ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 165-170 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

Anonymous Processing of Query in Road Networks

Sravan KumarTappa
Research Scholar, Dept of CSE
SVITS–Mahabubnagar, A. P.
sravankumar.tappa@gmail.com

B.J. Sunil
Associate Professor ,
Dept of ECE
SVITS–Mahabubnagar, A. P.

C. Srinivas
Associate Professor, Dept of IT
SVITS–Mahabubnagar, A. P.

Abstract—The increasing availability of location-aware mobile deviceshas given rise to a flurry of location-based services (LBS). Due to thenature of spatial queries, an LBS needs the user position in order to processthe requests. On the other hand, revealing exact user locations to (potentially untrusted) LBS may pinpoint their identities and breach theirprivacy. To address this issue, spatial anonymity techniques obfuscateuser locations, forwarding to the LBS a sufficiently large region instead.Existing methods explicitly target processing in the Euclidean space,and do not apply when proximity to the users is defined according tonetwork distance (e.g., driving time through the roads of a city). In thispaper, we propose a framework for anonymous query processing in roadnetworks. We design location obfuscation techniques that (i) provideanonymous LBS access to the users, and (ii) allow efficient queryprocessing at the LBS side. Our techniques exploit existing networkdatabase infrastructure, requiring no specialized storage schemes orfunctionalities. We experimentally compare alternative designs in realroad networks and demonstrate the effectiveness of our techniques.

Keywords: Location-based services, Spatial queries, Road networks.

INTRODUCTION

The low cost and small size of positioning equipment (e.g., GPS receivers) have allowed their embedding into PDAs and mobile phones. The wide availability of these location-aware portable devices has given rise to a flourishing industry of location-based services (LBS). An LBS makes spatial data available to the users through one or more location servers (LS) that index and answer user queries on them. Examples of spatial queries could be "Where is the closest hospital to my current location?" or "Which pharmacies are open within a 1 km radius?". In order for the LS to be able to answer such questions, it needs to know the position of the querying user. There exist many algorithms for efficient spatial query processing, but the main challenge in the LBS industry is of a different nature. In particular, users are reluctant to use LBSs, since revealing their position may link to their identity. Even though a user may create a fake ID to access the service, her location alone may disclose her actual identity. Linking a position to an individual is possible by various means, such as publicly available information (e.g., city maps and telephone directories), physical observation, cell-phone signal triangulation, etc.

User privacy may be threatened because of the sensitive nature of accessed data; e.g., inquiring for pharmacies that offer medicines for diseases associated with a social stigma, or asking for nearby addiction recovery groups (Alcoholics/Narcotics Anonymous, etc). Another source of threats comes from less sensitive data (e.g., gas station locations, shops, restaurants, etc) that may reveal the user's interests and shopping needs, resulting ina flood of unsolicited advertisements through e-coupons and personal messages. To solve this problem the following general approach is taken. When a user wishes to pose a query, she sends her location to a trusted server, the anonymizer (AZ), through a secure connection (e.g., SSL). The latter obfuscates her location, replacing it with an anonymizing spatial region (ASR) that encloses. The ASR is then forwarded to the LS. Ignoring where exactly is, the LS retrieves (and reports to the AZ) a candidate set (CS) that is guaranteed to contain the query results for any possible user location inside the ASR. The AZ receives the CS and reports to the subset of candidates that corresponds to her original query. In order for the AZ to produce valid ASRs, the users send location updates whenever they move (through their secure connection).

The ASR construction at the AZ (i.e., the anonymization process) abides by the user's privacy requirements. Particularly, specified an anonymity degreeK by the ASR satisfies two properties:

(i)it contains and at least anotherK−1 users. (ii) even if the LS knew the exact locations of all users in the system, it would not be able to infer with aprobability higher than1/K who among those included in the ASR is the querying oneUsers are often interested in location-based queries such as r-range and kNN queries, in the context of a road network.

Given a distance threshold r and a user location u, the r-range query returns all objects within (network)

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 165-170 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

distance r from u. On the other hand, the kNN query retrieves the k objects that are closest to u. In the rest of the paper, the term distance refers to the network distance, and the r-range and kNN queries refer to their network versions (unless otherwise specified). Papadias et al. [10] developed efficient indexing and processing methods for the above queries. (ORT) organizes the locations of the data objects. Recently, considerable research interest has focused on preventing identity inference in location-based services. Studies in this area typically assume the model described in Section 1, proposing spatial cloaking (i.e., location obfuscation) techniques. In the following, we describe existing techniques for ASR computation (at the AZ) and query processing (at the LS). Processing is based on Theorem

1. A direct implementation of the theorem uses (network-based) search operations as offthe-shelf building blocks. Thus, the NAP query evaluation methodology is readily deployable on existing systems, and can be easily adapted to different network storage schemes, as we discuss in Section 5.3. As a case study, in this section we focus on the storage scheme and the network expansion framework in order to provide a concrete NAP prototype. we propose the network-based anonymization and processing (NAP) framework, the first system for Kanonymous query processing in road networks. NAP relies on a global user ordering and bucketization that satisfies reciprocity and guarantees K-anonymity. We identify the ordering characteristics that affect subsequent processing, and qualitatively compare alternatives.

Then, we propose query evaluation techniques that exploit these characteristics. In addition to user privacy, NAP achieves low computational and communication costs, and quick responses overall. It is readily deployable, requiring only basic network operations. In the traditional spatial anonymity model, the data owner (e.g., a location-based service) makes its data available using a location server. It may, however, be the case that the owner is outsourcing its database to a third-party (and, thus, untrusted) location server. A challenge here is how to encrypt the owner's data so that they are hidden from the location server, while it can still process anonymous queries. Another interesting question is how (anonymous) users could verify that the location server did not tamper with the original owner data

RELATED WORK

Query Types

This section describes query types classification in a Anonymous query processing in road networks . The general query types are divided into two classes:

- Traditional Queries
- Mobile Queries.

The traditional query type category contains common query types that exist in a wirednetwork database, whereas the mobile query contains queries that exist only in awireless environment.The traditional query is the typical database queries.

If we classify the traditional query based on the geographical presentation, this type of query can be divided into two classes: Location-Aware and Non-location.

In the mobile computing environment, the location of mobile users is dynamic and the query results often depend on dynamic location. Therefore, this situation creates another additional class, which is called Location-Dependent Queries.

Location Query

These types of queries have one parameter which is location. It implies that thequery result is related to or depends on, that parameter.Location Dependent Query is a type of query where the answers depend on the current location of the sequesters.

For example," select all restaurants within 500 metres from my location". The answer should give a list of restaurants within 500 metres from the current location of the requester .If the requester moves to a new location, the list of restaurants will be changed.A location is an important feld in this type of query and this feld can be implicitlyor explicitly mentioned in the query. These types of queries can be further categorized into two groups. The first groupis based on sources and objects, and the second one is based on query retrieval. The sources and objects are represented as users while sending the query and thesearched objects. Their states can be either static or moving. The second state isbased on the states of the query retrieval either one-time or continuous. A one-time query is a query that expects a query result in one-time. On the other hand, a continuous query, as the name implies, is a query that receives a query result which is based on the current location of the source at some moment in time. This query is sent only once and updated location information is sent to notify the server that the client

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 165-170 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

has moved to a different location. Both groups mentioned above can be further elaborated as follows.

(a) Data sources and objects states

This group focuses on states of location for either users or objects while a user query is being proceed. The states of location for both can be static or dynamicduring the query processing shows the division of group one. As we can see from the table, category one is further divided into four subgroups. The first subgroup is a static user probes for static objects. This subgroup does not involve a mobility factor foreither users or objects. Whenever the query is sent, the query result returned will always be the same.

Server Query Processing

This section presents a discussion of existing work on location-dependent query processing at the server side. A brief overview is presented first to provide an idea of how a location-dependent query is processed, followed by query processing at the server side, indexing structures used at the server side and query processing at the client side.

Outstanding Problems

A discussion of the problems and shortcomings of existing works is presented in this section. Earlier in this chapter we reviewed the literature that dealt with works on mobile query processing at the client and server sides. Our review reveals that there are still problems and issues that need to be addressed and resolved.

An examination of existing problems from previous researchers is carried out, which is described in the next three subsections. A discussion of anonymous query processing in road networks problems is presented, followed by indexing mechanism problems for processing multi-cell queries. The last problem to be discussed is a client caching replacement policy, which will be presented in the last subsection.

SYSTEM ANALYSIS

EXISTING SYSTEM

Existing method a current location-based services where users have to report their exact locations to the database server in order to obtain their desired services. For example, a mobile user asking about her nearest restaurant has to report her exact location. With untrusted service providers, reporting private location information may lead to several privacy threats. LS make spatial data available to the users through one or more location servers (LS) that index and answer user queries on them.

For examples of spatial queries could be “Where is the closest hospital to my current location?” or “Which pharmacies are open within a 1 km radius?” In order for the LS to be able to answer such questions, it needs to know the position of the querying user.

Existing an peer-to-peer (P2P) spatial cloaking algorithm [2] in which mobile and stationary users can entertain location-based services without revealing their exact location information. The main idea is that before requesting any location-based service, the mobile user will form a group from her peers via single-hop communication and/or multi-hop routing. Then the spatial cloaked area is computed as the region that covers the entire group of peers.

PROPOSED SYSTEM

In this thesis paper, we propose the network-based anonymization and processing (NAP) framework, the first system for K- anonymous query processing in road networks. NAP relies on a global user ordering and bucketization that satisfies reciprocity and guarantees K-anonymity. We identify the ordering characteristics that affect subsequent processing, and qualitatively compare alternatives.

In thesis, we propose query evaluation techniques that exploit these characteristics. In addition to user privacy, NAP achieves low computational and communication costs, and quick responses overall. It is readily deployable, requiring only basic network operations. We propose a framework for anonymous query processing in road networks.

We design location obfuscation techniques that

(i) provide anonymous LBS access to the users, (ii) allow efficient query processing at the LBS side. Our techniques exploit existing network database infrastructure, requiring no specialized storage schemes or functionalities.

We experimentally compare alternative designs in real road networks and demonstrate the effectiveness of our techniques.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 165-170 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

MODULE DESCRIPTION

. NETWORK MODULE

Server - Client computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

LBS SERVICES

In particular, users are reluctant to use LBSs, since revealing their position may link to their identity. Even though a user may create a fake ID to access the service, her location alone may disclose her actual identity. Linking a position to an individual is possible by various means,such as publicly available information city maps. When a user u wishes to pose a query, she sends her location to a trusted server, the anonymizer [1] [6] through a secure connection (SSL). The latter obfuscates her location, replacing it with an anonymizing spatial region (ASR) that encloses u. The ASR is then forwarded to the LS. Ignoring where exactly u is, the LS retrieves (and reports to the AZ) a candidate set (CS) that is guaranteed to contain the query results for any possible user location inside the ASR. The AZ receives the CS and reports to u the subset of candidates that corresponds to her original query.

SYSTEM MODEL

The ASR construction at the anonymization process abides by the user's privacy requirements. Particularly, specified an anonymity degree K by u, the ASR satisfies two properties: (i) it contains u and at least another K * 1 users, and (ii) even if the LS knew the exact locations of all users in the system.

- We propose an edge ordering anonymization approach for users in road networks, which guarantees K-anonymity under the strict reciprocity requirement (described later).
- We identify the crucial concept of border nodes, an important indicator of the CS size and of the query processing cost at the LS.
- We consider various edge orderings, and qualitatively assess their query performance [9] based on border nodes.
- We design efficient query processing mechanisms that exploit existing network database infrastructure, and guarantee CS inclusiveness and minimality. Furthermore, they apply to various network storage schemes.
- We devise batch execution techniques for anonymous queries that significantly reduce the overhead of the LS by computation sharing.

ANONYMOUS LOCATION-BASED QUERIES

Recently, considerable research interest has focused on preventing identity inference in location-based services. Studies in this area [7], [4] typically assume the model proposing spatial cloaking techniques. In the following, we describe existing techniques for ASR computation (at the AZ) and query processing (at the LS). At the end, we cover alternative location privacy approaches and discuss why they are inappropriate to our problem setting. This offers privacy protection in the sense that the actual user position u cannot be distinguished from others in the ASR, even when malicious LS is equipped/advanced enough to possess all user locations. This spatial K-anonymity model is most widely used in location privacy research/applications, even though alternative models are emerging.

ANONYMOUS QUERY PROCESSING

Processing is based on implementation of the theorem uses (network-based) search operations as off the shelf building blocks. Thus, the NAP query evaluation methodology is readily deployable on existing systems, and can be easily adapted to different network storage schemes. In this case, the queries are evaluated in a batch. We propose the network-based anonymization and processing (NAP) framework, the first system for K- anonymous query processing in road networks. NAP relies on a global user ordering and bucketization that satisfies reciprocity and guarantees K-anonymity. We identify the ordering characteristics that affect subsequent processing, and qualitatively compare alternatives. Then, we propose query evaluation techniques that exploit these characteristics. In addition to user privacy, NAP achieves low computational and communication costs, and quick responses overall. It is readily deployable, requiring only basic network operations.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.2 , No.1, Pages : 165-170 (2013)
Special Issue of ICACSE 2013 - Held on 7-8 January, 2013 in Lords Institute of Engineering and Technology, Hyderabad

EXPERIMENTAL EVALUATION

In this section, we evaluate the robustness and scalability of our proposed methods on a real road network. Our algorithms were implemented in C++ and experiments were executed on a Pentium D 2.8GHz PC. We measured the average of the following performance values over a query workload of 100queries: (i) anonymization time and refinement time at the anonymizer AZ, [1] (ii) I/O time and CPU time for query processingat the location server LS, and (iii) the communicationcost (in terms of transmitted points) for the anonymizing edgelist AEL and the candidate set CS. Note that each edge inAEL is counted as two points.

Experiment Setup

By default, our experiments use a subnetwork with50000 edges. Weights of the edges are set to their lengths.We generate jUj users and jOj objects. The locations of usersand objects follow either uniform distribution (by default) orGaussian distribution4. At the LS, the disk page is 4Kbytesand each index structure (edge R-tree, ORT, etc) is associatedwith a memory buffer with capacity set to 5% of its disksize.

Robustness Experiments

We illustrate the achieved anonymity andstudy the performance of our methods for different orderings, location privacy models, and user/object distributions,Anonymity strength. NAP is theoretically guaranteed tohonor reciprocity and provide K-anonymity. Empiricallydemonstrates this fact, i.e., that no user in the AEL ismore than 1=K likely to have issued the query. We generate1000 random queries with K = 40 and record the positionof the querying user within the AEL according to ordu (weinclude results only for DF as those for other orderings arealmost identical). Figure 9(a) plots the querying frequencyper user position in the AEL. The dashed line, labeled "safebound", corresponds to probability 1=K = 0:025. There aremore than K = 40 positions (up to 48) because the AEL maycontain over K users. Figure 9(b) provides another viewpoint,considering the median AEL position as slot 0. No frequency exceeds the safe bound, i.e., an adversary withknowledge of all user locations and of the anonymizationalgorithm cannot pinpoint the querying

CONCLUSION

In this paper, we propose the network-based anonymization and processing (NAP) framework, the first system for Kanonymous query processing in road networks. NAP relies on a global user ordering and bucketization that satisfies reciprocity and guarantees K-anonymity. We identify the ordering characteristics that affect subsequent processing, and qualitatively compare alternatives.

Then, we propose query evaluation techniques that exploit these characteristics. In addition to user privacy, NAP achieves low computational and communication costs, and quick responses overall. It is readily deployable, requiring only basic network operations. In the traditional spatial anonymity model, the data owner (e.g., a location-based service) makes its data available using a location server. It may, however, be the case that the owner is outsourcing its database to a third-party (and, thus, untrusted) location server. A challenge here is how to encrypt the owner's data so that they are hidden from the location server, while it can still process anonymous queries. Another interesting question is how (anonymous) users could verify that the location server did not tamper with the original owner data.

ACKNOWLEDGEMENT

The authors express their deep gratitude to the Principal and the Management members of SVITS for their encouragement and extensive support in preparing and publishing of this paper.

REFERENCES

[1] http://www.anonymizer.com

[2] C.-Y. Chow, M. F. Mokbel, and X. Liu.A peer-to-peer spatial cloaking algorithm for anonymous location-based service.In GIS, 2006.

[3] M. Duckham and L. Kulik.A Formal Model of Obfuscation andNegotiation for Location Privacy.In PERVASIVE, 2005.

[4] B. Gedik and L. Liu. Location Privacy in Mobile Systems: A PersonalizedAnonymization Model. In ICDCS, 2005.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L.Tan.Private Queries in Location Based

Services: Anonymizers are notNecessary. In SIGMOD, 2008.

16] G. Ghinita, P. Kalnis, and S. Skiadopoulos. PRIVE: AnonymousLocation-based Queries in Distributed Mobile Systems. In WWW, 2007.

[7] M. Gruteser and D. Grunwald. Anonymous Usage of Location-BasedServices Through Spatial and Temporal Cloaking. In MobiSys, 2003.

[8] E. G. Hoel and H. Samet. Efficient Processing of Spatial Queries inLine Segment Databases.In SSD, 1991.

[9] X. Huang, C. S. Jensen, and S. Saltenis. The Islands Approach to NearestNeighbor Querying in Spatial Networks. In SSTD, 2005.

[10] D. Papadias, P. Kalnis, N. Mamoulis, and Y. Tao. Query processing in Spatial Network Databases. In VLDB, 2003.