International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Preserving Privacy & Content using Open OAuth and TTP Server for Location based Services

Swapnil R. Jadhav†* and R. N. Phursule†

†Department of Computer Engineering, ICOER, Pune, India

Accepted 02 Jan 2016, Available online 06 Jan 2016, **Vol.6, No.1 (Feb 2016)**

Abstract

Today's technology is developing rapidly. Due to wireless communication technologies, whole world gets closer. The best way for communication is smart phone. Number of peoples has their smart phones for daily use. Now with this people are using location based services, which provides service for user who want to know their surroundings. But major issue is privacy of user and server. Existing system provides privacy for both user and server. But it is time consuming at user side because they used grid concept. So when user moves from one region to another, it gets complicated for user to execute query every time and has to follow all the procedure regarding these protocol. Also existing system didn't play role in authentication. Number of Location Based Services is prepaid services. So authentication is necessary for a specific user because entrusted use can use these services in absence of trusted user. We proposed a major enhancement upon previous solution by introducing Authentication and Private Information Protocol to achieve secure solution for both the parties. The solution we present is efficient and practical in many scenarios. We implement our solution on a mobile device to access the efficiency of our protocol.

Keywords: *Privacy Preserving, Authentication Server, Anonymizer, Token*

1. Introduction

There are increasing mobile phone users worldwide. So location technologies can be currently used by wireless carrier operators to provide a good forecast of the user location. Now a days, number of users are use location based services which can provides location aware information.

Location based service is a service accessible with mobile phones; pocket PC's, GPS devices. It is like Google maps, map request. Mobile devices with positioning capabilities (e.g. GPS) facilities access to location based services that provide information relevant to the user's geospatial context. Number of users uses these services for retrieving Points of Interest from their current location. LBS can be query based and provides the end user with useful information such as where is the nearest restaurant?

Basically when user used specific location based service or registered for that, then LBS can provide number of other services like delivery coupons or other marketing information to customer who is in a specific geographical area. Now a days, there are number of user takes advantage of location based services and graph is steal increasing.

But there are certain problems while using LBS that it may collect and use vast amount of information about consumer for a wide range of purpose.

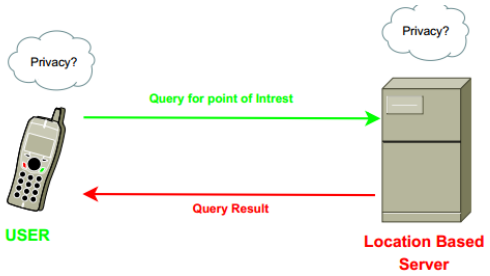


Fig.1 LBS Service

Location information is sensitive and users don't want to share such information to untrustworthy LBS servers. Because number of malicious adversaries may obtain more private knowledge of the user. Also, queries fire by the user having sensitive information about individuals, including health condition, lifestyle habits.

Existing solution for LBS provided privacy for user and server and used two protocols.

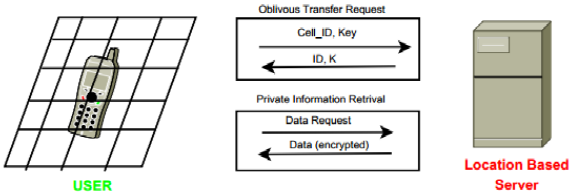


Fig.2 Two level Protocol

*Corresponding author: **Swapnil R. Jadhav**

1) Oblivious Transfer Protocol

The protocol is always carried out between a client P1 and a sender P2.The server P2 has a database of two elements x0, x1 ∈ M. The client P1 can fetch either x0 or x1 so that the server P2 cannot detect which element is fetched.

The client should not learn anything more than xb. Moreover, the client should be always aware of choice b. This protocol provides security for both user and server.

2) Private Information Retrieval

It provides security only for user. PIR protocol allows user to privately retrieve data D[i] without discovering i to server.

This approach provides security for user and server but problem comes when unauthorized user accessing a LBS server. Wireless communication is deeply depends on the internet and internet is an insecure network. LBS is basically provides their services through internet. So we have to secure our LBS service. We have to authenticate all users who are registered for LBS service. So we have used authenticate protocol to provide better security to Location Based Service.

Existing system allow only one query at a time. So that every user has to follow steps required for LBS service all the time. But it takes too much time when user is moving and using LBS service because every time user has to give identity to server. It is time consuming.

In this paper provided authentication protocol for secure service and TTP server treated as anonymizer. This server hides identity of user and plays role of intermediate between user and LBS server.

2. Literature Survey

A) Path Confusion

(R.Paulet et al, 2012) Protecting location privacy through path confusion with the help of path perturbation algorithm that continuously collects location sample from a large group of users. When two users met at one location, this algorithm can cross paths in area. So adversary would confuse the paths of different users. If two users move in parallel, the path perturbation algorithm perturbs the parallel segment into crossing segment. But this algorithm technique is unable to protect time-series location information.

B) Dummy Locations

(M. Duckham et al, 2005) A formal model of obfuscation and negotiation for location privacy This method mainly employs the idea of dummy locations to protect a user's location privacy. These methods propose to generate dummy trajectories in order to confuse the adversaries. In that when user can query to server with their mobile location and parameters, it can be converted into another query having user's real location and k-1 dummy locations and their parameters.

But observe that, privacy is not protected by replacing the real user identity with fake one because in order to process location dependent queries, the LBS needs the exact location of querying user.

C) K-anonymity

(B. Gedik et al, 2005)Location privacy in mobile systems: A personalized anonymization model K-anonymity is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (mobile users), the target object is indistinguishable from the other k – 1 objects.

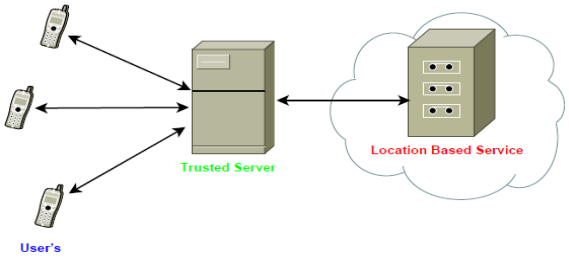


Fig.3 Use of TTP

With this technology it adds one concept ANONYMIZER which is trusted third party. A user sends its location, query and K to the anonymizer, which is a trusted third party in centralized systems or a peer in decentralized systems. The anonymizer removes the ID of the user. TTP regenerate cloak for user location by making K-anonymizer spatial region in which number of k-1 users are involved. Then anonymizer sends the K-ASR and query to the LBS sever, which calculates the candidate results respect to the cloaked region and sends them back to the anonymizer. Then the anonymizer which knows the locations of all the users calculates the actual results and sends them back to the user. There is a enhancement of this system that is rather sending all cloaked region to server, an anonymizer only sends a center of K-anonymizing spatial region (K-ASR). But still there are drawbacks in K-anonymity- (i) If attacker directly gains the access of anonymizer, the privacy of all users is compromised.(ii) At least minimum user should subscribe, otherwise CR cannot be constructed. (iii) User updating is another for making clocking regions. (iv) If user fire query out of the clocked region, user can be easily identified because user will be included in all CRs.

D) Private Information Retrieval

(G. Ghinita et al, 2008) Private queries in location based services: Anonymizers are not necessary The basic idea is to employ PIR to enable the user to query the location database without compromising the privacy of user. Existing system requires clocked region and a

TTP, but it doesn't need of anonymiser and privacy is achieve through cryptographic techniques. Here server forms the region regarding to POI and while answering to query, server first send regions to user. The user finds the region that contains him and utilizes PIR to request all points within that region. So, the server does not know which region was retrieved.

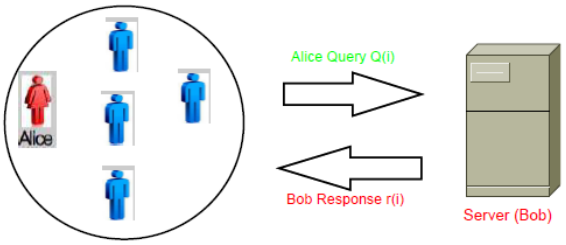


Fig.4 Use of Cloaked Region

But this technique is expensive and high CPU cost. Also user can go through high preliminary test, so extra time required to execute query is greater. Mainly correlation attack can occur due to this approach.

E) Private Queries

(G. Ghinita et al, 2009) A hybrid technique for private location-based queries with database protection Enhancement of hybrid region is that system doesn't use cloaked region. Instead of that use homomorphic encryption to allow the user to privately determine whether his/her location is contained within cell without disclosing his/her coordinates to server. It gives nearest neighbor and prevent user from correlation attack. But still there are certain problems with that system. While using encryption method computational power is increased and it is an expensive query. It doesn't support to the privacy of server's data.

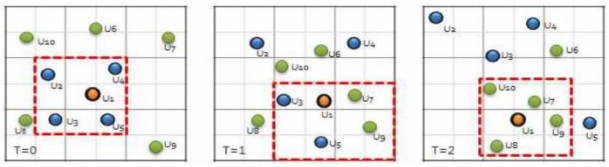


Fig.5 Correlation Attack

F) Oblivious Transfer

(R.Paulet et al, 2014) Privacy-preserving and content-protecting location based queries for enhancement of the private queries this paper introduced the oblivious transfer protocol. The purpose of this protocol is for user to obtain one and only one record from the cell. Also this paper introduced the concept of the Symmetric Key which can be used by both server and user for their private information retrieval phase. But this system didn't play role in authentication. So in insecure network any entrusted user can use LBS service pretend as a trusted user.

This system allows only one query at a time. So that every users has to follow steps required for LBS service all the time. But it takes too much time when user is moving and using LBS service because every time user has to authenticate his account. It is time consuming.

So from above literature survey conclude that our existing system provided better security than others. But this system also didn't take into account a user authentication. Also PIR protocol takes extra time to search query result. So proposed our own system from existing and overcomes drawback in it.

3. Problem Definition

In past few years, number of protocols has been used to secure Location Based Services. Existing system used two protocols which provide security for both user and server. Existing system used grid concept which is incompatible when user is moving continuously from one region to another region. It consumes more time at user side and every time user has to follow all the necessary steps to fire a certain query. All Location Based Services are prepared services. So we have to authenticate all users who are using this service. Existing system doesn't play role in that.

To resolve these problem we need to develop some policies and the model and along with its mechanism to implement that model in real time.

4. Implementation Details

A. Proposed Work

Proposed system use different architecture than our existing system. It can cover all the points in problem statement and provide privacy for both user and server. Also gave better query result than existing system.

Earlier system used grid concept in which user has to select region in that grid and request for database of that region to LBS server. But possibility is that user can't stay at one place for a long time. He can move from one region to another. So every time he has to follow all the necessary steps to execute query.

Our existing system used two protocols. But it takes extra processing time at user side. Also they used indexed databases, so it is difficult to manage these databases. None of existing system provide authentication of user who are going to use LBS. Because number of LBS service are prepaid services. User has to pay before use. So any unauthorized user can access or use these services pretend as a authorized user. So that to encounter this threat and better security, proposed system use authentication server.

a) Authentication Server Module

Here we proposed open authentication for LBS application. There is no need to user to fill up register

form of the application. Only user has to facebook account on social networking site. If user is attached with facebook then he can easily access LBS application without any data fill up. When he can logging with facebook for LBS application, FB OAuth server gives him a token which indicates that he is a valid user. So user sends this token to TTP server for further work.

Results | Messages

	GUID	UserID	LastLogin
1	0bc8b4f5-fb2b-446b-8406-acfcd454abb0	899335853436104	2015-11-04 17:16:13.033
2	110d5350-6b9b-440e-9521-23e2feef4836	896736643747680	2015-11-04 16:32:43.797
3	211b0b5a-0d77-4f70-97b0-f68e8f049c85	902497746482885	2015-11-04 16:12:49.400

Snapshot No.1: GUID of User

Here we used FB OAuth server which is basically used for open authentication. FB server gives a unique token for every user to register for the application. Due to this authentication process, LBS application gets only authorized user which is already have accounts on social networking sites. We can access any other information related to user profile. We can access his DOB and sends him a coupons or any off message on this special day.

b) Trusted Third Party Server Module

Here we proposed one trusted server treated as anonymise server. Third party can handle this server and user has to trust on that. This sever plays a role of intermediate between user and location server.

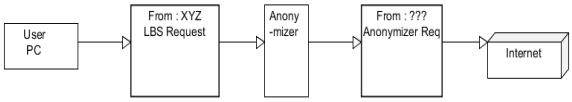


Fig.8: Working of Anonymizer

User sends a FB token to TTP server to register for the application. TTP server validates that token with FB OAuth server. If that token is valid, TTP generates access token which contains GUID. After that TTP register that user and sends him an access token. The whole procedure is encrypted using AES algorithm.

After getting access token user can use ay service which he wants using his GUID which is unique. TTP hides user identification and send only service type and GPS ordinates of user. LBS Server gives a list of locations related with GPS coordinates of use for a particular service type. So that LBS server doesn't know which user is using that application. And server also disclose is data for that particular service type. So that database of server is secured.

So here we provide privacy for both user and server. Also our system reduced time at client and server side.

B. System Architecture

As per discussion in proposed work, our architecture consists of two modules. This system add authentication server to authenticate all registered users who are going to use LBS Service and proposed a anonymize server as a Trusted Third Party (TTP). This server hides identity of user. Using TTP we achieved privacy for both user and server.

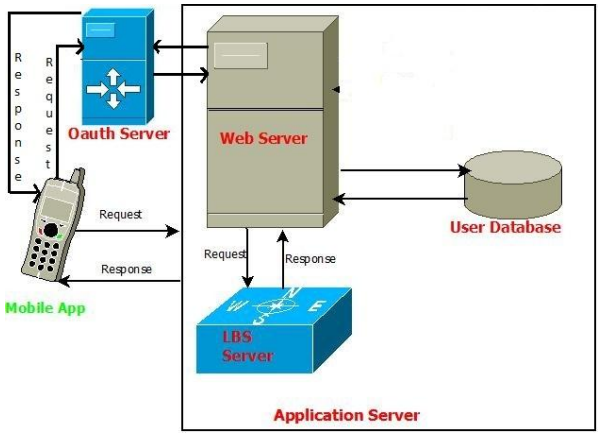


Fig.9 Architecture Diagram

C. Algorithm

- **Authentication and Private Information Retrieval Protocol**

This protocol authenticates all users who are going to use LBS service and provides access token for each user for further use. TTP server hides user's identity from LBS server.

* Algorithm
Input : Lat , Long , Type
Output : List<Locations>
i) C —req.→ FBToken To FB OAuth Server
ii) C ←resp.— [T]
iii)[T] —Validation→ TTP Server
iv) If (Validation == TRUE)
Continue.....
TTP Server —req.→ / ←resp.— User Profile to FB OAuth Server
v) TTP Server —user profile→ DB , User registered Successfully
vi) C ←(Er(Taccess),Secryt key)— TTP Server
vii) C —(dr(Taccess),Secryt key)→ GUID
viii) C —(Er[(Er(service type,lat,long),GUID),GUID],Secryt key)→ TTP Server
ix) TTP Server —(dr[(Er(service type,lat,long),GUID),GUID],secryt key)→ GUID
x)TTP Server —dr(service type,lat,long) using GUID→ LBS Server
xi) LBS Server —List<Locations>→ TTP Server
xii) TTP Server —(Er(List<Locations>),GUID)→ C

5. Mathematical Model

Deterministic Finite Automata (DFA)

DFA is a finite state machine that accepts/rejects finite strings of symbol and only produces a unique computation of the automaton for each input string. Deterministic refers to uniqueness of the computation.

A DFA is defined as an abstract mathematical concept, but due to the deterministic nature of a DFA, it is implementable in hardware and software for solving various specific problems.

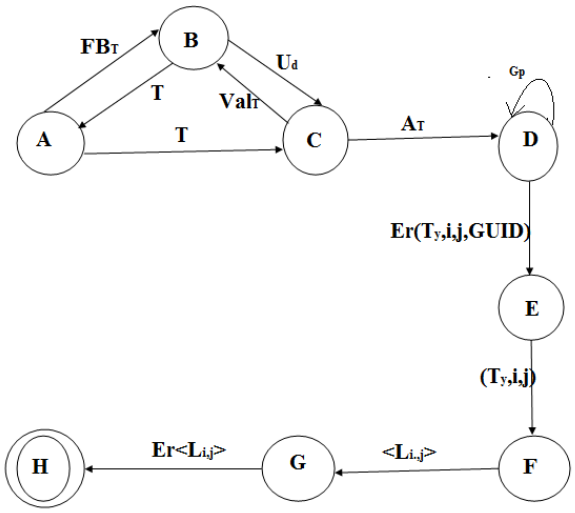


Fig.10 Deterministic Finite Automata

A deterministic finite automaton M is a 5-tuple, (Q, ∑, δ, q0, F) consisting of

- A finite set of states (Q)={A, B, C, D, E,F,G,H}
- A finite set of input symbols called the alphabet(∑)={FBT , T , ValT , Ud ,AT, Ty , i , j , GUID , Li,j , Gp, Er}
- A transition function (δ : Q * ∑ -> Q) = {}
- A start state (q0 € Q) = {q0}
- A set of accept states (F Q)= {q7}

WHERE,
FBT = Facebook Token
T = Token
ValT =Validates token
Ud =User details
AT=Access Token
Ty= Service Token
i = Latitude
j = Longitude
GUID = Global Unique ID
Li,j = List of coordinates
Gp = GPS coordinates
Er = Encrypted data

6. Experimental Evaluation

Basically our proposed system needs three servers. First for authentication, second one for trusted third party and third one for Location based service. Here we used only one TTP server. Facebook has own server for user authentication. So we can only request for token to validate user and gives access token to user. When TTP can communicate for token validation with FB OAuth server, it can request for user profile. Using this profile TTP can generate access token and register that user. And this access token can send to user for using LBS services. This access token contains unique GUID, which will use for encryption and decryption purpose. We used google map as LBS server because this is open source and easy to use.

Proposed system application is developed with android studio. Here we developed application for Location Based Service, so that any user having smart phone with android support can use this service. Experiment is done real time in which used mobile device with internet connection and one server machine. After setup we measured required time to test performance of system. The implementation on the mobile phone platform is programmed using the android development kit, which is java based programming environment. The mobile device used was micromax nitro 310A with octa core 1.7GHz processor and 2GB RAM. The whole solution is executed for 50 trials, where time taken for each service type was recorded and average time was calculated.

System Requirements

1) Software requirement

- Android SDK
- Eclipse
- VS 2012
- SQL SERVER 2008
- IIS 7.0 Server
- Connectify

2) Hardware requirements

- Windows Server
- Mobile device with Android Support

3) Operating System

- Any Android OS

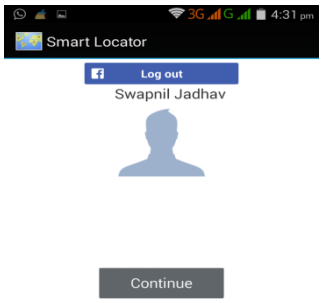
A) Result

First and foremost goal is to provide privacy for both user and server. And also reduce communication time between user and LBS server.

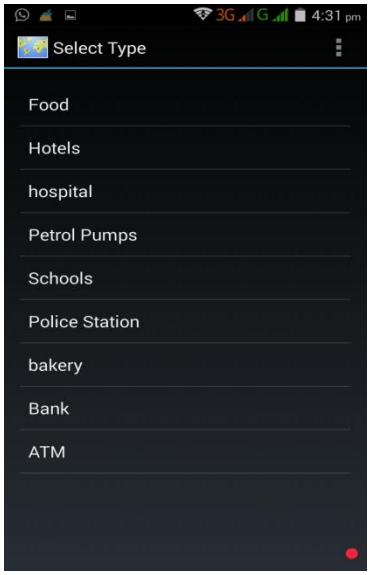
Here we authenticated user of application using FB OAuth server and gives GUID with his access token. Now user can access any service he wants. Till date our system is developed with anonymise server and provided better security than existing system. Our system reduced communication time by fast retrieval of query result from LBS database.

When compared our results with existing system, get result which is better than our existing system. Because earlier system used two protocols namely oblivious transfer and private information retrieval which takes extra processing at user and server side. So it takes extra time to get query result. Propose system remove these algorithms and introduced our

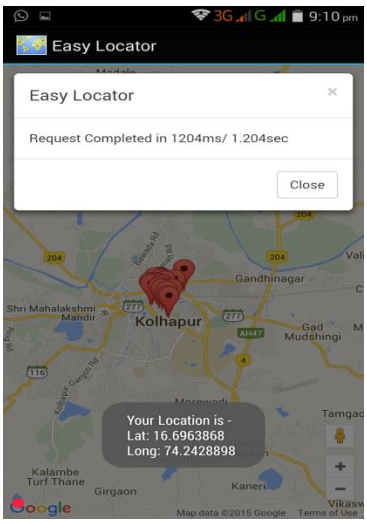
two protocols which can improve security and decrease time to get query result.



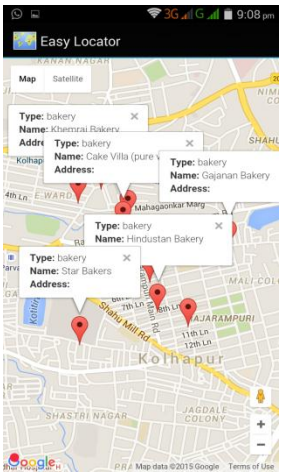
Snapshot No.1: FB Login



Snapshot No.2: Service Selection



Snapshot No.3: Requested Result



Snapshot No.4: Nearby POI

Comparison of PIR and Proposed protocol

Protocol	Average Time (s)
PIR Protocol	24.39
Proposed Protocol	1.204

Conclusion

In this work, our paper firstly summarized the general working of Oblivious and PIR protocol which are used to provide privacy for both user and server. Also, the existing systems are provided with their disadvantages.

This scheme has been proposed to provide better security for Location Based Service and improved query search result. Here proposed two basic modules to improve security and increase search result. First we authenticate user and then registered that user. We reduced extra processing time at user side and user can use this service moving from one place to another continuously.

We analyzed the performance of our protocol and found it to be both computationally and communicational more efficient than existing solution.

Acknowledgment

Thanks to all those who helped me in completion of this work knowingly or unknowingly like all those researchers, my lecturers and friends.

References

R.Paulet, M.GolamKaosar, X.Yi and E.Bertino (2012) , Privacy-preserving and content-protecting location based queries,, Proc. ICDE, Washington, DC, USA, pp. 4453.

G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan (2008), Private queries in location based services: Anonymizers are not necessary, inProc. ACM SIGMOD, Vancouver, BC, Canad, pp. 121–132.

B. Gedik and L. Liu (2005), Location privacy in mobile systems: A personalized anonymization model, in Proc. ICDCS, Columbus, OH, USA, pp. 620–629.

C. Gentry and Z. Ramzan (2010), Single-database private information retrieval with constant communication rate, In Proc. ICALP,L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung,Eds., Lisbon, Portugal, pp. 803–815, LNCS 3580.

G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino (2009), A hybrid technique for private location-based queries with database protection, in Proc. Adv. Spatial Temporal Databases, N. Mamoulis, T. Seidl, T. Pedersen, K. Torp, and I. Assent, Eds., Aalborg, Denmark, pp. 98–116, LNCS 5644.

G. Ghinita, P. Kalnis, M. Kantarcioglu, and E. Bertino (2010), Approximate and exact hybrid algorithms for private nearest-neighbor queries with database protection, GeoInformatica, vol. 15, no. 14, pp. 1–28.

Deepika Nair, Bhuvaneswari Raju (2014), Privacy Preserving in Participatory Sensing, in IJSR,Volume 3 Issue 5

R.Paulet, M.GolamKaosar, X.Yi,and E.Bertino (2014) Privacy-preserving and content-protecting location based queries, in Proc. ICDE, Washington, DC, USA, pp. 44–53

M. Duckham and L. Kulik (2005), A formal model of obfuscation and negotiation for location privacy, in Proc. 3rd Int. Conf. Pervasive Comput., H. Gellersen, R. Want, and A. Schmidt, Eds, pp. 243–251, LNCS 3468.

L. Sweeney (2002), k-Anonymity: A model for protecting privacy, Int. J. Uncertain. Fuzziness Knowl. Based Syst., vol. 10, no. 5, pp. 557–570.

A. Beresford and F. Stajano (2003), Location privacy in pervasive computing, IEEE Pervasive Computer vol. 2, no. 1, pp. 46–55.

B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan (1998), Private information retrieval, J. ACM, vol. 45, no. 6,pp. 965–981.

B. Hoh and M. Gruteser (2005), Protecting location privacy through path confusion, in Proc. 1st Int. Conf Secure Comm, pp. 194–205.