of Internet of Things (IoT), the delay caused by network transmission has led to low data processing efficiency. At the same time, the limited computing power and available energy consumption of IoT terminal devices are also the important bottlenecks that would restrict the application of blockchain, but edge computing could solve this problem. The emergence of edge computing can effectively reduce the delay of data transmission and improve data processing capacity. However, user data in edge computing is usually stored and processed in some honest-but-curious authorized entities, which leads to the leakage of users' privacy information. In order to solve these problems, this paper proposes a location data collection method that satisfies the local differential privacy to protect users' privacy. In this paper, a Voronoi diagram constructed by the Delaunay method is used to divide the road network space and determine the Voronoi grid region where the edge nodes are located. A random disturbance mechanism that satisfies the local differential privacy is utilized to disturb the original location data in each Voronoi grid. In addition, the effectiveness of the proposed privacy-preserving mechanism is verified through comparison experiments. Compared with the existing privacy-preserving methods, the proposed privacy-preserving mechanism can not only better meet users' privacy needs, but also have higher data availability.

Keywords: IoT; edge computing; local differential privacy; Voronoi diagram; privacy-preserving

I. INTRODUCTION

IN recent years, due to the contradictions between cloud computing model and inherent features of the Internet of Everything (IoE) [1], if we rely solely on this centralized computing processing method of cloud computing, it is no longer able to support applications running on IoT and massive data processing. In addition, cloud computing model cannot effectively solve some problems, such as cloud center load, data privacy-preserving [2] -[4] and other issues. Therefore, edge computing emerges as the times require, which combined with the existing cloud computing centralized processing model, can effectively solve the problem of big data processing at cloud center and edge of network [5]. Edge computing is a concept opposite to cloud computing. It is a new service model in which data or tasks could be computed on the edge of network near the data source [6]. In short, edge computing is a method of processing data physically close to where it was generated. However, location data usually contains a large amount of sensitive information. If there is no privacy-preserving mechanism, the location

Received: Jan. 7, 2020
Revised: Feb. 20, 2020
Editor: Shangguang Wang

data will be leaked, which will cause serious privacy problems and threaten users' privacy [7]. Therefore, privacy-preserving has become a very important issue in the edge environment [8]. Through solving this problem, the effectiveness of crowdsourcing platform could be improved better.

Edge computing has a tendency to decentralize, and another technology that also has a tendency to decentralize is blockchain technology [9]. From a technological perspective, blockchain involves many scientific and technological issues, such as mathematics, cryptography, the Internet, and computer programming. From an application point of view, in simple terms, blockchain is a distributed ledger and database, which is characterized by decentralization, immutability, leaving traces throughout, traceability, collective maintenance, and transparency. The limited computing power and available energy consumption of IoT terminal devices are the important bottlenecks that would restrict the application of blockchain, but edge computing could solve this problem.

Figure1 is the architecture of edge computing for IoT. It can be seen that in edge computing, the location data of mobile objects are collected by data collectors. There are two important assumptions: (1) mobile objects are willing to provide accurate location for data collectors; (2) data collectors are truthful and will not sell data maliciously or disclose data to a third party [10]. However, the above two assumptions are not valid in most cases. There are two reasons. First, a large number of data collectors are not truthful. In real life, many service providers sell users' personal data, which leads to serious problems of privacy leakage. Even if data collectors are truthful, a malicious attacker may attack the data collector's server, causing a large amount of personal data leakage. Second, as people pay more attention to personal privacy, more and more users are not willing to share their accurate location data, which also requires applications to maximize social welfare through some specific incentive mechanisms [11]-[14]. In addition to these, there are also some studies of incentive mechanisms that take into account the ability of participants to perform tasks, the data quality of the sensed tasks, or the credibility of the crowd workers [15]. According to the above analysis, users are more likely to want their data to be protected before leaving the device, even if data collectors cannot obtain user's accurate data.

This paper proposes a location data collection method that satisfies the local differential privacy to protect users' privacy.

Therefore, how to adopt effective location privacy-preserving mechanism to protect location data is an important research content of edge computing. Existing differential privacy [16], [17] technologies could be classified as centralized differential privacy (CDP) [18], [19] technology and local differential privacy (LDP) [20] technology. CDP believes that the third-party data collectors are truthful, which is not necessarily true in reality, and clearly does not meet our requirements for location privacy-preserving of edge computing. LDP, which has emerged in recent years, is the best way to solve this problem. In LDP model, clients first perturb the original data and then send it to the edge data center via edge network. Finally, edge data center makes analysis and statistics on the perturbed data to obtain an effective analysis result. In this process, even data collection center cannot get users' accurate location data, thus achieving personal

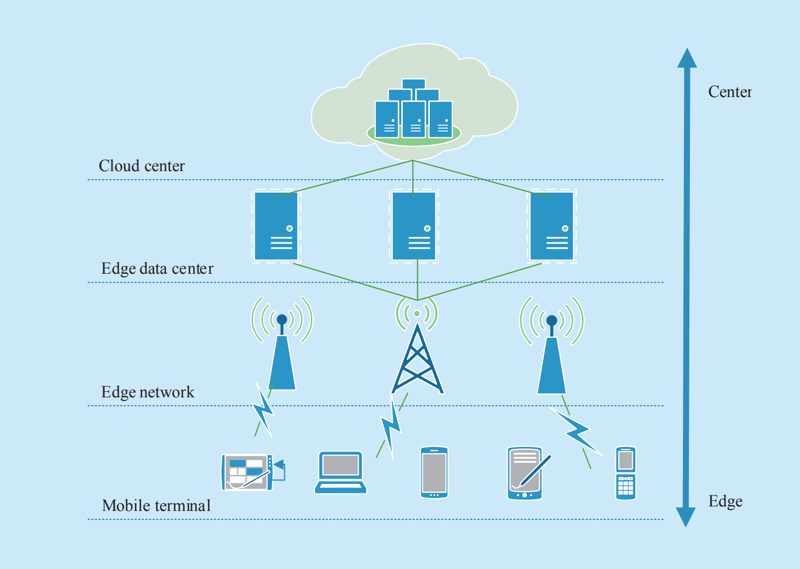


Fig. 1. *The architecture of edge computing for IoT.*

location privacy-preserving. In the process of data perturbation, we use the random response (W-RR) [21] disturbance mechanism to protect the privacy of original data with uncertainty response.

According to the above discussions, the effective location privacy-preserving mechanism of edge computing should be studied to solve following problems: (1) most methods are not sufficient to resist attacks by attackers with certain background knowledge; (2) prevent privacy attacks from untruthful third parties and provide more comprehensive protection for sensitive location data. Therefore, aiming at the existing problems, this paper studies location privacy-preserving mechanism in edge computing by combining LDP and Voronoi diagram [22].

This paper mainly studies the application of LDP in location data collection of edge computing. Specifically, the main contributions of this paper are summarized as follows.

1) Based on LDP model, a method of location data collection in edge computing is proposed, which satisfies LDP properties.

2) A road network space division method based on Voronoi diagram is proposed. The local differential privacy disturbance method is applied to each Voronoi grid to perturb original location data, and it is proved that our disturbance method satisfies LDP.

3) The method proposed in this paper is verified by comparison experiments, and it is proved that the LDP could not only effectively protect user's location privacy in edge computing, but also has better data availability.

The rest of this paper is organized as follows. Section 2 presents the related works. Section 3 introduces the proposed location privacy-preserving mechanism for edge computing. Section 4 illustrates the experimental settings, followed by the results analysis and discussion. Finally, Section 5 concludes this paper.

II. RELATED WORK

Edge computing is a type of distributed computing technology. It is a method of data processing at a location close to the terminal of an IoT device. In simple terms, it can be understood that in most cases, the device does not need to be connected to the cloud platform, and the intelligent control of IoT device can be achieved through local data calculation. In addition, edge computing can solve the bottleneck for the application of blockchain, that is, the limited computing power and available energy consumption of IoT terminal devices. Xu et al. [23] combined blockchain and mobile edge computing to solve the problems of untruthful network and network congestion.

User data in edge computing is typically stored and processed in some honest-but-curious authorized entities (edge data center, infrastructure provider), including multiple attributes such as user identity information, location information, and sensitive data [24]. The secondary goal of these honest-but-curious authorized entities is to obtain users' privacy information in order to achieve illegal profits and other purposes. But in this open ecosystem of edge computing, multiple trust domains are controlled by different infrastructure providers. In this case, it is impossible for users to know in advance whether a service provider is truthful. Problems that threaten users' privacy are likely to occur, such as data leakage or loss [6]. Therefore, privacy preserving has become a concerned research system in edge computing, which mainly includes data privacy-preserving, location privacy-preserving and identity privacy-preserving.

In this section, we will discuss related works from different location privacy-preserving technologies.

Location privacy-preserving technology could prevent user's accurate location from being leaked when a user obtains location-based services using location information. At present, location privacy-preserving could be divided into three main categories: anonymity, encryption and perturbation. For anonymous methods, k-anonymity and its extension models have far-reaching, and were widely researched in the field of privacy-preserving. K-anonymity was proposed by Samarati and Sweeney in 1998 [25]. It protects personal privacy by requiring a certain number (at least k) of indistinguishable records for the published data, so that an attacker cannot distinguish which specific individual the private information belongs to. For example, Zheng et al. [26] proposed a clustering algorithm based on k-anonymity location privacy-preserving model to eliminate outliers. In order to balance the conflict between privacy-preserving and query quality caused by location information's accuracy, the anonymous groups were established in this anonymity model. However, this kind of privacy-preserving methods failed to provide sufficient security for users. They constantly improved due to the emergence of new types of attacks. For example, in order to resist consistency attacks, l-diversity [27], t-closeness [28], (a, k)-anonymity [29], M-invariance [30] and other models were proposed. Wong et al.[31] proposed an m-confidentiality model to resist minimum attacks. Moreover, Rohilla et al. [32] used encryption technology to protect the security of users. Cai et al. [33] adopted position disturbance method to protect privacy information of users.

However, the above researches, such as k-anonymity [34], [35] and encryption technology, will consume a large amount of network bandwidth and computational overhead in practical applications. And they are not suitable for lightweight edge devices with limited resources. In addition, none of these methods considered attacks based on background knowledge, which cannot quantify the level of privacy-preserving. Nowadays, various operators and big data companies have rich user data. Large-scale data on Internet are interrelated. In addition, various data integration and fusion technologies are booming. At the same time, Internet has great convenience, making various types of information at your fingertips. The combination of these factors makes it is easy for attackers to obtain background knowledge. They can infer user's sensitive information by combining a large amount user-uploaded data [36], [37]. Therefore, researchers are trying to find a new privacy-preserving model. This model can resist all forms of attack when attackers have the greatest background knowledge. Differential privacy is a new privacy definition proposed by Dwork in 2006 to address this issue of privacy disclosure in statistical databases [38]. Differential privacy has strong privacy-preserving capability and does not rely on any background knowledge of attackers.

Traditional differential privacy technology centralizes raw data into a data center, and then publishes relevant statistical information satisfying differential privacy, i.e., CDP. Li et al. [39] proposed a privacy-preserving incentive scheme with a Truthful Third Party (TTP), which can protect users' privacy. Wang et al. [40] used differential privacy to establish an optimal model based on TTP. In this model, TTP can obtain some information from public datasets to better understand private datasets without breaking privacy. Wang et al. [41] proposed a location disturbance scheme based on differential privacy to protect location privacy with third-party geolocation services. It used TTP architecture to protect the location privacy of users. In the system architecture of [42], workers send their locations to a truthful Cellular Service Provider (CSP). It could achieve privacy-preserving based on TTP. Therefore, CDP's protection of sensitive information is always based on a premise: a truthful third-party data collector. In other words, it ensures that third-party data collectors will not steal or disclose sensitive information of users. However, in practical applications, even if third-party data collectors claim that they will not steal and disclose users' sensitive information, users' privacy is still not guaranteed. For example, some chat tools used every day may actually be monitoring our chat records, even if they claim that they will not disclose users' privacy information.

It can be seen that it is very difficult to find a truthful third-party data collection platform in practical applications, which greatly limits the application of CDP technology. According to the problem, in the scenario of untruthful third party data collectors, LDP technology emerges [43]. It inherits CDP to quantify privacy attacks' definition and refines sensitive personal information's protection. Specifically, it transfers the privacy process of data to each user, enabling users to individually process and protect personal sensitive information, that is, to perform more through privacy-preserving. For example, Wang et al. [44] proposed a method to protect the location of participants based on local differential privacy preference in response to the location privacy problem of participants in mobile crowd sensing. In [45], the authors proposed a location privacy-preserving task allocation framework based on geo-obfuscation to protect users' locations during task assignments. This framework does not require the involvement of any third-party entity.

Therefore, according to the above discussion, we apply LDP to the actual scenarios of edge computing. LDP is used to protect sensitive location data of each client in edge computing system and avoid disclosure of privacy by honest-but-curious authorized entities.

Nowadays, the concept of neural networks is very hot. Many scholars have done a lot of outstanding work on neural networks. For example, Jiang et al. [46] developed a new model based on neural networks by relying on NLP models for rich feature extraction. This model is called Mutual Attention Neural Network (abbreviated as MAN) to perform aspect-level sentiment classification tasks. Therefore, in future, we also look forward to using the knowledge of neural networks in the work of privacy protection. In addition, we also hope to apply the privacy-preserving work to the recommendation systems [47]. Recommendation system has become one of the main tools to search for users' interested papers. For example, Liu et al. [48] proposed a link prediction approach through combining time, keywords, and authors' information in order to optimize the existing paper citation network.

III. THE PROPOSED PRIVACY-PRESERVING MECHANISM FOR EDGE COMPUTING

In order to protect the privacy information of users effectively, a location data collection algorithm that satisfies LDP in edge computing is proposed. The proposed privacy-preserving mechanism is introduced in this section.

3.1 System structure

With the development of mobile devices, a large number of users hold a location data generated by their mobile devices. Untruthful servers want to know the number and distribution of mobile objects in a certain area. Due to privacy concerns, users do not send their precise location to servers, but send non-raw data that has been disturbed by our algorithm to protect users' location privacy.

The system structure of the proposed privacy-preserving mechanism is shown in Figure2. Cloud server sends Voronoi diagram division of a map to clients. Then clients will send their Voronoi diagram number of map to edge nodes. Edge nodes group users and feedback grouping information to clients. Finally, clients send their disturbed data via edge network to edge data center to complete location data collection.

3.2 Differential privacy technology

Previously, most privacy-preserving methods failed to define attack models and could not quantify the knowledge possessed by attackers [49]. According to this problem, differential privacy strictly defines an attack model and reduces privacy leakage's risk [50]. At present, differential privacy could be divided into two types: centralized differential privacy (CDP) and local differential privacy (LDP). In this paper, we adopt local differential privacy to propose a privacy-preserving mechanism for edge computing.

3.2.1 Centralized differential privacy technology

Traditional Differential Privacy (DP) technology, i.e., CDP, is the strongest privacy-preserving model currently known. However, CDP assumes that the third-party data collectors are truthful. It requires TTP to collect accurate data before privacy protection. But this assumption does not necessarily hold true in reality. For CDP technology, its privacy-pre-

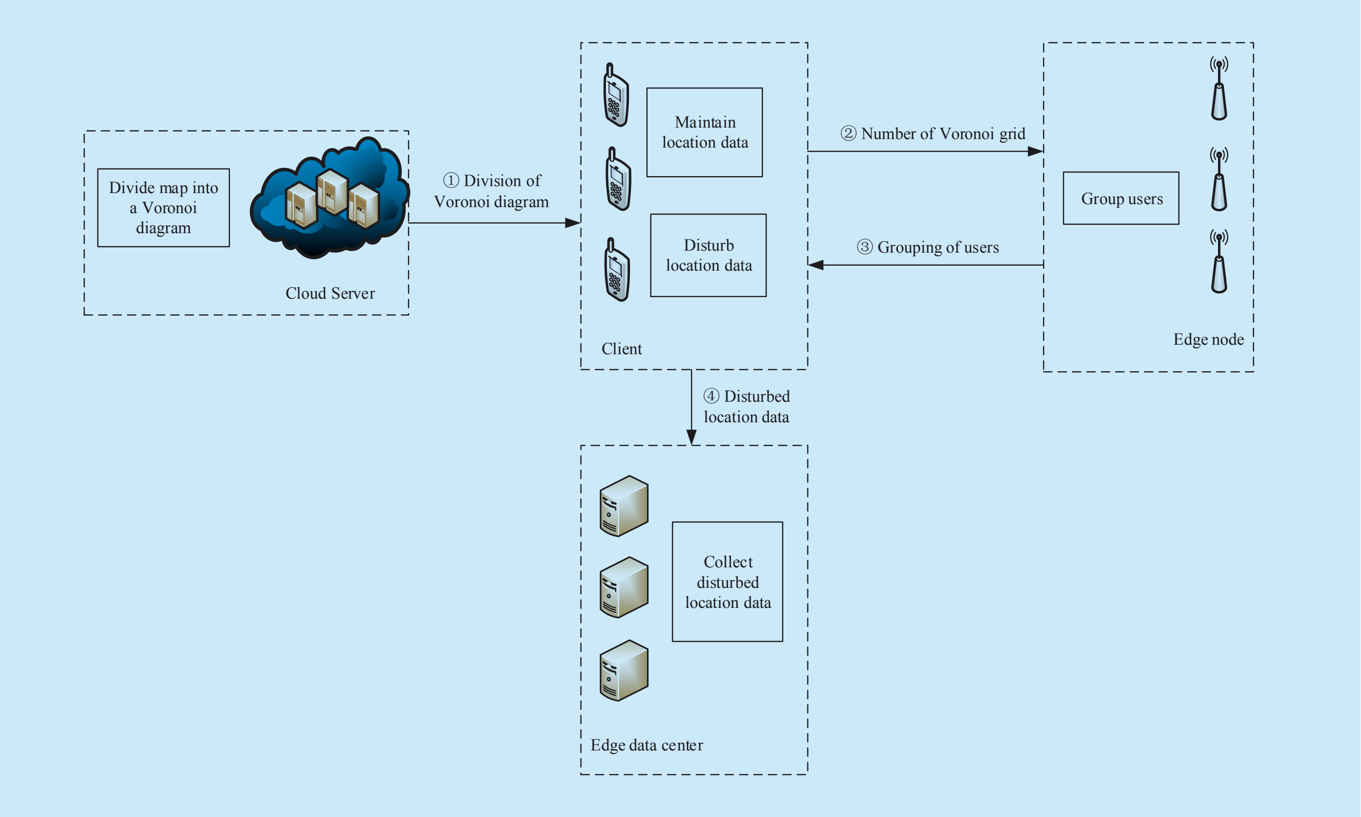


Fig. 2. *Location data collection system structure for privacy-preserving in edge computing.*

serving is performed by data collectors.

Suppose that the datasets D and D' have the same attribute structure, and the symmetric difference between them is denoted as $D\Delta D'$. $|D\Delta D'|$ represents the number of symmetric differences. If $|D\Delta D'| = 1$, then D and D' are called neighboring datasets.

Therefore, the formal definition of CDP is presented as follows.

Definition* 1**. (ε-CDP***) Given a random algorithm K, if any neighboring datasets D and D', and any output $S \subseteq Range(K)$ satisfies Eq.(1), the algorithm K satisfies ε-CDP [38].

$$\Pr[K(D) \in S] \leqslant e^{\varepsilon} \times \Pr[K(D') \in S]. \quad (1)$$

Differential privacy can ensure that adding or deleting a piece of data in the dataset will not affect the query output results. The choice of the random algorithm K is independent of the knowledge possessed by the attacker. As long as K satisfies Definition 1, the privacy of any data in the dataset can be protected, even if the attacker already has all the other data.

3.2.2 Local differential privacy technology

LDP is the improved method of CDP. The difference between LDP and CDP is that LDP does not require truthful data collectors. Therefore, data perturbation's function is transferred from data collectors to each user. Each user perturbs original data by privacy-preserving algorithms and then uploads the disturbance data to data collectors. For LDP technology, its privacy-preserving occurs on the client side. LDP has the characteristics of traditional differential privacy-preserving technology and expands with random response disturbance mechanism to resist privacy attacks from untruthful third-party data collectors.

The formal definition of LDP is presented as follows.

Definition* 2.** (ε-LDP***) Given n users, each user corresponds to a record. For a privacy algorithm M, its domain is $Dom(M)$, and range is $Ran(M)$. If algorithm M obtains the same output result $t^*(t^* \subseteq Ran(M))$ on any two records t and t' ($t, t' \in Dom(M)$) that satisfies Eq.(2), then M satisfies ε-LDP [43].

$$\Pr[M(t)=t^*] \leqslant e^{\varepsilon} \times \Pr[M(t')=t^*] \quad (2)$$

From Definition 2, it can be seen that LDP ensures that algorithm M satisfies ε-LDP by controlling the similarity of any two records' output. In short, according to a certain output result of privacy algorithm M, it is almost impossible to infer which record its input data is. In CDP, its privacy algorithm M is defined by neighbor dataset, so it requires truthful third-party data collectors to protect data analysis results. For LDP, each user can independently process individual data. The privacy process is transferred from data collectors to each client, so that no TTP's intervention is required. It also eliminates privacy attacks that may be caused by untruthful third-party data collectors.

LDP inherits two combined characteristics of CDP: sequence combinability and parallel combinability. Sequence combinability emphasizes that the privacy budget ε could be allocated in different steps. Parallel combinability could guarantee the privacy of algorithms that satisfy differential privacy on disjoint subsets of their datasets.

***Property* 1. (*Sequence Combinability*)** Given a dataset D and n privacy algorithms $\{M_1,...,M_n\}$, M_i ($1 \leq i \leq n$) satisfies ε_i-LDP[43]. Then the sequence combination of $\{M_1,...,M_n\}$ on D satisfies ε-LDP, where

$$\varepsilon = \sum_{i=1}^{n} \varepsilon_i. \quad (3)$$

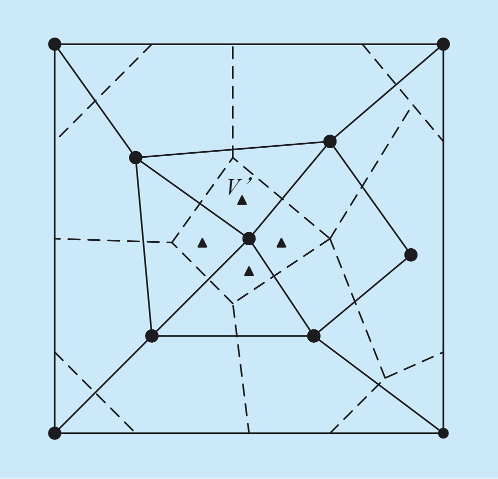


Fig. 3. *Division of road network space by a Voronoi diagram.*

***Property* 2. (*Parallel Combinability*)** Given a dataset D, divide it into n disjoint subsets, $D=\{D_1,...,D_n\}$, let M be any privacy algorithm that satisfies ε-LDP, then algorithm M satisfies ε-LDP on $\{D_1,...,D_n\}$[43].

3.3 Voronoi diagram

***Definition* 3. (*Voronoi Diagram*)** A Voronoi diagram consists of a set of continuous polygons that connect vertical bisectors of two adjacent line lines, also known as Tyson Polygon or Dirichlet Diagram. Among them, each continuous polygon is a Voronoi grid v. v contains only one point, called a generator. The distance from v's inner points to its generator is less than the distance to other generators, and the distance from points on the boundary to its generator is equal.

Figure3 shows the division of a road network space by a Voronoi diagram. Among them, solid black dots are road intersections on road network, solid lines indicate roads, and dotted lines indicate the boundary of Voronoi grids. In Voronoi grid v', there are 4 moving objects shown by four black triangles.

Each Voronoi grid v in Voronoi diagram has one generator. The distance from inner points of v to its generator is much smaller than the distance to other generators. We map each Voronoi grid generator in Voronoi diagram to an edge node of the region in edge computing. It satisfies the requirement that users can request services on the nearest edge of the network.

3.4 Location data collection algorithm satisfies LDP

Attackers may be from any party in our system structure. We assume that servers are all untruthful, that is, servers may also want to know mobile object's location. The biggest goal of attackers is to get mobile users' accurate location. Attack modes may include snooping, background knowledge association, collusion between servers and mobile users, etc.

The flow of location data collection algorithm that satisfies LDP in edge computing is summarized as follows:

1) Cloud server divides an entire map with a Voronoi diagram and stores Voronoi grids region and corresponding number v_i. Then it publishes the information to clients;

2) Each user sends its own Voronoi grid number v_i to the nearest edge node;

3) Edge nodes divide users in the same Voronoi grid into a group and send the group message to clients;

4) According to LDP mechanism, we disturb location data within the group and send disturbance data to the edge data center.

This paper assumes that edge nodes are untruthful. Edge nodes know which Voronoi grid a user is in, but does not know user's accurate location. For a user, its Voronoi grid is its security area.

3.4.1 Road network division based on Voronoi diagram

In this paper, we use Delaunay triangulation algorithm to divide network space into Voronoi grids. Generator point set $P=\{p_1,p_2,...,p_n\}$ is road intersections in road network space, which could be consider as edge nodes, as shown by solid black dots in Figure3.

Delaunay triangulation algorithm means that when generating a Voronoi diagram, the first step is to make its dual Delaunay triangulation network. Then find the circumscribed circle center of each triangle in triangle network. Finally, we connect circumcircle centers of adjacent triangles to form a polygon network, which takes each triangle vertex as its generator. The process is shown in Figure4.

Algorithm 1 shows our basic steps of generating a Voronoi diagram. When generating a Voronoi diagram, the first step is to generate a dual element Delaunay triangulation DT based on the generator dataset P (step 1-2). Then find the circumscribed circle center c_i of each triangle t_i in triangle network DT and get circumcenters point set C (step 3-6). Finally, for each c_i in C, connect the circumcenter c_i of adjacent triangles to get the Voronoi diagram V (step 7-10).

Delaunay triangulation has the following characteristics:

1) Empty circle: no other points are included in the circumcircle of any triangle.

2) Closest: a triangle is formed with the nearest three points, and each line segment (sides of this triangle) does not intersect.

3) Uniqueness: no matter where you start building from the region, you will end up with consistent results.

4) Optimality: if diagonals of the convex quadrilateral formed by any two adjacent triangles are interchangeable, then the smallest of these six internal angles of the two triangles does not become larger.

5) The most rule: if the minimum angle of each triangle in triangulation network is arranged in ascending order, the value obtained by the Delaunay triangulation's arrangement is the largest.

6) Regional: adding, deleting, and moving a vertex will only affect the adjacent triangles.

7) Shell with convex polygons: the outermost boundary of triangulation network forms

Algorithm 1. Voronoi diagram generation algorithm.

```
Input: Generator dataset $P=\{p_1,p_2,...,p_n\}$
Output: Voronoi diagram $V$
1:  Generate a dual element Delaunay triangulation $DT$
2:      based on $P$
3:  for each triangle $t_i$ in $DT$
4:      find the circumcenter $c_i$ of $t_i$
5:      get circumcenters point set $C$
6:  end for
7:  for each $c_i$ in $C$
8:      connect the circumcenter $c_i$ of adjacent triangles
9:  end for
10: Get Voronoi diagram $V$
```

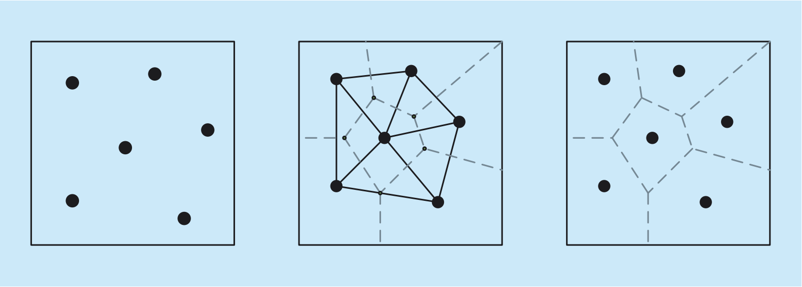


Fig. 4. *Delaunay triangulation algorithm generates a Voronoi diagram.*

a convex polygonal outer shell.

The key to establish a Voronoi diagram is to reasonably connect discrete data points into a triangulation network, that is, to construct a Delaunay triangulation network. Figure5 shows the Delaunay steps of generating a Delaunay triangulation network:

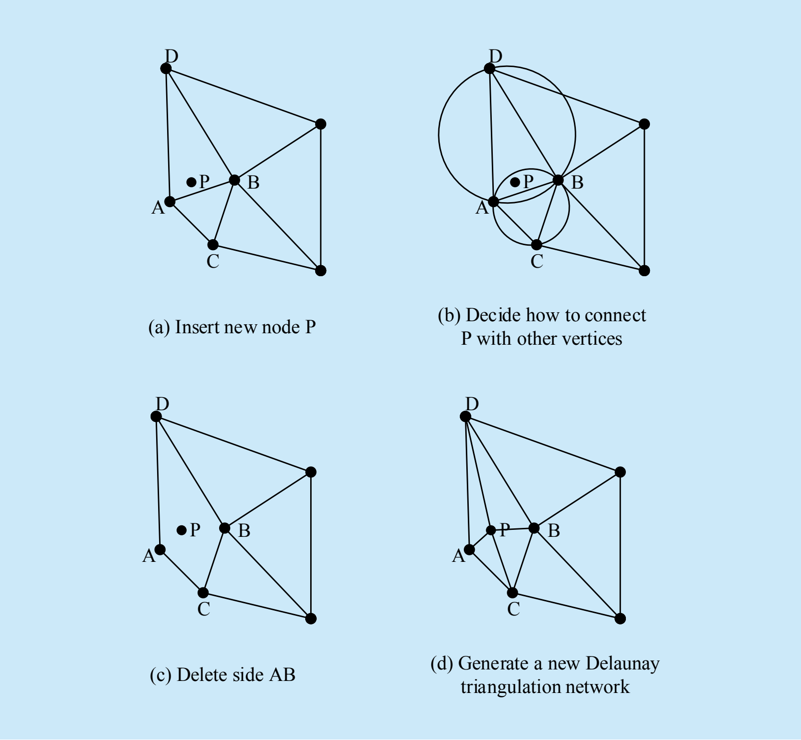
(a) insert a new point in this grid;

(b) associate the triangle to draw a circumcircle, record all triangles whose circumcircles contain new points;

(c) delete common edges that affect triangles;

(d) generate a new Delaunay triangulation network.

Road network division based on a Voronoi diagram is completed by cloud server, and division information is sent to clients. Then every client knows its Voronoi grid number and sends this number to the nearest edge node. Edge nodes divide moving objects in the same Voronoi grid into a group according to the received Voronoi grid number.



(a) Insert new node P

(b) Decide how to connect P with other vertices

(c) Delete side AB

(d) Generate a new Delaunay triangulation network

Fig. 5. *Delaunay steps of generating a Delaunay triangulation network.*

3.4.2 Disturbance of location data satisfies ε-LDP

Cloud server informs each client of packet data. Packet data could be represented as $G=\{gid,\ N,\ v_i,<a_1b_1,a_2b_2,\ldots,a_mb_m>\}$, where *gid* denotes group number, *N* is the number of moving objects in this group, v_i denotes this group of objects' Voronoi grid number, $<a_1b_1,a_2b_2,\ldots,a_mb_m>$ is the boundary information of this Voronoi grid. After a client receives packet data *G* sent by cloud server, it generates a vector $L=\{loc_0,\ loc_1,\ldots,\ loc_{n-1}\}$, where loc_0 is user's real location, loc_1, loc_2,.., loc_{n-1} are other false locations randomly generated by this user within v_i boundary.

Our disturbance method needs to satisfy ε-LDP. At present, random response mechanism is a mainstream technology for LDP. According to random response mechanism, given LDP's privacy parameter ε, the probability that each user sends its own real position or a position in *n*-1 false positions is shown by

$$P(loc_i \mid loc_i') = \begin{cases} \dfrac{e^{\varepsilon}}{n-1+e^{\varepsilon}}, loc_i = loc_i' \\ \dfrac{1}{n-1+e^{\varepsilon}}, loc_i \neq loc_i' \end{cases}. \quad (4)$$

Table I summarizes the notations used in our presentation.

Our location data collection algorithm in edge computing satisfies ε-LDP. The edge computing location data collection algorithm is shown by Algorithm 2. In Algorithm 2, the cloud server first uses the Voronoi diagram *V* to divide the map into a road network map *G* (*V*, *E*) and sends the packet data $G_i=\{gid,N,v_i,\langle a_1b_1,a_2b_2,\ldots,a_mb_m\rangle\}$ to each user u_i (step 1-3). Then every client u_i knows its Voronoi grid number v_i and sends this number to the nearest edge node p_j (step 5). Edge node p_j divides moving object u_i in the same Voronoi grid v_i into a group G_i according to the received Voronoi grid number v_i (step 6). Every u_i will generate some false locations loc_i' in v_i and send loc_i or one of loc_i' to its nearest p_j with $P(loc_i \mid loc_i')$ (step 7-11).

The privacy-preserving degree of Algorithm 2 satisfies Theorem 1.

***Theorem* 1.** For any moving object's position loc_i, given privacy-preserving parameter ε, the above disturbance method satisfies ε-LDP.

Proof. According to the definition of LDP, it is necessary to prove

$$\frac{\Pr[LP(loc_i,N,\varepsilon)=loc_i]}{\Pr[LP(loc_i,N,\varepsilon)=loc_i']}\leqslant e^{\varepsilon} \tag{5}$$

to indicate that privacy algorithm satisfies ε-LDP, where N represents total number of mobile users in Voronoi grids. According to the generation method of N in privacy algorithm, if N includes m positions, only one position is user's real position, and the remaining positions are false positions within its group. According to the generation rule, the probability that loc_i sends its real position is

$$\Pr[LP(loc_i,N,\varepsilon)=loc_i]=\frac{e^{\varepsilon}}{m-1+e^{\varepsilon}}, \tag{6}$$

and the probability of sending its false position is

$$\Pr[LP(loc_i,N,\varepsilon)=loc_i']=\frac{1}{m-1+e^{\varepsilon}}, \tag{7}$$

then

$$\frac{\Pr[LP(loc_i,N,\varepsilon)=loc_i]}{\Pr[LP(loc_i,N,\varepsilon)=loc_i']}=e^{\varepsilon} \tag{8}$$

is verified.

IV. Performance Evaluation

In this section, we conduct comparison experiments to evaluate the effectiveness of the proposed data collection method in edge computing. In experimental results, LDP represents the proposed mechanism based on local differential privacy technology. We evaluate the changes in loss of the Quality-of-Service (QoS) under different privacy budgets ε and different privacy levels. Then, in order to verify the effectiveness of LDP, it is compared with CDP mechanism with Laplace noise and Gaussian white noise, and k-anonymity mechanism respectively [51].The hardware environment of the experiments is equipped with 4GB RAM. The experiments are conducted on Win 7 OS. The experimental platform is MATLAB 2016a.

4.1 Experimental datasets

The real-world dataset Gowalla [52] is utilized in this paper. Gowalla dataset is a user location dataset, which is obtained from a location-based social networking website Gowalla, where users share their locations by checking-in. The collection period is from Feb. 2009 to Oct. 2010, which mainly includes user ID, check-in time, location coordinates, and location ID, with approximately 6,442,890

Table I. *Summary of notations.*

Symbol	Definition
gid	Group number
N	Total number of mobile users within a group
v_i	Voronoi grid number for a group of users
$<a_1b_1,a_2b_2,...,a_mb_m>$	Boundary information for a Voronoi grid
G_i	Packet data
loc_i	User's real location
loc_i'	User's false locations within v_i
$G(V,E)$	Road network diagram
ε	Local differential privacy parameter
V	Voronoi diagram
$P=\{p_1, p_2,..., p_n\}$	Edge node dataset
$U=\{u_1, u_2,..., u_m\}$	User dataset

Algorithm 2. Edge computing location data collection algorithm satisfies ε-LDP.

```
Input: $G(V,E)$, $\varepsilon$, $V$, $P$, $U$
Output: Location collection $L=\{loc, loc'\}$
Divide the road network map $G(V, E)$ with $V$
for each user $u_i$ in $U$
    Cloud server sends $G_i=\{gid, N, v_i, <a_1b_1, a_2b_2,..., a_mb_m>\}$ to $u_i$
    for each edge node $p_j$ in $P$
        $u_i$ informs its nearest $p_j$ of the $v_i$
        $p_j$ divides $u_i$ in the same $v_i$ into a group $G_i$
        $u_i$ loads its own real location data $loc_i$
        $u_i$ generates false locations data $loc_i'$ in $v_i$
        $L \leftarrow \{loc_i, loc_i'\}$
        $u_i$ sends $loc_i$ or one of $loc_i'$ to its nearest $p_j$ with probability
        $P(loc_i | loc_i')$
    end for
end for
```

records.

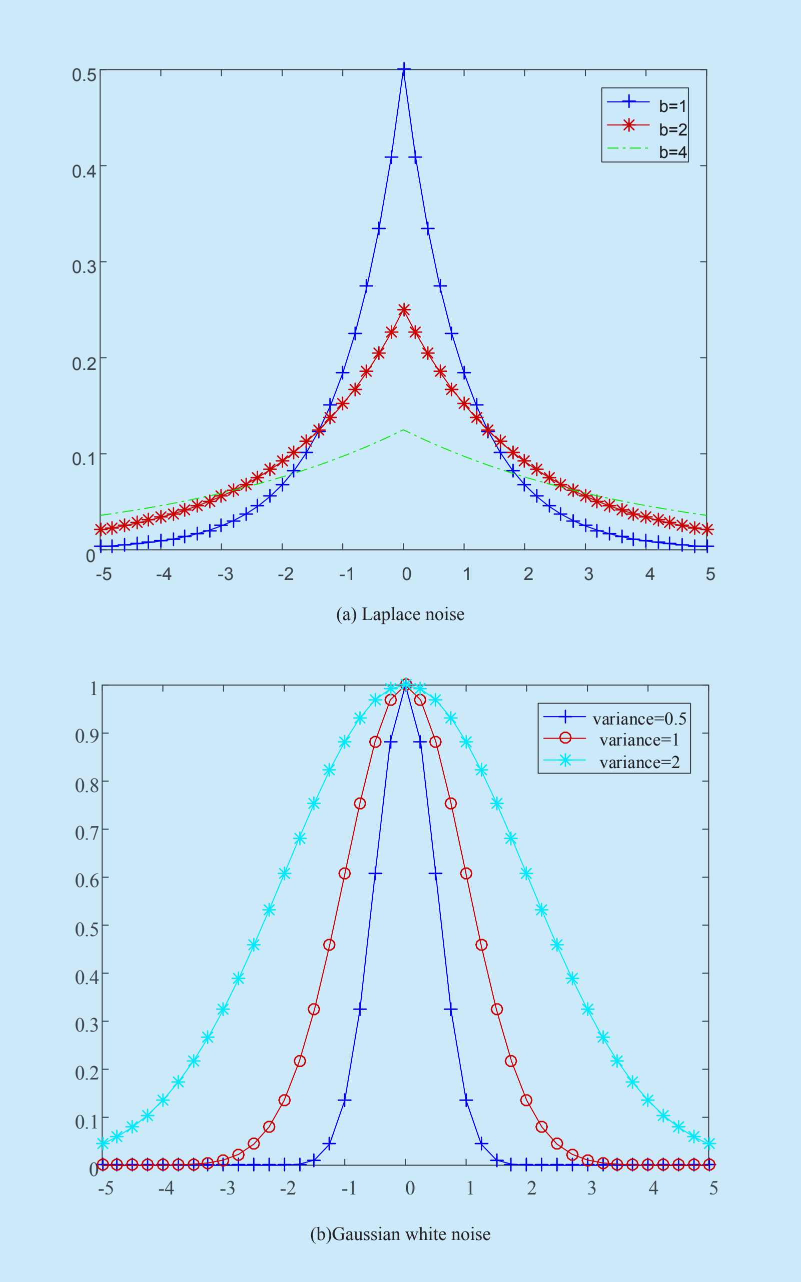
4.2 Utility metric

This paper uses the level of privacy-preserving (*PL*) and loss of service quality (*Qloss*) to evaluate the performances of privacy-preserving methods.

4.2.1 Level of privacy-preserving

In this paper, *h* represents the probability that an attacker will succeed, so *PL* could be expressed by

$$PL = 1 - h. \tag{9}$$



(a) Laplace noise

(b)Gaussian white noise

Fig. 6. *The probability density functions.*

a) In Voronoi diagram-based LDP mechanism, a user has a real position *l* and *n* false positions $\{l_1^{'}, \ldots, l_n^{'}\}$. The user may respond to any of these *n*+1 positions, so *h* could be expressed by

$$h_{LDP} = \frac{1}{n+1}. \tag{10}$$

b) In CDP mechanism with Laplace noise, Laplace mechanism [53] implements *ε*-differential privacy preserving. Adding Laplace-distributed random noise *Lap*(Δ*f*/*ε*) to the data, where Δ*f* indicates the sensitivity and *ε* is the privacy budget. The calculation method of Δ*f* is shown by

$$\Delta f = \max_{D_1, D_2} \| f(D_1) - f(D_2) \|. \tag{11}$$

D_1 and D_2 represent any two neighboring datasets, and *f*(*x*) is the real query result. There is at most one record difference between these two datasets. Therefore, in CDP-Laplace algorithm, *h* could be expressed by

$$h_{CDP} = 1 - \Delta f. \tag{12}$$

In addition, $b = \Delta f / \varepsilon$ is a scale parameter. From Figure 6(a), it can be seen that the added noise is proportional to Δ*f* and inversely proportional to *ε*. Therefore, the larger Δ*f* is, the larger the added noise is, but h_{Lap} is smaller.

c) Similarly, in CDP mechanism with Gaussian white noise, we utilize Gaussian white noise *Gau*(Δ*f*/*ε*) to achieve *ε*-differential privacy preserving. Gaussian white noise is statistical noise having a Probability Density Function (PDF) that obeys normal distribution, i.e., Gaussian distribution [50]. Gaussian white noise obeys $N\left(0, \sigma^2\right)$ normal distribution, where σ^2 is calculated by

$$\sigma^2 = \left(\frac{\Delta f}{\varepsilon}\right)^2. \tag{13}$$

The noise function is shown by

$$Gau(\sigma) = \frac{1}{\sqrt{2\pi}\sigma} \exp(-\frac{x^2}{2\sigma^2}). \tag{14}$$

From Figure6(b), it can be seen that the added noise is proportional to Δ*f*, and inversely proportional to *ε*. In CDP-Gaussian white algorithm, *h* could be represented by

$$h_{Gau} = 1 - \Delta f. \tag{15}$$

d) The k-anonymity mechanism publishes central location data with *k* location records through generalization and cloaking technology. Because there are at least *k* position records for the same published central position data, observers cannot connect to users' position records through the central position data. The implementation of k-anonymity model makes it impossible for an attacker to identify users through central location data with a confidence higher than 1/*k*. Therefore, *h* could be expressed by

$$h_{kanony} = \frac{1}{k}. \tag{16}$$

4.2.2 Loss of service quality

a) In Voronoi diagram-based LDP mechanism, we consider an user's *Qloss* as the average of the sum of *n* error distances *d*(*l*,*l*') between this user's *n* false locations and its real location. Suppose there are *p* Voronoi grids and *N* users, and each Voronoi grid has *m* users. The *Qloss* of *N* users is shown by

$$Qloss_{LDP} = \sum_{z=1}^{p} \sum_{j=1}^{m} \frac{\sum_{i=1}^{n} d_i(l_i, l_i')}{n}. \tag{17}$$

In CDP-Laplace mechanism, a user's *Qloss* could be regarded as the error distance between this user's real position *l* and its false position *l*'. Eq.(18) represents the *Qloss* of *N* users in CDP-Laplace mechanism.

$$Qloss_{Lap} = \sum_{i=1}^{N} d_i(l, l') \tag{18}$$

b) Similarly, in CDP-Gaussian white mechanism, Eq.(19) could be used to represent the *Qloss* of *N* users.

$$Qloss_{Gau} = \sum_{i=1}^{N} d_i(l, l') \tag{19}$$

c) In k-anonymity mechanism, a user's *Qloss* could be regarded as the error distance between this user's real location *l* and its published central location *lc*'. Therefore, the *Qloss* of *N* users is shown by Eq.(20) in k-anonymity mechanism.

$$Qloss_{kanony} = \sum_{i=1}^{N} d_i(l, lc') \tag{20}$$

4.3 Experimental settings

We randomly draw 50 points from Gowalla dataset as road intersections (edge nodes) to draw the Voronoi diagram. Then, the location points are randomly taken from the dataset as users' real location points, and each user randomly generates a false position in the Voronoi grid where it is located.

4.4 Comparison Experiments

In the comparison experiments, three different privacy-preserving methods were compared. In the same dataset, we set the three algorithms' privacy-preserving level as *PL*=75%, and then change different privacy budgets *ε* to observe the effectiveness of *Qloss*, as shown in Figure7. From Figure 7, it can be seen that among the three algorithms, with the increase of *ε*, *Qloss* tends to decrease. This is because that in the Voronoi diagram-based LDP mechanism, as *ε* increases, the higher the probability *p* that a user responds to its real location, the higher the availability of data. In the two

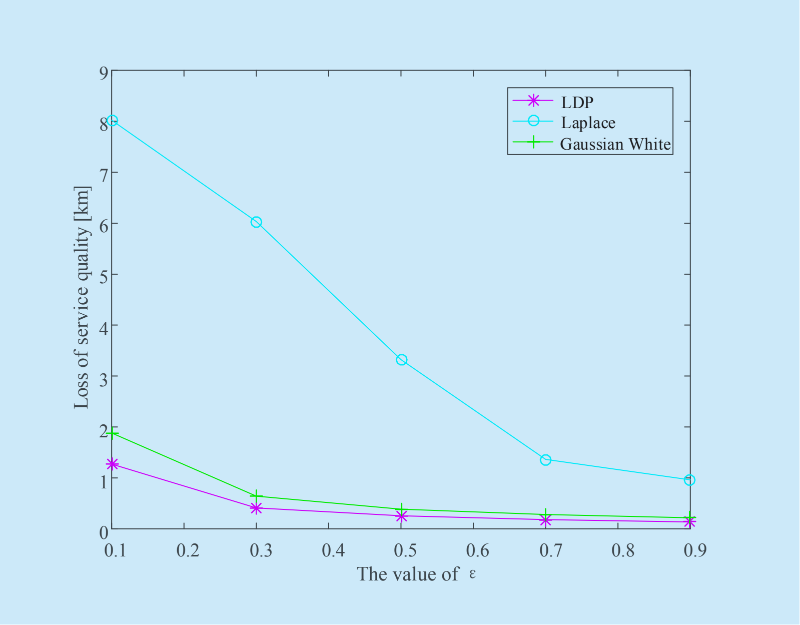


Fig. 7. *The comparison results of Qloss under different ε.*

mechanisms of Laplace noise and Gaussian white noise, as ε increases, the added noise decreases, so *Qloss* is reduced. From the experimental results, we can see that the proposed LDP mechanism has the least *Qloss*, so the performance of the algorithm is better than the other two mechanisms. Because k-anonymity mechanism does not have the same parameters as Laplace noise mechanism, Gaussian white noise mechanism, and LDP mechanism, we did not compare these three mechanisms with k-anonymity mechanism in this experiment. In future works, more algorithm mechanisms will be compared with LDP mechanism to discover more deficiencies in LDP mechanism and improve them.

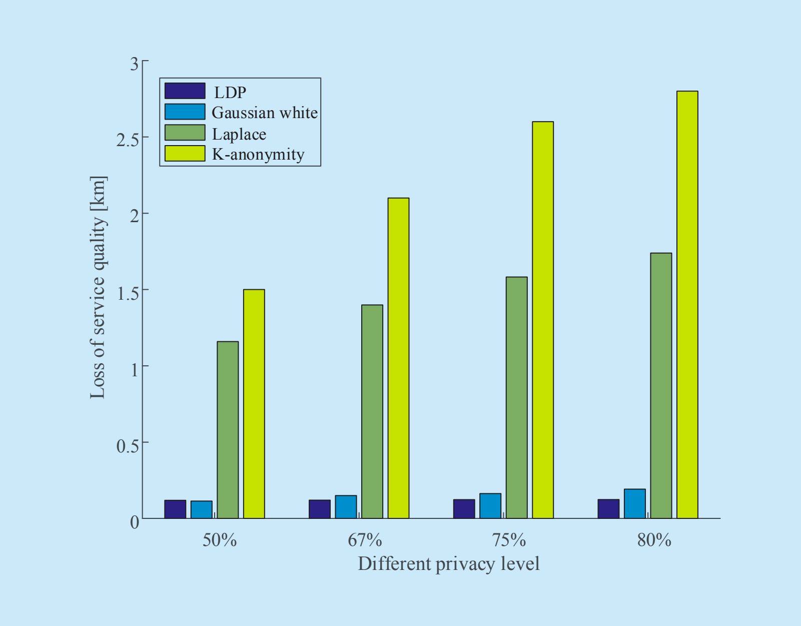


Fig. 8. *The comparison results of Qloss under different privacy levels.*

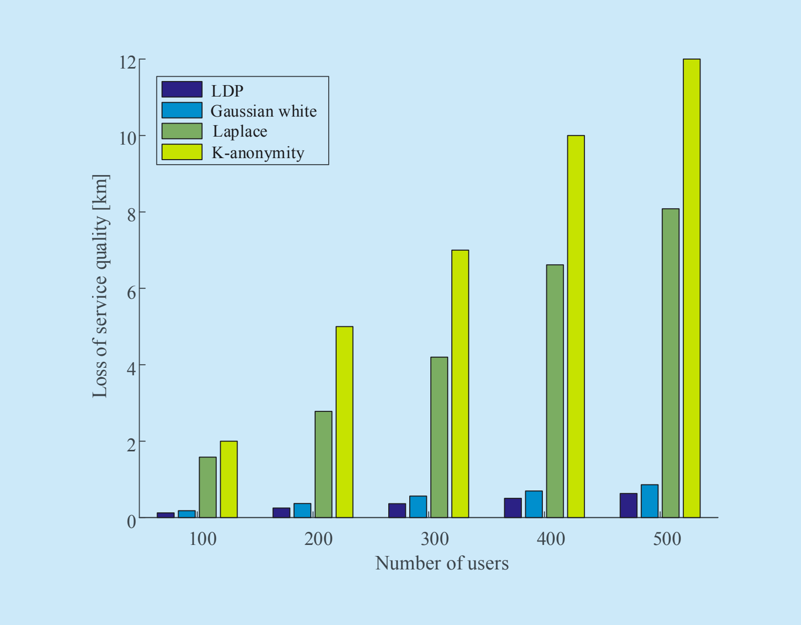


Fig. 9. *The comparison results of Qloss under different datasets.*

Figure 8 shows the comparison results of *Qloss* under different privacy levels in the same dataset. We randomly take 100 location points as the user's real locations, and observe the changes of *Qloss* by changing *PL*. From the experimental results, it can be seen that the values of *Qloss* of k-anonymity mechanism and Laplace noise mechanism are too large. Therefore, the quality of service for users cannot be guaranteed. In addition, the *Qloss* of Gaussian White noise mechanism increases with the increase of *PL*. Therefore, the higher the *PL*, the greater the *Qloss* of these three mechanisms. However, it can be seen that the proposed LDP has the best performance on *Qloss* through compared with other three algorithms. In addition, the *Qloss* of LDP is basically unchanged with the increase of privacy level. Therefore, in the same dataset, the *PL* has almost no effect on the *Qloss* of LDP mechanism.

Figure 9 shows the comparison results of *Qloss* in different numbers of users with the same *PL*. We randomly take 100, 200, 300, 400, 500 location points in Gowalla dataset as the user's 5 reallocation datasets, and observe the changes of *Qloss* under the same *PL*. From the experimental results, we can see that with the increase of users, the *Qloss* of each mechanism increases. Among them, Laplace noise mechanism and k-anonymity mechanism have a larger increase on *Qloss*. In addition, although the growth rate of the Gaussian white noise mechanism and LDP mechanism is small, LDP mechanism has the least *Qloss*. Therefore, by comparing with the other three mechanisms, we find that the proposed Voronoi diagram-based LDP mechanism has less *Qloss* and better algorithm performance.

V. Conclusions

In order to improve the efficiency of big data processing, edge computing is combined with cloud computing is an effective solution. In addition, how to establish an effective privacy-preserving mechanism has become increasingly important. LDP is an emerging privacy-preserving model after CDP. It breaks the assumption of truthful third-party data collectors in CDP and performs data privacy processing on the side of users. This paper proposes a location data collection method that satisfies LDP. A Voronoi diagram is used to divide the road network space to determine the Voronoi grid region where the edge nodes are located. The location data in each Voronoi grid is disturbed by random disturbance mechanism. The performance of the proposed Voronoi diagram-based location privacy-preserving mechanism is evaluated by comparing with three classical mechanisms respectively. Through comparison experiments, it is verified that the proposed LDP not only meets users' privacy needs, but also has higher data availability. However, since each user has to generate multiple fake locations to protect his real location, this mechanism may consume more resources.

In future work, we will continue to improve the privacy-preserving model and make the model to be in better accordance with the self-characteristics of edge computing. In addition, the convergence of edge computing and blockchain is the trend of IoT. We will focus on this issue to further research new and more effective privacy-preserving mechanism.

References

[1] W. Shi, H. Sun, J. Cao, Q. Zhang, and W. Liu, "Edge computing-an emerging computing model for the internet of everything era," *Journal of computer research and development*, vol. 54, no. 5, 2017, pp. 907–924.

[2] L. Qi, X. Zhang, W. Dou, and Q. Ni, "A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, 2017, pp. 2616-2624.

[3] Z. Cai, and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, 2020, pp. 766-755.

[4] X. Zheng, and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial IoTs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, 2020, pp. 968-979..

[5] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, 2016, pp. 637–646.

[6] J. Zhang, Y. Zhao, B. Chen, F. Hu, and K. Zhu, "Survey on data security and privacy-preserving for the research of edge computing," *Journal on Communications*, vol. 39, no. 3, 2018, pp. 1–21.

[7] L. Zhang, Z. Cai, and X. Wang, "Fakemask: A novel privacy preserving approach for smartphones," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, 2016, pp. 335–348.

[8] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A Two-stage Locality-Sensitive Hashing Based Approach for Privacy-Preserving Mobile Service Recommendation in Cross-Platform Edge Environment," *Future Generation Computer Systems*, vol. 88, 2018, pp. 636-643.

[9] Z. Zheng, S. Xie, H.N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, 2018, pp. 352–375.

[10] Z. Huo, K. Zhang, P. He, and Y. Wu, "Crowdsourcing location data collection for local differential privacy," *Journal of Computer Applications*, vol. 39, no. 3, 2019, pp. 763–768.

[11] Y. Wang, Z. Cai, G. Yin, Y. Gao, X. Tong, and G. Wu, "An incentive mechanism with privacy protection in mobile crowdsourcing systems," *Computer Networks*, vol. 102, 2016, pp. 157–171.

[12] Y. Wang, Z. Cai, Z.H. Zhan,Y.J. Gong, and X. Tong, "An optimization and auction-based incentive mechanism to maximize social welfare for mobile crowdsourcing," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, 2019, pp. 414–429.

[13] J. Xu, S. Wang, N. Zhang, F. Yang, and X. Shen, "Reward or penalty: Aligning incentives of stakeholders in crowdsourcing," *IEEE Transactions on Mobile Computing*, vol. 18, no. 4, 2019, pp. 974–985.

[14] Y. Wang, Y. Gao, Y. Li, and X. Tong, "A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems," *Computer Networks*, vol. 171, 2020, p. 107144.

[15] N. Jiang, D. Xu, J. Zhou, H. Yan, T. Wan, and J. Zheng, "Toward optimal participant decisions with voting-based incentive model for crowd sensing," *Information Sciences*, vol.512, 2020, pp. 1-17.

[16] C. Dwork, “Differential privacy,”*Proc. International Colloquium on Automata, Languages and Programming* (*ICALP*), 2006, pp.1–12.

[17] Z. Cai, X. Zheng, and J. Yu, “A differential-private framework for urban traffic flows estimation via taxi companies,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, 2019, pp. 6492–6499.

[18] Z. Chi, Y. Wang, Y. Huang, and X. Tong, “The novel location privacy-preserving CKD for mobile crowdsourcing systems,” *IEEE Access*, vol. 6, 2018, pp. 5678–5687.

[19] Z. Cai, and Z. He, “Trading private range counting over big IoT data,” *Proc. IEEE International Conference on Distributed Computing Systems* (*ICDCS*), 2019, pp. 144–153.

[20] H. Shin, S. Kim, J. Shin, and X. Xiao, “Privacy enhanced matrix factorization for recommendation with local differential privacy,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 9, 2018, pp. 1770–1782.

[21] S. L. Warner, “Randomized response: A survey technique for eliminating evasive answer bias,” *Journal of the American Statistical Association*, vol. 60, no. 309, 1965, pp. 63–69.

[22] L. Sun, Y. Luo, Y. Yu, and X. Ding, “Voronoi diagram generation algorithm based on delaunay triangulation,” *Journal of Software*, vol. 9, no. 3, 2014, pp. 777–784.

[23] J. Xu, S. Wang, B. K. Bhargava, and F. Yang, “A blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, 2019, pp. 3538–3547.

[24] Y. Hu, Y. Wang, Y. Li, and X. Tong, “An incentive mechanism based on multi-attribute reverse auction in mobile crowdsourcing,” *Sensors*, vol. 18, no. 10, 2018, p. 3453.

[25] P. Samarati, and L. Sweeney, “Generalizing data to provide anonymity when disclosing information,” *Proc. ACMSIGMOD Conference on Principles of Database Systems* (*PODS*), vol. 98, 1998, pp.188.

[26] L. Zheng, H. Yue, Z. Li, X. Pan, M. Wu, and F. Yang, “K-anonymity location privacy algorithm based on clustering,” *IEEE Access*, vol. 6, 2018, pp. 28328–28338.

[27] Y.Sei, H. Okumura, T. Takenouchi, and A. Ohsuga, “Anonymization of sensitive quasi-identifiers for l-diversity and t-closeness,” *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 4, 2019, pp. 580–593.

[28] S. Saraswathi, and K. Thirukumar, “Enhancing utility and privacy using t-closeness for multiple sensitive attributes,” *Advances in Natural and Applied Sciences*, vol. 10, no. 5, 2016, pp. 6–13.

[29] H. Li, F. Guo, W. Zhang, J. Wang, and J. Xing, “(a, k)-anonymous scheme for privacy-preserving data collection in IoT-based healthcare services systems,” *Journal of medical systems*, vol. 42, no. 3, 2018, p. 56.

[30] X. Xiao and Y. Tao, “M-invariance: Towards privacy preserving republication of dynamic datasets,” *Proc. ACM SIGMOD International Conference on Management of Data* (*MOD*), 2007, pp. 689–700.

[31] R. C.W. Wong, A. W.C. Fu, K. Wang, and J. Pei, “Minimality attack in privacy preserving data publishing,” *Proc. International Conference on Very Large Data Bases* (*VLDB*), 2007, pp. 543–554.

[32] A. Rohilla, M. Khurana, and L. Singh, “Location privacy using homomorphic encryption over cloud,” *International Journal of Computer Network and Information Security*, vol. 9, no. 8, 2017, pp. 32–40.

[33] Z. Cai, Z. He, X. Guan, and Y. Li, “Collective data-sanitization for preventing sensitive information inference attacks in social networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, 2018, pp. 577–590.

[34] J. Wang, Z. Cai, and J. Yu, “Achieving personalized k-anonymity based content privacy for autonomous vehicles in CPS,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, 2020, pp. 4242–4251.

[35] Y. Wang, Y. Li, Z. Chi, and X. Tong, “The truthful evolution and incentive for large-scale mobile crowd sensing networks,” *IEEE Access*, vol. 6, 2018, pp. 51187–51199.

[36] Z. He, Z. Cai, and J. Yu, “Latent-data privacy preserving with customized data utility for social network data,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, 2018, pp. 665–673.

[37] B. Zhao, Y. Wang, Y. Li, Y. Gao, and X. Tong, “Task allocation model based on worker friend relationship for mobile crowdsourcing,” *Sensors*, vol. 19, no. 4, 2019, p. 921.

[38] C. Dwork, “Differential privacy: A survey of results,” *Proc. International Conference on Theory and Applications of Models of Computation* (*TAMC*), 2008, pp. 1–19.

[39] Q. Li and G. Cao, “Providing privacy-aware incentives for mobile sensing,” *Proc. IEEE International Conference on Pervasive Computing and Communications* (*PerCom*), 2013, pp. 76–84.

[40] M. Wang, Z. Ji, H.E. Kim, S. Wang, L. Xiong, and X. Jiang, “Selecting optimal subset to release under differentially private m-estimators from hybrid datasets,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 3, 2018, pp. 573–584.

[41] Y. Wang, H. Zhang, and S. Su, “Enhancing location privacy for geolocation service through perturbation,” *Proc. International Conference on Cloud Computing and Security* (*ICCS*), 2018, pp. 502–511.

[42] H. To, G. Ghinita, L. Fan, and C. Shahabi, “Differentially private location protection for worker datasets in spatial crowdsourcing,” *IEEE Transactions on Mobile Computing*, vol. 16, no. 4, 2017, pp. 934–949.

[43] Q.Q. Ye, X.F. Meng, M.J. Zhu, and Z. Huo, “Survey on local differential privacy,” *Journal of Software*, vol. 29, no. 7, 2018, pp. 1981–2005.

[44] J. Wang, Y. Wang, G. Zhao, and Z. Zhao, “Location protection method for mobile crowd sensing based on local differential privacy preference,” *Peer-to-Peer Networking and Applications*, vol.12, no.5, 2019, pp. 1097-1109.

[45] L. Wang, D. Yang, X. Han, T. Wang, D. Zhang, and X. Ma, “Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation,” *Proc. International Conference on World Wide Web*, 2017, pp.627-646.

[46] N. Jiang, F. Tian, J. Li, X. Yuan, and J. Zheng, “MAN: Mutual Attention Neural Networks Model for Aspect-Level Sentiment Classification in SIoT,” *IEEE Internet of Things Journal*, vol.7, no.4, 2020, pp. 2901-2913.

[47] W. Gong, L. Qi, and Y. Xu, “Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment,” *Wireless Communications and Mobile Computing*, vol. 2018, 2018, pp. 1-8.

[48] H. Li, H. Kou, C. Yan, and L. Qi, “Link prediction in paper citation network to construct paper correlation graph,” *EURASIP Journal on Wireless Communications and Networking*, vol. 233, 2019, pp. 1-12.

[49] X. Zheng, Z. Cai, J. Li, and H. Gao, “Location-privacy-aware review publication mechanism for local business service systems,” *Proc. IEEE International Conference on Computer Communications* (*INFOCOM*), 2017, pp. 1–9.

[50] Y. Wang, Z. Cai, X. Tong, Y. Gao, and G. Yin, “Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems,” *Computer Networks*, vol. 135, 2018, pp. 32-43.

[51] L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, and X. Xu, “A QoS-aware virtual machine scheduling method for energy conservation in cloud-based cyber-physical systems,” *World Wide Web*, vol. 23, no. 2, 2020, pp. 1275-1297.

[52] http://snap.stanford.edu/data/loc-gowalla.html

[53] P. Xiong, T. Q. Zhu, and X. F. Wang, “A survey on differential privacy and applications,” *Chinese Journal of Computers*, vol. 37, no. 1, 2014, pp. 101– 122.

Biographies

Mengnan Bi, received the Bechelor degree in the School of Computer and Control Engineering, Yantai University. She is currently pursuing the Master degree in the School of Computer and Control Engineering, Yantai University. Her research interests are mobile crowdsourcing and edge computing.

Yingjie Wang, received the received the Ph.D. degree in College of Computer Science and Technology from Harbin Engineering University. She visited Georgia State University from 2013/09 to 2014/09 as a visiting scholar. Dr. Wang is currently an Associate Professor in the School of Computer and Control Engineering at Yantai University. She is a Postdoc in South China University of Technology. Her research interests are mobile crowdsourcing, privacy protection and trust computing. She has published more than 30 papers in well known journals and conferences in her research field, which include an ESI high cited paper. In addition, she has presided 1 National Natural Science Foundation of China project, 2 China Postdoctoral Science Foundation projects, and joined 3 National Natural Science Foundation of China projects and 1 Natural Science Foundation of Shandong Province project.

Zhipeng Cai, received his PhD and M.S. degrees in the Department of Computing Science at University of Alberta, and B.S. degree from Beijing Institute of Technology. Dr. Cai is currently an Associate Professor in the Department of Computer Science at Georgia State University. Prior to joining GSU, Dr. Cai was a research faculty in the School of Electrical and Computer Engineering at Georgia Institute of Technology. Dr. Cai's research areas focus on Cyber-Security, Privacy, Networking and Big data. Dr. Cai is the recipient of an NSF CAREER Award.

Xiangrong Tong, received the Ph.D. degree in School of Computer and Information Technology from Beijing Jiaotong University. Currently, he is a Full Professor of Yantai University. His research interests are computer science, intelligent information processing and social networks. He has published more than 50 papers in well known journals and conferences. In addition, he has presided and joined 3 national projects and 3 provincial projects.