PROS: A Peer-to-Peer System for Location Privacy Protection on Road Networks (Demo Paper)

Jie Bao
Dept. of Computer Science and Software Engineering
Auburn University
Auburn, AL 36849, USA
baojie@auburn.edu

Haiquan Chen
Dept. of Computer Science and Software Engineering
Auburn University
Auburn, AL 36849, USA
chenhai@auburn.edu

Wei-Shinn Ku
Dept. of Computer Science and Software Engineering
Auburn University
Auburn, AL 36849, USA
weishinn@auburn.edu

ABSTRACT

The k-anonymity technique is widely used to provide location privacy protection for accessing location-based services (LBS), i.e., the exact location of a query initiator is cloaked into a spatial region that contains at least k indistinguishable users. However, a centralized location anonymizer may pose serious privacy threats and could be the system bottleneck. Moreover, many cloaking methods are developed for the Euclidean space and fail to consider the features of road networks. In this demonstration, we present the technologies and implementations which protect location privacy by peer-to-peer based cloaking on road networks. We name the prototype system as *PROS*. With *PROS*, a mobile user forms a cloaked road segment set by collaborating with her peers when she needs to retrieve information from location-based service providers. Afterward, the cloaked road segment set is sent to the service provider for query processing and an inclusive query result set is returned to the query initiator after the query evaluation.

Categories and Subject Descriptors

H.2.8 [**Database Management**]: Database Application—*spatial databases and GIS*

General Terms

Algorithms and Experimentation

Keywords

Location-based services, location privacy and spatial cloaking

1. INTRODUCTION

Over the past few years location-based services (LBS) have become the major building blocks of numerous mobile applications. With LBS, users carrying mobile devices can acquire information related to their current locations by issuing queries to location-based service providers (LBSP). For retrieving the precise answers of these queries, users have to disclose their exact location information to LBSP. However, if any service provider is malicious, adversaries may easily access sensitive information about a particular user, for example, its current location and query sentences, which will lead to privacy leak. To remedy this, the k-anonymity model based cloaking solution [4] has been proposed to assure location privacy. However, with the centralized cloaking solution, the location anonymizer, which possesses the complete knowledge of mobile user locations may become the single point of failure in case it is compromised. Besides, many existing location privacy protection researches focus on the Euclidean space without taking road networks into account.

This demonstration presents *PROS* – a novel system which protects location privacy by peer-to-peer based cloaking on road networks. *PROS* consists of two main components, namely, the cloaking module and the searching module. With the cloaking module, a query initiator forms a cloaked road segment set by collaborating with its peers when it needs to launch a query to the LBSP. In addition, the searching module takes the derived cloaked road segment set as the input for query evaluation and an inclusive query result set is returned for the query initiator to filter out the exact answers.

GIS'09, November 4-6, 2009, Seattle, Washington, USA.

2. CLOAKING

2.1 Cloaked Road Segment Set

Prior research in [3] discovered that grid cell based cloaking solutions fail to consider the features of underlying road networks and the spatial-temporal moving behavior of mobile users. Therefore, the technique in [3] applies road segments as the unit for indexing and cloaking. Similar to [3], *PROS* employs road segment sets to represent the cloaked region to achieve advanced location privacy protection effect. Furthermore, *PROS* utilizes hash tables to facilitate the retrieval of adjacent road segments.

As far as the privacy profile is concerned, in traditional cloaking algorithms for the Euclidean space, a privacy profile is a pair of (k, A_{min}), where k is the number of indistinguishable users and A_{min} is the minimal area required for cloaked regions. However, because *PROS* is road network based, i.e., in *PROS*, a cloaked region is in fact a road segment set, we employ (k, L_{min}, N_{min}) as the privacy profile instead, where L_{min} and N_{min} are the minimal total road segment length and the minimal number of road segments required in a cloaked road segment set, respectively. A cloaked road segment set will be expanded iteratively until the privacy profile is satisfied.

2.2 Peer-to-Peer Cloaking

As mentioned in Section 1, with centralized cloaking, the location anonymizer may become a system bottleneck when the number

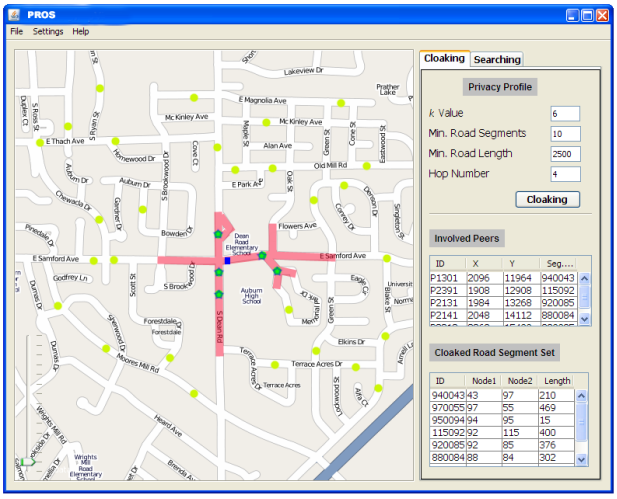

Figure 1: Cloaked road segment set.

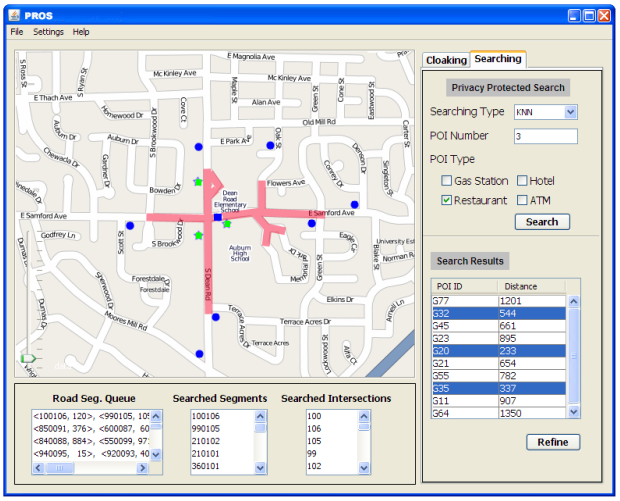

Figure 2: Inclusive and exact query result sets.

of mobile users increases or the locations of mobile users change very frequently. To avoid the bottleneck problem and a single point of failure, *PROS* forms a cloaked road segment set by single-hop or multi-hop peer searching [1], where mobile users communicate with each other to discover nearby peers. In other words, *PROS* blurs the exact location of a query initiator without any centralized location anonymizer.

With *PROS*, before launching a query, a query initiator q broadcasts a probe, which includes the hop count h specified by q to its neighboring peers and then q listens to the network to wait for the replies. When a peer receives a probe with h value greater than 1, it not only responds to the probe but also modifies the probe by decreasing h by 1 and then re-broadcasts the probe. On the contrary, when a peer receives a probe with the h value equal to 1, it only answers to the probe. Consequently, the probe will flood locally within hop count h in the wireless network. After collecting all the replies, the query initiator randomly chooses $k-1$ peers (therefore, the requestor will not always be in the center of the cloaking result) to form the cloaked road segment set. The cloaked road segment set should (1) include the $k-1$ discovered peers and (2) satisfy the requirements of L_{min} and N_{min}. If such a cloaked road segment set cannot be generated, the query initiator has to increase the initial hop count value.

3. QUERY PROCESSING

As the result of peer-to-peer cloaking, the cloaked road segment set is submitted with the LBS query to the location-based service provider for evaluation. In *PROS*, we adopt the privacy protected spatial network query algorithms, PSNN and PSRQ, as proposed in [2], for answering K nearest neighbor queries and range queries on road networks. Notice that since the cloaked regions discussed in [2] are based on grid cells rather than road segments, we extended both PSNN and PSRQ to retrieve inclusive query result sets according to the input cloaked road segment sets and the underlying road networks. Finally, the query initiator filters out the exact query results from the inclusive query result set returned by the LBSP.

4. DEMONSTRATION

4.1 Cloaked Road Segment Set

Figure 1 demonstrates a screen shot of the cloaking module GUI. A user firstly specifies its privacy profile (k, L_{min}, N_{min}) and the hop count. As the result of cloaking, the square, the pentagons and the circles on the map correspond to the query initiator, the discovered peers, and the uninvolved peers, respectively. In addition, the cloaked road segment set is highlighted on the map.

4.2 Inclusive and Exact Result Sets

The searching module GUI is illustrated in Figure 2. Users can specify query types (K nearest neighbor query, range query, etc.). Then, users select the POI types to be searched. Taking the cloaked road segment set as the input, the location-based service provider will return an inclusive query result set after the search. The GUI shows an example of a 3-nearest neighbor query. The pentagons and circles on the map represent the POIs in the inclusive result set answered by the service provider and in particular the pentagons are the exact results filtered out by the query initiator.

5. CONCLUSIONS

In this demonstration, we present *PROS*, a system which can protect location privacy by peer-to-peer based cloaking on road networks. In *PROS*, users communicate with each other to find collaborative peers to achieve k-anonymity and the cloaked region is represented as a road segment set to exploit features of road networks. Afterward, the cloaked road segment set is sent to the service provider, where the query evaluation is executed based on the cloaked road segment set and the underlying road networks. Finally, an inclusive query result set is returned to the query initiator to filter out the exact answers.

Acknowledgments

This research has been funded in part by the National Science Foundation grants CNS-0831502 (CT) and CNS-0855251 (CRI).

6. REFERENCES

[1] C.-Y. Chow, M. F. Mokbel, and X. Liu. A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services. In *GIS*, pages 171–178, 2006.

[2] W.-S. Ku, Y. Chen, and R. Zimmermann. Privacy Protected Spatial Query Processing for Advanced Location Based Services. In *Wireless Personal Communications*, 2008.

[3] P.-Y. Li, W.-C. Peng, T.-W. Wang, W.-S. Ku, J. Xu, and J. J.A.Hamilton. A Cloaking Algorithm based on Spatial Networks for Location Privacy. In *SUTC*, pages 90–97, 2008.

[4] M. F. Mokbel, C.-Y. Chow, and W. G. Aref. The New Casper: Query Processing for Location Services without Compromising Privacy. In *VLDB*, pages 763–774, 2006.