Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 782 – 789

Procedia Computer Science

International Conference on Information Security and Privacy (ICISP 2015), 11-12 December 2015, Nagpur, India.

Controlled Broadcast Protocol for Location Privacy in Mobile Applications

B N Jagdale[a], J W Bakal[b]

[a]*PhD Scholar at G H Raisoni College of Engineering, Nagpur, India*
[b]*Principal, S S Jondhale College of Engineering, Mumbai, India*

Abstract

For privacy protection, many architectures such as trusted third party, cryptography, client side privacy etc. have been proposed. These methods are neither fully support privacy nor efficient. We have proposed limited broadcast based application and one dynamic protocol for cloaking. We have simulated user broadcast model, to achieve location privacy where users are mobile and points of interests (POI) are stationary. Second experiment is a POI broadcast model to achieve location privacy. We have also presented dynamic cloaking protocol that considers speed, direction & location of mobile user for cloaking. We have experimentally recorded the results related to performance, energy and privacy strength. It shows that our system has more social and human value along with commercial attraction.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords: Mobile applications, Location Privacy, Cloaking, k-anonymity.

1. Introduction

Mobile device equipped with positioning capability (e.g. GPS) changing the norms of traditional communication system. To take benefit of LBS services a person must reveal her location to the service. For example, a mobile user

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.053

want to ask information about its nearest hospital has to report her exact location to LBS server. With untrusted service provider reporting private location may lead to privacy threat. So LBS cannot protect the privacy of the user. To protect the privacy attacks several protection mechanisms are available 1) Spatial K-Anonymity-In this query is considered private, if the probability of identifying the querying user does not exceed 1/K, where K is a user-specified anonymity requirement. 2) False Location -In this mechanism user send dummy location along with the correct location for protecting the privacy. 3) Use of Anonymizer- Anonymizer is nothing but Trusted Third Party which resides between user and server for protecting the privacy. 4) False Dummies-In this mechanism user along with the actual query send the dummy query to the server. 5) Access Controls-Access Controls are the access rights given to particular. 6) Cryptography Techniques.-The art of protecting information by transforming it (Encrypting) into an unreadable format, called Cipher Text. Only those who possess a secret *key* can decipher (or *Decrypt*) the message into plain text. 7) PIR Framework-This framework cannot make use of Anonymizer.
Existing technique for protecting location privacy uses TTP -Trusted Third Party. Only location parameter is considered for calculating cloaked area, trust is required among the users and has several drawbacks 1) Anonymizer becomes a bottleneck. 2) Anonymizer is a single point of attack. 3) A large number of users must subscribe to it. 4) Users are not protected against correlation attack. We have implemented 3 scenarios based on broadcast based LBS application in which TTP (i.e. Trusted Third Party) is not used and uses dynamic cloaking. Our motive is to protect user's location privacy by considering mobility of a user.

2. Related Work

In mobile privacy domain, mostly authors have presented the work of privacy with the architectures such as distributed, cooperative and peer to peer. In mobile Computing, database systems in mobile devices supports distributed system of heterogeneous nature[1]. Complex data base processing queries in mobile database system is a challenge in the time and space, however in mobile computing, location dependent queries are the main purpose in the mobile databases. In road network, authors designed anonymous data access to LBS services by users and also demonstrated efficient access of LBS services[2]. However disclosing owner's location data to location server poses challenge and use of encryption can be explored along with data misuse verification of location server. Peer to peer approach has been studied by Chi-yin Chow where special cloaking method[3] is adopted with users speed is considered as parameter. While doing this mobile and stationary entities helps the location based services and that too without indication their exact location. Author have proposed the distributed approach[4, 5] that participates with known infrastructures used in LBS systems. This approach is depending on holomorphic encryption. Computational cost is important to know for this approach. Hassan Takabi and others[6] have presented collaborative approach to achieve location privacy. This methods do not consider trusted party in between but among the collaborating users, confidence is required. In Papers[7, 8,10,11,14], authors have presented effectiveness of private query handling, but quality and performance is not balanced effectively. Moreover authors have explored collaborative[9,12,13] and distributed methods in which privacy strength is improved, but computing and communication overhead is high and even issues related to authenticity are not addressed. Julien and others[15] have analysed effect of non-cooperative mobile nodes to achieve maximum benefit of privacy as an individual. They have simulated this type of study in vehicular networks. Reza Shokri and others[16] have demonstrated Bayesian inference model for location privacy where users querying pattern and lifetime is studied. Moreover real traces are used as data set and finds method is lightweight and less costly.

3. Proposed Research work

3.1 Proposed work

Mobile device equipped with positioning capability (e.g. GPS) changing the norms of traditional communication system. Using LBS services a person have to report their exact location to LBS server. So LBS cannot protect the privacy of the user. Several techniques have been proposed to protect user's location privacy such as centralized privacy-preserving frameworks but it uses TTP (Trusted Third Party),only considers location parameter to form a cloaking area and require trust among the users and TTP could be the system bottleneck or single point of failure.

So we have simulated the broadcast based protocol which overcomes the drawbacks of existing technology.
We have implemented 3 scenarios based on broadcast based LBS application in which TTP (i.e. Trusted Third Party) is not used and uses dynamic cloaking i.e. cloak area is computed by considering the new parameters i.e. speed, direction and location of user i.e. by considering mobility of a user. Considering above 3 parameters for cloaking will help in improving the location privacy strength. We have designed a scheduler which is based on discrete asynchronous event based simulation which schedules all the events such as send, receive request of user as well as POI.

3.2 Problem Definition

To design and implement broadcast based protocol to protect user's location privacy by considering speed, direction and location of user as prime parameters. Moreover it satisfies k-anonymity and improves the location privacy.

Features and objectives:

Study based on mobility: As we are considering speed as a parameter for cloaking so users moving with different speed i.e. walking users, users moving on bike, users driving car etc. can be taken into consideration. *Study based on user density*: User density means we are going to increase the number of queries and see its impact on response *Study based on broadcast frequency*: Different broadcast frequencies are considered for simulation. *New parameters*: Speed, direction, location is considered to compute cloaking and satisfying k (privacy threshold) value. In this method, Querier and other users do not require to trust among each other. In addition, users other than Querier are not necessary to take part in service.
Objectives of this work are as follows. First is enhancing privacy of User broadcast protocol. Second is enhancing privacy of POI broadcast protocol and third is improvement of Dynamic cloaking algorithm with speed, direction and location as new parameter.
Scope of this work is limited to Wi-Fi communication technology which is a 100 meters, cloaking region is considered as area of base station, Speed, direction and location as parameters are considered for cloaking. Simulation works only for 25-30 users because of concept of multithreading.

3.3 Modules

User Broadcast Model

In this we have simulated User broadcast protocol using concept of Asynchronous Discrete Event Based Simulation. In which user or many users broadcast certain LBS query after certain time of interval. Whatever the POI (e.g. Hotel) comes in Wi-Fi range of user and satisfies user query can give response to particular user. In this model we have checked impact of user density, impact of mobility (i.e. speed of users), impact of energy spend.

POI Broadcast Model

In this we have implemented POI broadcast protocol using concept of Asynchronous Discrete Event Based Simulation. In which number of POI (e.g. Hotel) broadcast certain LBS query after certain time of interval. Whatever the user moving on road come in Wi-Fi range of POI and interested in POI query can give response to particular POI. In this model we have checked impact of broadcast frequency, impact of energy spend.

Dynamic Cloaking

In this we have implemented dynamic cloaking algorithm which consider new parameters i.e. speed, direction and location i.e. mobility of user for cloaking region and shown simulation of cloaking algorithm.

3.4 Simulation assumptions

- For simulation of this protocol we have considered 100m road.
- Number of POI i.e. point of interest (e.g. hotel) considered as 50-100.
- POI categories considered as – Hotel, Hospital, Mall.
- User mobility consideration as
  Speed between 5-10km/hr. = Walking users
  Speed between 25-30km/hr. = users on Bike
  Speed between 50-60km/hr. = users driving car

- Every area has Base Station (BS) located. So considered 2 BS (50m area each).Users in respective area can report to particular BS.
- Communication Technology used is Wi-Fi so processing time for POI and for User is considered in Milliseconds.
- Each mobile user can set its privacy level using k value and able to change his/her privacy level.
- In earlier implementation algorithm is executed at TTP and require trust among End-user and other k-1 users.
- In this project we are executing the algorithm on BS and not require trust among End-user and other k-1 users.
- Again earlier implementation uses some algorithm to form Cloaking Region.
- We are using BS area as CR so overhead of calculating CR is reduced.

3.5 Dynamic Cloaking Algorithm

Related Terms:

1. NN Query (Q)
2. Base Station (BS)
3. Cloaking region (CR) -It is the region which contain End-user location along with the other k -1 location. Considered as area of BS.
4. Location Based Server (LBS) – It is the server who has information of all POI.
5. S, D, L Parameter – Speed, Direction Location Parameter.
6. K Value

Algorithm dyna_cloak ()

1. Data [Input: Q, BS, CR], [Output: Q answer]
2. End-user sends Q and K value to BS.
3. BS finds k-1 companions in CR by matching (S, D, and L)
   Parameter with End-user.
4. At BS If (value of k is satisfied)
   BS forward tuple (Q, K, CR) to LBS
   Else Go to step 3
5. LBS execute Q with respect to CR.
6. LBS send range of answers to BS.
7. BS selects satisfied answer from it and sends it to End-user.
8. Stop.

3.6 System model

To benefit from a location-based service, a person must reveal her location to the service. Several k-Anonymity approaches have been used to protect users Location privacy. K-anonymity addresses this threat by cloaking the person's location such that there are at least k−1 other people within the cloaked area. A broadcast based protocol is presented which satisfies k-anonymity technique but to calculate cloak area 3 main parameters are considered which are Speed of User, Direction of User and Location of User. Considering this three parameters helps in improving location privacy strength. To demonstrate this protocol we have considered following scenarios.

3.6.1 Scenario I - User broadcast model to protect privacy

In this scenarios we have considered three main entities as User, POI and communication network.

User: This is the user carrying mobile device having positioning capability i.e. GPS. POI: This indicate any hotel, hospital, mall etc. which broadcast some information regarding any offers, sale etc. If the user query and broadcasted reply from POI matches then user get response of its query form particular of POI. Communication Network: Wi-Fi network is used for communication between users and POI.

Following diagram in figure 1, shows architecture of first scenario. First the user broadcast any LBS query using Wi-Fi as a communication network e.g. "which is nearest hotel". If any POI which satisfies user query comes in Wi-Fi range of the user , then that POI will responds to user query and user get response from particular POI and he

will visit POI and collect required information. User and POI must user same network for communication Wi-Fi.

3.6.2 Scenario II - POI broadcast model to protect privacy

Setup and component terminology is same as indicated in section 3.6.1. User: This is the user carrying mobile device having positioning capability i.e. GPS. POI: This indicates any hotel, hospital, mall etc. which broadcast some information regarding any offers, sale etc. If the user query and broadcasted reply from POI matches then user get response of its query form particular of POI.
Communication Network: Wi-Fi network is used for communication between users and POI. Diagram in figure 2 shows architecture of scenario II. In this scenario POI broadcast any query information related to any offer or sale using Wi-Fi as a communication network. If any user moving on road comes in Wi-Fi range of POI then he will get an alert of that broadcasted information from POI. If user interested in that offer then he will visit the POI. Here also POI and must use same communication network i.e. Wi-Fi.

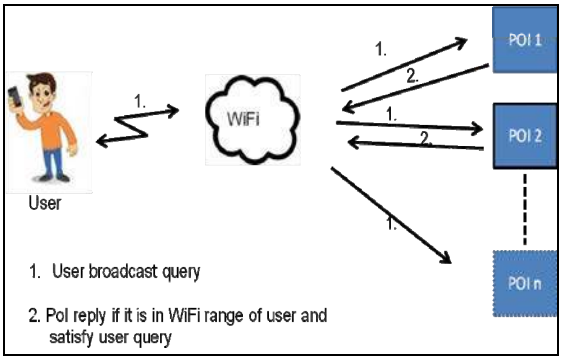

Figure1: Architecture of User broadcast Model

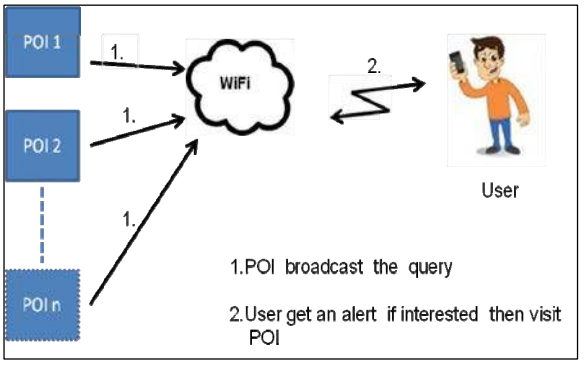

Figure 2: Architecture of POI broadcast Model

3.6.3 Scenario III –Dynamic Cloaking

In this scenarios we have considered four main entities such as LBS Server, Base Station, User and POI.
LBS Server: LBS Server stores all location information about all POI's and that information is used by server to reply for user query. Base Station: Every area has Base station located. Base station knows information of all users in his area. Users in particular area of base station can broadcast his speed, direction to Base Station. Area of base station is considered as Cloaking Region. User: This are the user carrying mobile device having positioning capability i.e. GPS and moving or walking on road. POI: This indicate any shops, hospital etc. which broadcast some information regarding any offers, sale etc. Wi-Fi: Bluetooth or Wi-Fi network is used for communication between user and Server.
Following figure 3 shows architecture of scenario III and in this scenario, we consider traffic on road. Any user on road request for any LBS query. Then proposed dynamic cloaking algorithm is executed on Base station to compute cloaking, satisfying user query and protecting user's location privacy.

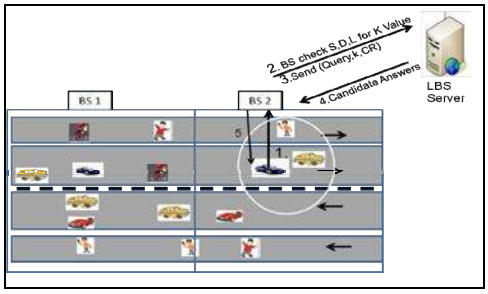

Figure 3: Dynamic cloaking Protocol

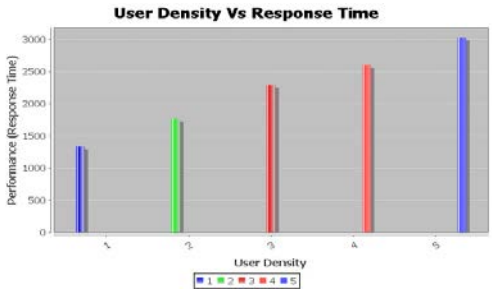

Figure 4: User Density vs. Response Time

User sends his query and k value to the base station. Base station find k-1 companion in his area by matching speed, direction and location of other users with End-user. If at base station value of k is satisfied then it will forward tuple (Query, K, and CR) to LBS. According to this tuple and with respect to the Cloaking Region LBS executes users query and returns set of candidate POIs to Base Station. Base Station selects satisfied POI from the candidate list and sends it to the End-user. Hence user's privacy can be protected by considering speed, direction and location parameter.

4.0 Results and discussions

4.1 User Broadcast Model

4.1.1 User density Vs. Response Time

In this graph (figure 4) of user broadcast model, we measure the response time to process query by varying User density. As number of user increases response time also increases.

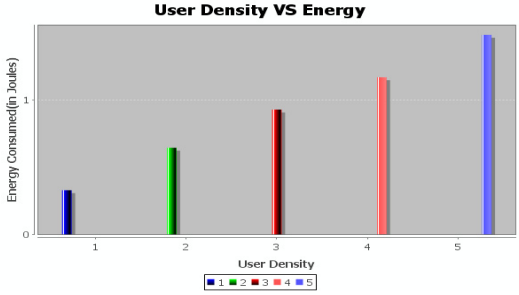

Figure 5: User Density vs. energy

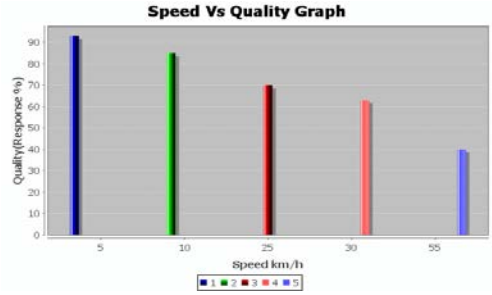

Figure 6: Speed vs. Quality

4.1.2 User Density vs. Energy

In this graph of figure 5, user broadcast model, we measure the total energy spend by user while broadcasting query & energy spend by POI to reply user query by varying user density. More the number of user total energy spend is more.

4.1.3 Speed (User Mobility) Vs. Quality

In this graph of figure 6, of user broadcast model, we measure the quality i.e. reply for the query by varying speed of user. More the speed of user chance of getting reply is missed hence quality degrades

4.2 POI Broadcast Model

4.2.1 Broadcast Interval Time vs. Quality

In this graph of figure 7, POI broadcast model, we measure the quality i.e. replies for the query & receiving query by varying broadcast interval time of POI. More the value of broadcast interval less is the quality.

4.2.2 Broadcast Interval Time vs. Energy

In this graph of figure 8, POI broadcast model, we measure the total energy spend by POI while broadcasting query & energy spend by user to receive /reply POI query by varying broadcast interval time of POI. More the broadcast interval time of POI total energy consumed is less

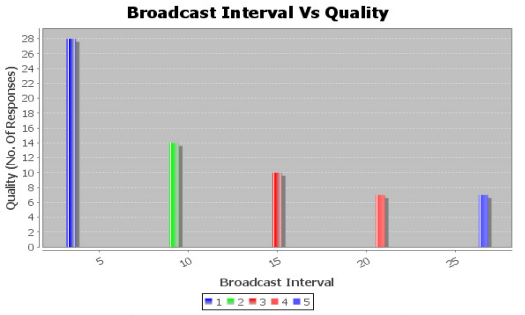

Fig 7: Broadcast Interval vs. Quality

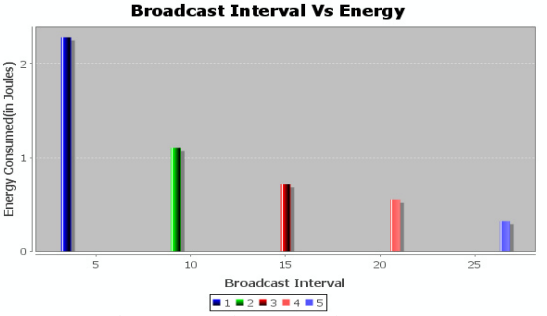

Figure 8: Broadcast Interval vs. Energy

5.0 Conclusions

Broadcast protocol provides more privacy, but cost for broadcast protocol is more. In proposed scheme location privacy is achieved with the help of broadcast, dynamic cloaking algorithm. This approach does not require trust among users for using LBS Service. Methods satisfy basic k- anonymity technique to achieve location privacy.
Our next work is registration & signed POI overhead study, 3D POI model and broadcast frequency estimation to reduce energy consumption.

Acknowledgements

We are thankful to GHRCOE, Nagpur, CSE department and MITCOE Pune, IT department for providing unlimited access to digital library, internet and research lab resources for this work.

REFERENCES:

1. Mehrnoosh Tarafdar and Mostafa S. Haghjoo. Location Privacy In Processing Location Dependent Queries In Mobile Database Systems. 5th *International Symposium On Telecommunications*; 2010.
2. Kyriakos Mouratidis And Man Lung Yiu. Anonymous Query Processing In Road Networks. *IEEE Transactions On Knowledge And Data Engineering*, Vol. 22, No. 1, January 2010.
3. Chi-yin Chow. Mohamed F. Mokbel And Xuan Liu . A Peer-to-peer Spatial Cloaking Algorithm For Anonymous Location-based Service," Acm-gis'06, November 10-11, Arlington, Virginia, USA,2006.
4. Ge Zhong And Urs Hengartner , "Toward A Distributed K-anonymity Protocol For Location Privacy. .In Proceeding Of Wpes'08, Alexandria, Virginia, USA, October 27, 2008,
5. Huang Zhangwei. Xin Mingjun. Distrbuted spatial cloaking Protocol For Location Privacy. Second *International Conference On Networks Security, Wireless Communications And Trusted Computing*,2010.
6. Hassan Takabi.James B. D. Joshi. Hassan A. Karimi. a Collaborative K Anonymity Approach for Location Privacy. *Digital Object Identifier: 10.41ob/ Icst. Collaboratecom*2009. B374, 2010.
7. Gabriel Ghinita1. Panos Kalnis1. Ali Khoshgozaran. Cyrus Shahabi. Kian-lee Tan1. Private Queries In Location Based Services. *Sigmod'08, June 9–12, Vancouver, Bc, Canada*; 2008.
8. Stavros Papadopoulos And Spiridon Bakiras And Dimitris Papadias. Nearest Neighbour Search With Strong Location Privacy. Presented At *The 36th International Conference On Very Large Data Bases*, September 1317,singapore,2010.
9. Mohamed F. Mokbel and Chi-yin Chow. Challenges in Preserving Location Privacy In Peer-to-peer Environment. *Preceding's of Seventh International Conference On Web-age Information Management Workshop*, IEEE, 2006.
10. CHI-YIN CHOW and MOHAMED F. MOKBEL. Casper: Query Processing for Location Services without Compromising Privacy. *ACM Transactions on Database Systems*. Vol. 34, No. 4, Article 24, December 2009.
11. Calvert L. Bowen. Thomas L. Martin . Preserving User Location Privacy Based on Web Queries and LBS Responses. *in Proceedings of the Workshop on Information Assurance*; 2007.
12. Stavros Papadopoulos and Spiridon Bakiras and Dimitris Papadias. Nearest Neighbour Search with Strong Location Privacy. presented at The *36th International Conference on Very Large Data Bases*. September 1317, 2010, Singapore.
13. Anoop Aryan and Sanjay Singh. Securing Location Privacy in Augmented Reality. 2010 *5th International Conference on Industrial and Information Systems, ICIIS 2010*; Jul 29 - Aug 01, 2010, India.

14. Gabriel Ghinital. Panos Kalnis1. Ali Khoshgozaran2. Cyrus Shahabi2. Kian-Lee Tan1. Private Queries in Location Based Services. *SIGMOD'08.*
15. Julien Freudiger. Mohammad Hossein. Jean-Pierre Hubaux and David C. Parkes. Non-Cooperative Location Privacy. *IEEE transactions on dependable and secure computing*. Vol 10, NO 2, March 2013.
16. Reza Shokri, George Theodorakopoulos.Panos Papadimitratos and Ehsan Kazemi. Hiding in the Mobile Crowd: Location Privacy through Collaboration. *IEEE transactions on dependable and secure computing.* VOL. 11, NO. 3, JUNE 2014.