Gao et al. EURASIP Journal on Wireless Communications and Networking (2016) 2016:205
DOI 10.1186/s13638-016-0708-z

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Location privacy protection algorithm for mobile networks

Kun Gao*, Yiwei Zhu, Songjie Gong and Hengsong Tan

Abstract

Mobile users often post nearest neighbor queries based on their current location. Usually, the mobile terminal (user) sends a request to query an untrusted location server, including the position information of the mobile terminal requests, thus leading to the disclosure of one's location. For mobile users providing location services, the privacy of mobile users is crucial. This demand is particularly evident in the mobile network application. According to the structural characteristics of the mobile network, the use of hidden ring and hidden tree can blur mobile subscriber location information in the mobile network and effectively ensure location privacy. This paper proposes a new method of protecting location privacy known as Hidden Ring and Hidden Forest (HRHF), which is the use of breadth-first search to meet certain requirements of the ring and forest in the graph. Based on experimental testing of real and simulated data sets, the HRHF method has demonstrated its effectiveness in protecting location privacy and efficiency in providing quality services.

Keywords: Location privacy, Location-based service, Mobile network

1 Introduction

In recent years, location-based services have been gradually integrated into everyday life and have consequently brought individuals greater convenience. For example, location service can be provided to a mobile user interested in queries such as, "where is the nearest bus stop?"; "how do I get to the station?"; and "is there traffic ahead?"

In order to utilize location-based services, mobile users must send their service provider accurate location information to fulfill the query request. Usually, the location service provider's server is not credible, and the location information of the user is vulnerable to theft. After stealing the location information of a mobile user, the thief, via location tracking or links to other public information (such as geographic database, encoding the phone book), may be able to confirm the user's identity and gain additional private information [1–3].

How can the location of mobile users be further protected? This problem has already aroused the attention of experts and scholars, and as a result, many solutions have been put forward. At present, most of the research revolves around mobile users in the mobile Euclidean space (free space), which is namely one's moving direction without any constraints. The main protection method used is the exact location of the user with a further comprise at least k −1 instead of individual regions of space, so that the attacker cannot obtain a person's location by way of inference attack to match its status. Simultaneously, this method uses much space area size and the number of included to measure the privacy protection provided by the user [4].

In reality, however, people either walk or ride a vehicle and always follow a fixed mobile network. As an illustration, a simple mobile network model with mobile users and their sites of interest is shown in Fig. 1. Obviously, in the highway network environment, you cannot use the size of the area of space to measure the strength of privacy, because the road network for two spatial regions of equal area, if one contains a link, and the other contains three sections, so to protect the strength of the latter than the former. In addition, the regional space contains only a section of the user that the attacker can easily use for tracking. As a result, space hidden no longer applies to the mobile network environment [5, 6].

In addition, in order to alleviate traffic pressure, many cities have implemented one-way traffic provisions, in

* Correspondence: kungao@live.com
Big Data Deep Analyzing Institute, Zhejiang Business Technology Institute, No. 1988 Airport road, Ningbo, China

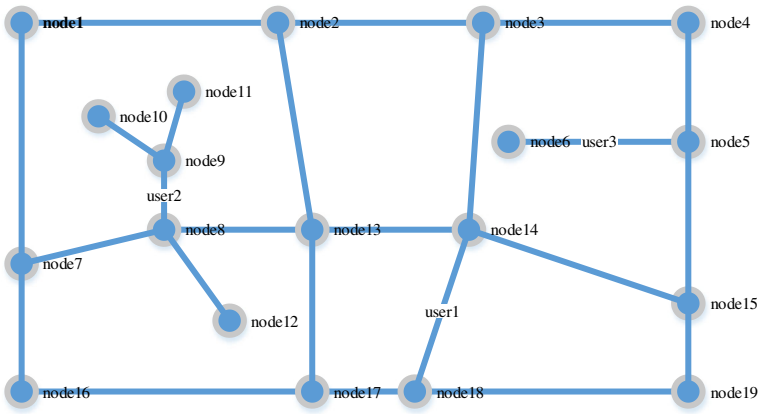

Fig. 1 A model of simple mobile network

which a vehicle can travel on some roads only in one direction. Diligent practice at home and abroad has proven that one-way traffic plays an important role in solving city traffic problems. Therefore, in the mobile network structure of a single line (complex mobile network), how can the protection of mobile user location privacy be ensured? This is a new challenge.

Challenge. The mobile network has its own characteristics; a tradeoff exists between location privacy protection based on efficiency and quality in location services. Excavating potential structural features in the mobile network to protect the mobile user's location privacy while providing high-quality services will be a significant challenge.

Contribution. Through the observation of simple and complex mobile network structures, two hidden subgraph structures have been defined: the cloaking ring and hidden tree (mobile user distribution and location privacy must meet certain requirements of the ring and the tree). The two hidden subgraph-based structures have brought forward a new method of location privacy protection—Hidden Ring and Hidden Forest (HRHF). This method not only can effectively protect a mobile user's location privacy but can also provide mobile users with high-quality location-based services. In addition, by considering that the mobile network consists of a single line and utilizing the HRHF, the network environment problems pertaining to complex mobile location privacy protection were successfully solved.

Section 2. reviews related work location privacy protection technology; Section 3. introduces the formal definition, and some background knowledge is provided to solve the problem; Sections 4. and 5. respectively introduce the simple model and construction of the mobile network in HRHF structure; Section 6. introduces the location privacy protection complex in the mobile network, the location privacy protection method, and gives the complete HRHF; the experimental results and analysis system will be introduced in Section 7.; and Section 8. summarizes the entire text.

2 Related work

In recent years, many methods have been brought forth to ensure the privacy protection of mobile users. These methods can be divided into two categories: spatial regions of occult [7–9] and false position [10–12]. Generally, space technology is used in the hidden location anonymity model k-. The model k-, first proposed in the literature [13–15], refers to the anonymous position occurring when the location information of at least one other individual and the position information of k-1 cannot be distinguished. As a result, the person's position to meet the position of k- becomes anonymous. Li et al. [16] also proposed an Interval Cloak algorithm based on binary tree 4. Given that the literature value of K is set in the system and does not meet the personalized needs of location privacy, Li and Jung [17] proposed that the k- anonymous user model could be customized to allow the user to specify the degree of anonymity, thereby proposing the Clique Cloak algorithm. Due to the anonymous success rate is low, Liu [18, 19] proposes an improved algorithm based on the directed graph [20]. Using Complete Pyramid Data Structure and Incomplete Pyramid Data Structure to maintain the location information of mobile users, and based on these two data structures, basic and adaptive algorithms were proposed. Ma et al. [21] have proposed a dynamic bottom-up and top-down grid hiding algorithm. Namiot and Sneps-Sneppe [22] propose Nearest Neighbor Cloak algorithm and Hilbert Cloak algorithm. The system architecture in the above literature consists of a central server structure [23, 24], which is used in distributed point-to-point structure. In Pan et al. [25], mobile users, before sending the query to the location server, send grouped requests first through to other peer nodes to form a space area, which will later be sent to the server along with the

query. Because the anonymous method will fail in many cases, Namiot [22] proposes a Hilbert space filling curve high k-anonymous space to build mechanisms to enhance anonymous success rates of the system. Puttaswamy et al. and Rahimi et al. [26, 27] use a false location technology. In Resch [28], mobile users generate a false position and location of their true position and send it to the server. Because the attacker cannot identify the true position of the user, the user's location privacy is effectively protected. In Puttaswamy et al. [26], mobile users only send specified false position. The server receives incremental nearest neighbor queries based on this false position, and query results are returned to the users; according to the returned results, the users no longer retrieve the answers they want.

The above assumes that all users are moving in a free space. However, in reality, people often walk in the mobile network. Shen and Zhao [29] first noticed this problem and brought forward the location privacy protection model XStar. However, Shen and Zhao [29] only consider the simple mobile network (all roads are double line) of the location privacy protection environment. This is considered to be simultaneously a both simple and complex mobile network (including the single line) on the basis of a new location privacy protection method based on a hidden subgraph.

3 Background knowledge and definition

This section describes the work closely related to the mobile network model, location anonymity system structure, mobile user location privacy, and problem definition.

3.1 Simple mobile network model

An undirected graph UG = (vertex, edge) can be used to represent simple mobile networks. For example, Fig. 1 shows a simple model of a mobile network. Each side of the model can be regarded as a moving double line. A vertex with 1 degree can be seen as the end of the network; a vertex with 2 degrees can be seen as the bend of the network; and a vertex with 3 degrees or more can be seen as the intersection of the network. In addition, the model also used small squares to represent mobile users, with a small dot indicating the location in which the mobile users are interested, such as shops, gas stations, and hotels.

3.2 Anonymous location system structure

The central server architecture [30], which is found between the mobile client and server-side position to add a trusted server, is commonly referred to as the anonymous location device. As shown in Fig. 2, location anonymity equipment will anonymity-process the user's accurate location information, and at the same time, it accurate processes the candidate results returned by the location server. The main work of this paper is to design an effective algorithm for the location of the anonymous device.

3.3 Mobile user location privacy

At present, two privacy protection models have been proposed: one being k- anonymity and the other is the road l- diversity. This paper combines these two models. The diversity of the mobile network model is proposed in [31–34]. In this system, if the user's location information to meet k- is anonymous, containing at least l different section, then the anonymous location satisfies road l- diversity. If an anonymous location contains only a link, then the attacker will easily track people traveling the road. On the contrary, if three or more sections of this anonymous location are present, then the tracking difficulty will increase. Furthermore, section l- diversity is an essential condition of user location privacy in the mobile network.

While K and L measure the location privacy protection strength parameters, this paper provides another parameter: $\text{Location}_{\max}$. $\text{Location}_{\max}$ outlined the number of sections containing an anonymous location in the upper limit. Although many sections of the number of users can provide strong privacy protection, this will result in a higher price for location server query processing and a decrease in service quality. In order to achieve balance in privacy protection, query processing cost, and service quality among the three, constraint parameters were proposed.

3.3.1 Definition 1: location privacy

K, Location, and $\text{Location}_{\max}$ represent the position of a mobile user's privacy, where K is the least amount of a mobile user's anonymous locations included and Location ($\text{Location}_{\max}$) represents the number of sections of an anonymous position included. Location privacy of

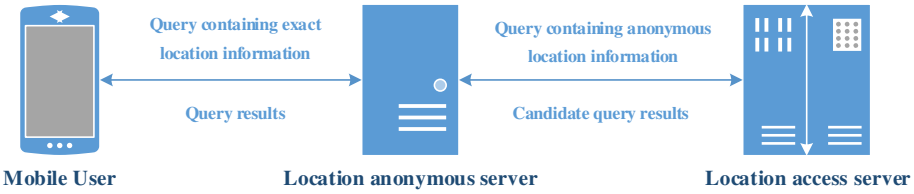

Fig. 2 Location anonymity architecture

user u (K, Location, and $\text{Location}_{\max}$) can be simply expressed as Privacy(user) = (K, Location, $\text{Location}_{\max}$).

The location privacy of a user by his own decision and the location privacy with accurate location information of the user's query will be sent to the anonymous device together.

3.4 Problem definition

Firstly, some assumptions about the attacker's background knowledge are required: the attacker must know in advance the location privacy protection algorithm and can obtain the number of mobile networks on each section. The problem provided in this paper is based on this definition.

Suppose there is a request for location-based services from a mobile user—the privacy of his or her position (K, Location, $\text{Location}_{\max}$). Then the position of the anonymous system should dictate how the mobile user finds a hidden section set S and make the S precise position cover not only u but also to meet Sk ' ≥ k, Location ≤ S. Location ' ≤ $\text{Location}_{\max}$. In addition, the attacker cannot infer a specific location U from S with high probability.

How do we extrapolate the user's specific location after stealing the hidden sections? Normally, the attacker in turn assumes that u is located in this section for each section S_i ($i = 1, 2,\ldots,$ L ') of S. Then the attacker will perform a location privacy protection algorithm on the section and get a hidden section set S'. It compares S' with S to reach the number of the same section of those two sets and the ratio of all sections in the S. Finally, the attacker deduces the probability of u belonging to the section S_i: $r_i/(r_1 + r_2 + \ldots r_3)$.

4 Simple hidden ring structure under mobile networks

This section first analyzes the protection characteristic of a simple mobile network and then introduces three steps to find the optimal hidden ring for users.

4.1 Hidden ring

The structural characteristics of the simple observation model in a mobile network are the result of the symmetry of the ring to the mobile user location privacy protection in the mobile network. Because for the ring, no matter which edge of the ring the attacker performs the lookup algorithm, he will get the same result, further deducing that the probability of each edge in the ring is equal. So the attacker cannot identify the user's edge (location), then the user's location privacy will be well protected.

The background knowledge of the attacker assumes that he or she knows the number of mobile users in each section, so it is possible for an attacker to use this information to exclude users where there can be no road. So, by the above analysis, the definition of a hidden ring is to protect the location privacy of mobile users.

4.1.1 Definition 2: hidden ring

A ring of an undirected graph, in which the number of mobile users and the number of sections it contains both meet the user's location privacy, has at least two sections of the mobile user.

In an undirected graph, covering a user's location may require more than one ring. For example, in Fig. 1, covering the user_1 ring with the exception of <node_{13}, node_{14}, node_{18}, node_{17}, node_{13}>, ring <node_{14}, node_{15}, node_{19}, node_{18}, node_{14}> and ring <node_{14}, node_{3}, node_{4}, node_{5}, node_{15}, node_{19}, node_{18}, node_{14}>, etc. So after finding his cover ring for the user, it must be determined whether these rings are the hidden rings. If more than one ring is in line with the concealed conditions, then one must select the number of sections and mobile subscribers closest to the user location privacy ring (called the ring for the optimal hidden ring) as users of the hidden position. This is because in all the hidden rings, the number of mobile users and sections will cause location server query processing cost to be higher. At the same time, it also can reduce the quality of mobile client service. So it is a necessary step to select the optimal hidden ring.

In order to be able to quickly find the optimal hidden ring, first, find the minimum coverage of the user's location and then determine whether these meet the hidden conditions. If only one ring meets the conditions, then it is the optimal hidden ring; if more than one ring simultaneously satisfies the conditions, then choose the optimal hidden ring; if no rings meet the conditions, then the number of mobile users and (or) section numbers is less than the user location privacy. Firstly, extend the ring and then determine whether the expansion ring meets hidden conditions. Finally, select the optimal hidden ring from the expansion ring.

4.2 Find the minimum ring

Using the method to map the width, first, search for users to discover the ring. In order to make the ring cover the location of the user, two edges must form where the end user is used as the initial search point and the target point of the minimum. First, based on the user's side, specify the starting point of the search and the target point (as in the undirected graph, whether to specify which endpoint is the starting point of the user or to find the minimum ring end is the same, so the starting point can be any two points. If the starting point is selected, then another endpoint becomes the target point). Then when the search reaches the vertex of the target point, the minimum ring covering the user's

location must be found. Next, use the recursive method to find the minimum edge of the structure from the access over the edge. The small details are found in algorithm 1.

Algorithm 1. Find the minimum ring.

Input: undirected graph G; user id; access vertex queue Q; access edge vector V

Output: constituting the respective sides of the minimum ring

1. According to the $User_{id}$ positioning the user's edge;
2. To obtain the relevant information $User_{info}$ on the edge;
3. Specify the starting point $Point_{start}$ and stopping point $Point_{stop}$ for the search;
4. Set all the vertices and edges of the G is not accessible;
5. Access vertex $Point_{start}$, $Point_{stop}$ and edge $Edge_{start\text{-}stop}$;
6. $Point_{start}$ into the queue Queue
7. While Queue is not empty
8. Head element out of Queue, and assigned it to the variable Variable;
9. for each adjacent vertices Vertice of Variable;
10. if Vertice is not accessible
11. access Vertice and insert into Queue;
12. access edge $Edge_{variable\text{-}vertice}$, get the information on the edge $Edge_{variable\text{-}vertice}$, and save (Variable, Vertice, $User_{info}$ to vector Vector;
13. Else
14. If $Edge_{variable\text{-}vertice}$ is not accessible
15. access edge $Edge_{variable\text{-}vertice}$, get the information on the edge $Edge_{variable\text{-}vertice}$, and save (Variable, Vertice, $User_{info}$ to vector Vector;
16. End if
17. End if
18. If Variable = $Point_{stop}$ and Vertice <>$Point_{start}$
19. insert ($Point_{start}$, $Point_{stop}$, $User_{info}$) into Vector;
20. Using recursive method to find respective edges constituting the smallest ring, and output;
21. End if
22. End for
23. End while

In Fig. 3, we take $user_1$ as an example to illustrate the minimum ring discovery process. First, because $user_1$'s edge is $node_{14}node_{18}$; $node_{18}$ should be specified as the starting point with $node_{14}$ as the stopping point (in Fig. 3a, gray solid circles represent the starting point and target point of the search). Then, all the vertices and edges of undirected graph G not being accessed should be set, with node14, node18 and $node_{14}node_{18}$ edges and vertices accessed. Search starting from $node_{18}$, the first access adjacent to point $node_{17}$, $node_{19}$, and the adjacent edge $node_{18}node_{17}$, $node_{18}node_{19}$, $node_{18}node_{17}$, and $node_{18}node_{19}$ which is not accessed by $node_{18}$. In the meantime, preserve the edge information of $node_{18}$-$node_{17}$and $node_{18}node_{19}$. Similarly, the adjacent nodes and edges (which cannot be accessed by $node_{17}$ and $node_{19}$) $node_{13}$, $node_{16}$, $node_{15}$, $node_{17}$ $node_{13}$ and $node_{19}node_{15}$ will be accessed in turn. When the adjacent $node_{14}$ is accessed, the minimum ring will be discovered. Finally, the two minimum rings for $user_1$ were found in these cases: "$node_{18}$, $node_{17}$, $node_{13}$, $node_{14}$, $node_{18}$" and "$node_{18}$, $node_{19}$, $node_{15}$, $node_{14}$, $node_{18}$." The thick lines in Fig. 3a show from the starting point to the target point $node_{18}$ $node_{14}$ accessed path. At the same time, the dotted lines in Fig. 3b show two minimum rings for $user_1$ found in the simple model mobile network.

4.3 Select the optimal hidden ring

After the statistics on the number of sections and each minimum ring on the mobile user, for those who meet the conditions of the minimum hidden ring, formula (1) can be used to measure the proximity of each privileged ring and user location privacy that is scoring for each ring hidden. The higher the score, the closer to the user's location privacy.

$$\text{rank} = (\alpha_i.\delta_j)/\delta_k + (\alpha_k.\varepsilon_p)/\varepsilon_c \quad (1)$$

In formula (1), α_i and α_k are two weight coefficients and their values are between 0 and 1, and $\alpha_i + \alpha_k = 1$. δ_j and ε_p represent the number of sections and the mobile

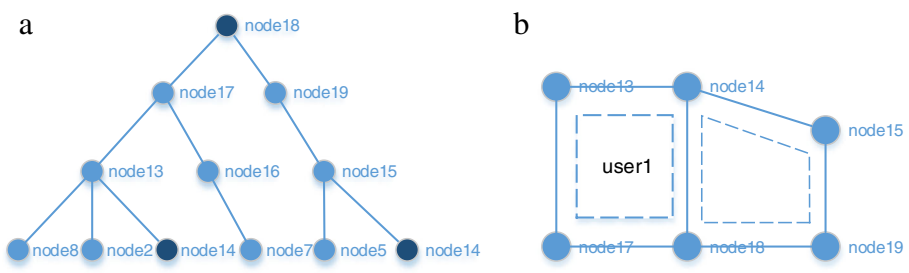

Fig. 3 Using breadth-first search for discovering minimum ring of $user_1$. **a** Discovering the minimum ring for $user_1$. **b** Minimum ring in simple mobile network

user in location privacy requirements, respectively, while δ_j and ε_p represent the number of mobile users and sections contained in the hidden ring, respectively. When $\delta_j = \delta_k$, $\varepsilon_p = \varepsilon_c$, the rank reached the maximum value of 1. Theoretically, the number of sections has a greater impact on the cost of query processing and, therefore, pays more attention to the close degree of ε_p and ε_c.

4.4 Expansion of the minimum ring

Expansion of the minimum ring occurs when the number of users and sections is less than the user location privacy and (or) the ring is provided with a mobile user number less than 2. With similar methods, begin with the smallest ring. First, save the vertices in which the vertex degree is greater than 2 in the minimum ring, then choose the starting point and target points of the search from these vertices. Next, search the extension of the minimum ring based on each pair of the starting point and the target point.

For example, in the minimum ring of $user_1$ <$node_{18}$, $node_{17}$, $node_{13}$, $node_{14}$, $node_{18}$>, if you choose ($node_{14}$, $node_{13}$) as the starting point and the target point, respectively, you can obtain the ring <$node_{14}$, $node_3$, $node_2$, $node_{13}$, $node_{17}$, $node_{18}$, $node_{14}$>; if you choose ($node_{13}$, $node_{17}$), you can get the ring <$node_{14}$, $node_{16}$, $node_{17}$, $node_{18}$, $node_{14}$>. In order to ensure that the expanded ring can still override the user's location, it cannot be selected ($node_{14}$, $node_{18}$) again as the starting point and destination of the search.

5 Constructing the hidden tree under simple mobile networks

This section firstly defines a subgraph hidden tree as complementary with a hidden tree, then describes how to find the user hidden tree.

5.1 Hidden tree

Although the hidden ring can protect the mobile user's location privacy, not all users can find the minimum ring covering their position.

For example, Fig. 4 shows the minimum discovery process for $user_2$. Because $user_2$ where the edge is $node_8$-$node_9$, the starting point of the search is specified as $node_9$ with a target point at $node_8$. Starting from the $node_9$ search algorithm, the search is expected to reach vertex $node_8$. Unfortunately, as $node_8$ is not found, $user_2$ is not covered in the position in the mobile network ring.

We found no subgraph smallest ring (for example, Fig. 4 subgraph) through observation; in fact, only free trees were found. The following were defining free trees which can protect the mobile user's location privacy.

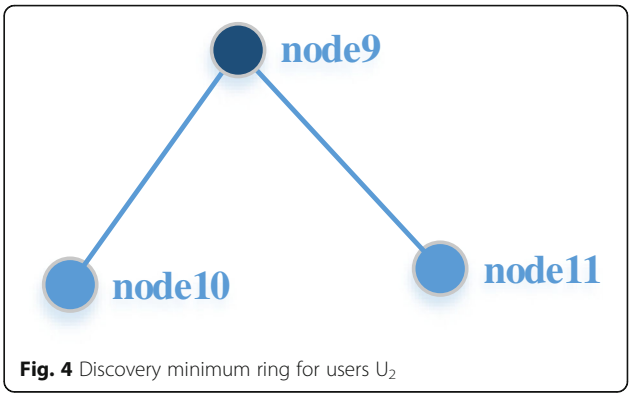

Fig. 4 Discovery minimum ring for users U_2

5.1.1 Definition 3: edge of the tree

An edge which is not covered by an undirected graph.

5.1.2 Definition 4: boundary of the tree

Free tree constructed only by edges in an undirected graph.

For example, a boundary tree is shown in Fig. 4. Because the edge n9n10, n9n11 is a tree.

5.1.3 Definition 5: relative maximum boundary tree

A boundary tree of an undirected graph, if adds an edge, is not a border tree.

For example, in Fig. 1, a boundary tree, which consists of $node_9node_{10}$, $node_9node_{11}$, $node_9node_8$, and $node_8$-$node_{12}$, is a relative maximum boundary tree.

For each relative maximum boundary edge of the tree, the tree is only a relative maximum boundary. Regardless of from which side the attacker is performing a search for the relative maximum boundary tree algorithm, he or she will receive a relative maximum boundary in the same tree, so that the attacker is unable to know each section of the mobile network and the number of mobile users. So, in the case of the attacker is not able to know the number of mobile users on each section of the mobile network, he will get the conclusion: the possibility of users in each edge is equal.

5.1.4 Definition 6: hidden tree

Relative maximum boundary trees, the number of sections and the number of mobile objects it contains that meet the user's location privacy, and the tree have at least two sections of the presence of the mobile user.

According to the hidden tree definition, to seek to cover one's position-concealed tree for the user, one should first find the cover of his position-relative maximum boundary tree, then the relative maximum boundary tree to determine whether it meets the latent tree condition. If satisfied, then we maximize the phase boundary tree, as the user's latent tree. However, if unsatisfied, then a relative maximum boundary tree

combination, namely by constructing hidden forests, must meet the user location privacy of mobile users and distribution in sections of the requirements.

5.2 Search the relative maximum boundary tree

The process of looking for the relative maximum boundary tree actually occurs in the process of gradually searching by the side of the tree. This is because the user's edge is a tree. To save the user's edge information and access the two vertices of the edge, they are successively inserted into the queue. For every vertex of the queue, one must first determine whether the vertex between adjacent vertices and the edges of the access is a tree. If it is a tree, then access the adjacent vertices and the adjacent vertices into the queue (that will continue down this path and then save the search) by the side of the tree information; if not, perform any operation on the right adjacent vertex (which is the path search so far). Repeat the above steps until the queue becomes an empty stop. Algorithm 2 gives details for the relative maximum boundary tree for users.

Algorithm 2. Looking for the relative maximum boundary tree.

Input: undirected graph UG; User; access vertices Queue; save a tree edge Vector

Output: the relative maximum boundary edges of the tree

1. According to the $user_{id}$ to get user's edge $node_inode_j$;
2. To obtain relevant information $user_{info}$ of edge $node_inode_j$;
3. To save ($Node_i$, $Node_j$, $user_{info}$) in Vector;
4. No to all vertices of UG are set to not be accessed;
5. Access vertex $node_inode_j$;
6. Insert $node_inode_j$ into the Queue;
7. While Queue is not empty
8. Move head element out of the queue, and assignment to user;
9. For each adjacent vertices
10. If vertices not being accessed
11. Access the vertices;
12. Analyzing the edge whether is the edge of the tree;
13. If the edge is a tree edge
14. Inset it into the queue;
15. Obtain relevant information;
16. Save those information into the vector;
17. Endif
18. Endif
19. Endfor
20. Endwhile

In Fig. 5, we take the search for the relative maximum boundary tree for $user_2$ as an example to illustrate the process. Because $user_2$'s edge is $node_9node_8$, the edge $node_9node_8$ information has been saved. In addition, the vertices of $node_9$ and $node_8$ have been accessed and they inserted in the queue. Then the $node_9$ has been moved out of the queue, with the first search to start from $node_9$. As shown in Fig. 5a, $node_9$ is not accessible. Its adjacent vertices are $node_{10}$, $node_{11}$, and $node_9node_{10}$, and $node_9node_{11}$ function as the tree. Furthermore, after $node_{10}$, $node_{11}$ has been set to visit, they will be inserted into the queue. The edge of $node_9node_{10}$, $node_9node_{11}$ will be saved and mapped with thick lines to indicate the edge preservation. Then the $node_8$ is out of the queue, as the edges of $node_8node_{13}$ and $node_8node_7$ being not the edge of the tree, so do not do any action for vertex $node_7$, $node_{13}$. $node_8node_{12}$ is a tree, after access $node_{12}$, which will be inserted into the queue and saves the edge information of $node_8node_{12}$. Given that the adjacent vertex $node_{10}$, $node_{11}$ and $node_{12}$ have been unvisited, they must terminate after they are taken out of the queue algorithm. Finally, one will find that the $user_2$-relative maximum boundary tree is composed of $node_9node_{10}$, $node_9node_{11}$, $node_9node_8$, edge graph of $node_8node_{12}$. The dotted lines in Fig. 5b show that $user_2$ is the relative maximum boundary tree found in the simple model of the mobile network.

5.3 Constructing hidden forest

In order to reduce the cost of location server query processing, the required number of mobile users and sections contained within the structure hidden in the forest

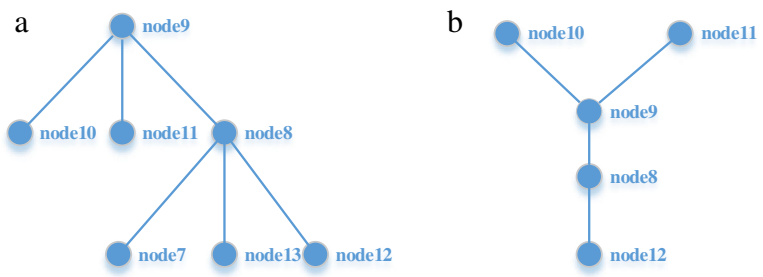

Fig. 5 Looking for the relative maximum boundary tree for U_2. **a** Looking for RMBT for U_2. **b** RMBT in the model of simple mobile network

must be the closest to the location privacy number of the user. So how can this be achieved? This paper's preservation section numbers were 1, 3, and 5, with low query processing costs, relative maximum boundary tree information, and each section of the number of relative maximum boundary tree, according to the information contained in the number of trees from the smallest to the largest number of mobile users in sequential order. If a small number of mobile users had constructed the hidden forest, then calculate the difference_k value of the number of mobile users and from the road number 1 relative maximum boundary tree information in a select number of mobile users closest to difference_k the relative maximum boundary tree. If it is due to a small number of road to go construction of hidden forest, then calculate the difference of difference_l out of the number of segments. Next, according to the difference_l, calculate the required number of sections of the number of relative maximum boundary tree according to the number of sequence selected for each relative maximum boundary tree. If due to the small number of sections and mobile users to construct hidden forest, then in addition to calculating the required number of sections of the relative maximum boundary tree based on difference, select the number of mobile users which is closest to difference_k.

6 Location privacy protection under the complex mobile networks

These two sections mainly introduce how to protect mobile user's location privacy through the method of undirected graph structure and tree ring hidden in the simple mobile network model. Then this section will introduce the problem surrounding location privacy in the complex mobile network model. The complete location privacy protection algorithm is provided at the end of this section.

The real life mobile network is a very common method. In easing city traffic congestion, reducing the intersection point of conflict and improving the running speed of the vehicle play a very big role. At present, many one-way traffic systems exist in cities such as New York, London, and Singapore.

For mobile networks consisting of a single line, a directed graph can be abstracted. For example, Fig. 6 shows a complex model of the mobile network. In this model, there are four single lines: $\text{node}_{17}\text{node}_{13}$, node_{13}-node_2, $\text{node}_3\text{node}_{14}$, and $\text{node}_{14}\text{node}_{18}$. In the complex mobile network model, the study found that the subgraph structure hidden ring and concealed tree can still provide users with location privacy protection.

6.1 Constructing the directed hidden ring

In the directed graph, vertices are connected by the arc, so that the phase diagram of the ring maintains direction (clockwise or counterclockwise), without hindering any protection. For a ring, the attacker, whether using the executive loop algorithm which arc to find the ring, will obtain the same results. This ring is a ring, so if a ring can meet the user's location privacy, and it has at least two arcs that have mobile users, then the ring can protect the user's location privacy. Such a ring is called to conceal the ring. Wherein selecting the best method to hide the ring with the best non-selective methods of occult ring to figure the same, and the other two steps and the undirected slightly different figure, this describes the smallest, found to have a ring and extends the minimum directed ring. For example, Fig. 7a, b shows that in the case of different starting points for the user to find the two minimal directional ring, that is, the ring <node_{14},

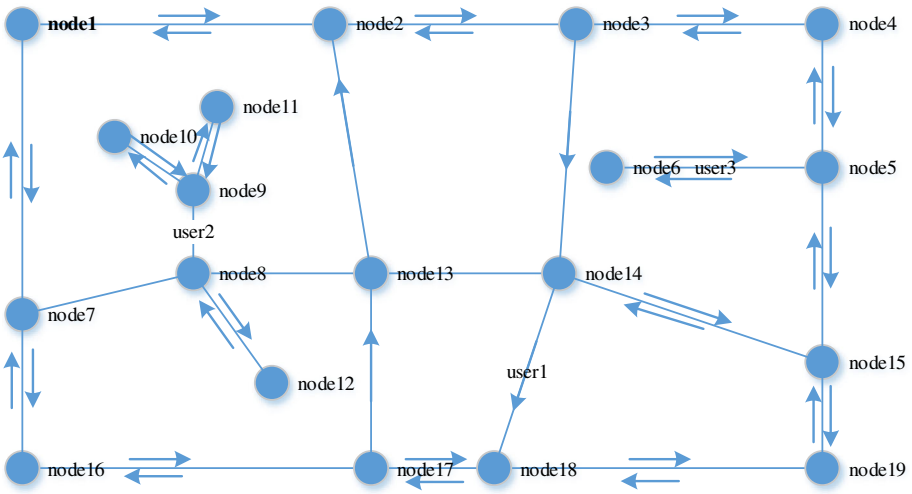

Fig. 6 A complex model of mobile network

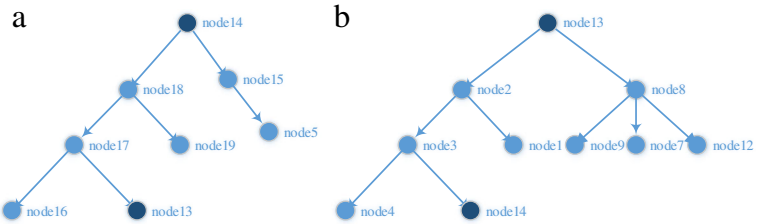

Fig. 7 Different starting points for $User_4$ found minimum directional ring. **a** <$node_{14}$, $node_{13}$>. **b** <$node_{13}$, $node_{14}$>

$node_{18}$, $node_{17}$, $node_{13}$, $node_{14}$> and <$node_{13}$, $node_2$, $node_3$, $node_{14}$, $node_{13}$>.

For the extension of the minimum ring in a directed graph, the degree of a vertex has a different direction. The selection of the starting point and the target point of the expansion ring is different with that of the undirected graph. The minimum to the vertex ring and the degrees were reduced by 1. Next, save and penetrate more than 0 of the remaining vertices, then select the starting point of the search and target point from the two kinds of vertices.

For example, in Fig. 6, assuming the coverage of $user_1$, minimum directed ring is <$node_{18}$, $node_{17}$, $node_{13}$, $node_{14}$, $node_{18}$>, after each vertex ring, and the degrees were reduced by 1, from $node_{17}$, $node_{13}$, $node_{18}$, vertex $node_{14}$, and the degrees are greater than 0. If you choose <$node_{13}$ $node_{14}$> as the starting point of the search and target points, it will be extended to the ring <$node_{18}$, $node_{17}$, $node_{13}$, $node_2$, $node_3$, $node_{14}$, $node_{18}$>; <$node_{17}$ $node_{13}$ > if, then, will be extended to the ring <$node_{18}$, $node_{17}$, $node_{16}$, $node_7$, $node_8$ $node_{13}$, $node_{14}$, $node_{18}$>.

6.2 Hidden tree in the directed graph

In the directed graph, we cannot find the smallest ring for the user, but the users are generally located within the double line. Because a single line in the mobile network layout meets the specific complementary theory—namely in a single line to design an opposite direction of the single line—they should be as close as possible. Given the single complementary theoretical guarantee of users starting from a single line, he was able to return to the other through the line and single line. Therefore, if the user is located within a single line, he will certainly be able to find his position to cover the ring. As the user is only in the double line when he could not find the minimum ring, then this kind of double line can function as a tree. To protect location privacy in the user tree on the edge, we can construct hidden tree or hidden forest for users.

For example, in Fig. 6, $user_2$, due to the discovery in "$node_8$, $node_9$" as the starting point and the target point not having been found in the ring, and "$node_9$ $node_8$" as the starting point and the target point has also failed to find a minimum, to determine the $node_8node_9$ tree is difficult. How can $user_2$ find the relative maximum boundary tree? As shown in Fig. 8, first, visit the vertices of $node_9$, $node_8$ and insert them in the queue. Then search starting from the vertex $node_9$. Adjacent vertex $node_{10}$ first reveals that $node_9$ is not accessible, because $node_9node_{10}$ does not have any arc ring cover. Next, judge whether $node_{10}node_9$ would not be any arc ring cover. If it is, then $node_9node_{10}$ is a tree, and you can access the vertex $node_{10}$. Insert it into the queue and save the information of $node_9node_{10}$ tree. In the same way, judging from $node_9node_{11}$, $node_8node_{12}$ will also be a tree, so for the user $user_2$ to find the relative maximum boundary tree is the tree by $node_9node_{10}$, $node_9node_{11}$, $node_9node_8$, $node_8node_{12}$ graph.

If the number of mobile users, for users to find the relative maximum boundary tree, contains a section number less than the user location privacy and (or) does not meet the distribution of mobile users in the sections of the requirements, it is the same for the user to construct hidden forest. The construction method of undirected graph hidden forest is basically the same.

6.3 Protection method for hidden ring and forest

When a request message receives the anonymous location of a user, for the user to construct the first attempt to conceal ring, if the ring has been found, and then choose the optimal execution hidden ring, the minimum ring expansion algorithm is necessary. If the ring is not

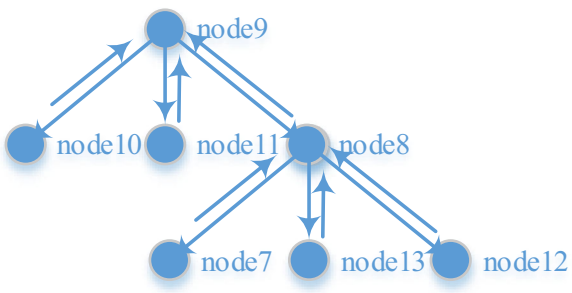

Fig. 8 Looking for a relative maximum boundary tree for a user under complex mobile network

found, then the position of the anonymous system for the user structure will be hidden or hidden in forest trees. Algorithm 3 describes the details.

Algorithm 3. Hidden Ring and Hidden Forest - HRHF.
Input: undirected graph UG; $user_{id}$;
Output: Hidden section set

1. Find the minimum ring for $user_{id}$ (algorithm 1);
2. If find the ring
3. Choose the best hiding ring;
4. if choose the optimal hidden ring
5. Returns this optimal ring as the user hidden position;
6. Else
7. If there can be expansion ring
8. Extended minimum;
9. Choose the best hiding ring;
10. Endif
11. Endif
12. Else
13. Looking for the relative maximum boundary tree for $user_{id}$ (algorithm 2);
14. To determine whether or not the relative maximum boundary tree is hidden tree;
15. If is a hidden tree
16. Return this hidden tree as the user hidden position;
17. Else
18. Construct hidden forest for users;
19. Endif
20. Endif

7 The experimental results and analysis

This algorithm is implemented using the C++ programming language, and the programming environment is Microsoft Visual C++. The hardware environment is 3.0 GHz Intel dual core CPU, 8 GB memory. The operating system is Microsoft Windows 10.

7.1 Experimental data sets and parameter setting

The experimental data is set by the mobile network data of California San Joaquin County in the USA. The mobile network data includes 17,585 vertices and 239,906 edges. In order to demonstrate that the mobile network contains a single line, the experiment set up 5458 special edges, and the single line with a single complementary theory. The use of Singhal and Shukla's [35] mobile network object generator is based on 10,000 generation mobile objects. In addition, 13,738 points of interest are generated in the mobile network, including shops and gas stations. At the same time, the experiment set up 990 mobile users of the nearest neighbor query request message.

The user's query request message includes four parameters: Location, K, $Location_{max}$, and K_{mmp}. The K, Location, and $Location_{max}$ are used on behalf of the user's location privacy, while K_{mmp} functions on behalf of the user to query the nearest neighbor points of interest. All query requests assume these four parameters are subject to normal distribution. Table 1 provides the average value and variance of the four default parameters. In the experiment, one parameter takes different averages, while the other three parameters were collected and their default values remain unchanged.

7.2 Algorithm evaluation

Experiments pertained to testing average information entropy, anonymous success rates, the average execution time of anonymity, and the relative anonymity of the average execution time of the query results, and the average size of candidate results in six aspects of the proposed algorithm was measured.

(1) The average information entropy. The attacker will come through the calculation of the user probability of $probability_j$ in each section of the concealed position ($j = 1, 2,\ldots, L'$), providing users with strong protection, so the information entropy can measure the probability distribution of Wang et al.[36], the calculation formula is as shown in formula (2):

$$\begin{aligned} H = & -\text{probability}_1 \log 10 \text{probability}_1 \\ & -\text{probability}_2 \log 10 \text{probability}_2 - \ldots \\ & -\text{probability}_{l'} \log 10 \text{probability}_{l'} \end{aligned} \quad (2)$$

If the information entropy is greater, the attacker's need guesses that the average user's exact location is greater, further increasing the user protection strength.

(2) The anonymous success rate refers to the percentage of successful message number sent by the algorithm and message number sent by all mobile users [37–39]. This can reflect the location privacy protection algorithm query response ability request of the user; the higher the value, the better algorithm.

For unsuccessful anonymous messages, this paper will use the false position method [40]—if the

Table 1 The parameters in the request message and the default values

Parameter	Average value	Variance
K	4	1
Location	4	1
$Location_{max}$	18	1
K_{mmp}	4	1

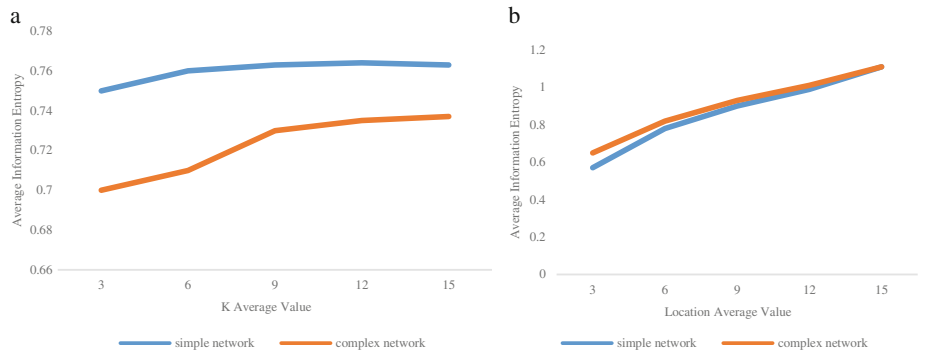

Fig. 9 Average information entropy

mobile network randomly generated other k-1 false position, then the user's real position and the false position are sent to the location server. The attacker cannot identify which position is the true position of the user, so the user's location information will be protected.

(3) The average time of anonymous execution refers to the position of average anonymous system of user's exact location for anonymous time.
This is used to measure a location privacy protection algorithm efficiency; the smaller the value, the higher the efficiency of the algorithm.

(4) The relative degree of anonymity, refers to the mobile object contains an anonymous position in the number of j (the number of sections' n') and the number of mobile users in the j object location privacy (section number n). It can be expressed as a formula (3).

$$\mathrm{RDA_j} = \mathrm{j}\,'/\mathrm{j},\ \mathrm{RDA_l} = \mathrm{n}'/\mathrm{n} \tag{3}$$

When n' and $\mathrm{Location_{max}}$ are unchanged, $\mathrm{RDA_j}$ improves with any increases. This is because the number of fixed sections on moving objects with greater strength will protect users more effectively. When j', $\mathrm{Location_{max}}$ are constant, the closer $\mathrm{RDA_n}$ to 1, the result is better, because too many sections will lead to higher cost of query processing and the service quality will decline.

(5) The average query execution time uses the average location server to query an anonymous location time. It is used to measure the position of the server query execution cost and query time spent. If the

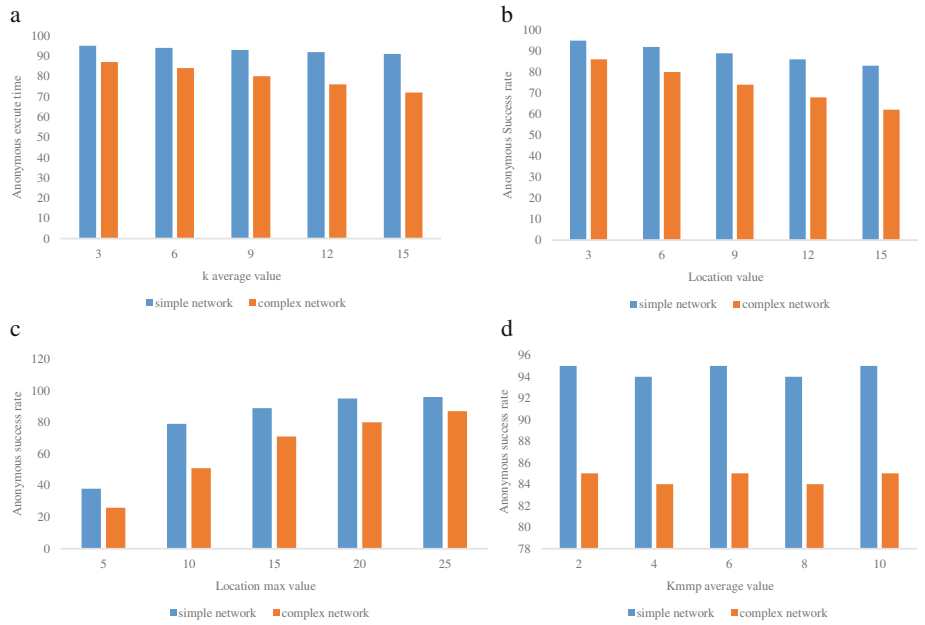

Fig. 10 Anonymous success rate

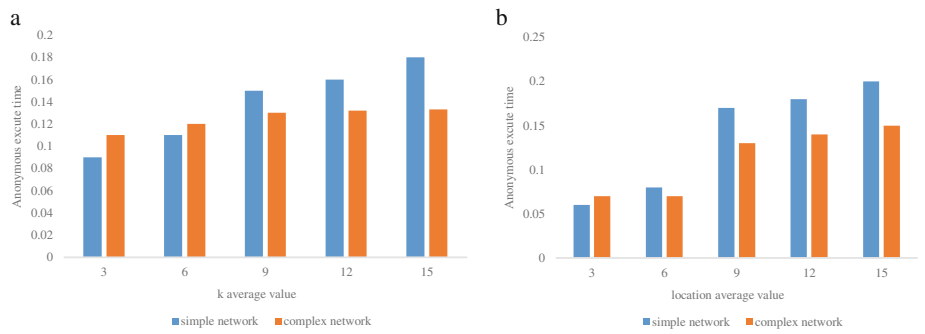

Fig. 11 The average anonymous execution time

server query execution cost is lower, the performance of algorithm will be improved. The location server simulation experiment, the hidden subgraph for a K_{mm} query, tests the performance of the proposed algorithm.

(6) The average size of the candidate refers to the location server for an anonymous location query. The average candidate results returned to the location server size. It is used to measure the cost of communication between the server and the position of the anonymous system. The average number of candidate results is fewer if communication cost is lower, and the performance of the algorithm is improved.

7.3 Experiment results and analysis

(1) The average information entropy. Figure 9a, b shows that when the parameters *K* and l are taking different average values, this paper provides the strength of privacy protection algorithm for mobile users.

From Fig. 9 we can see that regardless of the complexity of the mobile network, the average information entropy is greater than 0. 5. When the average information entropy of a complex mobile network is higher than a simple mobile network, the algorithm for privacy protection strength provided to users is greater in simple mobile networks than in complex mobile networks. In addition, from Fig. 9a, b the contrast can also be seen that the more hidden position of section number is, the more protection strength of customers receives.

(2) Anonymous success rate. Figure 10 shows the change of anonymous success rate in each parameter under different settings. From this figure, we can see that four simple anonymous successes in the mobile network rate are higher than in the complex mobile network. This is because after adding a single line, some roads are restrained in the direction of traffic, resulting in the reduction of the number of mobile networks. The original ring can be extended. However, after adding a single line it cannot be extended, resulting in more anonymous failure situations.

In Fig. 10a, b, with the increase of *K* and Location, the simple mobile network anonymous success rate dropped slightly, and the complex mobile network anonymous success rate decreased significantly. When the average Location value was equal to 15, the anonymous success rate was less than 70 %. This shows that the algorithm in the complex network of mobile location privacy is too high (*K* and Location average value is greater than or equal to 13) and the protective effect is unsatisfactory. In Fig. 10c, with the increase of $Location_{max}$, the anonymous success rate also increased. When the average $Location_{max}$ value was equal to 5, the anonymous success rate

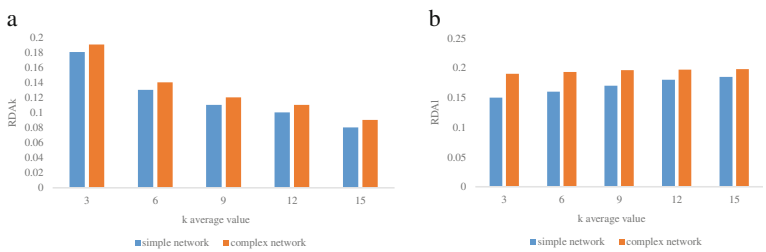

Fig. 12 RDA_k, RDA_l with respect to different parameter *K* settings

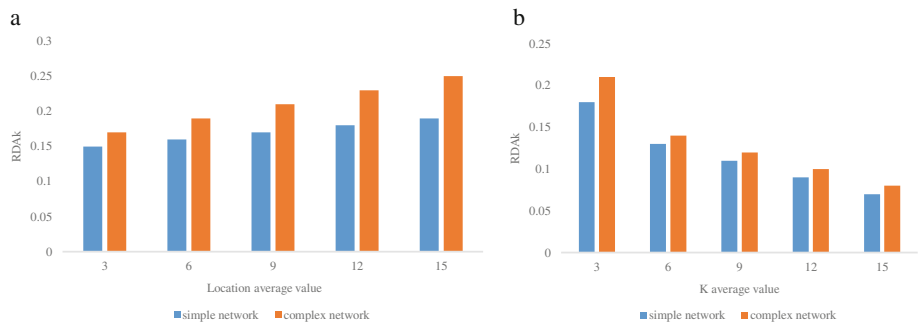

Fig. 13 RDA_k and RDA_l with respect to different parameter *K* settings

was very low. This may be because the users could find the hidden location. The road number is greater than 5 in many cases, resulting in the hidden location for Location' > $Location_{max}$ causing frequent anonymous failures. The default $Location_{max}$ value is set too small. From Fig. 10d can be seen when the parameters were obtained from the default privacy, anonymous success simple in the mobile network rate close to 96 %, and the anonymous complex in the mobile network success rate close to 86 %.

(3) The average execution time of anonymous. To find the relative maximum boundary tree algorithm, because in each search to judge one side is the side of the tree, so the time complexity than looking for hidden ring high time complexity. In order to reduce the cost of the server query processing, this paper takes too much time in choosing optimal hidden ring and hidden in the process of forest. You can see from Fig. 11 that with the increase of the value of the parameters, the execution time spent in anonymous location anonymity has increased, especially in the simple mobile network. This is mainly because when the *K* and L average values are greater than or equal to 9, the success of simple anonymity in the mobile network is much higher than the rate of success of complex anonymity, so the average time spent anonymous is relatively greater.

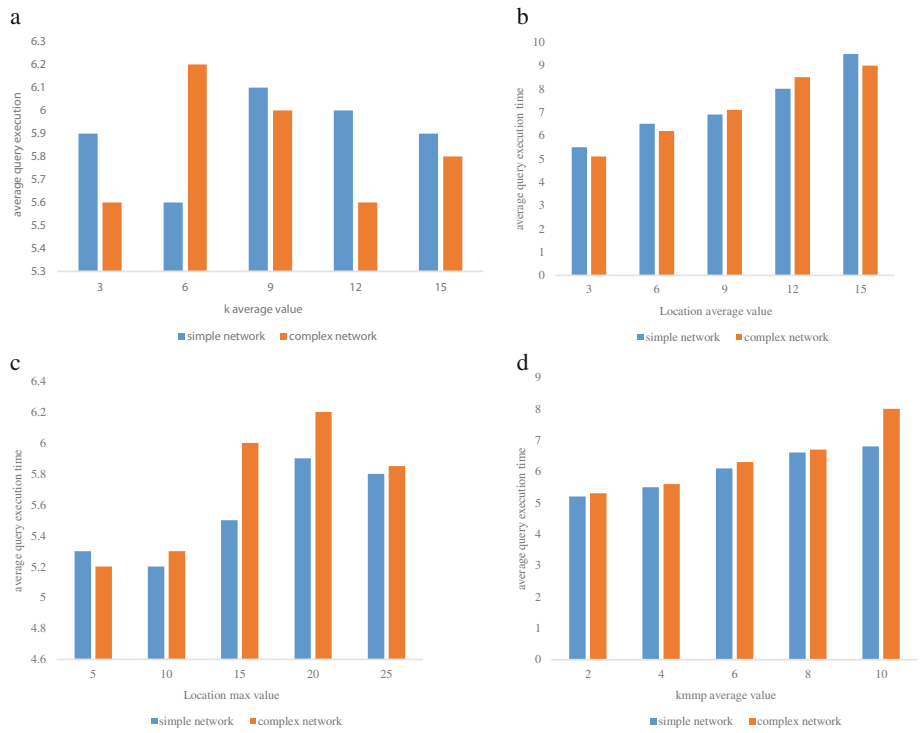

Fig. 14 The average query execution time

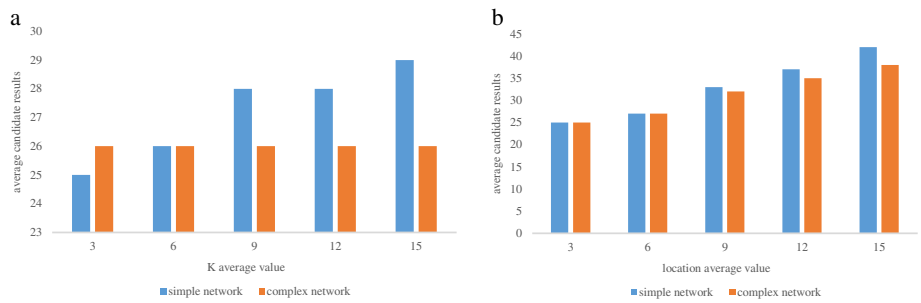

Fig. 15 The average candidate results 1

(4) The relative degree of anonymity. Figures 12 and 13 show the variation of K and Location relative anonymity degrees, respectively, in the case of different settings.
In Fig. 12, with the increase of K, RDA_k and RDA_l experience rapidly declines and slightly increases, respectively. This shows that the mobile user's number does not increase the number of too many sections, and thus will not lead to higher cost of query processing. As can be seen from Fig. 13, with a significant increase of L, RDA_k gradually increased while RDA_l declined sharply. This contains the number of hidden location sections, the increasing number of mobile users, and the greater user protection strength.

(5) The average query execution time. Because the k_{MM} query is the most common location service, the k_{MM} query processes on the hidden subgraph. As can be seen from Fig. 14, only when l and K_{mmp} increases, the average query execution time is gradually increasing, indicating hidden position of road section number, the query cost more time, and with the increase in the number of users query nearest neighbor points of interest, query the time needed to be increased.

(6) The average size of the candidate. Figures 15 and 16 show that with the increase of parameters, the query returns an increase in the number of candidate results. In Fig. 15a, the candidate complex mobile network number with the increase of K did not change, but in Fig. 15b, the number of candidates with the increase of location also increased gradually. In the complex mobile network, the cost of road communication can impact how much the communication can influence the number of large moving objects.

8 Conclusions

Previous studies on location privacy pay little attention to the location of the mobile network environment. We have found two forms of a hidden subgraph used to protect the privacy of a user's location—hidden ring and hidden tree—through observing simple and complex mobile network structural features. We have proposed a new method for ensuring privacy protection of location—-Hidden Ring and Hidden Forest (HRHF)—based on these two hidden subgraph structures. Not only that HRHF is effective for simple mobile networks but it can also solve the mobile network when it contains a single line in the position of privacy concerns. In the test results of the experiment based on real and simulated data sets, the HRHF method shows its effectiveness in terms of location privacy and efficiency in the provision of quality services.

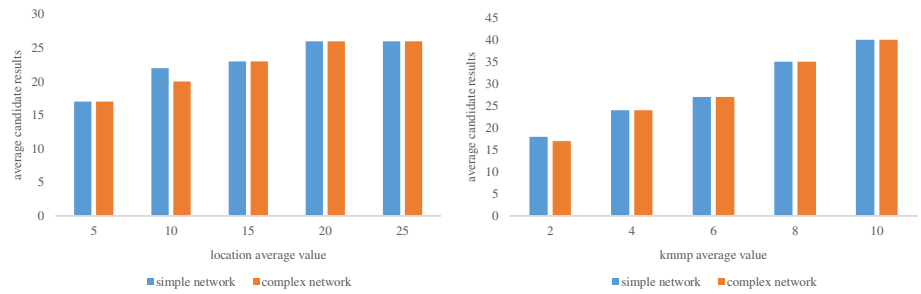

Fig. 16 The average candidate results 2

Acknowledgements
This research is supported in part by Zhejiang Provincial Natural Science Foundation of China (No. LY16F020012) and Ningbo Key Laboratory of Intelligent Home Appliances (No. 2016A22008).

Competing interests
The authors declare that they have no competing interests.

Received: 2 April 2016 Accepted: 26 August 2016
Published online: 05 September 2016

References

1. Altman, S.H., et al., Location-based advertising message serving for mobile communication devices. 2012, Google Patents.
2. Xu, Z., et al., Crowdsourcing based social media data analysis of urban emergency events. Multimedia Tools and Applications, 2015: p. 1–18.
3. Xu, Z., et al., Crowdsourcing based description of urban emergency events using social media big data. 2016
4. Z Xu et al., Participatory sensing-based semantic and spatial analysis of urban emergency events using mobile social media. EURASIP J Wirel Commun Netw. **2016**(1), 1–9 (2016)
5. Brush, A.J.B., et al., Mobile search based on predicted location. 2015, Google Patents.
6. Xu, Z., et al., Building knowledge base of urban emergency events based on crowdsourcing of social media. Concurrency & Computation Practice & Experience, 2016
7. Y-A de Montjoye et al., Unique in the crowd: the privacy bounds of human mobility. Sci Rep **3**, 1376 (2013)
8. HT Dinh et al., A survey of mobile cloud computing: architecture, applications, and approaches. Wirel. Commun. Mob. Comput. **13**(18), 1587–1611 (2013)
9. W Enck et al., TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. ACM Trans. Comput. Syst. **32**(2), 5 (2014)
10. Havlark, A., V. Burton, and J. Ahrens, Wireless telecommunications location based services scheme selection. 2014, Google Patents.
11. Hu, H., et al. Authenticating location-based services without compromising location privacy. in Proceedings of the 2012 ACM SIGMOD International Conference on Management of Data. 2012. ACM.
12. Joseph, B.L.I., B. Patel, and S. Sivalingham, Location-aware instant messaging. 2014, Google Patents.
13. AN Khan et al., Towards secure mobile cloud computing: a survey. Futur. Gener. Comput. Syst. **29**(5), 1278–1299 (2013)
14. Leontiadis, I., et al. Don't kill my ads!: balancing privacy in an ad-supported mobile application market. in Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications. 2012. ACM.
15. K Li, TC Du, Building a targeted mobile advertising system for location-based services. Decis.Support. Syst **54**(1), 1–8 (2012)
16. Li, M., et al. All your location are belong to us: breaking mobile social networks for automated user location tracking. in Proceedings of the 15th ACM international symposium on Mobile ad hoc networking and computing. 2014. ACM.
17. Li, X.-Y. and T. Jung. Search me if you can: privacy-preserving location query service. in INFOCOM, 2013 Proceedings IEEE. 2013. IEEE.
18. F Liu et al., Gearing resource-poor mobile devices with powerful clouds: architectures, challenges, and applications. IEEE Wirel. Commun. **20**(3), 14–22 (2013)
19. Liu, X., et al. Traffic-aware multiple mix zone placement for protecting location privacy. in INFOCOM, 2012 Proceedings IEEE. 2012. IEEE.
20. R Lu et al., A dynamic privacy-preserving key management scheme for location-based services in VANETs. IEEE Trans. Intell. Transp. Syst. **13**(1), 127–139 (2012)
21. CY Ma et al., Privacy vulnerability of published anonymous mobility traces. IEEE/ACM Trans. Networking **21**(3), 720–733 (2013)
22. Namiot, D. and M. Sneps-Sneppe, Geofence and network proximity, in Internet of Things, Smart Spaces, and Next Generation Networking. 2013, Springer. p. 117–127.
23. EC-H Ngai, I Rodhe, On providing location privacy for mobile sinks in wireless sensor networks. Wirel. Netw **19**(1), 115–130 (2013)
24. J Novak et al., Application of mobile phone location data in mapping of commuting patterns and functional regionalization: a pilot study of Estonia. J Maps **9**(1), 10–15 (2013)
25. X Pan, J Xu, X Meng, Protecting location privacy against location-dependent attacks in mobile services. IEEE Trans J Maps **24**(8), 1506–1519 (2012)
26. KP Puttaswamy et al., Preserving location privacy in geosocial applications. IEEE Trans. Mob. Comput. **13**(1), 159–173 (2014)
27. MR Rahimi et al., Mobile cloud computing: a survey, state of art and future directions. Mob Netw Appl **19**(2), 133–143 (2014)
28. Resch, B., People as sensors and collective sensing-contextual observations complementing geo-sensor network measurements, in Progress in Location-Based Services. 2013, Springer. p. 391–406.
29. H Shen, L Zhao, ALERT: an anonymous location-based efficient routing protocol in MANETs. IEEE Trans. Mob. Comput. **12**(6), 1079–1093 (2013)
30. KG Shin et al., Privacy protection for users of location-based services. IEEE Wirel. Commun. **19**(1), 30–39 (2012)
31. Shokri, R., et al. Protecting location privacy: optimal strategy against localization attacks. in Proceedings of the 2012 ACM conference on Computer and communications security. 2012. ACM.
32. T Zhou, Examining location-based services usage from the perspectives of unified theory of acceptance and use of technology and privacy risk. J Electron. Commer. Res. **13**(2), 135 (2012)
33. T Zhou, An empirical examination of user adoption of location-based services. Electron. Commer. Res. **13**(1), 25–39 (2013)
34. Z Zhu, G Cao, Toward privacy preserving and collusion resistance in a location proof updating system. IEEE Transactions on Mobile Computing **12**(1), 51–64 (2013)
35. M Singhal, A Shukla, Implementation of location based services in Android using GPS and Web services. IJCSI Int J Comput Sci Issues **9**(1), 237–242 (2012)
36. Wang, Y., et al. L2P2: Location-aware location privacy protection for location-based services. in INFOCOM, 2012 Proceedings IEEE. 2012. IEEE.
37. Wei, W., F. Xu, and Q. Li. Mobishare: flexible privacy-preserving location sharing in mobile online social networks. in INFOCOM, 2012 Proceedings IEEE. 2012. IEEE.
38. H Xu et al., Research note-effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. Inf. Syst. Res. **23**(4), 1342–1363 (2012)
39. L Zhao, Y Lu, S Gupta, Disclosure intention of location-related information in location-based social network services. Int. J. Electron. Commer. **16**(4), 53–90 (2012)
40. M Wernke et al., A classification of location privacy attacks and approaches. Pers. Ubiquit. Comput. **18**(1), 163–175 (2014)