Location Privacy Preservation in Location-Based Services over Road Networks

Shu Chen[1,*] and Hoong Shen[1,2]

[1]School of Information Science and Technology, Sun Yat-Sen University, China
[2]School of Computer Science, University of Adelaide, Australia

[*]Email: chenshu_chen [AT] 163.com

Abstract—**With the development of Internet of Things (IoT) and smart devices, location-based services are becoming increasingly popular. People are able to make spatial range queries as well as share location information with friends anywhere at any time. However, this is also accompanied by risks since location information is considered to be one kind of quasi-identifiers and hence sensitive. In this paper, we consider the following scenario: a user sends different location-based requests continuously on a map, and is gradually exposed to location attacks. Numerous algorithms have been proposed to solve this problem. But most of them are targeted for locations in the Euclidean space, and hence not applicable for the more practical scenarios of road networks. Moreover, though several studies have addressed the popularity of locations in road networks, none has considered the sensitivity of locations, let alone the correlation between popularity and sensitivity at the same location. In this paper, we explore the impacts of sensitivity and popularity on a cloaking region, and develop a cloaking algorithm called *RCliqueCloak* to reduce the risk of location leakage in road networks. Experimental results show that our algorithms behave better than other cloaking algorithms in incorporating map information.**

Keywords-cloaking algorithm; location-based services; privacy preservation; road network.

I. INTRODUCTION

With the development of wireless networks and mobile computing technology, location-based services (LBS) have become more and more popular. The players of Social Network Sites (SNS) would like to share their daily lives as well as locations with friends by Facebook, twitter, even email and SMS. Businessmen would love to pay great attention to research their potential customers group, such as the study of which people often went through their own stores. Drivers would like to use navigation software to help find their destinations. However, such applications will also cause location privacy problems. Actually, the knowledge of "where you stay" exposes the privacy of "what you are doing". Further, the adversary can speculate your profession, health condition, religion and education background etc. from your daily location information. Two main techniques for location privacy protection in LBS are the *k*-anonymity model (eg. [1, 2]) and the location cloaking model. The *k*-anonymity model, which has been widely used in data privacy preservation, is to make the target user's information indistinguishable from that of at least $k-1$ other users, so that the probability of location leakage or user identity is therefore $1/k$. It can be used to prevent snapshot location attacks, especially the location linking attacks. While the location cloaking model is also based on a similar notion which is to blur an exact position into a cloaked region so that the adversary cannot find out the accurate location of the target user, thereby unable to infer the information of the target user. A variety of cloaking algorithms have been developed for different privacy metrics. Nowadays, the *k*-anonymity model and cloaking algorithm are often used together for location privacy preservation.

Unlike the snapshot location attacks, the continuous attacks are more secret but common. In the continuous cases, even though each location update can be considered as an independent event, a series of cloaking regions in chronological order may be linked to recur the user's movement trajectory. More specifically, if an adversary (e.g. the Service Provider) is able to collect the historical cloaking regions of a user as well as the user mobility pattern (e.g. speed limit), the location privacy of the user might be compromised [3]. As is shown in Fig. 1, a user sends a query q_i at time t_i in cloaking region R_i , and then sends another query q_{i+1} at time t_{i+1} in cloaking region R_{i+1}. If the adversary somehow knows that the user's maximum possible moving speed in this area is V_{max}, then it can easily get the user's maximum activity area as R^{α} . As a consequence, the adversary can infer that the user is certainly in the intersection area of R^{α} and R_{i+1} (the shaded area in Fig. 1). Obviously, this would degrade the quality of location cloaking and may make it fail to meet the expected privacy requirement. In the worst case, if the intersection area is just a location point, the exact user location will be disclosed. Besides, the above example is based on the Euclidean space without any constraints, and it will be more complicated in road networks. In this paper, we consider the following scenario: the user sends different location-based requests

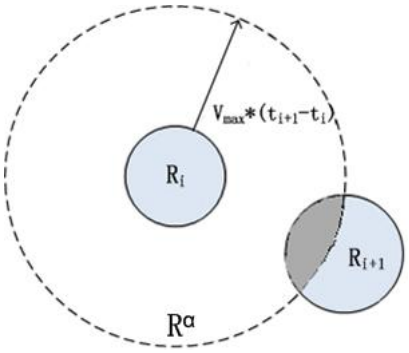


Figure 1. Continuous Location Attacks Example

continuously while walking or driving in a road network. The problem is not only to prevent against continuous location attacks, but to make sure that an adversary cannot determine that a user was near somewhere sensitive. Most existing methods for preventing continuous location attacks are targeted in the Euclidean space and hence not applicable for the road networks. So we propose a cloaking algorithm called *RCliqueCloak* to prevent against continuous location attacks in a road network. Our new algorithm *RCliqueCloak* also considers the time of the user's stay in the cloaking region, which is often overlooked by other methods in continuous location queries. The main contributions of this paper are:

- We differentiate between the popularity and sensitivity for the same location and explore their impacts on the cloaking region in road networks.
- We propose a new cloaking algorithm for road networks that takes the correlation between the popularity and sensitivity of a location into consideration by extending the *ICliqueCloak* algorithm [4] for the Euclidean plane.
- We conduct a set of simulation experiments to evaluate the performance of our algorithm *RCliqueCloak* on a wide range of location data generated from a well-known road network simulator and show that *RCliqueCloak* is more effective than *ICliqueCloak*.

The remainder of this paper is organized as follows. We overview the related work on two main location attacks (snapshot and continuous location attacks) and the road-network model in Section 2. In Section 3, we present the system architecture and give the problem formulation. Our new cloaking algorithm is presented in Section 4. Section 5 shows the experimental results followed by a conclusion in Section 6.

II. RELATED WODK

The research about our topic mainly concerns location privacy preservation in LBS as well as modeling of road networks. In this section, we first introduce two main location attack models as well as the basic techniques. Then we expound several main techniques for location privacy in road networks in detail.

A. Location Attacks

1) Snapshot Location Attacks: The research on location privacy protection starts with snapshot location attacks. In this scenario, the user prossibly proposes querys like that "lead us to the nearest hospital from here", or "show me all the restaurants within one mile of here". However, the adversary still might perform location attacks by combining several snapshot queries, which is called query sampling attacks. Chow et al. [5] introduced *k*-sharing regions to deal with such attacks, that is, a cloaking region should be shared by at least *k* users, instead of only covering at least *k* users of all. Besides, Gedik et al. [6] extended the *k*-anonymity model to personalization. It transformed the problem of finding the cloaking set into Maximum Clique Problem (MCP) that satisfies certain conditions in the constraint graph, which is known as Clique-Cloak theorem. Mokbel et al. [7] also proposed a Quad-tree-like algorithm to generate cloaking region. Moreover, Ghinita et al. [8] employed the Hilbert curve to approximate the spatial proximity between queries. Bamba et al. [9] applied both *k*-anonymity and *l*-diversity algorithms to generating the cloaking region.

2) Continuous Location Attacks: Continuous Location Attacks (illustrated in Fig. 1) are the interests of present research as well as the focus of our work. Cheng et al. [10] presented two approaches, namely patching and delaying, to prevent the user's location from being deduced. The first one, patching, is to enlarge the current cloaking region so that the user's maximum activity area can cover its last cloaking region as much as possible. Obviously, the larger the overlapped area is, the safer it will be. The second one, delaying, is to extend the response time so that the maximum activity area grows large enough to meet the safety requirements. Then Xu and Cai [11] proposed a novel technique with polynomial time complexity to deal with this problem. Xu et al. [12] designed two cloaking algotithms, namely MaxAccu_Cloak and MinComm_Cloak, based on different performance objectives. Pan et al. [13] proposed a new incremental clique-based cloaking algorithm, called ICliqueCloak, to defend against such attacks. Furthermore, a set of cloaking regions in chronological order may be linked to recur users' movement trajectory by an adversary. Kido et al. [14] used a set of location dummies that move in human-like trajectories to prevent trajectory leakage. Niu et al. [15] selected dummy locations carefully instead of randomly in consideration of side information like query probability which may be acquired by an adversary. You et al. [16] introduced two schemes for generating a false trail about users' movements in a long run to protect trajectories of users. Palanisamy et al. [17] presented an approach called MobiMix to break the continuity of location exposure by using mix-zones, where users can change or interchange their pseudonyms secretly so that no applications can trace their movements.

B. Road Networks

Different from the Euclidean space, a road network is based on the real streetscape with lots of constraints, for instance, one has to walk or drive along the road and the places around him

are all open to the public. Usually a real map of streetscape is abstracted as a graph.

In general, a road network is modeled as a weighted graph $G = (V, E, w(e))$ in which V is the set of nodes and E is the set of edges. Weight $w(e)$ possibly presents the travelling time from one node to the other. However, it is often not enough. Wang and Liu [18] introduced the concept of segment, with which a road network is able to be partitioned into a series of segments uniquely. And the anonymous region for certain user, if it is a rectangle, can be replaced by a set of segments. In addition, Yigitoglu et al. [19] proposed an improved model for road networks called Annotated city network. It divided the places into different types and tagged them with values between 0 and 1 as their popularities.

Existing algorithms only consider popularity or mix up popularity and sensitivity. In this paper, we point out that the two parameters are different. One place (e.g. restaurants) may have high popularity but low sensitivity, and vice versa (e.g. private club). We take both of them into consideration to hide the sensitive information more effectively.

III. PROBLEM FORMULATION

In this section, we first describe the system architecture, and then formulate the problem including our road-network model as well as location protection model.

A. System Architecture

The system architecture in our paper is shown in Fig 2. We employ a trusted proxy, called *Anonymizer*, to be placed between mobile users and the Service Provider. Each time the user sends a location-based query, the agent anonymizes the user's accurate location into a cloaking region before forwarding the query to the LBS provider in accordance with its own map data and the user's privacy requirements. Then the Service Provider returns a candidate results based on the blurry information sent by the proxy. The *Anonymizer* refines the result according to the exact user information and sends it to the user.

B. Road Networks

In this paper, we model the road network as a connected and undirected weighted graph $G = (V, E, w(e), pt, < sen, pop >)$ where E refers to the set of edges and V to the set of network nodes including street intersections as well as places. Also there is a nonnegative weight $w(e)$ of every edge e indicating the estimated traveling time from one node to the other. Thus we can calculate the total weight in the cloaking region as the whole traveling time. In addition, considering the complexity of a real streetscape we may do some abstraction instead of a precise depiction.

Definition 1. Sensitivity is the quantification of the privacy level of a user's location, indicating that how reluctant the user is to reveal this location to others.

For instance, the patient may be afraid of being found in the hospital, while the doctor may not mind that. Thus the sensitivity degree of hospital for a patient may be higher than that for a doctor.

Definition 2. Popularity is the quantification of the crowd density of a location in a certain time slice. It is common that each place has its own active time. Thus the popularities of a same location in different time may differ a lot.

For instance, restaurants are popular at mealtimes, while not at other times. Nightclubs are full of people at night but quiet in the daytime.

We divide places into several types using *pt* and each type has its own sensitivity degree *sen* and popularity degree *pop* which are all within the range between 0 and 1. These two parameters of the same place type *pt* are different from each other. For example, a park has high popularity but low sensitivity, while a private club has low popularity but high sensitivity. As the result, it is significant to differentiate between them and take both of them into account.

An example of the abstraction of a road network is shown in Fig. 3. Each node is labeled by a tuple $< sen, pop >$, which represents a user-specified sensitivity degree and a system-defined popularity degree of a place respectively. It explains two meanings as follow:

- Users don't need to worry about the popularity, which is based on the average value of data gathered in the system from users' queries.
- Users specify their own sensitive places in the range from 0 to 1, as each of them has different privacy requirements. Once the sensitivity is fixed, it will not change in the query process. For example, Alice specified the sensitivity of Pub A is 0.5 and then put forward two queries at time t_1 and t_2, the sensitivity of Pub A in the corresponding cloaking region CR_1

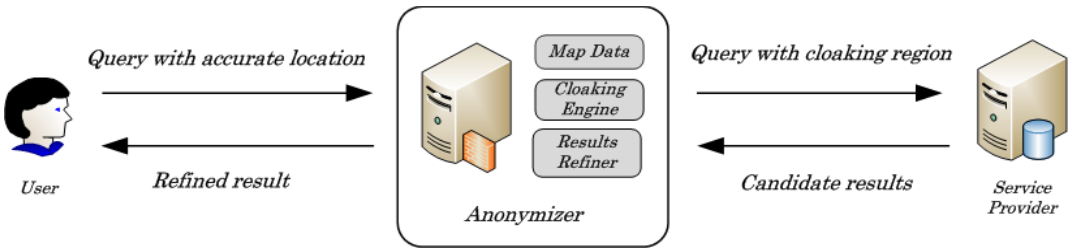


Figure 2. System Architecture

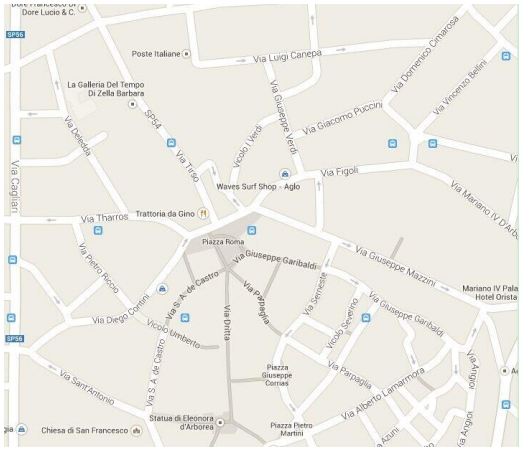
and CR_2 keeps to be 0.5 unless Alice change it again manually.

In particular, *sen* becomes continuous rather than discrete (0 or 1), and the correlation between *sen* and *pop* is taken into account. We believe that these measures will make a better cloaking region in the road-network environment.

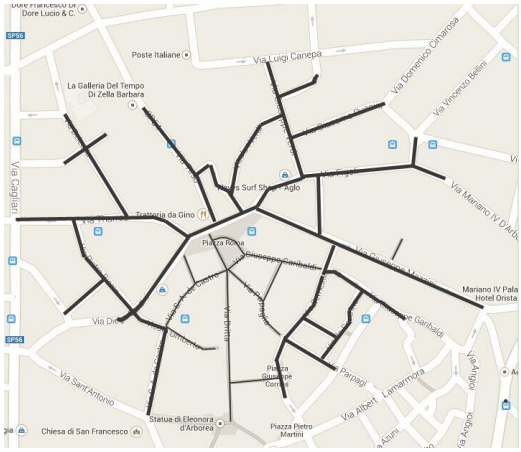
C. Location Protection Model

Definition 3. (knowledge of the adversary) Anyone who owns the following information can be a potential adversary:

- The road-network model including the real street map and the corresponding graph *G*.
- A series of historical cloaking regions: $\{(t_1,CR_1),(t_2,CR_2),\cdots\cdots,(t_{i-1},CR_{i-1})\}$.
- The maximum possible movement speed V_{max} of user.



(a) A real street map



(b) Graph-based representation of street

Figure 3. Road-network Model Example

According to our system architecture described above, the Service Provider could be a potential adversary because it knows not only all the historical cloaking regions as well as the current road-network model of the user, but also the maximum possible moving speed of user.

Definition 4. (Cloaking Region) Denote a rounded rectangle region of size more than A_{min} containing the exact spot of the user as the cloaking region CR, and A_{min} specified by the user indicates the minimum area of the cloaking region. The following conditions must be satisfied:

- A_{min} cannot be too small, or it might be an exact location. With that the user's location information might be revealed even it satisfies the preset privacy requirements.
- CR cannot lead to continuous location attacks described above, so that the adversary cannot infer user's historical and current locations from a series of CR sequences.

According to the road network, we point out that:

Given the cloaking region $CR_{A,t_{i-1}}$ and CR_{A,t_i}, as well as the road-network model, the adversary calculates the maximum time throughout the region as $\bar{t}$. If

$\bar{t} \square\ t_i - t_{i-1}$: the user probably stays at one of the positions in the cloaking region $CR_{A,t_{i-1}}$ for a while, the adversary may infer the position of the user by integrating the time of the user spend on the road and the *pop* of the position in the graph of current CR and it will be worse especially when the position has high sensitivity degree *sen* .

Therefore, in each CR we should make sure that

$$\frac{pop(pt)}{\sum pop(.)} \times sen(pt) \le \delta . \qquad (1)$$

where δ is a parameter specified by the user. Obviously, the bigger δ is, the safer it will be. In general, a place which is popular as well as sensitive, like hospital, is treated as the key protection object, and we need to adjust the cloaking region to low down its popularity ratio $\frac{pop(pt)}{\sum pop(.)}$ since $sen(pt)$ is relatively fixed. Here we recommend translation and rotation of cloaking region as a solution, so that it contains not only the user's exact position but also satisfies the (1) .

Problem formulation. In summary, the problem of our study can be formulated as follows: Assume that a user sends different location-based requests continuously on a map and the adversary, by definition, exists. The problem is to generate a cloaking region not only against continuous location attacks, but also to make those sensitive places around the user in the road network difficult to be identified.

IV. ALGORITHMS

According to the above analysis, we extend the *ICliqueCloak* algorithm from the Euclidean plane into a road network represented by an undirected weighted graph $G = (V, E, w(e), pt, < sen, pop >)$. We need to protect the sensitivity while the user might stay in the region for a while. Algorithm 1 first generates the initial cloaking region $Initial\_CR_{t_i}$ by finding the maximum clique which satisfies certain conditions, and makes sure that the $Initial\_CR_{t_i}$ is in the maximum movement boundary (MMB) of its last cloaking region $CR_{t_{i-1}}$ so that it will not weaken the security degree of current cloaking region. Then it calls Algorithm 2 *ProtectSensitivityCR* to prevent adversary from inferring where the user used to stay from time t_{i-1} to t_i, if the lag time t_i-t_{i-1} is far greater than the average movement time *t* from cloaking region $CR_{t_{i-1}}$ to current location based on the map information. Because it is common that the user has spent some time at one of the places in the cloaking region with great probability if it takes too long to go to the next location. Afterwards Algorithm 2 returns its result, called $Sensitive\_CR_{t_i}$. Finally the main algorithm adjusts $Sensitive\_CR_{t_i}$ to make it also in its maximum arrival boundary (MAB) in order that the previous and following cloaking region is not exposed to location leakages.

Algorithm 1 *RCliqueCloak*

Input:

1. A set of historical cloaking regions $\{(t_1, CR_1), (t_2, CR_2), \cdots\cdots, (t_{i-1}, CR_{i-1})\}$;
2. An abstract streetscape map $G = (V, E, w(e), pt, < sen, pop >)$;
3. The user-specified minimum size of cloaking region A_{min}.

Output: current cloaking region CR_{t_i}.

1. $Initial\_CR_{t_i}$ = GenerateInitialCR;
2. Calculate the maximum spending time $\bar{t}$ in $Initial\_CR_{t_i}$;
3. if $\bar{t} \square\ t_i - t_{i-1}$ then
4. $Sensitive\_CR_{t_i}$ = *ProtectSensitivityCR*($Initial\_CR_{t_i}$);
5. CR_{t_i} =ExtendCR($Sensitive\_CR_{t_i}$, A_{min});
6. else
7. CR_{t_i} =ExtendCR($Initial\_CR_{t_i}$, A_{min});
8. end if
9. return CR_{t_i};

If the user's stay time in the cloaking region far outweights the possible maximum spending time in the region, we believe that an eligible adversary with map information can infer what place the user is likely to stay during that time. So Algorithm 2 is called to adjust the initial cloaking region and make it not expose sensitive location information as much as possible by translation and rotation. When th does not satisfy the privacy requirements, we translate the initial cloaking region $Initial\_CR_{t_i}$ and then rotate it appropriately. We do this repeatedly in the maximum cycle times, so that the new cloaking region not only contains the user's exact position but also satisfies (1). If it cannot find any cloaking region satisfying the privacy requirements, then return the current optimal solution.

Algorithm 2 *ProtectSensitivityCR*

Input:

1. $Initial\_CR_{t_i}$
2. Cloaking region map $G = (V, E, w(e), pt, < sen, pop >)$
3. User-specified threshold δ
4. maxLoop

Output: $Sensitive\_CR_{t_i}$

1. for each $v \in V$ and v in $Initial\_CR_{t_i}$ do
2. for $i = 1$ to maxLoop do
3. $th \leftarrow \frac{pop(v.pt)}{\sum pop(.)} \times sen(v.pt)$;
4. Push($current\_th$, $current\_CR$);
5. if $th \le \delta$ then
6. break;
7. end if
8. Generate two values respectively for the direction and distance of translation randomly;
9. ▷ *translating*
10. Generate two values respectively for the direction and angle of rotation randomly;
11. ▷ *rotating*
12. i++;
13. Mark the CR with smallest th as current $Sensitive\_CR_{t_i}$;
14. return $Sensitive\_CR_{t_i}$;

V. EXPERIMENTAL EVALUATION

In this section, we evaluate the performance of our proposed algorithm *RCliqueCloak* from two aspects of time and space. The following two metrics are taken into consideration. 1) Average protection level. It refers to the probability of not leaking the sensitive location information from the cloaking region. 2) Average success rate. Find a proper value of privacy index δ by analyzing the average success rate.

A. Experiment Setup

All the algorithms are implemented in Java and performed on a Windows 7 PC with an Intel Core i7-3770 CPU, a 3.40 GHz processor and a 4.00 GB main memory. We pick a real road map of Oristano from OpenStreetMap, a city in the central-western part of the island of Sardinia, Italy. OpenStreetMap is a free-use map of the world edited by users themselves. It contains the following four core elements: nodes, ways, relations, and tags. In our experiments, road data contains 4026 nodes, 6108 edges and 28 tags. Tags, shown as key-value pairs, are not free-standing, but always attached to an object (node, way or relation). That is sufficient for our study, as we can tag place types with popularity and sensitivity. Other default values of each parameter are listed as in Table I.

B. Experiment Results

We compare the average protection level with another algorithm, *ICliqueCloak* [21] which is the original scheme of our algorithm *RCliqueCloak*. *ICliqueCloak* is based on the Euclidean plane without consideration of various place types in the cloaking region, let alone the sensitivity and popularity of them. As is shown in Fig. 4, *RCliqueCloak* behaves better than *ICliqueCloak* on the protection level when the minimum number of anonymous users K are the same on road-network environment.

Fig. 5 provides the performance results when the user-defined privacy index δ is from 0.2 to 0.8. The average protection level of our algorithm *RCliqueCloak* increases slowly and reaches the top at about 0.55, then goes down. However, the average success rate of *RCliqueCloak* remains at more than 90 percent of the high level when δ is less than 0.5 and then declines rapidly. Since it is hard to find an appropriate cloaking region when δ becomes large, so the average success rate falls down afterwards. Meanwhile, the average protection level is influenced by the average success rate, also getting down later. Because when the sub-algorithm *ProtectSensitivityCR* cannot find a cloaking region in full with privacy requirements including a big δ, it will return an optimal solution that it could find. Undoubtfully it would impair the protection level somehow. Consequently, it is very important to select an appropriate value of δ, and around 0.5 seems best with the current setting. We believe that with a proper setting, the performance of our algorithm *RCliqueCloak* will behave well in consideration of the map information.

TABLE I. PARAMETER SETTINGS

Parameter	Default Values
Place type	Restaurants(0.3, 0.35), Nightclub(0.7, 0.05), Residence(0.5, 0.25), School(0.25, 0.6), Hospital(0.7, 0.4), Market(0.2, 0.5), Park(0.25, 0.29)
δ	[0.2, 0.8]
K-anonymity	at least 2
A_{min}	0.005% to 0.01% of the space
MaxLoop	[5, 10]
Speed profile	medium

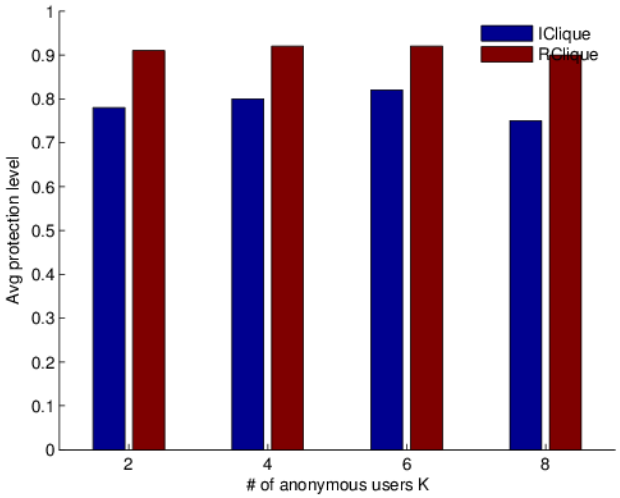


Figure 4. Protection Level between *RCliqueCloak* and *ICliqueCloak*

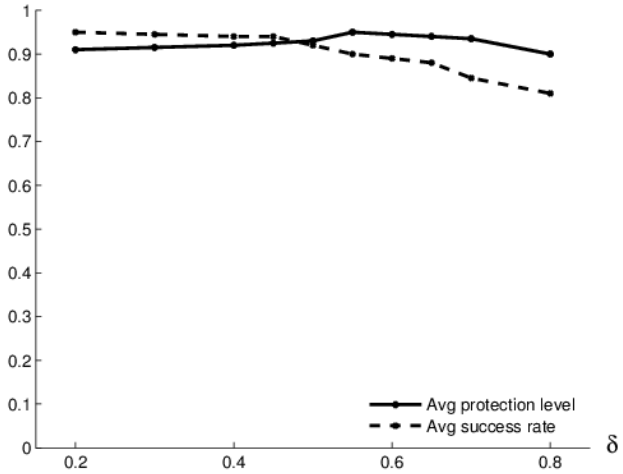


Figure 5. Impact of Privacy Index δ

VI. CONCLUSION

In this paper, we have proposed an algorithm called *RCliqueCloak*, as an extension of the *ICliqueCloak* algorithm, that protects location privacy against continuous location attacks over a road network. We consider the characteristics of various types of places and the correlation between sensitivity and popularity for the same place. Meanwhile, we introduce translation and rotation to adjust cloaking region in order to satisfy the privacy requirements. A series of experiments have been conducted to evaluate our algorithm *RCliqueCloak* under certain system settings. The experimental results show that *RCliqueCloak* achieves a higher protection level than *ICliqueCloak*, and behaves well in incorporating map information.

ACKNOWLEDGMENT

This work is supported by Research Initiative Grant of Sun Yat-Sen University under Project 985, National Science Foundation of China under its General Projects funding #61170232, Australian Research Council Discovery Project DP150104871. The corresponding author is Hong Shen.

REFERENCES

[1] Mikhail J Atallah, and Keith B Frikken, "Privacy-preserving location-dependent query processing," Pervasive Services, 2004. ICPS 2004. Proceedings. The IEEE/ACS International Conference on, pages 9-17. IEEE, 2004.

[2] Bhuvan Bamba, Ling Liu, Peter Pesti, and Ting Wang, "Supporting anonymous location queries in mobile environments with privacygrid," Proceedings of the 17th international conference on World Wide Web, pages 237-246. ACM, 2008.

[3] Reynold Cheng, Yu Zhang, Elisa Bertino, and Sunil Prabhakar, "Preserving user location privacy in mobile data management infrastructures" Privacy Enhancing Technologies, pages 393-412. Springer, 2006.

[4] Chi-Yin Chow and Mohamed F Mokbel, "Enabling private continuous queries for revealed user locations" Advances in Spatial and Temporal Databases, pages 258-275. Springer, 2007.

[5] Bugra Gedik and Ling Liu, "Location privacy in mobile systems: A personalized anonymization model" Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on, pages 620-629. IEEE, 2005.

[6] Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, and Kian-Lee Tan, "Private queries in location based services: anonymizers are not necessary" Proceedings of the 2008 ACM SIGMOD international conference on Management of data, pages 121-132. ACM, 2008.

[7] Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos, "Prive: anonymous location-based queries in distributed mobile systems" Proceedings of the 16th international conference on World Wide Web, pages 371-380. ACM, 2007

[8] Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh, "An anonymous communication technique using dummies for location-based services" Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on, pages 88-97. IEEE, 2005.

[9] Mohamed F Mokel, Chi-Yin Chow, and Walid G Aref, "The new casper: query processing for location services without compromising privacy" Proceedings of the 32nd international conference on Very large data bases, pages 763-774. VLDB Endowment, 2006.

[10] Ben Niu, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li, "Achieving k-anonymity in privacy-aware location-based services" INFOCOM, 2014 Proceedings IEEE, pages 754-762. IEEE, 2014.

[11] Balaji Palanisamy and Ling Liu, "Mobimix: Protecting location privacy with mix-zones over road networks" Data Engineering (ICDE), 2011 IEEE 27th International Conference on, pages 494-505. IEEE, 2011.

[12] Xiao Pan, Jianliang Xu and Xiaofeng Meng, "Protecting location privacy against location-dependent attacks in mobile services" Knowledge and Data Engineering, IEEE Transactions on, 24(8): 1506-1519, 2012.

[13] Ting Wang and Ling Liu, "Privacy-aware mobile services over road networks" Proceedings of the VLDB Endowment, 2(1): 1042-1053, 2009.

[14] Jianliang Xu, Xueyan Tang, Haibo Hu, and Jing Du, "Privacy-conscious location-based queries in mobile environments" Parallel and Distributed Systems, IEEE Transactions on, 21(3): 313-326, 2010.

[15] Toby Xu and Ying Cai, "Location anonymity in continuous location-based services" Proceedings of the 15th annual ACM international symposium on Advances in geographic information systems, page 39. ACM, 2007.

[16] Emre Yigitoglu, Maria Luisa Damiani, Osman Abul, and Claudio Silvestri, "Privacy-preserving sharing of sensitive semantic locations under road-network constraints" Mobile Data Management (MDM), 2012 IEEE 13th International Conference on, pages 186-195. IEEE, 2012.

[17] Tun-Hao You, Wen-Chih Peng, and Wang-Chien Lee, "Protecting moving trajectories with dummies" Mobil Data Management, 2007 International Conference on, pages 278-282. IEEE, 2007.