# A Collaborative Approach to Enhance Security in Location Based Services by Answering Range Queries in WSN

[1]Anandhi, [2]S.Amudha
[1]Student, [2]Assistant Professor
[1]Software Engineering,
SRM University, Chennai, India

***Abstract* - We propose a privacy preserved location monitoring system using wireless sensor network. Here we are using two localized algorithms such as Resource aware algorithm and Quality aware algorithm. Our aim is to provide high quality privacy preserved Location Based Services for the user. If user is giving query , person will receive only aggregate location information based on K-anonymity value which prevent privacy breach in their transaction. By giving latitude and longitude value the user can receive updated location information. The aggregate location contains a cloaked region with number of monitored person residing in that region. In cloaked region there will be N persons in M region The user can get their location information by answering range queries. The system will give high quality privacy preserved location based services for individual persons .If the user is authorized user PIR(Private Information Retrieval) also possible in secure manner. The implementation is done using J2EE technology. Finally this result also compare with lots of existing technologies.**

***Index Terms* - Location privacy Resource aware, Quality aware algorithm, Aggregate location, KNN query, PIR.**

## I. INTRODUCTION

Mobile devices, such as smart phones and PDAs, are playing an increasingly important role in people’s lives. Location based services take advantage of user location information and provides mobile users with a unique style of resource and services. Nowadays more and more location-based applications and services provides users about their locations information. As location proof plays a critical role in enabling these applications, they are location-sensitive. The common theme across all these applications is that they offer a reward or benefit to users locating them in a certain geographical location. But users wants their exact locations to be pointed. There are many kinds of location-sensitive applications. One category is location-based access control. Today’s location-sensitive service relies on user’s mobile device to determine its location and send the location to the user. Till now we can only find the area postal code. To address this issue, we propose A Privacy Preserved Location Monitoring in WSN which is used to find and update their personal location information by using the authorized access from the server.

A web portal link is designed and credentials will be given for every user. All the user credential information are maintained in the server. The System can be implemented with the existing network infrastructure and the current user module using Java Technology , and can be easily deployed with Netbeans IDE. Extensive experimental results show that our scheme, besides providing location of the device and also maintain the updated history.

Location Services use the geographical location of mobile user equipment to offer a range of value added services to consumer and enterprise users. Location Based technologies offer the opportunity to deliver contextual services. As such services are specifically orientated towards the position of the mobile handset it enables to provide services that are more targeted and effective.

.

## II. RELATED WORK

The location and Research and development of location based services has been in progress since the early 1990’s. The mandatory use of LBS technology for emergency location purposes began in 1996.T. Xu and Y. Cai designed a model which allows a user to express her privacy requirement by specifying a public region, which the user would feel comfortable if the region is reported as her location. The popularity of the public region, measured using entropy based on its visitors' footprints inside it, is then used as the user's desired level of privacy protection. With this model in place, we present a novel technique that allows a user's location information to be reported as accurate as possible while providing her sufficient location privacy protection.

Ledan shou, He Bai demonstrated the effectiveness of quality of various search services on internet. they propose PWS framework called UPS,where user queries and profiles can be preserved.by using Greedy Dp and Greedy Il for runtime generalization.Profile based web search used to improve quality of web search,on the other hand it will hide privacy contents.Each client accessing search service,privacy protection is an online profiler implemented as a search proxy running on client machine itself(offline,online) .Anusuriya Devaraju ,Simon Beddus describe the development of location-based service components using Java technologies. The technologies include J2ME, Servlet , Java Server Pages (JSP) and XML Java

Binding Tool. The developed components are the location server simulator, location service application and device client application.

This paper is structured into several parts. The first part opens discussion leads to the formulation of the problem that is to be analyzed. The second part contains theory; focusing on basic concepts and technologies to build LBS. The third part presents design and development of each component in the system. In the last part, the future and open work items are clarified and conclusions are presented.

## III. BASIC CONCEPTS AND TECHNOLOGY

In order to develop location-based service system, the location APIs, protocols, technologies and infrastructure of LBS must be understood and reconciled.

### 3.1 Introduction

In WSN location privacy is main concern nowadays. Location-dependent systems are realized by using either identity sensors or counting sensors. **Identity sensors,** each individual has to carry a signal sender/receiver unit with a globally unique identifier, the system can pinpoint the exact location of each monitored person. **Counting sensors** are deployed to report the number of persons located in their sensing areas to a server.

### 3.2 Positioning technology

There are two basic of positioning a mobile device, firstly by using satellite for instance, Global Positioning system (GPS); secondly by using mobile telephone network. This section will discuss the most prominent network based positioning, the Global System for Mobile Communications or GSM. GSM is the leading digital cellular radio network. While the current GSM system was originally designed with an emphasis on voice sessions, the General Packet Radio Service (GPRS) system brings the packet switched bearer services to the existing GSM system. GPRS uses the bandwidth more efficiently because it does not require a dedicated line. The call charging is solely based on amount of transmitted data.

### 3.3 Positioning method

The common positioning methods found basis for providing location services in all networks is the Cell-based Positioning. This method provides a location coordinate based on the cell the subscriber is within. The location infrastructure contains information on the location coordinate of each cell centric. The current Cell ID can be used to identify the Base Transceiver Station (BTS) that the device is communicating with and the location of that BTS. The accuracy of this method depends on the size of the cell. Positioning is generally more accurate in urban areas with a dense network of smaller cells. Rural areas have a lower density of base stations.

### 3.4 Types of Sensors

| SENSOR NAME | UNIQUE FEATURE | PROBLEMS | EXAMPLES |
|---|---|---|---|
| **Identity Sensor** | **Individual has to Carry A signal sender/receiver unit with a globally unique identifier** | **System can Pinpoint the exact location of each monitored person** | **Bat & Cricket** |
| **Counting Sensor** | **Report the number Of persons located in their sensing areas to a server.** | **Not Privacy Preserved** | **Photoelectric sensors and Thermal Sensors** |
| **Privacy Preserved Sensor** | **Privacy Preserved** | **PIR& Probabilistic techniques** | **-** |

## IV. PROBLEM IDENTIFICATION

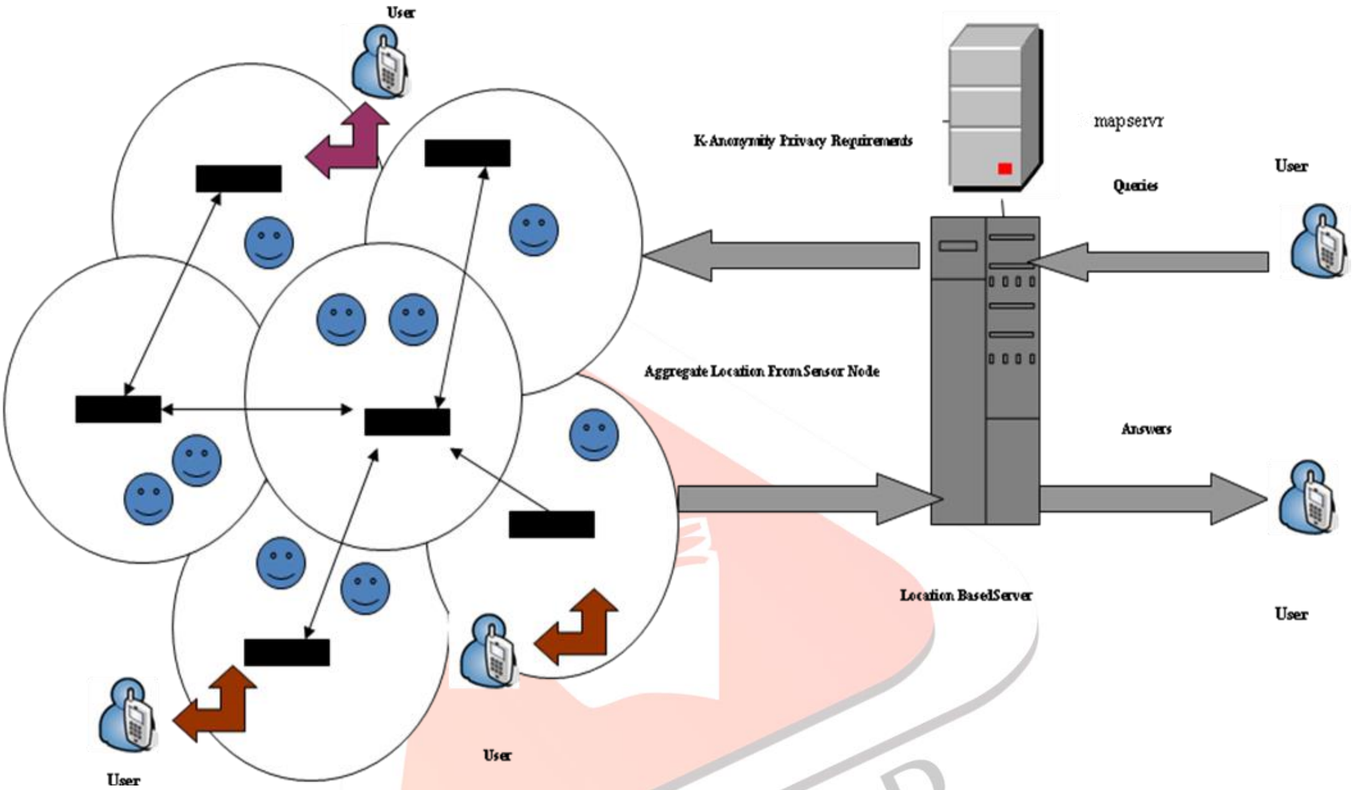
In Existing system ,system can pinpoint exact location of each monitored person, no privacy is preserved.

- **False dummies**

- **Landmark objects**
- **Location perturbation**
- **Avoid location tracking**

The accuracy is low since the query results are correct only at the time instances of periodic updates, but not in between them or at any time of deviation updates. The updates are performed regardless of the existence of Queries a high update frequency may improve the monitoring accuracy, but is at the cost of unnecessary updates and query reevaluation. The privacy issue is simply ignored by assuming that the clients are always willing to provide their exact positions to the server. So ,In Existing system individual person data can be viewed.

## V. PROPOSED SYSTEM ARCHITECTURE


User
K-Anonymity Privacy Requirements
mapservr
Queries
User
Aggregate Location From Sensor Node
Answers
Location BasedServer
User
User
User

The following steps describe the interaction between components in the system.

1. This system is a Java Swing API client application which supports location information view by using latitude and longitude values. New Location updation also possible. The mobile id, username and password are sent to the location service application via HTTP to request the map of the subscriber.
2. When the location service application receives the request, it identifies the subscriber and the service requested by the subscriber.
3. If the user is not registered they have to complete proper registration to access location based services like person, hotel and Café details etc.
4. After successful login the Location Monitor Server will display location details such as Region name ,Coverage range and Number of Monitored person residing in that region based on K-Anonymity values.
5 .Then if the user send range values the server will display region name and number of person in that region.
6. After successful login if the user want to retrieve their personal details that also possible in secure manner.

## VI. MODULE DESCRIPTION

**NETWORK TOPOLOGY**

1) **Sensor Nodes**
2) **Server**
3) **Users**
4) **PRIVACY MODEL**
5) **AGGREGATE LOCATION**
6) **BROADCASTING.**
7) **KNN QUERY EVALUATION**
8) **PIR MODULE**

### 6.1 Sensor nodes

It will sense the number of person in a monitored area.Sensor nodes blurs its sensing area into a cloaked area, which includes N objects, and reports with the number of objects located in exact location as an aggregate location ,it transfer information to the server

### 6.2 Server

Server collects aggregate location from sensor nodes. using a spatial histogram to estimate the distribution of the monitored objects. Also server answers range queries raised by users, based on the estimated object distribution.

The system provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques. Each sensor node is responsible for location and sensing area.

Administrator can change the anonymized level k of the system at anytime by disseminating a message with a new value of k to all the sensor nodes.

### 6.3 User

Each and every user updates their location information to sensor node, user can issue range queries to the system through the sensor nodes. They can get reply for query like, what is the number of persons in a certain area? The server uses the spatial histogram to answer their queries.

### 6.4 Privacy model

Sensor node constitute a trusted zone communicate with each other through secure Network channel to avoid internal network attacks. eg, eavesdropping, traffic analysis ,malicious nodes. The system provides anonymous communication between the sensor nodes and the server by employing existing anonymous communication techniques.

### 6.5 Aggregate location

Sensor node blurs its sensing area into cloaked area in which at least k persons are residing Each sensor node reports only aggregate location information, which is in a form of a cloaked area A, along with the number of persons, N, located in A, where N ≥ k, to server.

### 6.6 Broadcasting

The system model guarantees each sensor node knows an adequate number of objects to compute a cloaked area. To reduce communication cost, this step relies on a heuristic that a sensor node only forwards its received messages to its neighbors when some of them have not yet found an adequate number of objects.

### 6.7 KNN Query evaluation

In privacy Preserved Location monitoring system, we can add location based KNN(K-nearest Neighbor) query. The location based KNN query can be arrived for getting best query services for user.

### 6.8 PIR MODULE

If user is a authorized user for a particular person ,so that user can know the details of the particular person ,if not authorised user , The user cannot know the details about specific person like location,data related to that specific person

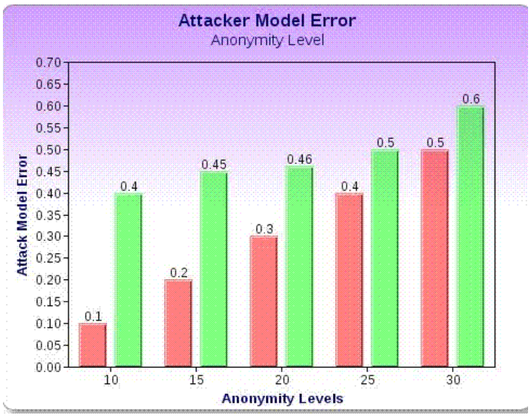
## VII EXPERIMENTAL RESULTS AND ANALYSIS

In this section, We analyze the experimental results with respect to the privacy protection and the quality of location monitoring services of our system. The evaluation of our system is based on the following criteria

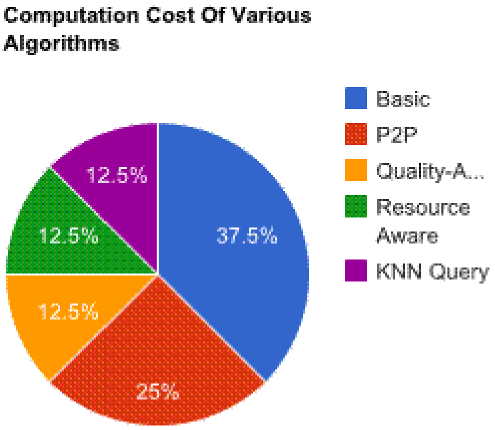
7.1 **Attack model error.** This measures the resilience of our system to the attacker model by the relative error between the estimated number of objects N' in a sensor node's sensing area and the actual one N. The error is measured as [ N'- N ] / N . When N = 0, we consider N' as the error.

The basic idea about attacker model error is the attacker cannot infer the location information corresponding to an individual object directly. We consider the worst-case scenario if the attacker knows the map layout of the system, the location of each sensor node, the sensing area of each sensor node, the total number of objects currently residing in the system based on GSM and GPRS technology then data fusion may happened.

Attacker model is defined as: Given an area A (that corresponds to the monitored area of a sensor node) and a set of aggregate locations R={R1;R2; . . .;R[n] overlapping with A, the attacker estimates the number of persons within A. In this figure the red line is Resource Aware Algorithm and Green lines are Quality aware algorithms. When the anonymity level is high the efficiency of the system is also high based on this algorithms.



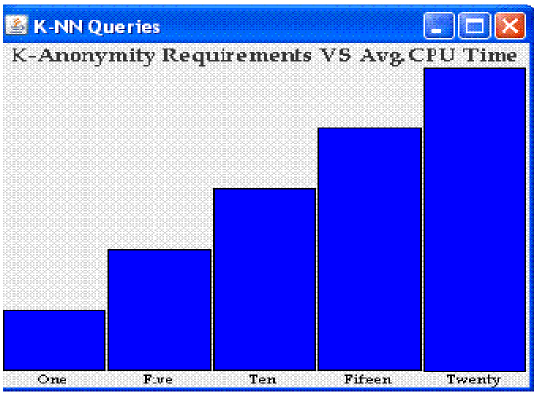
**7.2 Communication cost.** We measure the communication cost of our location anonymization algorithms in terms of the average number of bytes sent by each sensor node per reporting period. This metric also indicates the network traffic and the power consumption of the sensor nodes. **Cloaked area size** measures the quality of the aggregate locations reported by the sensor nodes. The smaller the cloaked area, the better the accuracy of the aggregate location is.



We measure the computational cost of our location anonymization algorithms in terms of the average number of the MBR computations that are needed to determine a resource or quality-aware cloaked area. We compare KNN-Query algorithm with a basic approach ,P2P ,Quality aware, Resource Aware, which computes the MBR for each combination of the peers in the required search space to find the minimal cloaked area. The basic approach does not employ any optimization techniques proposed for our quality-aware algorithm.

### 7.3 Anonymization Strength

When the anonymity level gets stricter, our algorithms generate larger cloaked areas,which reduce the accuracy of the aggregate locations reported to the server. This figure shows that the attacker model error reduces, as the number of objects gets larger. This is because when there are more objects, our algorithms generate smaller cloaked areas, which increase the accuracy of the aggregate locations reported to the server.



## VIII .FUTURE WORK AND CONCLUSION

In this paper, we propose a privacy-preserving location monitoring system for wireless sensor networks. We design two in-network location anonymization algorithms, they are, resource and quality-aware algorithms, that preserve personal location privacy, while enabling the system to provide location monitoring services. Both algorithms rely on the well-established k-anonymity privacy concept that require a person is indistinguishable among k persons. In our system, sensor nodes execute our location anonymization algorithms to provide k-anonymous aggregate locations, in which each aggregate location is a cloaked area A with the number of monitored objects, N, located in A, where N _ k, for the system. The resource-aware algorithm aims to minimize communication and computational cost, the quality-aware algorithm aims to minimize the size of cloaked areas in order to generate more accurate aggregate locations.by using KNN query individual person data cannot be viewed. In If user is a authorized user for a particular person ,so that user can know the details of the particular person ,if not authorised user , The user cannot know the details about specific person like location,information and personal information for that specific person.

This project has focused on mobile location service solution developed using Java. A wide range of Java technology has been introduced to build components in the system. The deployment of Java in building location-based applications provides benefits, which include ease of use, cross-platform architecture, language simplification, and access to the Internet's established Java API development.

In future we can use high complex cryptographic algorithms to ensure high security in the authentication part.Multiway authentication factor such as RFID,Biometric and face recognition can be considered as future enhancement in this paper to include some more enhancement in the existing systems.

## VIII. References

[1] A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster, “The Anatomy of a Context-Aware Application,” Proc. ACM MobiCom,1999.

[2] N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, “The Cricket Location-Support System,” Proc. ACM MobiCom, 2000 .

[3] B. Son, S. Shin, J. Kim, and Y. Her, “Implementation of the Real-Time People Counting System Using Wireless Sensor Networks,”Int’l J. Multimedia and Ubiquitous Eng., vol. 2, no. 2, pp. 63-80, 2007.

[4]OnesystemsTechnologiesCountingPeopleinBuildings,”http://www.onesystemstech.com.sg/index.php?option=com_content&task=view&id=10, 2009

[5] Traf-Sys Inc., “People Counting Systems,” http://www.trafsys.com/products/people-counters/thermal-sensor.aspx, 2009.

[6] M. Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, “Privacy-Aware Location Sensor Networks,” Proc. Ninth Conf. Hot Topics in Operating Systems (HotOS), 2003.

[7] G. Kaupins and R. Minch, “Legal and Ethical Implications of Employee Location Monitoring,” Proc. 38th Ann. Hawaii Int’l Conf.

[8] Location Privacy Protection Act of 2001, http://www.techlawjournal.com/cong107/privacy/location/s1164is.asp, 2010.

[9] D. Culler and M.S. Deborah Estrin, “Overview of Sensor Networks,” Computer, vol. 37, no. 8, pp. 41-49, Aug. 2004