# A Method of Constructing Arc Edge Anonymous Area Based on LBS Privacy Protection in the Internet of Vehicles

Peng-Shou Xie, Xue-Ming Han, Tao Feng, Yan Yan, and Guo-Qiang Ma
*(Corresponding author: Xue-ming Han)*

School of Computer and Communications, Lanzhou University of Technology
No.287 Lan-gong-ping Road, Lanzhou, Gansu 730050, China
(Email: hxmhan@163.com)

*(Received Oct. 9, 2019; Revised and Accepted Jan. 6, 2020; First Online Feb. 9, 2020)*

## Abstract

For the users of Internet of Vehicle, a larger value of the privacy protection factor K means the privacy can be better protected. However, too excessive value of safety factor will cause the decrease of query quality and the accuracy of location information in the Internet of Vehicles. In order to balance the contradiction between privacy protection security and query service quality caused by the accuracy of location information, an arc-edge anonymous area constructing method is proposed based on the location k-anonymity principle, which is used to optimize and improve the boundary-based polygonal anonymous region. Experiment results show that the generalization area can effectively reduce the anonymous region and the relative anonymity, which improves the quality of service on the basis of satisfying the privacy of the Internet of Vehicles.

*Keywords: Anonymity; Anonymous Regions Constructed; Arc Edge Anonymous Area; Internet of Vehicles; Location Privacy*

## 1 Introduction

With the continuous development of the Internet of Things, and the increasing popularity of various networks, such as Wifi and the rapid spread of 4G cellular networks, people are increasingly relying on location-based services. For example, check out nearby supermarkets and restaurants, how to find the nearest subway station, *etc.* The Internet of Vehicles comes from the Internet of Things, which can be used in multiple areas [3]. The Internet of Vehicles is also called the vehicular ad hoc networks (VANETs) [5], which is designed to provide vehicle-to-vehicle (V2V) communication and vehicle to infrastructure (V2I). The system of Internet of Vehicles mainly includes onboard unit (OBU), application unit (AU) and road side unit [4] (RSU). OBU is mainly used to exchange information with OBUs in other vehicles or with RSUs; AUs are mainly devices that use OBU's communication capabilities to implement communication functions; RSUs are wireless access devices along both sides of the road or dedicated fixed locations. In the Internet of Vehicles, data transmission and sharing operations are realized through wireless access technology. Location-Based Service (LBS) is a location-based server that provides value-added services to users based on their own location information provided by mobile users.

GPS and location-based services bring great convenience to people's travel and can be used in many industries. But at the same time, personal privacy leaks have become a serious problem [7, 8]. Personal occupation, hobbies, and health conditions are easily leaked, and personal identity information may be fraudulently used. It's no exception for the Internet of Vehicles. A series of information such as the location and trajectory of the vehicle are easily leaked, and these leaks provide convenience to the attacker [1]. So how to protect LBS-based location services is a hot issue studied by many scholars today.

Dummy position and pseudonym [18], cryptography [19] and fuzzy generalization [2] are common methods for location privacy protection. The earliest example of applying K-anonymity to location privacy protection is to generalize an area containing K users into a rectangular plane on the plane.The user send a request to the LBS anonymous server by the area, so that the probability of the user being attacked is 1/K. Rectangle area generalization is considered as an effective k-anonymity privacy protection model [10], which has certain security performance. And many subsequent studies are basically based on this idea. Later scholars adopted a quad-tree structure and indexed blocks to calculate anonymity [12]. Later the P2PSC algorithm was proposed [11], which forms an anonymous region through P2P and multi-hop communication. Lin Ying used Hilbert method to further optimize

the anonymous region, and some invalid grids were reduced [9]. But this approach puts itself in the center of the anonymous zone which is easy to be attacked. In addition to rectangular anonymous areas, circularly divided anonymous areas are also used for privacy protection [14]. Jia Zongqi proposes a privacy protection method based on fan-shaped anonymous region aiming at the problem of weak anti-central attack ability [6], Experiments show that anonymous performance and energy consumption can achieve good results under different user densities. Later scholars proposed the SCABGE algorithm [13], they divide the plane into multiple grid planes, and continually doubles to find the anonymous areas that meet the requirements, and caches the results. But this method will also leak the user's location. In addition to the regular graphics being used for anonymous areas, boundary-based polygons are also used in anonymous areas [15].

In the Vento-based location privacy nearest neighbor query method [20], In order to solve the problem that spatial anonymous regions are vulnerable to multiple queries and inference attacks, Zhou Yihua constructed a random k-hidden set to satisfy the location k-anonymity and l-diversity. The grid distance between the random k-hidden sets is greater than the threshold S. Using private information retrieval protocol to ensure the privacy of query results in the retrieval process, and the service provider provides the location-based services to the users without knowing the accurate query results of the users. Pei Zhuoxiong considered the query service area of location service providers [17], Introduce it into anonymous region construction. Generate subdomain areas and merge them according to the size of service providers finally the quality of the query service is improved. Aiming at the problems of high communication overhead, low anonymity efficiency and low success rate in the formation of location privacy protection anonymous area under mobile point-to-point (P2P) architecture, Xu Mingyan proposed a distributed user awareness scheme [16], it Recommends privacy parameters and search radius for candidate users according to user distribution characteristics and help users quickly form anonymous areas. The simulation results show that the algorithm has low communication overhead and high success rate. However, some of the above methods have a large anonymity area, some do not consider the center attack, some reduce the quality of the query, Some increase the amount of calculation and thus lower the quality of service.

From these aspects, We improve the arc-edge anonymity area based on location-based service privacy protection in Internet of Vehicles. The system structure is based on a central server structure. The algorithm is based on k-anonymity, starting from the initiator, forming a gradually expanding polygon, Searching the networking object from the counterclockwise direction. As the polygon expands, until the K target objects form an anonymous polygon area. And finally the arc polygon is constructed, the initiator of this algorithm is a virtual object, the real object is located at a random position of the arc-edge polygon, Central attack is effectively avoided. At the same time, since the anonymous area is an arc-side polygon, the anonymous area is reduced and the quality of service is improved.

# 2 Process of Constructing Arc Edge Polygon

## 2.1 Architecture

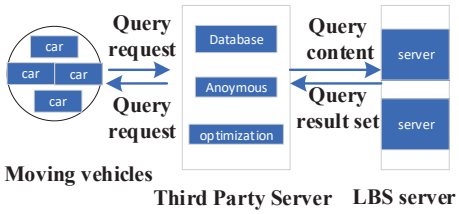


Figure 1: Architecture of location-based privacy protection anonymous system for Internet of Vehicle

Limited by bandwidth between vehicles and LBS server, The anonymous system structure of the privacy protection of the Internet of Vehicle consists of three parts to meet the real-time anonymity process. As shown Figure 1. The first part is vehicle network, the second part is the central anonymous server, It's used for anonymous related processes. The third part is the LBS server, which is used to process data and return or receive requests for location services. Data is transmitted between the vehicle and a third-party anonymous server using a secure channel, such as SSL. And the third-party anonymous server hides vehicle IP, identity and geographic information. Each vehicle is equivalent to a node, which has the ability of communication and data processing, and it can receive GPS signals with positioning function. Vehicle Nodes can communicate with other intelligent terminal nodes by single or multiple hops. Nodes self-organize through 3G/4G/Wi-Fi network and communicate with base stations and roadside units. Finally, the location request is sent to the third party central server. The central server carries out the process of vehicle anonymity and generalizes the network node anonymity to form a K-anonymous node set. Then the third party server sends the anonymous set to the LBS location server. The LBS location server performs location query after authentication. Finally, the query results are returned to the third-party server, and the third-party server returns the final results to the proxy point vehicle. The proxy point broadcasts the results to the vehicle network node in the anonymous area. After the request node is broadcasted by the query results, it calculates the location, and finally obtains the required information. This is the service process of the Anonymous Structure Diagram of Internet of Vehicle.

The query process is showed in Figure 2.

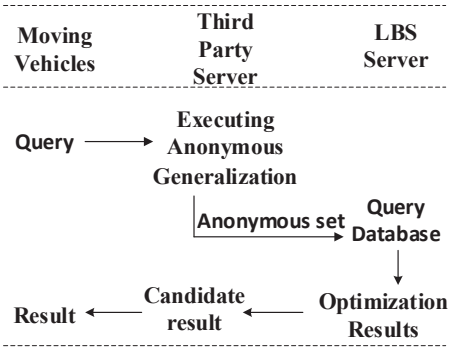


Figure 2: Query process

The paper is based on certain assumptions:

1) Moving vehicles and Third Parity server are trusted, and LBS is semi-trusted, providing services to users. And users' privacy may be leaked.

2) Attackers can obtain some prior knowledge through public databases. At the same time, they have the ability to analyze and reason, and can obtain delayed knowledge through anonymous information and prior knowledge.

3) The distribution of vehicles has certain rules, but has different distribution density.

## 2.2 Related Instructions

1) K-Anonymity: The k-anonymity mechanism requires that each record in the table be at least consistent with the quasi-identifier of the k-1 records in the table. In short, it means that a user cannot be distinguished from another k-1 users at least. The algorithm is also based on this basic principle, K users are placed in a region of a specific generalized area.

2) The Anonymous demand parameter Q: $\{(x_q,y_q),d_q,\text{k},s_{min},s_{max},t_q\}$, Different node privacy requirements are not necessarily the same. Q represents the set,$(x_q, y_q)$ Represents the coordinates containing the request point, and $d_q$ represents the distance between the request point and the proxy point. K is a privacy requirement. The larger the K, the higher the privacy, indicating that more privacy protection is needed.$s_{min}$ represents the minimum area of anonymity, the smallest anonymous area that required to satisfy privacy requirements.$s_{max}$ represents the maximum anonymous area required for anonymity. Once this area is exceeded, It shows that the request scope is too large and the anonymity condition cannot be met, so the anonymous process will fail. The Internet of Vehicles is a dynamic network, and every moment the vehicle is in a dynamic change. Points added in the anonymous area will exit at the next moment.Therefore, we set a certain delay $t_q$ for it, and it is necessary to reanonymize when beyond this delay. Timeliness is a problem that must be considered. It is worth noting that the anonymous area S is not the bigger the better. Under normal circumstances, the larger S, the larger K, and the probability of being attacked is q=1/k, but the excessively large anonymous area will cause the resource consumption of the server. So set the interval for S. In this way, while satisfying the location privacy, the resource consumption of the server can also be reduced, As a result, the latency of server processing is reduced and the quality of service is improved.

3) Area control: Let the points of the arc-shaped polygons that make up the anonymous area be from the middle to the periphery: $\{(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots, (x_n, y_n)\}$, The distance between the request node and the proxy point d ≤ R. R is the maximum distance of the center of gravity of the anonymous polygon $G(x_0, y_0)$ to the node constituting the polygon of the anonymous region, *i.e.*:

$$R = Max\{\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2}\} \tag{1}$$

Among them, i=0,1,2,⋯ n, $x_0 = \frac{\sum_{i=1}^{n} x_i}{n}$, $y_0 = \frac{\sum_{i=1}^{n} y_i}{n}$. According to R, the size of the area can be controlled.

4) Process description of privacy protection: The agent point sends a broadcast to the surrounding vehicle node. The broadcast radius is r. The node closest to the agent point receives the broadcast first, and the surrounding nodes receive the message and return the confirmation message to the agent point. And the agent point calculates the anonymous basis according to the privacy requirement. Suppose that the number of nodes around the proxy point is N at this time, but the point required to form an anonymous region is K. Anonymous area S ∈ $[S_{min},S_{max}]$. K is positively related to S. Recorded as K∝ S.

**Step 1.** At this time, N< K, and the broadcast radius is r=$r_0$, the counting starts from the counterclockwise direction, and the angle $\alpha$ between the initial counting position and the x-axis of the Cartesian plane rectangular coordinate system is $0^0$. As the angle $\alpha$ increases, the point gradually increases. ($\alpha$ ∈ $[0^0,360^0]$).

**Step 2.** If N=K, the coordinates of the Kth point at this time are $k(x_k,y_k)$, r=$r_k$.

$$tan\alpha = \frac{y_k}{x_k}. \tag{2}$$

Perform the anonymous generalization process, calculate the area S of the arc-side polygon, and calculate the total delay $t_q$ of the anonymous process. If S ∈ $[S_{min}, S_{max}]$ and t<T, Anonymous process completed. otherwise if: S < $S_{min}$ or if S>$S_{max}$ or

timeout, the anonymity fails, and adaptive adjustment should be made at this time. Increase K or increase $S_{max}$.

**Step 3.** If there is still N<K, all the points added after the first broadcast are selected, and then the broadcast area is enlarged, let r=$r_1$, $\alpha = 0$, and $\alpha$ continues to increase. Calculate K again. If N=K at this time, perform Step 2. Otherwise continue this process until N=K. At this time, if S $\epsilon$[$S_{min}$,$S_{max}$], Anonymous process completed, otherwise the anonymity fails.

After the anonymity succeeds, The anonymous server sends the query result to the RSU. The RSU broadcasts the result, and the initiator receives the RSU broadcast and calculates the result that is needed. The entire process is completed at this time. As is shown in Algorithm 1.

**Algorithm 1** The process of anonymous generalization in the environment of Internet of Vehicles

Begin
$\alpha$=0, N=0, r=0; t=0 // Variable initialization
if N < K
r=$r_N$,$\alpha \uparrow$, N++; t++ // Start loop
if N < K
Go back to Step 3
else
Perform an anonymous generalization process and calculate the area S,calculate the total delay t
if S$\epsilon$ [$S_{min}$,$S_{max}$] $\bigvee$ t< $t_q$
succeed
else
failed
$S_{max} \uparrow$ // Adaptive adjustment if the anonymous //requirement is not met
or K++
Return to Step 3
End

## 2.3 Anonymous Generalization Area Process Description

The area of the polygonal area is currently superior. Because the polygon is based on the boundary, that is, there are some points on the vertices and edges of the polygon. We optimize and improve the polygonal region division to form an anonymous area of the arc-edge polygon. This anonymous area is better than a polygon only in terms of the area of the anonymous area. Treating the vehicle as a particle, Suppose there are K vehicles at a certain time that need to complete the network formation. That is, K particles are placed in a closed area. The area of this closed area directly affects the processing speed of the server, so we are trying to find a smaller anonymous area.

**Step 1.** First connect the outermost particles with a straight line to get a random polygon. Random means that the shape is not fixed. It is a polygon of any side. Usually it is a convex polygon. Let the number of sides be i, i=3, 4, 5... k. At this time, a polygon is obtained, such as the polygon formed by the dashed line segments of d, d1, d2, d3, d4, and d5 in Figure 3. The final result of the boundary-based polygon generalization region is similar to this polygon. And it's a convex polygon.

**Step 2.** Let the inner angles of the polygons be: $\theta_1$,$\theta_2$,$\theta_3$,$\cdots$ $\theta_n$, and select the minimum angle $\theta_{min}$ of the polygon. Starting the arc from the side number d,$d_2$,$d_3$,$\cdots$ $d_n$ in siquence, two points as the starting and ending points of one side of the arc. From the geometric knowledge:

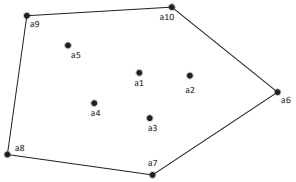


Figure 3: Anonymous region optimization process 1

$$sin(\frac{\theta_{min}}{2}) = \frac{d}{2r} \tag{3}$$

from which the radius of the arc is calculated:

$$r = \frac{d}{2\sin(\frac{\theta_{min}}{2})} \tag{4}$$

and an arc is made in each line segment. In the end a closed region is obtained, where d is the maximum of the two sides forming $\theta_{min}$. As is show in Figure 4.

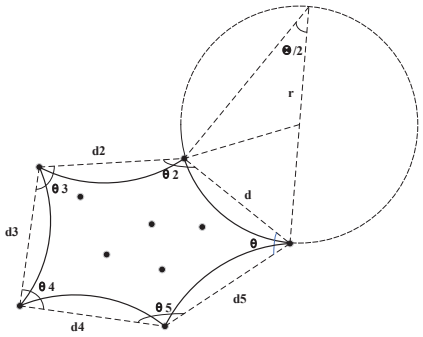


Figure 4: Anonymous region optimization process 2

**Step 3.** At this point, the area formed by the arc is obtained:

It can be seen from the image that the area of the arc side is smaller than the polygon, so it is superior. Here

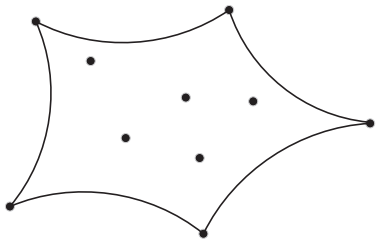

Figure 5: The resulting arc polygon

only the area of the arc and the area of the polygon are calculated. Then we only need to calculate the area $\Delta_s$ of the arc and the edge of the polygon. Let the area of the polygon be $s_p$ and the area enclosed by the arc edge be $s_a$, then get the Equation (5):

$$\begin{aligned}\Delta_s &= \sum_{i=1}^{n}(\frac{\pi r^2\theta_i}{360}-\frac{1}{2}r^2\sin\theta_i) \\ &= \sum_{i=1}^{n}[\frac{\pi r^2\theta_i}{360}-\frac{1}{2}(\frac{d}{2\sin(\frac{\theta_{min}}{2})})^2]. \end{aligned} \quad (5)$$

Simplify Equation (5) and get the Equation (6):

$$\Delta_s = \sum_{i=1}^{n}[\frac{\pi r^2\theta_i}{360}-\frac{d^2\sin\theta_i}{4\sin^2(\frac{\theta_{min}}{2})}] \quad (6)$$

Then Equation (7):

$$\begin{aligned} s_a = s_p - \Delta_s = \frac{1}{2}\{\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} + \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} + ..... + \\ \begin{vmatrix} x_n & y_n \\ x_1 & y_1 \end{vmatrix}\} - \sum_{i=1}^{n}[\frac{\pi r^2\theta_i}{360}-\frac{d^2\sin\theta_i}{4\sin^2(\frac{\theta_{min}}{2})}] \end{aligned} \quad (7)$$

So $s_a < s_p$. The time complexity for calculating the arc area is O(kn).

## 2.4 An Example of the Whole Process of Anonymous Generalization

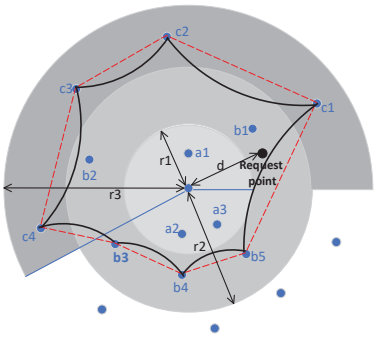


Figure 6: Anonymous generalization process of arc edge polygon

This is an example for whole process of anonymous generalization in the environment of the Internet of Vehicles.As shown in Figure 6, K=16 is taken as an example. When r=$r_1$, the angle is 0, and then the angle is continuously increased to 360 degrees. The nodes added in sequence are $a_1$, $a_2$, $a_3$, and when r=$r_2$, the scanning is gradually started from 0 degrees to 360 degrees. Adding the number of nodes $b_1$, $b_2$, $b_3$, $b_4$, $b_5$ in turn. Then join the request node, a total of 6 nodes. Similarly, r=$r_3$, adding $c_1$, $c_2$, $c_3$, $c_4$ in turn. This constitutes an anonymous area of K=16. After the generalization process, the shape is an arc-edge polygon.

# 3 Experiment and Analysis

## 3.1 Experiment Environment

The experiment used the Matalab 2018b environment. On Intel(R) Core i7-7700HQ CPU @2.80 GHZ processor, 16GB RAM. Nvidia GTX 1060 graphic display. Microsoft Windows 10 Professional operating system. The location simulation data of the mobile terminal is generated by the Thomas Brinkhoff road network data generator, using the traffic map of the German city of Oldenburg, to generate 2000 nodes.

Experiments start from three aspects: Hidden area, communication cost and relative anonymity. Compared with rectangular area, circular anonymous area and polygon anonymous area, demonstrated the superiority of an optimized anonymous area.

## 3.2 Analysis of Results

1) When the number of sides of the arc edge polygon is 6 and each arc edge is equal, we compare it to the perimeter and area of a regular hexagon. Let L be the perimeter and S be the area. It can be seen from Figure 7 that when the perimeters are equal, the arc-sided polygon has a smaller area. So, when the area is equal, the perimeter of the arc edge polygon is longer. In extreme cases, when all vehicles are distributed on the boundary,vehicles located on arc-side polygons are less likely to be attacked.

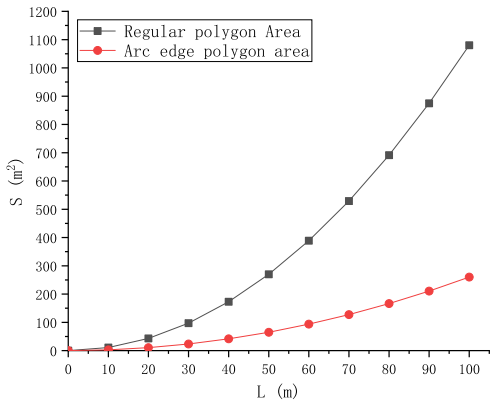


Figure 7: Relationship between perimeter and area

2) Anonymous areas : Comparing the arc-shaped polygon area with the rectangular area, the circular anonymous area, and the polygon anonymous area, it can be seen Figure 8 that the arc-side polygon area has the smallest area. The average anonymous area is an important indicator to measure the strength of privacy protection. Arc-shaped polygons are smaller and more flexible, and reduced invalid anonymous area, so the method in this paper has a smaller anonymous area. Therefore, the quality of service can be improved and the resource consumption of the server reduced.

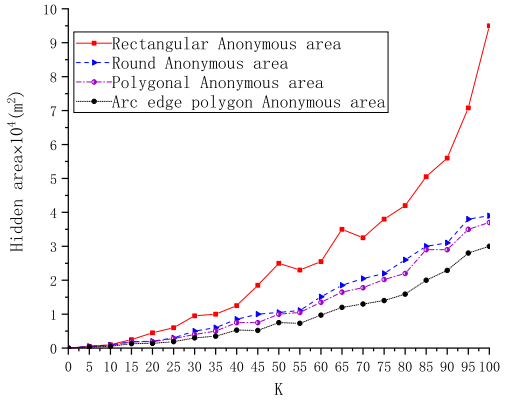


Figure 8: Comparison of different anonymous areas

3) Comprehensive evaluation index : The time consumption of the algorithm can be considered from the following aspects: anonymous waiting time $T_w$, anonymous processing time $T_d$, transmission delay $T_t$ and query time $T_q$. The algorithm consumption time can be expressed as:

$$T = T_w + T_d + T_t + T_q. \tag{8}$$

Anonymous waitting time and transmission delay time are usually ignored. Only considering anonymous processing time and query time. When considering the performance of the algorithm, only the anonymous processing time Td is considered. And the average anonymous time is generally used to measure the performance of the algorithm. As Equation (9).

$$\bar{T_d} = \frac{\Sigma T_d}{\Sigma U_s} \tag{9}$$

Us is a user who is anonymously successful and Td is the time this user spent anonymously.

The average anonymity time includes the total delay that constitutes the anonymous area. The total delay of the algorithm is roughly equal to the delay in forming the anonymous region. Because the methods that the anonymous made up area are more flexible, And there is also no time to adjust nodes. so the delay is reduced. The algorithm complexity is: O(kn), so anonymous time is acceptable.

The arc polygon segmentation process has an arc segmentation process, so the time consumption is slightly more. But the area of the anonymous is effectively reduced. In this method, the smaller the area and the less time consumed, the better the system performance. But it's difficult to reduce both time and area. Therefore, a comprehensive evaluation index EI is used to measure the effect of considering both time and area. As is showed in Equation (10).

$$EI = \bar{T_d} * S. \tag{10}$$

Among them, S is the anonymous area. The smaller the EI, the better the system performance. Figure is a comparison of EI. It can be seen from Figure 9 that the anonymous area with arc edges has better system performance.

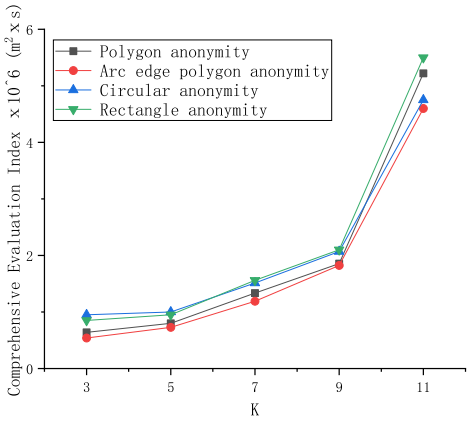


Figure 9: System performance comparison

4) Relative anonymity comparison:

$$K_{rel} = \frac{K_{act}}{K} \tag{11}$$

In Equation (11), Kact represents the number of vehicles that actually complete the anonymity, and K represents the number of vehicles that satisfy the K anonymity requirement. Due to the inherent properties of geometry, it is often difficult to accurately satisfy K anonymity in the actual anonymity process. There will be more than K vehicles in a fixed generalization area, so the number of users participating in anonymity tends to be larger than K. However, the anonymity of polygons and arc polygons is more flexible, the relative anonymity is smaller. And it is easier and more accurate to be controlled.

# 4 Conclusions

Privacy protection of Location-based service has become a research hotspot. How to provide better location privacy becomes a very important issue in privacy protection.

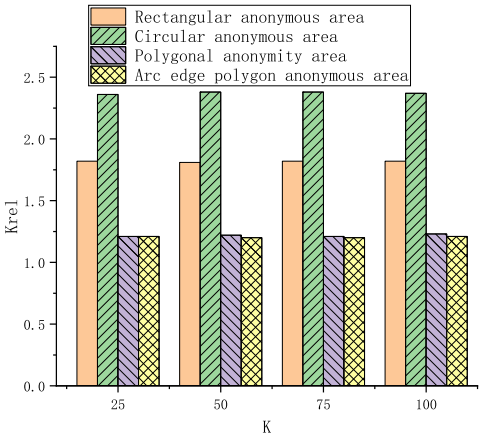


Figure 10: Relative anonymity

The paper compared some common anonymous region construction methods, such as rectangular anonymity, grid doubled, mesh layering, circular area division, sector division, and polygon division. On this basis, an arc-edge anonymous area constructing method is proposed to further reduce the anonymous areas. The proposed method improved service quality based on protecting user privacy in certain extent.

However, the proposed method also has some defects. The partition method is more complicated, and the time complexity is increased. The actual system of Internet of Vehicle is in a very complex environment, whether from the road network or the vehicle itself. From the perspective of road network, the method of regional generalization may not be entirely suitable because there are disturbances from buildings and other objects. So, it is a big challenge to design a regional construction method that fits the real Internet of Vehicle system. It is also the focus of the next step of research. Meanwhile, simplifying the partition method and reducing the time complexity are the further research contents.

## Acknowledgments

This study was supported by the National Natural Science Foundations of China under Grants No.61862040 and No. 61762060 and No.61762059, The authors gratefully acknowledge the anonymous reviewers for their helpful comments and suggestions.

## References

[1] R. A. Dhubhani, J. M. Cazala, "An adaptive geo-indistinguishability mechanism for continuous LBS queries," *Wireless Networks*, vol. 24, no. 8, pp. 3221–3239, 2018.

[2] P. Galdames, C. Gutierrez-Soto, A. Curiel, "Batching location cloaking techniques for location privacy and safety protection," *Mobile Information Systems*, vol. 2019, pp. 1–11, 2019.

[3] S. Hong, "Authentication techniques in the Internet of Things environment: A survey Sunghyuck Hong," *International Journal of Network Security*, vol. 21, no. 3, pp. 462–470, 2019.

[4] S. Ibrahim, M. Hamdy, E. Shaaban, "Towards an optimum authentication service allocation and availability in VANETs," *International Journal of Network Security*, vol. 19, no. 6, pp. 955–965, 2017.

[5] T. Jeyaprakash, R. Mukesh, "A new trusted routing protocol for vehicular ad hoc networks using trusted metrics," *International Journal of Network Security*, vol. 19, no. 4, pp. 537–545, 2017.

[6] Z. Jia, W. Liu, "Location privacy protection based on sector region in dynamic P2P network," *Computer Applications and Software (in Chinese)*, vol. 34, no. 3, pp. 316–328, 2017.

[7] H. Kang, W. Zhu, "Privacy protection of location services," *Journal of Shandong University (Science Edition)(in Chinese)*, vol. 53, no. 11, pp. 35–50, 2018.

[8] S. Liu, A. Liu, Z. Yan, W. Feng, "Efficient LBS queries with mutual privacy preservation in IoV," *Vehicular Communications*, vol. 16, pp.62–71, 2019.

[9] Y. Lin, Y. Xie, Y. Zhu, *et al.*, "Design and implementation of Hilbert's position k-anonymity algorithm based on spatial quartering," *Wuhan University Journal (Science Edition) (in Chinese)*, vol. 64, no. 3, pp. 225–230, 2018.

[10] S. Ni, M. Xie, Q. Qian, "Clustering based k-anonymity algorithm for privacy preservation," *International Journal of Network Security*, vol. 19, no. 6, pp. 1062–1071, 2017.

[11] A. S. Saxena, D. Bera, V. Goyal, "Modeling location obfuscation for continuous query," *Journal of Information Security and Applications*, vol. 44, pp. 130–143, 2019.

[12] G. Suna, V. Changc, *et al.*, "Efficient location privacy algorithm for Internet of Things (IoT) services and applications," *Journal of Network and Computer Applications*, vol. 89, pp. 3–13, 2017.

[13] D. Wu, X. Lu, "Anonymous region construction algorithm based on user cooperation in distributed architecture," *Computer Science (in Chinese)*, vol. 41, no. 4, pp. 90–94, 2019.

[14] X. Wu, M. Luo, "Privacy protection method based on location service in sparse environment," *Computer Engineering (in Chinese)*, vol. 43, no. 5, pp. 108–114, 2017.

[15] P. Xie, T. Fu, *et al.*, "An algorithm of the privacy security protection based on location service in the Internet of Vehicles," *International Journal of Network Security*, vol. 21, no. 4, pp. 556–565, 2019.

[16] M. Xu, H. Zhao, X. Ji, W. Shen, "Mobile P2P fast location anonymity algorithm based on user distribution perception," *Journal of Software (in Chinese)*, vol. 29, no. 7, pp. 1852–1862, 2018.

[17] Z. Zhai, X. Li, H. Liu, K. Lei, J. Ma, H. Li, "An anonymous zone construction scheme based on query range in LBS privacy protection," *Journal on Communications (in Chinese)*, vol. 38, no. 9, pp. 1311–1318, 2017.

[18] Y. B. Zhang, Q. Y. Zhang, Z. Y. Li, Y. Yan, and M. Y. Zhang, "A k-anonymous location privacy protection method of dummy based on geographical semantics," *International Journal of Network Security*, vol. 21, no. 6, pp. 937–946, 2019.

[19] L. Zhang, C. G. Ma, S. T. Yang, Z. P. Li, "CP-ABE based users collaborative privacy protection scheme for continuous query," *Journal on Communications*, vol. 38, no. 9, pp. 76–85, 2017.

[20] Y. Zhou, J. Du *et al.*, "Location privacy nearest neighbor query method based on Veno diagram," *Journal of Beijing University of Technology (in Chinese)*, vol. 44, no. 2, pp. 225–233, 2018.

## Biography

**Peng-shou Xie** was born in Jan. 1972. He is a professor and a supervisor of master student at Lanzhou University of Technology. His major research field is Security on Internet of Things.E-mail: xiepsh_lut@163.com.

**Xue-ming Han** was born in Jan. 1990. He is a master student at Lanzhou University of Technology. His major research field is network and information security. E-mail: hxmhan@163.com.

**Tao Feng** was born in Dec. 1970. He is a professor and a supervisor of Doctoral student at Lanzhou University of Technology. His major research field is modern cryptography theory, network and information security technology.E-mail: fengt@lut.cn.

**Yan Yan** was born in Oct. 1980. She is a associate professor and a supervisor of master student at Lanzhou University of Technology. Her major research field is privacy protection, multimedia information security.E-mail: yanyan@lut.cn.

**Guo-qiang Ma** was born in Jun. 1992. He is a master student at Lanzhou University of Technology. His major research field is network and information security.E-mail: magq1514@163.com.