International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Dynamic Framework for Protection of Location Services

DR. MAHESH KANDAKATLA[1]& MS. BITLA PRANATHI[2]

[1]Assistant Professor Department of CSE Vaagdevi Engineering College, Bollikunta, Warangal, and Telangana State, India.

[2]M-Tech Computer Science & Engineering Department of CSE Vaagdevi Engineering College, Bollikunta, Warangal, and Telangana State, India.

ABSTRACT

Location-based services facilitate services for mobile users by getting the current location of a user and user needs to send his location data continuously to the un trusted server to obtain this service. This causes security issue revealing user's private data in the network. In the existing privacy-preserving technique, there are some draw backs while providing these services like it requires a fully-trusted third party, offers minimal security assurance and high range of communication overhead. We define a user-defined privacy grid system known as Dynamic grid system (DGS) which fills the gaps of existing technique for privacy-preserving snapshot and continuous LBS which fulfills below: 1) This requires a semi trusted party which performs the matching operations accurately and it doesn't have access to user's location or private data. 2) Secure snapshot and continuous location privacy is assured. 3) Low communication over head since it depends on POIs of users in his area but not the level of privacy. 4) Extends support to other spatial queries by not changing the algorithms but the required area needs to be sent as spatial regions. From the analysis, it is proved that the DGS is more efficient in terms of privacy preserving than the state-of-the-art technique for continuous location based services.

INTRODUCTION

With the advancement of internet connectivity and mobility, there is an increase in the use of location based services by the users to request their point of interests from various service providers based on their current locations.

This includes finding nearby point of interests (POIs) like restaurants and hotels, traffic information. However, this service can disclose the details about the user to the untrustworthy third party service provider. The movement of the user can be tracked based on the user's details which might lead to reveal user's work location, medical records, political view, most visiting places etc.

Location Based Services (LSB) is used to deliver services based on user's current location from TTP (Trusted third party) or Service Provider (SP). Mostly, LBS is used to request information from various service providers based on their current location based on their Point of Interests like nearby restaurants & stores etc.

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Mobile computing is used in implementing various services for the mobile users, which can be accessed from anywhere. They can be used in Vehicles for Road conditions, weather reports, and other broadcast information through digital audio broad casting.

Location based services are implemented in Mobile devices which have GPS installed in it to send the current location of the user to obtain the Location based services. This process can lead to privacy risks since user gets chance to expose the user's location information in public networks due to the untrusty third party service providers. They can steal the user's valuable information in the network zone with the existing system as the fully TTP model is rarely possible.

SYSTEM ARCHITECTURE:

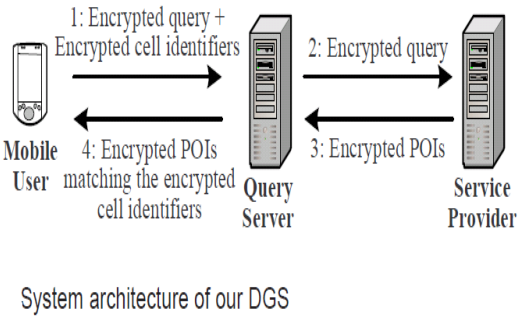


Fig 1. DGS Architecture for LBS

In this approach, a mobile user first sends an encrypted query area along with encrypted grid structure and identifiers to the Query server. As shown in Fig 1, Query server then sends the encrypted query to the Service provider and Service provider fetches the results from the database and returns the results back to the Query server. Finally, Query server send encrypted POIs to the mobile user to decrypt the view the results.

Adversarial models:

In Adversarial Models, we try to provide security by eliminating malicious or not trusted QS and SP which tries know the user's data.

We do not allow QS or SP to access user's information:

Below are the Adversarial Models for DGS:

User anonymity:

Query Server and Service provider de-anonymize the query with the information provided to them in the protocol to find the query results.

QS will avoids the other users from the lists and prefers the users which matches the specific query.

While SP has access to the query region and the grid parameters and cannot know where the user's resides exactly in the query region.

When the SP is paid service, it has to pass through payment gateway which needs user's details for billing. However there are some works of Yau and An , which can give privacy guarantees though there is authentication of user to provide paid service. It can provide better privacy than TTP. While TTP knows exact location of the user and neither QS nor SP know the exact location of the user. It only knows the query area of the user.

In De-anonymization, the type of POI or the density of POIs doesn't have any impact in Query server in providing the information to reduce anonymity set.

One of the choices for Query server is the make use of network service provider. Though network service provide can locate the user's location due cellular networks but when it act as query server it won't.

Other attacks:

There are few other attacks that are existing in Dynamic Grid System for user's location in the network.

IP localization:

One of the attacks for existing system is by determining the IP address of the user by the Query Server by which position of the user can be traced. When comes to Mobile phone networks, the location of the user cannot be located accurately. Because, the IP address can be hidden for the mobile devices by anonymzing software such as tor which can provide privacy for the user's information.

Timing attacks:

The other attacks including timing attacks, in which the Query Server traces the timing information of the user. It observes the traffic close to originating user. However, QS tries to trace the traffic of the user, the privacy can be compromised without the timing attacks since QS holds the query area information of the user's location.

Query server as client:

Sometimes, Query Server tries to gain information of the user's location by acting as Client. QS Doesn't have any information to do this attack, not even approximate location of the user. Also, no of POIs returned to client doesn't allow QS to interfere as it doesn't know about query area or the grid parameters.

Network traffic fingerprinting:

This attack is based on the statistics of encrypted network connections and it is not applicable to existing system. In this attack, Query Server which is used by the user id determined and communicated with Query server in the network traffic.

Commuter problem:

In this attack, attacker can find the home and office location of the user through location traces. Also, this is not applicable to existing system since the user's doesn't pass plain text in the network. Side channel attacks for this out of scope in this paper.

Timing attacks:

It is a side channel attack in which the attacker attempts to compromise a cryptosystem, by analyzing the time taken to execute cryptographic algorithms.

Side channel attack:

It is any attack based on information gained from the physical implementation of cryptosystem.

DYNAMICGRID SYSTEM (DGS):

DGS supports two types of privacy preserving techniques for location based services as below:

a) Range Queries
b) K-Nearest Neighbor Queries

Range Queries:

DGS has mainly two phases in privacy-preserving for continuous range query processing.

The first phase finds the initial answer for range query which is also known snapshot of LBS process.

The second phase finds the query answers for a range query continuously based on the user's updated location.

Range Query Processing:

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

A continuous range query is defined as for a certain time period, the POIs of the users are tracked within the user's specified region which are at certain distance from the user's location.

The main idea of DGS

In this technique, a user first identifies the query area, in which user wishes to reveal the area in which he stays. Then the query area is divided into equal sized grid cells which are created based on the grid structure provided by the user where the user encrypts a query which has the query area information and the dynamic grid structure and encrypts the identity of each grid cell which meets the required search area of the spatial query area to produce a set of identifiers.

In the next step, the user sends a request which includes the encrypted query and the encrypted identifiers to QS. QS is a semi trusted party placed between the user and the service provider. QS Stores the encrypted identifiers and encrypted is sent to specified service provider by the user. Once the user receives the encrypted POIs, the user decrypts and gets the location he wants by computing query answer.

As the user continuously moves and needs information about POIs with in query area, located in other grid cells which are not requested from QS before. QS Simply returns the required POIs whose encrypted identifiers which equals to at least one of the newly needed encrypted identifiers to the mobile user.

When the mobile user get the POIs which are encrypted from QS, user evaluates the query locally. Along with this, when the required search area of a query intersects the location which is away from the present query area, the mobile user logs off the query with QS and re-issues a new query with a new query area.

SECURITY ANALYSIS:

In this phase, we outline several safety models which formalize the place privateness of our DGS, and display that the proposed schemes in section 3 are comfortable. this isn't always the case in our scheme. The challenger prepares the machine parameters, and gives them to A. A specifies a POI-type, the grid shape, a question vicinity and two locations (x0, y0) and (x1, y1) on this location, and gives them to C. C chooses at random b ∈ zero, 1, uses (xb, yb), the required grid shape and POI-kind to generate Msgb 2 with admire to the identity of A, i.e., the message that the malicious SP expects to acquire. C then offers Msgb 2 to A. A outputs a chunk b′ and wins the recreation if b′ = b.

EXPERIMENTAL RESULTS:

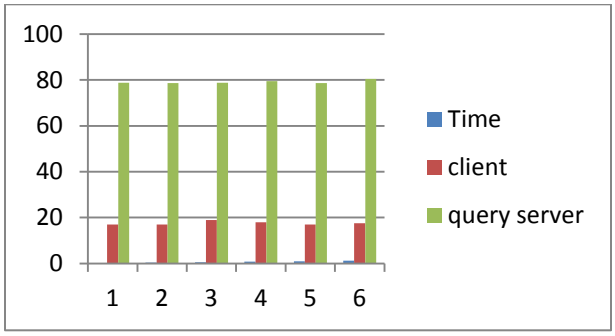
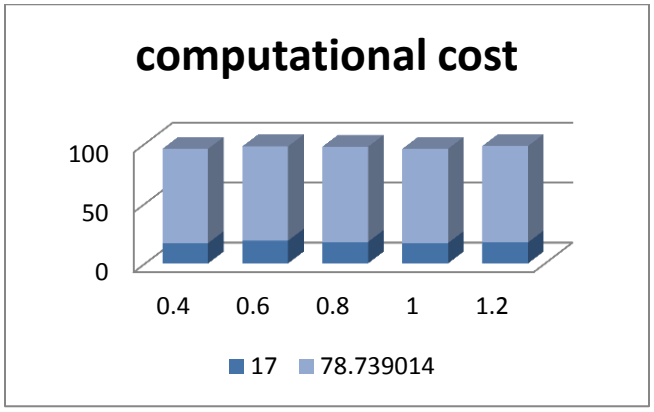


Fig 2. Query Server-Client Communication Cost Analysis



International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Fig 3. System Computational Cost Analysis

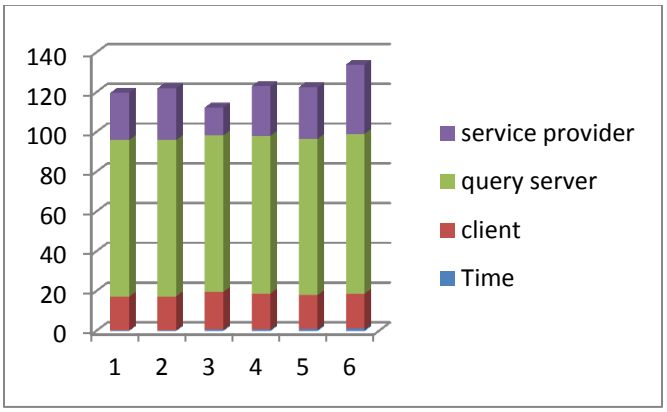


Fig 4. Service Provider-Query Server Communication Cost Analysis

In this Phase, We analyze the performance of DGS on Continuous range queries and k-NN queries based on the simulations. We have applied a continuous spatial cloaking scheme based on the *fully-trusted third party model.* A list of Point of interests is returned by the privacy-secured query processor at service provider via location anonymizer. Finally, the mobile user calculates the desired query results from the received Point of Interests.

Attributes of location based techniques

Accuracy and precision

Different techniques provider different resolutions from centimeters of radio frequency to kilometers from cell ID approaches, measured as degree of accuracy.

Scale

This indicates the location techniques limit where the user device is located like the area size with in which the technique works.

Cost

LBS require a high accuracy with a reasonable cost depends on factors like handset device modification.

Tracking/Positioning

Various Location Based Services techniques are used for Tracking/Positioning of the system using satellite positioning system with reasonable cost and coverage.

Category

This attribute indicates the techniques users whether Satellite Positioning system or Communication Network.

Medium

These medium vary based on the coverage by the system service that it provides. It uses the mediums like Radio Signals, Infrared signals.

POSITIONING TECHNIQUES

Positioning techniques can be applied in two ways Self-positioning and remote positioning. In self-positioning approach, the mobile terminal utilizes the signals which are produced by the gateways/antennas to measure its own position.

Self positioning techniques:

Some of the positioning techniques are GPS and Assisted GPS (A-GPS), Indoor Global Positioning System (Indoor GPS), Mobile Terminal Positioning over Satellite UMTS (S-UMTS)

Remote positioning techniques: Some of the Remote positioning techniques are Cell Identification (Cell-ID), Direction or Angle of Arrival (AOA), Time delay. Two types of methods can be identified under Time delay as Absolute Timing or Time of Arrival (TOA) and Differential Time of Arrival (TDOA) or Hyperbolic Technique

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

Techniques	Accuracy	Cost	Scale / Coverage	Category	Tracking/ Positioning	Mechanism	Medium	Precision
GPS	50-100 meters	Initial cost driven by GPS receiver Maintenance cost is negligible	World Wide	Satellite	Positioning	TOA	Radio	25m
DGPS	10 meters or better	Cost depends on accuracy	World Wide	Satellite	Positioning	TOA	Radio	3m
WAAS	7.6 meters or better	Moderate	World Wide	Satellite	Positioning	TOA	Radio	3m
GSM	10 meters to 15kms	Low	World Wide	Network	Both	COO,AOA, TOA	Radio	Cell, distance in 555m steps
Active Badge	7cm	High	Indoor	Indoor	Tracking	COO	Infrared	Cell
Active Bat	3cm-9cm	Moderate	World Wide	Indoor	Tracking	TOA	Ultrasound/Radio	0.1m
Cricket	4*4ft regions (~100%) (1-2cm)	Low	World Wide	Indoor	Positioning	TOA	Ultrasound/Radio	0.3m
Spot ON	Depends on cluster size	Low	Indoor	Indoor	Tracking	Signal Strength	Radio	3m

Table 2: Overview of comparisons between various positioning systems

Techniques	Accuracy	Cost	Scale / Coverage	Category	Tracking/ Positioning	Mechanism	Medium	Precision
RFID	2cm	Moderate	Indoor	Indoor	Tracking	COO	Radio	Cell
MPS	10m	Moderate	Outdoor (upto 150meters)	Network	Both	COO,AOA,TOA	Radio	150m
Visual Tags	Accuracy tradeoff of 6% error-rate	Low	Outdoor/ Indoor	Indoor	Both	Video	Optical	Depends on camera resolution
Nibble	5–10 m	Moderate	World Wide	Network	Positioning	Signal Strength	Radio	3m
WIPS	Better accuracy with Mobile terminals	Moderate	World Wide	Indoor	Positioning	COO	Infrared	Cell
RADAR	2.37m	Moderate	1-50m Room Scale	Indoor	Both	Electromagnetic Signals	Echo	2-3m

Table 3: Strength and Weakness for various positioning systems

Techniques	Strength	Weakness
GPS	High accurate. No new Infrastructure. Enhanced Privacy for user	Poor service in urban area. Cellular handset modification. Delay in calculating location. Bulky size of receivers
DGPS	Improves GPS Positioning and speed measurement. Enhanced quality of location data. Improves Data Integrity	Limited coverage area. Degrades position accuracy. Limitation of Timing signals
WAAS	Doesn't require additional receiving equipment. Extended Coverage	No exact target location
GSM	Numerous Handset and Service Provider. Quality of calling is better and secured. Consumption power is less	High Roaming call charges. Lose of all data once SIM gets lost
Active Badge	Integrate with other systems. Low Cost. Accurate	Poor Performance in sunlight, significant installation and Maintenance Costs
Active Bat	Influenced by reflection and obstacles between a tag and a receiver	Deploying large number of sensors on the ceiling for each room is Time Consuming task Required ceiling sensor Grid.

Cricket	Good Performance	Mobile Device's Power Consumption. No central management receiver computation
Spot ON	Attenuation measurement using Low-Cost tags	Attenuation less accurate than Time-Of-Light
RFID	Complex Indoor Environments. Cheap Identification and Flexible Wireless technology	Cost of tags is Higher. Need numerous Infrastructure Components
MPS	Error Handling and Network Infrastructure Stability	Provide Services only within Geographic region
WIPS	Higher Location information accuracy	Signal Strength fades with distance and multipath
RADAR	Cost Effective. Reduces Aliasing Effect	Relocation. Needs an initial Data Set

Table 4: Summary of attributes of location technologies

Cellular Networks										
Techniques	**Accuracy**	**Cost**	**Scale / Coverage**	**Category**	**Tracking/ Positioning**	**Mechanism**	**Medium**	**Precision**	**Strength**	**Weakness**
Cell ID/Cell of Origin	200-300 meters	Low Initial Cost. Low Maintenance cost	Limited to availability of Network	Outdoor	Positioning	TOA	Radio	100 to 1000m	Available Now No Handset Modification Easy to implement	Lower Accuracy Loss of Privacy for user
AOA (Angle of Arrival)	100-300 meters	Low Initial Cost. Low Maintenance cost	Limited to availability of Network	Outdoor	Positioning	TDOA	Infrared	up to 500 m	No Handset Modification	Problem with Multipath reception special antennas & receivers at Base station & Privacy Loss

O-TDOA and E-OTD (Time Difference of Arrival)	50-250 meters	Initial and Maintenance Cost is High. Network investment is required	Limited to availability of Network	Indoor	Positioning	TDOA	Infrared	within 50 meters	Good Accuracy Enhanced Privacy for end user	Requires Handset changes Difficult to Implement Requires Location measuring unit
Indoor Localization technique	20-50 meters	Building cost on database for wireless access point. Low Cost	Limited to Network area such as room building, campus and Depends upon Wi-Fi routers	Indoor	Tracking	TOA	Radio	3-5m	Best used for indoor localization of end user. Used in Urban Areas where dense deployment of sensor present	End user should carry badges Dependent upon dense deployment of sensors Gives proximate location information
SLS	High	Low	Good	Outdoor	Tracking	TOA	Radio	100m	Locating/ Tracking people and objects using low cost radio receiver	Ambiguity when two widely spaced antenna elements are used. Insensitive to multipath

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 17
November 2016

RELATED WORK:

1) Anonymous location queries role in Privacy Grid mobile environments:

AUTHORS: B. Bamba, L. Liu, P. Pesti, and T.Wang Privacy Grid assists anonymous location queries in mobile data delivery system. It provides following three services.

a) In first Service, the mobile user can define the preferred location privacy requirement for location hiding measures like location k-anonymity and l-diversity of location and service quality of location measures measures like maximum spatial resolution and maximum temporal resolutions. It uses a model for location privacy knows as Protection Preference Profile model.

b) In second service, Fast and accurate location cloaking algorithms can be derived for location k-anonymity and l-diversity for mobile users. Dynamic bottom-up and top-down grid cloaking is developed to achieve the high anonymization success rate and for efficient time complexity and maintenance cost. To reduce further anonymization time, a hybrid approach to strengthen bottom-up and top-down cloaking techniques is developed.

c) In third service, the success rate of location anonymization is achieved by adopting the temporal cloaking into location cloaking process. Privacy grid can be used to optimize location k-anonymity as per the user requirements.

2) Privacy for disclosed user's location by activating continuous queries.

AUTHORS: C.-Y. Chow and M. F. Mokbel

Currently, Service provider's offers location based services by getting the exact location of the users. Due to untrusted providers, location based services can lead to privacy issues by knowing the user's work locations by tracking the user's location time to time. However, there are some existing techniques for secured location based services for the mobile users and these services are limited since they cannot differentiate location privacy (where user hides his location) and query privacy(where user discloses location but not query) which is critical to provide privacy.

A robust spatial cloaking technique for snapshot and continuous location based services which differentiate location privacy and query privacy is proposed which fulfills the two goals as following:

a) For Customers with public locations, private location based services can be achieved.

b) Spatial cloaking can be performed on demand basis instead of single location service update.

c) Based on the experimental results, it is found that a robust cloaking technique is efficient and scalable for providing anonymity of huge continuous queries without hiding user's locations.

3) Secured Location based Services with personalized k-anonymity: Architecture and algorithms

AUTHORS: B. Gedik and L. Liu

With the advancement in mobile networks and positioning technologies, a demand for location based services has been raised. Some of the applications include location-aware emergency response, location-based advertisement, and location-based entertainment and so on. In all these services, managing privacy of location

Information is critical to protect location privacy for mobile users against the intruders or hackers. In this Architecture, a personalized location anonymization model and location based algorithms.

In this technique, flexible privacy personalization framework is used to assist

location k-anonymity for wide range of mobile users for providing the context sensitive privacy requirements. This is enabled for mobile users to provide minimum level of anonymity as needed and maximum temporal and spatial tolerances that are accepted while seeking k-anonymity safeguarding location based services. An efficient message engine is installed to implement this privacy framework.

This framework is developed to be run by the anonymity server using trusted platform and does location anonymization for mobile users for location based services request like identity removal and spatial temporal cloaking of user's location data.

It effectiveness of location cloaking algorithms can be learnt using realistic conditions of location data which is generated from real road map and traffic volume data. This experiment shows that personalized location k-anonymity model with location perturbation engine achieve high privacy for the location data without any attacks.

4) Anonymous utilization of Location-Based Services using Spatial and Temporal Cloaking

AUTHORS: M. Gruteser and D. Grunwald

With Sensing and tracking technology advancements, location based services came into existence which involves privacy threats. Anonymity assures high range of security and prevents service users to deal with service providers and reduces the service provider's job to protect the user's information.

But the anonymity for the location based services can be guaranteed by requiring the precise location information to be transmitted by the user should not be used for re identifying the subject. We propose middle ware architecture and algorithms for centralized location broker services.

These algorithms can be used for adjusting resolution of location data with respect to the inputs from the users who uses location services.

With automotive traffic counts and catographic material model, spatial resolution for various anonymity constraints can be calculated. Based on this algorithm the median generated is about 125 meters. So with this analysis, the urban areas location based services have the same accuracy. It provides the necessary resolution for finding way in automated bus routing services and services similar to this.

5) Avoiding location-based identity inference in anonymous spatial queries

AUTHORS: P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias

The demand for the location-based services increased with the increase in technology of embedding position services like GPS in mobile device applications.

To succeed these applications, privacy is important. Current techniques depend on encryption to protect network channels and to protect user identities.

CONCLUSION:

In this paper, to preserve privacy by providing continuous LBS, we proposed a user defined grid system know as Dynamic Grid System (DGS). This technique contains a Query Server (QS), Service Provider (SP) and a Cryptographic functions which separates the Query processing tasks in two parts which are operated by Query Server (QS) and Service Provider (SP) separately. This proposed system doesn't need a fully-trusted third party (TTP) but it requires a Query server which is a semi trusted third party and which doesn't store any private data. This helps to overcome the communication over head

due the separation of Query server, Service provider and loads the data easier in expensively between SP and QS.

Also, efficient protocols for DGS to carry both continuous k-nearest-neighbor (NN) and range queries are defined in this system. To analyze the performance of DGS, we resemble DGS to state-of-the-art technique which requires a trusted third party. This result in DGS providing better preservation of privacy than the TTP technique and DGS is more efficient than TTP in terms of communication overhead. Also, the computation cost in DGS is more than TTP in terms of NN queries and slightly expensive for TTP technique for range queries.

REFERENCES

[1] C.-Y. Chow and M. F. Mokbel, "Enabling private continuous queries for
revealed user locations," in *SSTD*, 2007.
[2] T. Xu and Y. Cai, "Location anonymity in continuous location-based
services," in *ACM GIS*, 2007.
[3] J.M. Kang,M. F.Mokbel, S. Shekhar, T. Xia, and D. Zhang, "Continuous
evaluation of monochromatic and bichromatic reverse nearest neighbors,"
in *IEEE ICDE*, 2007.
[4] C. S. Jensen, D. Lin, B. C. Ooi, and R. Zhang, "Effective density queries
of continuously moving objects," in *IEEE ICDE*, 2006.
[5] P. Golle and K. Partridge, "On the anonymity of home/work location
pairs," in *Pervasive Computing*, 2009.
[6] C.-Y. Chow, M. F. Mokbel, and W. G. Aref, "Casper*: Query processing
for location services without compromising privacy," *ACM TODS*,
vol. 34, no. 4, 2009.
[7] T. Xu and Y. Cai, "Feeling-based location privacy protection for locationbased
services," in *ACM CCS*, 2009.
[8] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private
queries in location based services: Anonymizers are not necessary,"
in *ACM SIGMOD*, 2008.
[9] M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, "Where's that
phone?: Geolocating ip addresses on 3G networks," in *ACM SIGCOMM
IMC*, 2009.

Authors Profiles:

Dr. Mahesh Kandakatla earned his PhD from OPJS University Rajasthan, India. Presently, working at Vaagdevi College of Engineering as a Assistant Professor and his research interests include Data Mining, Network Security and Adhoc Networks.
Mail ID: maheshkandakatla@gmail.com

Ms. Bitla Pranathi is pursuing M.Tech degree in Computer Science & Engineering in CSE Department in Vaagdevi Engineering College, Telangana State, India.

Mail id: bitlapranathi@gmail.com