Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 9948543, 18 pages
https://doi.org/10.1155/2021/9948543

Research Article

Location Privacy Protection Scheme for LBS in IoT

Hongtao Li,[1,2] **Xingsi Xue**,[3] **Zhiying Li**,[1] **Long Li**,[4] **and Jinbo Xiong**[5]

[1]*College of Mathematics and Computer Science, Shanxi Normal University, Linfen 041000, China*
[2]*Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, China*
[3]*School of Computer Science and Mathematics, Fujian University of Technology, Fuzhou 350118, China*
[4]*Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China*
[5]*College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350118, China*

Correspondence should be addressed to Long Li; lilong@guet.edu.cn

Received 30 March 2021; Revised 19 July 2021; Accepted 2 August 2021; Published 17 August 2021

Academic Editor: Cong Pu

The widespread use of Internet of Things (IoT) technology has promoted location-based service (LBS) applications. Users can enjoy various conveniences brought by LBS by providing location information to LBS. However, it also brings potential privacy threats to location information. Location data that contains private information is often transmitted among IoT networks in LBS, and such privacy information should be protected. In order to solve the problem of location privacy leakage in LBS, a location privacy protection scheme based on k-anonymity is proposed in this paper, in which the Geohash coding model and Voronoi graph are used as grid division principles. We adopt the client-server-to-user (CS2U) model to protect the user's location data on the client side and the server side, respectively. On the client side, the Geohash algorithm is proposed, which converts the user's location coordinates into a Geohash code of the corresponding length. On the server side, the Geohash code generated by the user is inserted into the prefix tree, the prefix tree is used to find the nearest neighbors according to the characteristics of the coded similar prefixes, and the Voronoi diagram is used to divide the area units to complete the pruning. Then, using the Geohash coding model and the Voronoi diagram grid division principle, the G-V anonymity algorithm is proposed to find k neighbors in an anonymous area so that the user's location data meets the k-anonymity requirement in the area unit, thereby achieving anonymity protection of location privacy. Theoretical analysis and experimental results show that our method is effective in terms of privacy and data quality while reducing the time of data anonymity.

1. Introduction

With the rapid development of the Internet of Things (IoT), mobile computing, GPS, and wireless communication technology, location-based service (LBS) has been widely used in many important fields [1–4]. As the core of the IoT, sensors enable the Internet of Things to realize intelligent perception, object recognition, information collection, and other functions [5, 6]. IoT devices form the backbone of the LBS or LBS applications. Users can enjoy the convenience of location service applications, such as shopping, travel, and accommodation. However, when enjoying the convenience of LBS, users must provide their own location information to LBS servers or IoT devices, which may lead to the disclosure of users' location privacy [7, 8]. Therefore, privacy protection of users' location has become the focus of research in LBS.

At present, domestic and foreign researchers have conducted a large number of studies on location privacy protection and proposed a variety of solutions to the privacy protection problems in LBS, such as location privacy protection technology based on interference, location privacy protection technology based on encryption, and k-anonymity.

The privacy protection technology based on interference mainly uses false information and redundant information to interfere with the attacker's stealing of user information. According to the different user information (identity information and location information), privacy protection technology based on interference can be divided into pseudonym technology and false location technology. The

pseudonym technology hides the real identity of the user by assigning an untraceable identifier to the user, and the user uses the identifier to replace his own identity information for inquiries. False location technology uses false location or adds redundant location information to interfere with the user's location information when the user submits query information.

The location privacy protection technology based on encryption encrypts the user's location and points of interest and then searches or calculates in the ciphertext space, while the attacker cannot obtain the user's location and the specific content of the query. Two typical location privacy protection technologies based on encryption are location privacy protection technology based on private information retrieval (PIR) and location privacy protection technology based on homomorphic encryption.

k-anonymity is a technology proposed by Samarati and Sweeney in 1998. This technology can ensure that each individual record stored in the release dataset cannot be distinguished from other $k-1$ individuals for sensitive attributes so that the probability of a specific individual being found is $1/k$; namely, the k-anonymity mechanism requires at least k records of the same quasi-identifier, so observers cannot connect records through the quasi-identifier. k-anonymity is divided into centralized k-anonymity and k-anonymity under the P2P structure.

Applications based on location-based services bring a lot of convenience to people's lives, but at the same time, it also brings severe challenges to users' privacy and security. When users query information from LBS servers, they need to send personal identity, location, interests, and other information to LBS servers. If this information is leaked by untrusted or malicious LBS servers, the attackers can not only link the user's identity with location and interests but also infer more user private information. Therefore, location privacy protection in LBS is becoming more and more important and has been attached great importance to relevant fields.

The filling curve of Geohash encoding is Peano. The Peano curve was discovered by the Italian mathematician Piano. This curve can fill the space, but it has the shortcoming of sudden change. The commonly used method to solve this problem is to calculate the surrounding 8 areas or fill them with the Hilbert curve space. Because it is in the environment of the road network, this article uses the Voronoi diagram to divide the road network. The use of Voronoi can solve the defect problem of Geohash Base32. Based on Geohash coding and the Voronoi diagram, this paper proposes a road network-oriented location privacy protection method (G-V anonymity algorithm). It can ensure privacy protection, improve the quality of service and the availability of published data, and reduce the time of data anonymity. The main contributions of this paper are as follows:

(1) In the client, this paper proposes the Geohash algorithm, which converts the user's position coordinates into a Geohash code of the corresponding length. The Geohash algorithm converts two-dimensional longitude and latitude into strings, and each string represents a rectangular region. In other words, all the points (longitude and latitude coordinates) in this rectangular area share the same Geohash string, which can protect privacy and make caching easier

(2) On the server side, the user-generated Geohash code is inserted into the prefix tree, the prefix tree is used to find the nearest neighbors according to the characteristics of the coded similar prefixes, and the Voronoi diagram is used to divide the area units to complete the pruning. The advantages of the prefix tree are as follows: use the common prefix of the string to reduce the query time, minimize the unnecessary string comparison, and the query efficiency is higher than the hash tree

(3) Based on the Geohash coding model and Voronoi diagram grid generation principle, this paper proposes the G-V anonymity algorithm, which can find k neighbors in the anonymous area and make the user's location data meet the k-anonymity requirement in the area unit, so as to protect the location privacy. When the number of users is scarce, a corresponding number of dummy elements are produced to meet the k-anonymity requirement and realize location privacy protection

(4) A comprehensive theoretical and experimental analysis is carried out on the proposed method. The experimental results show that the algorithm has high service quality and data availability while completing privacy protection and at the same time has a short data anonymity time

The rest of this paper is organized as follows. Section 2 introduces the related works. Section 3 introduces Definitions, Geohash Code, Voronoi Diagram, LBS Framework Based on IoT, System Architecture, A Practical Application Scenario, and Attack Model. Section 4 introduces the Geohash algorithm and G-V anonymity algorithm proposed in this paper. Section 5 conducts experiments on the G-V anonymity algorithm in terms of the anonymous success rate, degree of privacy protection, algorithm running time, and antiattack ability of the algorithm. Section 6 is the conclusion of this paper.

2. Related Works

As LBS privacy has become the focus of research, more and more scholars have paid close attention to LBS privacy protection methods. At present, the main methods of location privacy protection include location privacy protection technology based on interference, location privacy protection technology based on encryption, and k-anonymity.

The privacy protection technology based on interference mainly uses false information and redundant information to interfere with the attacker's stealing of user information [9–12]. In Reference [13], they proposed a dynamic pseudonymous-based multiple mix-zones authentication protocol that only requires mobile vehicles to communicate with the reported server for registration and dynamic

pseudonym change. Furthermore, a mechanism is proposed to provide users with dynamic pseudonyms, named as base pseudonyms and short-time pseudonyms, to achieve users' privacy. In Reference [14], a new privacy-preserving solution for pseudonym on-road on-demand refilling is proposed where the vehicle anonymously authenticates itself to the regional authority subsidiary of the central trusted authority to request a new pseudonym pool. The logical demonstration proved that this privacy-preserving authentication is assured. In Reference [15], a novel dynamic mixed zone establishment scheme is proposed to protect the location privacy of autonomous vehicles in the convoy driving context. Compared with the scheme to protect location privacy in the traditional vehicular network, the proposed scheme has less overhead and a higher level of security.

Location privacy protection technology based on encryption can be divided into two categories: location privacy protection technology based on private information retrieval (PIR) [16, 17] and location privacy protection technology based on homomorphic encryption [18, 19]. In Reference [20], they proposed a new method to adjust the vehicle speed which reduces the vehicle delay that suffers from the network gap problem. It has the advantages of short response time, low cost, less packet loss information, and strong privacy protection capabilities. In Reference [21], they proposed a novel dynamic path privacy protection scheme for continuous query service in road networks. This scheme also conceals DPP (dynamic path privacy) users' identities from adversaries; this is provided in the initiator untraceability property of the scheme. The security analysis shows that the model can effectively protect the user's identity anonymously, location information, and service content in LBS. In Reference [22], a fully homomorphic encryption method is used to ensure the safety of the anonymous server itself, and they designed a LBS privacy protection model; the model uses the onion algorithm and asymmetric encryption methods to protect user information.

k-anonymity requires that the same quasi-identifier must have at least k records; each individual record cannot be distinguished from other $k-1$ individuals for sensitive attributes, so the attackers cannot link the records through the quasi-identifier [23–26]. Zhou et al. [27] proposed a neighbor query algorithm that does not rely on trusted third-party anonymous servers to protect the user's location privacy information GHNNQ (Geohash Nearest Neighbor Querying). Guochao et al. [28], according to the rapid search superiority of Geohash coding, proposed a location-based privacy protection method based on interval regions. This approach first generalizes the user's real location to the interval region, then indexes the location with the same code based on the Geohash coding principle as a candidate location set, and then provides personalized k-anonymity privacy protection service for the user, which satisfies the user's privacy requirements.

The filling of the Geohash code can be realized by the Peano curve. Although this curve can fill the space, it has the shortcoming of strong mutability. The common method to solve this problem is to fill the space with the Hilbert curve [29]. In the environment of the road network, using the Voronoi graph [30–32] to partition the road network can solve the defect problem of Geohash Base32, and the Voronoi graph is directly used to prune around the Geohash code region and delete users who are not in the Voronoi unit. On the server side, the user-generated Geohash code is inserted into the prefix tree. The advantages of the prefix tree are as follows: use the common prefix of the string to reduce the query time, minimize the unnecessary string comparison, and the query efficiency is higher than the hash tree. In this paper, we propose a location privacy protection method for road networks based on k-anonymity, in which the Geohash coding model and Voronoi graph are used as grid division principles. Theoretical analysis and experimental results show that it not only achieves privacy protection but also improves the quality of service and data availability.

Comparing the work in this paper with References [27–29], the results are shown in Table 1. Reference [27] proposes the GHNNQ algorithm, which does not rely on third-party servers; that is, the client sends the Geohash-encoded user's location data to the LBS server. By configuring the corresponding query processing algorithm on the server side, the direct interaction between the user and the LBS location server is realized. But it did not combine the actual situation of the road network. Reference [28] uses the superiority of Geohash coding to quickly retrieve information and proposes a location privacy protection method based on interval regions. The user's real location is generalized to the interval area, the same coded location is retrieved as a candidate location set according to the Geohash coding principle, and then according to the user's privacy needs, the user is provided with a personalized k-anonymity privacy protection service. It does not consider the actual situation of the road network and relies on a trusted third-party server. Once the trusted third party is unreliable, it will cause the disclosure of users' privacy. Reference [29] proposed a location privacy protection scheme based on the Hilbert curve. Firstly, a Hilbert curve corresponding to the Hilbert coordinate is generated according to the given coordinate transformation parameters. Secondly, the user's points are transmitted to the location service provider (LSP) through the randomly generated points of the fog server, instead of using k-anonymity and other methods to meet the needs of the location service provider. Then, the weighted KNN algorithm of LSP is used to get the user's interest points. Finally, the POI of the user is transmitted back to the client. This scheme does not use k-anonymity technology and avoids background knowledge attacks and homogeneous attacks. However, this scheme does not combine the actual situation of the road network, nor does it reduce the dimension of the location coordinates. Comparison of related works is shown in Table 1.

3. Preliminaries

3.1. Definitions

Definition 1 (Query information). Generally, the user's query information has the form $Q = (\mathrm{QID}, \mathrm{CGh}, k, t, l_{\min}, R)$. QID represents the user's quasi-identifier, CGh represents the Geohash code, k represents the degree of privacy protection

Table 1: Comparison of related works.

References	Actual road situation considering	Third-party needing	Geohash encoding	k-anonymity technology
Reference [27]	×	×	√	×
Reference [28]	×	√	√	√
Reference [29]	×	×	×	×
This article	√	√	√	√

of the user, t represents the time of sending the request, $l_{\min}$ represents the shortest prefix length of the same code that the user can accept, and R represents the content of the user's query.

Definition 2 (Request information). Generally, request information sent by the server has the form $\mathrm{REQ} = (\mathrm{AS}, R)$. AS represents the formed anonymous set, and R represents the content of the user's query.

Definition 3 (Trie tree). The trie tree is a prefix tree obtained by transforming hash trees that are often used to count and sort large numbers of strings [33]. The idea of a trie tree is to exchange space for time and use the common prefix of strings to reduce the cost of query time to achieve the purpose of improving efficiency.

3.2. Geohash Code. The Geohash code is a geocoding that is essentially used to encode the latitude and longitude into a one-dimensional string. The idea of the Geohash code is to treat the earth as a plane and then divide the longitude and latitude into alternating dichotomies, using binary 0 or 1 to represent the regions divided (the latitude range is -90~90, and the longitude range is -180~180). Every 5 times of division is regarded as a level, and the binary code of each level is converted into a 32-base code (as shown in Table 2), which finally becomes a unique identifier to represent each coordinate on the earth, making it have the characteristics of global uniqueness, multilevel recursion, and one-dimensionality. Since the Geohash code is formed using a dichotomy, it represents a rectangular area rather than a point. The accuracy of the Geohash string is determined by the length of the string, with longer strings having higher accuracy and shorter strings having lower accuracy. When the precision is high enough, the more the prefixes overlap, the closer the two places are, so the Geohash code is often used to query the nearest neighbor.

3.3. Voronoi Diagram. The Voronoi diagram, also known as the Tyson polygon, is a group of continuous polygons composed of vertical bisectors connecting two adjacent points. N points which are different in the plane are divided into planes according to the nearest neighbor principle, and each point is associated with its nearest neighbor region. In this paper, the Voronoi diagram is applied to the road network, and the road network is divided into Voronoi diagram units. The steps to generate the road network Voronoi diagram are as follows. Firstly, the road network is abstracted into a road network model. The undirected graph $G = (V, E)$ is used to represent the road network model, where V represents the intersection point of the road network and E represents the road section between the intersection points. Secondly, based on the road network model, the vertical bisector is drawn for the E, and it is extended to intersect with other vertical lines; then, the polygon formed by these vertical lines is the Voronoi unit. Finally, the above steps are repeated to obtain the Voronoi diagram of the road network intersection. The corresponding Voronoi diagram of the road network is shown in Figure 1.

3.4. LBS Framework Based on IoT. According to the characteristics of information perception and interaction of the IoT and the requirements of location-aware service, the LBS service framework based on the IoT consists of the perception layer, the network layer, the platform layer, and the application layer, as shown in Figure 2.

The perception layer is the foundation of LBS service, which mainly realizes the acquisition of location information, scene information perception, the perception of location-related dynamic spatiotemporal information, etc., and uploads the collected perception information and location data to the network layer.

The network layer mainly realizes the fast, safe, and reliable transmission and exchange of data and transits the perceived data and location information to the platform layer for data sharing and processing. Then, the user's location information and location service request are transmitted to the platform layer, and the intelligent information processing results of the platform layer are returned to the application layer.

The platform layer is based on the cloud computing platform and big data platform to realize the storage and management of massive data. It uses cloud computing, big data, data mining, artificial intelligence, and other technologies to provide personalized location services for the users of the application layer. It also realizes the tracking, control, and monitoring of physical objects in the perception layer.

The application layer is mainly composed of various LBS applications. Users send location information and location service request commands containing service requirements to the LBS server, and the LBS server provides users with location-based navigation, location social interaction, object monitoring, and other responsive interactive services according to the intelligent information processing results of user requests. The LBS system can also use sensors, positioning devices, RFID tags, and other real-time access to the user's current location or activity trajectory and then provide location-related services to the user or automatically achieve the tracking and monitoring of the target object.

Table 2: The Base32.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Base32	0	1	2	3	4	5	6	7	8	9	b	c	d	e	f	g
Decimal	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Base32	h	g	k	m	n	p	q	r	s	t	u	v	w	x	y	z

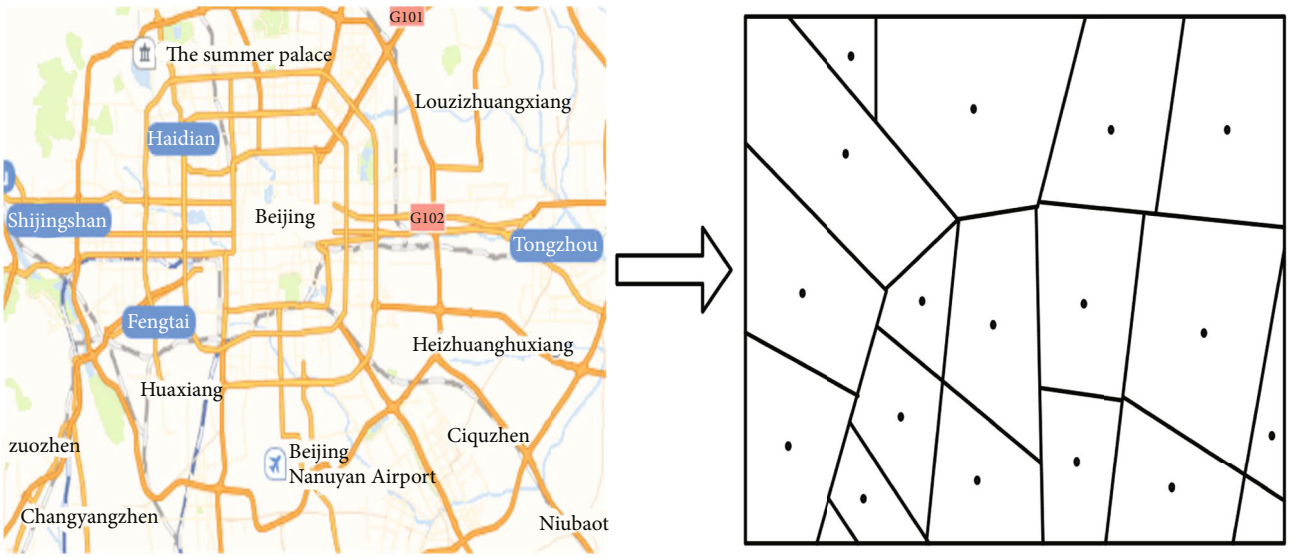


Figure 1: The Voronoi diagram corresponding to the intersection of the road network.

Data transmitted and exchanged between layers of the LBS service framework usually includes personal privacy such as the user's real identity, property account, interests and hobbies, and activity track, as well as business privacy such as the enterprise marketing plan and new product development plan.

From the perspective of the overall architecture of the Internet of Things, location awareness is an indispensable part of the perception layer, which provides the basic location information for the whole Internet of Things system. From the perspective of the application, location-based services will penetrate into many Internet of Things application scenarios to provide differentiated services. Location service is the infrastructure service of the Internet of Things. The intelligent terminal positioning device collects location information, and the location information is provided to the cloud control center as important data. The cloud platform uses the location information of multiple devices to draw a visual interface, which is helpful for the comprehensive analysis and intelligent decision-making of the Internet of Things system.

3.5. System Architecture. The location privacy protection system adopted in this paper consists of three parts: the mobile users, the third-party servers, and the location servers. The system framework is shown in Figure 3.

The system structure of this article is shown in Figure 3, which is mainly composed of a client module, a third-party server, and a location service provider module. The client module is composed of two parts: the positioning module and the conversion mechanism. The positioning module mainly obtains the user's position information through GPS and other positioning devices, and the conversion mechanism converts the user's position coordinates into Geohash codes. The third-party server consists of a database, an anonymous module, and a filtering module. The database is used to store data such as geographic information, road network information, and Geohash codes. The anonymous module selects an anonymous area, generates an anonymous set, and feeds back the anonymity to the database. The location service provider can respond to the query request of the anonymous module and feed back the query result to the screening module, and the screening module will feed back the screening result to the user after screening.

3.6. A Practical Application Scenario. A practical scenario illustrated in Figure 4 is the social network application in smartphones, which brings people a lot of convenience in life. Our intention is to protect and process location information of social applications in smartphones. The client refers to APPs in mobile phones in the social network, and the server refers to location service providers. The server provides the APPs' API interface to obtain the relevant data, adopt the minimum distance grouping algorithm to protect the data, upload the processed data to the APPs' database in the privacy protection processor, adopt the minimum selectivity priority algorithm to achieve secondary protection of the

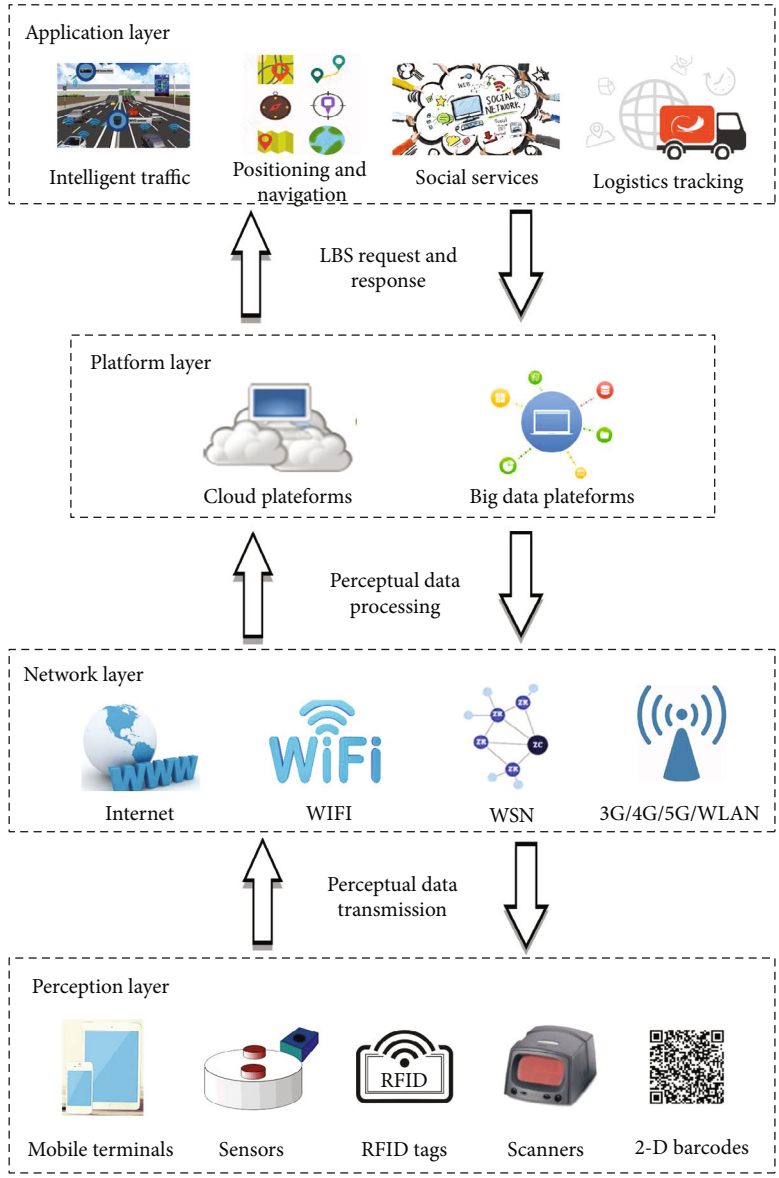


Figure 2: LBS framework based on IoT.

location data, and finally upload the processed data to the database. Users can obtain location query results from the APPs' service providers.

3.7. Attack Model. Almost all LBS providers collect users' personal data, such as identity, location, and interests. Many LBS providers provide different security guarantees, such as Google, Twitter, and YouTube. Once these LBS providers are attacked, users' privacy information will be leaked. The threat model of this paper is shown in Figure 5. The users' location data is acquired through smart mobile devices equipped with positioning technology, such as mobile phones, portable computers, and cars, and the obtained location data is uploaded to the database. Then, the location data is transferred to the LBS servers for further intelligent data processing, which allows users to get convenient services from the LBS providers. The attackers can obtain the user's personal data by attacking the user's smart terminals, LBS servers, or location service providers, which will result in the users' privacy being breached.

4. Algorithm Implementation

In this paper, a location privacy protection algorithm is proposed based on Geohash coding and the Voronoi diagram. The privacy protection algorithm mainly consists of the conversion mechanism and anonymity process. Firstly, the Geohash code generation algorithm is proposed in the conversion mechanism, in which two-dimensional coordinates are transformed into one-dimensional Geohash codes in the mobile client. Then, the G-V anonymity algorithm is proposed in the anonymity process, in which the Voronoi diagram unit is used to protect the location privacy anonymously on the third-party server.

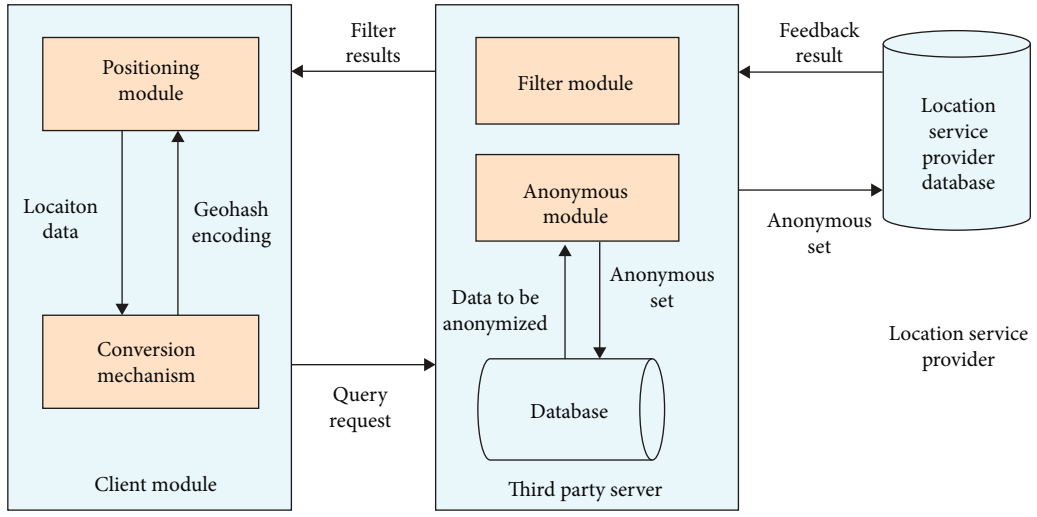


Figure 3: The system architecture.

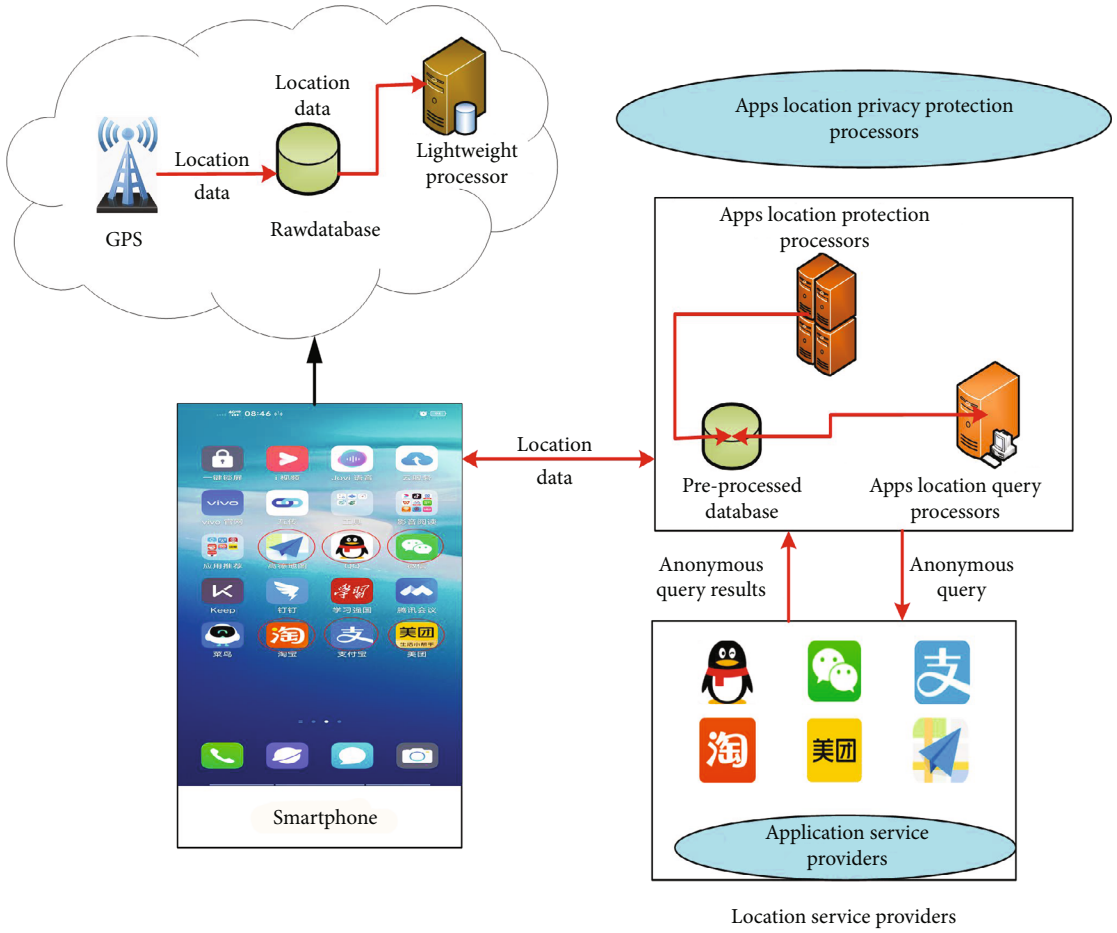


Figure 4: A practical application scenario in smartphones.

4.1. The Conversion Mechanism. The function of the conversion mechanism is to convert the user's location coordinates into codes. Based on the nature of Geohash encoding, the users can choose the degree of accuracy and anonymity. In the Geohash code generation algorithm, the user's latitude and longitude coordinates are bisected and converted into binary firstly, then recording the number of bisection as i. Then, determine the latitude range of the x value of the user

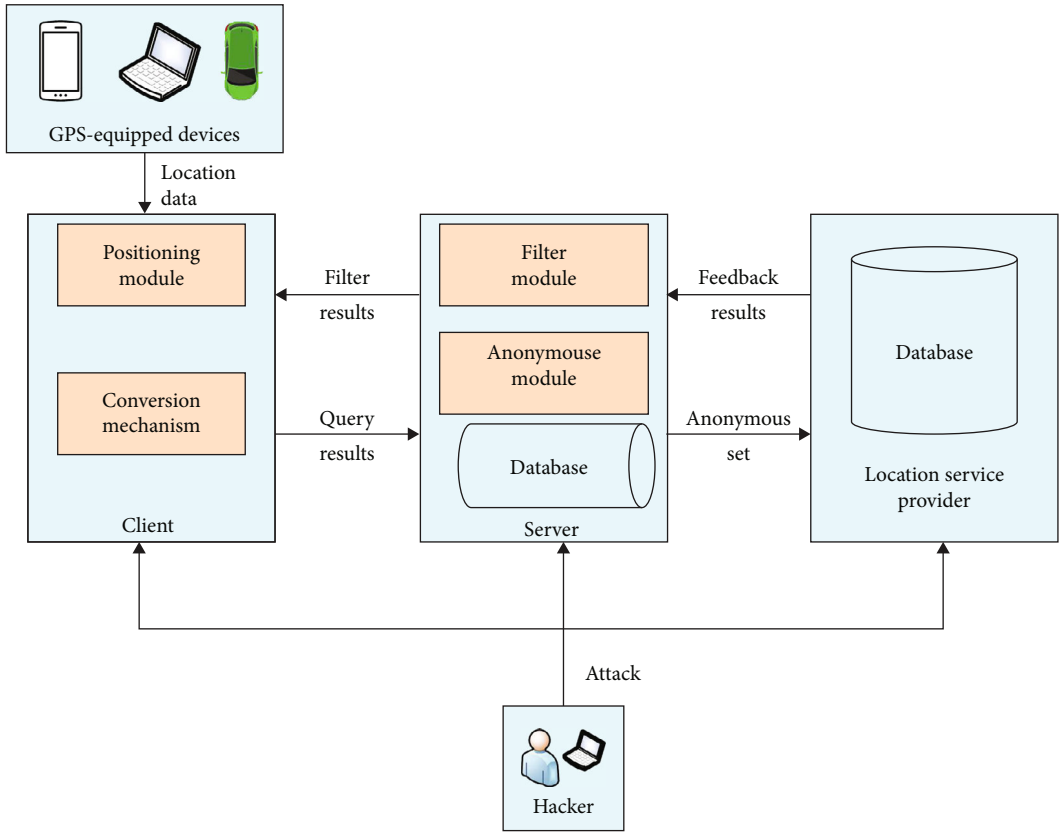


Figure 5: The attack model.

coordinate, and determine the longitude range of the y value of the user coordinate. The left side of the median is marked as 0, and the right side of the median is marked as 1. Finally, Base32 is used for encoding to divide the binary one-dimensional array into a group of five, mapping each group according to Table 2 until the Geohash code output is completed. The Geohash code generation algorithm is as follows.

Take Beijing Tiananmen Square as an example (39.9096 N, 116.3972 E).

As shown in Table 3, the binary code obtained by latitude division is 1011100011. Similarly, the binary code of longitude 116.3972 E is 1101001011 by dividing the longitude region of the earth. The string obtained by combining longitude and latitude is 11100111010010001111. The even bits put the longitude, and the odd bits put the latitude. Every five digits were divided into a group. There are four groups: 11100 (28), 11101 (29), 00100 (4), and 01111 (15). The Geohash code is wx4g, as shown in Table 2.

4.2. G-V Anonymity Algorithm. In this section, the G-V anonymity algorithm is proposed based on the Geohash coding model and Voronoi diagram meshing principle. The basic idea of the algorithm is to find k nearest neighbors in the anonymous region, combine the Geohash with the Voronoi diagram, determine the nearest neighbor by using the characteristics of the Geohash code, delete the mutative users by using the Voronoi diagram, and finally realize the anonymity protection of location privacy. The details are as follows. Firstly, the user who makes the request at time t forms a set to be anonymous in the database and uploads the relevant data to the anonymous module. Secondly, generate a prefix tree to initialize the root node, insert the Geohash code of the unknown user into the prefix tree, and traverse the Geohash string. If there is such a character in the prefix tree, add one to the original number; otherwise, allocate a new node and record the number of new characters until all characters are inserted. Then, query the strings with the same prefix. If there is no application for generating dummy elements, the number of users will be counted, and the anonymous users with the same prefix but not in the Voronoi diagram unit will be deleted to form a new array $U*$. Finally, judge whether the number of users in the new array meets the$k$value; if it is satisfied, output it directly; otherwise, the corresponding number of dummy$D = k - m$will be generated. Dummy location technology is also a fake location technology, and k -anonymity can also be achieved by adding fake locations. The dummy location technology requires that in the query process, in addition to the real location, a number of additional fake location information must be added. The server not only responds to requests for real locations but also responds to requests for fake locations so that the attacker cannot tell which is the real location of the user.

The G-V anonymity algorithm is as follows.

4.3. The Algorithm Analysis

4.3.1. Security Analysis. The client converts the user's location coordinates into one-dimensional Geohash codes.

Input: Position coordinates (x, y), code length l
Output: Geohash code (CGh)
1. lat = $\{-90.0, 90.0\}$, lon = $\{-180.0, 180.0\}$;
2. numbits = $(l * 5)/2$; //The separate code length of longitude and latitude
3. Base32 = {'0,' '1,' '2,' '3,' '4,' '5,' '6,' '7,' '8,' '9,' 'b,' 'c,' 'd,' 'e,' 'f,' 'g,' 'h,' 'j,' 'k,' 'm,' 'n,' 'p,' 'q,' 'r,' 's,' 't,' 'u,' 'v,' 'w,' 'x,' 'y,' 'z'};
4. int $i = 0$, $j = 0$; //i is the number of latitudinal dichotomies, and j is the number of longitude dichotomies
5. latmid = lat/2, lonmid = lon/2; //Dichotomizing the latitude and the longitude
6. while (latmid) //Convert longitude coordinates to binary
7. {
8. char lat$B[i] = 0$;
9. if (x> = latmid)
10. lat$B[i] = 1$;
11. else lat$B[i] = 0$;
12. $i++$;
13. }
14. while (lonmid) //Convert latitude coordinates to binary
15. {
16. char lon$B[j] = 0$;
17. if (y> = lonmid)
18. lon$B[j] = 1$;
19. else lon$B[j] = 0$;
20. $j++$;
21. }
22. while (lat$B[i]$! = Null || lon$B[j]$! = Null) //The longitude and latitude are combined, and the even bit is used to put the longitude, and the odd bit is used to put the latitude
23. {
24. int $k = 0$;
25. char $B[k]$;
26. if (k%2 == 0)
27. {
28. $B[k]$ = lon$B[j]$;
29. $j++$;
30. $k++$;
31. }
32. else
33. {
34. $B[k]$ = lat$B[i]$;
35. $i++$;
36. $k++$;
37. }
38. return $B[k]$;
39. }
40. int $m = 0$;
41. for ($k = 0$; $k +$ = 4)
42. {
43. $B[m] = B[k, k + 4]$; //Divide $B[k]$ into groups of five digits
44. $B[m] \longrightarrow$ Base32; //Map binary to Base32
45. $m++$;
46. CGh = $B[m]$;
47. }
48. return CGh; //Get Geohash code

Algorithm 1: Geohash code generation algorithm.

Geohash uses a string to represent the two coordinates of longitude and latitude. It represents a rectangular area. Every point in the rectangular area may be the exact location of the user, which makes the attacker unable to determine the exact location of the user. The longer the Geohash-encoded string is, the smaller the rectangular area is, the more accurate the result is, but the weaker the privacy protection is. Because the Geohash string encoding algorithm is implemented in the client, the privacy protection strength can be controlled by the user. This is the first layer of protection for location privacy.

In the third-party server, according to the user's anonymity requirement, we can find no less than k nearest neighbors in the Voronoi unit to form an anonymous set. The

Table 3: The calculation of latitude.

Latitude region	Left interval 0	Right interval 1	39.909
(-90.0, 90.0)	(-90.0, 0.0)	(0.0, 90.0)	1
(0.0, 90.0)	(0.0, 45.0)	(45.0, 90.0)	0
(0.0, 45.0)	(0.0, 22.5)	(22.5, 45.0)	1
(22.5, 45.0)	(22.5, 33.75)	(33.75, 45.0)	1
(33.75, 45.0)	(33.75, 39.37)	(39.38, 45.0)	1
(39.375, 45.0)	(39.375, 42.18)	(42.19, 45.0)	0
(39.375, 42.19)	(39.375, 40.78)	(40.78, 42.19)	0
(39.375, 40.78)	(39.375, 40.07)	(40.08, 40.78)	0
(39.375, 40.08)	(39.375, 39.72)	(39.73, 40.08)	1
(39.73, 40.08)	(39.73, 39.90)	(39.90, 40.08)	1

maximum probability that an attacker can lock a user is $p(ui) = 1/k$. The higher the value of k, the lower the probability of an attacker finding the user. Moreover, in the anonymous area formed by the Voronoi unit, the user's specific location is further blurred. k-anonymity technology can guarantee the following three points. (1) The attacker cannot know whether a specific individual is in the public data. (2) Given a person, the attacker cannot confirm whether he has a certain sensitive attribute. (3) The attacker cannot confirm which person a piece of data corresponds to. This is the second layer of protection for location privacy.

To sum up, even if the attacker intercepts the information sent by the user, he cannot find the specific location of the user.

4.3.2. Complexity Analysis. There is no need to use the Euclidean distance calculation when finding the k nearest neighbors; just find the user with the same prefix who sent the request at time t. In this paper, a *trie* tree is used to search. The time complexity of finding the nearest neighbor is related to the length of the Geohash code, so its time complexity is linear $O(l)$, where l is the length of the code. The disadvantage of the *trie* tree is to trade space for time. Base32 used in this paper has 32 characters, so the space complexity is $O(32^n)$. When there are few users and when there is a need to generate dummy elements, the time complexity of successfully constructing an anonymous set depends on the number of generated dummy $D = k - N$, which is linear order $O(D)$.

4.3.3. Mathematical Analysis. The central idea of the algorithm in this paper is as follows. Firstly, convert the user's location coordinates into a Geohash code of the corresponding length on the client side. Secondly, insert the Geohash code into the prefix tree on the server side, and the prefix tree finds the nearest neighbors based on the characteristics of the coded similar prefixes, and the Voronoi diagram divides the area unit to complete the pruning. Finally, according to the Geohash coding model and the Voronoi diagram grid division principle, the G-V anonymity algorithm is proposed. The basic idea of the algorithm is to find k nearest neighbors in the anonymous area to meet the k -anonymity requirement.

According to the G-V anonymity algorithm selection scheme, the anonymous set obtained is $c, c = \{l_1, l_2, \cdots, l_{k-1}, l_k\}$, that is, $|c| = k$. Then, the probability Q that the attacker obtains the user's real location from the anonymous set is calculated as follows:

$$Q = \frac{1}{|c|} = \frac{1}{k}. \tag{1}$$

The k-anonymity technology can ensure that each individual record stored in the release dataset cannot be distinguished from other $k-1$ individuals for sensitive attributes; that is, the k-anonymity mechanism requires at least k records of the same quasi-identifier. The implementation of k-anonymity technology makes it impossible for observers to identify users through quasi-identifiers with a confidence higher than $1/k$, so k-anonymity technology is effective in terms of privacy protection.

5. Experimental Analysis

In this section, we analyze the experimental results of the G-V anonymous location privacy protection method and illustrate the actual performance of the method by analyzing the results of four indicators: anonymous success rate, privacy protection degree, algorithm running time, and algorithm antiattack on simulated datasets.

The algorithm is compared with the G-Casper and Casper algorithms. The G-Casper algorithm uses a bottom-up mechanism to make a string fuzzy query on the Geohash code of the target location to determine the $k-1$ nearest neighbors of the anonymous region. When expanding the scanning area, it scans the grid of the user and the surrounding grid across the domain and then performs hierarchical recursion. At the same time, it uses two parameters $L_{\max}$ and $L_{\min}$ to control the anonymous region. Finally, the redundant grid is removed by the pruning algorithm, and a candidate grid area is randomly sent to replace the user's original location to achieve the effect of k-anonymity. The idea of the Casper algorithm is to adopt the quadtree architecture, select the vertical grid and horizontal grid which meet the conditions each time, and store the information of each grid in the form of quadtree layer by layer until the grid is reclassified into a region and satisfies k-anonymity and minimum anonymity.

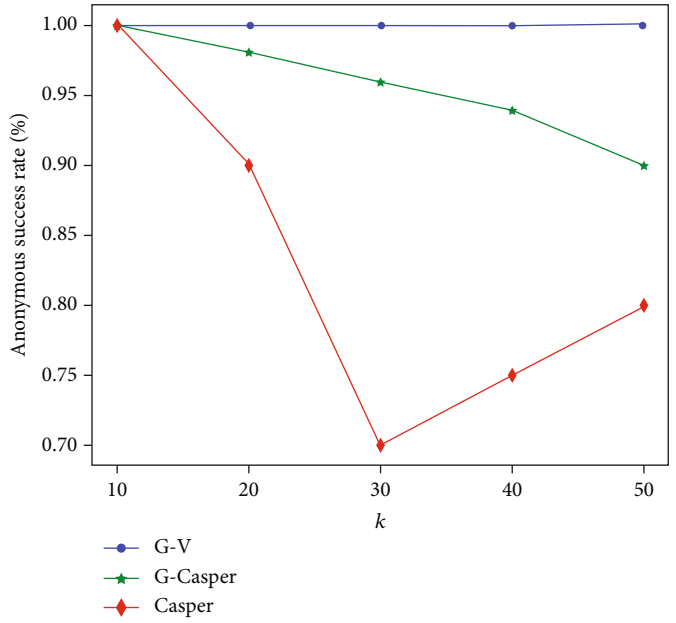
5.1. Environment Setting. The hardware environment is as follows: Intel® Core i5, CPU 1.7 GHz, and memory 4.00 GB. The software environment is as follows: Windows 10 64-bit operating system, compiled language using the C++ language. The experiment is implemented using Python. The experiment is carried out on two datasets. One is the POI dataset [34] from several provinces in China, which contains about 4 million pieces and is stored in the MySQL database. One is the Gowalla dataset [35]. The algorithm proposed in this paper is compared with G-Casper [36] and Casper [37] algorithms in terms of the anonymous success rate, privacy protection degree, algorithm running time, and algorithm antiattack.

Input: The user set to be anonymous $U = \{u_1, u_2, u_3, \cdots, u_n\}$, the Voronoi diagram of the road network, k, $l_{\min}$
Output: The anonymous set AS
1. send($Q\{u_1, u_2, u_3, \cdots, u_n\}$); //Sending anonymous request from users
2. receive($Q\{u_1, u_2, u_3, \cdots, u_n\}$); //The server received information from n users
3. send($Q\{u_1, u_2, u_3, \cdots, u_n\}$ Voronoi); //Sending data to the anonymous module
4. receive($Q\{u_1, u_2, u_3, \cdots, u_n\}$ Voronoi); //The anonymous module accepts users' data
5. int Max = 32; //Max represents the size of the character set
6. int count = 0; //count represents the number of times the character appears
7. struct trieNode next[Max] //The next array represents the type of each character
8. for ($i = 0$; $i <$ Max ; i++) //Building the prefix tree
9. {
10. if ($i = 0$)
11. next[i] = Null; //Initializing root node
12. else
13. next[i] = CGh; //Insert the Geohash code into the prefix tree
14. }
15. while (prefix tree! = Null) //Traverse the prefix tree
16. {
17. if (next[i] == CGh)
18. {
19. count + +;
20. i + +;
21. }
22. if (next[i]! = CGh)
23. {
24. next[i] = newnode[++num]; //The node is none. Assigning a new node
25. count + +;
26. }
27. }
28. while (search! = Null) //Querying strings with the same prefix
29. {
30. if (search'CGh' == Null)
31. return 0;
32. else
33. {search + +;
34. return m = search; //Number of users with the same prefix
35. }
36. }
37. $U* = \{u_1, u_2, u_3, \cdots, u_m\}$
38. if ($m >= k$)
39. AS $\longleftarrow U*$;
40. else
41. {
42. $D = k - m$; //Generating dummy D
43. AS $\longleftarrow U* + D$;
44. }
45. return AS; //Anonymous success

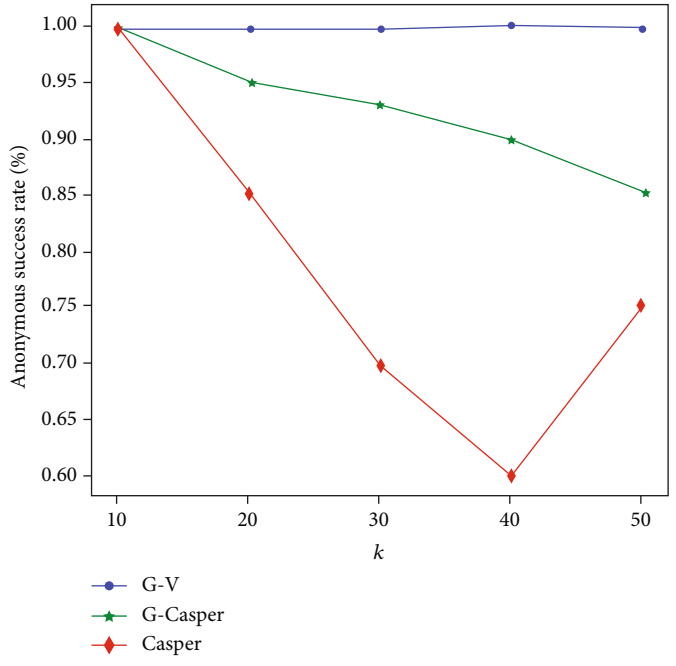
Algorithm 2: The G-V anonymity algorithm.

5.2. Anonymous Success Rate. When the Geohash code length l is unchanged, the algorithm proposed in this paper is compared with the G-Casper and Casper algorithms in terms of the anonymous success rate, and the result is shown in Figure 6. The x-axis represents the size of the anonymous area, and the y-axis represents the anonymous success rate. The anonymous success rate of the G-V anonymity algorithm has nothing to do with the value of k, while the anonymous success rate of the G-Casper and Casper algorithms decreases with the increase of the value of k. Therefore, compared with the G-Casper and Casper algorithms, the algorithm proposed in this paper has the best anonymous success rate, followed by the G-Casper algorithm. As the value of k increases, the anonymous area of the Casper algorithm is too large to be accurate enough, and it requires a lot of storage space to store the information of each grid. Therefore, the Casper algorithm has the worst anonymous success rate.

When the anonymous region k is unchanged, the algorithm proposed in this paper is compared with the G-Casper and Casper algorithms in terms of the anonymous success rate. The result is shown in Figure 7. The x-axis



(a) Gowalla

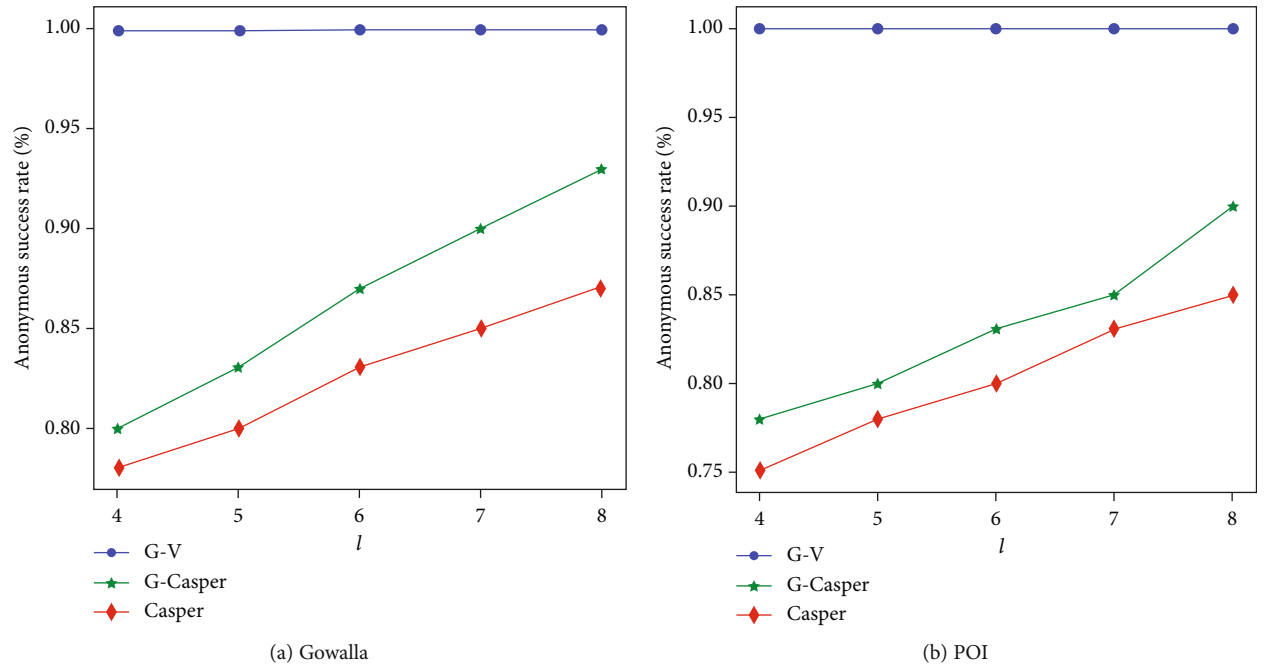


(b) POI

Figure 6: The anonymous success rate of the algorithm when the l is unchanged.

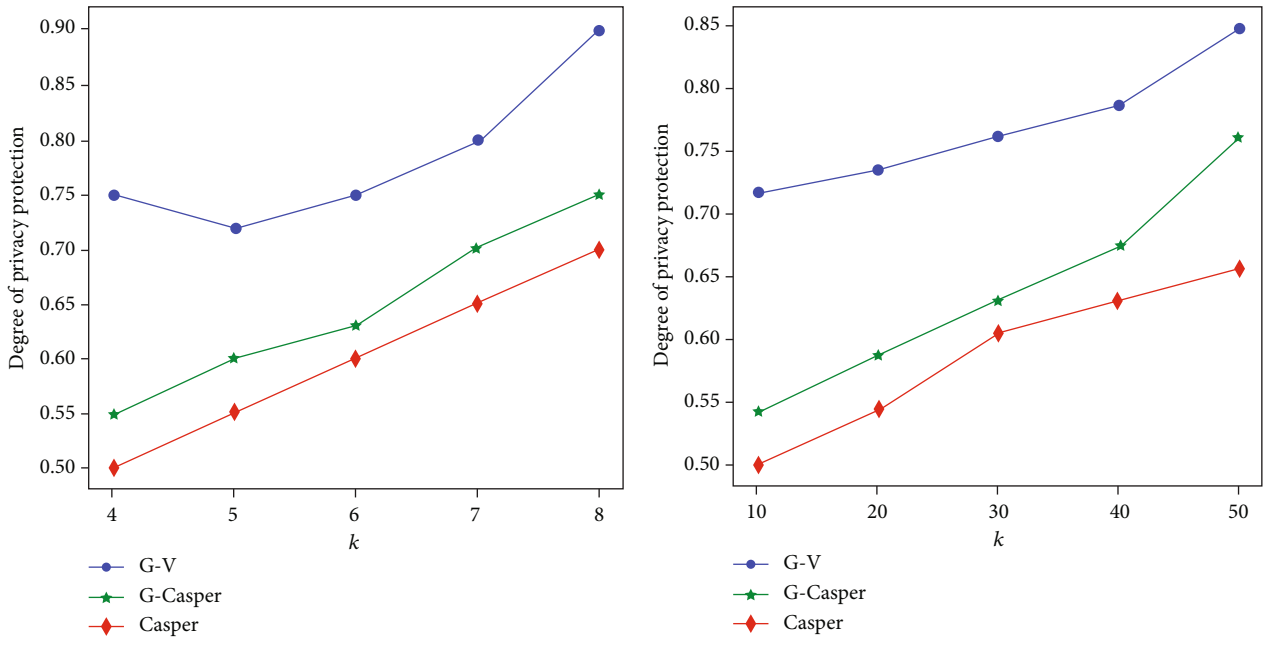
represents the length of the Geohash code, and the y-axis represents the anonymous success rate. The anonymous success rate of the G-V anonymity algorithm has nothing to do with the value of l, while the anonymous success rate of the G-Casper and Casper algorithms decreases with the increase of the value of l. Therefore, compared with the G-Casper and Casper algorithms, the algorithm proposed in this paper has the best anonymous success rate, followed by the G-Casper algorithm, and the Casper algorithm has the worst anonymous success rate.

5.3. Degree of Privacy Protection. The proposed algorithm is compared with the G-Casper and Casper algorithms in terms of privacy protection under the condition that the Geohash encoding length l remains unchanged. The results are shown in Figure 8. The x-axis represents the size of the anonymous region, and the y-axis represents the degree of privacy protection. The larger the k value is, the lower the risk of leakage is, and the better the privacy protection is. With the increase of the k value, the degree of privacy protection increases. The privacy protection of the G-V anonymity algorithm is



(a) Gowalla (b) POI

Figure 7: The anonymous success rate of the algorithm when the k is unchanged.

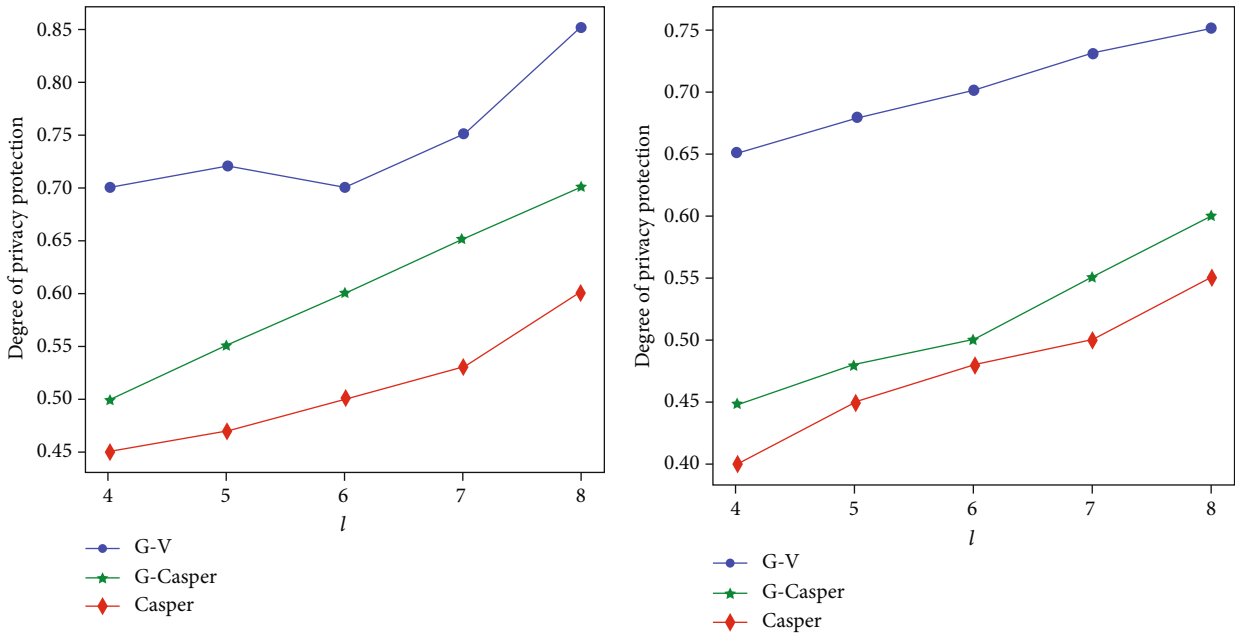


(a) Gowalla (b) POI

Figure 8: The degree of privacy protection of the algorithm when the l is unchanged.

affected by two factors: k and l. When the value of k increases, the number of users in the anonymous area increases, and the probability of the attacker inferring the user's location decreases. Therefore, the privacy protection degree of the algorithm proposed in this paper is the best, followed by the G-Casper algorithm. With the increase of the k value, the anonymous region of the Casper algorithm is too large to be accurate, and the privacy protection degree is poor.

The proposed algorithm is compared with the G-Casper and Casper algorithms in terms of privacy protection under the condition that the anonymous region$k$ remains unchanged. The results are shown in Figure 9. The x-axis represents the length of Geohash encoding, and the y-axis represents the degree of privacy protection. The higher the l value is, the lower the risk of leakage is, and the better the privacy protection is. The G-V anonymity algorithm is affected



(a) Gowalla (b) POI

Figure 9: The degree of privacy protection of the algorithm when the k is unchanged.

by the encoding length l. When the encoding length l increases, the probability of the attacker guessing the user's location decreases. Therefore, the proposed algorithm has the best degree of privacy protection, followed by the G-Casper algorithm, which has a poor degree of privacy protection.

5.4. Algorithm Running Time. When the length of the Geohash code l remains unchanged, the algorithm proposed in this paper is compared with the G-Casper and Casper algorithms in terms of algorithm running time. The results are shown in Figure 10. The x-axis represents the size of the anonymous area, and the y-axis represents the running time of the algorithm. The larger the anonymous area, the more time the algorithm will run. Regardless of the value of k, the anonymity time of the algorithm proposed in this article will not fluctuate much. Therefore, the running time of the algorithm proposed in this paper is less, followed by the G-Casper algorithm, and the Casper algorithm requires more time.

In the case of the anonymous region when$k$ is unchanged, the algorithm in this paper is compared with the G-Casper and Casper algorithms in terms of algorithm running time. The results are shown in Figure 11. The x -axis represents the encoding length, and the y-axis represents the running time of the algorithm. The larger the encoding length l is, the longer the algorithm runs. The algorithm proposed in this paper uses the prefix tree structure, so the query time is less, followed by the G-Casper algorithm, and the Casper algorithm requires more time.

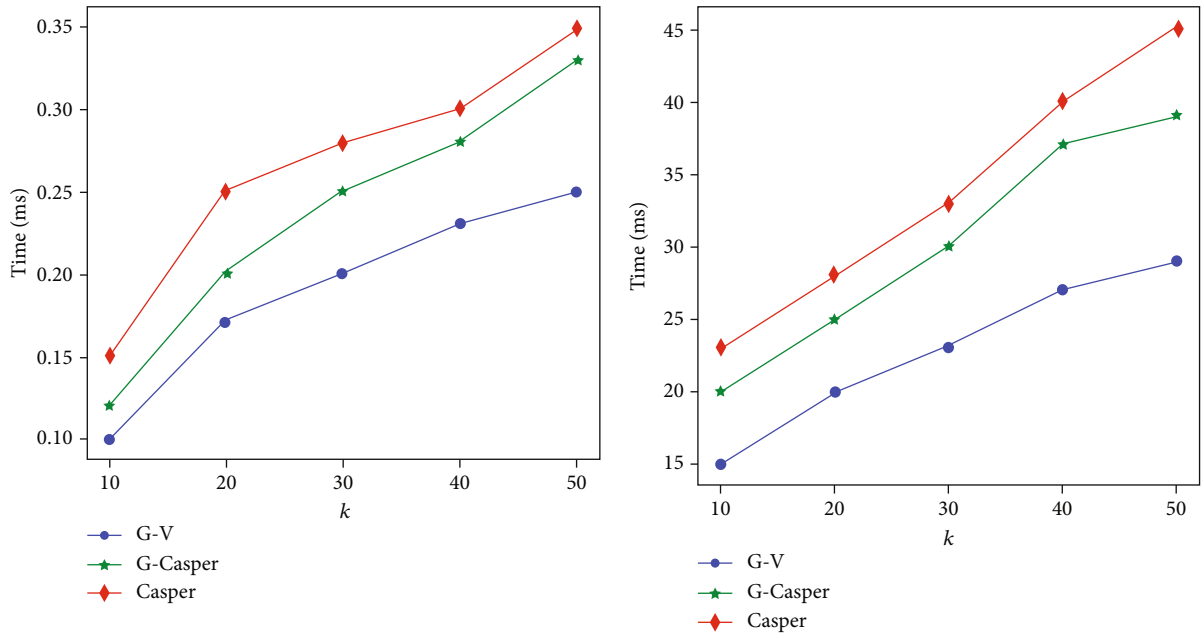
5.5. The Antiattack Ability. The privacy protection object in data publishing is mainly the corresponding relationship between the user's sensitive data and individual identity. Generally, the way of deleting identifiers to publish data cannot really prevent privacy disclosure. Attackers can obtain individual privacy data through link attacks.

The chain attack refers to the link operation between the published data and the external data obtained from other channels to infer the privacy data, thus causing privacy leakage, which is equivalent to an expansion of the dimension of personal information. The simplest example is that two tables in the database get more information through primary key association.

In order to solve the problem of privacy leakage caused by link attacks, the k-anonymity method is introduced. k -anonymity publishes data with low precision through generalization and concealment technology, which makes each record at least have the same quasi-identifier attribute value as other $k-1$ records in the data table, so as to reduce the privacy leakage caused by link attacks.

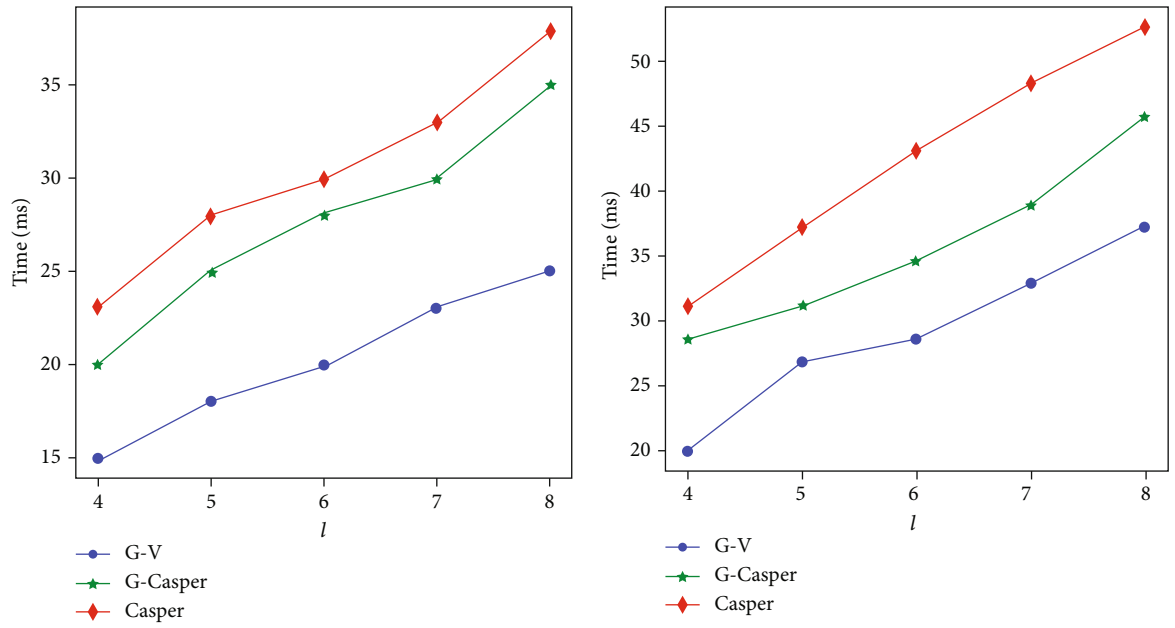
Under the condition that the length l of the Geohash code is unchanged, the algorithm in this paper is compared with the G-Casper and Casper algorithms in terms of antiattack. The result is shown in Figure 12. The x-axis represents the size of the anonymous area, and the y-axis represents the attack resistance of the algorithm. The larger the anonymous area, the stronger the algorithm's resistance to chain attacks. The algorithm proposed in this paper converts the location coordinates into Geohash codes, and Geohash codes represent a region, not a location. Therefore, the location is blurred, showing strong resistance to attacks. The second is the G-Casper algorithm. The Casper algorithm is weaker against attacks.

When the anonymous domain k is unchanged, the algorithm in this paper is compared with the G-Casper and Casper algorithms in terms of antiattack. The result is shown in Figure 13. The x-axis represents the length of the Geohash code, and the y-axis represents the attack resistance of the



(a) Gowalla (b) POI

Figure 10: The running time of the algorithm when the l is unchanged.

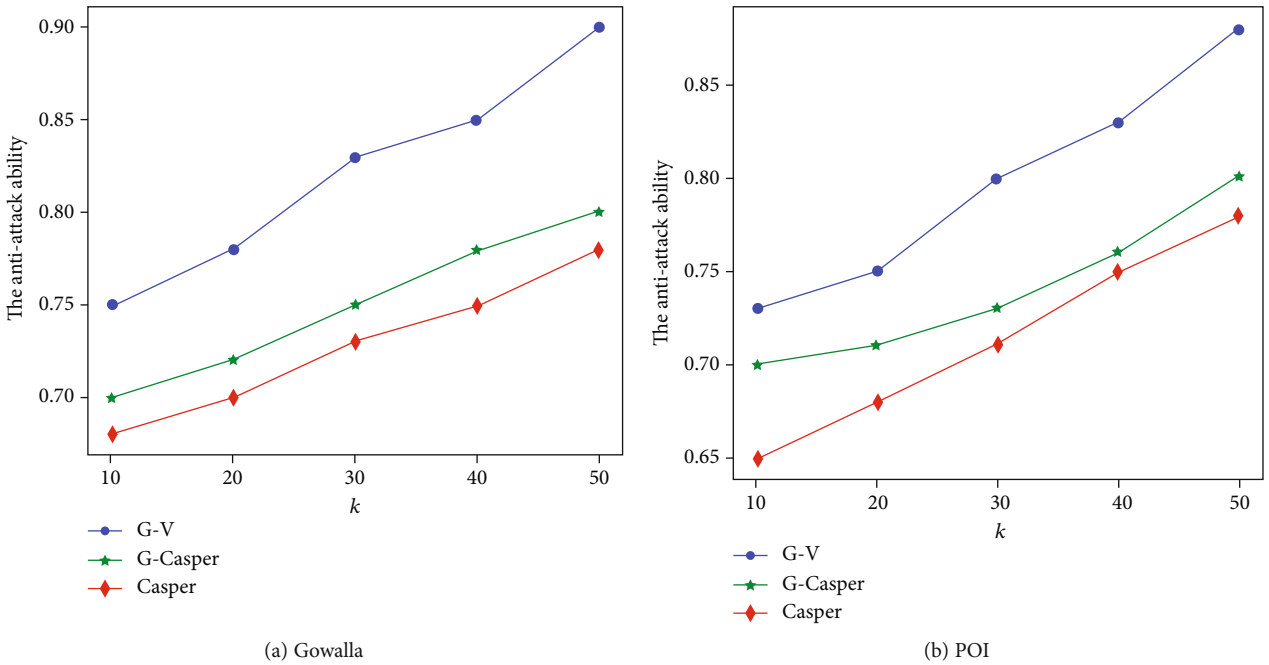


(a) Gowalla (b) POI

Figure 11: The running time of the algorithm when the k is unchanged.

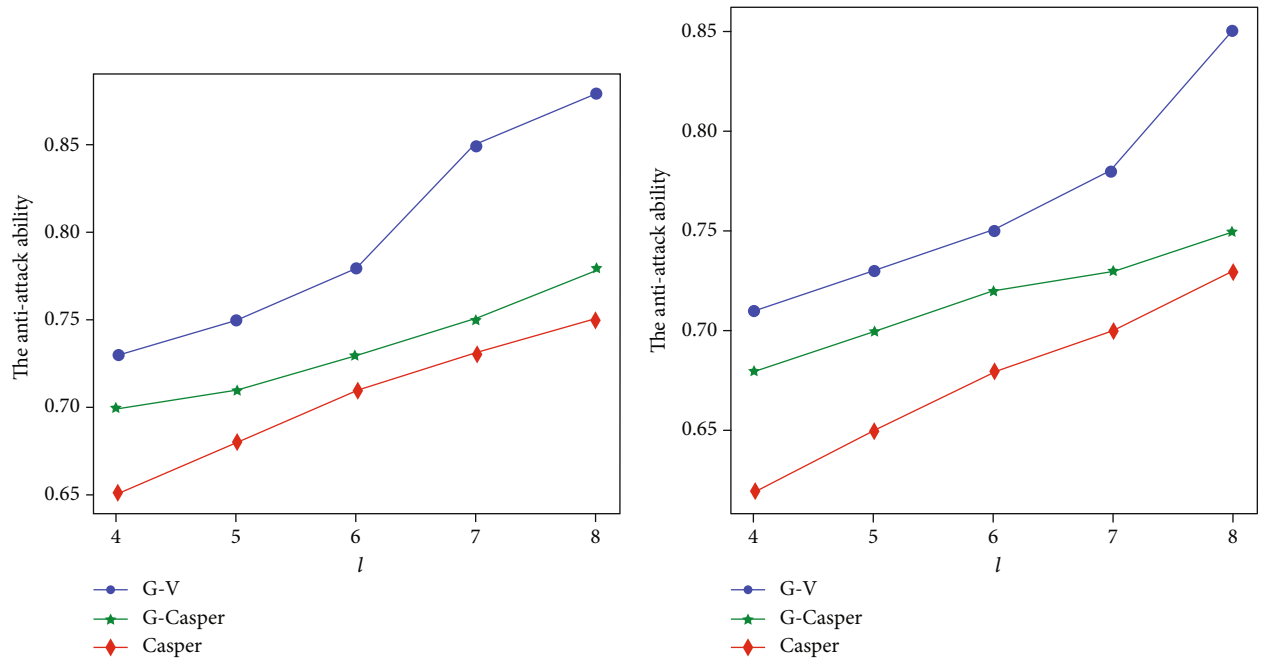
algorithm. The larger the code length, the stronger the algorithm's resistance to chain attacks. The algorithm proposed in this paper adopts a prefix tree structure, which has a strong antiattack, followed by the G-Casper algorithm, and the Casper algorithm is weaker.

5.6. Discussion Section. The design features of the algorithm in this paper are as follows. On the client side, the Geohash algorithm is proposed, which converts the user's location coordinates into a Geohash code of the corresponding length. On the server side, the Geohash code generated by the user is inserted into the prefix tree, the prefix tree is used to find the nearest neighbors according to the characteristics of the coded similar prefixes, and the Voronoi diagram is used to divide the area units to complete the pruning. Then, using the Geohash coding model and the Voronoi diagram grid



(a) Gowalla (b) POI

Figure 12: The antiattack of the algorithm when the l is unchanged.



(a) Gowalla (b) POI

Figure 13: The antiattack of the algorithm when the k is unchanged.

division principle, the G-V anonymity algorithm is proposed to find k neighbors in an anonymous area so that the user's location data meets the k-anonymity requirement in the area unit, thereby achieving anonymity protection of location privacy.

Traditional location privacy protection methods mostly use GPS locations to calculate anonymous areas. Anonymous servers use an anonymous area that satisfies k-anonymity instead of the user's real location for query processing. This often requires the server and the user to perform a lot of GPS calculations. This article uses the Geohash code instead of GPS location and then inserts the Geohash code into the prefix tree, which saves time. Since the G-V anonymity algorithm assumes that the third parties and mobile users involved in the calculation are credible, future research work can be carried out on semitrusted or untrusted third parties

or users in the system. The *k*-anonymity technology can resist chain attacks but cannot resist background knowledge attacks, homogenization attacks, and supplementary data attacks. Future work will consider how to better resist the above attacks and better protect users' privacy.

6. Conclusions

The rapid development of IoT technology promotes the rise of LBS, which brings a lot of convenience to people's lives, but it also brings severe challenges to the privacy security of users. Location data usually relates to the user's privacy information. Once the location information is leaked, it will bring serious threats to the user's privacy. In this paper, based on the Geohash coding model and Voronoi diagram meshing principle, we propose a location privacy protection method for road networks. We use the third-party server architecture. In the third-party server, the prefix tree is used to compare the Geohash code to find the nearest neighbors. Voronoi is used to complete the pruning. Then, the number of remaining users determines whether to generate dummy elements. The dimensional coordinates are reduced to a one-dimensional array, avoiding the calculation of floating-point numbers. The experimental result shows that the proposed anonymity algorithm has the advantages of short anonymity time, high success rate, and good service quality while ensuring privacy protection. Since the G-V anonymity algorithm assumes that the third party and mobile user participating in the operation are trusted, future research work can be carried out on the existence of the semitrusted or untrusted third party or user in the system.

Data Availability

All data, models, and codes generated or used during the study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the National Natural Science Foundation of China under grant nos. 61702316 and 61872088, the Natural Science Foundation of Shanxi Province under grant nos. 201801D221177 and 201901D111280, the Educational Research Projects of Young and Middle-Aged Teachers in Fujian Education Department under grant no. JAT170142, the Key Research and Development Project of Shandong Province under grant no. 2019JZZY010134, the Graduate Education Reform Research Project of Shanxi Province under grant no. 2020YJJG145, the Guangxi Key Laboratory of Trusted Software under grant no. KX202042, the Opening Foundation of Fujian Provincial Key Laboratory of Network Security and Cryptology Research Fund, Fujian Normal University under grant no. NSCL-KF2021-06, and the Natural Science Foundation of Fujian Province under grant no. 2019J01276.

References

[1] H. Huang, G. Gartner, J. M. Krisp, M. Raubal, and N. van de Weghe, "Location based services: ongoing evolution and research agenda," *Journal of Location Based Services*, vol. 12, no. 2, pp. 63–93, 2018.

[2] R. Gupta and U. P. Rao, "A hybrid location privacy solution for mobile LBS," *Mobile Information Systems*, vol. 2017, Article ID 2189646, 11 pages, 2017.

[3] R. Gupta and U. P. Rao, "VIC-PRO: vicinity protection by concealing location coordinates using geometrical transformations in location based services," *Wireless Pers Commun*, vol. 107, no. 2, pp. 1041–1059, 2019.

[4] R. Gupta and U. P. Rao, "Achieving location privacy through CAST in location based services," *Journal of Communications & Networks*, vol. 19, no. 3, pp. 239–249, 2017.

[5] X. S. Xue and J. F. Chen, "Using Compact Evolutionary Tabu Search algorithm for matching sensor ontologies," *Swarm and Evolutionary Computation*, vol. 48, pp. 25–30, 2019.

[6] X. S. Xue, X. Wu, C. Jiang, G. Mao, and H. Zhu, "Integrating sensor ontologies with global and local alignment extractions," *Wireless Communications and Mobile Computing*, vol. 2021, 10 pages, 2021.

[7] J. B. Xiong, J. Ren, L. Chen et al., "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1530–1540, 2019.

[8] J. B. Xiong, R. Ma, L. Chen et al., "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4231–4241, 2020.

[9] J. Zhang, B. Zhong, B. Fang, and J. Ding, "An improvement of track privacy protection method based on K-anonymity technology," *Intelligent Computer and Applications*, vol. 9, no. 5, 2019.

[10] A. Mille, L. Karim, J. Almhana, and N. Khan, "Location privacy-preserving mobile crowd sensing with anonymous reputation," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1812–1817, Limassol, Cyprus, 2020.

[11] N. Ravi, C. M. Krishna, and I. Koren, "Enhancing vehicular anonymity in ITS: a new scheme for mix zones and their placement," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 10372–10381, 2019.

[12] R. Zhang, X. Wang, P. Cheng, and J. Chen, "A novel pseudonym linking scheme for privacy inference in VANETs," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, pp. 1–5, Antwerp, Belgium, 2020.

[13] Q. A. Arain, D. Zhongliang, I. Memon et al., "Privacy preserving dynamic pseudonym-based multiple mix-zones authentication protocol over road networks," *Wireless Personal Communications*, vol. 95, no. 2, pp. 505–521, 2017.

[14] L. Benarous, B. Kadri, S. Bitam, and A. Mellouk, "Privacy-preserving authentication scheme for on-road on-demand refilling of pseudonym in VANET," *International Journal of Communication Systems*, vol. 33, no. 10, 2020.

[15] X. Ye, J. Zhou, Y. Li, M. Cao, D. Chen, and Z. Qin, "A location privacy protection scheme for convoy driving in autonomous driving era," *Peer-to-Peer Networking and Applications*, vol. 14, no. 3, pp. 1388–1400, 2021.

[16] L. Zhao, X. Wang, and X. Huang, "Verifiable single-server private information retrieval from LWE with binary errors," *Information Sciences*, vol. 546, no. 2, 2021.

[17] H. Sun and S. A. Jafar, "The capacity of symmetric private information retrieval," *IEEE Transactions on Information Theory*, vol. 65, no. 1, pp. 322–329, 2019.

[18] J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes," *Information Sciences*, vol. 526, pp. 166–179, 2020.

[19] S. Gupta and G. Arora, "Use of homomorphic encryption with GPS in location privacy," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, pp. 42–45, Mathura, India, 2019.

[20] I. Memon, Q. A. Arain, H. Memon, and F. A. Mangi, "Efficient user based authentication protocol for location based services discovery over road networks," *Wireless Personal Communications*, vol. 95, no. 4, pp. 3713–3732, 2017.

[21] I. Memon and Q. A. Arain, "Dynamic path privacy protection framework for continuous query service over road networks," *World Wide Web*, vol. 20, no. 4, pp. 639–672, 2017.

[22] Q. A. Arain, R. A. Shaikh, and H. Memon, "User privacy protection based on road network model for location based services," *Journal of Information & Communication Technology (JICT)*, vol. 10, 2016.

[23] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Generation Computer Systems*, vol. 94, pp. 40–50, 2019.

[24] K. Zhou and J. Wang, "Trajectory protection scheme based on fog computing and K-anonymity in IoT," in *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 1–6, Matsue, Japan, 2019.

[25] X. Yang, L. Gao, H. Wang, J. Zheng, and H. Guo, "A semantic k-anonymity privacy protection method for publishing sparse location data," in *2019 Seventh International Conference on Advanced Cloud and Big Data (CBD)*, pp. 216–222, Suzhou, China, 2019.

[26] I. Santos, E. Coutinho, and L. Moreira, "K-anonymity technique for privacy protection: a proof of concept study," in *2019 Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pp. 391–396, Português (Brasil), 2019.

[27] Y.-H. Zhou, G.-H. Li, Y.-G. Yang, and W.-M. Shi, "Location privacy protection nearest neighbor querying based on Geohash," *Computer Science*, vol. 46, no. 8, pp. 212–216, 2019.

[28] S. Guochao, C. Guanghui, and W. Shaoxin, "Location privacy protection approach based on interval region," *College of Computer Science and Engineering*, vol. 56, no. 8, pp. 66–73, 2020.

[29] Y. Zhong, T. Wang, C. Gan, and X. Luo, "The location privacy preserving scheme based on Hilbert curve for indoor LBS," in *Advances in Swarm Intelligence*, Y. Tan, Y. Shi, and B. Niu, Eds., pp. 387–399, Springer, 2019.

[30] X. Sun, Y. Sun, Z. Xia, and J. Zhang, "The one-round multiplayer discrete Voronoi game on grids and trees," *Theoretical Computer Science*, vol. 838, pp. 143–159, 2020.

[31] Y. H. Zhang, Y. J. Gong, Y. Gao, H. Wang, and J. Zhang, "Parameter-free Voronoi neighborhood for evolutionary multimodal optimization," *IEEE Transactions on Evolutionary Computation*, vol. 24, no. 2, pp. 335–349, 2020.

[32] H. Kaplan, W. Mulzer, L. Roditty, P. Seiferth, and M. Sharir, "Dynamic planar Voronoi diagrams for general distance functions and their algorithmic applications," *Discrete & Computational Geometry*, vol. 64, no. 3, pp. 838–904, 2020.

[33] X. Zhao, D. Pi, and J. Chen, "Novel trajectory privacy-preserving method based on prefix tree using differential privacy," *Knowledge-Based Systems*, vol. 198, 2020.

[34] Y.-H. Zhou, G.-H. Li, Y.-G. Yang, and W.-M. Shi, "Location privacy preserving nearest neighbor querying based on Geohash," *Computer Science*, vol. 46, no. 8, 2019.

[35] K. Cao, Q. Sun, H. Liu, Y. Liu, G. Meng, and J. Guo, "Social space keyword query based on semantic trajectory," *Neurocomputing*, vol. 428, 2021.

[36] K. Xing, Y. Luo, X. Ning, and X. Zheng, "Location privacy protection algorithm based on Geohash encoding," *Computer Engineering and Applications*, vol. 55, no. 1, pp. 102–108, 2019.

[37] C. Y. Chow, M. F. Mokbel, and W. G. Aref, "The new Casper: query processing for location services without compromising privacy," *ACM Transactions on Database Systems*, vol. 34, 2009.